Fully Secure Unbounded Inner-Product and Attribute-Based Encryption

Tatsuaki Okamoto
NTT
okamoto.tatsuaki@lab.ntt.co.jp

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

November 28, 2012

Abstract

In this paper, we present the first inner-product encryption (IPE) schemes that are *unbounded* in the sense that the public parameters do not impose additional limitations on the predicates and attributes used for encryption and decryption keys. All previous IPE schemes were *bounded*, or have a bound on the size of predicates and attributes given public parameters fixed at setup. The proposed unbounded IPE schemes are *fully (adaptively) secure and fully attribute-hiding* in the standard model under a standard assumption, the decisional linear (DLIN) assumption. In our unbounded IPE schemes, the inner-product relation is generalized, where the two vectors of inner-product can be different sizes and it provides a great improvement of efficiency in many applications. We also present the first *fully secure unbounded* attribute-based encryption (ABE) schemes, and the security is proven under the DLIN assumption in the standard model. To achieve these results, we develop novel techniques, *indexing* and *consistent randomness amplification*, on the (extended) dual system encryption technique and the dual pairing vector spaces (DPVS).

Contents

1 Introduction

1.1 Background

1.1.1 IPE and ABE

The notions of *inner-product encryption* (IPE) and *attribute-based encryption* (ABE) introduced by Katz, Sahai and Waters [7] and Sahai and Waters [20] constitute an advanced class of encryption, *functional encryption* (FE), and provide more flexible and fine-grained functionalities in sharing and distributing sensitive data than traditional symmetric and public-key encryption as well as identity-based encryption (IBE).

In FE, there is a relation $R(v, x)$, that determines whether a secret key associated with a parameter v can decrypt a ciphertext encrypted under another parameter x. The parameters for IPE are expressed as vectors $\vec{x}$ (for encryption) and $\vec{v}$ (for a secret key), where $R(\vec{v}, \vec{x})$ holds, i.e., a secret key with $\vec{v}$ can decrypt a ciphertext with $\vec{x}$, iff $\vec{v} \cdot \vec{x} = 0$. (Here, $\vec{v} \cdot \vec{x}$ denotes the standard inner-product.) 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) or (monotone) span program 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, where a secret key can decrypt a ciphertext, 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).

For some applications, the parameters for encryption are required to be hidden from ciphertexts. To capture the security requirement, Katz, Sahai and Waters [7] introduced *attribute-hiding* (based on the same notion for hidden vector encryption (HVE) by Boneh and Waters [5]), a security notion for FE that is stronger than the basic security requirement, *payload-hiding*. Roughly speaking, attribute-hiding requires that a ciphertext conceal the associated parameter as well as the plaintext, while payload-hiding only requires that a ciphertext conceal the plaintext. A weaker notion of attribute-hiding than the original one [7] was given by [8]. The weaker notion is called *weakly attribute-hiding*, and the original one is *fully attribute-hiding*. Informally, in the fully attribute-hiding, the secrecy of attribute x is ensured even against an adversary having a secret key with v such that $R(v, x)$ holds (i.e., no information is released on x except $R(v, x)$ holds), while it is ensured only when $R(v, x)$ does not hold in the weakly attribute-hiding (see Definition 5 for the definition of the fully attribute-hiding).

To the best of our knowledge, the widest class of attribute-hiding FE is IPE [7, 8, 14, 16] (KSW08, LOS^{+}10, OT10 and OT12 schemes). Inner-products for IPE represent a fairly wide class of relations including equality tests as the simplest case (i.e., anonymous IBE and HVE are very special classes of attribute-hiding IPE), disjunctions or conjunctions of equality tests, and, more generally, CNF or DNF formulas. We note, however, that inner-product relations are less expressive than a class of relations (on span programs) for ABE, while existing ABE schemes for such a wider class of relations are not attribute-hiding but only payload-hiding.

Among the existing IPE schemes, only the OT12 IPE scheme [16] achieves the *full (adaptive)* security and *fully attribute-hiding* simultaneously, whereas other attribute-hiding IPE schemes [7, 13, 8, 14] are selectively secure or weakly attribute-hiding, and some IPE schemes [1, 15] only achieve payload-hiding. As for ABE, Lewko et.al. and Okamoto-Takashima ABE schemes [8, 14] are fully secure in the standard model, while ABE schemes [20, 6, 18, 22] before [8, 14] were *selectively* secure.

1.1.2 Unbounded IPE and ABE

All previous constructions of IPE and ABE except the Lewko-Waters ABE scheme [11] have restriction, or are *bounded*, in the choice of the parameters for secret key and encryption once the public parameters have been set. The only *unbounded* ABE scheme [11], however, is *selectively* secure, while they presented an *unbounded* hierarchical identity-based encryption (HIBE) that is *fully secure* in the standard model. No *unbounded* IPE scheme has been presented. Therefore, no *fully secure* and *unbounded* scheme for an advanced class of encryption like IPE or ABE has been presented.

In practice, it is highly desirable that the parameters for secret key and encryption should be flexible or *unbounded* by the public parameters fixed at setup, since if we set the public parameters for a possible maximum size (e.g., the maximum dimension of predicate and attribute vectors for IPE), the size of the public parameters should be huge.

Removing the restrictions for fully secure IPE and ABE, however, is quite challenging. As mentioned above, no *fully secure* and *unbounded* scheme for an advanced class of encryption like IPE or ABE has been presented. The difficulty resides in the existing techniques for proving the *full (or adaptive) security* of such an advanced class of encryption.

The only known technique to prove the full security of an (attribute-hiding) IPE or ABE system is the dual system encryption by Waters [21] and its extension [16]. In the techniques, information theoretical arguments (e.g., conceptual change due to the same distribution and the independent randomness of two distributions etc.) over some (hidden) parts of a secret-key and challenge ciphertext play a key role in the security proof, provided that the adversary follows the secret-key-query condition in the security games. To execute a security proof based on the information theoretical arguments, an appropriate distribution of randomness consistent with the key-query condition should be supplied in the proof games transformed from the original proof game.

As for *bounded* IPE and ABE schemes, the public parameters can supply immanent randomness enough for the arguments, since the size of parameters for secret-keys and encryption is bounded by the public parameters. For example, when the dimension of vectors for IPE is required to be n, the public parameters whose size is $O(n)$ with respect to n should be given in *bounded* IPE, and the size of secret randomness to generate the public parameter is $O(n^2)$. Such an amount of randomness can be enough for the arguments over n-dimensional vectors.

In contrast, for *unbounded* IPE and ABE schemes, some (unbounded amount of) randomness whose distribution is consistent with the key-query condition should be supplied in addition to the randomness provided by the public parameters. For example, even when the dimension of vectors for IPE is required to be n, the size of the public parameters is $O(1)$ in *unbounded* IPE, i.e., the size of secret randomness to generate the public parameters is $O(1)$. Clearly, such a size of randomness is not sufficient for the information theoretical arguments over n-dimensional vectors. Therefore, any additional source of randomness should be provided, and the distribution of the randomness should be specific (i.e., consistent with the key-query condition). For the unbounded HIBE scheme [11], where the equality (un-)matching is the key-query condition, a simple compression technique works well to create such randomness since equality can be simply compressed with preserving the property. The key-query condition for IPE and ABE, however, is in general much more complicated than just the equality matching for (H)IBE, and no technique was known to create randomness consistent with such a complicated condition in some security proofs. This is a reason why [11] succeeds in realizing a fully secure unbounded HIBE but not for ABE (and not for IPE).

1.1.3 Restriction on IPE

The existing IPE schemes have another restriction on the parameters (i.e., vectors) for secret key and encryption that the dimensions of $\vec{x}$ (for encryption) and $\vec{v}$ (for a secret key) should be equivalent. Such a restriction may be considered to be inevitable for the inner-product relation on $\vec{v}\cdot\vec{x}$, but it is required to be relaxed in various applications to improve the efficiency, especially in *unbounded* IPE systems where the setup (public) parameters give no restriction on the dimensions of vectors.

Let us consider an example on a genetic profile data of an individual. It is desirable that such a sensitive data be treated as encrypted data even for data processing and retrievals. Although a genetic profile may include a large amount of information, only a part of the profile is examined in many applications. For example, let $X_1, \dots, X_{100}$ be variables of 100 genetic properties and $x_1, \dots, x_{100}$ be Alice's values of these variables. To evaluate if $f(x_1, \dots, x_{100}) = 0$ for any examination (multivariate) polynomial f with degree 3, or the truth value of the corresponding predicate $\phi_f(x_1, \dots, x_{100})$, the attribute vector $\vec{x}$ of Alice should be a monomial vector of Alice's values with degree 3, $\vec{x} := (1, x_1, \dots, x_{100}, x_1^2, x_1x_2, \dots, x_{100}^2, x_1^3, x_1^2x_2, \dots, x_{100}^3)$, whose dimension is around 10^6. A predicate vector $\vec{v}$ for a secret key can be associated with predicate ϕ_f.

To ensure the private data processing of $\vec{x}$, it should be encrypted (say c for a ciphertext of $\vec{x}$) by a *fully attribute-hiding* IPE scheme, since whether $\phi_f(x_1, \dots, x_{100})$ holds can be examined with releasing no other information by checking whether c can be decrypted by a secret key with $\vec{v}$ (i.e., $R(\vec{v}, \vec{x})$ holds). Here, if c is encrypted by *fully* attribute-hiding IPE, it releases no information on $\vec{x}$ except that $R(\vec{v}, \vec{x})$ holds, or $\phi_f(x_1, \dots, x_{100})$ holds, however, if it is encrypted by *weakly* attribute-hiding IPE, such desirable security cannot be ensured.

Let a predicate for $\vec{v}$ be $((X_5 = a) \vee (X_{16} = b)) \wedge (X_{57} = c)$, which focuses only three factors, X_5, X_{16}, X_{57}, among the 100 genetic properties. It can be represented by a polynomial equation, $r_1(X_5 - a)(X_{16} - b) + r_2(X_{57} - c) = 0$ (where $r_1, r_2 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$), i.e., $(r_1ab - r_2c) - r_1bX_5 - r_1aX_{16} + r_2X_{57} + r_1X_5X_{16} = 0$. In order that $r_1(x_5 - a)(x_{16} - b) + r_2(x_{57} - c) = 0$ iff $\vec{v}\cdot\vec{x} = 0$, vector $\vec{v}$ should be $((r_1ab - r_2c), 0, \dots, 0, -r_1b, 0, \dots, 0, -r_1a, 0, \dots, 0, r_2, 0, \dots, 0, r_1, 0, \dots, 0)$, whose dimension is equivalent to that of $\vec{x}$, i.e., around 10^6, although the effective dimension of $\vec{v}$ is just 5. This is due to the above-mentioned restriction on the inner-product relation of the existing IPE schemes. The size of secret key for $\vec{v}$ then should be in proportion to the dimension of $\vec{v}$ (and $\vec{x}$), around 10^6. This example shows us a strong practical motivation, especially for *unbounded* IPE schemes, to relax this restriction on the inner-product relation and to shorten the length of the secret key to that in proportion to the effective dimension, e.g., 5, instead of around 10^6.

1.2 Our Results

1. This paper introduces a new concept of IPE, generalized IPE, which relaxes the above-mentioned restriction of IPE and consists of three types of IPE, Types 0, 1 and 2. Here the notion of Types 1 and 2 is introduced in this paper, and Type 0 is the traditional one (see Remark below).

   Remark: We now roughly explain the three types of inner-product relations. To relax the above-mentioned restriction on the inner-product relation, we introduce a new type of inner-product (generalized inner-product) for $\vec{v}$ and $\vec{x}$, where their dimensions can be different (say n and n' for the dimensions of $\vec{v}$ and $\vec{x}$). In this notion, vector $\vec{v}$ and $\vec{x}$ are expressed by $\{(t, v_t) \mid t \in I_{\vec{v}}, \sharp I_{\vec{v}} = n\}$ and $\{(t, x_t) \mid t \in I_{\vec{x}}, \sharp I_{\vec{x}} = n'\}$, respectively, where $t \in \mathbb{N}$ is an index for vectors, whose semantics is given by each ap-

Table 1: Comparison of *attribute-hiding IPE schemes*, where $|\mathbb{G}|$ and $|\mathbb{G}_T|$ represent size of an element of $\mathbb{G}$ and that of $\mathbb{G}_T$, respectively. AH, IP, PK, SK, CT, GSD and eDDH stand for attribute-hiding, inner-product, master public key (public parameters), secret key, ciphertext, general subgroup decision [3] and extended decisional Diffie-Hellman [8], respectively. And, $n := \sharp I_{\vec{v}}$ and $n' := \sharp I_{\vec{x}}$. (Then, $n = n'$ except for the proposed unbounded IPE schemes.)

	KSW08 [7]	LOS$^+$10 [8]	OT10 [14]	OT12 [16]		Proposed IPE	
				(basic)	(variant)	(type 1 or 2) Section 5.1	(type 0) Section 5.3
Bounded or Unbounded	bounded	bounded	bounded	bounded		unbounded	
Restriction on IP relation	restricted*	restricted	restricted	restricted		relaxed	restricted
Security	selective & fully-AH	adaptive & weakly-AH	adaptive & weakly-AH	adaptive & fully-AH		adaptive & fully-AH	
Order of $\mathbb{G}$	composite	prime	prime	prime		prime	
Assump.	2 variants of GSD	n-eDDH	DLIN	DLIN		DLIN	
PK size	$O(n)\lvert\mathbb{G}\rvert$	$O(n^2)\lvert\mathbb{G}\rvert$	$O(n^2)\lvert\mathbb{G}\rvert$	$O(n^2)\lvert\mathbb{G}\rvert$	$O(n)\lvert\mathbb{G}\rvert$	$O(1)\lvert\mathbb{G}\rvert$	$O(1)\lvert\mathbb{G}\rvert$
SK size	$(2n+1)\lvert\mathbb{G}\rvert$	$(2n+3)\lvert\mathbb{G}\rvert$	$(3n+2)\lvert\mathbb{G}\rvert$	$(4n+2)\lvert\mathbb{G}\rvert$	$11\lvert\mathbb{G}\rvert$	$(15n+5)\lvert\mathbb{G}\rvert$	$(21n+9)\lvert\mathbb{G}\rvert$
CT size	$(2n+1)\lvert\mathbb{G}\rvert$ $+ \lvert\mathbb{G}_T\rvert$	$(2n+3)\lvert\mathbb{G}\rvert$ $+ \lvert\mathbb{G}_T\rvert$	$(3n+2)\lvert\mathbb{G}\rvert$ $+ \lvert\mathbb{G}_T\rvert$	$(4n+2)\lvert\mathbb{G}\rvert$ $+ \lvert\mathbb{G}_T\rvert$	$(5n+1)\lvert\mathbb{G}\rvert$ $+ \lvert\mathbb{G}_T\rvert$	$(15n'+5)\lvert\mathbb{G}\rvert$ $+ \lvert\mathbb{G}_T\rvert$	$(21n'+9)\lvert\mathbb{G}\rvert$ $+ \lvert\mathbb{G}_T\rvert$

* It can be easily relaxed.

plication. Here note that we abuse the same vector notation, $\vec{v}$, for the new expression as well as for the conventional one, $(v_1, \ldots, v_n)$. In the above-mentioned example, $\vec{x} := \{(1,1), (2, x_1), \ldots, (101, x_{100}), (102, x_1^2), (103, x_1x_2), \ldots, (n', x_{100}^3)\}$ where $I_{\vec{x}} := \{1, 2, \ldots, n'\}$, and $\vec{v} := \{(1, r_1ab - r_2c), (6, -r_1b), (17, -r_1a), (58,\ r_2), (517, r_1)\}$ where $I_{\vec{v}} := \{1, 6, 17, 58, 517\}$. The generalized inner-product of $\vec{v}$ over $\vec{x}$ is defined by $\sum_{t \in I_{\vec{v}}} v_t x_t$ if $I_{\vec{v}} \subseteq I_{\vec{x}}$. Otherwise, it is undefined. By using the generalized inner-product notion, the secret key size can be in proportion to the effective dimension (e.g., 5 instead of around 10^6).

We then introduce three types of IPE schemes. For Type 1, relation $R(\vec{v}, \vec{x})$ holds iff the generalized inner-product of $\vec{v}$ over $\vec{x}$ is 0, while for Type 2 it holds iff the generalized inner-product of $\vec{x}$ over $\vec{v}$ is 0. We call Type 0 for the conventional inner-products, i.e., relation $R(\vec{v}, \vec{x})$ is defined by the standard inner-product of $\vec{v}$ and $\vec{x}$, where $\vec{v}$ and $\vec{x}$ have the same dimension (in other words, the inner-product for Type 0 is defined iff these dimensions are equivalent.)

2. We present the first *unbounded* inner-product encryption (IPE) schemes. The proposed unbounded IPE schemes are *fully (adaptively) secure and fully attribute-hiding* in the standard model under a standard assumption, the decisional linear (DLIN) assumption. The proposed unbounded IPE schemes consist of the above-mentioned types of generalized IPE, Types 0, 1 and 2, For comparison of attribute-hiding IPE schemes, see Table 1.

3. We present the first *unbounded* KP- and CP-ABE schemes that are *fully secure* (adaptively

Table 2: Comparison of *KP-ABE Schemes*, where $|\mathbb{G}|$ represents the size of an element of $\mathbb{G}$, and PK, SK, CT and GSD stand for master public key (public parameters), secret key, ciphertext and general subgroup decision [3], respectively. And, d, n, n_{max}, ℓ and k_{max} are the number of sub-universes of attributes, the number of attributes for a CT, the maximum number of attributes for a CT, the row size of an access policy matrix for a SK and the maximum value of the degree of access policies, respectively.

	LW11 [11]	LOS$^+$10 [8]		OT10 [14]		Proposed KP-ABE	
		(basic)	(modified)	(basic)	(modified)	(basic) Section 6.1	(modified) Section 6.2
Bounded or Unbounded	unbounded	bounded		bounded		unbounded	
Security	selective	full		full		full	
Order of $\mathbb{G}$	composite	composite		prime		prime	
Assump.	GSD	GSD		DLIN		DLIN	
Degree of access policies	arbitrary	1	arbitrary	1	arbitrary	1	arbitrary
PK size	$O(1)\vert\mathbb{G}\vert$	$O(n_{\mathsf{max}})\vert\mathbb{G}\vert$		$O(d)\vert\mathbb{G}\vert$		$O(1)\vert\mathbb{G}\vert$	
SK size	$O(\ell)\vert\mathbb{G}\vert$	$O(\ell)\vert\mathbb{G}\vert$		$O(\ell)\vert\mathbb{G}\vert$		$O(\ell)\vert\mathbb{G}\vert$	
CT size	$O(n)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$	$O(k_{\mathsf{max}}n)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$	$O(k_{\mathsf{max}}n)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$	$O(k_{\mathsf{max}}n)\vert\mathbb{G}\vert$

payload-hiding) in the standard model. The proposed unbounded ABE schemes are fully secure under the DLIN assumption, and are for a wide class of relations, non-monotone access structures. See Table 2 for comparison of KP-ABE schemes.

Remark: Similarly to the existing fully secure ABE schemes in the standard model [8, 14, 10] except [12], our basic ABE scheme (Section 6.1) has a restriction that the degree of access policies is 1 [1]. A modified KP-ABE scheme is shown in Section 6.2 to relax the restriction or to achieve an arbitrary degree k of access policies with preserving the fully secure and unbounded property. It, however, shares a shortcoming of the existing fully secure (modified) ABE schemes [8, 14, 10] that the ciphertext size grows linearly with k. Here, a (maximum) value of k can be determined in each application of our ABE scheme, while the public parameters are fixed and commonly shared by all applications and users.

1.3 Key Techniques

As mentioned above, the difficulty of realizing a fully secure unbounded IPE or ABE scheme arises from the hardness of supplying an *unbounded amount of* randomness *consistent* with the complicated key-query condition for the (dual system encryption) security arguments on IPE or ABE. To overcome this difficulty, we develop novel techniques, *indexing* and *consistent randomness amplification*, on the dual system encryption and the dual pairing vector spaces (DPVS). Roughly speaking, the *indexing* technique is for supplying a source of unbounded amount of randomness and the *consistent randomness amplification* technique is for amplifying the randomness of the source through a computational assumption (e.g., the DLIN assumption

[1] Informally, the degree may imply the number of appearance of a variable in a formula, e.g., formula $((x = a) \vee (x = b)) \wedge (y = c)$ has degree 2 for variable x. For the definition of the degree of access policies in our schemes, see Section 6.2. The degree should be a bit differently defined in [20, 6, 18, 22, 8, 10], where degree 1 is called *one-use*.

in our case) and the randomness of hidden bases as well as for adjusting the distribution of the amplified randomness to be consistent with a condition. This methodology could provide a general framework for proving the security in unbounded situations.

In DPVS, a pair of dual (or orthonormal) bases for N-dimensional linear spaces, $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$, are randomly generated using a secret random linear transformation X (random $N \times N$ matrix) (see Section 2). In a typical application of DPVS to cryptography, a part of $\mathbb{B}$ (say $\hat{\mathbb{B}}$) is used as a public key (public parameters), and $\mathbb{B}^*$ as a secret key, where X is the top level secret key and the source of randomness.

In a typical construction of *bounded* IPE schemes [8, 14, 16] which are based on DPVS, once a basis of DPVS, a part of the basis of a N-dimensional space is published as public parameters, the dimension n of predicate and attribute vectors for secret key and encryption is bounded or fixed, e.g., $n \leq N/4$ (i.e., $N = O(n)$). The full security is proven through the information theoretical arguments, and the randomness of secret matrix X (e.g., the amount of the randomness is $O(n^2)$) supplies enough randomness for the arguments.

In contrast, the dimension, n, of the predicate and attribute vectors is not bounded by the public parameters in *unbounded* IPE. For example, in one of the proposed IPE schemes (Section 5), the public parameters consist of a constant number of elements, 9 elements of bases (or 105 pairing group elements), $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15})$, where random matrices of constant sizes, $X_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{5\times 5}$ and $X_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{15\times 15}$, are employed to generate the public parameters. The randomness of the public parameters, just a constant amount with respect to n, is clearly insufficient for the (dual system encryption) arguments on the proof of full security.

To supply additional randomness for the purpose, in our IPE schemes, we introduce a technique called *indexing*, where two-dimensional index vectors, $\sigma_t(1, t)$ and $\mu_t(t, -1)$ are embedded into ciphertext $\boldsymbol{c}_t$ and secret key $\boldsymbol{k}_t^*$, respectively, where σ_t and μ_t are freshly random for each t. In our IPE scheme (Section 5) where $n = n'$ for simplicity, for example, secret key $(\boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_n^*)$ for $\vec{v} := (v_1, \ldots, v_n)$ can be expressed by a coefficient vector, $(\mu_t(t, -1), \delta v_t, \ldots)$, for $t = 1, \ldots, n$, over basis $\mathbb{B}^*$, i.e., $\boldsymbol{k}_t^* := (\mu_t(t, -1), \delta v_t, \ldots)_{\mathbb{B}^*}$ and ciphertext $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n)$ for $\vec{x} := (x_1, \ldots, x_n)$ can be expressed by $\boldsymbol{c}_t := (\sigma_t(1, t), \omega x_t, \ldots)_{\mathbb{B}}$ for $t = 1, \ldots, n$, where δ, ω are randomly selected. While the size of the public parameters or its randomness is constant in n, an unbounded amount of randomness, $\{\mu_t\}_{t=1,\ldots,n}, \{\sigma_t\}_{t=1,\ldots,n}$, can be supplied to secret key and ciphertext. This is a key idea of the *indexing* technique.

Although the technique supplies an unbounded amount of randomness, i.e., $O(n)$-size of randomness, it is not enough for our purpose. We need more and a specific distribution of randomness. This is because: in the proof of full security on dual system encryption and the extension, such a *real* randomness provided by the indexing technique should be expanded into a *hidden* part in spaces over bases $\mathbb{B}$ and $\mathbb{B}^*$, and the distribution should be also adjusted to (or consistent with) the key-query condition for IPE or ABE. For this purpose, i.e., in order to amplify the randomness to a hidden subspace and to adjust it to a specific distribution, we develop another technique, *consistent randomness amplification*.

For a bit more detailed explanation of the consistent randomness amplification technique, we will briefly review a hidden part (subspace) of DPVS. As mentioned above, in a typical application of DPVS to cryptography, a part of $\mathbb{B}$ (say $\hat{\mathbb{B}}$) is used as a public key (public parameters). Therefore, the basis, $\mathbb{B} - \hat{\mathbb{B}}$, is information theoretically concealed against an adversary, i.e., even an infinite power adversary has no idea on which basis is selected as $\mathbb{B} - \hat{\mathbb{B}}$ when $\hat{\mathbb{B}}$ is published. The underlying dual vector spaces, $\mathsf{span}\langle\mathbb{B}\rangle$ and $\mathsf{span}\langle\mathbb{B}^*\rangle$, are 15-dimensional for our IPE scheme (Type 1 or 2) and 14-dimensional for our ABE scheme. The subspaces employed for public parameters are just 6-dimensional and other 2 dimensional basis can be public. Hence, the basis for the remaining 7 or 6-dimensional subspace is information theoretically concealed (uncertain). The consistent randomness amplification technique is executed over these 7 or 6-dimensional hidden subspaces. For example, as mentioned above, a real secret key $\{\boldsymbol{k}_t^*\}$ and ciphertext $\{\boldsymbol{c}_t\}$ are expressed by $\boldsymbol{k}_t^* := (\mu_t(t,-1), \delta v_t, s_t, \boxed{0^7}, \ldots)_{\mathbb{B}^*}$ and $\boldsymbol{c}_t := (\sigma_t(1,t),\ \omega x_t,\ \widetilde{\omega}, \boxed{0^7}, \ldots)_{\mathbb{B}}$. This technique provides a transformation (for the dual system encryption technique and the extension) to the following forms: $\boldsymbol{k}_t^* := (\mu_t(t,-1), \delta v_t, s_t, \boxed{0^4, (\pi v_t, a_t)\cdot U_t, 0},\ \ldots)_{\mathbb{B}^*}$ and $\boldsymbol{c}_t := (\sigma_t(1,\ t), \omega x_t,\ \widetilde{\omega}, \boxed{\ldots, (\tau x_t, \widetilde{\tau})\cdot Z_t,\ 0}, \ldots)_{\mathbb{B}}$, where Z_t is an independently random 2×2 matrix for each t and $U_t := (Z_t^{\mathrm{T}})^{-1}$, and other new variables are random. Here, the box-framed parts are the information theoretically hidden subspaces, the randomness of the hidden parts is amplified and the distribution of $(\pi v_t, a_t)\cdot U_t$ and $(\tau x_t, \widetilde{\tau})\cdot Z_t$ is consistent with the key-query condition.

The consistent randomness amplification technique is composed of several computational and conceptual (information theoretical) transformations. One of the key tricks of the transformations is to amplify a source of randomness to a hidden part by applying a computational assumption, the DLIN assumption. Another computational trick is to swap two vectors in different positions under DLIN. Information theoretical key tricks are inter-subspace and intra-subspace types of conceptual transformations (see Section 7 for more details).

The security proofs of our IPE and ABE schemes are hierarchically constructed in a modular manner. The very top level of the security proof is based on the dual system encryption and its extension. Several problems in the middle level support the top level arguments. Our key techniques, the indexing and consistent randomness amplification techniques, which are also constructed in a hierarchical manner, are employed in the lowest level to reduce the hardness of the middle level problems to the DLIN assumption. The top level of the security proof of our IPE scheme (for $\kappa = 1$) is outlined in Section 5.1.7, and that of our ABE scheme is outlined in the upper part of Figure 2 in Appendix A.4.

1.4 Notations

When A is a random variable or distribution, $y \xleftarrow{\mathsf{R}} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \xleftarrow{\mathsf{U}} A$ denotes that y is uniformly selected from A. We denote the finite field of order q by $\mathbb{F}_q$, $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^\times$, and the set of positive integers by $\mathbb{N}$. A vector symbol denotes a vector representation over $\mathbb{F}_q$, e.g., $\vec{x}$ denotes $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. 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. I_ℓ and 0_ℓ denote the $\ell \times \ell$ identity matrix and the $\ell \times \ell$ zero matrix, respectively. 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 $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^N y_i \boldsymbol{b}_i^*$. $\vec{e}_1$ and $\vec{e}_2$ denote the canonical basis vectors in $\mathbb{F}_q^2$, i.e., $\vec{e}_1 := (1, 0)$ and $\vec{e}_2 := (0, 1)$. $GL(n, \mathbb{F}_q)$ denotes the general linear group of degree n over $\mathbb{F}_q$.

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

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.*

Definition 2 *"Dual pairing vector spaces (DPVS)"* $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ *by a direct product of symmetric pairing groups* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *are a tuple of prime* q*,* N*-dimensional vector space* $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$ *over* $\mathbb{F}_q$*, cyclic group* $\mathbb{G}_T$ *of order* q*, canonical basis* $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$ *of* $\mathbb{V}$*, where* $\boldsymbol{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G, \overbrace{0, \ldots, 0}^{N-i})$*, 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* $\boldsymbol{x} = \boldsymbol{0}$*. For all* i *and* j*,* $e(\boldsymbol{a}_i, \boldsymbol{a}_j) = e(G, G)^{\delta_{i,j}}$ *where* $\delta_{i,j} = 1$ *if* $i = j$*, and* 0 *otherwise, and* $e(G, G) \neq 1 \in \mathbb{G}_T$*. DPVS generation algorithm* $\mathcal{G}_{\mathsf{dpvs}}$ *takes input* 1^λ *(*$\lambda \in \mathbb{N}$*) and* $N \in \mathbb{N}$*, and outputs a description of* $\mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ *with security parameter* λ *and* N*-dimensional* $\mathbb{V}$*. It can be constructed by using* $\mathcal{G}_{\mathsf{bpg}}$*.*

For matrix $W := (w_{i,j})_{i,j=1,\ldots,N} \in \mathbb{F}_q^{N \times N}$ *and element* $\boldsymbol{x} := (G_1, \ldots, G_N)$ *in* N*-dimensional* $\mathbb{V}$*,* $\boldsymbol{x}W$ *denotes* $(\sum_{i=1}^{N} G_i w_{i,1}, \ldots, \sum_{i=1}^{N} G_i w_{i,N}) = (\sum_{i=1}^{N} w_{i,1} G_i, \ldots, \sum_{i=1}^{N} w_{i,N} G_i)$ *by a natural multiplication of a* N*-dim. row vector and a* $N \times N$ *matrix. Thus it holds an associative law, i.e.,* $(\boldsymbol{x}W_1)W_2 = \boldsymbol{x}(W_1 W_2)$*.*

For the asymmetric version of DPVS, see Appendix A.2 in [14]. We describe random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}$, which is used as a subroutine in our IPE and ABE schemes.

$$
\begin{aligned}
&\mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_t)_{t=0,1}) : \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \quad \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}, \\
&\quad \text{for } t = 0, 1, \qquad \mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t, \mathsf{param}_{\mathbb{G}}), \\
&\qquad X_t := (\chi_{t,i,j})_{i,j=1,\ldots,N_t} \xleftarrow{\mathsf{U}} GL(N_t, \mathbb{F}_q), \ X_t^* := (\vartheta_{t,i,j})_{i,j=1,\ldots,N_t} := \psi \cdot (X_t^{\mathrm{T}})^{-1}, \text{ hereafter,} \\
&\qquad \vec{\chi}_{t,i} \text{ and } \vec{\vartheta}_{t,i} \text{ denote the } i\text{-th rows of } X_t \text{ and } X_t^* \text{ for } i = 1, \ldots, N_t, \text{ respectively,} \\
&\qquad \boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})_{\mathbb{A}_t} = \textstyle\sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j} \ \text{ for } i = 1, \ldots, N_t, \ \ \mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,N_t}), \\
&\qquad \boldsymbol{b}^*_{t,i} := (\vec{\vartheta}_{t,i})_{\mathbb{A}_t} = \textstyle\sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j} \ \text{ for } i = 1, \ldots, N_t, \ \ \mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,N_t}), \\
&\quad g_T := e(G, G)^{\psi}, \ \ \mathsf{param} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,1}, \ \psi G, \ g_T), \quad \text{return } \ (\mathsf{param}, \mathbb{B}, \mathbb{B}^*).
\end{aligned}
$$

We note that $g_T = e(\boldsymbol{b}_{t,i}, \boldsymbol{b}^*_{t,i})$ for $t = 0, 1; i = 1, \ldots, N_t$. Hereafter, for simplicity, we denote $N := N_1, \mathbb{V} := \mathbb{V}_1, \mathbb{A} := \mathbb{A}_1, \mathbb{B} := \mathbb{B}_1$ and $\mathbb{B}^* := \mathbb{B}^*_1$ for variables with $t = 1$.

3 Decisional Linear (DLIN) Assumption

Definition 3 (DLIN: Decisional Linear Assumption [4]) *The DLIN problem is to guess* $\beta \in \{0, 1\}$*, given* $(\mathsf{param}_{\mathbb{G}}, \ G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$*, where*

$$
\begin{aligned}
\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda) : \mathsf{param}_{\mathbb{G}} &:= (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \\
\kappa, \delta, \xi, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad & Y_0 := (\delta + \sigma)G, \quad Y_1 \xleftarrow{\mathsf{U}} \mathbb{G}, \\
\text{return } \ (\mathsf{param}_{\mathbb{G}}, \ & G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta),
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$*. For a probabilistic machine* $\mathcal{F}$*, we define the advantage of* $\mathcal{F}$ *for the DLIN problem as:* $\mathsf{Adv}_{\mathcal{F}}^{\mathsf{DLIN}}(\lambda) := \left| \mathsf{Pr}\left[\mathcal{F}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda)\right] - \mathsf{Pr}\left[\mathcal{F}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)\right] \right|$*. The DLIN assumption is: For any probabilistic polynomial-time adversary* $\mathcal{F}$*, the advantage* $\mathsf{Adv}_{\mathcal{F}}^{\mathsf{DLIN}}(\lambda)$ *is negligible in* λ*.*

4 Definitions of Generalized Inner-Product Encryption (IPE) and Attribute-Based Encryption (ABE)

4.1 Generalized Inner-Product Encryption

This section defines generalized inner product encryption (IPE) and its security.

The parameters of generalized inner-product predicates are expressed as a vector $\vec{x} := \{(t, x_t) \,|\, t \in I_{\vec{x}},\ x_t \in \mathbb{F}_q\} \setminus \{\vec{0}\}$ with finite index set $I_{\vec{x}} \subset \mathbb{N}$ for encryption and a vector $\vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}},\ v_t \in \mathbb{F}_q\} \setminus \{\vec{0}\}$ with finite index set $I_{\vec{v}} \subset \mathbb{N}$ for a secret key, respectively. Here there are three types of unbounded IPE with respect to the decryption condition. For Type 1, $R(\vec{v}, \vec{x}) = 1$ iff $I_{\vec{v}} \subseteq I_{\vec{x}}$ and $\sum_{t \in I_{\vec{v}}} v_t x_t = 0$. For Type 2, $R(\vec{v}, \vec{x}) = 1$ iff $I_{\vec{v}} \supseteq I_{\vec{x}}$ and $\sum_{t \in I_{\vec{x}}} v_t x_t = 0$.

We will consider Type 0 inner-product predicate only for conventional prefix type vectors $\vec{v} := (v_1, \ldots, v_n)$ and $\vec{x} := (x_1, \ldots, x_{n'})$. For Type 0, $R(\vec{v}, \vec{x}) = 1$ iff $n = n'$ and $\vec{v} \cdot \vec{x} := \sum_{t=1}^{n} v_t x_t = 0$.

Definition 4 *An inner product encryption scheme (for generalized inner-product relation $R(\vec{v}, \vec{x})$) consists of probabilistic polynomial-time algorithms* Setup, KeyGen, Enc *and* Dec*. They are given as follows:*

Setup *takes as input security parameter 1^λ. It outputs public parameters* pk *and (master) secret key* sk*.*

KeyGen *takes as input public parameters* pk*, secret key* sk*, and vector $\vec{v}$. It outputs a corresponding secret key* $\mathsf{sk}_{\vec{v}}$*.*

Enc *takes as input public parameters* pk*, message m in some associated message space,* msg*, and vector $\vec{x}$. It returns ciphertext* $\mathsf{ct}_{\vec{x}}$*.*

Dec *takes as input the master public key* pk*, secret key* $\mathsf{sk}_{\vec{v}}$ *and ciphertext* $\mathsf{ct}_{\vec{x}}$*. It outputs either $m' \in \mathsf{msg}$ or the distinguished symbol $\perp$.*

A generalized IPE scheme should have the following correctness property: for all $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda)$, all vectors $\vec{v}$ and $\vec{x}$, all secret keys $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$, all messages m, all ciphertext $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m, \vec{x})$, it holds that $m = \mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \mathsf{ct}_{\vec{x}})$ if $R(\vec{v}, \vec{x}) = 1$. Otherwise, it holds with negligible probability.

Definition 5 *The model for defining the adaptively fully-attribute-hiding security of IPE against adversary $\mathcal{A}$ (under chosen plaintext attacks) is given by the following game:*

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

Phase 1 *$\mathcal{A}$ may adaptively make a polynomial number of key queries for vectors, $\vec{v}$, to the challenger. In response, the challenger gives the corresponding key $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$ to $\mathcal{A}$.*

Challenge *$\mathcal{A}$ submits challenge vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ with the same index set $I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ (or $n'^{(0)} = n'^{(1)}$ for Type 0) and challenge messages $(m^{(0)}, m^{(1)})$, subject to the following restrictions:*

- *Any key query $\vec{v}$ in Phase 1 satisfies $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = 0$, or*

- *Two challenge messages are equal, i.e., $m^{(0)} = m^{(1)}$, and any key query $\vec{v}$ in Phase 1 satisfies $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)})$.*

The challenger flips a coin $b \xleftarrow{\mathsf{U}} \{0,1\}$, and gives $\mathsf{ct}_{\vec{x}^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m^{(b)}, \vec{x}^{(b)})$ to $\mathcal{A}$.

Phase 2 *Phase 1 is repeated with the above restriction for key query $\vec{v}$ and challenge, $(\vec{x}^{(0)}, \vec{x}^{(1)})$ and $(m^{(0)}, m^{(1)})$.*

Guess *$\mathcal{A}$ outputs a bit b', and wins if $b' = b$.*

The advantage of $\mathcal{A}$ in the above game is defined as $\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{A}}(\lambda) := \mathsf{Pr}[\mathcal{A} \text{ wins }] - 1/2$ for any security parameter λ. An IPE scheme is adaptively fully-attribute-hiding (AH) against chosen plaintext attacks *if all probabilistic polynomial-time adversaries $\mathcal{A}$ have at most negligible advantage in the above game. For each run of the game, the variable s is defined as $s := 0$ if $m^{(0)} \neq m^{(1)}$ for challenge messages $m^{(0)}$ and $m^{(1)}$, and $s := 1$ otherwise.*

4.2 Attribute-Based Encryption with Non-Monotone Access Structures

4.2.1 Span Programs and Non-Monotone Access Structures

Definition 6 (Span Programs [2]) *Let $\{p_1, \ldots, p_n\}$ be a set of variables. A span program over $\mathbb{F}_q$ is a labeled matrix $\hat{M} := (M, \rho)$ where M is a $(\ell \times r)$ matrix over $\mathbb{F}_q$ and ρ is a labeling of the rows of M by literals from $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ (every row is labeled by one literal), i.e., $\rho : \{1, \ldots, \ell\} \to \{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$.*

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

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

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

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

Definition 7 (Access Structures) *$\mathcal{U}_t$ $(t = 1, \ldots, d$ and $\mathcal{U}_t \subset \{0,1\}^*)$ is a sub-universe, a set of attributes, each of which is expressed by a pair of sub-universe id and value of attribute, i.e., (t, v), where $t \in \{1, \ldots, d\}$ and $v \in \mathbb{F}_q$.*

We now define such an attribute to be a variable p of a span program $\hat{M} := (M, \rho)$, i.e., $p := (t, v)$. An access structure $\mathbb{S}$ is span program $\hat{M} := (M, \rho)$ along with variables $p := (t, v), p' := (t', v'), \ldots$, i.e., $\mathbb{S} := (M, \rho)$ such that $\rho : \{1, \ldots, \ell\} \to \{(t, v), (t', v'), \ldots, \neg(t, v), \neg(t', v'), \ldots\}$.

Let Γ be a set of attributes, i.e., $\Gamma := \{(t, x_t) \mid x_t \in \mathbb{F}_q, 1 \le t \le d\}$, where $1 \le t \le d$ means that t is an element of some subset of $\{1, \ldots, d\}$.

When Γ is given to access structure $\mathbb{S}$, map $\gamma : \{1, \ldots, \ell\} \to \{0,1\}$ for span program $\hat{M} := (M, \rho)$ is defined as follows: For $i = 1, \ldots, \ell$, set $\gamma(i) = 1$ if $[\rho(i) = (t, v_i)] \wedge [(t, x_t) \in \Gamma] \wedge [v_i = x_t]$ or $[\rho(i) = \neg(t, v_i)] \wedge [(t, x_t) \in \Gamma] \wedge [v_i \neq x_t]$. Set $\gamma(i) = 0$ otherwise.

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

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

Definition 8 *A secret-sharing scheme for span program $\hat{M} := (M, \rho)$ is:*

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

4.2.2 Key-Policy Attribute-Based Encryption

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 9 (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. 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, $\Gamma := \{(t, x_t) | x_t \in \mathbb{F}_q, 1 \le t \le d\}$. 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 $m' \in$* msg *or the distinguished symbol $\perp$.*

A KP-ABE scheme should have the following correctness property: for all $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda)$, 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 10 *The model for defining the adaptively payload-hiding security of KP-ABE under chosen plaintext attack is given by the following game:*

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

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

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

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

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

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

4.2.3 Ciphertext-Policy Attribute-Based Encryption

Definition 11 (Ciphertext-Policy Attribute-Based Encryption : CP-ABE) *A ciphertext-policy attribute-based encryption scheme consists of four algorithms.*

Setup *takes as input security parameter. It outputs the public parameters* pk *and a master key* sk*.*

KeyGen *takes as input a set of attributes, $\Gamma := \{(t, x_t) | x_t \in \mathbb{F}_q, 1 \le t \le d\}$,* pk *and* sk*. It outputs a decryption key.*

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

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

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

Definition 12 *The model for proving the adaptively payload-hiding security of CP-ABE under chosen plaintext attack is:*

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

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

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

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

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

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

We note that the model can easily be extended to handle chosen-ciphertext attacks (CCA) by allowing for decryption queries in Phase 1 and 2.

5 Proposed IPE Schemes

5.1 Type 1 IPE Scheme

5.1.1 Construction Idea for Our Type 1 and 2 IPE Schemes

In the existing constructions [13, 8, 14, 15, 16, 17] of IPE on DPVS, around cn ($c \geq 1$) dimensional vector spaces are used for n-dimensional attribute and predicate vectors. Here, the vectors are encoded in an n-dimensional subspace. Although this is a typical strategy of constructing IPE on DPVS, we cannot employ this idea in the *unbounded* setting, where we can use only constant dimensional spaces. In our construction, each component x_t of $\vec{x}$ (resp. v_t of $\vec{v}$) is encoded in a constant dimensional space. In order to meet the decryption condition, we employ the *indexing* technique and n-out-of-n secret sharing trick. For example, in Type 1 construction, 4-dimensional vector $(\mu_t(t, -1), \delta v_t, s_t)$ is encoded in key $\boldsymbol{k}_t^*$, and $(\sigma_t(1, t), \omega x_t, \widetilde{\omega})$ is encoded in ciphertext $\boldsymbol{c}_t$. The first 2-dimension is used for indexes, and s_t in the fourth component of $\boldsymbol{k}_t^*$ is for the secret sharing. Informally, a ciphertext can be decrypted if all n pieces of shares s_t are recovered. A Type 2 IPE scheme can be constructed from our Type 1 scheme by setting the secret-sharing mechanism in the ciphertext side instead of the secret key side.

5.1.2 Construction

Let $d := poly(\lambda)$, where $poly(\cdot)$ is an arbitrary polynomial. Random dual basis generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_t)_{t=0,1})$ is defined at the end of Section 2. We refer to Section 1.4 for notations on DPVS.

$\mathsf{Setup}(1^\lambda):\quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \overset{\mathsf{R}}{\leftarrow} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 15)),$

$\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15}),$

$\quad \widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, .., \boldsymbol{b}_4^*, \boldsymbol{b}_{12}^*, \boldsymbol{b}_{13}^*),$

$\quad$ return $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}),\ \mathsf{sk} := (\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*).$

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}} \subseteq \{1, \ldots, d\}\}) : s_t, \delta, \eta_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$ for $t \in I_{\vec{v}},\ s_0 := \sum_{t \in I_{\vec{v}}} s_t,$

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

$$\text{for } t \in I_{\vec{v}},\ \mu_t, \eta_{t,1}, \eta_{t,2} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q,\ \boldsymbol{k}_t^* := (\ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t,}^{4}\ \ \overbrace{0^7,}^{7}\ \ \overbrace{\eta_{t,1}, \eta_{t,2},}^{2}\ \ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*},$$

$\quad$ return $\mathsf{sk}_{\vec{v}} := (I_{\vec{v}}, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}}).$

$\mathsf{Enc}(\mathsf{pk},\ m,\ \vec{x} := \{(t, x_t) \,|\, t \in I_{\vec{x}} \subseteq \{1, \ldots, d\}\}) :\ \omega, \widetilde{\omega}, \zeta, \varphi_0 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q,$

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

$$\text{for } t \in I_{\vec{x}},\ \sigma_t, \varphi_{t,1}, \varphi_{t,2} \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q,\ \boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega x_t,\ \widetilde{\omega},}^{4}\ \ \overbrace{0^7,}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\varphi_{t,1}, \varphi_{t,2}}^{2}\ )_{\mathbb{B}},$$

```
    return $\mathsf{ct}_{\vec{x}} := (I_{\vec{x}}, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$.
$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := (I_{\vec{v}}, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}}),\ \mathsf{ct}_{\vec{x}} := (I_{\vec{x}}, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T))$ :
    if $I_{\vec{v}} \subseteq I_{\vec{x}},\ K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot \prod_{t \in I_{\vec{v}}} e(\boldsymbol{c}_t, \boldsymbol{k}_t^*),$ return $m' := c_T / K$,
    else return $\perp$.
```

[Correctness] If $I_{\vec{v}} \subseteq I_{\vec{x}}$ and $\sum_{t \in I_{\vec{v}}} v_t x_t = 0,\ \ e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot \prod_{t \in I_{\vec{v}}} e(\boldsymbol{c}_t, \boldsymbol{k}_t^*) =$ $g_T^{-\widetilde{\omega} s_0 + \zeta} \cdot \prod_{t \in I_{\vec{v}}} g_T^{\delta \omega v_t x_t + \widetilde{\omega} s_t} = g_T^{-\widetilde{\omega} s_0 + \zeta} \cdot g_T^{\delta \omega (\sum_{t \in I_{\vec{v}}} v_t x_t) + \widetilde{\omega} (\sum_{t \in I_{\vec{v}}} s_t)} = g_T^{-\widetilde{\omega} s_0 + \zeta + \widetilde{\omega} s_0} = g_T^{\zeta}$.

5.1.3 Security

Theorem 1 *The proposed Type 1 IPE scheme is adaptively fully-attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{F}$'s, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IPE,AH}}(\lambda)$ is upper-bounded by the sum of the right hand of Eq. (1) and the right hand of Eq. (2). The sum is given by the total of $(\nu(12d^2 + 6d + 3) + 4d + 6)$ advantages of DLIN for $\mathcal{F}$ algorithms, which are $\mathcal{F}$ machines with parameters (h, ι, p, j, l) as described in Lemmas 1 and 2. Here, ν is the maximum number of $\mathcal{A}$'s key queries.

Theorem 1 is proven based on Lemmas 1 and 2.

Proof. First, we execute a preliminary game transformation from Game 0 (original security game in Definition 5) to Game 0', which is the same as Game 0 except that flips a coin $\kappa \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted in step 3 if $\kappa \neq s$. We define that $\mathcal{A}$ wins with probability 1/2 when the game is aborted (and the advantage in Game 0' is $\mathsf{Pr}[\mathcal{A}$ wins $] - 1/2$ as well). Since κ is independent from s, the game is aborted with probability 1/2. Hence, the advantage in Game 0' is a half of that in Game 0, i.e., $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IPE,AH,0'}}(\lambda) = 1/2 \cdot \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IPE,AH}}(\lambda)$. Moreover, $\Pr[\mathcal{A}\text{ wins}] = 1/2 \cdot (\Pr[\mathcal{A}\text{ wins} \mid \kappa = 0] + \Pr[\mathcal{A}\text{ wins} \mid \kappa = 1])$ in Game 0' since κ is uniformly and independently generated. As for the conditional probability with $\kappa = 0$, i.e., $\Pr[\mathcal{A}\text{ wins} \mid \kappa = 0]$, Lemma 1 (Eq. (1)) holds. As for the conditional probability with $\kappa = 1$, i.e., $\Pr[\mathcal{A}\text{ wins} \mid \kappa = 1]$, Lemma 2 (Eq. (2)) holds. Since $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IPE,AH}}(\lambda) = 2 \cdot \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IPE,AH,0'}}(\lambda) = \Pr[\mathcal{A}\text{ wins} \mid \kappa = 0] + \Pr[\mathcal{A}\text{ wins} \mid \kappa = 1] - 1 = (\Pr[\mathcal{A}\,\text{wins} \,|\, \kappa = 0] - 1/2) + (\Pr[\mathcal{A}\,\text{wins} \,|\, \kappa = 1] - 1/2)$, we obtain Theorem 1 from Lemmas 1 and 2. □

Lemma 1 *The proposed Type 1 IPE scheme is adaptively fully-attribute-hiding against chosen plaintext attacks under the DLIN assumption when $\kappa = 0$.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{F}_{1\text{-}0}, \mathcal{F}_{1\text{-}1}, \mathcal{F}_{1\text{-}2}, \mathcal{F}_{2\text{-}1}, \mathcal{F}_{2\text{-}2\text{-}1}, \ldots, \mathcal{F}_{2\text{-}2\text{-}5}$, $\mathcal{F}_3$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$
\begin{aligned}
\Pr[\mathcal{A}\text{ wins in Game } 0' \mid \kappa = 0] - 1/2 \le{} & \mathsf{Adv}_{\mathcal{F}_{1\text{-}0}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{1\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \textstyle\sum_{p=1}^{d} \sum_{j=1}^{2} \mathsf{Adv}_{\mathcal{F}_{1\text{-}2\text{-}p\text{-}j}}^{\mathsf{DLIN}}(\lambda) \\
& \textstyle\sum_{h=1}^{\nu} \Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}h\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \sum_{p=1}^{d} \sum_{j=1}^{2} \Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}1\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}2\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \\
& \quad \textstyle\sum_{l=1,\ldots,d;\ l \neq p} \Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}3\text{-}j\text{-}l}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}4\text{-}j\text{-}l}}^{\mathsf{DLIN}}(\lambda) \Big) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}5\text{-}j}}^{\mathsf{DLIN}}(\lambda) \Big) \Big) + \\
& \textstyle\sum_{j=1}^{2} \mathsf{Adv}_{\mathcal{F}_{3\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \epsilon,
\end{aligned}
\tag{1}
$$

where $\mathcal{F}_{1\text{-}2\text{-}p\text{-}j}(\cdot) := \mathcal{F}_{1\text{-}2}(h, p, j, \cdot), \mathcal{F}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{F}_{2\text{-}1}(h, \cdot), \mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}1\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}2\text{-}1}(h, p, j, \cdot)$, $\mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}2\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}2\text{-}2}(h, p, j, \cdot), \mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}3\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}2\text{-}3}(h, p, j, l, \cdot), \mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}4\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}2\text{-}4}(h, p, j, l, \cdot), \mathcal{F}_{2\text{-}h\text{-}2\text{-}p\text{-}5\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}2\text{-}5}(h, p, j, \cdot), \mathcal{F}_{3\text{-}j}(\cdot) := \mathcal{F}_3(j, \cdot),$ ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (20d^2\nu + 10d\nu + 5\nu + 10\nu + 20)/q$.

Proof outline (resp. proof) of Lemma 1 is given in Section 5.1.5 (resp. 5.1.6).

Lemma 2 *The proposed Type 1 IPE scheme is adaptively fully-attribute-hiding against chosen plaintext attacks under the DLIN assumption when* $\kappa = 1$*.*

For any adversary $\mathcal{A}$*, there exist probabilistic machines* $\mathcal{F}_{1\text{-}0}, \mathcal{F}_{1\text{-}1}, \mathcal{F}_{1\text{-}2}, \mathcal{F}_{2\text{-}1}, \mathcal{F}_{2\text{-}2\text{-}1}, \ldots, \mathcal{F}_{2\text{-}2\text{-}5}, \mathcal{F}_{2\text{-}3\text{-}1}, \ldots, \mathcal{F}_{2\text{-}3\text{-}5}, \mathcal{F}_{2\text{-}4}$*, whose running times are essentially the same as that of* $\mathcal{A}$*, such that for any security parameter* λ*,*

$$\begin{aligned}
&\Pr[\mathcal{A} \text{ wins in Game } 0' \mid \kappa = 1] - 1/2 \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{1\text{-}0}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{1\text{-}1}}(\lambda) + \textstyle\sum_{p=1}^{d} \sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{1\text{-}2\text{-}p\text{-}j}}(\lambda) \\
&\quad \textstyle\sum_{h=1}^{\nu} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}1}}(\lambda) + \sum_{\iota=2}^{3} \sum_{p=1}^{d} \sum_{j=1}^{2} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}1\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}2\text{-}j}}(\lambda) + \\
&\qquad \textstyle\sum_{l=1,\ldots,d;\ l\neq p} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}3\text{-}j\text{-}l}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}4\text{-}j\text{-}l}}(\lambda) \Big) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}5\text{-}j}}(\lambda) \Big) + \\
&\qquad \textstyle\sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}4\text{-}j}}(\lambda) \Big) + \epsilon, \qquad (2)
\end{aligned}$$

where $\mathcal{F}_{1\text{-}2\text{-}p\text{-}j}(\cdot) := \mathcal{F}_{1\text{-}2}(h, p, j, \cdot), \mathcal{F}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{F}_{2\text{-}1}(h, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}1\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}1}(h, p, j, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}2\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}2}(h, p, j, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}3\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}3}(h, p, j, l, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}4\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}4}(h, p, j, l, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}5\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}5}(h, p, j, \cdot)$ *for* $\iota = 2, 3$, $\mathcal{F}_{2\text{-}4\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}4}(j, \cdot)$, ν *is the maximum number of* $\mathcal{A}$*'s key queries and* $\epsilon := (40d^2\nu + 20d\nu + 10\nu + 10d + 10)/q$*.*

Proof outline (resp. proof) of Lemma 2 is given in Section 5.1.7 (resp. 5.1.8).

5.1.4 Lemmas (and Problems) for the proof of Lemmas 1 and 2

Computational Problems and Assumptions for Proofs of Lemmas 1 and 2 While our IPE scheme uses 15 dimensional space $\mathbb{V}$, our KP-ABE in Section 6.1 uses 14 dimensional $\mathbb{V}$. This 1-dimensional difference arises from the difference of the required security, fully-attribute-hiding for IPE but only payload-hiding for KP-ABE. The security of our KP-ABE is proven using Problem 1-ABE and 2-ABE. Note that while these problems are made for KP-ABE, they are also key techniques or basic building blocks for the security proof of IPE. The security proofs for Problems 1-ABE and 2-ABE (Lemmas 23 and 24) are given in Appendix A.4. The security proofs of IPE and ABE are reduced to the security (intractability) of these problems.

We will introduce 5 computational problems on DPVS for our IPE, Problems 1-IPE, ..., 5-IPE. These are classified into 3 types, ones based on Problem 1-ABE, ones based on Problem 2-ABE, and ones directly reduced from DLIN. Since the security of Problems 1-ABE and 2-ABE is proven using the *indexing* and *consistent randomness amplification* techniques, the security of the former two types essentially depends on these techniques.

The security lemma of Problem 1-IPE for unbounded IPE is reduced to that of Problem 1-ABE (Lemma 32 in Appendix A.1.1), and the security lemmas of Problems 2-IPE and 4-IPE are reduced to that of Problem 2-ABE (Lemma 33 in Appendix A.1.2). The security proofs of the other problems (Problems 3-IPE and 5-IPE) are not based on Problems 1-ABE or 2-ABE, but can be directly reduced from the DLIN assumption.

Definition 13 (Problem 1-IPE) *Problem 1-IPE is to guess* β*, given* $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,i}\}_{t=1,\ldots,d; i=1,2}, \widetilde{\boldsymbol{e}}_{\beta,1}, \widetilde{\boldsymbol{e}}_2) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1\text{-}IPE}}_{\beta}(1^\lambda, d)$*, where*

$$\begin{aligned}
\mathcal{G}^{\mathsf{P1\text{-}IPE}}_{\beta}(1^\lambda, d): \quad & (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 15)), \\
& \varphi_0, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}, \\
& \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}), \ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15}), \\
& \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}), \ \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, .., \boldsymbol{b}^*_4, \boldsymbol{b}^*_{12}, \boldsymbol{b}^*_{13}),
\end{aligned}$$

$$\boldsymbol{e}_{0,0} := (\omega,0,0,0,\varphi_0)_{\mathbb{B}_0},\ \boldsymbol{e}_{1,0} := (\omega,\tau,0,0,\varphi_0)_{\mathbb{B}_0},\ Z_t \xleftarrow{\mathsf{U}} GL(2,\mathbb{F}_q) \ \text{ for } t=1,\ldots,d,$$

$$\text{for } t=1,\ldots,d;\ i=1,2;\qquad \vec{e}_1 := (1,0),\ \vec{e}_2 := (0,1)\in\mathbb{F}_q^2,\quad \sigma_{t,i},\varphi_{t,i,1},\varphi_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\begin{array}{rccccccl}
 & & \overbrace{\hphantom{\sigma_{t,i}(1,\ t),\ \omega\vec{e}_i,}}^{4} & \overbrace{\hphantom{\tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i Z_t,\ 0,}}^{7} & \overbrace{\hphantom{0^2,}}^{2} & \overbrace{\hphantom{\varphi_{t,i,1},\varphi_{t,i,2}}}^{2} & & \\
\boldsymbol{e}_{0,t,i} := & (& \sigma_{t,i}(1,\ t),\ \omega\vec{e}_i, & 0^7, & 0^2, & \varphi_{t,i,1},\varphi_{t,i,2} &)_{\mathbb{B}}, & \\
\boldsymbol{e}_{1,t,i} := & (& \sigma_{t,i}(1,\ t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i\, Z_t,\ 0, & 0^2, & \varphi_{t,i,1},\varphi_{t,i,2} &)_{\mathbb{B}}, & \\
\widetilde{\boldsymbol{e}}_{0,1} := & (& \widetilde{\sigma},\ 0^3, & 0^7, & 0^2, & \widetilde{\varphi}_1,\widetilde{\varphi}_2 &)_{\mathbb{B}}, & \\
\widetilde{\boldsymbol{e}}_{1,1} := & (& \widetilde{\sigma},\ 0^3, & 0^6,\ \theta, & 0^2, & \widetilde{\varphi}_1,\widetilde{\varphi}_2 &)_{\mathbb{B}}, &
\end{array}$$

$$\widetilde{\boldsymbol{e}}_2 := \widetilde{\sigma}\boldsymbol{b}_2,$$

$$\text{return } (\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,i}\}_{t=1,..,d;i=1,2}, \widetilde{\boldsymbol{e}}_{\beta,1}, \widetilde{\boldsymbol{e}}_2),$$

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

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

For any adversary $\mathcal{B}$, *there exist probabilistic machines* $\mathcal{F}_0,\mathcal{F}_1,\mathcal{F}_2$, *whose running times are essentially the same as that of* $\mathcal{B}$, *such that for any security parameter* λ, $\mathsf{Adv}^{\mathsf{P1\text{-}IPE}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_0}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_1}(\lambda) + \sum_{p=1}^{d}\sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}j}}(\lambda) + \epsilon$, *where* $\mathcal{F}_{2\text{-}p\text{-}j}(\cdot) := \mathcal{F}_2(p,j,\cdot), \epsilon := (10d+5)/q$.

Lemma 3 is proven in Appendix A.1.1.

Definition 14 (Problem 2-IPE) *Problem 2-IPE is to guess* β, *given* $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2\text{-}IPE}}_{\beta}(1^\lambda,d)$, *where*

$$\mathcal{G}^{\mathsf{P2\text{-}IPE}}_{\beta}(1^\lambda,d):\ \ (\mathsf{param},(\mathbb{B}_0,\mathbb{B}^*_0),(\mathbb{B},\mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda,(N_0 := 5, N := 15)),$$

$$\delta,\eta_0,\varphi_0,\omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \tau,\rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,$$

$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1},\boldsymbol{b}_{0,3},\boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1,..,\boldsymbol{b}_4,\boldsymbol{b}_{14},\boldsymbol{b}_{15}),$$

$$\widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1},..,\boldsymbol{b}^*_{0,4}),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1,..,\boldsymbol{b}^*_4,\boldsymbol{b}^*_{11},\boldsymbol{b}^*_{12},\boldsymbol{b}^*_{12},\boldsymbol{b}^*_{13}),$$

$$\boldsymbol{h}^*_{0,0} := (\delta,0,0,\eta_0,0)_{\mathbb{B}^*_0},\ \boldsymbol{h}^*_{1,0} := (\delta,\rho,0,\eta_0,0)_{\mathbb{B}^*_0},\ \boldsymbol{e}_0 := (\omega,\tau,0,0,\varphi_0)_{\mathbb{B}_0},$$

$$Z_t \xleftarrow{\mathsf{U}} GL(2,\mathbb{F}_q),\ U_t := (Z_t^{-1})^{\mathrm{T}},\ \text{ for } t=1,..,d,$$

$$\text{for } t=1,\ldots,d;\ i=1,2;\quad \vec{e}_1 := (1,0),\vec{e}_2 := (0,1)\in\mathbb{F}_q^2,$$

$$\mu_{t,i},\sigma_{t,i},\eta_{t,i,1},\eta_{t,i,2},\varphi_{t,i,1},\varphi_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\begin{array}{rccccccl}
 & & \overbrace{\hphantom{\mu_{t,i}(t,\ -1),\ \delta\vec{e}_i,}}^{4} & \overbrace{\hphantom{\tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i Z_t,\ 0,}}^{7} & \overbrace{\hphantom{\eta_{t,i,1},\eta_{t,i,2}}}^{2} & \overbrace{\hphantom{\varphi_{t,i,1},\varphi_{t,i,2}}}^{2} & & \\
\boldsymbol{h}^*_{0,t,i} := & (& \mu_{t,i}(t,\ -1),\ \delta\vec{e}_i, & 0^7, & \eta_{t,i,1},\eta_{t,i,2} & 0^2 &)_{\mathbb{B}^*}, & \\
\boldsymbol{h}^*_{1,t,i} := & (& \mu_{t,i}(t,\ -1),\ \delta\vec{e}_i, & 0^4,\quad \rho\vec{e}_i\, U_t,\ 0, & \eta_{t,i,1},\eta_{t,i,2} & 0^2 &)_{\mathbb{B}^*}, & \\
\boldsymbol{e}_{t,i} := & (& \sigma_{t,i}(1,\ t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i\, Z_t,\ 0, & 0^2, & \varphi_{t,i,1},\varphi_{t,i,2} &)_{\mathbb{B}}, &
\end{array}$$

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{B}$, *the advantage of* $\mathcal{B}$ *for Problem 2-IPE,* $\mathsf{Adv}^{\mathsf{P2\text{-}IPE}}_{\mathcal{B}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 4 *Problem 2-IPE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, there exist probabilistic machines $\mathcal{F}_1, \mathcal{F}_{2\text{-}1}, \ldots, \mathcal{F}_{2\text{-}5}$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P2\text{-}IPE}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_1}(\lambda) + \sum_{p=1}^{d} \sum_{j=1}^{2} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}2\text{-}j}}(\lambda) + \sum_{l=1,\ldots,d;\ l\neq p} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}}(\lambda) \Big) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}5\text{-}j}}(\lambda) \Big) + \epsilon$, where $\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}1}(p, j, \cdot), \mathcal{F}_{2\text{-}p\text{-}2\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}2}(p, j, \cdot)$, $\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}3}(p, j, l, \cdot), \mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}4}(p, j, l, \cdot), \mathcal{F}_{2\text{-}p\text{-}5\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}5}(p, j, \cdot)$ and $\epsilon := (20d^2 + 10d + 5)/q$.

Lemma 4 is proven in Appendix A.1.2.

Definition 15 (Problem 3-IPE) *Problem 3-IPE is to guess β, given $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*, \boldsymbol{e}_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P3\text{-}IPE}}_{\beta}(1^\lambda)$, where*

$$\mathcal{G}^{\mathsf{P3\text{-}IPE}}_{\beta}(1^\lambda): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 15)),$$

$$r, u, \omega, \tau, z_i, \eta_i, \varphi_i \xleftarrow{\mathsf{U}} \mathbb{F}_q \text{ for } i = 1, 2, \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \boldsymbol{b}_4^*, \boldsymbol{b}_6^*, \ldots, \boldsymbol{b}_{15}^*),$$

$$\begin{array}{rlccccl}
 & & \overbrace{\qquad\qquad\qquad}^{4} & \overbrace{\qquad\qquad\qquad\qquad\qquad}^{7} & \overbrace{\qquad\qquad}^{2} & \overbrace{\qquad\qquad}^{2} & \\
\boldsymbol{h}^* := & (& 0^2,\ u,\ 0, & 0^4,\ \ r,\ \ 0^2, & \eta_1, \eta_2, & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{e}_0 := & (& 0^4, & 0^4,\ \ z_1,\ z_2,\ 0, & 0^2, & \varphi_1, \varphi_2 &)_{\mathbb{B}}, \\
\boldsymbol{e}_1 := & (& 0^2,\ \omega,\ 0, & \tau,\ \ 0^3,\ \ z_1,\ z_2,\ 0, & 0^2, & \varphi_1, \varphi_2 &)_{\mathbb{B}},
\end{array}$$

$$\text{return } (\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*, \boldsymbol{e}_\beta),$$

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 3-IPE, $\mathsf{Adv}^{\mathsf{P3\text{-}IPE}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 13.

Lemma 5 *Problem 3-IPE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, there exist probabilistic machines $\mathcal{F}$ whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P3\text{-}IPE}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + \epsilon$, where $\epsilon := 5/q$.

Lemma 5 is proven by combining proofs of (straightforward extensions of) Lemmas 1 and 2 in [14].

Definition 16 (Problem 4-IPE) *Problem 4-IPE is to guess β, given $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{h}_0^*, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,..,d; i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P4\text{-}IPE}}_{\beta}(1^\lambda, d)$, where*

$$\mathcal{G}^{\mathsf{P4\text{-}IPE}}_{\beta}(1^\lambda, d): \ (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 15)), \ \eta_0, \varphi_0, \tau, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}), \ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{11}, \boldsymbol{b}_{14}, \boldsymbol{b}_{15}),$$

$$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*), \ \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, .., \boldsymbol{b}_4^*, \boldsymbol{b}_{11}^*, \boldsymbol{b}_{12}^*, \boldsymbol{b}_{13}^*),$$

$$\boldsymbol{h}_0^* := (0, \rho, 0, \eta_0, 0)_{\mathbb{B}_0^*}, \ \boldsymbol{e}_0 := (0, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0},$$

$$Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q), \ U_t := (Z_t^{-1})^{\mathrm{T}}, \text{ for } t = 1, .., d,$$

$$\text{for } t = 1, \ldots, d; \ i = 1, 2; \quad \vec{e}_1 := (1, 0), \vec{e}_2 := (0, 1) \in \mathbb{F}_q^2,$$

$$\mu_{t,i}, \sigma_{t,i}, \eta_{t,i,1}, \eta_{t,i,2}, \varphi_{t,i,1}, \varphi_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\begin{array}{rlccccl}
 & & \overbrace{\qquad\qquad\qquad}^{4} & \overbrace{\qquad\qquad\qquad\qquad\qquad}^{7} & \overbrace{\qquad\qquad}^{2} & \overbrace{\qquad\qquad}^{2} & \\
\boldsymbol{h}^*_{0,t,i} := & (& \mu_{t,i}(t,\ -1),\ 0^2, & 0^4,\ \ \rho\vec{e}_i\,U_t,\ 0, & \eta_{t,i,1}, \eta_{t,i,2} & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{h}^*_{1,t,i} := & (& \mu_{t,i}(t,\ -1),\ 0^2, & \rho\vec{e}_i,\ \ \ 0^5, & \eta_{t,i,1}, \eta_{t,i,2} & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{e}_{t,i} := & (& \sigma_{t,i}(1,\ t),\ 0^2, & \tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i\,Z_t,\ 0, & 0^2, & \varphi_{t,i,1}, \varphi_{t,i,2} &)_{\mathbb{B}},
\end{array}$$

$$\text{return } (\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{h}_0^*, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d; i=1,2}),$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{B}$, *the advantage of* $\mathcal{B}$ *for Problem 4-IPE,* $\mathsf{Adv}^{\mathsf{P4\text{-}IPE}}_{\mathcal{B}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 6 *Problem 4-IPE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, *there exist probabilistic machines* $\mathcal{F}_{3\text{-}1}, \ldots, \mathcal{F}_{3\text{-}5}$, *whose running times are essentially the same as that of* $\mathcal{B}$, *such that for any security parameter* λ, $\mathsf{Adv}^{\mathsf{P4\text{-}IPE}}_{\mathcal{B}}(\lambda) \leq \sum_{p=1}^{d} \sum_{j=1}^{2} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{3\text{-}p\text{-}1\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{3\text{-}p\text{-}2\text{-}j}}(\lambda) + \sum_{l=1,\ldots,d;\ l \neq p} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{3\text{-}p\text{-}3\text{-}j\text{-}l}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{3\text{-}p\text{-}4\text{-}j\text{-}l}}(\lambda) \Big)$ $+ \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{3\text{-}p\text{-}5\text{-}j}}(\lambda) \Big) + \epsilon$, *where* $\mathcal{F}_{3\text{-}p\text{-}1\text{-}j}(\cdot) := \mathcal{F}_{3\text{-}1}(p,j,\cdot), \mathcal{F}_{3\text{-}p\text{-}2\text{-}j}(\cdot) := \mathcal{F}_{3\text{-}2}(p,j,\cdot)$, $\mathcal{F}_{3\text{-}p\text{-}3\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{3\text{-}3}(p,j,l,\cdot), \mathcal{F}_{3\text{-}p\text{-}4\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{3\text{-}4}(p,j,l,\cdot), \mathcal{F}_{3\text{-}p\text{-}5\text{-}j}(\cdot) := \mathcal{F}_{3\text{-}5}(p,j,\cdot)$ *and* $\epsilon := (20d^2 + 10d)/q$.

Lemma 6 is proven in a similar manner to Lemma 4.

Definition 17 (Problem 5-IPE) *Problem 5-IPE is to guess* β, *given* $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{h}^*_\beta, \{\boldsymbol{e}_j\}_{j=0,1}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P8\text{-}IPE}}_{\beta}(1^\lambda)$, *where*

$$\begin{array}{l}
\mathcal{G}^{\mathsf{P5\text{-}IPE}}_{\beta}(1^\lambda): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 15)), \\
\quad \tau_i, \theta_i, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ for } i = 0,1, \quad \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_6, \ldots, \boldsymbol{b}_{10}, \boldsymbol{b}_{12}, \ldots, \boldsymbol{b}_{15}), \\
\quad \text{for } i = 0,1; \quad \eta_1, \eta_2, \varphi_{i,1}, \varphi_{i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,
\end{array}$$

$$\begin{array}{rccccccl}
 & \overbrace{\hphantom{0^4,}}^{4} & \multicolumn{3}{c}{\overbrace{\hphantom{\tau_i, \quad 0^6, \quad \theta_i,}}^{7}} & \overbrace{\hphantom{\eta_1,\eta_2}}^{2} & \overbrace{\hphantom{\varphi_{i,1},\varphi_{i,2}}}^{2} & \\
\boldsymbol{h}^*_0 := \ (& 0^4, & \rho, & 0^6, & & \eta_1, \eta_2 & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{h}^*_1 := \ (& 0^4, & & 0^6, & \rho, & \eta_1, \eta_2 & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{e}_i := \ (& 0^4, & \tau_i, & 0^5, & \theta_i, & 0^2, & \varphi_{i,1}, \varphi_{i,2} &)_{\mathbb{B}},
\end{array}$$

$$\quad \text{return } (\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{h}^*_\beta, \{\boldsymbol{e}_i\}_{i=0,1}),$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{B}$, *the advantage of* $\mathcal{B}$ *for Problem 5-IPE,* $\mathsf{Adv}^{\mathsf{P5\text{-}IPE}}_{\mathcal{B}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 7 *Problem 5-IPE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, *there exist probabilistic machines* $\mathcal{F}$ *whose running times are essentially the same as that of* $\mathcal{B}$, *such that for any security parameter* λ, $\mathsf{Adv}^{\mathsf{P5\text{-}IPE}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + \epsilon$, *where* $\epsilon := 8/q$.

Lemma 7 is proven in a similar manner to Lemma 4 in [16] (i.e., security of Problem 3 in [16]).

Next is a key probabilistic (or information-theoretic) lemma used in the proofs of Lemmas 11 and 19.

Lemma 8 (Lemma 3 in [14]) *For* $p \in \mathbb{F}_q$, *let* $C_p := \{(\vec{x}, \vec{v}) | \vec{x} \cdot \vec{v} = p\} \subset V \times V^*$ *where* V *is* n*-dimensional vector space* $\mathbb{F}_q^n$, *and* V^* *its dual. For all* $(\vec{x}, \vec{v}) \in C_p$, *for all* $(\vec{r}, \vec{w}) \in C_p$, $\Pr[\vec{x}U = \vec{r} \ \wedge \ \vec{v}Z = \vec{w}] = \Pr[\vec{x}Z = \vec{r} \ \wedge \ \vec{v}U = \vec{w}] = 1/\sharp C_p$, *where* $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$.

5.1.5 Proof Outline of Lemma 1

At the top level of strategy of the security proof, we follow the dual system encryption methodology proposed by Waters [21]. In the methodology, ciphertexts and secret keys have two forms, *normal* and *semi-functional*. In the proof herein, we also introduce another form of secret keys called *pre-semi-functional*, which is called nominally semi-functional in [9]. The real system uses only normal ciphertexts and normal secret keys, and semi-functional ciphertexts and semi-functional/pre-semi-functional keys are used only in a sequence of security games for the security proof.

To prove this theorem, we employ Game 0' (defined in the proof of Theorem 1) through Game 4. As in the original dual system encryption, challenge ciphertexts have a final (or *randomized*) form in the final game (Game 4). In the proof herein, we also use another form of ciphertext, which we call *semi-randomized* form, in Game 3. This form and an additional game transformation from Game 3 to 4 is necessary for achieving security using limited randomness in public parameters.

In Game 1, the challenge ciphertext is changed to semi-functional. When at most ν key queries are issued, there are 2ν game changes from Game 1 (Game 2-0-2), Game 2-1-1, Game 2-1-2, through Game 2-ν-2.

In Game 2-h-1, the first $(h-1)$ keys are semi-functional and the h-th key is *pre-semi-functional*, while the remaining keys are normal, and the challenge ciphertext is semi-functional. In Game 2-h-2, the first h keys are semi-functional (i.e., and the h-th key is *semi-functional*), while the remaining keys are normal, and the challenge ciphertext is semi-functional.

The next game (Game 3) with *semi-randomized* challenge ciphertext is conceptually changed from Game 2-ν-2, and the final game (Game 4) with *randomized* challenge ciphertext is computationally changed from Game 3. As usual, we prove that the advantage gaps between neighboring games are negligible. In this proof outline, we ignore a negligible factor in the (informal) descriptions of this proof outline. For example, we say "A is bounded by B" when $A \leq B + \epsilon(\lambda)$ where $\epsilon(\lambda)$ is negligible in security parameter λ.

When at most ν key queries are issued by an adversary, we set a sequence of $\mathsf{sk} := \mathsf{sk}_{\vec{v}}$'s, i.e., $(\mathsf{sk}^{(1)*}, \ldots, \mathsf{sk}^{(\nu)*})$, in the order of the adversary's queries. A *normal* secret key, $\mathsf{sk}_{\vec{v}}^{(h)*\mathsf{norm}}$, is the correct form of the secret key of the proposed IPE scheme, and is expressed by Eq. (3). Similarly, a *normal* ciphertext $\mathsf{ct}_{\vec{x}}^{\mathsf{norm}}$, is expressed by Eq. (4). A *pre-semi-functional* secret key, $\mathsf{sk}_{\vec{v}}^{(h)*\ \mathsf{psemi}}$, is expressed by Eq. (6), a *semi-functional* secret key, $\mathsf{sk}_{\vec{v}}^{(h)*\ \mathsf{semi}}$, is expressed by Eq. (7), and a *semi-functional* ciphertext, $\mathsf{ct}_{\vec{x}}^{\mathsf{semi}}$, is expressed by Eq. (5). A *semi-randomized* ciphertext is expressed by Eq. (8), and a *randomized* ciphertext is expressed by Eq. (9).

To prove that the advantage gap between Games 0 and 1 is bounded by the advantage of Problem 1-IPE (to guess $\beta \in \{0,1\}$), we construct a simulator of the challenger of Game 0' (or 1) (against an adversary $\mathcal{A}$) by using an instance with $\beta \xleftarrow{\mathsf{U}} \{0,1\}$ of Problem 1-IPE. 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 Game 1 when $\beta = 1$. That is, the advantage gap between Games 0 and 1 is bounded by the advantage of Problem 1-IPE (Lemma 9). The advantage of Problem 1-IPE is proven to be bounded by that of the DLIN assumption (Lemma 3).

The advantage gap between Games 2-$(h-1)$-2 and 2-h-1 is similarly shown to be bounded by the advantage of Problem 2-IPE (i.e., advantage of the DLIN assumption) (Lemmas 10 and 4).

The distributions of *pre-semi-functional* secret key $\mathsf{sk}_{\vec{v}}^{(h)*\ \mathsf{psemi}}$ (Eq. (6)) and *semi-functional* secret key $\mathsf{sk}_{\vec{v}}^{(h)*\ \mathsf{semi}}$ (Eq. (7)) are distinguishable by the simulator or challenger, but the joint distributions of $(\mathsf{sk}_{\vec{v}}^{(h)*\ \mathsf{psemi}}, \mathsf{ct}_{\vec{x}}^{\mathsf{semi}})$ and $(\mathsf{sk}_{\vec{v}}^{(h)*\ \mathsf{semi}}, \mathsf{ct}_{\vec{x}}^{\mathsf{semi}})$ along with the other keys are (information theoretically) equivalent for the adversary's view, when $\vec{v}$ and $\vec{x}$ are not orthogonal. Therefore, as shown in Lemma 11, the advantages of Games 2-h-1 and 2-h-2 are equivalent.

We show that Game 2-ν-2 can be conceptually changed to Game 3 (Lemma 12) by using the fact that basis vectors of $\boldsymbol{b}_{0,2}$ and $\boldsymbol{b}_{0,3}^{*}$ are unknown to the adversary (and matrices Z_t are uniformly and independently distributed).

Finally, we show the advantage gap between Games 3 and 4 is bounded by the advantage of Problem 3-IPE (i.e., advantage of the DLIN assumption) (Lemmas 13 and 5).

5.1.6 Proof of Lemma 1

To prove Lemma 1, we consider the following 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 an experiment from the previous game. Games proceed as follows:

Game 0' ⇒ Game 1 ⇒ (for $h = 1, \ldots, \nu$; Game 2-h-1 ⇒ Game 2-h-2) ⇒ Game 3 ⇒ Game 4

Game 0' : Same as Game 0 except that flip a coin $\kappa \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted in step 3 if $\kappa \neq s$. In order to prove Lemma 1, we consider the case with $\kappa = 0$. The reply to a key query for $\vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}}\}$ is:

$$\left.\begin{array}{l}
\boldsymbol{k}_0^* := (\, -s_0,\ \boxed{0},\ 1,\ \eta_0,\ 0\,)_{\mathbb{B}_0^*}, \\
\text{for } t \in I_{\vec{v}},\ \ \boldsymbol{k}_t^* := (\ \ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t}^{4}\ \ \overbrace{0^4,\ \boxed{0^2},0,}^{7}\ \ \overbrace{\vec{\eta}_t,}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*}.
\end{array}\right\} \tag{3}$$

This is called a normal key. The challenge ciphertext for challenge plaintexts $(m^{(0)}, m^{(1)})$ and attributes $\vec{x}^{(b)} := \{(t, x_t^{(b)}) \,|\, t \in I_{\vec{x}}\}$ with $I_{\vec{x}} := I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ is:

$$\left.\begin{array}{l}
\boldsymbol{c}_0 := (\, \widetilde{\omega},\ \boxed{0},\ \boxed{\zeta},\ 0,\ \varphi_0\,)_{\mathbb{B}_0}, \quad c_T := g_T^{\zeta} m^{(b)}, \\
\text{for } t \in I_{\vec{x}},\ \ \boldsymbol{c}_t := (\ \ \overbrace{\sigma_t(1,\ t),\ \boxed{\omega x_t^{(b)}},\ \widetilde{\omega}}^{4}\ \ \overbrace{\boxed{0^2},\ 0^2,\ \boxed{0^2},0,}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_t}^{2}\ \ )_{\mathbb{B}},
\end{array}\right\} \tag{4}$$

where $b \xleftarrow{\mathsf{U}} \{0,1\}$. This is called a normal ciphertext.

Game 1: Same as Game 0' except that the challenge ciphertext is:

$$\left.\begin{array}{l}
\boldsymbol{c}_0 := (\, \widetilde{\omega},\ \boxed{\widetilde{\tau}},\ \zeta,\ 0,\ \varphi_0\,)_{\mathbb{B}_0}, \quad c_T := g_T^{\zeta} m^{(b)}, \\
\text{for } t \in I_{\vec{x}}, \\
\boldsymbol{c}_t := (\ \ \overbrace{\sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},}^{4}\ \ \overbrace{\boxed{\tau x_t^{(b)},\ \widetilde{\tau}},\ 0^2, \boxed{(\tau x_t^{(b)},\ \widetilde{\tau}) \cdot Z_t},\ 0,}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_t}^{2}\ \ )_{\mathbb{B}},
\end{array}\right\} \tag{5}$$

where $\tau, \widetilde{\tau} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}$, $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$, and all the other variables are generated as in Game 0'. This is called a semi-functional ciphertext.

Game 2-h-1 ($h = 1, \ldots, \nu$)**:** Game 2-0-2 is Game 1. Game 2-h-1 is the same as Game 2-$(h-1)$-2 except the reply, $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$, for the h-th key query for $\vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}}\}$ are:

$$\left.\begin{array}{l}
\boldsymbol{k}_0^* := (\, -s_0,\ \boxed{-a_0},\ 1,\ \eta_0,\ 0\,)_{\mathbb{B}_0^*}, \\
\text{for } t \in I_{\vec{v}},\ \boldsymbol{k}_t^* := (\ \ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t,}^{4}\ \ \overbrace{0^4,\ \boxed{(\pi v_t,\ a_t) \cdot U_t},\ 0,}^{7}\ \ \overbrace{\vec{\eta}_t,}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},
\end{array}\right\} \tag{6}$$

where $a_t \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ a_0 := \sum_{t\in I_{\vec v}} a_t,\ U_t := (Z_t^{-1})^{\mathrm{T}}$ for $Z_t \xleftarrow{\mathsf{U}} GL(2,\mathbb{F}_q)$ used in Eq. (19) and $t \in I_{\vec v}$, and $\pi \xleftarrow{\mathsf{U}} \mathbb{F}_q$. All the other variables are generated as in Game 2-$(h-1)$-2. This is called a pre-semi-functional key.

Game 2-h-2 $(h = 1,\dots,\nu)$**:** Game 2-h-2 is the same as Game 2-h-1 except the reply, $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t\in I_{\vec v}})$, for the h-th key query for $\vec v := \{(t, v_t)\,|\, t \in I_{\vec v}\}$ are:

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (\ -s_0,\ \boxed{r_0},\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}_0^*}, \\ \text{for } t \in I_{\vec v},\quad \boldsymbol{k}_t^* := (\ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t,}^{4}\ \ \overbrace{0^4,\ \boxed{\vec r_t},\ 0,}^{7}\ \ \overbrace{\vec\eta_t,}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*}, \end{array}\right\} \qquad (7)$$

where $r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec r_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$. All the other variables are generated as in Game 2-h-1. This is called a semi-functional key.

Game 3: Same as Game 2-ν-2 except that the challenge ciphertext is:

$$\left.\begin{array}{l} \boldsymbol{c}_0 := (\ \widetilde\omega,\ \widetilde\tau,\ \boxed{\zeta'},\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, \qquad c_T := g_T^{\zeta} m^{(b)}, \\ \text{for } t \in I_{\vec x}, \\ \quad \boldsymbol{c}_t := (\ \ \overbrace{\sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde\omega,}^{4}\ \ \overbrace{\tau x_t^{(b)},\ \widetilde\tau,\ 0^2, \boxed{z_{t,1}, z_{t,2}},\ 0,}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec\varphi_t}^{2}\ \ )_{\mathbb{B}}, \end{array}\right\} \qquad (8)$$

where $\zeta', z_{t,1}, z_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and all the other variables are generated as in Game 2-ν-2. This is called a semi-randomized ciphertext.

Game 4: Same as Game 3 except that the challenge ciphertext is:

$$\left.\begin{array}{l} \boldsymbol{c}_0 := (\ \widetilde\omega,\ \widetilde\tau,\ \zeta',\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, \qquad c_T := g_T^{\zeta} m^{(b)}, \\ \text{for } t \in I_{\vec x},\quad \boldsymbol{c}_t := (\ \ \overbrace{\sigma_t(1,\ t),\ \boxed{0},\ \widetilde\omega,}^{4}\ \ \overbrace{\boxed{0},\ \widetilde\tau,\ 0^2,\ z_{t,1}, z_{t,2},\ 0,}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec\varphi_t}^{2}\ \ )_{\mathbb{B}}, \end{array}\right\} \qquad (9)$$

where all the variables are generated as in Game 3. Note that the ciphertext is independent from bit b. This is called a randomized ciphertext.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}j)}(\lambda)$ $(h = 1,\dots,\nu; j = 1,2)$, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0, 1, 2\text{-}h\text{-}j, 3$ and 4 when $\kappa = 0$, respectively. $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda)$ is equivalent to $\Pr[\mathcal{A}\,\text{wins}\,|\kappa = 0]$ and it is obtained that $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda) = 0$ by Lemma 14.

We will show five lemmas (Lemmas 9-13) that evaluate the gaps between pairs of $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)$ for $h = 1,\dots,\nu$, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)$. From these lemmas, we obtain $\Pr[\mathcal{A}\,\text{wins}\,|\kappa = 0] = \mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) \le \left|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| + \sum_{h=1}^{\nu} \Big(\Big|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)\Big| + \Big|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)\Big|\Big) + \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)\right| + \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda) \le \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1\text{-}IPE}}(\lambda) + \sum_{h=1}^{\nu} \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2\text{-}IPE}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_3}^{\mathsf{P3\text{-}IPE}}(\lambda) + (2\nu + 4)/q$. Therefore, from Lemmas 3–5, we obtain the upperbound in Lemma 1. This completes the proof of Lemma 1. □

Lemmas 9–13 are proven in Appendix A.2.

Lemma 9 *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,* $|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1\text{-}IPE}}(\lambda)$.

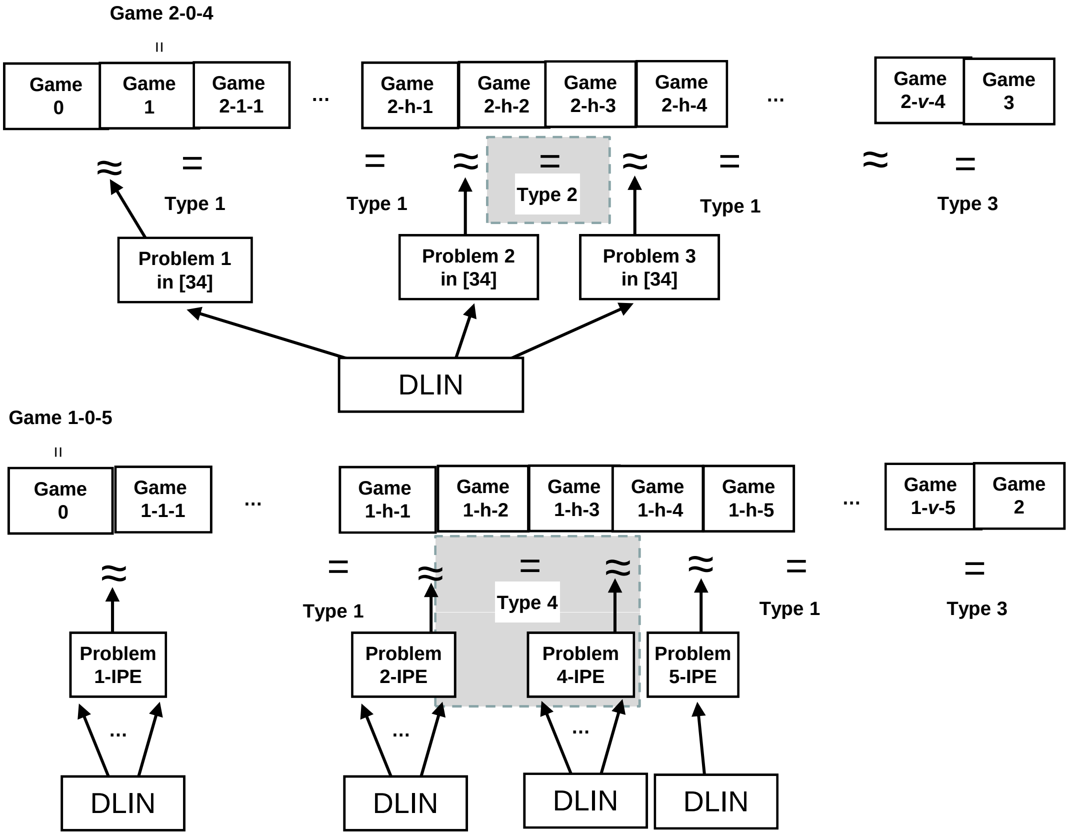


Figure 1: Structures of Reductions: The upper one is that used in [16], and the lower one is that used in the proof of Lemma 2.

Lemma 10 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2\text{-}IPE}}(\lambda) + 2/q$, where $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.*

Lemma 11 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)$.*

Lemma 12 *For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \leq 1/q$.*

Lemma 13 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_3$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_3}^{\mathsf{P3\text{-}IPE}}(\lambda) + 3/q$.*

Lemma 14 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda) = 0$.*

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

5.1.7 Proof Outline of Lemma 2

Structure of Game Transformation for Proof of Lemma 2 At the top level strategy of the security proof, an extended form of the dual system encryption (DSE), which was introduced in [16], is employed. We will first explain the extended methodology comparing with the original DSE, briefly.

In the original form [21, 14], the first goal of game transformations is to insert a pair of random coefficients in a hidden subspace of challenge ciphertext and queried keys (e.g., Game 2-h-2 in the proof of Lemma 1), and then the random distribution of the pairs is reflected to the real (or normal) encoded part, i.e., the challenge vector $\vec{x}^{(b)}$ is totally randomized (e.g., Game 3 in the proof of Lemma 1). For dealing with the $\kappa = 1$ case, the main difficulty resides in how to change a (normal) secret key queried with $\vec{v}$ to another form, without knowing whether $R(\vec{v}, \vec{x}^{(b)}) = 0$ or not (non-matching or matching). Here, an adversary may issue key queries with $\vec{v}$ before issuing the challenge ciphertext query with $\vec{x}^{(b)}$ $(b = 0, 1)$ and two possible cases, $R(\vec{v}, \vec{x}^{(b)}) = 0$ (for all $b = 0, 1$) and $R(\vec{v}, \vec{x}^{(b)}) = 1$ (for all $b = 0, 1$), are allowed.

Here, a key fact is that $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = R(\vec{v}, \omega_0\vec{x}^{(0)} + \omega_1\vec{x}^{(1)})$ for $\omega_0, \omega_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ with all but negligible probability. Based on that relation, our goal of game transformations turns out to change a challenge ciphertext to the ciphertext for *unbiased* vector $\omega_0\vec{x}^{(0)} + \omega_1\vec{x}^{(1)}$ with respect to bit $b \in \{0, 1\}$. For achieving that change, [16] also used hidden subspace in a different manner from the original DSE (e.g., the proof of Lemma 1). In [16], only $\vec{v}$ is encoded in a hidden subspace of the temporal forms of a secret key, and a random vector in $\mathsf{span}\langle\vec{x}^{(0)}, \vec{x}^{(1)}\rangle$ is encoded in the corresponding hidden subspace for the temporal and final forms of a ciphertext. The change is based on a pairwise independence lemma (Lemma 8), which can be only applied one by one for a pair of key and ciphertext. Since the encoded vectors ($\vec{v}$, $\omega_0\vec{x}^{(0)} + \omega_1\vec{x}^{(1)}$) have non-uniform distribution, which are different from the original DSE case, we need one more n-dimensional block to accumulate the transformed pairs of coefficients. Moreover, the swapping of coefficients between two (hidden) blocks is achieved by a computational change in [16]. After that, [16] has *unbiased* ciphertext for $b \in \{0, 1\}$ by reflecting the accumulated results to real encoding part, by a conceptual change.

In this paper, we must accomplish the above transformations *with limited public parameter randomness.* We turn to the outline of our game transformation. Figure 1 compares the structures of the security reductions in [16] (the upper figure) and that for Lemma 2 (the lower figure). The security of the schemes is hierarchically reduced to the intractability of the DLIN problem. In [16], three types of computational changes by Problems 1, 2, and 3 and three types of conceptual changes (Types 1, 2, and 3) are used alternately. With limited randomness in public parameters, Type 2 conceptual change is impossible to achieve, so we need an alternative mean for our purpose.

Type 2 conceptual change is shaded in the reduction used in [16]. In fact, that change is given by combining 3 conceptual changes, in which the first and third conceptual changes are not achievable under unbounded setting. The changes needed public parameter randomness *for each index* t, which generates hidden (from the adversary) parameters in transient games. Therefore, we replace these changes by *computational* changes in our reduction, i.e., (a part of) the computational change by Problem 2-IPE and the computational change by Problem 4-IPE, respectively. Together with the central conceptual change (of Type 4), these changes are also shaded in the lower one of Figure 1.

Game Description At the top level strategy of the security proof, an extended form of the dual system encryption (DSE), which was introduced in [16], is employed. In our game transformations, ciphertexts have four forms, *normal*, *1-st temporary*, *2-nd temporary*, and *unbiased*, and secret keys have four forms, *normal*, *1-st temporary*, *2-nd temporary*, and *final*. The real system uses only normal ciphertexts and normal secret keys, and the other types of ciphertexts and keys are used only in a sequence of security games for the security proof.

To prove this lemma, we only consider the $\kappa = 1$ case. We employ Game 0' (described in

Table 3: Outline of Game Descriptions

Game	Challenge	Queried keys				
	ciphertext	1	$\cdots$ $h-1$	h	$h+1$ $\cdots$	ν
0’	normal	normal				
1-1-1	1-st temp.	normal				
1-1-2	1-st temp.	1-st temp.	normal			
1-1-3	2-nd temp.	1-st temp.	normal			
1-1-4	2-nd temp.	2-nd temp.	normal			
1-1-5	2-nd temp.	final	normal			
$\vdots$						
1-h-1	1-st temp.	final		normal		
1-h-2	1-st temp.	final		1-st temp.	normal	
1-h-3	2-nd temp.	final		1-st temp.	normal	
1-h-4	2-nd temp.	final		2-nd temp.	normal	
1-h-5	2-nd temp.	final		final	normal	
$\vdots$						
1-ν-5	2-nd temp.	final				final
2	unbiased	final				

the proof of Theorem 1) through Game 2. When at most ν secret key queries are issued by an adversary, there are 5ν game changes from Game 0’ (Game 1-0-5), Game 1-1-1 through Game 1-ν-5.

In Game 1-h-1, the challenge ciphertext is changed to 1-st temporary form, and the first $h-1$ keys are final form, while the remaining keys are normal. In Game 1-h-2, the h-th key is changed to 1-st temporary form while the challenge ciphertext and the remaining keys are the same as in Game 1-h-1. In Game 1-h-3, the challenge ciphertext is changed to 2-nd temporary form while all the queried keys are the same as in Game 1-h-2. In Game 1-h-4 and 1-h-5, the h-th key is changed to 2-nd temporary and final form while the remaining keys and the challenge ciphertext are the same as the previous games, i.e., in Game 1-h-3 and 1-h-4, respectively. At the end of the Game 1 sequence, in Game 1-ν-5, all the queried keys are final form (and the challenge ciphertext is 2-nd temporary form), which allows the next conceptual change to Game 2. In Game 2, the challenge ciphertext is changed to *unbiased* form (while all the queried keys are final form). In the final game, advantage of the adversary is zero.

We summarize these changes in Table 3, where shaded parts indicate the challenge ciphertext or queried key(s) which were changed in a game from the previous game

As usual, we prove that the advantage gaps between neighboring games are negligible. In this proof outline, we ignore a negligible factor in the (informal) descriptions of this proof outline. For example, we say "A is bounded by B" when $A \le B + \epsilon(\lambda)$ where $\epsilon(\lambda)$ is negligible in security parameter λ.

A normal secret key, $\mathsf{sk}^{*\,\mathsf{norm}}$ (with vector $\vec{v}$), is the correct form of the secret key of the proposed IPE scheme, and is expressed by Eq. (10). Similarly, a normal ciphertext (with vector $\vec{x}$), $\mathsf{ct}^{\,\mathsf{norm}}$, is expressed by Eq. (11). A 1-st and 2-nd temporary ciphertexts, i.e., $\mathsf{ct}^{\,\mathsf{temp1}}$ and $\mathsf{ct}^{\,\mathsf{temp2}}$, are expressed by Eq. (12) and Eq. (14), respectively. An unbiased ciphertext is expressed by Eq. (17). A 1-st and 2-nd temporary secret key, i.e., $\mathsf{sk}^{*\,\mathsf{temp1}}$ and $\mathsf{sk}^{*\,\mathsf{temp2}}$, are expressed by Eq. (13) and Eq. (15), respectively. A final key, $\mathsf{sk}^{*\,\mathsf{final}}$, is expressed by Eq. (16).

To prove that the advantage gap between Games 0' and 1-1-1 is bounded by the advantage of Problem 1-IPE (to guess $\beta \in \{0,1\}$), we construct a simulator of the challenger of Game 0' (or 1-1-1) (against an adversary $\mathcal{A}$) by using an instance with $\beta \overset{\mathsf{U}}{\leftarrow} \{0,1\}$ of Problem 1-IPE. 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 1-1-1 when $\beta = 1$. That is, the advantage of Problem 1-IPE is equivalent to the advantage gap between Games 0' and 1-1-1 (Lemma 15). The advantage of Problem 1-IPE is proven to be equivalent to that of the DLIN assumption (Lemma 3).

The advantage gaps between Games 1-h-1 and 1-h-2, and Games 1-h-i and 1-h-$(i+1)$ for $i = 3, 4$ are shown to be bounded by the advantages of computational problems, i.e., Problems 2-IPE, 4-IPE, 5-IPE, respectively (Lemmas 17, 19, 20). These advantages are also upper-bounded by sums of advantages of the DLIN assumption (Lemmas 4, 6, 7).

In Lemma 18, we show that Game 1-h-2 can be conceptually changed to Game 1-h-3. In this conceptual change, we use the fact that all key queries $\vec{v}$ satisfy $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = 1$ or $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = 0$. Here, we notice that 1-st temporary key and 1-st temporary challenge ciphertext, $(\mathsf{sk}^{*\,\mathsf{temp1}}, \mathsf{ct}^{\mathsf{temp1}})$, are equivalent to 1-st temporary key and 2-nd temporary challenge ciphertext, $(\mathsf{sk}^{*\,\mathsf{temp1}}, \mathsf{ct}^{\mathsf{temp2}})$, except that random linear combination $\tau_0 \vec{x}^{(0)} + \tau_1 \vec{x}^{(1)}$ (with $\tau_0, \tau_1 \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$) is used in $\boldsymbol{c}_t^{\mathsf{temp2}}$ instead of $\tau \vec{x}^{(b)}$ (with $\tau \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$) for the 9-th and 10-th coefficients in $\boldsymbol{c}_t^{\mathsf{temp1}}$ for any $t \in I_{\vec{x}}$. This conceptual change is based on Lemma 8.

We then show that Game 1-ν-5 can be conceptually changed to Game 2 (Lemma 21) by using the fact that parts of bases, $\boldsymbol{b}_{11}$ and $\boldsymbol{b}_3^*$, are unknown to the adversary.

5.1.8 Proof of Lemma 2

To prove Lemma 2, we consider the following 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 an experiment from the previous game. Games proceed as in Figure 1 in Section 5.1.7.

Game 0' : Same as Game 0 except that flip a coin $\kappa \overset{\mathsf{U}}{\leftarrow} \{0,1\}$ before setup, and the game is aborted in step 3 if $\kappa \neq s$. In order to prove Lemma 1, we consider the case with $\kappa = 1$. The reply to a key query for $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$ is:

$$\left.\begin{aligned}
&\boldsymbol{k}_0^* := (\,-s_0,\ \boxed{0^2},\ 1,\ \eta_0,\ 0\,)_{\mathbb{B}_0^*},\\
&\text{for } t \in I_{\vec{v}},\quad \boldsymbol{k}_t^* := (\ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t}^{4}\quad \overbrace{\boxed{0^2},\ 0^2,\ \boxed{0^3},}^{7}\quad \overbrace{\vec{\eta}_t,}^{2}\quad \overbrace{0^2}^{2}\quad)_{\mathbb{B}^*},
\end{aligned}\right\} \qquad (10)$$

The challenge ciphertext for challenge plaintext $m := m^{(0)} = m^{(1)}$ and attributes $\vec{x}^{(b)} := \{(t, x_t^{(b)}) \mid t \in I_{\vec{x}}\}$ with $I_{\vec{x}} := I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ is:

$$\left.\begin{aligned}
&\boldsymbol{c}_0 := (\,\widetilde{\omega},\ \boxed{0^2},\ \zeta,\ 0,\ \varphi_0\,)_{\mathbb{B}_0},\qquad c_T := g_T^{\zeta} m,\\
&\text{for } t \in I_{\vec{x}},\quad \boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \boxed{\omega x_t^{(b)}},\ \widetilde{\omega}}^{4}\quad \overbrace{\boxed{0^2},\ 0^2,\ \boxed{0^3},}^{7}\quad \overbrace{0^2,}^{2}\quad \overbrace{\vec{\varphi}_t}^{2}\quad)_{\mathbb{B}},
\end{aligned}\right\} \qquad (11)$$

where $b \overset{\mathsf{U}}{\leftarrow} \{0,1\}$

Game 1-h-1 $(h = 1, \ldots, \nu)$**:** Game 1-0-5 is Game 0'. Game 1-h-1 is the same as Game

1-$(h-1)$-5 except the challenge ciphertext is:

$$\left.\begin{aligned}
&\boldsymbol{c}_0 := (\ \widetilde{\omega},\ \boxed{\widetilde{\tau}},\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, \quad c_T := g_T^{\zeta} m,\\
&\text{for } t \in I_{\vec{x}},\\
&\boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},}^{4}\\
&\qquad \overbrace{\boxed{\tau x_t^{(b)},\ \widetilde{\tau}},\ 0^2,\ \boxed{(\tau x_t^{(b)},\ \widetilde{\tau}) \cdot Z_t},\boxed{\theta_0 x_t^{(0)} + \theta_1 x_t^{(1)}},}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_t}^{2}\ \ )_{\mathbb{B}},
\end{aligned}\right\}\qquad (12)$$

where $\tau, \widetilde{\tau}, \theta_0, \theta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$, and all the other variables are generated as in Game 1-$(h-1)$-5.

Game 1-h-2 ($h = 1, \ldots, \nu$)**:** Game 1-h-2 is the same as Game 1-h-1 except the reply, $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$, for the h-th key query for $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$ are:

$$\left.\begin{aligned}
&\boldsymbol{k}_0^* := (\ -s_0,\ \boxed{-a_0},\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}_0^*},\\
&\text{for } t \in I_{\vec{v}},\ \ \boldsymbol{k}_t^* := (\ \ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t,}^{4}\ \ \overbrace{0^4,\ \boxed{(\pi v_t,\ a_t) \cdot U_t},\ 0,}^{7}\ \ \overbrace{\vec{\eta}_t,}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},
\end{aligned}\right\}(13)$$

where $a_t \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ a_0 := \sum_{t \in I_{\vec{v}}} a_t,\ U_t := (Z_t^{-1})^{\mathrm{T}}$ for $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$ used in Eq. (19) and $t \in I_{\vec{v}}$, and $\pi \xleftarrow{\mathsf{U}} \mathbb{F}_q$. All the other variables are generated as in Game 1-h-1.

Game 1-h-3 ($h = 1, \ldots, \nu$)**:** Same as Game 1-h-2 except that that the challenge ciphertext is:

$$\left.\begin{aligned}
&\boldsymbol{c}_0 := (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, \quad c_T := g_T^{\zeta} m,\\
&\text{for } t \in I_{\vec{x}},\\
&\boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},}^{4}\\
&\overbrace{\boxed{\tau_0 x_t^{(0)} + \tau_1 x_t^{(1)}},\ \widetilde{\tau},\ 0^2,\ \boxed{(\tau_0 x_t^{(0)} + \tau_1 x_t^{(1)},\ \widetilde{\tau}) \cdot Z_t},\ \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_t}^{2}\ \ )_{\mathbb{B}},
\end{aligned}\right\}(14)$$

where $\tau_0, \tau_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and all the other variables are generated as in Game 1-h-2.

Game 1-h-4 ($h = 1, \ldots, \nu$)**:** Same as Game 1-h-3 except the reply, $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$, for the h-th key query for $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$ are:

$$\left.\begin{aligned}
&\boldsymbol{k}_0^* := (\ -s_0,\ -a_0,\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}_0^*},\\
&\text{for } t \in I_{\vec{v}},\ \ \boldsymbol{k}_t^* := (\ \ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t,}^{4}\ \ \overbrace{\boxed{\pi v_t,\ a_t},\ 0^2,\ \boxed{0^2},\ 0,}^{7}\ \ \overbrace{\vec{\eta}_t,}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},
\end{aligned}\right\}(15)$$

where all the variables are generated as in Game 1-h-3.

Game 1-h-5 ($h = 1, \ldots, \nu$)**:** Same as Game 1-h-4 except the reply, $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$, for the

h-th key query for $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$ are:

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (\ -s_0,\ -a_0,\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}_0^*}, \\ \text{for } t \in I_{\vec{v}},\ \ \boldsymbol{k}_t^* := \ (\ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t,}^{4}\ \overbrace{\boxed{0},\ a_t,\ 0^4,\ \boxed{\widetilde{\pi} v_t},}^{7}\ \overbrace{\vec{\eta}_t,}^{2}\ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*}, \end{array}\right\} \quad (16)$$

where all the variables are generated as in Game 1-h-4.

Game 2: Game 2 is the same as Game 1-ν-5 except that the challenge ciphertext is:

$$\left.\begin{array}{l} \boldsymbol{c}_0 := (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, \quad c_T := g_T^{\zeta} m, \\ \text{for } t \in I_{\vec{x}}, \\ \boldsymbol{c}_t := \ (\ \overbrace{\sigma_t(1,\ t),\ \boxed{\omega_0 x_t^{(0)} + \omega_1 x_t^{(1)}},\ \widetilde{\omega},}^{4} \\ \quad \overbrace{\tau_0 x_t^{(0)} + \tau_1 x_t^{(1)},\ \widetilde{\tau},\ 0^2,\ (\tau_0 x_t^{(0)} + \tau_1 x_t^{(1)},\ \widetilde{\tau}) \cdot Z_t,\ \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},}^{7}\ \overbrace{0^2,}^{2}\ \overbrace{\vec{\varphi}_t}^{2}\ )_{\mathbb{B}}, \end{array}\right\} (17)$$

where $\omega_0, \omega_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and all the other variables are generated as in Game 1-ν-5.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}j)}(\lambda)$ $(h = 1, \ldots, \nu; j = 1, \ldots, 5)$ and $\mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0', 1$-h-j and 2 when $\kappa = 1$, respectively. $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda)$ is equivalent to $\Pr[\mathcal{A} \text{ wins} \mid \kappa = 1]$ and it is obtained that $\mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda) = 0$ by Lemma 22.

We will show seven lemmas (Lemmas 15-21) that evaluate the gaps between pairs of $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}1)}(\lambda), \ldots, \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}5)}(\lambda)$, for $h = 1, \ldots, \nu$ and $\mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda)$. From these lemmas, we obtain $\Pr[\mathcal{A} \text{ wins in Game } 0' \mid \kappa = 1] = \mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) \leq \sum_{h=1}^{\nu} \Big(\Big| \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}(h-1)\text{-}5)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}1)}(\lambda) \Big| + \sum_{j=1}^{4} \Big| \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}j)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}(j+1))}(\lambda) \Big| \Big) + \Big| \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\nu\text{-}5)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda) \Big| + \mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1\text{-}IPE}}(\lambda)$ $+ \sum_{h=1}^{\nu} \big(\mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2\text{-}IPE}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{3\text{-}h}}^{\mathsf{P4\text{-}IPE}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{4\text{-}h}}^{\mathsf{P5\text{-}IPE}}(\lambda) \big) + (15\nu + 1)/q$. Therefore, from Lemmas 3, 4, 6 and 7, we obtain the upperbound of $\Pr[\mathcal{A} \text{ wins in Game } 0' \mid \kappa = 1]$ in Lemma 2. This completes the proof of Lemma 2. □

Lemmas 15–21 are proven in Appendix A.3.

Lemma 15 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}1\text{-}1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1\text{-}IPE}}(\lambda) + 1/q$.*

Lemma 16 *Let $h \geq 2$. For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}(h-1)\text{-}5)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}1)}(\lambda)| \leq 1/q$.*

Lemma 17 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}2)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2\text{-}IPE}}(\lambda) + 2/q$, where $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.*

Lemma 18 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}2)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}3)}(\lambda)$.*

Lemma 19 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_3$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P4\text{-}IPE}}_{\mathcal{B}_{3\text{-}h}}(\lambda) + 4/q$, where $\mathcal{B}_{3\text{-}h}(\cdot) := \mathcal{B}_3(h,\cdot)$.*

Lemma 20 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_4$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}h\text{-}5)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P5\text{-}IPE}}_{\mathcal{B}_{4\text{-}h}}(\lambda)$, where $\mathcal{B}_{4\text{-}h}(\cdot) := \mathcal{B}_4(h,\cdot)$.*

Lemma 21 *For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}\nu\text{-}5)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda)| \le 1/q$.*

Lemma 22 *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda) = 0$.*

Proof. The value of b is independent from $\mathcal{A}$'s view in Game 3. Hence, $\mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda) = 0$. □

5.2 Type 2 IPE Scheme

Let $d := poly(\lambda)$, where $poly(\cdot)$ is an arbitrary polynomial.

$\mathsf{Setup}(1^\lambda):\quad (\mathsf{param}, (\mathbb{B}_0,\mathbb{B}_0^*), (\mathbb{B},\mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 15))$,
$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15})$,
$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, .., \boldsymbol{b}^*_4, \boldsymbol{b}^*_{12}, \boldsymbol{b}^*_{13})$,
return $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}),\ \mathsf{sk} := (\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*)$.

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}} \subseteq \{1,\dots,d\}\}):\ \omega, \widetilde{\omega}, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$,
$\boldsymbol{k}^*_0 := (\ \widetilde{\omega},\ 0,\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}^*_0}$,

$$\text{for } t \in I_{\vec{v}},\ \mu_t, \eta_{t,1}, \eta_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \boldsymbol{k}^*_t := (\ \overbrace{\mu_t(t,\ -1),\ \omega v_t,\ \widetilde{\omega},}^{4}\ \ \overbrace{0^7,}^{7}\ \ \overbrace{\eta_{t,1}, \eta_{t,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},$$

return $\mathsf{sk}_{\vec{v}} := (I_{\vec{v}}, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{t \in I_{\vec{v}}})$.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \vec{x} := \{(t, x_t) \,|\, t \in I_{\vec{x}} \subseteq \{1,\dots,d\}\}) : s_t, \delta, \zeta, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t \in I_{\vec{x}},\ s_0 := \sum_{t \in I_{\vec{x}}} s_t$,
$\boldsymbol{c}_0 := (\ -s_0,\ 0,\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0},\ c_T := g_T^\zeta m$,

$$\text{for } t \in I_{\vec{x}},\ \sigma_t, \varphi_{t,1}, \varphi_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \boldsymbol{c}_t := (\ \ \overbrace{\sigma_t(1,\ t),\ \delta x_t,\ s_t,}^{4}\ \ \overbrace{0^7,}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\varphi_{t,1}, \varphi_{t,2}}^{2}\ \ )_{\mathbb{B}},$$

return $\mathsf{ct}_{\vec{x}} := (I_{\vec{x}}, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := (I_{\vec{v}}, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{t \in I_{\vec{v}}}),\ \mathsf{ct}_{\vec{x}} := (I_{\vec{x}}, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)) :$
if $I_{\vec{v}} \supseteq I_{\vec{x}},\ K := e(\boldsymbol{c}_0, \boldsymbol{k}^*_0) \cdot \prod_{t \in I_{\vec{x}}} e(\boldsymbol{c}_t, \boldsymbol{k}^*_t),$ return $m' := c_T/K$,
else return $\perp$.

Correctness is shown in a similar manner to the Type 1 IPE scheme.

Theorem 2 *The proposed Type 2 IPE scheme is adaptively fully-attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

Theorem 2 is proven in a similar manner to Theorem 1.

5.3 Type 0 IPE Scheme

5.3.1 Construction Idea for Our Type 0 IPE Scheme

In Type 1 construction, 4-dimensional vector $(\mu_t(t,-1), \delta v_t, s_t)$ is encoded in key $\boldsymbol{k}^*_t$, and $(\sigma_t(1,t), \omega x_t,\ \widetilde{\omega})$ is encoded in ciphertext $\boldsymbol{c}_t$. Here, secret-sharing system, s_t for $t \in I_{\vec{v}}$, in $\boldsymbol{k}^*_t$ are used to assure one of the decryption conditions, $I_{\vec{v}} \subseteq I_{\vec{x}}$. In Type 0 scheme, to achieve its decryption condition $I_{\vec{v}} = I_{\vec{x}}$ for $\vec{v} := (v_1, \ldots, v_n), \vec{x} := (x_1, \ldots, x_{n'})$ i.e., that is equivalent to $n = n'$, we use the above mechanism also to ciphertext side. Then, in our Type 0 scheme, we encode 5-dimensional $(\mu_t(t,-1), \delta v_t, s_t, \widetilde{\delta})$ in the first part of $\boldsymbol{k}^*_t$, and $(\sigma_t(1,t), \omega x_t, \widetilde{\omega}, f_t)$ in the first part of $\boldsymbol{c}_t$ with random $\mu_t, \sigma_t, \omega, \widetilde{\omega}, \delta, \widetilde{\delta}, s_t, f_t \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

5.3.2 Construction and Security

Let $d := poly(\lambda)$, where $poly(\cdot)$ is an arbitrary polynomial.

```
$\mathsf{Setup}(1^\lambda):\quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 9, N := 21)),$
  $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,2}, \boldsymbol{b}_{0,5}, \boldsymbol{b}_{0,8}, \boldsymbol{b}_{0,9}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{19}, \ldots, \boldsymbol{b}_{21}),$
  $\widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,2}, \boldsymbol{b}^*_{0,5}, \ldots, \boldsymbol{b}^*_{0,7}),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, .., \boldsymbol{b}^*_4, \boldsymbol{b}^*_{16}, \ldots, \boldsymbol{b}^*_{18}),$
  return $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}),\ \mathsf{sk} := (\widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}^*).$
$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v} := (v_1, \ldots, v_n)$ such that $n \le d):$
  $s_t, \delta, \widetilde{\delta}, \eta_{0,1}, \eta_{0,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t = 1, \ldots, n,\ s_0 := \sum_{t=1}^{n} s_t,$
  $\boldsymbol{k}^*_0 := (\ -s_0,\ \widetilde{\delta},\ 0^2,\ 1,\ \eta_{0,1}, \eta_{0,2},\ 0^2\ )_{\mathbb{B}^*_0},$
  for $t = 1, \ldots, n,\quad \mu_t, \eta_{t,1}, .., \eta_{t,3} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$
  $\boldsymbol{k}^*_t := (\ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t,\ \widetilde{\delta},}^{5}\ \overbrace{0^{10},}^{10}\ \overbrace{\eta_{t,1}, .., \eta_{t,3},}^{3}\ \overbrace{0^3}^{3}\ )_{\mathbb{B}^*},$
  return $\mathsf{sk}_{\vec{v}} := \{\boldsymbol{k}^*_t\}_{t=0,\ldots,n}.$
$\mathsf{Enc}(\mathsf{pk},\ m,\ \vec{x} := (x_1, \ldots, x_{n'})$ such that $n' \le d):$
  $f_t, \omega, \widetilde{\omega}, \zeta, \varphi_{0,1}, \varphi_{0,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t = 1, \ldots, n,\ f_0 := \sum_{t=1}^{n'} f_t,$
  $\boldsymbol{c}_0 := (\ \widetilde{\omega},\ -f_0,\ 0^2,\ \zeta,\ 0^2,\ \vec{\varphi}_0\ )_{\mathbb{B}_0},\qquad c_T := g_T^{\zeta} m,$
  for $t = 1, \ldots, n',\quad \sigma_t, \varphi_{t,1}, .., \varphi_{t,3} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$
  $\boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega x_t,\ \widetilde{\omega},\ f_t,}^{5}\ \overbrace{0^{10},}^{10}\ \overbrace{0^3,}^{3}\ \overbrace{\varphi_{t,1}, .., \varphi_{t,3}}^{3}\ )_{\mathbb{B}},$
  return $\mathsf{ct}_{\vec{x}} := (\{\boldsymbol{c}_t\}_{t=0,\ldots,n'}, c_T).$
$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := \{\boldsymbol{k}^*_t\}_{t=0,\ldots,n},\ \mathsf{ct}_{\vec{x}} := (\{\boldsymbol{c}_t\}_{t=0,\ldots,n'}, c_T)):$
  if $n = n',\ K := \prod_{t=0}^{n} e(\boldsymbol{c}_t, \boldsymbol{k}^*_t),$ return $m' := c_T / K,$ else return $\perp.$
```

Correctness of the scheme can be shown in a similar manner to that of our Type 1 IPE.

Theorem 3 *The proposed Type 0 IPE scheme is adaptively fully-attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

Theorem 3 is proven in a similar manner to Theorem 1.

6 Proposed ABE Schemes

6.1 Basic KP-ABE Scheme

6.1.1 Construction

We define function $\widetilde{\rho} : \{1,..,\ell\} \to \{1,..,d\}$ by $\widetilde{\rho}(i) := t$ if $\rho(i) = (t,v)$ or $\rho(i) = \neg(t,v)$, where ρ is given in access structure $\mathbb{S} := (M,\rho)$. In the proposed scheme, we assume that $\widetilde{\rho}$ is injective for $\mathbb{S} := (M,\rho)$ in $\mathsf{sk}_{\mathbb{S}}$. For the modified scheme without such a restriction, see Section 6.2. Let $d := \mathit{poly}(\lambda)$, where $\mathit{poly}(\cdot)$ is an arbitrary polynomial.

```
$\mathsf{Setup}(1^\lambda)$ :   $(\mathsf{param}, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14))$,
  $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$,  $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14})$,
  $\widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4})$,  $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, .., \boldsymbol{b}^*_4, \boldsymbol{b}^*_{11}, \boldsymbol{b}^*_{12})$,
  return  $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$,  $\mathsf{sk} := (\widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}^*)$.
$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (M,\rho))$ :  $\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$,  $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$,  $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$,
  $\eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$,  $\boldsymbol{k}^*_0 := (-s_0,\ 0,\ 1,\ \eta_0,\ 0)_{\mathbb{B}^*_0}$,
  for $i = 1, \ldots, \ell$,   $\mu_i, \theta_i, \eta_{i,1}, \eta_{i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,
    if $\rho(i) = (t, v_i)$,
      $\boldsymbol{k}^*_i := (\ \overbrace{\mu_i(t,\ -1),\ s_i + \theta_i v_i,\ -\theta_i}^{4}\quad \overbrace{0^6,}^{6}\quad \overbrace{\eta_{i,1},\ \eta_{i,2},}^{2}\quad \overbrace{0^2}^{2}\ )_{\mathbb{B}^*}$,
    if $\rho(i) = \neg(t, v_i)$,
      $\boldsymbol{k}^*_i := (\ \overbrace{\mu_i(t,\ -1),\ s_i(v_i,\ -1),}^{4}\quad \overbrace{0^6,}^{6}\quad \overbrace{\eta_{i,1},\ \eta_{i,2},}^{2}\quad \overbrace{0^2}^{2}\ )_{\mathbb{B}^*}$,
  return  $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}^*_0, \boldsymbol{k}^*_1, \ldots, \boldsymbol{k}^*_\ell)$.
$\mathsf{Enc}(\mathsf{pk},\ m,\ \Gamma := \{(t, x_t) \mid 1 \le t \le d\})$ :  $\omega, \zeta, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$,
  $\boldsymbol{c}_0 := (\omega,\ 0,\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0}$,  $c_{d+1} := g_T^\zeta m$,
  for $(t, x_t) \in \Gamma$,  $\sigma_t, \varphi_{t,1}, \varphi_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,
    $\boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega(1,\ x_t),}^{4}\quad \overbrace{0^6,}^{6}\quad \overbrace{0^2,}^{2}\quad \overbrace{\varphi_{t,1},\ \varphi_{t,2}}^{2}\ )_{\mathbb{B}}$,
  return  $\mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}, c_{d+1})$.
$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}^*_1, \ldots, \boldsymbol{k}^*_\ell),\ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}, c_{d+1}))$ :
  If $\mathbb{S} := (M,\rho)$ accepts $\Gamma := \{(t, x_t)\}$, then compute $I$ and $\{\alpha_i\}_{i\in I}$ such that
    $\vec{1} = \sum_{i\in I} \alpha_i M_i$,  where $M_i$ is the $i$-th row of $M$, and
    $I \subseteq \{i \in \{1, \ldots, \ell\} \mid [\rho(i) = (t, v_i)\ \wedge\ (t, v_i) \in \Gamma]$
                    $\vee\ [\rho(i) = \neg(t, v_i)\ \wedge\ (t, x_t) \in \Gamma\ \wedge\ v_i \ne x_t]\,\}$,
    $K := e(\boldsymbol{c}_0, \boldsymbol{k}^*_0) \displaystyle\prod_{i\in I\ \wedge\ \rho(i)=(t,v_i)} e(\boldsymbol{c}_t, \boldsymbol{k}^*_i)^{\alpha_i} \prod_{i\in I\ \wedge\ \rho(i)=\neg(t,v_i)} e(\boldsymbol{c}_t, \boldsymbol{k}^*_i)^{\alpha_i/(v_i - x_t)}$,
    return  $m' := c_{d+1}/K$,  else return $\perp$.
```

[Correctness] If $\mathbb{S} := (M,\rho)$ accepts $\Gamma := \{(t, x_t)\}$,
$K = g_T^{-\omega s_0 + \zeta} \prod_{i\in I\ \wedge\ \rho(i)=(t,v_i)} g_T^{\omega\alpha_i s_i} \prod_{i\in I\ \wedge\ \rho(i)=\neg(t,v_i)} g_T^{\omega\alpha_i s_i(v_i - x_t)/(v_i - x_t)} = g_T^{\omega(-s_0 + \sum_{i\in I}\alpha_i s_i)+\zeta} = g_T^\zeta$.

6.1.2 Structural Comparison of our KP-ABE Scheme with the KP-ABE in [14]

We compare our *unbounded* KP-ABE with the existing *bounded* one [14].

Okamoto-Takashima [14] gave an adaptively secure KP-FE scheme on DPVS framework, and the specialized KP-ABE scheme, i.e., $n_t := 2$, is given in Appendix G.1 in the full version of the paper. Ciphertexts (CT) and secret-keys (SK) of the scheme have dimension $7 = 2 + 2 + 2 + 1$, where the first 2 dimension is the real-encoding part (real part, for short) for CT and SK vectors, the second is the hidden part for semi-functional CT and SK, the third is the SK randomness part, and the fourth is the CT randomness part. CT and SK of our KP-ABE have the same form, but dimension of each part is different, with 14 = 4+6+2+2 inner-structure. Particularly, 6 dimensional hidden part is crucial for our security proof of an elaborated Problem 2-ABE. For the outline of the proof, see Section 7.

$$\begin{array}{c} \text{CT \& SK in} \\ \text{[14] KP-ABE} \end{array} : \Big(\overbrace{\quad \text{real} \quad}^{2} \; \overbrace{\quad \text{hidden} \quad}^{2} \; \overbrace{\quad \text{SK ran.} \quad}^{2} \; \overbrace{\quad \text{CT ran.} \quad}^{1} \Big),$$

$$\begin{array}{c} \text{CT \& SK in} \\ \text{our KP-ABE} \end{array} : \Big(\overbrace{\qquad\quad \text{real} \qquad\quad}^{4} \; \overbrace{\qquad\qquad \text{hidden} \qquad\qquad}^{6} \; \overbrace{\quad \text{SK ran.} \quad}^{2} \; \overbrace{\quad \text{CT ran.} \quad}^{2} \Big).$$

6.1.3 Security

Theorem 4 *The proposed KP-ABE scheme is adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{F}_{1\text{-}1}, \mathcal{F}_{1\text{-}2}, \mathcal{F}_{2\text{-}1\text{-}0}, \ldots, \mathcal{F}_{2\text{-}1\text{-}5}, \mathcal{F}_{2\text{-}2\text{-}0}, \ldots, \mathcal{F}_{2\text{-}2\text{-}5}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\begin{aligned} &\mathsf{Adv}^{\text{KP-ABE}}_{\mathcal{A}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{1\text{-}1}}(\lambda) + \textstyle\sum_{p=1}^{d} \sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{1\text{-}2\text{-}p\text{-}j}}(\lambda) \\ &\quad \textstyle\sum_{h=1}^{\nu} \sum_{\iota=1}^{2} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}0}}(\lambda) + \sum_{p=1}^{d} \sum_{j=1}^{2} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}1\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}2\text{-}j}}(\lambda) + \\ &\qquad \textstyle\sum_{l=1,\ldots,d;\ l \ne p} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}3\text{-}j\text{-}l}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}4\text{-}j\text{-}l}}(\lambda) \Big) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}5\text{-}j}}(\lambda) \Big) \Big) + \epsilon, \end{aligned}$$

where $\mathcal{F}_{1\text{-}2\text{-}p\text{-}j}(\cdot) := \mathcal{F}_{1\text{-}2}(h, p, j, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}0}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}0}(h, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}1\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}1}(h, p, j, \cdot)$, $\mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}2\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}2}(h, p, j, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}3\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}3}(h, p, j, l, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}4\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}4}(h, p, j, l, \cdot), \mathcal{F}_{2\text{-}h\text{-}\iota\text{-}p\text{-}5\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}\iota\text{-}5}(h, p, j, \cdot)$ for $\iota = 1, 2$, ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (40d^2\nu + 20d\nu + 10\nu + 10d + 5)/q$.

As shown in Section 1.3, the central part of the proof of Theorem 4 is that of Lemma 24 (see Section 7 for the proof outline, and Appendix A.4 for the proof). The top level of the proof of this theorem (see Section 6.1.4) is similar to that in [14] using Lemmas 23 and 24.

Definition 18 (Problem 1-ABE) *Problem 1-ABE is to guess β, given $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,i}\}_{t=1,\ldots,d; i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\text{P1-ABE}}_{\beta}(1^\lambda, d)$, where*

$$\begin{aligned} &\mathcal{G}^{\text{P1-ABE}}_{\beta}(1^\lambda, d) : (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)), \\ &\quad \varphi_0, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \\ &\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14}), \\ &\quad \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, .., \boldsymbol{b}^*_4, \boldsymbol{b}^*_{11}, \boldsymbol{b}^*_{12}), \\ &\quad \boldsymbol{e}_{0,0} := (\omega, 0, 0, 0, \varphi_0)_{\mathbb{B}_0},\ \boldsymbol{e}_{1,0} := (\omega, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0},\ Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q) \ \text{ for } t = 1, \ldots, d, \end{aligned}$$

$$\text{for } t=1,\dots,d;\ i=1,2;\qquad \vec{e}_1 := (1,0),\ \vec{e}_2 := (0,1) \in \mathbb{F}_q^2,\ \ \sigma_{t,i},\varphi_{t,i,1},\varphi_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\begin{array}{rlccccl}
\boldsymbol{e}_{0,t,i} := & (& \overbrace{\sigma_{t,i}(1,\ t),\ \omega\vec{e}_i,}^{4} & \overbrace{0^6,}^{6} & \overbrace{0^2,}^{2} & \overbrace{\varphi_{t,i,1},\varphi_{t,i,2}}^{2} &)_{\mathbb{B}}, \\
\boldsymbol{e}_{1,t,i} := & (& \sigma_{t,i}(1,\ t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i\, Z_t, & 0^2, & \varphi_{t,i,1},\varphi_{t,i,2} &)_{\mathbb{B}},
\end{array}$$

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{B}$*, the advantage of* $\mathcal{B}$ *for Problem 1-ABE,* $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P1\text{-}ABE}}(\lambda)$*, is similarly defined as in Definition 13.*

Lemma 23 *Problem 1-ABE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$*, there exist probabilistic machines* $\mathcal{F}_1,\mathcal{F}_2$*, whose running times are essentially the same as that of* $\mathcal{B}$*, such that for any security parameter* λ*,* $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P1\text{-}ABE}}(\lambda) \le \mathsf{Adv}_{\mathcal{F}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{p=1}^{d}\sum_{j=1}^{2}\mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}j}}^{\mathsf{DLIN}}(\lambda)+\epsilon$*, where* $\mathcal{F}_{2\text{-}p\text{-}j}(\cdot) := \mathcal{F}_2(p,j,\cdot), \epsilon := (10d+5)/q$.

Lemma 23 is proven in Appendix A.4.3.

Definition 19 (Problem 2-ABE) *Problem 2-ABE is to guess* β*, given* $(\mathsf{param},\widehat{\mathbb{B}}_0,\widehat{\mathbb{B}}_0^*,\widehat{\mathbb{B}},\widehat{\mathbb{B}}^*,\boldsymbol{h}_{\beta,0}^*,\boldsymbol{e}_0,\{\boldsymbol{h}_{\beta,t,i}^*,\boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\beta}^{\mathsf{P2\text{-}ABE}}(1^\lambda,d)$*, where*

$$\mathcal{G}_{\beta}^{\mathsf{P2\text{-}ABE}}(1^\lambda,d):\ (\mathsf{param},(\mathbb{B}_0,\mathbb{B}_0^*),(\mathbb{B},\mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda,(N_0:=5,N:=14)),$$

$$\delta,\eta_0,\varphi_0,\omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \tau,\rho \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times},$$

$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1},\boldsymbol{b}_{0,3},\boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1,..,\boldsymbol{b}_4,\boldsymbol{b}_{13},\boldsymbol{b}_{14}),$$

$$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*,..,\boldsymbol{b}_{0,4}^*),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*,..,\boldsymbol{b}_4^*,\boldsymbol{b}_{11}^*,\boldsymbol{b}_{12}^*),$$

$$\boldsymbol{h}_{0,0}^* := (\delta,0,0,\eta_0,0)_{\mathbb{B}_0^*},\ \boldsymbol{h}_{1,0}^* := (\delta,\rho,0,\eta_0,0)_{\mathbb{B}_0^*},\ \boldsymbol{e}_0 := (\omega,\tau,0,0,\varphi_0)_{\mathbb{B}_0},$$

$$Z_t \xleftarrow{\mathsf{U}} GL(2,\mathbb{F}_q),\ U_t := (Z_t^{-1})^{\mathrm{T}},\ \text{for } t=1,..,d,$$

$$\text{for } t=1,\dots,d;\ i=1,2;$$

$$\vec{e}_1 := (1,0), \vec{e}_2 := (0,1) \in \mathbb{F}_q^2,\quad \mu_{t,i},\sigma_{t,i},\eta_{t,i,1},\eta_{t,i,2},\varphi_{t,i,1},\varphi_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\begin{array}{rlccccl}
\boldsymbol{h}_{0,t,i}^* := & (& \overbrace{\mu_{t,i}(t,\ -1),\ \delta\vec{e}_i,}^{4} & \overbrace{0^6,}^{6} & \overbrace{\eta_{t,i,1},\eta_{t,i,2}}^{2} & \overbrace{0^2}^{2} &)_{\mathbb{B}^*}, \\
\boldsymbol{h}_{1,t,i}^* := & (& \mu_{t,i}(t,\ -1),\ \delta\vec{e}_i, & 0^4,\quad \rho\vec{e}_i\, U_t, & \eta_{t,i,1},\eta_{t,i,2} & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{e}_{t,i} := & (& \sigma_{t,i}(1,\ t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i\, Z_t, & 0^2, & \varphi_{t,i,1},\varphi_{t,i,2} &)_{\mathbb{B}},
\end{array}$$

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{B}$*, the advantage of* $\mathcal{B}$ *for Problem 2-ABE,* $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2\text{-}ABE}}(\lambda)$*, is similarly defined as in Definition 13.*

Lemma 24 *Problem 2-ABE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$*, there exist probabilistic machines* $\mathcal{F}_1,\mathcal{F}_{2\text{-}1},\dots,\mathcal{F}_{2\text{-}5}$*, whose running times are essentially the same as that of* $\mathcal{B}$*, such that for any security parameter* λ*,* $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2\text{-}ABE}}(\lambda) \le \mathsf{Adv}_{\mathcal{F}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{p=1}^{d}\sum_{j=1}^{2}\Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}2\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \sum_{l=1,...,d;\ l\neq p}\Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}}^{\mathsf{DLIN}}(\lambda)\Big) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}5\text{-}j}}^{\mathsf{DLIN}}(\lambda)\Big) + \epsilon$*, where* $\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}1}(p,j,\cdot), \mathcal{F}_{2\text{-}p\text{-}2\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}2}(p,j,\cdot)$*,* $\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}3}(p,j,l,\cdot), \mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}4}(p,j,l,\cdot), \mathcal{F}_{2\text{-}p\text{-}5\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}5}(p,j,\cdot)$ *and* $\epsilon := (20d^2+10d+5)/q$.

Lemma 24 is proven in Appendix A.4.4.

6.1.4 Proof of Theorem 4

Proof Outline of Theorem 4: At the top level of strategy of the security proof, we follow the dual system encryption methodology over dual pairing vector space (DPVS) described in [14]. To prove the security of KP-ABE, we use Problems 1-ABE and 2-ABE, instead of Problems 1 and 2 in [14]. The rest of the proof is similar to that in [14].

Proof of Theorem 4: To prove Theorem 4, we consider the following 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 an experiment from the previous game. Games proceed as follows (see Figure 2 in Appendix A.4):

Game 0 $\Rightarrow$ Game 1 $\Rightarrow$ (for $h = 1, .., \nu$; Game 2-h-1 $\Rightarrow$ Game 2-h-2 $\Rightarrow$ Game 2-h-3) $\Rightarrow$ Game 3

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

$$\left.\begin{array}{l}
\boldsymbol{k}_0^* := (-s_0,\ \boxed{0},\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}, \\
\text{for } i = 1, \ldots, \ell, \\
\text{ if } \rho(i) = (t, v_i), \\
\quad \boldsymbol{k}_i^* := (\ \overbrace{\mu_i(t,\ -1),\ s_i + \theta_i v_i,\ -\theta_i,}^{4}\ \ \overbrace{0^4,\ \boxed{0^2},}^{6}\ \ \overbrace{\eta_{i,1},\ \eta_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*}, \\
\text{ if } \rho(i) = \neg(t, v_i), \\
\quad \boldsymbol{k}_i^* := (\ \overbrace{\mu_i(t,\ -1),\ s_i(v_i,\ -1),}^{4}\ \ \overbrace{0^4,\ \boxed{0^2},}^{6}\ \ \overbrace{\eta_{i,1},\ \eta_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},
\end{array}\right\} \tag{18}$$

where $\mu_i, \theta_i, \eta_0, \eta_{i,1}, \eta_{i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r,\ s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},\ \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$. The challenge ciphertext for challenge plaintext $(m^{(0)}, m^{(1)})$ and attributes $\Gamma := \{(t, x_t) | 1 \le t \le d\}$ is:

$$\begin{array}{l}
\boldsymbol{c}_0 := (\omega,\ \boxed{0},\ \boxed{\zeta},\ 0,\ \varphi_0)_{\mathbb{B}_0^*}, \\
\text{for } (t, x_t) \in \Gamma,\ \boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega(1,\ x_t),}^{4}\ \ \overbrace{\boxed{0^2},\ 0^2,\ \boxed{0^2},}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\varphi_{t,1},\ \varphi_{t,2}}^{2}\ \ )_{\mathbb{B}}, \\
c_{d+1} := g_T^{\zeta} m^{(b)},
\end{array}$$

where $b \xleftarrow{\mathsf{U}} \{0, 1\},\ \omega, \zeta, \sigma_t, \varphi_0, \varphi_{t,1}, \varphi_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

Game 1: Same as Game 0 except that the challenge ciphertext is:

$$\left.\begin{array}{l}
\boldsymbol{c}_0 := (\omega,\ \boxed{\tau},\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0}, \\
\text{for } (t, x_t) \in \Gamma, \\
\quad \boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega(1,\ x_t),}^{4}\ \ \overbrace{\boxed{\tau(1,\ x_t)},\ 0^2,\ \boxed{\tau(1,\ x_t) \cdot Z_t},}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\varphi_{t,1}, \varphi_{t,2}}^{2}\ \ )_{\mathbb{B}},
\end{array}\right\} \tag{19}$$

where $\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times},\ Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$, and all the other variables are generated as in Game 0.

Game 2-h-1 $(h = 1, \ldots, \nu)$**:** Game 2-0-3 is Game 1. Game 2-h-1 is the same as Game 2-$(h-1)$-3 except the reply, $(\boldsymbol{k}_i^*)_{i=0,\ldots,\ell}$, for the h-th key query for $\mathbb{S} := (M, \rho)$ are:

$$\boldsymbol{k}_0^* := (-s_0,\ \boxed{-a_0},\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}, \tag{20}$$

$$\left.\begin{array}{l}
\text{for } i = 1, \ldots, \ell, \\
\ \text{if } \rho(i) = (t, \vec{v}_i), \\
\quad \boldsymbol{k}_i^* := (\ \overbrace{\mu_i(t,\ -1),\ s_i + \theta_i v_i,\ -\theta_i,}^{4} \\
\qquad\qquad \overbrace{0^4,\ \boxed{(a_i + \pi_i v_i,\ -\pi_i) \cdot U_t}}^{6},\ \ \overbrace{\eta_{i,1}, \eta_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*}, \\
\ \text{if } \rho(i) = \neg(t, v_i), \\
\quad \boldsymbol{k}_i^* := (\ \overbrace{\mu_i(t,\ -1),\ s_i(v_i,\ -1),}^{4} \\
\qquad\qquad \overbrace{0^4,\ \boxed{a_i(v_i,\ -1) \cdot U_t}}^{6},\ \ \overbrace{\eta_{i,1}, \eta_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},
\end{array}\right\} \tag{21}$$

where $\vec{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $a_0 := \vec{1} \cdot \vec{g}^{\mathrm{T}}$, $\vec{a}^{\mathrm{T}} := (a_1, \ldots, a_\ell)^{\mathrm{T}} := M \cdot \vec{g}^{\mathrm{T}}$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$ used in Eq. (19) and $t = 1, \ldots, d$, and $\pi_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, \ell$. All the other variables are generated as in Game 2-$(h-1)$-3.

Game 2-h-2 $(h = 1, \ldots, \nu)$**:** Same as Game 2-h-1 except that $\boldsymbol{k}_0^*$ of the reply for the h-th key query is:

$$\boldsymbol{k}_0^* := (-s_0,\ \boxed{r_0},\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}, \tag{22}$$

$r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and all the other variables are generated as in Game 2-h-1.

Game 2-h-3 $(h = 1, \ldots, \nu)$**:** Game 2-h-3 is the same as Game 2-h-2 except $(\boldsymbol{k}_i^*)_{i=1,\ldots,\ell}$ of the reply for the h-th key query are:

$$\left.\begin{array}{l}
\boldsymbol{k}_0^* := (-s_0,\ r_0,\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}, \\
\text{for } i = 1, \ldots, \ell, \\
\ \text{if } \rho(i) = (t, v_i), \\
\quad \boldsymbol{k}_i^* := (\ \overbrace{\mu_i(t,\ -1),\ s_i + \theta_i v_i,\ -\theta_i,}^{4}\ \ \overbrace{0^4,\ \boxed{0^2},}^{6}\ \ \overbrace{\eta_{i,1}, \eta_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*}, \\
\ \text{if } \rho(i) = \neg(t, v_i), \\
\quad \boldsymbol{k}_i^* := (\ \overbrace{\mu_i(t,\ -1),\ s_i(v_i,\ -1),}^{4}\ \ \overbrace{0^4,\ \boxed{0^2},}^{6}\ \ \overbrace{\eta_{i,1}, \eta_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},
\end{array}\right\} \tag{23}$$

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

Game 3: Game 3 is the same as Game 2-ν-3 except that $\boldsymbol{c}_0$ of the challenge ciphertext is:

$$\boldsymbol{c}_0 := (\omega,\ \tau,\ \boxed{\zeta'},\ 0,\ \varphi_0)_{\mathbb{B}_0},\quad c_{d+1} := g_T^{\zeta} m^{(b)},$$

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-3.

Let $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(2\text{-}h\text{-}j)}_{\mathcal{A}}(\lambda)$ $(h = 1, \ldots, \nu; j = 1, 2, 3)$ and $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0, 1, 2\text{-}h\text{-}j$ and 3, respectively. $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$ is equivalent to $\mathsf{Adv}^{\mathsf{KP\text{-}ABE,PH}}_{\mathcal{A}}(\lambda)$ and it is obtained that $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = 0$ by Lemma 30.

We will show five lemmas (Lemmas 25-29) that evaluate the gaps between pairs of $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda), \ldots, \mathsf{Adv}^{(2\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda)$, for $h = 1, \ldots, \nu$ and $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$. From these lemmas, we obtain $\mathsf{Adv}^{\mathsf{KP\text{-}ABE,PH}}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) \leq \left|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)\right| + \sum_{h=1}^{\nu} \Big(\Big|\mathsf{Adv}^{(2\text{-}(h-1)\text{-}3)}_{\mathcal{A}}(\lambda) -$ $\mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)\Big| + \sum_{j=1}^{2} \left|\mathsf{Adv}^{(2\text{-}h\text{-}j)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}(j+1))}_{\mathcal{A}}(\lambda)\right|\Big) + \left|\mathsf{Adv}^{(2\text{-}\nu\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)\right| +$ $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{P1\text{-}ABE}}_{\mathcal{B}_1}(\lambda) + \sum_{h=1}^{\nu} \left(\mathsf{Adv}^{\mathsf{P2\text{-}ABE}}_{\mathcal{B}_{2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P2\text{-}ABE}}_{\mathcal{B}_{2\text{-}h\text{-}2}}(\lambda)\right) + (4\nu + 1)/q$. Therefore, from Lemmas 23 and 24, we obtain the upperbound of $\mathsf{Adv}^{\mathsf{KP\text{-}ABE,PH}}_{\mathcal{A}}(\lambda)$ in Theorem 4. This completes the proof of Theorem 4. □

Lemma 25 *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, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1\text{-}ABE}}_{\mathcal{B}_1}(\lambda)$.*

Lemma 26 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}(h-1)\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2\text{-}ABE}}_{\mathcal{B}_{2\text{-}h\text{-}1}}(\lambda) + 2/q$, where $\mathcal{B}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{2\text{-}1}(h, \cdot)$.*

Lemma 27 *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda)$.*

Lemma 28 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2\text{-}ABE}}_{\mathcal{B}_{2\text{-}h\text{-}2}}(\lambda) + 2/q$, where $\mathcal{B}_{2\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{2\text{-}2}(h, \cdot)$.*

Lemma 29 *For any adversary $\mathcal{A}$, $|\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}\nu\text{-}3)}_{\mathcal{A}}(\lambda)| \leq 1/q$.*

Lemma 30 *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = 0$.*

Proof. The value of b is independent from the adversary's view in Game 3. Hence, $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = 0$. □

6.2 Modified KP-ABE Scheme with Arbitrary Degree

6.2.1 Construction

Let function $\widetilde{\rho} : \{1, \ldots, \ell\} \to \{1, \ldots, d\}$ be $\widetilde{\rho}(i) := t$ if $\rho(i) = (t, v)$ or $\rho(i) = \neg(t, v)$, where ρ is given in access structure $\mathbb{S} := (M, \rho)$. Let k_t be the number of elements of preimage set $\widetilde{\rho}^{-1}(t)$, i.e., $k_t := \#\widetilde{\rho}^{-1}(t)$, and the k_t elements of $\widetilde{\rho}^{-1}(t)$ are expressed by $\{i_1, \ldots, i_{k_t} \mid 1 \leq i_1 \leq i_2 \leq \cdots \leq i_{k_t} \leq \ell\}$ in the ascending order. Degree k of access structure (M, ρ) is defined by $\max_{1 \leq t \leq d}(k_t)$. For $t = 1, \ldots, d$ and $i_j \in \widetilde{\rho}^{-1}(t)$ $(j = 1, \ldots, k_t)$, we define $\hat{\rho} : \{1, \ldots, \ell\} \to \mathbb{F}_q$ by $\hat{\rho}(i_j) := [\![t, j]\!]$, where $[\![t, j]\!] := t \cdot 2^{\lfloor |q|/2 \rfloor} + j \in \mathbb{F}_q$ with $t, j = O(\lambda^c)$ for a constant c and $|q| = \Theta(\lambda)$.

In the proposed scheme shown in Section 6.1, we assume that $\widetilde{\rho}$ is injective (or degree k is 1) for $\mathbb{S} := (M, \rho)$ with decryption key $\mathsf{sk}_{\mathbb{S}}$. Using a simple encoding technique given in [8] with some modification to our situation, we can easily construct a fully secure unbounded KP-ABE scheme where $\widetilde{\rho}$ is not necessarily injective, or arbitrary (unbounded) degree k is available.

Suppose that the maximum degree k_{max} is given to users, i.e., the degree k of any access policy with decryption key $\mathsf{sk}_{\mathbb{S}}$ is at most k_{max}. With this condition, in the modified scheme, an extended index $\hat{t} := [\![t, j]\!] = \hat{\rho}(i)$ for $i \in \{1, \dots, \ell\}$ is employed for decryption key in place of $t = \widetilde{\rho}(i)$ with the original proposed scheme where $1 \le j \le k_t \le k_{\mathsf{max}}$ for each t. Note that map $\hat{\rho}$ is always injective, even when $\widetilde{\rho}$ is not injective. The size of the secret key of the modified scheme is the same as that of the original scheme. A ciphertext for attribute set Γ consists of components for $(t, x_t) \in \Gamma$ in the original scheme, while a ciphertext for attribute set Γ consists of components for $([\![t, j]\!], x_t) \in \hat{\Gamma}$ in the modified scheme, where $\hat{\Gamma} := \{([\![t, j]\!], x_t) \mid (t, x_t) \in \Gamma,\ j = 1, \dots, k_{\mathsf{max}}\}$. Therefore, the ciphertext size of the modified scheme is k_{max} times greater than that of the original scheme, and a user who makes a ciphertext should know the value of k_{max}.

Let $d := poly(\lambda)$, where $poly(\cdot)$ is an arbitrary polynomial. Random dual basis generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_t)_{t=0,1})$ is defined at the end of Section 2. We refer to Section 1.4 for notations on DPVS.

```
$\mathsf{Setup}(1^\lambda):\quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)),$
  $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14}),$
  $\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, .., \boldsymbol{b}_4^*, \boldsymbol{b}_{11}^*, \boldsymbol{b}_{12}^*),$
  return  $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}),\ \mathsf{sk} := (\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*).$
$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (M, \rho)):\ \vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r,\ s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},\ \vec{s}^{\mathrm{T}} := (s_1, \dots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}},$
  $\eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\quad \boldsymbol{k}_0^* := (-s_0,\ 0,\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*},$
  for $i = 1, \dots, \ell,\quad \mu_i, \theta_i, \eta_{i,1}, \eta_{i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$
    if $\rho(i) = (t, v_i),\quad \hat{t} := [\![t, j]\!] := \hat{\rho}(i),$
      $\boldsymbol{k}_i^* := (\ \overbrace{\mu_i(\hat{t},\ -1),\ s_i + \theta_i v_i,\ -\theta_i}^{4}\ \ \overbrace{0^6,}^{6}\ \ \overbrace{\eta_{i,1},\ \eta_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},$
    if $\rho(i) = \neg(t, v_i),\quad \hat{t} := [\![t, j]\!] := \hat{\rho}(i),$
      $\boldsymbol{k}_i^* := (\ \overbrace{\mu_i(\hat{t},\ -1),\ s_i(v_i,\ -1),}^{4}\ \ \overbrace{0^6,}^{6}\ \ \overbrace{\eta_{i,1},\ \eta_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}^*},$
  return  $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \dots, \boldsymbol{k}_\ell^*).$
$\mathsf{Enc}(\mathsf{pk},\ m,\ \Gamma := \{(t, x_t) \mid 1 \le t \le d\}):\ \hat{\Gamma} := \{([\![t, j]\!], x_t)\ \mid\ (t, x_t) \in \Gamma,\ j = 1, \dots, k_{\mathsf{max}}\},$
  $\omega, \zeta, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\quad \boldsymbol{c}_0 := (\omega,\ 0,\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0},\quad c_{d+1} := g_T^\zeta m,$
  for $([\![t, j]\!], x_t) \in \hat{\Gamma};\quad \hat{t} := [\![t, j]\!],\quad \sigma_{\hat{t}}, \varphi_{\hat{t},1}, \varphi_{\hat{t},2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$
      $\boldsymbol{c}_{\hat{t}} := (\ \overbrace{\sigma_{\hat{t}}(1,\ \hat{t}\ ),\ \omega(1,\ x_t),}^{4}\ \ \overbrace{0^6,}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\varphi_{\hat{t},1},\ \varphi_{\hat{t},2}}^{2}\ \ )_{\mathbb{B}},$
  return  $\mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_{\hat{t}}\}_{(\hat{t}, x_t) \in \hat{\Gamma}}, c_{d+1}).$
$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_1^*, \dots, \boldsymbol{k}_\ell^*),\ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_{\hat{t}}\}_{(\hat{t}, x_t) \in \hat{\Gamma}}, c_{d+1})):$
  If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(\hat{t}, x_{\hat{t}})\}$, then compute $I$ and $\{\alpha_i\}_{i \in I}$ such that
    $\vec{1} = \sum_{i \in I} \alpha_i M_i,$ where $M_i$ is the $i$-th row of $M,$ and
    $I \subseteq \{i \in \{1, \dots, \ell\} \mid [\rho(i) = (t, v_i)\ \wedge\ (\hat{\rho}(i), v_i) \in \hat{\Gamma}]$
                      $\vee\, [\rho(i) = \neg(t, v_i)\ \wedge\ (\hat{\rho}(i), x_t) \in \hat{\Gamma}\ \wedge\ v_i \neq x_t]\,\},$
```

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i \in I \,\wedge\, \rho(i)=(t,v_i)} e(\boldsymbol{c}_{\hat{\rho}(i)}, \boldsymbol{k}_i^*)^{\alpha_i} \prod_{i \in I \,\wedge\, \rho(i)=\neg(t,v_i)} e(\boldsymbol{c}_{\hat{\rho}(i)}, \boldsymbol{k}_i^*)^{\alpha_i/(v_i-x_t)},$$

$$\text{return} \;\; m' := c_{d+1}/K.$$

[Correctness] If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(\hat{t}, x_{\hat{t}})\}$, $e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i \in I \,\wedge\, \rho(i)=(t,v_i)} e(\boldsymbol{c}_{\hat{\rho}(i)}, \boldsymbol{k}_i^*)^{\alpha_i} \prod_{i \in I \,\wedge\, \rho(i)=\neg(t,v_i)} e(\boldsymbol{c}_{\hat{\rho}(i)}, \boldsymbol{k}_i^*)^{\alpha_i/(v_i-x_t)} =$ $g_T^{-\omega s_0+\zeta} \prod_{i \in I \,\wedge\, \rho(i)=(t,v_i)} g_T^{\omega\alpha_i s_i} \prod_{i \in I \,\wedge\, \rho(i)=\neg(t,v_i)} g_T^{\omega\alpha_i s_i (v_i-x_t)/(v_i-x_t)} = g_T^{\omega(-s_0+\sum_{i\in I}\alpha_i s_i)+\zeta} = g_T^{\zeta}$.

6.2.2 Security

Theorem 5 *The modified KP-ABE scheme with arbitrary degree is adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

t (resp. $\widetilde{\rho}$) in Theorem 4 is replaced by $\hat{t}$ (resp. $\hat{\rho}$) in Theorem 5. Since $\hat{\rho}$ is injective in the modified KP-ABE scheme, Theorem 5 is reduced from Theorem 4.

6.3 Basic CP-ABE Scheme

6.3.1 Construction

We define function $\widetilde{\rho} : \{1, \ldots, \ell\} \to \{1, \ldots, d\}$ by $\widetilde{\rho}(i) := t$ if $\rho(i) = (t, v)$ or $\rho(i) = \neg(t, v)$, where ρ is given in access structure $\mathbb{S} := (M, \rho)$. In the proposed scheme, we assume that $\widetilde{\rho}$ is injective for $\mathbb{S} := (M, \rho)$ with ciphertexts $\mathsf{ct}_{\mathbb{S}}$. To remove this restriction, we can apply the technique in Section 6.2 to the basic CP-ABE scheme.

Let $d := poly(\lambda)$, where $poly(\cdot)$ is an arbitrary polynomial. Random dual basis generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_t)_{t=0,1})$ is defined at the end of Section 2. We refer to Section 1.4 for notations on DPVS.

$$\mathsf{Setup}(1^\lambda): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)),$$

$$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}), \quad \widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14}),$$

$$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_4^*, \boldsymbol{b}_{11}^*, \boldsymbol{b}_{12}^*),$$

$$\text{return} \;\; \mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}), \;\; \mathsf{sk} := (\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*),$$

$$\mathsf{KeyGen}(\mathsf{pk}, \; \mathsf{sk}, \; \Gamma := \{(t, x_t) \mid 1 \le t \le d\}): \quad \omega, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\boldsymbol{k}_0^* := (\omega, \; 0, \; 1, \; \varphi_0, \; 0)_{\mathbb{B}_0^*},$$

$$\text{for } (t, x_t) \in \Gamma, \quad \sigma_t, \varphi_{t,1}, \varphi_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\boldsymbol{k}_t^* := (\; \overbrace{\sigma_t(1, \; t), \; \omega(1, \; x_t),}^{4} \quad \overbrace{0^6,}^{6} \quad \overbrace{\varphi_{t,1}, \; \varphi_{t,2},}^{2} \quad \overbrace{0^2}^{2} \;)_{\mathbb{B}^*}$$

$$\text{return} \;\; \mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,x_t)\in\Gamma}).$$

$$\mathsf{Enc}(\mathsf{pk}, \; m, \; \mathbb{S} := (M, \rho)):$$

$$\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, \;\; s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, \;\; \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \;\; \zeta, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\boldsymbol{c}_0 := (-s_0, \; 0, \; \zeta, \; 0, \; \eta_0)_{\mathbb{B}_0}, \qquad c_{d+1} := g_T^{\zeta} m,$$

$$\text{for } i = 1, \ldots, \ell,$$

$$\text{if } \rho(i) = (t, v_i), \quad \mu_i, \theta_i, \eta_{i,1}, \eta_{i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\boldsymbol{c}_i := (\; \overbrace{\mu_i(t, \; -1), \; s_i + \theta_i v_i, \; -\theta_i}^{4} \quad \overbrace{0^6,}^{6} \quad \overbrace{0^2,}^{2} \quad \overbrace{\eta_{i,1}, \; \eta_{i,2}}^{2} \;)_{\mathbb{B}},$$

```
    if $\rho(i) = \neg(t, v_i)$,   $\mu_i, \eta_{i,1}, \eta_{i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,
      $\boldsymbol{c}_i := ( \overbrace{\mu_i(t,\ -1),\ s_i(v_i,\ -1),}^{4} \overbrace{0^6,}^{6} \overbrace{0^2,}^{2} \overbrace{\eta_{i,1},\ \eta_{i,2}}^{2} )_{\mathbb{B}}$,
    return  $\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$.
  $\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,x_t)\in\Gamma}),\ \mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1}))$ :
    If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, x_t)\}$, then compute $I$ and $\{\alpha_i\}_{i\in I}$ such that
      $\vec{1} = \sum_{i\in I} \alpha_i M_i$, where $M_i$ is the $i$-th row of $M$, and
      $I \subseteq \{i \in \{1, \ldots, \ell\}\ \mid\ [\rho(i) = (t, v_i)\ \wedge\ (t, x_t) \in \Gamma\ \wedge\ v_i = x_t]$
                $\vee\ [\rho(i) = \neg(t, v_i)\ \wedge\ (t, x_t) \in \Gamma\ \wedge\ v_i \neq x_t]\ \}$.
    $K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i\in I\ \wedge\ \rho(i)=(t,v_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i} \prod_{i\in I\ \wedge\ \rho(i)=\neg(t,v_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i/(v_i - x_t)}$
    return  $m' := c_{d+1}/K$.
```

[Correctness] If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, x_t)\}$,
$e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i\in I\ \wedge\ \rho(i)=(t,v_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i} \cdot \prod_{i\in I\ \wedge\ \rho(i)=\neg(t,v_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i/(v_i-x_t)} =$
$g_T^{-\omega s_0+\zeta} \prod_{i\in I\ \wedge\ \rho(i)=(t,v_i)} g_T^{\omega\alpha_i s_i} \prod_{i\in I\ \wedge\ \rho(i)=\neg(t,v_i)} g_T^{\omega\alpha_i s_i(v_i-x_t)/(v_i-x_t)} = g_T^{\omega(-s_0+\sum_{i\in I}\alpha_i s_i)+\zeta} = g_T^{\zeta}$.

6.3.2 Security

Theorem 6 *The proposed CP-ABE scheme is adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

The proof of Theorem 6 is similarly given to that of Theorem 4.

7 Consistent Randomness Amplification (Proof Outline of Lemma 24)

Lemma 24 is proven by the hybrid argument through $8d + 2$ experiments (Appendix A.4.4). To clarify the idea, we only consider several highlighted experiments. The highlighted game transformation with the same experiment numbers as in Appendix A.4.4 consists of $5d + 2$ experiments:

Experiment 0 ⇒ Experiment 1 ⇒

for $p = 1, \ldots, d$;   Experiment 2-p-1 ⇒ Experiment 2-p-4 ⇒ Experiment 2-p-5 ⇒
Experiment 2-p-6 ⇒ Experiment 2-p-8

Section 7.1 gives basic building blocks for the transformation. Section 7.2 describes some useful combinations of the basic changes. Section 7.3 explain the transformations through the highlighted experiments, and how randomness are amplified consistently (with the key condition).

7.1 Basic Changes

7.1.1 Basic Computational Changes

In the game description, we employ two types of elementary computational changes. Using a (toy) example in 2-dimensional 3 blocks, i.e., total is 6-dimension, we illustrate them. The first block is included in the real-encoding part, the second one is in the hidden part, and the third one is included in the ciphertext randomness part (resp. secret-key randomness part) for the first type change (resp. second type change). (For the terminology, see Section 6.1.2.) We remark that neither the first nor third part is described in the highlighted transformation in Section 7.3, where coefficients only in the hidden part are described.

Type I: The first type change transforms a ciphertext element $\boldsymbol{e} := (\omega\vec{\psi}, 0^2, \vec{\varphi})_{\mathbb{B}}$ to $\widetilde{\boldsymbol{e}} := (\omega\vec{\psi}, \tau\vec{\psi}, \vec{\varphi})_{\mathbb{B}}$ where a secret-key element $\boldsymbol{h}^*$ has a form, $(\delta\vec{\xi}, 0^2, 0^2)_{\mathbb{B}^*}$, with $\omega, \tau, \delta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\varphi} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ (and with any $\vec{\psi}, \vec{\xi} \in \mathbb{F}_q^2$, not necessarily uniform ones). The transformation is given by a special form of Problem 1 in [14], and the security is proven from the DLIN assumption. Change of coefficients in the 6-dimensional space are given as: (Hereafter, a blank indicates zero coefficients)

$$\boldsymbol{e} = \begin{array}{|c|c|c|}\hline \omega\vec{\psi} & \quad\quad & \vec{\varphi} \\ \hline\end{array}$$

$$\xrightarrow{\text{Type I}} \widetilde{\boldsymbol{e}} = \begin{array}{|c|c|c|}\hline \omega\vec{\psi} & \tau\vec{\psi} & \vec{\varphi} \\ \hline\end{array} \quad \text{where } \boldsymbol{h}^* = \begin{array}{|c|c|c|}\hline \delta\vec{\xi} & \quad\quad & \quad\quad \\ \hline\end{array}$$

Type II: The second type change transforms a key element $\boldsymbol{h}^* := (\delta\vec{\xi}, 0^2, \vec{\eta})_{\mathbb{B}^*}$ to $\widetilde{\boldsymbol{h}}^* := (\delta\vec{\xi}, \rho\vec{\xi}, \vec{\eta})_{\mathbb{B}^*}$ where a ciphertext element $\boldsymbol{e}$ has a form, $\boldsymbol{e} := (\omega\vec{\psi}, \tau\vec{\psi}, 0^2)_{\mathbb{B}}$, with $\omega, \tau, \delta, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ (and with any $\vec{\psi}, \vec{\xi} \in \mathbb{F}_q^2$, not necessarily uniform). The transformation is given by a special form of Problem 2 in [14], and the security is proven from the DLIN assumption. Change of coefficients in the 6-dimensional space are given as:

$$\boldsymbol{h}^* = \begin{array}{|c|c|c|}\hline \delta\vec{\xi} & \quad\quad & \vec{\eta} \\ \hline\end{array}$$

$$\xrightarrow{\text{Type II}} \widetilde{\boldsymbol{h}}^* = \begin{array}{|c|c|c|}\hline \delta\vec{\xi} & \rho\vec{\xi} & \vec{\eta} \\ \hline\end{array} \quad \text{where } \boldsymbol{e} = \begin{array}{|c|c|c|}\hline \omega\vec{\psi} & \tau\vec{\psi} & \quad\quad \\ \hline\end{array}$$

7.1.2 Basic Information-Theoretical Changes

In the game description, we employ two types of elementary conceptual changes. Using a (toy) example in 2-dimensional 2 blocks (resp. 1 block), i.e., total is 4-dimension (resp. 2-dimension), with $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_4^*)$ (resp. $\mathbb{B} := (\boldsymbol{b}_1, \boldsymbol{b}_2)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*)$), we illustrate them. All the blocks are included in the hidden part. Hence, they are described in the highlighted transformation in Section 7.3, where coefficients only in the hidden part are described.

Inter-subspace Type: We set new dual orthonormal bases $\mathbb{D} := (\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{d}_3 := \boldsymbol{b}_3 + \chi\boldsymbol{b}_1, \boldsymbol{d}_4 := \boldsymbol{b}_4 + \chi\boldsymbol{b}_2)$ and $\mathbb{D}^* := (\boldsymbol{d}_1^* := \boldsymbol{b}_1^* - \chi\boldsymbol{b}_3^*, \boldsymbol{d}_2^* := \boldsymbol{b}_2^* - \chi\boldsymbol{b}_4^*, \boldsymbol{b}_3^*, \boldsymbol{b}_4^*)$ with $\chi \in \mathbb{F}_q$. Then, ciphertext element $\boldsymbol{e} := (\vec{\psi}_1, \vec{\psi}_2)_{\mathbb{B}}$ with $\vec{\psi}_1, \vec{\psi}_2 \in \mathbb{F}_q^2$ is equal to $(\vec{\psi}_1 - \chi\vec{\psi}_2, \vec{\psi}_2)_{\mathbb{D}}$, and secret-key elements $\boldsymbol{h}^* := (\vec{\xi}_1, \vec{\xi}_2)_{\mathbb{B}^*}$ with $\vec{\xi}_1, \vec{\xi}_2 \in \mathbb{F}_q^2$ is equal to $(\vec{\xi}_1, \vec{\xi}_2 + \chi\vec{\xi}_1)_{\mathbb{D}^*}$. We remark that this change affects all elements represented with $\mathbb{B}$ and $\mathbb{B}^*$. This change is represented by bases transform matrix as $\mathsf{Inter}\begin{pmatrix} I & 0 \\ \chi I & I \end{pmatrix}$, where $I := I_2$ and $0 := 0_2$. Change of coefficients of $\boldsymbol{e}$ and $\boldsymbol{h}^*$ in the 4-dimensional space are given as:

$$\boldsymbol{e} = \begin{array}{|c|c|}\hline \vec{\psi}_1 & \vec{\psi}_2 \\ \hline\end{array} \quad \boldsymbol{h}^* = \begin{array}{|c|c|}\hline \vec{\xi}_1 & \vec{\xi}_2 \\ \hline\end{array}$$

$$\xrightarrow{\mathsf{Inter}\begin{pmatrix} I & 0 \\ \chi I & I \end{pmatrix}} \begin{array}{|c|c|}\hline \vec{\psi}_1 - \chi\vec{\psi}_2 & \vec{\psi}_2 \\ \hline\end{array} \quad \begin{array}{|c|c|}\hline \vec{\xi}_1 & \vec{\xi}_2 + \chi\vec{\xi}_1 \\ \hline\end{array}$$

Intra-subspace Type: We set new dual orthonormal bases $\mathbb{D} := (\boldsymbol{d}_1, \boldsymbol{d}_2)$ and $\mathbb{D}^* := (\boldsymbol{d}_1^*, \boldsymbol{d}_2^*)$ where $U \in GL(2, \mathbb{F}_q), Z := (U^{-1})^{\mathrm{T}}$, $(\boldsymbol{d}_1, \boldsymbol{d}_2)^{\mathrm{T}} := Z^{-1} \cdot (\boldsymbol{b}_1, \boldsymbol{b}_2)^{\mathrm{T}}$ and $(\boldsymbol{d}_1^*, \boldsymbol{d}_2^*)^{\mathrm{T}} := U^{-1} \cdot (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*)^{\mathrm{T}}$. Then, ciphertext element $\boldsymbol{e} := (\vec{\psi})_{\mathbb{B}}$ with $\vec{\psi} \in \mathbb{F}_q^2$ is equal to $(\vec{\psi}Z)_{\mathbb{D}}$, and secret-key elements

$\boldsymbol{h}^* := (\vec{\xi})_{\mathbb{B}^*}$ with $\vec{\xi} \in \mathbb{F}_q^2$ is equal to $(\vec{\xi}U)_{\mathbb{D}^*}$. We remark that this change affects all elements represented with $\mathbb{B}$ and $\mathbb{B}^*$. This change is represented by bases transform matrix as $\mathsf{Intra}(\ Z^{-1}\ )$. Change of coefficients of $\boldsymbol{e}$ and $\boldsymbol{h}^*$ in the 2-dimensional space are given as:

$$\boldsymbol{e} = \boxed{\ \vec{\psi}\ } \quad \boldsymbol{h}^* = \boxed{\ \vec{\xi}\ } \xrightarrow{\mathsf{Intra}(Z^{-1})} \quad \boldsymbol{e} = \boxed{\ \vec{\psi}Z\ } \quad \boldsymbol{h}^* = \boxed{\ \vec{\xi}U\ }$$

7.2 Combinations of Basic Changes

7.2.1 Combination for Coefficient Vector Swapping

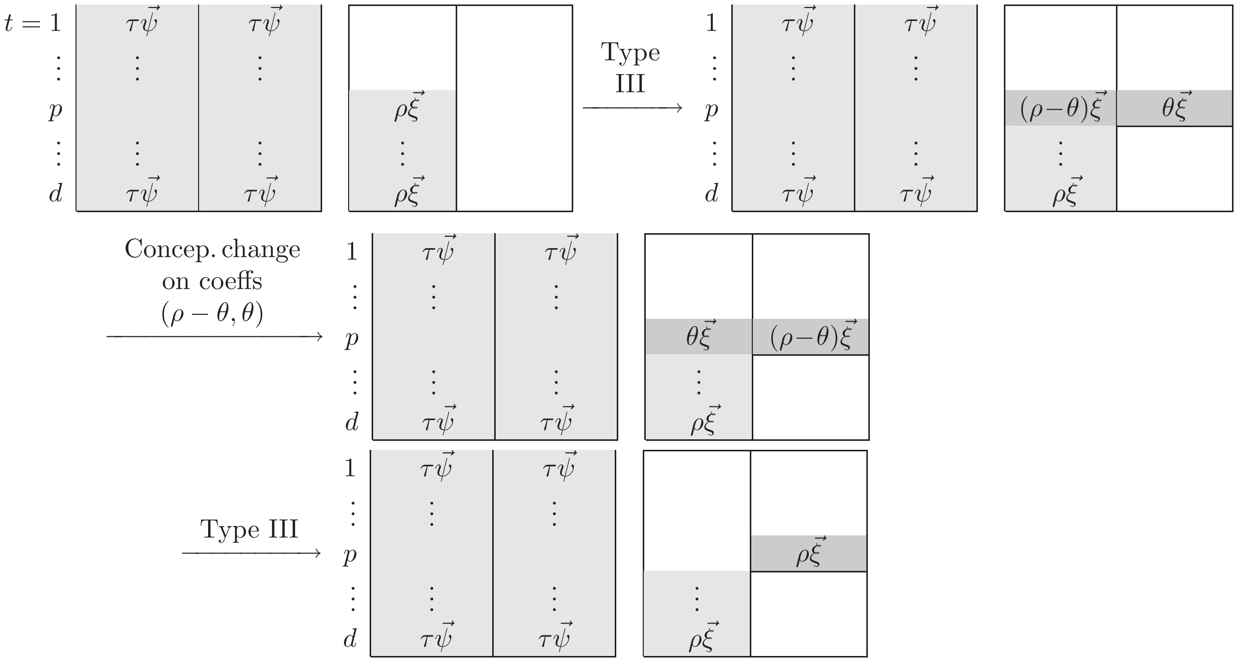
For the transition from Experiment 2-p-1 to Experiment 2-p-4, we use a game change based on a new type of computational change, the third type, which itself consisted of the first type computational change and an inter-subspace type conceptual change. Using a (toy) example in 2-dimensional 4 blocks, i.e., total is 8-dimension, we illustrate the third type change. The first block is included in the real-encoding part, the second and third ones are in the hidden part, and the fourth one is included in the secret-key randomness part. We remark that neither the first nor fourth part is described in the highlighted transformation in Section 7.3, where coefficients only in the hidden part are described.

Type III: The third type change transforms a key element $\boldsymbol{h}^* := (\delta\vec{\xi}, 0^2, 0^2, \vec{\eta})_{\mathbb{B}^*}$ to $\widetilde{\boldsymbol{h}}^* := (\delta\vec{\xi}, \theta\vec{\xi}, -\theta\vec{\xi}, \vec{\eta})_{\mathbb{B}^*}$ where a ciphertext element $\boldsymbol{e}$ has a form, $\boldsymbol{e} := (\omega\vec{\psi}, \tau\vec{\psi}, \tau\vec{\psi}, 0^2)_{\mathbb{B}}$, with $\omega, \tau, \delta, \theta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ (and with any $\vec{\psi}, \vec{\xi} \in \mathbb{F}_q^2$, not necessarily uniform). The change is composed of Type I change and an inter-subspace type conceptual change, so the security is proven from the DLIN assumption. Change of coefficients in the 8-dimensional space are given as:

$$\boldsymbol{e} = \begin{array}{|c|c|c|c|}\hline \omega\vec{\psi} & \tau\vec{\psi} & \tau\vec{\psi} & \phantom{\omega\vec{\psi}} \\ \hline\end{array} \qquad \boldsymbol{h}^* = \begin{array}{|c|c|c|c|}\hline \delta\vec{\xi} & \phantom{-\theta\vec{\xi}} & \phantom{-\theta\vec{\xi}} & \vec{\eta} \\ \hline\end{array}$$

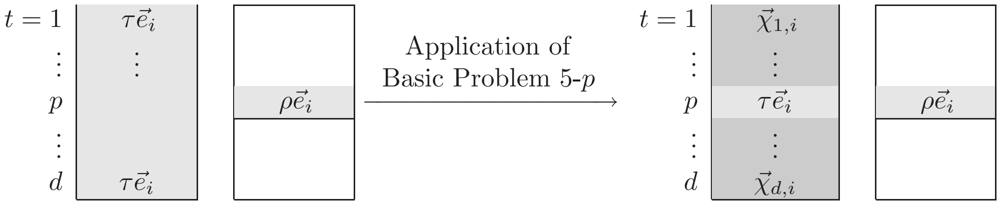
$$\xrightarrow{\text{Type III}} \quad \boldsymbol{e} = \begin{array}{|c|c|c|c|}\hline \omega\vec{\psi} & \tau\vec{\psi} & \tau\vec{\psi} & \phantom{\omega\vec{\psi}} \\ \hline\end{array} \qquad \widetilde{\boldsymbol{h}}^* = \begin{array}{|c|c|c|c|}\hline \delta\vec{\xi} & -\theta\vec{\xi} & \theta\vec{\xi} & \vec{\eta} \\ \hline\end{array}$$

The swapping using Type III changes is shown below pictorially, i.e., change of coefficients of $\boldsymbol{e}_t$ and $\boldsymbol{h}_t^*$ $(t = 1, \ldots, d)$ in 4-dimensional space in the hidden part are given as follows:



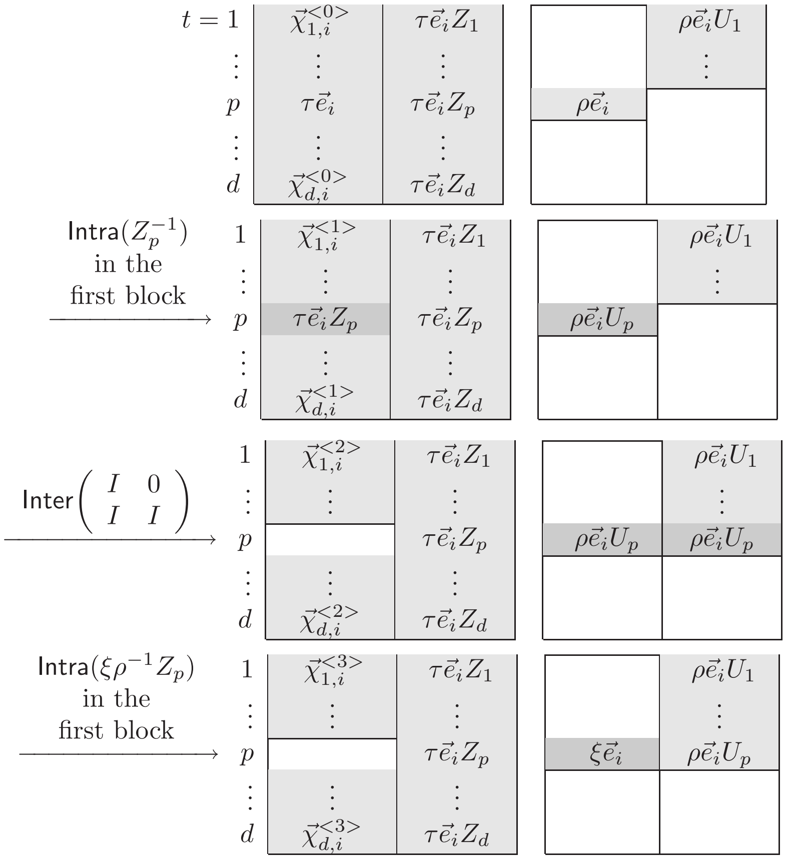
7.2.2 Randomness Masking (Application of Basic Problem 5-p)

For the transition from Experiment 2-p-4 to Experiment 2-p-5, we use a randomness masking transformation by applying Basic Problem 5-p in Definition 24. The problem consists of basic transformations in Section 7.1 (Appendix A.4.2). Change of coefficients of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ ($t = 1, \ldots, d; i = 1, 2$) in 2-dimensional space in the hidden part are given below, where $\vec{e}_i \in \mathbb{F}_q^2$ ($i = 1, 2$) are canonical basis vectors and $\vec{\chi}_{t,i}$ for $t = 1, \ldots, p-1, p+1, \ldots, d; i = 1, 2$ are random vectors in $\mathbb{F}_q^2$. To achieve this computational change, we employ the fact that indexes $\sigma_t(1, t)$ ($t \neq p$) and $\mu_p(p, -1)$ have random inner-product values.



7.2.3 Key Combination of Three Basic Conceptual Changes

For the transition from Experiment 2-p-5 to Experiment 2-p-6, we use a key conceptual change combined with three basic conceptual changes in Section 7.1.2, i.e., intra-subspace, inter-subspace, and intra-subspace transformations, given below pictorially. Change of coefficients of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ ($t = 1, \ldots, d; i = 1, 2$) in 4-dimensional space in the hidden part are given below, where $\vec{e}_i \in \mathbb{F}_q^2$ ($i = 1, 2$) are canonical basis vectors. After the series of the transformations, the U_p-multiplied canonical basis vectors $\rho\vec{e}_i U_p$ are inserted to the second block p-th row.

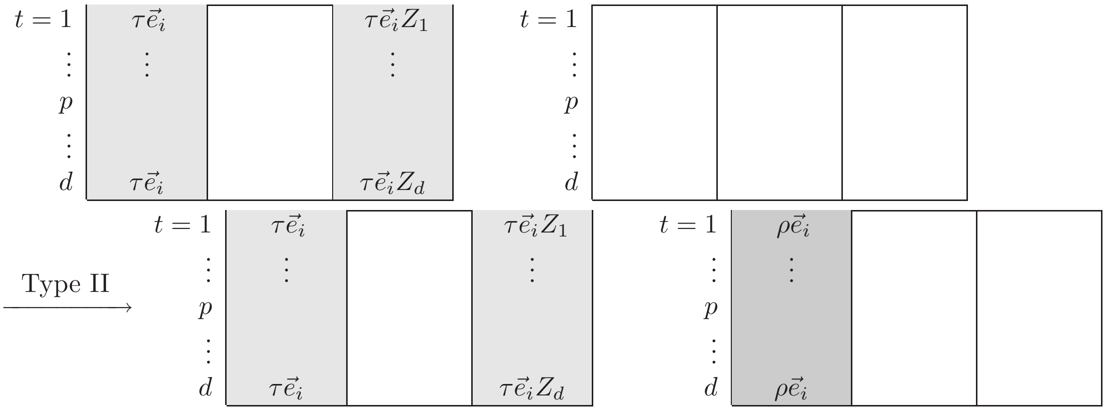


We will consider the effect to the other (i.e., $t \neq p$) rows in the first and second blocks. For the second block, only coefficients in $\boldsymbol{h}^*_{t,i}$ ($t \neq p$) are effected, where only the second change is related. Since the rows in the first block in $\boldsymbol{h}^*_{t,i}$ ($t \neq p$) are zero, the corresponding rows in the second block remain unchanged after the change. For the first block, all three changes are related in $\boldsymbol{e}_{t,i}$. By the first change, coefficients $\vec{\chi}^{<0>}_{t,i}$ ($t \neq p$) are changed to $\vec{\chi}^{<1>}_{t,i} := \vec{\chi}^{<0>}_{t,i} Z_p$, and changed to $\vec{\chi}^{<2>}_{t,i} := \vec{\chi}^{<1>}_{t,i} - \tau \vec{e}_i Z_t$ by the second change, and $\vec{\chi}^{<3>}_{t,i} := \xi^{-1}\rho\vec{\chi}^{<2>}_{t,i} Z_p^{-1}$ by the third change. Consequently, $\vec{\chi}^{<3>}_{t,i} := \xi^{-1}\rho(\vec{\chi}^{<0>}_{t,i} - \tau\vec{e}_i Z_t Z_p^{-1})$. Note that if $\vec{\chi}^{<0>}_{t,i}$ are uniformly and independently distributed, then $\vec{\chi}^{<3>}_{t,i}$ are so, and this is crucial for our (highlighted) transformation in Section 7.3.

7.3 Highlighted Transformation for the Proof of Lemma 24

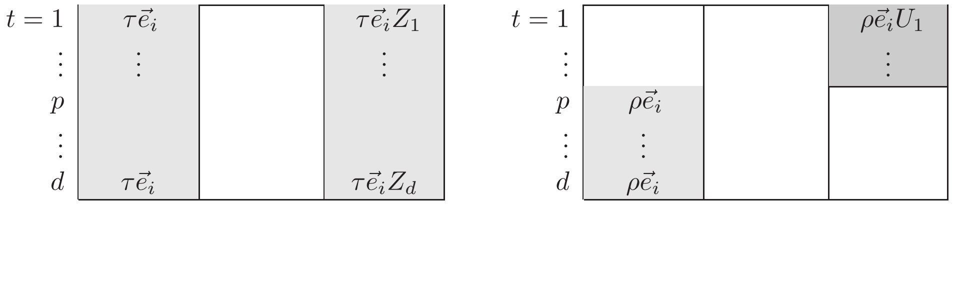
Our description focuses changes of coefficients in the hidden part with 2-dimensional 3 blocks i.e., total is 6-dimension, of ciphertexts elements $\boldsymbol{e}_{t,i}$ and secret-key elements $\boldsymbol{h}^*_{t,i}$ ($t = 1, \ldots, d; i = 1, 2$).

Experiments 0 and 1: Experiment 0 is equal to a Problem 2-ABE instance with $\beta := 0$. In Experiment 1, $\rho\vec{e}_i$ for $i = 1, 2$ are embedded to the first block of $\boldsymbol{h}^*_{t,i}$, by Type II computational change. Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ at Experiments 0 and 1 are given as follows:

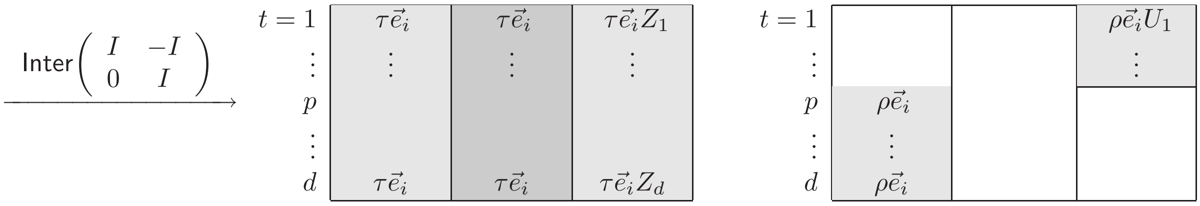


Experiment 2-p Sequence: The goal of the Experiment 2-p sequence is to change the coefficients $\rho\vec{e}_i$ in the p-th row in the first block of $\boldsymbol{h}^*_{p,i}$ to $\rho\vec{e}_i U_p$, and to transfer the changed one to the third block (of the p-th row). In other words, it is to embed a new matrix U_p to the third block.

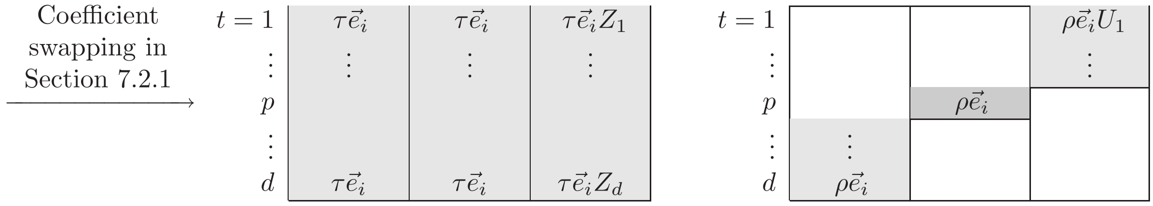
Just before the Experiment 2-p sequence, in Experiment 2-$(p-1)$-8, target matrices U_t, i.e., the adjoint matrices of Z_t, for $t < p$ are embedded in the t-th row of the third block in the hidden part of $\boldsymbol{h}^*_{t,i}$. Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ in Experiment 2-$(p-1)$-8 are given as follows:



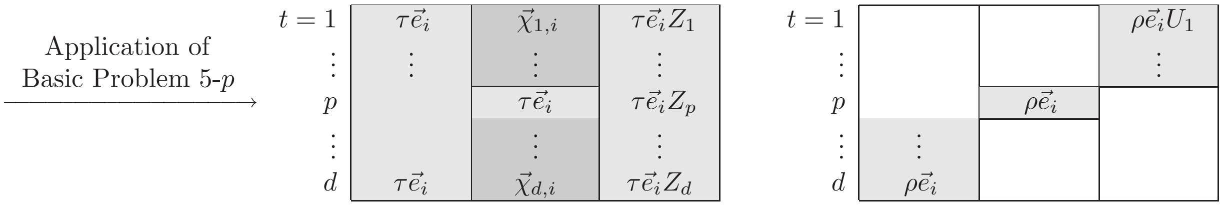
In Experiment 2-p-1, the first of the Experiment 2-p sequence, by the conceptual change $\mathsf{inter}\begin{pmatrix} I & -I \\ 0 & I \end{pmatrix}$ between the first and second blocks, coefficient vectors $\tau\vec{e}_i$ are embedded into the second block of $\boldsymbol{e}_{t,i}$ respectively for $i = 1, 2$. Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-1 are given as follows:


$\mathsf{Inter}\begin{pmatrix} I & -I \\ 0 & I \end{pmatrix}$
$t=1$ $\tau\vec{e}_i$ $\tau\vec{e}_i$ $\tau\vec{e}_iZ_1$
p
d $\tau\vec{e}_i$ $\tau\vec{e}_i$ $\tau\vec{e}_iZ_d$
$t=1$ $\rho\vec{e}_iU_1$
p $\rho\vec{e}_i$
d $\rho\vec{e}_i$

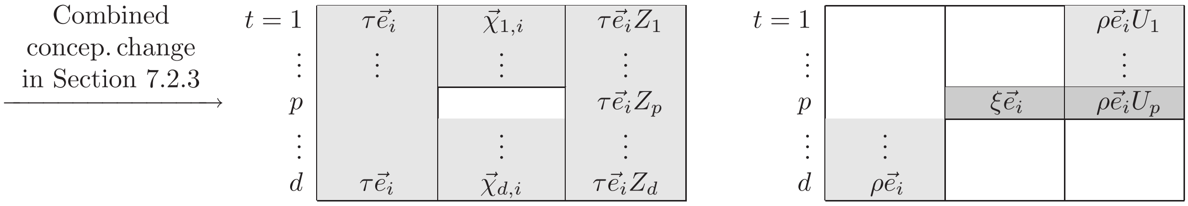
Then, by a swapping transformation in Section 7.2.1, we achieve a swapping of coefficients in the p-th row, between the first and second blocks of $\boldsymbol{h}^*_{p,i}$. Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-4 are given as follows:


Coefficient swapping in Section 7.2.1
$t=1$ $\tau\vec{e}_i$ $\tau\vec{e}_i$ $\tau\vec{e}_iZ_1$
p
d $\tau\vec{e}_i$ $\tau\vec{e}_i$ $\tau\vec{e}_iZ_d$
$t=1$ $\rho\vec{e}_iU_1$
p $\rho\vec{e}_i$
d $\rho\vec{e}_i$

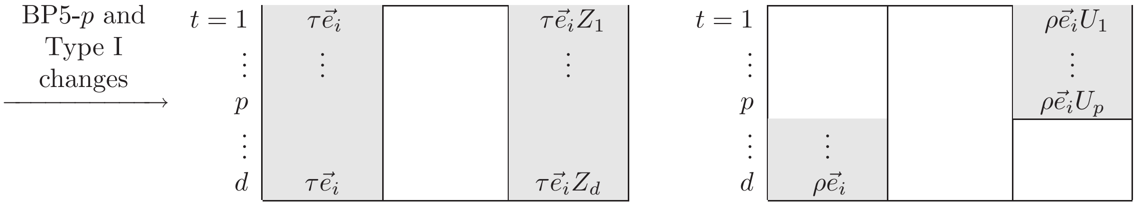
Next step to Experiment 2-p-5 is one of crucial points in the reduction. In the second block of $\boldsymbol{e}_{t,i}$, coefficient vectors except for the p-th row are changed to uniformly random. Since, indexes $\mu_{p,i}(p, -1)$ in $\boldsymbol{h}^*_{p,i}$ and $\sigma_{t,i}(1, t)$ in $\boldsymbol{e}_{t,i}$ for $t \neq p$ have uniformly and independently distributed inner product values, application of Basic Problem 5-p can make such a randomization. Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-5 are given as follows:


Application of Basic Problem 5-p
$t=1$ $\tau\vec{e}_i$ $\vec{\chi}_{1,i}$ $\tau\vec{e}_iZ_1$
p $\tau\vec{e}_i$ $\tau\vec{e}_iZ_p$
d $\tau\vec{e}_i$ $\vec{\chi}_{d,i}$ $\tau\vec{e}_iZ_d$
$t=1$ $\rho\vec{e}_iU_1$
p $\rho\vec{e}_i$
d $\rho\vec{e}_i$

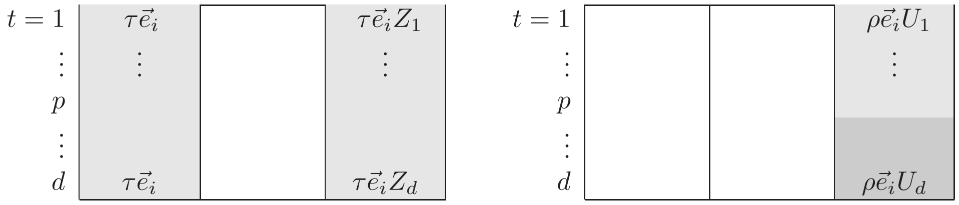
Note that, in Experiment 2-p-5, the p-th coefficients in the second block of $\boldsymbol{e}_{p,i}$ are independent from others in the same block. By applying a combined conceptual change composed of intra- and inter-subspace type changes given in Section 7.2.3, random dual matrices (U_p, Z_p) are embedded (Experiment 2-p-6). Note that since coefficients in the t-th ($t \neq p$) rows are random, their distributions are not affected by the conceptual change. Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-6 are given as follows:


Combined concep. change in Section 7.2.3
$t=1$ $\tau\vec{e}_i$ $\vec{\chi}_{1,i}$ $\tau\vec{e}_iZ_1$
p $\tau\vec{e}_iZ_p$
d $\tau\vec{e}_i$ $\vec{\chi}_{d,i}$ $\tau\vec{e}_iZ_d$
$t=1$ $\rho\vec{e}_iU_1$
p $\xi\vec{e}_i$ $\rho\vec{e}_iU_p$
d $\rho\vec{e}_i$

Here, we achieved the main aim, i.e., $\rho\vec{e}_i$ in the first block p-th row is changed to $\vec{e}_iU_p$ (in the second block), and it is embedded into the third block p-th row. Roughly speaking, the rest of the Experiment 2-p sequence reverses the process before Experiment 2-p-5, and arrives at Experiment 2-p-8, i.e., the initial state of the Experiment 2-$(p+1)$ sequence. Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-8 are given as follows:



Final Experiment: After all the Experiment 2-p sequences for $p=1,\ldots,d$, we reach Experiment 2-d-8, where independent pairs of dual (adjoint) matrices (U_t, Z_t) for $t=1,\ldots,d$ are embedded into the third block, i.e., which is equal to a Problem 2-ABE instance with $\beta := 1$. Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ and $\boldsymbol{h}^*_{t,i}$ in Experiment 2-d-8 are given as follows:



References

[1] Nuttapong Attrapadung and Benoît Libert. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 384–402. Springer, 2010.

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

[3] Mihir Bellare, Brent Waters, and Scott Yilek. Identity-based encryption secure against selective opening attack. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 235–252. Springer, 2011.

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

[5] Dan Boneh and Brent Waters. Conjunctive, subset, and range queries on encrypted data. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 535–554. Springer, 2007.

[6] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 2006*, pages 89–98. ACM, 2006.

[7] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 146–162. Springer, 2008.

[8] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91. Springer, 2010. Full version is available at `http://eprint.iacr.org/2010/110`.

[9] Allison B. Lewko and Brent Waters. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 455–479. Springer, 2010.

[10] Allison B. Lewko and Brent Waters. Decentralizing attribute-based encryption. In Paterson [19], pages 568–588.

[11] Allison B. Lewko and Brent Waters. Unbounded HIBE and attribute-based encryption. In Paterson [19], pages 547–567.

[12] Allison B. Lewko and Brent Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 180–198. Springer, 2012.

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

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

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

[16] Tatsuaki Okamoto and Katsuyuki Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In David Pointcheval and Thomas Johansson, editors, *Eurocrypt 2012*, volume 7237 of *LNCS*, pages 591–608. Springer, 2012. Full version is available at `http://eprint.iacr.org/2011/543`.

[17] Tatsuaki Okamoto and Katsuyuki Takashima. Efficient (hierarchical) inner product encryption tightly reduced from the decisional linear assumption. *To appear in IEICE Trans. Fundamentals*, vol.E96-A, no.1, Jan. 2013, 2013.

[18] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *ACM CCS 2007*, pages 195–203. ACM, 2007.

[19] Kenneth G. Paterson, editor. *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *LNCS*. Springer, 2011.

[20] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, 2005.

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

[22] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 53–70. Springer, 2011.

A Proofs of Lemmas

A.1 Proofs of Lemmas 3 and 4 in Section 5.1.4

A.1.1 Proof of Lemma 3

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

For any adversary $\mathcal{B}$, there exist probabilistic machines $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P1\text{-}IPE}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_0}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_1}(\lambda) + \sum_{p=1}^{d}\sum_{j=1}^{2}\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}j}}(\lambda) + \epsilon$, where $\mathcal{F}_{2\text{-}p\text{-}j}(\cdot) := \mathcal{F}_2(p, j, \cdot), \epsilon := (10d + 5)/q$.

Proof. Lemma 3 is proven by a hybrid argument consisting of three experiments, i.e., Exp 1, 2, 3, where the differences of the experiments are given by a choice of $(\beta_1, \beta_2) \in \{0,1\}^2$ for $(\boldsymbol{e}_{\beta_1,0}, \{\boldsymbol{e}_{\beta_1,t,i}\}_{t=1,\dots,d;\ i=1,2})$ and $\widetilde{\boldsymbol{e}}_{\beta_2,1}$. (The other variables are given in the same manner as in Problem 1-IPE.) Exp 1 uses the choice of $(\beta_1, \beta_2) = (0,0)$, then is the same as Problem 1-IPE for $\beta = 0$. Exp 2 uses the choice of $(\beta_1, \beta_2) = (0,1)$. Exp 3 uses the choice of $(\beta_1, \beta_2) = (1,1)$, then is the same as Problem 1-IPE for $\beta = 1$. Therefore, Lemma 3 is obtained by combining of Lemmas 31, 32 and 23. □

Lemma 31 *Exp 1 and 2 are computationally indistinguishable under the DLIN assumption.*

For any adversary $\mathcal{B}$, there exist a probabilistic machine $\mathcal{F}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\Pr[\mathsf{Exp1}_{\mathcal{B}}(\lambda) \to 1] - \Pr[\mathsf{Exp2}_{\mathcal{B}}(\lambda) \to 1]| \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + \epsilon$, where $\epsilon := 5/q$.

Lemma 31 is proven in a similar manner to Lemma 1 in [14].

Problem 1-ABE is given in Definition 18 in Section 6.1.3.

Lemma 32 *Exp 2 and 3 are computationally indistinguishable under the computational intractability of Problem 1-ABE.*

For any adversary $\mathcal{B}$, there exist a probabilistic machine $\mathcal{C}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\Pr[\mathsf{Exp2}_{\mathcal{B}}(\lambda) \to 1] - \Pr[\mathsf{Exp3}_{\mathcal{B}}(\lambda) \to 1]| \le \mathsf{Adv}^{\mathsf{P1\text{-}ABE}}_{\mathcal{C}}(\lambda)$.

Proof. In order to prove Lemma 32, we construct a probabilistic machine $\mathcal{C}$ against Problem 1-ABE using an adversary $\mathcal{B}$ in an experiment (Exp 2 or 3) as a black box as follows: $\mathcal{C}$ is given a Problem 1-ABE instance, $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,i}\}_{t=1,\dots,d;i=1,2})$. Note that the dimension $N := 14$, and $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \dots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14}), \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \dots, \boldsymbol{b}^*_4, \boldsymbol{b}^*_{11}, \boldsymbol{b}^*_{12})$. From the basis vectors, $\mathcal{C}$ calculates new basis vectors in 15 dimensional spaces

$$\begin{aligned}
&\boldsymbol{d}_i := (\boldsymbol{b}_i, 0)\, W, \quad \boldsymbol{d}^*_i := (\boldsymbol{b}^*_i, 0)\, (W^{-1})^{\mathrm{T}} \text{ for } i = 1, \dots, 10, \\
&\boldsymbol{d}_{11} := (0^{14}, G)\, W, \quad \boldsymbol{d}^*_{11} := (0^{14}, \psi G)\, (W^{-1})^{\mathrm{T}}, \\
&\boldsymbol{d}_i := (\boldsymbol{b}_{i-1}, 0)\, W, \quad \boldsymbol{d}^*_i := (\boldsymbol{b}^*_{i-1}, 0)\, (W^{-1})^{\mathrm{T}} \text{ for } i = 12, \dots, 15, \\
&\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \dots, \boldsymbol{d}_4, \boldsymbol{d}_{14}, \boldsymbol{d}_{15}), \ \widehat{\mathbb{D}}^* := (\boldsymbol{d}^*_1, \dots, \boldsymbol{d}^*_4, \boldsymbol{d}^*_{12}, \boldsymbol{d}^*_{13}),
\end{aligned}$$

where $W \xleftarrow{\mathsf{U}} GL(15, \mathbb{F}_q)$. Then, $\mathcal{C}$ calculates

$$\{\boldsymbol{f}_{\beta,t,i} := \boldsymbol{e}_{\beta,t,i}\, W\}_{t=1,\dots,d;i=1,2},\ \ \widetilde{\boldsymbol{e}}_{1,1} := (\widetilde{\sigma}, 0^9, \theta, 0^2, \widetilde{\phi}_1, \widetilde{\phi}_2)_{\mathbb{D}},\ \ \widetilde{\boldsymbol{e}}_2 := \widetilde{\sigma}\boldsymbol{d}_2,$$

where $\widetilde{\sigma}, \theta, \widetilde{\phi}_1, \widetilde{\phi}_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\mathcal{C}$ gives an instance $\varrho := (\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{D}}, \widehat{\mathbb{D}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{f}_{\beta,t,i}\}_{t=1,\dots,d;i=1,2}, \widetilde{\boldsymbol{e}}_{1,1}, \widetilde{\boldsymbol{e}}_2)$ to $\mathcal{B}$. When $\beta = 0$ (resp. $\beta = 1$), ϱ is an instance for Exp 2 (resp. Exp 3). Then, the inequality in Lemma 32 holds, and this completes the proof of Lemma 32. □

A.1.2 Proof of Lemma 4

Lemma 4 *Problem 2-IPE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, there exist probabilistic machines $\mathcal{F}_1, \mathcal{F}_{2\text{-}1}, \dots, \mathcal{F}_{2\text{-}5}$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P2\text{-}IPE}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_1}(\lambda) + \sum_{p=1}^{d} \sum_{j=1}^{2} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}2\text{-}j}}(\lambda) + \sum_{l=1,\dots,d;\ l\neq p} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}}(\lambda)\Big) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}5\text{-}j}}(\lambda)\Big) + \epsilon$, where $\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}1}(p, j, \cdot), \mathcal{F}_{2\text{-}p\text{-}2\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}2}(p, j, \cdot)$, $\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}3}(p, j, l, \cdot), \mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}4}(p, j, l, \cdot), \mathcal{F}_{2\text{-}p\text{-}5\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}5}(p, j, \cdot)$ and $\epsilon := (20d^2 + 10d + 5)/q$.

Lemma 4 is proven by combining Lemma 33 and 24.

Lemma 33 *Problem 2-IPE is computationally intractable under the computational intractability of Problem 2-ABE.*

For any adversary $\mathcal{B}$, there exist a probabilistic machine $\mathcal{C}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P2\text{-}IPE}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{P2\text{-}ABE}}_{\mathcal{C}}(\lambda)$.

Proof. In order to prove Lemma 33, we construct a probabilistic machine $\mathcal{C}$ against Problem 2-ABE using an adversary $\mathcal{B}$ against Problem 2-IPE as a black box as follows: $\mathcal{C}$ is given a Problem 2-ABE instance, $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\dots,d;i=1,2})$. Note that the dimension $N := 14$, and $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \dots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14}), \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \dots, \boldsymbol{b}^*_4, \boldsymbol{b}^*_{11}, \boldsymbol{b}^*_{12})$. From the basis vectors, $\mathcal{C}$ calculates new basis vectors in 15 dimensional spaces

$$\begin{aligned}
&\boldsymbol{d}_i := (\boldsymbol{b}_i, 0)\, W,\ \ \boldsymbol{d}^*_i := (\boldsymbol{b}^*_i, 0)\, (W^{-1})^{\mathrm{T}} \text{ for } i = 1, \dots, 10,\\
&\boldsymbol{d}_{11} := (0^{14}, G)\, W,\ \ \boldsymbol{d}^*_{11} := (0^{14}, \psi G)\, (W^{-1})^{\mathrm{T}},\\
&\boldsymbol{d}_i := (\boldsymbol{b}_{i-1}, 0)\, W,\ \ \boldsymbol{d}^*_i := (\boldsymbol{b}^*_{i-1}, 0)\, (W^{-1})^{\mathrm{T}} \text{ for } i = 12, \dots, 15,\\
&\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \dots, \boldsymbol{d}_4, \boldsymbol{d}_{14}, \boldsymbol{d}_{15}),\ \ \widehat{\mathbb{D}}^* := (\boldsymbol{d}^*_1, \dots, \boldsymbol{d}^*_4, \boldsymbol{d}^*_{12}, \boldsymbol{d}^*_{13}),
\end{aligned}$$

where $W \xleftarrow{\mathsf{U}} GL(15, \mathbb{F}_q)$. Then, $\mathcal{C}$ calculates

$$\{\boldsymbol{f}_{t,i} := \boldsymbol{e}_{t,i}\, W,\ \ \boldsymbol{p}^*_{\beta,t,i} := \boldsymbol{h}^*_{\beta,t,i}\, (W^{-1})^{\mathrm{T}}\}_{t=1,\dots,d;i=1,2}.$$

$\mathcal{C}$ gives an instance $\varrho := (\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{p}^*_{\beta,t,i}, \boldsymbol{f}_{t,i}\}_{t=1,\dots,d;i=1,2})$ to $\mathcal{B}$. ϱ is an instance of Problem 2-IPE for β. Then, the inequality in Lemma 33 holds, and this completes the proof of Lemma 33. □

A.2 Proofs of Lemmas 9–13 in Section 5.1.6

Lemma 9 *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, $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1\text{-}IPE}}_{\mathcal{B}_1}(\lambda)$.*

Proof. In order to prove Lemma 9, we construct a probabilistic machine $\mathcal{B}_1$ against Problem 1-IPE using an adversary $\mathcal{A}$ in a security game (Game 0' or 1) as a black box as follows:

1. $\mathcal{B}_1$ is given a Problem 1-IPE instance, $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,i}\}_{t=1,\dots,d;i=1,2}, \widetilde{\boldsymbol{e}}_{\beta,1}, \widetilde{\boldsymbol{e}}_2)$.
2. $\mathcal{B}_1$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_1$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$ of Game 0' (and 1), where $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \dots, \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15})$.
4. When a key query is issued for vector $\vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}}\}$, $\mathcal{B}_1$ answers normal key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ with Eq. (3), that is computed using $\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*$ of the Problem 1-IPE instance.
5. When $\mathcal{B}_1$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\vec{x}^{(0)} := \{(t, x_t^{(0)}) \,|\, t \in I_{\vec{x}}\}, \vec{x}^{(1)} := \{(t, x_t^{(1)}) \,|\, t \in I_{\vec{x}}\}$ with $I_{\vec{x}} := I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ from $\mathcal{A}$, $\mathcal{B}_1$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ such that

   $$\boldsymbol{c}_0 := \boldsymbol{e}_{\beta,0} + \zeta \boldsymbol{b}_{0,3}, \qquad \boldsymbol{c}_t := x_t^{(b)} \boldsymbol{e}_{\beta,t,1} + \xi_1 \boldsymbol{e}_{\beta,t,2} + \xi_2 \boldsymbol{b}_4, \qquad c_T := g_T^\zeta m^{(b)},$$

   where $\zeta, \xi_1, \xi_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\boldsymbol{b}_{0,3}, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,i}\}_{t=1,\dots,d;i=1,2}, \boldsymbol{b}_4)$ is a part of the Problem 1-IPE instance.
6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_1$ executes the same procedure as that of step 4.
7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_1$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_1$ outputs $\beta' := 0$.

It is straightforward that the distribution by $\mathcal{B}_1$'s simulation given a Problem 1-IPE instance with β is equivalent to that in Game 0' (resp. Game 1), when $\beta = 0$ (resp. $\beta = 1$). □

Lemma 10 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2\text{-}IPE}}(\lambda) + 2/q$, where $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.*

Proof. In order to prove Lemma 10, we construct a probabilistic machine $\mathcal{B}_2$ against Problem 2-IPE 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. $\mathcal{B}_2$ is given an integer h and a Problem 2-IPE instance, $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{\beta,t,j}^*, \boldsymbol{e}_{t,j}\}_{t=1,\dots,d;j=1,2})$.
2. $\mathcal{B}_2$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_2$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$ of Game 2-$(h-1)$-2 (and 2-h-1), where $\widehat{\mathbb{B}}_0$ and $\widehat{\mathbb{B}}$ are obtained from the Problem 2-IPE instance.
4. When the ι-th key query is issued for vector $\vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}}\}$, $\mathcal{B}_2$ answers as follows:
   (a) When $1 \le \iota \le h-1$, $\mathcal{B}_2$ answers semi-functional key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ with Eq. (7), that is computed using $\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*$ of the Problem 2-IPE instance.
   (b) When $\iota = h$, $\mathcal{B}_2$ calculates $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ using $(\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_4^*, \boldsymbol{h}_{\beta,0}^*, \{\boldsymbol{h}_{\beta,t,j}^*\}_{t=1,\dots,d;j=1,2})$ of the Problem 2-IPE instance as follows:

   $$\begin{aligned}&\text{for } t \in I_{\vec{v}}, \quad g_t, \xi_t \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \boldsymbol{p}_{\beta,0,t}^* := g_t \boldsymbol{h}_{\beta,0}^* + \xi_t \boldsymbol{b}_{0,1}^*, \ \boldsymbol{p}_{\beta,t,2}^* := g_t \boldsymbol{h}_{\beta,t,2}^* + \xi_t \boldsymbol{b}_4^*,\\ &\boldsymbol{k}_0^* := -\textstyle\sum_{t \in I_{\vec{v}}} \boldsymbol{p}_{\beta,0,t}^* + \boldsymbol{b}_{0,3}^*,\\ &\text{for } t \in I_{\vec{v}}, \quad \boldsymbol{k}_t^* := v_t \boldsymbol{h}_{\beta,t,1}^* + \boldsymbol{p}_{\beta,t,2}^*.\end{aligned}$$

(c) When $\iota \geq h+1$, $\mathcal{B}_2$ answers normal key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ with Eq. (3), that is computed using $\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*$ of the Problem 2-IPE instance.

5. When $\mathcal{B}_2$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\vec{x}^{(0)} := \{(t, x_t^{(0)}) \,|\, t \in I_{\vec{x}}\}, \vec{x}^{(1)} := \{(t, x_t^{(1)}) \,|\, t \in I_{\vec{x}}\}$ with $I_{\vec{x}} := I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ from $\mathcal{A}$, $\mathcal{B}_2$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ such that

$$\boldsymbol{c}_0 := \boldsymbol{e}_0 + \zeta \boldsymbol{b}_{0,3}, \qquad \boldsymbol{c}_t := x_t^{(b)} \boldsymbol{e}_{t,1} + \theta_1 \boldsymbol{e}_{t,2} + \theta_2 \boldsymbol{b}_4, \qquad c_T := g_T^{\zeta} m^{(b)},$$

where $\zeta, \theta_1, \theta_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\boldsymbol{b}_{0,3}, \boldsymbol{e}_0, \{\boldsymbol{e}_{t,j}\}_{t=1,..,n; j=1,2})$ is a part of the Problem 2-IPE instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_2$ executes the same procedure as that of step 4.

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

Claim 1 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_2$ given a Problem 2-IPE instance with $\beta \in \{0,1\}$ is the same as that in Game 2-$(h-1)$-2 (resp. Game 2-h-1) if $\beta = 0$ (resp. $\beta = 1$) except with probability $1/q$ (resp. $1/q$).*

Proof. It is straightforward that the distribution by $\mathcal{B}_2$'s simulation given a Problem 2-IPE instance with $\beta = 0$ is equivalent to that in Game 2-$(h-1)$-2 except that δ defined in Problem 2-IPE is zero, i.e., except with probability $1/q$.

When $\beta = 1$, the challenge ciphertext in the above simulation is given as:

$\boldsymbol{c}_0 := (\widetilde{\omega},\ \widetilde{\tau},\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0}$,
for $t \in I_{\vec{x}}$,

$$\boldsymbol{c}_t := (\ \overbrace{\widetilde{\sigma}_t(1,\ t),\ \omega x_t^{(b)}, \widetilde{\omega},}^{4}\ \ \overbrace{(\tau x_t^{(b)},\ \widetilde{\tau}),\ 0^2,\ (\tau x_t^{(b)},\ \widetilde{\tau}) \cdot Z_t,\ 0,}^{7}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\widetilde{\varphi}_{t,1}, \widetilde{\varphi}_{t,2}}^{2}\ )_{\mathbb{B}},$$

where $\widetilde{\sigma}_t := x_t^{(b)} \sigma_{t,1} + \sigma_{t,2}, \widetilde{\omega} := \theta_1 \omega + \theta_2, \widetilde{\tau} := \theta_1 \tau, \widetilde{\varphi}_{t,j} := x_t^{(b)} \varphi_{t,1,j} + \varphi_{t,2,j}$ for $j = 1,2$, $\omega, \tau, \{\sigma_{t,j}, \varphi_{t,i,j}\}_{t \in I_{\vec{x}};\ i,j=1,2}$ are defined in Problem 2-IPE.

$\boldsymbol{p}_{\beta,0,t}^*, \boldsymbol{p}_{\beta,t,2}^*$ for $t \in I_{\vec{v}}$ calculated in case (b) of steps 4 and 6 in the above simulation are expressed as:

$$s_t := g_t \delta + \xi_t, \quad a_k := g_k \rho, \quad \boldsymbol{p}_{0,0,t}^* = (s_t, 0, 0, g_t \eta_0, 0)_{\mathbb{B}_0^*}, \quad \boldsymbol{p}_{1,0,t}^* = (s_t, a_t, 0, g_t \eta_0, 0)_{\mathbb{B}_0^*},$$

$$\begin{array}{llcccc}
\boldsymbol{p}_{0,t,2}^* := & (\ \overbrace{g_t \mu_{t,2}(t,\ -1),\ 0,\ s_t,}^{4} & \overbrace{0^7,}^{7} & \overbrace{g_t(\eta_{t,2,1}, \eta_{t,2,2}),}^{2} & \overbrace{0^2}^{2} &)_{\mathbb{B}^*}, \\
\boldsymbol{p}_{1,t,2}^* := & (\ g_t \mu_{t,2}(t,\ -1),\ 0,\ s_t, & 0^4,\ (0,\ a_t) U_t,\ 0, & g_t(\eta_{t,j,1}, \eta_{t,j,2}), & 0^2 &)_{\mathbb{B}^*},
\end{array}$$

where $\delta, \rho, \eta_0, \{\mu_{t,2}, U_t, \eta_{t,2,1}, \eta_{t,2,2}\}_{t \in I_{\vec{v}}}$ are defined in Problem 2-IPE. Therefore, $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ are expressed as:

$s_0 := \sum_{t=1}^n s_t, \quad a_0 := \sum_{t=1}^n a_t, \quad \widetilde{\eta}_0 := (\sum_{t=1}^n g_t) \eta_0,$
if $\beta = 0$, $\ \widetilde{\boldsymbol{k}}_0^* = (-s_0, 0, 1, \widetilde{\eta}_0, 0)_{\mathbb{B}_0^*}$, $\quad$ if $\beta = 1$, $\ \widetilde{\boldsymbol{k}}_0^* = (-s_0, -a_0, 1, \widetilde{\eta}_0, 0)_{\mathbb{B}_0^*}$,

$$\begin{array}{llcccc}
\text{if } \beta = 0, \ \ \boldsymbol{k}_t^* := & (\ \overbrace{\widetilde{\mu}_t(t,\ -1),\ \delta v_t,\ s_t,}^{4} & \overbrace{0^7,}^{7} & \overbrace{\widetilde{\eta}_{t,1}, \widetilde{\eta}_{t,2},}^{2} & \overbrace{0^2}^{2} &)_{\mathbb{B}^*}, \\
\text{if } \beta = 1, \ \ \boldsymbol{k}_t^* := & (\ \widetilde{\mu}_t(t,\ -1),\ \delta v_t,\ s_t, & 0^4,\ (\rho v_t,\ a_t) \cdot U_t,\ 0, & \widetilde{\eta}_{t,1}, \widetilde{\eta}_{t,2}, & 0^2 &)_{\mathbb{B}^*},
\end{array}$$

where $\delta, \rho, s_t, a_t, \widetilde{\mu}_t := v_t\mu_{t,1} + g_t\mu_{t,2}, \widetilde{\eta}_{t,j} := v_t\eta_{t,j} + g_t\eta_{t,j}$ for $t \in I_{\vec{v}}; j = 1, 2$ are independently and uniformly distributed. Therefore, $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t\in I_{\vec{v}}})$ and $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t\in I_{\vec{x}}})$ are distributed as in Eqs. (6) and (5), respectively. Therefore, when $\beta = 1$, the distribution by $\mathcal{B}_2$'s simulation is equivalent to that in Game 2-h-1 except that δ defined in Problem 2-IPE is zero, i.e., except with probability $1/q$. □

This completes the proof of Lemma 10. □

Lemma 11 *For any adversary $\mathcal{A}$, for any security parameter λ,* $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)$.

Proof. It is clear that the distribution of the public-key and the ι-th key query's answer for $\iota \neq h$ in Game 2-h-1 and Game 2-h-2 are exactly the same. Therefore, to prove this lemma we will show that the joint distribution of the h-th key query's answer and the challenge ciphertext in Game 2-h-1 and Game 2-h-2 are equivalent.

Let $\vec{r}_t := (\pi v_t, a_t) \cdot U_t$, which is coefficients of the t-th key element $\boldsymbol{k}_t^*$ for $t \in I_{\vec{v}}$, and $\vec{w}_t := (\tau x_t^{(b)}, \widetilde{\tau}) \cdot Z_t$, which is coefficients of the t-th ciphertext element $\boldsymbol{c}_t$ for $t \in I_{\vec{x}}$ in Game 2-h-1. Let $n := \sharp(I_{\vec{v}}),\ n' := \sharp(I_{\vec{x}})$, and n elements of $I_{\vec{v}}$ are expressed by $\{t_1, \ldots, t_n \,|\, 1 \leq t_1 \leq t_2 \leq \cdots \leq t_n \leq d\}$. We will show that $(a_0, \{\vec{r}_t\}_{t\in I_{\vec{v}}}, \{\vec{w}_t\}_{t\in I_{\vec{x}}}) \in \mathbb{F}_q \times \left(\mathbb{F}_q^2\right)^n \times \left(\mathbb{F}_q^2\right)^{n'}$ are uniformly and independently distributed from the other variables in the joint distribution of adversary $\mathcal{A}$'s view.

When $I_{\vec{v}} \not\subseteq I_{\vec{x}}$, there exist an index $t_i \in I_{\vec{v}} \setminus I_{\vec{x}}$, and coefficients $\vec{w}_{t_i} := (\pi v_{t_i}, a_{t_i}) \cdot U_{t_i}$ of $\boldsymbol{k}_{t_i}^*$ is uniformly and independently distributed in $\mathbb{F}_q^2$ since $U_{t_i} \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$ is uniformly and independently distributed from the other variables in $\mathcal{A}$'s view. Moreover, variables a_{t_j} for $j = 1, \ldots, i-1, i+1, \ldots, n$ and $a_0 := \sum_{j=1,,\ldots,i-1,i+1,\ldots,n} a_{t_j}$ are also uniformly and independently distributed in $\mathbb{F}_q$ since a_{t_i} appears only in $\vec{w}_{t_i}$ in $\mathcal{A}$'s view. Therefore, from Lemma 8, variables $(a_0, \{\vec{r}_t\}_{t\in I_{\vec{v}}}, \{\vec{w}_t\}_{t\in I_{\vec{x}}})$ are uniformly and independently distributed from the other variables.

When $I_{\vec{v}} \subseteq I_{\vec{x}}$, it holds that $\sum_{t\in I_{\vec{v}}} v_t x_t \neq 0$ from the definition of the security game. Since $\vec{r}_t \cdot \vec{w}_t = \pi\tau v_t x_t + \widetilde{\tau} a_t$, $(a_0, \{\vec{r}_t \cdot \vec{w}_t\}_{t\in I_v}) = (a_0, \vec{r}_{t_1} \cdot \vec{w}_{t_1}, \ldots, \vec{r}_{t_n} \cdot \vec{w}_{t_n})$ are represented as

$$\begin{pmatrix} a_0 \\ \vec{r}_{t_1} \cdot \vec{w}_{t_1} \\ \vdots \\ \vec{r}_{t_n} \cdot \vec{w}_{t_n} \end{pmatrix} = M \cdot \begin{pmatrix} \pi \\ a_{t_1} \\ \vdots \\ a_{t_n} \end{pmatrix}, \quad \text{where } M := \begin{pmatrix} 0 & 1 & \ldots & 1 \\ \tau v_{t_1} x_{t_1} & \widetilde{\tau} & & \\ \vdots & & \ddots & \\ \tau v_{t_n} x_{t_n} & & & \widetilde{\tau} \end{pmatrix} \tag{24}$$

The determinant of M is given by $\det(M) = (\widetilde{\tau})^{n-1}\,\tau(\sum_{i=1}^{n} v_{t_i} x_{t_i}) = (\widetilde{\tau})^{n-1}\,\tau(\sum_{t\in I_{\vec{v}}} v_t x_t)$, which is nonzero since $\sum_{t\in I_{\vec{v}}} v_t x_t \neq 0$ with all but negligible probability $2/q$, i.e., except when $\tau = 0$ or $\widetilde{\tau} = 0$. Since fresh variables $(\pi, \{a_t\}_{t\in I_{\vec{v}}})$ appear only in $(a_0, \{\vec{r}_t \cdot \vec{w}_t\}_{t\in I_{\vec{v}}})$ in $\mathcal{A}$'s view, these variables $(a_0, \{\vec{r}_t \cdot \vec{w}_t\}_{t\in I_{\vec{v}}})$ are also fresh, i.e., uniformly and independently distributed from the other variables. Then, from Lemma 8, variables $(a_0, \{\vec{r}_t\}_{t\in I_{\vec{v}}}, \{\vec{w}_t\}_{t\in I_{\vec{x}}})$ are uniformly and independently distributed from the other variables when $I_{\vec{v}} \subseteq I_{\vec{x}}$, too.

Therefore, the view of adversary $\mathcal{A}$ in the Game 2-h-1 is the same as that in Game 2-h-2. This completes the proof of Lemma 11. □

Lemma 12 *For any adversary $\mathcal{A}$, for any security parameter λ,* $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \leq 1/q$.

Proof. To prove Lemma 12, we will show distribution of public parameters, queried keys, and challenge ciphertext, $(\mathsf{param}, \widehat{\mathbb{B}}, \{\mathsf{sk}^{(h)} := (\boldsymbol{k}_0^{(h)*}, \{\boldsymbol{k}_t^{(h)*}\}_{t\in I_{\vec{v}}})\}_{h=1,\ldots,\nu}, \mathsf{ct} := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t\in I_{\vec{x}}}, c_T))$, in Game 2-$\nu$-2 and that in Game 3 are equivalent.

First, we note that a part of ciphertext $\{\boldsymbol{c}_t\}_{t\in I_{\vec{v}}}$ in Game 2-ν-2 and that in Game 3 are equivalently distributed since matrices $\{Z_t \xleftarrow{\mathsf{U}} GL(2,\mathbb{F}_q)\}_{t\in I_{\vec{v}}}$ of $\{\boldsymbol{c}_t\}_{t\in I_{\vec{v}}}$ in Game 2-ν-2 are uniformly and independently distributed from other variables.

For the distribution of $\boldsymbol{k}_0^*$ and $\boldsymbol{c}_0$, we define new dual orthonormal bases $(\mathbb{D}_0, \mathbb{D}_0^*)$ of $\mathbb{V}_0$ as follows:

We generate $\chi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and set

$$\begin{aligned}&\boldsymbol{d}_{0,2} := \boldsymbol{b}_{0,2} - \chi\boldsymbol{b}_{0,3},\ \ \boldsymbol{d}_{0,3}^* := \boldsymbol{b}_{0,3}^* + \chi\boldsymbol{b}_{0,2}^*\\ &\mathbb{D}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{d}_{0,2}, \boldsymbol{b}_{0,3}, \ldots, \boldsymbol{b}_{0,5}),\ \ \mathbb{D}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,2}^*, \boldsymbol{d}_{0,3}^*, \boldsymbol{b}_{0,4}^*, \boldsymbol{b}_{0,5}^*).\end{aligned}$$

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 $t = 0$ elements of keys and challenge ciphertext $(\{\boldsymbol{k}_0^{(h)*}\}_{h=1,\ldots,\nu}, \boldsymbol{c}_0)$ in Game 2-ν-2 are expressed over bases $(\mathbb{B}_0, \mathbb{B}_0^*)$ and $(\mathbb{D}_0, \mathbb{D}_0^*)$ as

$$\begin{aligned}\boldsymbol{k}_0^{(h)*} &:= (\ -s_0^{(h)},\ r_0^{(h)},\ 1,\ \eta_0^{(h)},\ 0\ )_{\mathbb{B}_0^*} = (\ -s_0^{(h)},\ r_0^{(h)} - \chi,\ 1,\ \eta_0^{(h)},\ 0\ )_{\mathbb{D}_0^*}\\ &= (\ -s_0^{(h)},\ \widetilde{r}_0^{(h)},\ 1,\ \eta_0^{(h)},\ 0\ )_{\mathbb{D}_0^*}\\ \boldsymbol{c}_0 &:= (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0} = (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta + \chi\widetilde{\tau},\ 0,\ \varphi_0\ )_{\mathbb{D}_0} = (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta',\ 0,\ \varphi_0\ )_{\mathbb{D}_0},\\ &\quad \text{where } c_T := g_T^{\zeta} m^{(b)},\end{aligned}$$

where $\widetilde{r}_0^{(h)} := r_0^{(h)} - \chi, \zeta' := \zeta + \chi\widetilde{\tau} \in \mathbb{F}_q$ are uniformly, independently (from other variables) distributed since $r_0^{(h)}, \chi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, except for the case $\widetilde{\tau} = 0$, i.e., except with probability $1/q$.

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 $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$. Therefore, $\{\mathsf{sk}^{(h)} := (\boldsymbol{k}_0^{(h)*}, \{\boldsymbol{k}_t^{(h)*}\}_{t\in I_{\vec{v}}})\}_{h=1,\ldots,\nu}$ and $\mathsf{ct} := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t\in I_{\vec{x}}}, c_T)$ above can be expressed as keys and ciphertext in two ways, in Game 2-ν-2 over bases $((\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*))$ and in Game 3 over bases $((\mathbb{D}_0, \mathbb{D}_0^*), (\mathbb{B}, \mathbb{B}^*))$. Thus, Game 2-$\nu$-2 can be conceptually changed to Game 3. □

Lemma 13 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_3$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,* $|\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_3}^{\mathsf{P3\text{-}IPE}}(\lambda) + 2/q$.

Proof. In order to prove Lemma 13, we construct a probabilistic machine $\mathcal{B}_3$ against Problem 3-IPE using an adversary $\mathcal{A}$ in a security game (Game 3 or 4) as a black box as follows:

1. $\mathcal{B}_3$ is given a Problem 3-IPE instance, $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*, \boldsymbol{e}_\beta)$.

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 $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$ of Game 3 (and 4), where $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15})$.

4. When a key query is issued for vector $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$, $\mathcal{B}_3$ answers $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t\in I_{\vec{v}}})$ such that

$$\begin{aligned}&\boldsymbol{k}_0^* := (\ -s_0,\ 0,\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}_0^*},\\ &\boldsymbol{k}_t^* := \widetilde{\delta} v_t \boldsymbol{h}^* + (\ \mu_t(t,\ -1),\ 0,\ s_t,\ 0^6,\ \vec{r}_t',\ 0,\ \vec{\eta}_t,\ 0^2\ )_{\mathbb{B}^*}\ \text{ for } t \in I_{\vec{v}},\end{aligned}$$

where $s_t, \mu_t, \eta_0, \widetilde{\delta} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{r}_t', \vec{\eta}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^2, s_0 := \sum_{t\in I_{\vec{v}}} s_t$, and $(\mathbb{B}_0^*, \boldsymbol{h}^*, \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_4, \ldots, \boldsymbol{b}_{15}))$ is a part of the Problem 3-IPE instance.

5. When $\mathcal{B}_3$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and vectors $\vec{x}^{(0)} := \{(t, x_t^{(0)}) \mid t \in I_{\vec{x}}\}, \vec{x}^{(1)} := \{(t, x_t^{(1)}) \mid t \in I_{\vec{x}}\}$ with $I_{\vec{x}} := I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ from $\mathcal{A}$, $\mathcal{B}_3$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ such that

   $$\begin{aligned} &\boldsymbol{c}_0 := (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta',\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, \\ &\boldsymbol{c}_t := x_t^{(b)} \boldsymbol{e}_\beta + (\ \sigma_t(1,\ t),\ 0,\ \widetilde{\omega},\ 0,\ \widetilde{\tau},\ 0^2,\ \vec{z}_t',\ 0^3,\ \vec{\varphi}_t\ )_{\mathbb{B}} \ \text{ for } t \in I_{\vec{x}}, \\ &c_T := g_T^{\zeta} m^{(b)}, \end{aligned}$$

   where $\zeta, \zeta', \widetilde{\omega}, \widetilde{\tau}, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{z}_t', \vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^2, b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\mathbb{B}_0, \boldsymbol{e}_\beta, \mathbb{B})$ is a part of the Problem 3-IPE instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_3$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_3$ outputs $\beta' := 0$. Otherwise, $\mathcal{B}_3$ outputs $\beta' := 1$.

Claim 2 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_3$ given a Problem 3-IPE instance with $\beta \in \{0,1\}$ is the same as that in Game 3 (resp. Game 4) if $\beta = 1$ (resp. $\beta = 0$) with all but negligible probability $1/q$.*

Proof. We will consider the joint distribution of $\boldsymbol{k}_t^{(h)*}$ for $h = 1, \ldots, \nu;\ t \in I_{\vec{v}^{(h)}}$ and $\boldsymbol{c}_t$ for $t \in I_{\vec{x}}$.

The h-th queried key $\{\boldsymbol{k}_t^{(h)*}\}_{h=1,\ldots,\nu}$ for $\vec{v}^{(h)} := \{(t, v_t^{(h)}) \mid t \in I_{\vec{v}^{(h)}}\}$ generated in steps 4 and 6 is

$$\begin{aligned} \boldsymbol{k}_t^{(h)*} &= \widetilde{\delta}^{(h)} v_t^{(h)} \boldsymbol{h}^* + (\ \mu_t^{(h)}(t,\ -1),\ 0,\ s_t^{(h)},\ 0^4,\ \vec{r}_t^{\prime(h)},\ 0,\ \vec{\eta}_t^{(h)},\ 0^2\ )_{\mathbb{B}^*} \\ &= (\ \mu_t^{(h)}(t,\ -1),\ \widetilde{\delta}^{(h)} u v_t^{(h)},\ s_t^{(h)},\ 0^4,\ \vec{r}_t^{\prime(h)} + \widetilde{\delta}^{(h)} v_t^{(h)}(r, 0),\ 0,\ \vec{\eta}_t^{\prime(h)},\ 0^2\ )_{\mathbb{B}^*} \\ &= (\ \mu_t^{(h)}(t,\ -1),\ \delta^{(h)} v_t^{(h)},\ s_t^{(h)},\ 0^4,\ \vec{r}_t,\ 0,\ \vec{\eta}_t^{\prime(h)},\ 0^2\ )_{\mathbb{B}^*} \end{aligned}$$

where $\delta^{(h)} := \widetilde{\delta}^{(h)} u \in \mathbb{F}_q, \vec{r}_t^{(h)} := \vec{r}_t^{\prime(h)} + \widetilde{\delta}^{(h)} v_t^{(h)}(r, 0)$ are uniformly and independently distributed since $\widetilde{\delta}^{(h)} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{r}_t^{\prime(h)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, except for the case $u = 0$, i.e., except with probability $1/q$.

When $\beta = 0$, ciphertext $\boldsymbol{c}_t$ generated in step 5 is

$$\begin{aligned} \boldsymbol{c}_t &= x_t^{(b)} \boldsymbol{e}_0 + (\ \sigma_t(1,\ t),\ 0,\ \widetilde{\omega},\ 0,\ \widetilde{\tau},\ 0^2,\ \vec{z}_t',\ 0^3,\ \vec{\varphi}_t\ )_{\mathbb{B}} \\ &= (\ \sigma_t(1,\ t),\ 0,\ \widetilde{\omega},\ 0,\ \widetilde{\tau},\ 0^2,\ \vec{z}_t' + x_t^{(b)}(z_1,\ z_2),\ 0^3,\ \vec{\varphi}_t\ )_{\mathbb{B}} \\ &= (\ \sigma_t(1,\ t),\ 0,\ \widetilde{\omega},\ 0,\ \widetilde{\tau},\ 0^2,\ \vec{z}_t,\ 0^3,\ \vec{\varphi}_t\ )_{\mathbb{B}} \end{aligned}$$

where $\vec{z}_t := \vec{z}_t' + x_t^{(b)}(z_1,\ z_2) \in \mathbb{F}_q^2$ is uniformly and independently distributed since $\vec{z}_t' \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$.

When $\beta = 1$, ciphertext $\boldsymbol{c}_t$ generated in step 5 is

$$\begin{aligned} \boldsymbol{c}_t &= x_t^{(b)} \boldsymbol{e}_0 + (\ \sigma_t(1,\ t),\ 0,\ \widetilde{\omega},\ 0,\ \widetilde{\tau},\ 0^2,\ \vec{z}_t',\ 0^3,\ \vec{\varphi}_t\ )_{\mathbb{B}} \\ &= (\ \sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ \tau x_t^{(b)},\ \widetilde{\tau},\ 0^2,\ \vec{z}_t' + x_t^{(b)}(z_1,\ z_2),\ 0^3,\ \vec{\varphi}_t\ )_{\mathbb{B}} \\ &= (\ \sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ \tau x_t^{(b)},\ \widetilde{\tau},\ 0^2,\ \vec{z}_t,\ 0^3,\ \vec{\varphi}_t\ )_{\mathbb{B}} \end{aligned}$$

where $\vec{z}_t := \vec{z}_t' + x_t^{(b)}(z_1,\ z_2) \in \mathbb{F}_q^2$ are uniformly and independently distributed since $\vec{z}_t' \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$.

Therefore, the above $\{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}$ and $\boldsymbol{c}_0 := (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta',\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, c_T := g_T^{\zeta} m^{(b)}$ give a challenge ciphertext in Game 3 when $\beta = 1$, and that in Game 4 when $\beta = 0$. □

From Claim 2, $\left|\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)\right| \le \left|\Pr\left[\mathcal{B}_3(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P3\text{-}IPE}}(1^\lambda)\right] - \Pr\left[\mathcal{B}_3(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P3\text{-}IPE}}(1^\lambda)\right]\right| + 2/q = \mathsf{Adv}_{\mathcal{B}_3}^{\mathsf{P3\text{-}IPE}}(\lambda) + 2/q$. This completes the proof of Lemma 13. □

A.3 Proofs of Lemmas 15–21 in Section 5.1.8

Lemma 15 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}1\text{-}1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1\text{-}IPE}}(\lambda) + 1/q$.*

Proof. In order to prove Lemma 15, we construct a probabilistic machine $\mathcal{B}_1$ against Problem 1-IPE using an adversary $\mathcal{A}$ in a security game (Game 0' or 1-1-1) as a black box as follows:

1. $\mathcal{B}_1$ is given a Problem 1-IPE instance, $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,i}\}_{t=1,\ldots,d;i=1,2}, \widetilde{\boldsymbol{e}}_{\beta,1}, \widetilde{\boldsymbol{e}}_2)$.

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

3. At the first step of the game, $\mathcal{B}_1$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$ of Game 0' (and 1-1-1), where $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}}$ is obtained from the Problem 1-IPE instance.

4. When a key query is issued for vector $\vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}}\}$, $\mathcal{B}_1$ answers normal key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ with Eq. (10), that is computed using $\mathbb{B}_0^*, \widehat{\mathbb{B}}^*$ of the Problem 1-IPE instance.

5. When $\mathcal{B}_1$ receives an encryption query with challenge plaintext $m := m^{(0)} = m^{(1)}$ and vectors $\vec{x}^{(0)} := \{(t, x_t^{(0)}) \,|\, t \in I_{\vec{x}}\}, \vec{x}^{(1)} := \{(t, x_t^{(1)}) \,|\, t \in I_{\vec{x}}\}$ with $I_{\vec{x}} := I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ from $\mathcal{A}$, $\mathcal{B}_1$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ such that
$$\begin{aligned}
&\boldsymbol{c}_0 := \boldsymbol{e}_{\beta,0} + \zeta \boldsymbol{b}_{0,3}, \qquad c_T := g_T^{\zeta} m, \\
&\boldsymbol{c}_t := (x_t^{(0)} + x_t^{(1)} \widetilde{\theta})(\widetilde{\boldsymbol{e}}_{\beta,1} + t\widetilde{\boldsymbol{e}}_2) + x_t^{(b)} \boldsymbol{e}_{\beta,t,1} + \xi_1 \boldsymbol{e}_{\beta,t,2} + \xi_2 \boldsymbol{b}_4 \ \text{ for } t \in I_{\vec{x}},
\end{aligned}$$
where $\zeta, \widetilde{\theta}, \xi_1, \xi_2, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\boldsymbol{e}_{\beta,0}, \boldsymbol{b}_{0,3}, \widetilde{\boldsymbol{e}}_{\beta,1}, \widetilde{\boldsymbol{e}}_2, \{\boldsymbol{e}_{\beta,t,i}\}_{t \in I_{\vec{x}};\, i=1,2}, \boldsymbol{b}_4)$ is a part of the Problem 1-IPE instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_1$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_1$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_1$ outputs $\beta' := 0$.

Claim 3 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_1$ given a Problem 1-IPE instance with $\beta \in \{0,1\}$ is the same as that in Game 0' (resp. Game 1-1-1) if $\beta = 0$ (resp. $\beta = 1$ with all but negligible probability $1/q$).*

Proof. We will consider the distribution of $\boldsymbol{c}_t$ for $t \in I_{\vec{x}}$.

When $\beta = 0$, ciphertext $\boldsymbol{c}_t$ generated in step 5 is

$$\begin{aligned}
\boldsymbol{c}_t &= (x_t^{(0)} + x_t^{(1)} \widetilde{\theta})(\widetilde{\boldsymbol{e}}_{0,1} + t\widetilde{\boldsymbol{e}}_2) + x_t^{(b)} \boldsymbol{e}_{0,t,1} + \xi_1 \boldsymbol{e}_{0,t,2} + \xi_2 \boldsymbol{b}_4 \\
&= (x_t^{(0)} + x_t^{(1)} \widetilde{\theta})(\widetilde{\sigma}(\boldsymbol{b}_1 + t\boldsymbol{b}_2)) + (x_t^{(b)} \sigma_{t,1} + \xi_1 \sigma_{t,2})(\boldsymbol{b}_1 + t\boldsymbol{b}_2) \\
&\qquad\qquad + \omega x_t^{(b)} \boldsymbol{b}_3 + (\xi_1 \omega + \xi_2)\boldsymbol{b}_4 + \widetilde{\varphi}_1 \boldsymbol{b}_{14} + \widetilde{\varphi}_2 \boldsymbol{b}_{15} \\
&= ((x_t^{(0)} + x_t^{(1)} \widetilde{\theta})\widetilde{\sigma} + x_t^{(b)} \sigma_{t,1} + \xi_1 \sigma_{t,2})(\boldsymbol{b}_1 + t\boldsymbol{b}_2) + \omega x_t^{(b)} \boldsymbol{b}_3 + (\xi_1 \omega + \xi_2)\boldsymbol{b}_4 + \widetilde{\varphi}_1 \boldsymbol{b}_{14} + \widetilde{\varphi}_2 \boldsymbol{b}_{15} \\
&= (\ \sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ \ 0^9,\ \ \widetilde{\varphi}_1,\ \widetilde{\varphi}_2\ )_{\mathbb{B}}
\end{aligned}$$

where $\sigma_t := (x_t^{(0)} + x_t^{(1)} \widetilde{\theta})\widetilde{\sigma} + x_t^{(b)} \sigma_{t,1} + \xi_1 \sigma_{t,2}, \zeta, \omega, \widetilde{\omega} := \xi_1 \omega + \xi_2, \widetilde{\varphi}_1, \widetilde{\varphi}_2 \in \mathbb{F}_q$ are uniformly and independently distributed.

When $\beta = 1$, ciphertext $\boldsymbol{c}_t$ generated in step 5 is

$$\begin{aligned}\boldsymbol{c}_t &= (x_t^{(0)} + x_t^{(1)}\widetilde{\theta})(\widetilde{\boldsymbol{e}}_{1,1} + t\widetilde{\boldsymbol{e}}_2) + x_t^{(b)}\boldsymbol{e}_{1,t,1} + \xi_1\boldsymbol{e}_{1,t,2} + \xi_2\boldsymbol{b}_4 \\ &= (\ \sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ \ 0^9,\ \widetilde{\varphi}_1,\ \widetilde{\varphi}_2\ )_{\mathbb{B}} \\ &\qquad\qquad +(\ 0^4,\ \tau x_t^{(b)},\ \xi_1\tau,\ 0^2,\ (\tau x_t^{(b)},\ \xi_1\tau)Z_t,\ \theta(x_t^{(0)} + x_t^{(1)}\widetilde{\theta}),\ 0^4\ )_{\mathbb{B}}\end{aligned}$$

where $\sigma_t := (x_t^{(0)} + x_t^{(1)}\widetilde{\theta})\widetilde{\sigma} + x_t^{(b)}\sigma_{t,1} + \xi_1\sigma_{t,2}, \zeta, \omega, \widetilde{\omega} := \xi_1\omega + \xi_2, \tau, \xi_1\tau, \theta, \theta\widetilde{\theta}, \widetilde{\varphi}_1, \widetilde{\varphi}_2 \in \mathbb{F}_q$ are uniformly and independently distributed with all but negligible probability $2/q$, i.e., except when $\tau = 0$ or $\theta = 0$.

Therefore, the above $\boldsymbol{c}_1$ and $\boldsymbol{c}_0 := (\ \widetilde{\omega},\ 0,\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0}, c_T := g_T^{\zeta}m$ give a challenge ciphertext in Game 0' when $\beta = 0$, and that in Game 1-1-1 when $\beta = 1$ with all but negligible probability $1/q$. □

From Claim 3, $\left|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}1\text{-}1)}(\lambda)\right| \le \left|\mathsf{Pr}\left[\mathcal{B}_1(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P1\text{-}IPE}}(1^\lambda)\right] - \mathsf{Pr}\left[\mathcal{B}_1(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P1\text{-}IPE}}(1^\lambda)\right]\right| + 1/q = \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1\text{-}IPE}}(\lambda) + 1/q$. This completes the proof of Lemma 15. □

Lemma 16 *Let $h \ge 2$. For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}(h-1)\text{-}5)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}1)}(\lambda)| \le 1/q$.*

Proof. Since matrices $\{Z_t\}_{t \in I_{\vec{x}}}$ only appear in coefficients in $\{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}$ in Games 1-$(h-1)$-5 and 1-h-1, all coefficients $\{(\tau_0 x_t^{(0)} + \tau_1 x_t^{(1)}, \widetilde{\tau})Z_t\}_{t \in I_{\vec{x}}}$ in Game 1-$(h-1)$-5 and $\{(\tau x_t^{(b)}, \widetilde{\tau})Z_t\}_{t \in I_{\vec{x}}}$ in Game 1-h-1 are uniformly and independently distributed in $\mathbb{F}_q^2$.

To finish the proof of Lemma 16, we will show distribution of public parameters, queried keys, and challenge ciphertext, $(\mathsf{param}, \widehat{\mathbb{B}}, \{\mathsf{sk}^{(h)} := (\boldsymbol{k}_0^{(h)*}, \{\boldsymbol{k}_t^{(h)*}\}_{t \in I_{\vec{v}^{(h)}}})\}_{h=1,\dots,\nu}, \mathsf{ct} := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T))$, in Game 1-$(h-1)$-5 and that in Game 1-$h$-1 are equivalent. For that purpose, we define new dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ (in Game 1-h-1) as follows:

We generate $\chi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and set

$$\begin{aligned}&\boldsymbol{d}_{11} := \boldsymbol{b}_{11} - \chi\boldsymbol{b}_5, \quad \boldsymbol{d}_5^* := \boldsymbol{b}_5^* + \chi\boldsymbol{b}_{11}^* \\ &\mathbb{D} := (\boldsymbol{b}_1, \dots, \boldsymbol{b}_{10}, \boldsymbol{d}_{11}, \boldsymbol{b}_{12}, \dots, \boldsymbol{b}_{15}), \quad \mathbb{D}^* := (\boldsymbol{b}_1^*, \dots, \boldsymbol{b}_4^*, \boldsymbol{d}_5^*, \boldsymbol{b}_6^*, \dots, \boldsymbol{b}_{15}^*).\end{aligned}$$

We then easily verify that $\mathbb{D}$ and $\mathbb{D}^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}$ and $\mathbb{B}^*$.

Parts of queried keys and challenge ciphertext, $\{\boldsymbol{k}_t^{(h)*}\}$ and $\{\boldsymbol{c}_t\}$, in Game 1-h-1 are expressed over bases $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ as

$$\left.\begin{aligned}\boldsymbol{k}_t^{(h)*} &:= (\mu_t^{(h)}(t,\ -1),\ \delta^{(h)}v_t^{(h)},\ s_t^{(h)},\ 0, \dots \qquad ,\ \vec{\eta}_t^{(h)},\ 0^2)_{\mathbb{B}^*} \\ &= (\mu_t^{(h)}(t,\ -1),\ \delta^{(h)}v_t^{(h)},\ s_t^{(h)},\ 0, \dots \qquad ,\ \vec{\eta}_t^{(h)},\ 0^2)_{\mathbb{D}^*} \\ \boldsymbol{c}_t &:= (\sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ \tau x_t^{(b)},\ \widetilde{\tau},\ 0^2,\ (\tau x_t^{(b)},\ \widetilde{\tau}) \cdot Z_t,\ \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},\ 0^2,\ \vec{\varphi}_t)_{\mathbb{B}} \\ &= (\sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ \tau x_t^{(b)} + \chi(\theta_0 x_t^{(0)} + \theta_1 x_t^{(1)}),\ \widetilde{\tau}, \dots, \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},\ 0^2,\ \vec{\varphi}_t)_{\mathbb{D}} \\ &= (\sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ \tau_0 x_t^{(0)} + \tau_1 x_t^{(1)},\ \widetilde{\tau}, \dots, \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},\ 0^2,\ \vec{\varphi}_t)_{\mathbb{D}}\end{aligned}\right\} \quad (25)$$

where $\tau_b := \tau + \chi\theta_b,\ \tau_{1-b} := \chi\theta_{1-b} \in \mathbb{F}_q$ are uniformly, independently (from other variables) distributed since $\tau, \chi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, except for the case $\theta_{1-b} = 0$, i.e., except with probability $1/q$.

In the light of the adversary's view, both $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ are consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$. Therefore, $\{\mathsf{sk}^{(h)} := (\boldsymbol{k}_0^{(h)*}, \{\boldsymbol{k}_t^{(h)*}\}_{t \in I_{\vec{v}^{(h)}}})\}_{h=1,\dots,\nu}$ and $\mathsf{ct} := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ above can be expressed as keys and ciphertext in two ways, in Game 1-h-1 over bases $(\mathbb{B}, \mathbb{B}^*)$ and in Game 1-$(h-1)$-5 over bases $(\mathbb{D}, \mathbb{D}^*)$. Thus, Game 1-$(h-1)$-5 can be conceptually changed to Game 1-h-1.

Therefore, the view of adversary $\mathcal{A}$ in the Game 1-$(h-1)$-5 is the same as that in Game 1-h-1. This completes the proof of Lemma 16. □

Lemma 17 *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,* $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}2)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2\text{-}IPE}}(\lambda) + 2/q$*, where* $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.

Lemma 17 is proven in a similar manner to Lemma 10.

Lemma 18 *For any adversary $\mathcal{A}$, for any security parameter λ,* $\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}2)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}3)}(\lambda)$.

Proof. It is clear that the distribution of the public-key and the ι-th key query's answer for $\iota \neq h$ in Game 1-h-2 and Game 1-h-3 are exactly the same. Therefore, to prove this lemma we will show that the joint distribution of the h-th key query's answer and the challenge ciphertext in Game 1-h-2 and Game 1-h-3 are equivalent.

Let $\vec{r}_t := (\pi v_t, a_t) \cdot U_t$, which is coefficients of the t-th key element $\boldsymbol{k}_t^*$ for $t \in I_{\vec{v}}$, and $\vec{w}_t^{(b)} := (\tau_b x_t^{(b)}, \widetilde{\tau}) \cdot Z_t$, which is coefficients of the t-th ciphertext element $\boldsymbol{c}_t$ for $t \in I_{\vec{v}}$ in Game 1-h-2. In Game 1-h-3, the ciphertext coefficients are given by $\vec{w}_t^{\mathsf{unbias}} := (\tau_0 x_t^{(0)} + \tau_1 x_t^{(1)}, \widetilde{\tau}) \cdot Z_t$. Let $n := \sharp(I_{\vec{v}})$, $n' := \sharp(I_{\vec{x}})$, and n elements of $I_{\vec{v}}$ are expressed by $\{t_1, \ldots, t_n \,|\, 1 \leq t_1 \leq t_2 \leq \cdots \leq t_n \leq d\}$.

We will show that $V^{(b)} := (a_0, \{\vec{r}_t\}_{t \in I_{\vec{v}}}, \{\vec{w}_t^{(b)}\}_{t \in I_{\vec{x}}}) \in \mathbb{F}_q \times \left(\mathbb{F}_q^2\right)^n \times \left(\mathbb{F}_q^2\right)^{n'}$ and $V^{\mathsf{unbias}} := (a_0, \{\vec{r}_t\}_{t \in I_{\vec{v}}}, \{\vec{w}_t^{\mathsf{unbias}}\}_{t \in I_{\vec{x}}})$ have the same distribution in $\mathcal{A}$'s view.

When $I_{\vec{v}} \not\subseteq I_{\vec{x}}$, both $V^{(b)}$ and V^{unbias} are uniformly and independently distributed from the other variables in $\mathcal{A}$'s view as in the proof of Lemma 11.

Therefore, we will consider the case when $I_{\vec{v}} \subseteq I_{\vec{x}}$, below. Then, we first note that $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = R(\vec{v}, \tau_0 \vec{x}^{(0)} + \tau_1 \vec{x}^{(1)})$ with all but negligible probability. Therefore, if $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = 0$, we can show that both $V^{(b)}$ and V^{unbias} are uniformly and independently distributed from the other variables in $\mathcal{A}$'s view from the proof of Lemma 11, too.

When $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = 1$, i.e., $\sum_{t \in I_{\vec{v}}} v_t x_t = \sum_{i=1}^n v_{t_i} x_{t_i} = 0$, as in Eq. (24), since

$$\begin{pmatrix} \vec{r}_{t_1} \cdot \vec{w}_{t_1}^{(b)} \\ \vdots \\ \vec{r}_{t_n} \cdot \vec{w}_{t_n}^{(b)} \end{pmatrix} = \widetilde{M} \cdot \begin{pmatrix} \pi \\ a_{t_1} \\ \vdots \\ a_{t_n} \end{pmatrix}, \quad \text{where } \widetilde{M} := \begin{pmatrix} \tau v_{t_1} x_{t_1}^{(b)} & \widetilde{\tau} & & \\ \vdots & & \ddots & \\ \tau v_{t_n} x_{t_n}^{(b)} & & & \widetilde{\tau} \end{pmatrix}$$

and the rank of $\widetilde{M}$ is n with all but negligible probability $1/q$, i.e., except when $\widetilde{\tau} = 0$, inner product values $\{p_t^{(b)} := \vec{r}_t \cdot \vec{w}_t^{(b)}\}_{t \in I_{\vec{v}}}$ are uniformly distributed. And, among $\{p_t^{(b)}\}_{t \in I_{\vec{v}}}$ and a_0, a relation $\sum_{t \in I_{\vec{v}}} p_t^{(b)} = \widetilde{\tau} a_0$ holds. Similarly, $\{p_t^{\mathsf{unbias}} := \vec{r}_t \cdot \vec{w}_t^{\mathsf{unbias}}\}_{t \in I_{\vec{v}}}$ are uniformly distributed, and among $\{p_t^{\mathsf{unbias}}\}_{t \in I_{\vec{v}}}$ and a_0, the relation $\sum_{t \in I_{\vec{v}}} p_t^{\mathsf{unbias}} = \widetilde{\tau} a_0$ also holds. This shows that $(a_0, \{p_t^{(b)}\}_{t \in I_{\vec{v}}})$ and $(a_0, \{p_t^{\mathsf{unbias}}\}_{t \in I_{\vec{v}}})$ have the same distribution.

Therefore, from Lemma 8, $V^{(b)}$ and V^{unbias} have the same joint distribution in this case, too.

To finish the proof of Lemma 18, we will show distribution of public parameters, queried keys, and challenge ciphertext, $(\mathsf{param}, \widehat{\mathbb{B}}, \{\mathsf{sk}^{(h)} := (\boldsymbol{k}_0^{(h)*}, \{\boldsymbol{k}_t^{(h)*}\}_{t \in I_{\vec{v}^{(h)}}})\}_{h=1,\ldots,\nu}, \mathsf{ct} := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T))$, in Game 1-$h$-2 and that in Game 1-$h$-3 are equivalent. For that purpose, we define new dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ as follows:

We generate $\chi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and set

$$\boldsymbol{d}_{11} := \boldsymbol{b}_{11} - \chi \boldsymbol{b}_5, \quad \boldsymbol{d}^*_5 := \boldsymbol{b}^*_5 + \chi \boldsymbol{b}^*_{11}$$
$$\mathbb{D} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{10}, \boldsymbol{d}_{11}, \boldsymbol{b}_{12}, \ldots, \boldsymbol{b}_{15}), \quad \mathbb{D}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_4, \boldsymbol{d}^*_5, \boldsymbol{b}^*_6, \ldots, \boldsymbol{b}^*_{15}).$$

We then easily verify that $\mathbb{D}$ and $\mathbb{D}^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}$ and $\mathbb{B}^*$.

Parts of queried keys and challenge ciphertext, $\{\boldsymbol{k}^{(h)*}_t\}$ and $\{\boldsymbol{c}_t\}$, in Game 1-h-2 are expressed over bases $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ as in Eq. (25) except for the case $\theta_{1-b} = 0$, i.e., except with probability $1/q$.

In the light of the adversary's view, both $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ are consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$. Therefore, $\{\mathsf{sk}^{(h)} := (\boldsymbol{k}^{(h)*}_0, \{\boldsymbol{k}^{(h)*}_t\}_{t \in I_{\vec{v}^{(h)}}})\}_{h=1,\ldots,\nu}$ and $\mathsf{ct} := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ above can be expressed as keys and ciphertext in two ways, in Game 1-h-2 over bases $(\mathbb{B}, \mathbb{B}^*)$ and in Game 1-h-3 over bases $(\mathbb{D}, \mathbb{D}^*)$. Thus, Game 1-$h$-2 can be conceptually changed to Game 1-h-3.

Therefore, the view of adversary $\mathcal{A}$ in the Game 1-h-2 is the same as that in Game 1-h-3. This completes the proof of Lemma 18. □

Lemma 19 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_3$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P4\text{-}IPE}}_{\mathcal{B}_{3\text{-}h}}(\lambda) + 4/q$, where $\mathcal{B}_{3\text{-}h}(\cdot) := \mathcal{B}_3(h, \cdot)$.*

Proof. In order to prove Lemma 19, we construct a probabilistic machine $\mathcal{B}_3$ against Problem 4-IPE using an adversary $\mathcal{A}$ in a security game (Game 1-h-3 or 1-h-4) as a black box as follows:

1. $\mathcal{B}_{2\text{-}2}$ is given a Problem 4-IPE instance, $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*_0, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=1,2})$.

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 $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}')$ of Game 1-h-3 (and 1-h-4), where $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}}' := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15})$.

4. When the ι-th key query is issued for vector $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$, $\mathcal{B}_3$ answers as follows:

   (a) When $1 \leq \iota \leq h-1$, $\mathcal{B}_3$ answers final key $(\boldsymbol{k}^*_0, \ldots, \boldsymbol{k}^*_n)$ with Eq. (16), that is computed using $\widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}^*$ of the Problem 4-IPE instance.

   (b) When $\iota = h$, $\mathcal{B}_3$ calculates $(\boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{t \in I_{\vec{v}}})$ using $(\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}^*_3, \boldsymbol{b}^*_4, \boldsymbol{h}^*_0, \{\boldsymbol{h}^*_{\beta,t,i}\}_{t=1,\ldots,d;i=1,2})$ of the Problem 4-IPE instance as follows:

$$\delta \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad s_t, g_t, \widetilde{\mu}_t, \widetilde{\eta}_{t,1}, \widetilde{\eta}_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q \text{ for } t \in I_{\vec{v}},$$
$$s_0 := \textstyle\sum_{t=1}^n s_t, \; g_0 := \sum_{t=1}^n g_t, \quad \boldsymbol{k}^*_0 := -(s_0 \boldsymbol{b}^*_{0,1} + g_0 \boldsymbol{h}^*_0) + \boldsymbol{b}^*_{0,3},$$
$$\boldsymbol{k}^*_t := v_t(\delta \boldsymbol{b}^*_3 + \boldsymbol{h}^*_{\beta,t,1}) + s_t \boldsymbol{b}^*_4 + g_t \boldsymbol{h}^*_{\beta,t,2} + \widetilde{\mu}_t(t\boldsymbol{b}^*_1 - \boldsymbol{b}^*_2) + \widetilde{\eta}_{t,1} \boldsymbol{b}^*_{12} + \widetilde{\eta}_{t,2} \boldsymbol{b}^*_{13} \text{ for } t \in I_{\vec{v}}.$$

   (c) When $\iota \geq h+1$, $\mathcal{B}_3$ answers normal key $(\boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{I_{\vec{v}}})$ with Eq. (10), that is computed using $\widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}^*$ of the Problem 4-IPE instance.

5. When $\mathcal{B}_3$ receives an encryption query with challenge plaintexts $m := m^{(0)} = m^{(1)}$ and $\vec{x}^{(0)} := \{(t, x_t^{(0)}) \,|\, t \in I_{\vec{x}}\}, \vec{x}^{(1)} := \{(t, x_t^{(1)}) \,|\, t \in I_{\vec{x}}\}$ with $I_{\vec{x}} := I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ from $\mathcal{A}$, $\mathcal{B}_3$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ such that

$$\boldsymbol{c}_0 := \widetilde{\omega}\boldsymbol{b}_{0,1} + \xi\boldsymbol{e}_0 + \zeta\boldsymbol{b}_{0,3}, \quad c_T := g_T^{\zeta} m,$$
$$\boldsymbol{c}_t := \omega x_t^{(b)}\boldsymbol{b}_3 + \widetilde{\omega}\boldsymbol{b}_4 + x_t^{(b)}\boldsymbol{e}_{t,1} + \xi\boldsymbol{e}_{t,2} + (\theta_0 x_t^{(0)} + \theta_1 x_t^{(1)})\boldsymbol{b}_{13},$$

where $\omega, \widetilde{\omega}, \zeta, \xi, \theta_0, \theta_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\{\boldsymbol{b}_{0,i}\}_{i=1,3}, \boldsymbol{e}_0, \{\boldsymbol{b}_i\}_{i=3,4,13}, \{\boldsymbol{e}_{t,i}\}_{t \in I_{\vec{x}};\ i=1,2})$ is a part of the Problem 4-IPE instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_3$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_3$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_3$ outputs $\beta' := 0$.

Claim 4 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_3$ given a Problem 4-IPE instance with $\beta \in \{0,1\}$ is the same as that in Game 1-h-3 (resp. Game 1-h-4) if $\beta = 0$ (resp. $\beta = 1$) except with probability $2/q$.*

Proof. We will consider the joint distribution of the h-th queried key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ and challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}})$ (and c_T).

The h-th queried key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ for $\vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}}\}$ generated in steps 4 and 6 is

$$\begin{aligned}
&\boldsymbol{k}_0^* := -(s_0\boldsymbol{b}_{0,1}^* + g_0\boldsymbol{h}_0^*) + \boldsymbol{b}_{0,3}^* = (\ -s_0,\ -a_0,\ 1,\ \widetilde{\eta}_0,\ 0\ )_{\mathbb{B}_0^*}, \quad \text{where } a_0 = g_0\rho, \\
&\text{when } \beta = 0, \\
&\quad \boldsymbol{k}_t^* := v_t(\delta\boldsymbol{b}_3^* + \boldsymbol{h}_{t,1}^*) + s_t\boldsymbol{b}_4^* + g_t\boldsymbol{h}_{t,2}^* + \widetilde{\mu}_t(t\boldsymbol{b}_1^* - \boldsymbol{b}_2^*) + \widetilde{\eta}_{t,1}\boldsymbol{b}_{12}^* + \widetilde{\eta}_{t,2}\boldsymbol{b}_{13}^* \\
&\qquad = (\ \widetilde{\widetilde{\mu}}_t(t,\ -1),\ \delta v_t,\ s_t,\quad 0^4,\quad (\rho v_t,\ a_t)U_t,\ 0,\ \widetilde{\widetilde{\eta}}_{t,1}, \widetilde{\widetilde{\eta}}_{t,2},\ 0^2\ )_{\mathbb{B}^*}, \\
&\text{when } \beta = 1, \\
&\quad \boldsymbol{k}_t^* := v_t(\delta\boldsymbol{b}_3^* + \boldsymbol{h}_{0,t,1}^*) + s_t\boldsymbol{b}_4^* + g_t\boldsymbol{h}_{0,t,2}^* + \widetilde{\mu}_t(t\boldsymbol{b}_1^* - \boldsymbol{b}_2^*) + \widetilde{\eta}_{t,1}\boldsymbol{b}_{12}^* + \widetilde{\eta}_{t,2}\boldsymbol{b}_{13}^* \\
&\qquad = (\ \widetilde{\widetilde{\mu}}_t(t,\ -1),\ \delta v_t,\ s_t,\ \rho v_t,\ a_t,\quad 0^4,\quad 0,\ \widetilde{\widetilde{\eta}}_{t,1}, \widetilde{\widetilde{\eta}}_{t,2},\ 0^2\ )_{\mathbb{B}^*},
\end{aligned}$$

where $a_t = g_t\rho, \widetilde{\widetilde{\mu}}_t := v_t\mu_{t,1} + g_t\mu_{t,2} + \widetilde{\mu}, \widetilde{\widetilde{\eta}}_{t,i} := v_t\eta_{t,1,i} + g_t\eta_{t,2,i} + \widetilde{\eta}_{t,i}$ for $i = 1,2$, and $\rho, \mu_{t,i}, \eta_{t,i,j}, U_t$ are defined in Problem 4-IPE. Note that $a_0 = \sum_{t \in I_{\vec{v}}} a_t$, and $a_t, \widetilde{\widetilde{\mu}}_t$ are uniformly and independently distributed since $g_t, \widetilde{\mu}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q$ except for the case $\rho = 0$, i.e., except with probability $1/q$.

$\boldsymbol{c}_0$ of the challenge ciphertext is given as

$$\boldsymbol{c}_0 := \widetilde{\omega}\boldsymbol{b}_{0,1} + \xi\boldsymbol{e}_0 + \zeta\boldsymbol{b}_{0,3} = (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta,\ 0,\ \widetilde{\varphi}_0\ ),$$

where $\widetilde{\tau} := \xi\tau$, which is uniformly and independently distributed since $\xi \xleftarrow{\mathsf{U}} \mathbb{F}_q$ except for the case $\tau = 0$, i.e., except with probability $1/q$.

The challenge ciphertext in the above simulation is given as:

$$\begin{aligned}
\boldsymbol{c}_t &:= \omega x_t^{(b)}\boldsymbol{b}_3 + \widetilde{\omega}\boldsymbol{b}_4 + x_t^{(b)}\boldsymbol{e}_{0,t,1} + \xi\boldsymbol{e}_{0,t,2} + (\theta_0 x_t^{(0)} + \theta_1 x_t^{(1)})\boldsymbol{b}_{11} \\
&= (\ \widetilde{\sigma}_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ (\tau x_t^{(b)},\ \widetilde{\tau}),\ 0^2,\ (\tau x_t^{(b)},\ \widetilde{\tau})Z_t,\ \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},\ 0^2,\ \widetilde{\varphi}_{t,1}, \widetilde{\varphi}_{t,2}\ )_{\mathbb{B}}
\end{aligned}$$

where $\widetilde{\sigma}_t := x_t^{(b)}\sigma_{t,1} + \xi\sigma_{t,2}, \widetilde{\varphi}_{t,j} := x_t^{(b)}\varphi_{t,1,j} + \xi\varphi_{t,2,j}$ for $j = 1,2$, and $\tau, \{\sigma_{t,j}, \varphi_{t,i,j}, Z_t\}_{t \in I_{\vec{x}};\ i,j=1,2}$ are defined in Problem 4-IPE. Note that $\widetilde{\sigma}_t, \widetilde{\varphi}_{t,j}$ are uniformly and independently distributed since $\sigma_{t,2}, \varphi_{t,2,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ except for the case $\xi = 0$, i.e., except with probability $1/q$.

Therefore, when $\beta = 0$ (resp. $\beta = 1$), the distribution by $\mathcal{B}_{2\text{-}2}$'s simulation is equivalent to that in Game 1-h-3 (resp. Game 1-h-4) except with probability $2/q$. □

This completes the proof of Lemma 19. □

Lemma 20 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_4$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}h\text{-}5)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{4\text{-}h}}^{\mathsf{P5\text{-}IPE}}(\lambda)$, where $\mathcal{B}_{4\text{-}h}(\cdot) := \mathcal{B}_4(h, \cdot)$.*

Proof. In order to prove Lemma 20, we construct a probabilistic machine $\mathcal{B}_4$ against Problem 5-IPE using an adversary $\mathcal{A}$ in a security game (Game 1-h-4 or 1-h-5) as a black box as follows:

1. $\mathcal{B}_4$ is given a Problem 5-IPE instance, $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{h}_\beta^*, \{\boldsymbol{e}_j\}_{j=0,1})$.

2. $\mathcal{B}_4$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. At the first step of the game, $\mathcal{B}_4$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}')$ of Game 1-h-4 (and 1-h-5), where $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}}' := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15})$.

4. When the ι-th key query is issued for vector $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$, $\mathcal{B}_4$ answers as follows:

   (a) When $1 \leq \iota \leq h - 1$, $\mathcal{B}_4$ answers final key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ with Eq. (16), that is computed using $\mathbb{B}_0^*, \mathbb{B}^*$ of the Problem 5-IPE instance.

   (b) When $\iota = h$, $\mathcal{B}_4$ calculates $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ using $(\mathbb{B}_0^*, \mathbb{B}^*, \boldsymbol{h}_\beta^*)$ of the Problem 5-IPE instance as follows:

   $$\begin{aligned} &\delta, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \mu_t, s_t, a_t \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \vec{u}_t, \vec{\eta}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^2 \text{ for } t \in I_{\vec{v}}, \\ &s_0 := \textstyle\sum_{t \in I_{\vec{v}}} s_t, \ a_0 := \textstyle\sum_{t \in I_{\vec{v}}} a_t, \quad \boldsymbol{k}_0^* := (\ -s_0, \ -a_0, \ 1, \ \eta_0, \ 0\ )_{\mathbb{B}_0^*}, \\ &\boldsymbol{k}_t^* := v_t \boldsymbol{h}_\beta + (\ \mu_t(t, \ -1), \ \delta v_t, \ s_t, \ 0, \ a_t, \ 0^5, \ \vec{\eta}_t, \ 0^2\ )_{\mathbb{B}^*} \text{ for } t \in I_{\vec{v}}. \end{aligned}$$

   (c) When $\iota \geq h+1$, $\mathcal{B}_4$ answers normal key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}})$ with Eq. (10), that is computed using $\mathbb{B}_0^*, \mathbb{B}^*$ of the Problem 5-IPE instance.

5. When $\mathcal{B}_4$ receives an encryption query with challenge plaintexts $m := m^{(0)} = m^{(1)}$ and $\vec{x}^{(0)} := \{(t, x_t^{(0)}) \mid t \in I_{\vec{x}}\}, \vec{x}^{(1)} := \{(t, x_t^{(1)}) \mid t \in I_{\vec{x}}\}$ with $I_{\vec{x}} := I_{\vec{x}^{(0)}} = I_{\vec{x}^{(1)}}$ from $\mathcal{A}$, $\mathcal{B}_4$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ such that

   $$\begin{aligned} &\omega, \widetilde{\omega}, \widetilde{\tau}, \zeta, \varphi_0, \sigma_t \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^2 \text{ for } t \in I_{\vec{x}}, \\ &\boldsymbol{c}_0 := (\ \widetilde{\omega}, \ \widetilde{\tau}, \ \zeta, \ 0, \ \varphi_0\ )_{\mathbb{B}_0}, \qquad c_T := g_T^\zeta m, \\ &\boldsymbol{c}_t := x_t^{(0)} \boldsymbol{e}_0 + x_t^{(1)} \boldsymbol{e}_1 + (\ \sigma_t(1, \ t), \ \omega x_t^{(b)}, \ \widetilde{\omega}, \ 0, \ \widetilde{\tau}, \ 0^7, \ \vec{\varphi}_t\ )_{\mathbb{B}} \text{ for } t \in I_{\vec{x}}, \end{aligned}$$

   where $b \xleftarrow{\mathsf{U}} \{0, 1\}$, and $(\mathbb{B}_0, \widehat{\mathbb{B}}, \{\boldsymbol{e}_i\}_{i=0,1})$ is a part of the Problem 5-IPE instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_4$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_4$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_4$ outputs $\beta' := 0$.

Claim 5 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_4$ given a Problem 5-IPE instance with $\beta \in \{0, 1\}$ is the same as that in Game 1-h-4 (resp. Game 1-h-5) if $\beta = 0$ (resp. $\beta = 1$) except with probability $1/q$ (resp. $1/q$).*

Proof. We will consider the joint distribution of the h-th queried key $(\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t\in I_{\vec{v}}})$ and challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t\in I_{\vec{x}}})$ (and c_T).

The challenge ciphertext in the above simulation is given as:

$$\begin{aligned}
\boldsymbol{c}_0 &:= (\ \widetilde{\omega},\ \widetilde{\tau},\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0},\\
\boldsymbol{c}_t &:= x_t^{(0)}\boldsymbol{e}_0 + x_t^{(1)}\boldsymbol{e}_1 + (\ \sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ 0,\ \widetilde{\tau},\ 0^7,\ \vec{\varphi}_t\ )_{\mathbb{B}}\\
&:= (\ \sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ \tau_0 x_t^{(0)} + \tau_1 x_t^{(1)},\ \widetilde{\tau},\ 0^6,\ \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},\ \vec{\varphi}_t'\ )_{\mathbb{B}} \text{ for } t \in I_{\vec{x}},
\end{aligned}$$

where $\{\tau_i, \theta_i\}_{i=0,1}$ are defined in Problem 5-IPE.

$\boldsymbol{k}_0^*$ of the h-th queried key for $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$ generated in steps 4 and 6 is

$$\boldsymbol{k}_0^* \ := \ (\ -s_0,\ -a_0,\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}_0^*},$$

When $\beta = 0$, the h-th queried key $\{\boldsymbol{k}_t^*\}_{t\in I_{\vec{v}}}$ for $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$ is

$$\begin{aligned}
\boldsymbol{k}_t^* &:= v_t \boldsymbol{h}_0 + (\ \mu_t(t,\ -1),\ \delta v_t,\ s_t,\ 0,\ a_t,\ 0^5,\ \vec{\eta}_t,\ 0^2\ )_{\mathbb{B}^*}\\
&= (\ \mu_t(t,\ -1),\ \delta v_t,\ s_t,\ \rho v_t,\ a_t,\ 0^5,\ \vec{\eta}_t,\ 0^2\ )_{\mathbb{B}^*} \text{ for } t \in I_{\vec{v}}.
\end{aligned}$$

When $\beta = 1$, the h-th queried key $\{\boldsymbol{k}_t^*\}_{t\in I_{\vec{v}}}$ for $\vec{v} := \{(t, v_t) \mid t \in I_{\vec{v}}\}$ is

$$\begin{aligned}
\boldsymbol{k}_t^* &:= v_t \boldsymbol{h}_1 + (\ \mu_t(t,\ -1),\ \delta v_t,\ s_t,\ 0,\ a_t,\ 0^5,\ \vec{\eta}_t,\ 0^2\ )_{\mathbb{B}^*}\\
&= (\ \mu_t(t,\ -1),\ \delta v_t,\ s_t,\ 0,\ a_t,\ 0^4,\ \rho v_t,\ \vec{\eta}_t,\ 0^2\ )_{\mathbb{B}^*} \text{ for } t \in I_{\vec{v}}.
\end{aligned}$$

Therefore, when $\beta = 0$ (resp. $\beta = 1$), the distribution by $\mathcal{B}_4$'s simulation is equivalent to that in Game 1-h-4 (resp. Game 1-h-5). □

This completes the proof of Lemma 20. □

Lemma 21 *For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\nu\text{-}5)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda)| \leq 1/q$.*

Proof. To prove Lemma 21, we will show distribution of public parameters, queried keys, and challenge ciphertext, $(\mathsf{param}, \widehat{\mathbb{B}}, \{\mathsf{sk}^{(h)} := \{(\boldsymbol{k}_0^{(h)*}, \{\boldsymbol{k}_t^{(h)*}\}_{t\in I_{\vec{v}^{(h)}}})\}_{h=1,\ldots,\nu}, \mathsf{ct} := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t\in I_{\vec{x}}}, c_T))$, in Game 1-$\nu$-5 and that in Game 2 are equivalent. For that purpose, we define new dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ as follows:

We generate $\chi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and set

$$\begin{aligned}
&\boldsymbol{d}_{11} := \boldsymbol{b}_{11} - \chi \boldsymbol{b}_3, \quad \boldsymbol{d}_3^* := \boldsymbol{b}_3^* + \chi \boldsymbol{b}_{11}^*\\
&\mathbb{D} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{10}, \boldsymbol{d}_{11}, \boldsymbol{b}_{12}, \ldots, \boldsymbol{b}_{15}), \quad \mathbb{D}^* := (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \boldsymbol{d}_3^*, \boldsymbol{b}_4^*, \ldots, \boldsymbol{b}_{15}^*).
\end{aligned}$$

We then easily verify that $\mathbb{D}$ and $\mathbb{D}^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}$ and $\mathbb{B}^*$.

Parts of queried keys and challenge ciphertext, $\{\{\boldsymbol{k}_t^{(h)*}\}_{t\in I_{\vec{v}^{(h)}}}\}_{h=1,\ldots,\nu}, \{\boldsymbol{c}_t\}_{t\in I_{\vec{x}}}$, in Game 1-$\nu$-5 are expressed over bases $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ as

$$\begin{aligned}
\boldsymbol{k}_t^{(h)*} &:= (\ \mu_t^{(h)}(t,\ -1),\ \delta^{(h)} v_t^{(h)},\ s_t^{(h)},\ 0,\ a_t^{(h)},\ 0^4,\ \widetilde{\pi}^{(h)} v_t^{(h)},\ \vec{\eta}_t^{(h)},\ 0^2\ )_{\mathbb{B}^*}\\
&= (\ \mu_t^{(h)}(t,\ -1),\ \delta^{(h)} v_t^{(h)},\ s_t^{(h)},\ 0,\ a_t^{(h)},\ 0^4,\ \widetilde{\pi}^{(h)} v_t^{(h)} - \chi \delta^{(h)} v_t^{(h)},\ \vec{\eta}_t^{(h)},\ 0^2\ )_{\mathbb{D}^*}\\
&= (\ \mu_t^{(h)}(t,\ -1),\ \delta^{(h)} v_t^{(h)},\ s_t^{(h)},\ 0,\ a_t^{(h)},\ 0^4,\ \xi^{(h)} v_t^{(h)},\ \vec{\eta}_t^{(h)},\ 0^2\ )_{\mathbb{D}^*},\\
\boldsymbol{c}_t &:= (\ \sigma_t(1,\ t),\ \omega x_t^{(b)},\ \widetilde{\omega},\ 0^6,\ \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},\ 0^2,\ \vec{\varphi}_t\ )_{\mathbb{B}}\\
&= (\ \sigma_t(1,\ t),\ \omega x_t^{(b)} + \chi(\theta_0 x_t^{(0)} + \theta_1 x_t^{(1)}),\ \widetilde{\omega},\ 0^6,\ \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},\ 0^2,\ \vec{\varphi}_t\ )_{\mathbb{D}}\\
&= (\ \sigma_t(1,\ t),\ \omega_0 x_t^{(0)} + \omega_1 x_t^{(1)},\ \widetilde{\omega},\ 0^6,\ \theta_0 x_t^{(0)} + \theta_1 x_t^{(1)},\ 0^2,\ \vec{\varphi}_t\ )_{\mathbb{D}}
\end{aligned}$$

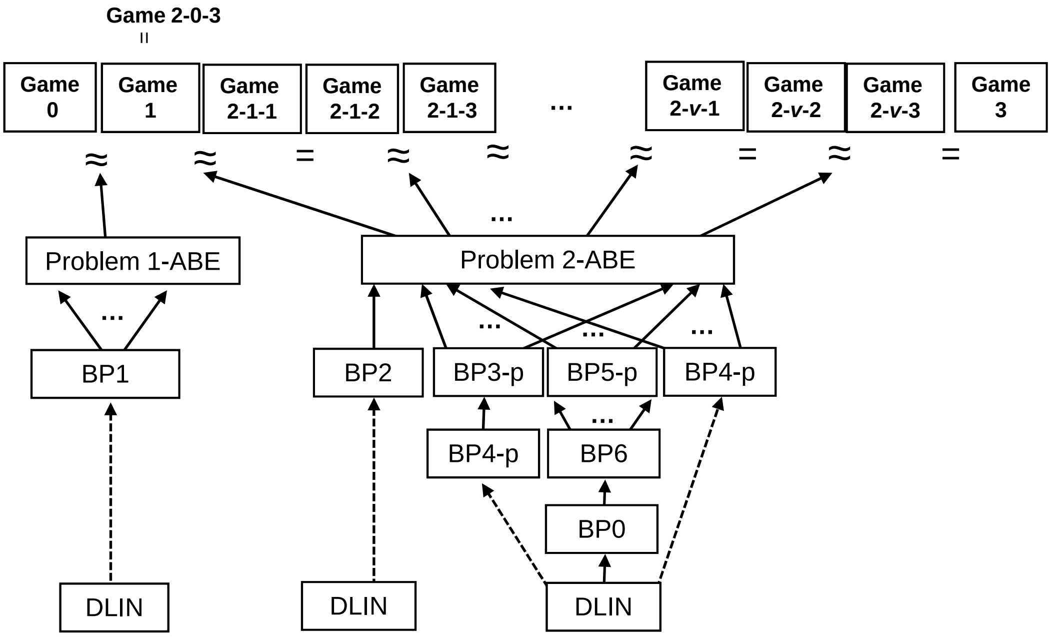


Figure 2: Structure of Hierarchical Reductions for the Proof of Theorem 4

where $\omega_b := \omega + \chi\theta_b$, $\omega_{1-b} := \chi\theta_{1-b}$ and $\xi^{(h)} := \widetilde{\pi}^{(h)} - \chi\delta^{(h)} \in \mathbb{F}_q$ are uniformly, independently (from other variables) distributed since $\omega, \chi, \widetilde{\pi}^{(h)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, except for the case $\theta_{1-b} = 0$, i.e., except with probability $1/q$.

In the light of the adversary's view, both $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ are consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$. Therefore, $\{\mathsf{sk}^{(h)} := \{\boldsymbol{k}_0^{(h)*}, \{\boldsymbol{k}_t^{(h)*}\}_{t \in I_{\vec{v}^{(h)}}}\}_{h=1,\dots,\nu}$ and $\mathsf{ct} := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T)$ above can be expressed as keys and ciphertext in two ways, in Game 1-ν-5 over bases $(\mathbb{B}, \mathbb{B}^*)$ and in Game 2 over bases $(\mathbb{D}, \mathbb{D}^*)$. Thus, Game 1-$\nu$-5 can be conceptually changed to Game 2. □

A.4 Proofs of Lemmas 23 and 24 in Section 6.1.3

A.4.1 Outline

Intractability of (complicated) Problems 1-ABE and 2-ABE are reduced to that of the DLIN Problem through several intermediate steps, or intermediate problems, as indicated below (Figure 2):

1. DLIN Problem (in Definition 3)

2. BP1, BP2, BP3-p, BP4-p, BP5-p, BP6, BP0 for $p = 1, \dots, d$: Basic Problems with DPVS $\mathbb{V}_0$ of dimension 5 and $\mathbb{V}$ of dimension 14 (in Definitions 20–26)

3. P1-ABE, P2-ABE : Problems 1-ABE and 2-ABE (in Definitions 18 and 19)

We will explain how the simplest problem, DLIN, is sequentially transformed to more complicated ones.

DLIN → Basic Problems : In this first reduction step, DLIN instances on (symmetric) pairing group are transformed to a Basic Problem instance on the DPVS, $\mathbb{V}$, i.e., higher level concept. The reductions are given in Lemmas 34–44 (Appendix A.4.2). The reductions are indicated in Figure 2 by arrows or dotted arrows. The proofs of reductions by dotted arrows are similar to those in [14], and those by arrows are given in Appendix A.4.2.

Basic Problems → P1-ABE, P2-ABE : The reductions are given in Lemmas 45–56 (Appendices A.4.3 and A.4.4). They are indicated in Figure 2 by arrows.

A.4.2 Basic Problems

Definition 20 (Basic Problem 1) *Basic Problem 1 is to guess β, given* $(\mathsf{param}, \mathbb{B}_0, \widehat{\mathbb{B}}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,i}\}_{i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{BP1}}(1^\lambda, d)$, *where*

$$
\begin{array}{l}
\mathcal{G}_\beta^{\mathsf{BP1}}(1^\lambda, d): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)), \\
\quad \widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \ldots, \boldsymbol{b}_{0,5}^*), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_6^*, \boldsymbol{b}_9^*, \ldots, \boldsymbol{b}_{14}^*), \\
\quad \omega, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \quad \boldsymbol{e}_{0,0} := (\omega, 0, 0, 0, \varphi_0)_{\mathbb{B}_0}, \quad \boldsymbol{e}_{1,0} := (\omega, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0}, \\
\quad \text{for } i = 1, 2; \quad \vec{e}_i := (0^{i-1}, 1, 0^{2-i}) \in \mathbb{F}_q^2, \quad \vec{\varphi}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^2, \\
\qquad \begin{array}{rlcccccccl}
 & & \overbrace{\hphantom{0^2,\ \omega\vec{e}_i,}}^{4} & & \overbrace{\hphantom{\tau\vec{e}_i,\ 0^4,}}^{6} & & \overbrace{\hphantom{0^2,}}^{2} & & \overbrace{\hphantom{\vec{\varphi}_i}}^{2} & \\
\boldsymbol{e}_{0,i} := & (& 0^2,\ \omega\vec{e}_i, & & 0^6, & & 0^2, & & \vec{\varphi}_i &)_{\mathbb{B}} \\
\boldsymbol{e}_{1,i} := & (& 0^2,\ \omega\vec{e}_i, & & \tau\vec{e}_i,\ 0^4, & & 0^2, & & \vec{\varphi}_i &)_{\mathbb{B}}
\end{array} \\
\quad \text{return } (\mathsf{param}, \mathbb{B}_0, \widehat{\mathbb{B}}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,i}\}_{i=1,2}),
\end{array}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{C}$, the advantage of $\mathcal{C}$ for Basic Problem 1, $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{BP1}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 34 *For any adversary $\mathcal{C}$, there exists a probabilistic machine $\mathcal{F}$, whose running time is essentially the same as that of $\mathcal{C}$, such that for any security parameter λ,* $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{BP1}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}}^{\mathsf{DLIN}}(\lambda) + 5/q$.

Lemma 34 is proven in a similar manner to Lemma 1 in [14].

Definition 21 (Basic Problem 2) *Basic Problem 2 is to guess β, given* $(\mathsf{param}, \widehat{\mathbb{B}}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_i\}_{i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{BP2}}(1^\lambda, d)$, *where*

$$
\begin{array}{l}
\mathcal{G}_\beta^{\mathsf{BP2}}(1^\lambda, d): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)), \\
\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \ldots, \boldsymbol{b}_{0,5}), \quad \widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6, \boldsymbol{b}_9, \ldots, \boldsymbol{b}_{14}), \qquad \delta, \omega, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \rho, \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \\
\quad \boldsymbol{h}_{0,0}^* := (\delta, 0, 0, \eta_0, 0)_{\mathbb{B}_0}, \ \boldsymbol{h}_{1,0}^* := (\delta, \rho, 0, \eta_0, 0)_{\mathbb{B}_0}, \ \boldsymbol{e}_0 := (\omega, \tau, 0, 0, 0)_{\mathbb{B}_0}, \\
\quad \text{for } i = 1, 2; \quad \vec{e}_i := (0^{i-1}, 1, 0^{2-i}) \in \mathbb{F}_q^2, \quad \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^2, \\
\qquad \begin{array}{rlcccccccl}
 & & \overbrace{\hphantom{0^2,\ \delta\vec{e}_i,}}^{4} & & \overbrace{\hphantom{\rho\vec{e}_i,\ 0^4,}}^{6} & & \overbrace{\hphantom{\vec{\eta}_i,}}^{2} & & \overbrace{\hphantom{0^2}}^{2} & \\
\boldsymbol{h}_{0,i}^* := & (& 0^2,\ \delta\vec{e}_i, & & 0^6, & & \vec{\eta}_i, & & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{h}_{1,i}^* := & (& 0^2,\ \delta\vec{e}_i, & & \rho\vec{e}_i,\ 0^4, & & \vec{\eta}_i, & & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{e}_i := & (& 0^2,\ \omega\vec{e}_i, & & \tau\vec{e}_i,\ 0^4, & & 0^2, & & 0^2 &)_{\mathbb{B}}
\end{array} \\
\quad \text{return } (\mathsf{param}, \widehat{\mathbb{B}}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_i\}_{i=1,2}),
\end{array}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{C}$, the advantage of $\mathcal{C}$ for Basic Problem 2, $\mathsf{Adv}_{\mathcal{C}}^{\mathsf{BP2}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 35 *For any adversary $\mathcal{C}$, there exists a probabilistic machine $\mathcal{F}$, whose running time is essentially the same as that of $\mathcal{C}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{BP2}}_{\mathcal{C}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + 5/q$.*

Lemma 35 is proven in a similar manner to Lemma 2 in [14].

Definition 22 (Basic Problem 3-p for $p = 1, \ldots, d$) *Basic Problem 3-p is to guess β, given $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,p,i}, \boldsymbol{e}_i, \boldsymbol{g}_i\}_{i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP3}\text{-}p}_{\beta}(1^\lambda, d)$, where*

$$
\begin{array}{l}
\mathcal{G}^{\mathsf{BP3}\text{-}p}_{\beta}(1^\lambda, d): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)), \\
\quad \widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6, \boldsymbol{b}_{11}, \ldots, \boldsymbol{b}_{14}), \quad \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \quad \boldsymbol{e}_0 := (0, \tau, 0, 0, 0)_{\mathbb{B}_0}, \\
\quad \text{for } i = 1, 2; \quad \vec{e}_i := (0^{i-1}, 1, 0^{2-i}) \in \mathbb{F}_q^2, \quad \vec{\eta}_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2, \quad \mu_{p,i}, \theta_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\
\quad \begin{array}{rcccccl}
 & & \overbrace{\hphantom{\mu_{p,i}(p,-1),\ 0^2,}}^{4} & \overbrace{\hphantom{-\theta_{p,i}\vec{e}_i,\ \theta_{p,i}\vec{e}_i,\ 0^2,}}^{6} & \overbrace{\hphantom{\vec{\eta}_{p,i},}}^{2} & \overbrace{\hphantom{0^2}}^{2} & \\
\boldsymbol{h}^*_{0,p,i} := & (& \mu_{p,i}(p, -1),\ 0^2, & 0^6, & \vec{\eta}_{p,i}, & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{h}^*_{1,p,i} := & (& \mu_{p,i}(p, -1),\ 0^2, & -\theta_{p,i}\vec{e}_i,\ \theta_{p,i}\vec{e}_i,\ 0^2, & \vec{\eta}_{p,i}, & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{e}_i := & (& 0^4, & \tau\vec{e}_i,\ \tau\vec{e}_i,\ 0^2, & 0^2, & 0^2 &)_{\mathbb{B}} \\
\boldsymbol{g}_i := & (& 0^4, & 0^4,\quad \tau\vec{e}_i, & 0^2, & 0^2 &)_{\mathbb{B}}
\end{array} \\
\quad \text{return } (\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,p,i}, \boldsymbol{e}_i, \boldsymbol{g}_i\}_{i=1,2}),
\end{array}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic adversary $\mathcal{C}$, the advantage of $\mathcal{C}$ for Basic Problem 3, $\mathsf{Adv}^{\mathsf{BP3}\text{-}p}_{\mathcal{C}}(\lambda)$, is similarly defined as in Definition 13.

Lemma 36 *For any adversary $\mathcal{C}$, there exists a probabilistic machine $\mathcal{F}$, whose running time is essentially the same as that of $\mathcal{C}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{BP3}\text{-}p}_{\mathcal{C}_p}(\lambda) \leq \sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{p,j}}(\lambda) + 10/q$, where $\mathcal{C}_p(\cdot) := \mathcal{C}(p, \cdot), \mathcal{F}_{p,j}(\cdot) := \mathcal{F}(p, j, \cdot)$.*

Lemma 36 is obtained by combining Lemma 37 and Lemma 38.

Definition 23 (Basic Problem 4-p for $p = 1, \ldots, d$) *Basic Problem 4-p is to guess β, given $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,p,i}\}_{i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP4}\text{-}p}_{\beta}(1^\lambda, d)$, where*

$$
\begin{array}{l}
\mathcal{G}^{\mathsf{BP4}\text{-}p}_{\beta}(1^\lambda, d): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)), \\
\quad \widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6, \boldsymbol{b}_9, \ldots, \boldsymbol{b}_{14}), \\
\quad \text{for } i = 1, 2; \quad \vec{e}_i := (0^{i-1}, 1, 0^{2-i}) \in \mathbb{F}_q^2, \quad \vec{\eta}_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2, \mu_{p,i}, \theta_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\
\quad \begin{array}{rcccccl}
 & & \overbrace{\hphantom{\mu_{p,i}(p,-1),\ 0^2,}}^{4} & \overbrace{\hphantom{0^2,\ \theta_{p,i}\vec{e}_i,\ 0^2,}}^{6} & \overbrace{\hphantom{\vec{\eta}_{p,i},}}^{2} & \overbrace{\hphantom{0^2}}^{2} & \\
\boldsymbol{h}^*_{0,p,i} := & (& \mu_{p,i}(p, -1),\ 0^2, & 0^6, & \vec{\eta}_{p,i}, & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{h}^*_{1,p,i} := & (& \mu_{p,i}(p, -1),\ 0^2, & 0^2,\ \theta_{p,i}\vec{e}_i,\ 0^2, & \vec{\eta}_{p,i}, & 0^2 &)_{\mathbb{B}^*},
\end{array} \\
\quad \text{return } (\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,p,i}\}_{i=1,2}),
\end{array}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic adversary $\mathcal{D}$, the advantage of $\mathcal{D}$ for Basic Problem 4, $\mathsf{Adv}^{\mathsf{BP4}\text{-}p}_{\mathcal{D}}(\lambda)$, is similarly defined as in Definition 13.

Lemma 37 *For any adversary $\mathcal{C}$, there exists a probabilistic machine $\mathcal{D}$, whose running time is essentially the same as that of $\mathcal{C}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{BP3}\text{-}p}_{\mathcal{C}_p}(\lambda) \leq \mathsf{Adv}^{\mathsf{BP4}\text{-}p}_{\mathcal{D}_p}(\lambda)$, where $\mathcal{C}_p(\cdot) := \mathcal{C}(p, \cdot), \mathcal{D}_p(\cdot) := \mathcal{D}(p, \cdot)$*

Proof. $\mathcal{D}$ is given an integer p and a $\mathsf{BP4}\text{-}p$ instance $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,p,i}\}_{i=1,2})$. $\mathcal{D}$ can calculate

$$\boldsymbol{e}_0 := (0, \tau, 0, 0, 0)_{\mathbb{B}_0},$$

$$\begin{array}{lccccccc}
 & & \overbrace{\qquad\qquad}^{4} & \overbrace{\qquad\qquad\qquad\qquad}^{6} & & \overbrace{\quad}^{2} & \overbrace{\quad}^{2} & \\
\boldsymbol{e}_i := & (& 0^4, & \tau\vec{e}_i, \quad 0^4, & & 0^2, & 0^2 &)_{\mathbb{B}} \\
\boldsymbol{g}_i := & (& 0^4, & 0^4, \quad \tau\vec{e}_i, & & 0^2, & 0^2 &)_{\mathbb{B}},
\end{array}$$

where $\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q$ using $\mathbb{B}_0$ and $\widehat{\mathbb{B}}$ in the $\mathsf{BP4}\text{-}p$ instance. $\mathcal{D}$ sets

$$\begin{aligned}
&\boldsymbol{d}_{4+i} := \boldsymbol{b}_{4+i} - \boldsymbol{b}_{6+i}, \quad \boldsymbol{d}^*_{6+i} := \boldsymbol{b}^*_{6+i} + \boldsymbol{b}^*_{4+i}, \quad \text{for } i = 1, 2, \\
&\mathbb{D} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \ \boldsymbol{d}_5, \boldsymbol{d}_6, \ \boldsymbol{b}_7, \ldots, \boldsymbol{b}_{14}), \quad \mathbb{D}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_6, \ \boldsymbol{d}^*_7, \boldsymbol{d}^*_8, \ \boldsymbol{b}^*_9, \ldots, \boldsymbol{b}^*_{14}), \\
&\widehat{\mathbb{D}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \ \boldsymbol{b}_9, \ldots, \boldsymbol{b}_{14}).
\end{aligned}$$

$\mathcal{D}$ can calculate $\widehat{\mathbb{D}}$, but cannot calculate all the $\mathbb{D}$ using $\widehat{\mathbb{B}}$ given in the $\mathsf{BP4}\text{-}p$ instance. $\mathcal{D}$ then gives integer p and $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{D}}, \mathbb{D}^*, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,p,i}, \boldsymbol{e}_i, \boldsymbol{g}_i\}_{i=1,2})$ to $\mathcal{C}$, and outputs $\beta' \in \{0, 1\}$ if $\mathcal{C}$ outputs β'.

With $\mathbb{D}$ and $\mathbb{D}^*$, $\boldsymbol{h}^*_{0,p,i}, \boldsymbol{h}^*_{1,p,i}, \boldsymbol{e}_i, \boldsymbol{g}_i$ are represented as

$$\begin{array}{lcccccc}
 & & \overbrace{\qquad\qquad\qquad\qquad}^{4} & \overbrace{\qquad\qquad\qquad\qquad}^{6} & \overbrace{\quad}^{2} & \overbrace{\quad}^{2} & \\
\boldsymbol{h}^*_{0,p,i} := & (& \mu_{p,i}(p, -1), \ 0^2, & 0^6, & \vec{\eta}_{p,i}, & 0^2 &)_{\mathbb{D}^*}, \\
\boldsymbol{h}^*_{1,p,i} := & (& \mu_{p,i}(p, -1), \ 0^2, & -\theta_{p,i}\vec{e}_i, \ \theta_{p,i}\vec{e}_i, \ 0^2, & \vec{\eta}_{p,i}, & 0^2 &)_{\mathbb{D}^*}, \\
\boldsymbol{e}_i := & (& 0^4, & \tau\vec{e}_i, \ \tau\vec{e}_i, \ 0^2, & 0^2, & 0^2 &)_{\mathbb{D}} \\
\boldsymbol{g}_i := & (& 0^4, & 0^4, \quad \tau\vec{e}_i, & 0^2, & 0^2 &)_{\mathbb{D}}
\end{array}$$

Therefore, the distribution of $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{D}}, \mathbb{D}^*, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,p,i}, \boldsymbol{e}_i, \boldsymbol{g}_i\}_{i=1,2})$ is exactly the same as $\left\{ \varrho \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{BP3}\text{-}p}(1^\lambda, d) \right\}$. □

Lemma 38 *For any adversary $\mathcal{D}$, there exists a probabilistic machine $\mathcal{F}$, whose running time is essentially the same as that of $\mathcal{D}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{BP4}\text{-}p}_{\mathcal{D}_p}(\lambda) \le \sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{p,j}}(\lambda) + 10/q$, where $\mathcal{D}_p(\cdot) := \mathcal{D}(p, \cdot), \mathcal{F}_{p,j}(\cdot) := \mathcal{F}(p, j, \cdot)$.*

Lemma 38 is proven in a similar manner to Lemma 1 in [14].

Definition 24 (Basic Problem 5-p for $p = 1, \ldots, d$) *Basic Problem 5-p is to guess β, given $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*_0, \{\boldsymbol{h}^*_{p,i}, \boldsymbol{e}_{\beta,l,i}\}_{l=1,\ldots,p-1,p+1,\ldots,d;\ i=1,2}, \{\widetilde{\boldsymbol{h}}^*_j\}_{j=5,6,9,10}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{BP5}\text{-}p}(1^\lambda, d)$, where*

$$\begin{aligned}
\mathcal{G}_\beta^{\mathsf{BP5}\text{-}p}(1^\lambda, d): \quad & (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)), \\
& \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_6, \boldsymbol{b}^*_9, \ldots, \boldsymbol{b}^*_{14}), \quad \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\
& \text{for } l = 1, \ldots, p-1, p+1, \ldots, d; \ i = 1, 2; \\
& \quad \vec{e}_i := (0^{i-1}, 1, 0^{2-i}) \in \mathbb{F}_q^2, \quad \vec{\eta}_{p,i}, \vec{\chi}_{l,i}, \vec{\varphi}_{l,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2, \mu_{p,i}, \sigma_{l,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q,
\end{aligned}$$

$$\begin{array}{lcccccc}
 & & \overbrace{\qquad\qquad\qquad\qquad}^{4} & \overbrace{\qquad\qquad\qquad\qquad}^{6} & \overbrace{\quad}^{2} & \overbrace{\quad}^{2} & \\
\boldsymbol{h}^*_{p,i} := & (& \mu_{p,i}(p, -1), \ 0^2, & 0^2, \ \rho\vec{e}_i, \ 0^2, & \vec{\eta}_{p,i}, & 0^2 &)_{\mathbb{B}^*}, \\
\boldsymbol{e}_{0,l,i} := & (& \sigma_{l,i}(1, l), \ 0^2, & 0^6, & 0^2, & \vec{\varphi}_{l,i} &)_{\mathbb{B}}, \\
\boldsymbol{e}_{1,l,i} := & (& \sigma_{l,i}(1, l), \ 0^2, & 0^2, \ \vec{\chi}_{l,i}, \ 0^2, & 0^2, & \vec{\varphi}_{l,i} &)_{\mathbb{B}},
\end{array}$$

$$\begin{aligned}
& \boldsymbol{h}^*_0 := \rho \boldsymbol{b}^*_{0,2}, \quad \widetilde{\boldsymbol{h}}^*_j := \rho \boldsymbol{b}^*_j \ \text{ for } j = 5, 6, 9, 10, \\
& \text{return } (\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{h}^*_0, \{\boldsymbol{h}^*_{p,i}, \boldsymbol{e}_{\beta,l,i}\}_{l=1,\ldots,p-1,p+1,\ldots,d;\ i=1,2}, \{\widetilde{\boldsymbol{h}}^*_j\}_{j=5,6,9,10}),
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{C}$, *the advantage of* $\mathcal{C}$ *for Basic Problem 5,* $\mathsf{Adv}^{\mathsf{BP5}\text{-}p}_{\mathcal{C}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 39 *For any adversary* $\mathcal{C}$, *there exists a probabilistic machine* $\mathcal{F}$, *whose running time is essentially the same as that of* $\mathcal{C}$, *such that for any security parameter* λ, $\mathsf{Adv}^{\mathsf{BP5}\text{-}p}_{\mathcal{C}_p}(\lambda) \leq \sum_{l=1,\ldots,p-1,p+1,\ldots,d}(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{p,l,1}}(\lambda)+\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{p,l,2}}(\lambda))+\epsilon$, *where* $\mathcal{C}_p(\cdot) := \mathcal{C}(p,\cdot), \mathcal{F}_{p,l,\iota}(\cdot) := \mathcal{F}(p,l,\iota,\cdot), \epsilon := 5(d-1)/q$.

Proof. Combining Lemmas 40, 42 and 43, $\mathsf{Adv}^{\mathsf{BP5}\text{-}p}_{\mathcal{C}_p}(\lambda) \leq \sum_{l=1,\ldots,p-1,p+1,\ldots,d}\mathsf{Adv}^{\mathsf{BP6}}_{\mathcal{D}_{p,l}}(\lambda) \leq \sum_{l=1,\ldots,p-1,p+1,\ldots,d}(\mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{D}_{p,l,1}}(\lambda)+\mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{D}_{p,l,2}}(\lambda)) \leq \sum_{l=1,\ldots,p-1,p+1,\ldots,d}(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{p,l,1}}(\lambda)+\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{p,l,2}}(\lambda))+\epsilon$, where $\epsilon := 5(d-1)/q$. This completes the proof of Lemma 39. □

Definition 25 (Basic Problem 6) *Basic Problem 6 is to guess* β, *given* $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{h}_0^*, \{\boldsymbol{h}_i^*, \boldsymbol{e}_{\beta,i}\}_{i=1,2}, \{\widetilde{\boldsymbol{h}}_j^*\}_{j=5,6,9,10}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP6}}_{\beta}(1^\lambda)$, *where*

$$\begin{array}{l}
\mathcal{G}^{\mathsf{BP6}}_{\beta}(1^\lambda): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14)),\\
\quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_6^*, \boldsymbol{b}_9^*, \ldots, \boldsymbol{b}_{14}^*),\\
\quad \text{for } i = 1,2; \quad \vec{e}_i := (0^{i-1}, 1, 0^{2-i}) \in \mathbb{F}_q^2, \ \mu_i, \rho, \sigma_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \vec{\chi}_i, \vec{\varphi}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^2,\\
\qquad \begin{array}{rcccccl}
 & & \overbrace{\qquad\qquad}^{2} & \overbrace{\qquad\qquad\qquad}^{6} & \overbrace{\qquad}^{2} & \overbrace{\qquad}^{2} & \\
\boldsymbol{h}_i^* := & (& \mu_i, \ 0^3, & 0^2, \ \rho\vec{e}_i, \ 0^2, & 0^2, & 0^2 &)_{\mathbb{B}^*},\\
\boldsymbol{e}_{0,i} := & (& \sigma_i, \ 0^3, & 0^6, & 0^2, & \vec{\varphi}_i &)_{\mathbb{B}},\\
\boldsymbol{e}_{1,i} := & (& \sigma_i, \ 0^3, & 0^2, \ \vec{\chi}_i, \ 0^2, & 0^2, & \vec{\varphi}_i &)_{\mathbb{B}},
\end{array}\\
\quad \boldsymbol{h}_0^* := \rho\boldsymbol{b}_{0,2}^*, \quad \widetilde{\boldsymbol{h}}_j^* := \rho\boldsymbol{b}_j^* \ \text{ for } j = 5,6,9,10,\\
\quad \text{return}\,(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{h}_0^*, \{\boldsymbol{h}_i^*, \boldsymbol{e}_{\beta,i}\}_{i=1,2}, \{\widetilde{\boldsymbol{h}}_j^*\}_{j=5,6,9,10}),
\end{array}$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{D}$, *the advantage of* $\mathcal{D}$ *for Basic Problem 6,* $\mathsf{Adv}^{\mathsf{BP6}}_{\mathcal{D}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 40 *For any adversary* $\mathcal{C}$, *there exists a probabilistic machine* $\mathcal{D}$, *whose running time is essentially the same as that of* $\mathcal{C}$, *such that for any security parameter* λ,
$\mathsf{Adv}^{\mathsf{BP5}\text{-}p}_{\mathcal{C}_p}(\lambda) \leq \sum_{l=1,\ldots,p-1,p+1,\ldots,d}\mathsf{Adv}^{\mathsf{BP6}}_{\mathcal{D}_{p,l}}(\lambda)$, *where* $\mathcal{C}_p(\cdot) := \mathcal{C}(p,\cdot), \mathcal{D}_{p,l}(\cdot) := \mathcal{D}(p,l,\cdot)$

Proof. To prove Lemma 40, we consider the following experiments. Basic Problem 5-p is the hybrid of the following Experiment $0, 1, \ldots, p-1, p+1, \ldots, d$, i.e.,
$\mathsf{Adv}^{\mathsf{BP5}\text{-}p}_{\mathcal{C}_p}(\lambda) = \left|\mathsf{Pr}\left[\mathsf{Exp}^{0}_{\mathcal{C}_p}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}^{d}_{\mathcal{C}_p}(\lambda) \to 1\right]\right|$. Therefore, from Lemma 41, we obtain Lemma 40. □

Experiments: In Experiment 0, a part framed by a box indicates positions of coefficients to be changed in a subsequent game. In the other experiments, a part framed by a box indicates coefficients which were changed in an experiment from the previous experiment. Experiments proceed as follows:

Experiment 0 ⇒ Experiment 1 ⇒ $\cdots$ ⇒ Experiment $p-1$ ⇒ Experiment $p+1$ ⇒ $\cdots$ ⇒ Experiment d

For a probabilistic adversary $\mathcal{C}_p$, we define an experiment $\mathsf{Exp}^{0}_{\mathcal{C}_p}$ using Problem BP5-p generator $\mathcal{G}^{\mathsf{BP5}\text{-}p}_{0}(1^\lambda, d)$ in Definition 24 as follows:

1. $\mathcal{C}_p$ is given $\varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{BP5}\text{-}p}(1^\lambda, d)$.

2. Output $\beta' \xleftarrow{\mathsf{R}} \mathcal{C}_p(1^\lambda, \varrho)$.

Experiment 0 ($\mathsf{Exp}^0_{\mathcal{C}_p}$) **:** $\beta = 0$ case of Basic Problem 5. That is,

for $l = 1, \ldots, p-1, p+1, \ldots, d;\ i = 1, 2;$

$$\boldsymbol{e}_{l,i} := (\ \overbrace{\sigma_{l,i}(1,\ l),\ 0^2,}^{4}\ \ \overbrace{0^2,\ \boxed{0^2},\ 0^2,}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_{l,i}}^{2}\ )_{\mathbb{B}}$$

where all variables are generated as in Basic Problem 5.

Experiment l ($\mathsf{Exp}^l_{\mathcal{C}_p}$, for $l = 1, \ldots, p-1, p+1, \ldots, d$) : Same as Experiment $l-1$ if $l \neq p+1$ and $p-1$ if $l = p+1$ except that

$$\boldsymbol{e}_{l,i} := (\ \overbrace{\sigma_{l,i}(1,\ l),\ 0^2,}^{4}\ \ \overbrace{0^2,\ \boxed{\vec{\chi}_{l,i}},\ 0^2,}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_{l,i}}^{2}\ )_{\mathbb{B}} \tag{26}$$

where $\vec{\chi}_{l,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, and all the other variables are generated as in Experiment $l-1$ if $l \neq p+1$ and $p-1$ if $l = p+1$.

Lemma 41 *For any adversary $\mathcal{C}$, there exists a probabilistic machine $\mathcal{D}$, whose running time is essentially the same as that of $\mathcal{C}$, such that for any security parameter λ, $|\mathsf{Pr}[\mathsf{Exp}^l_{\mathcal{C}_{p,l}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^{l-1}_{\mathcal{C}_{p,l}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{BP6}}_{\mathcal{D}_{p,l}}(\lambda)$ if $l \neq p+1$, $|\mathsf{Pr}[\mathsf{Exp}^{p+1}_{\mathcal{C}_{p,p+1}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^{p-1}_{\mathcal{C}_{p,p+1}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{BP6}}_{\mathcal{D}_{p,p+1}}(\lambda)$ if $l \neq p+1$, where $\mathcal{C}_{p,l}(\cdot) := \mathcal{C}(p, l, \cdot), \mathcal{D}_{p,l}(\cdot) := \mathcal{D}(p, l, \cdot)$.*

Proof. Since the case with $l = p+1$ is proven in a similar manner as the case with $l \neq p+1$, hereafter, we deal with the $l \neq p+1$ case only.

Given a BP6 instance $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}_i^*, \boldsymbol{e}_{\beta,i}\}_{i=1,2})$ and integers p, l, $\mathcal{D}$ calculates

$$\begin{pmatrix} \boldsymbol{d}_1 \\ \boldsymbol{d}_2 \end{pmatrix} := Z \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix} := \begin{pmatrix} p & l \\ -1 & -1 \end{pmatrix} \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}, \quad \text{where } Z := \begin{pmatrix} p & l \\ -1 & -1 \end{pmatrix},$$

$$\begin{pmatrix} \boldsymbol{d}_1^* \\ \boldsymbol{d}_2^* \end{pmatrix} := U \begin{pmatrix} \boldsymbol{b}_1^* \\ \boldsymbol{b}_2^* \end{pmatrix} := (l-p)^{-1} \begin{pmatrix} -1 & 1 \\ -l & p \end{pmatrix} \begin{pmatrix} \boldsymbol{b}_1^* \\ \boldsymbol{b}_2^* \end{pmatrix}, \quad \text{where } U := \left(Z^{-1}\right)^{\mathrm{T}},$$

$$\mathbb{D} := (\boldsymbol{d}_1, \boldsymbol{d}_2, \boldsymbol{b}_3, \ldots, \boldsymbol{b}_{14}),\ \mathbb{D}^* := (\boldsymbol{d}_1^*, \boldsymbol{d}_2^*, \boldsymbol{b}_3^*, \ldots, \boldsymbol{b}_{14}^*),\ \widehat{\mathbb{D}}^* := (\boldsymbol{d}_1^*, \boldsymbol{d}_2^*, \boldsymbol{b}_3^*, \ldots, \boldsymbol{b}_6^*, \boldsymbol{b}_9^*, \ldots, \boldsymbol{b}_{14}^*),$$
$$\boldsymbol{h}_{p,i}^* := \boldsymbol{h}_i^*,\ \boldsymbol{e}_{\beta,l,i} := \boldsymbol{e}_{\beta,i},$$

and $\{\boldsymbol{e}_{\beta,t,i}\}_{t=1,\ldots,d, t\neq p,l;\ i=1,2}, \{\widetilde{\boldsymbol{h}}_j^*\}_{j=5,6,9,10}$ with $\rho, \sigma_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\chi}_{t,i}, \vec{\varphi}_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ and dual basis $(\mathbb{D}, \mathbb{D}^*)$ as in the definition of Experiment l. $\mathcal{D}$ then gives $\varrho := (\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{D}, \widehat{\mathbb{D}}^*,$ $\{\boldsymbol{h}_{p,i}^*, \boldsymbol{e}_{\beta,l,i}\}_{l=1,\ldots,p-1,p+1,\ldots,d;\ i=1,2}, \{\widetilde{\boldsymbol{h}}_j^*\}_{j=5,6,9,10})$ to $\mathcal{C}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{C}$ outputs β'.

Claim 6 *When $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances in Experiment $l-1$ (resp. Experiment l).*

Proof. We will consider the joint distribution of $(\mathbb{D}, \widehat{\mathbb{D}}^*, \{\boldsymbol{h}_{p,i}^*, \boldsymbol{e}_{\beta,l,i}\}_{l=1,\ldots,p-1,p+1,\ldots,d;\ i=1,2},$ $\{\widetilde{\boldsymbol{h}}_j^*\}_{j=5,6,9,10})$. $\{\boldsymbol{h}_{p,i}^*, \boldsymbol{e}_{\beta,l,i}\}_{l=1,\ldots,p-1,p+1,\ldots,d;\ i=1,2}$ are given as

$$\boldsymbol{h}_{p,i}^* := (\ \mu_{p,i}(1,\ 0),\ 0^4,\ \rho\vec{e}_i,\ 0^2,\ \vec{\eta}_i,\ 0^2\ )_{\mathbb{B}^*} = (\ \mu_{p,i}(p,\ -1),\ 0^4,\ \rho\vec{e}_i,\ 0^2,\ \vec{\eta}_i,\ 0^2\ )_{\mathbb{D}^*},$$
$$\boldsymbol{e}_{0,l,i} := (\ \sigma_i(1,\ 0),\ 0^6,\ 0^2,\ 0^2,\ \vec{\varphi}_i\ )_{\mathbb{B}} = (\ \widetilde{\sigma}_i(1,\ l),\ 0^6,\ 0^2,\ 0^2,\ \vec{\varphi}_i\ )_{\mathbb{D}},$$
$$\boldsymbol{e}_{1,l,i} := (\ \sigma_i(1,\ 0),\ 0^6,\ \vec{\chi}_i,\ 0^2,\ \vec{\varphi}_i\ )_{\mathbb{B}} = (\ \widetilde{\sigma}_i(1,\ l),\ 0^6,\ \vec{\chi}_i,\ 0^2,\ \vec{\varphi}_i\ )_{\mathbb{D}},$$

where $\widetilde{\sigma}_i := (p-l)\sigma_i$ since

$$\begin{pmatrix} \boldsymbol{b}_1^* \\ \boldsymbol{b}_2^* \end{pmatrix} = U^{-1} \begin{pmatrix} \boldsymbol{d}_1^* \\ \boldsymbol{d}_2^* \end{pmatrix} = Z^{\mathrm{T}} \begin{pmatrix} \boldsymbol{d}_1^* \\ \boldsymbol{d}_2^* \end{pmatrix} = \begin{pmatrix} p & -1 \\ l & -1 \end{pmatrix} \begin{pmatrix} \boldsymbol{d}_1^* \\ \boldsymbol{d}_2^* \end{pmatrix},$$
$$\begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix} = Z^{-1} \begin{pmatrix} \boldsymbol{d}_1 \\ \boldsymbol{d}_2 \end{pmatrix} = U^{\mathrm{T}} \begin{pmatrix} \boldsymbol{d}_1 \\ \boldsymbol{d}_2 \end{pmatrix} = (p-l) \begin{pmatrix} 1 & l \\ -1 & -p \end{pmatrix} \begin{pmatrix} \boldsymbol{d}_1 \\ \boldsymbol{d}_2 \end{pmatrix}.$$

Since $(\mathbb{B}, \widehat{\mathbb{B}}^*)$ and $(\mathbb{D}, \widetilde{\mathbb{D}}^*)$ have the same distribution, the distribution of ϱ is exactly same as that of instances in Experiment $l-1$ (resp. Experiment l) when $\beta = 0$ (resp. $\beta = 1$). □
Claim 6 completes the proof of Lemma 41. □

For upper-bounding $\mathsf{Adv}^{\mathsf{BP6}}_{\mathcal{D}_{p,l}}(\lambda)$ by the advantage for the DLIN problem, we use an intermediate problem, Basic Problem 0, below.

Definition 26 (Basic Problem 0) *Basic Problem 0 is to guess β, given $(\mathsf{param}_{\mathsf{BP0}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}_i^*\}_{i=1,2}, \boldsymbol{e}_\beta, \kappa G, \xi G, \rho\xi G) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{BP0}}(1^\lambda)$, where*

$$\mathcal{G}_\beta^{\mathsf{BP0}}(1^\lambda): \quad (\mathsf{param}_{\mathsf{BP0}}, (\mathbb{B}, \mathbb{B}^*), \kappa G, \xi G) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N := 5)), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \boldsymbol{b}_4^*, \boldsymbol{b}_5^*),$$
$$\mu_1, \mu_2, \rho, \sigma, \chi_1, \chi_2, \phi_1, \phi_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$
$$\boldsymbol{h}_1^* := (\ \mu_1,\ \rho,\ 0,\ 0,\ 0\ )_{\mathbb{B}^*}, \quad \boldsymbol{h}_2^* := (\ \mu_2,\ 0,\ \rho,\ 0,\ 0\ )_{\mathbb{B}^*},$$
$$\boldsymbol{e}_0 := (\ \sigma,\ 0,\ 0,\ \phi_1,\ \phi_2\ )_{\mathbb{B}}, \quad \boldsymbol{e}_1 := (\ \sigma,\ \chi_1,\ \chi_2,\ \phi_1,\ \phi_2\ )_{\mathbb{B}},$$
$$\text{return } (\mathsf{param}_{\mathsf{BP0}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}_i^*\}_{i=1,2}, \boldsymbol{e}_\beta, \kappa G, \xi G, \rho\xi G),$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{E}$, the advantage of $\mathcal{E}$ for Basic Problem 0, $\mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{E}}(\lambda)$, is similarly defined as in Definition 13.

Lemma 42 *For any adversary $\mathcal{E}$, there exists a probabilistic machine $\mathcal{F}$, whose running time is essentially the same as that of $\mathcal{E}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{E}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}}(\lambda) + 5/q$.*

Proof. Given a DLIN instance $(\mathsf{param}_{\mathbb{G}},\ G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta)$, $\mathcal{F}$ calculates

$$\mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 5, \mathsf{param}_{\mathbb{G}}),$$
$$g_T := e(\kappa G, \xi G) \ \left(= e(G,G)^{\kappa\xi}\right), \quad \mathsf{param}_{\mathsf{BP0}} := (\mathsf{param}_{\mathbb{V}},\ g_T).$$

$\mathcal{F}$ sets 5×5 matrices Π^*, Π as follows:

$$\Pi := \begin{pmatrix} \xi & & & 1 & 1 \\ & & & \pi_1^{-1} & \\ & & & & \pi_2^{-1} \\ & \kappa & & 1 & \\ & & \kappa & & 1 \end{pmatrix}, \quad \Pi^* := \begin{pmatrix} \kappa & & & & \\ -\pi_1\kappa & -\pi_1\xi & & \pi_1\kappa\xi & \\ -\pi_2\kappa & & -\pi_2\xi & & \pi_2\kappa\xi \\ & \xi & & & \\ & & \xi & & \end{pmatrix},$$

where $\pi_1, \pi_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q$. Then, $\Pi \cdot (\Pi^*)^{\mathrm{T}} = \kappa\xi \cdot I_5$. By using matrices Π and Π^*, $\mathcal{F}$ sets

$$\boldsymbol{u}_1 := (\xi, 0, 0, 1, 1)_{\mathbb{A}}, \quad \boldsymbol{u}_2 := (0, 0, 0, \pi_1^{-1}, 0)_{\mathbb{A}}, \quad \boldsymbol{u}_3 := (0, 0, 0, 0, \pi_2^{-1})_{\mathbb{A}},$$
$$\boldsymbol{u}_4 := (0, \kappa, 0, 1, 0)_{\mathbb{A}}, \quad \boldsymbol{u}_5 := (0, 0, \kappa, 0, 1)_{\mathbb{A}},$$
$$\boldsymbol{u}_1^* := (\kappa, 0, 0, 0, 0)_{\mathbb{A}}, \quad \boldsymbol{u}_2^* := (-\pi_1\kappa, -\pi_1\xi, 0, \pi_1\kappa\xi, 0)_{\mathbb{A}}, \quad \boldsymbol{u}_3^* := (-\pi_2\kappa, 0, -\pi_2\xi, 0, \pi_2\kappa\xi)_{\mathbb{A}},$$
$$\boldsymbol{u}_4^* := (0, \xi, 0, 0, 0)_{\mathbb{A}}, \quad \boldsymbol{u}_5^* := (0, 0, \xi, 0, 0)_{\mathbb{A}},$$

$\mathcal{F}$ can compute $\boldsymbol{u}_i$ for $i = 1, \ldots, 5$ and $\boldsymbol{u}_i^*$ for $i = 1, 4, 5$ from the above DLIN instance. Let bases $\mathbb{U} := (\boldsymbol{u}_i)_{i=1,\ldots,5}$, $\mathbb{U}^* := (\boldsymbol{u}_i^*)_{i=1,\ldots,5}$ of $\mathbb{V}$. $\mathcal{F}$ then generates $\eta, \varphi_1, \varphi_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ such that $\eta \neq 0$, and sets

$$\begin{aligned}
&\boldsymbol{v}_1^* := (\varphi_1 G, -\pi_1\eta G, 0, \pi_1\eta(\kappa G), 0) \quad (= (\varphi_1, -\pi_1\eta, 0, \pi_1\eta\kappa, 0)_{\mathbb{A}}), \\
&\boldsymbol{v}_2^* := (\varphi_2 G, 0, -\pi_2\eta G, 0, \pi_2\eta(\kappa G)) \quad (= (\varphi_2, 0, -\pi_2\eta, 0, \pi_2\eta\kappa)_{\mathbb{A}}), \\
&\boldsymbol{w}_\beta := (\delta\xi G, \sigma\kappa G, \sigma\kappa G, Y_\beta, Y_\beta).
\end{aligned}$$

$\mathcal{F}$ generates a random matrix $W \xleftarrow{\mathsf{U}} GL(5, \mathbb{F}_q)$, then calculates

$$\begin{aligned}
&\boldsymbol{b}_i^* := \boldsymbol{u}_i^* W \ \text{ for } i = 1, 4, 5, \quad \boldsymbol{b}_i := \boldsymbol{u}_i (W^{-1})^{\mathrm{T}} \ \text{ for } i = 1, \ldots, 5, \\
&\widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \boldsymbol{b}_4^*, \boldsymbol{b}_5^*). \quad \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_5), \\
&\boldsymbol{f}_i^* = \boldsymbol{v}_i^* W \ \text{ for } i = 1, 2, \qquad \boldsymbol{y}_\beta = \boldsymbol{w}_\beta (W^{-1})^{\mathrm{T}}.
\end{aligned}$$

$\mathcal{F}$ then gives $(\mathsf{param}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{f}_i^*\}_{i=1,2}, \boldsymbol{y}_\beta, \kappa G, \xi G, \eta G)$ to $\mathcal{E}$, where $\kappa G, \xi G, G$ are contained in the DLIN instance, and outputs $\beta' \in \{0, 1\}$ if $\mathcal{E}$ outputs β'.

If we set

$$\rho := \xi^{-1}\eta, \quad \mu_1 := \rho\pi_1 + \kappa^{-1}\varphi_1, \quad \mu_2 := \rho\pi_2 + \kappa^{-1}\varphi_2,$$

then $\rho \neq 0$ (since $\eta \neq 0$),

$$\begin{aligned}
\boldsymbol{v}_1^* &= (\varphi_1, -\pi_1\eta, 0, \pi_1\eta\kappa, 0)_{\mathbb{A}} = ((\mu_1 - \rho\pi_1)\kappa, -\pi_1\rho\xi, 0, \rho\pi_1\kappa\xi, 0)_{\mathbb{A}} \\
&= \mu_1\boldsymbol{u}_1^* + \rho\boldsymbol{u}_2^* = (\mu_1, \rho, 0, 0, 0)_{\mathbb{U}^*}, \\
\boldsymbol{v}_2^* &= (\varphi_2, 0, -\pi_2\eta, 0, \pi_2\eta\kappa)_{\mathbb{A}} = ((\mu_2 - \rho\pi_2)\kappa, 0, -\pi_2\rho\xi, 0, \rho\pi_2\kappa\xi)_{\mathbb{A}} \\
&= \mu_2\boldsymbol{u}_1^* + \rho\boldsymbol{u}_3^* = (\mu_2, 0, \rho, 0, 0)_{\mathbb{U}^*}, \\
\boldsymbol{f}_1^* &= \boldsymbol{v}_1^* W = ((\mu_1, \rho, 0, 0, 0)_{\mathbb{U}^*}) W = (\mu_1, \rho, 0, 0, 0)_{\mathbb{B}^*}. \\
\boldsymbol{f}_2^* &= \boldsymbol{v}_2^* W = ((\mu_2, 0, \rho, 0, 0)_{\mathbb{U}^*}) W = (\mu_2, 0, \rho, 0, 0)_{\mathbb{B}^*},
\end{aligned}$$

where ρ, μ_1, μ_2 are uniformly and independently distributed since $\eta, \varphi_1, \varphi_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

If $\beta = 0$, i.e., $Y_\beta = Y_0 = (\delta + \sigma)G$, then

$$\begin{aligned}
\boldsymbol{w}_0 &= (\delta\xi G, \sigma\kappa G, \sigma\kappa G, (\delta+\sigma)G, (\delta+\sigma)G) = (\delta\xi, \sigma\kappa, \sigma\kappa, \delta+\sigma, \delta+\sigma)_{\mathbb{A}} \\
&= \delta\boldsymbol{u}_1 + \sigma\boldsymbol{u}_4 + \sigma\boldsymbol{u}_5 = (\delta, 0, 0, \sigma, \sigma)_{\mathbb{U}} \\
\boldsymbol{y}_0 &= \boldsymbol{w}_0 (W^{-1})^{\mathrm{T}} = ((\delta, 0, 0, \sigma, \sigma)_{\mathbb{U}}) (W^{-1})^{\mathrm{T}} = (\delta, 0, 0, \sigma, \sigma)_{\mathbb{B}}.
\end{aligned}$$

Therefore, the distribution of $(\mathsf{param}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{f}_i^*\}_{i=1,2}, \boldsymbol{y}_0, \kappa G, \xi G, \kappa G, \xi G, \eta G = \rho\xi G)$ is exactly the same as $\left\{\varrho \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{BP0}}(1^\lambda)\right\}$ when $\kappa \neq 0$ and $\xi \neq 0$, i.e., except with probability $2/q$.

If $\beta = 1$, i.e., $Y_\beta = Y_1$ $(= \psi G)$ is uniformly distributed in $\mathbb{G}$, we set $\tau := \psi - \delta - \sigma$. Then

$$\begin{aligned}
\boldsymbol{w}_1 &= (\delta\xi G, \sigma\kappa G, \sigma\kappa G, (\delta+\tau+\sigma)G, (\delta+\tau+\sigma)G) = (\delta\xi, \sigma\kappa, \sigma\kappa, \delta+\tau+\sigma, \delta+\tau+\sigma)_{\mathbb{A}} \\
&= \delta\boldsymbol{u}_1 + \pi_1\tau\boldsymbol{u}_2 + \pi_2\tau\boldsymbol{u}_3 + \sigma\boldsymbol{u}_4 + \sigma\boldsymbol{u}_5 = (\delta, \pi_1\tau, \pi_2\tau, \sigma, \sigma)_{\mathbb{U}}, \quad \text{and} \\
\boldsymbol{y}_1 &= \boldsymbol{w}_1 (W^{-1})^{\mathrm{T}} = ((\delta, \chi_1, \chi_2, \sigma, \sigma)_{\mathbb{U}}) (W^{-1})^{\mathrm{T}} = (\delta, \chi_1, \chi_2, \sigma, \sigma)_{\mathbb{B}},
\end{aligned}$$

where $\chi_i := \pi_i\tau$ for $i = 1, 2$ are also uniformly and independently distributed. Therefore, the distribution of $(\mathsf{param}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{f}_i^*\}_{i=1,2}, \boldsymbol{y}_1, \kappa G, \xi G, \eta G = \rho\xi G)$ is exactly the same as $\left\{\varrho \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{BP0}}(1^\lambda)\right\}$ when $\kappa \neq 0$, $\xi \neq 0$ and $\rho \neq 0$, i.e., except with probability $3/q$.

Therefore, $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{BP0}}(\lambda) \le \mathsf{Adv}_{\mathcal{F}}^{\mathsf{DLIN}}(\lambda) + 2/q + 3/q = \mathsf{Adv}_{\mathcal{F}}^{\mathsf{DLIN}}(\lambda) + 5/q$. □

Lemma 43 *For any adversary $\mathcal{D}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{D}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{BP6}}_{\mathcal{D}_{p,l}}(\lambda) \leq \mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{E}_{p,l,1}}(\lambda) + \mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{E}_{p,l,2}}(\lambda)$, where $\mathcal{D}_{p,l}(\cdot) := \mathcal{D}(p,l,\cdot), \mathcal{E}_{p,l,\iota}(\cdot) := \mathcal{E}(p,l,\iota,\cdot)$.*

Proof. To prove Lemma 43, we consider the following experiments. Basic Problem 6 is the hybrid of the following Experiment $0, 1, 2$, i.e., $\mathsf{Adv}^{\mathsf{BP6}}_{\mathcal{D}_p}(\lambda) = \left|\mathsf{Pr}\left[\mathsf{Exp}^{0}_{\mathcal{D}_p}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}^{2}_{\mathcal{D}_p}(\lambda) \to 1\right]\right|$. Therefore, from Lemmas 48–56, and Lemmas in Appendix A.4.2, we obtain Lemma 43. □

Experiments: In Experiment 0, a part framed by a box indicates positions of coefficients to be changed in a subsequent game. In the other experiments, a part framed by a box indicates coefficients which were changed in an experiment from the previous experiment.

For a probabilistic adversary $\mathcal{D}_p$, we define an experiment $\mathsf{Exp}^{0}_{\mathcal{D}_p}$ using Problem BP6 generator $\mathcal{G}^{\mathsf{BP6}}_{0}(1^\lambda, d)$ in Definition 24 as follows:

1. $\mathcal{D}_p$ is given $\varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP6}}_{0}(1^\lambda, d)$.

2. Output $\beta' \xleftarrow{\mathsf{R}} \mathcal{D}_p(1^\lambda, \varrho)$.

Experiment 0 ($\mathsf{Exp}^{0}_{\mathcal{C}_p}$) **:** $\beta = 0$ case of Basic Problem 6. That is,

for $i = 1, 2$;
$$\boldsymbol{e}_i := (\ \overbrace{\sigma_i\ 0^3,}^{4}\ \ \overbrace{0^2,\ \boxed{0^2},\ 0^2,}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_i}^{2}\ )_{\mathbb{B}}$$

where all variables are generated as in Basic Problem 6.

Experiment i ($\mathsf{Exp}^{i}_{\mathcal{C}_p}$, for $i = 1, 2$) : Same as Experiment $i-1$ except that

$$\boldsymbol{e}_i := (\ \overbrace{\sigma_i,\ 0^3,}^{4}\ \ \overbrace{0^2,\ \boxed{\vec{\chi}_i},\ 0^2,}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_i}^{2}\ )_{\mathbb{B}} \tag{27}$$

where $\vec{\chi}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, and all the other variables are generated as in Experiment $i-1$.

Lemma 44 *For any adversary $\mathcal{D}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{D}$, such that for any security parameter λ, $|\mathsf{Pr}[\mathsf{Exp}^{i}_{\mathcal{D}_{p,l}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^{i-1}_{\mathcal{D}_{p,l}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{E}_{p,l}}(\lambda)$, where $\mathcal{D}_{p,l}(\cdot) := \mathcal{D}(p,l,\cdot), \mathcal{E}_{p,l}(\cdot) := \mathcal{E}(p,l,\cdot)$.*

Proof. We will show only the case of $i = 1$ below. Lemma 44 when $i = 2$ is proven in a similar way.

$\mathcal{E}$ is given a Basic Problem 0 instance

$$(\mathsf{param}_{\mathsf{BP0}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_i\}_{i=1,2}, \boldsymbol{e}_\beta, \kappa G, \xi G, \rho\xi G).$$

By using $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e)$ underlying $\mathsf{param}_{\mathsf{BP0}}$, $\mathcal{E}$ calculates

$$\begin{aligned}
&\mathsf{param}_0 := (q, \mathbb{V}_0, \mathbb{G}_T, \mathbb{A}_0, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 5, \mathsf{param}_{\mathbb{G}}),\\
&\mathsf{param} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 14, \mathsf{param}_{\mathbb{G}}),\\
&\mathsf{param}_{\vec{n}} := (\mathsf{param}_0, \mathsf{param}, g_T),
\end{aligned}$$

where g_T is contained in $\mathsf{param}_{\mathsf{BP0}}$. $\mathcal{E}$ generates random matrices $W_0 \xleftarrow{\mathsf{U}} GL(5,\mathbb{F}_q), W \xleftarrow{\mathsf{U}} GL(14,\mathbb{F}_q)$, then sets

$$
\begin{aligned}
&\boldsymbol{d}_{0,\iota} := (0^{\iota-1}, \kappa G, 0^{5-\iota})\, W_0,\ \ \boldsymbol{d}^*_{0,\iota} := (0^{\iota-1}, \xi G, 0^{5-\iota})\, (W_0^{-1})^{\mathrm{T}} \quad \text{for } \iota = 1,\dots,5,\\
&\boldsymbol{d}_1 := (\boldsymbol{b}_1, 0^9)W,\ \ \boldsymbol{d}^*_1 := (\boldsymbol{b}^*_1, 0^9)(W^{-1})^{\mathrm{T}},\\
&\boldsymbol{d}_7 := (\boldsymbol{b}_2, 0^9)W,\ \ \boldsymbol{d}^*_7 := (\boldsymbol{b}^*_2, 0^9)(W^{-1})^{\mathrm{T}},\ \ \boldsymbol{d}_8 := (\boldsymbol{b}_3, 0^9)W,\ \ \boldsymbol{d}^*_8 := (\boldsymbol{b}^*_3, 0^9)(W^{-1})^{\mathrm{T}},\\
&\boldsymbol{d}_{13} := (\boldsymbol{b}_4, 0^9)W,\ \ \boldsymbol{d}^*_{13} := (\boldsymbol{b}^*_4, 0^9)(W^{-1})^{\mathrm{T}},\ \ \boldsymbol{d}_{14} := (\boldsymbol{b}_5, 0^9)W,\ \ \boldsymbol{d}^*_{14} := (\boldsymbol{b}^*_5, 0^9)(W^{-1})^{\mathrm{T}},\\
&\boldsymbol{d}_\iota := (0^5, 0^{\iota-2}, \kappa G, 0^{10-\iota})W,\ \ \boldsymbol{d}^*_\iota := (0^5, 0^{\iota-2}, \xi G, 0^{10-\iota})(W^{-1})^{\mathrm{T}} \quad \text{for } \iota = 2,\dots,6,\\
&\boldsymbol{d}_\iota := (0^{\iota+1}, \kappa G, 0^{12-\iota})W,\ \ \boldsymbol{d}^*_\iota := (0^{\iota+1}, \xi G, 0^{12-\iota})(W^{-1})^{\mathrm{T}} \quad \text{for } \iota = 9,\dots,12,\\
&\boldsymbol{g}_{\beta,1} := (\boldsymbol{e}_\beta, 0^9)W,\ \ \boldsymbol{g}_{\beta,2} := (\sigma_2, 0^{11}, \vec{\varphi}_2)_{\mathbb{D}^*}, \text{where } \sigma_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\varphi}_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q^2,\\
&\boldsymbol{p}^*_0 := (0, \rho\xi G, 0^3)(W_0^{-1})^{\mathrm{T}},\ \ \boldsymbol{p}^*_i := (\boldsymbol{h}^*_i, 0^9)(W^{-1})^{\mathrm{T}} \quad \text{for } i = 1,2,\\
&\widetilde{\boldsymbol{p}}^*_j := (0^{j-1}, \rho\xi G, 0^{14-j})(W^{-1})^{\mathrm{T}} \quad \text{for } j = 5,6,9,10,
\end{aligned}
$$

where $(\boldsymbol{v}, 0^9) := (\widetilde{G}_1,\dots,\widetilde{G}_5, 0^9)$ for any $\boldsymbol{v} := (\widetilde{G}_1,\dots,\widetilde{G}_5) \in \mathbb{G}^5$. Then, $\mathbb{D}_0 := (\boldsymbol{d}_{0,i})_{i=1,\dots,5}$ and $\mathbb{D}^*_0 := (\boldsymbol{d}^*_{0,i})_{i=1,\dots,5}$, $\mathbb{D} := (\boldsymbol{d}_i)_{i=1,\dots,14}$ and $\mathbb{D}^* := (\boldsymbol{d}^*_i)_{i=1,\dots,14}$ are dual orthonormal bases. $\mathcal{E}$ can compute $\mathbb{D}_0 := (\boldsymbol{d}_{0,1},\dots,\boldsymbol{d}_{0,5})$, $\mathbb{D}^*_0 := (\boldsymbol{d}^*_{0,1},\dots,\boldsymbol{d}^*_{0,5})$, $\mathbb{D} := (\boldsymbol{d}_1,\dots,\boldsymbol{d}_{14})$, $\widehat{\mathbb{D}}^* := (\boldsymbol{d}^*_1,\dots,\boldsymbol{d}^*_6,\boldsymbol{d}^*_9,\dots,\boldsymbol{d}^*_{14})$ from $\mathbb{B}, \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \boldsymbol{b}^*_4, \boldsymbol{b}^*_5), \kappa G$, and ξG. $\mathcal{D}$ then gives $\varrho := (\mathsf{param}, \mathbb{D}_0, \mathbb{D}^*_0, \mathbb{D}, \widehat{\mathbb{D}}^*, \boldsymbol{p}^*_0, \{\boldsymbol{p}^*_i, \boldsymbol{g}_{\beta,i}\}_{i=1,2}, \{\widetilde{\boldsymbol{p}}^*_j\}_{j=5,6,9,10})$ to $\mathcal{D}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{D}$ outputs β'.

We can see that the distribution of ϱ is exactly the same as in $\mathsf{Exp}^0_{\mathcal{C}_p}$ (resp. $\mathsf{Exp}^1_{\mathcal{C}_p}$) if $\beta = 0$ (resp. $\beta = 1$). □

A.4.3 Proof of Lemma 23

Lemma 23. *Problem 1-ABE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, there exist probabilistic machines $\mathcal{F}_1, \mathcal{F}_2$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P1\text{-}ABE}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_1}(\lambda) + \sum_{p=1}^{d}\sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{F}_{2\text{-}p\text{-}j}}(\lambda) + \epsilon$, where $\mathcal{F}_{2\text{-}p\text{-}j}(\cdot) := \mathcal{F}_2(p, j, \cdot), \epsilon := (10d+5)/q$.

Proof. To prove Lemma 23, we consider the following experiments. Problem 1-ABE is the hybrid of the following Experiment $0, 1, \dots, 2\text{-}d\text{-}2\text{-}2$, i.e., $\mathsf{Adv}^{\mathsf{P1\text{-}ABE}}_{\mathcal{B}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^0_{\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{2\text{-}d\text{-}2\text{-}2}_{\mathcal{B}}(\lambda) \to 1\right]\right|$. Therefore, from Lemmas 45, 46, 47 and Lemmas in Appendix A.4.2, we obtain Lemma 23. □

Experiments In Experiment 0, a part framed by a box indicates positions of 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 experiment. Experiments proceed as follows:

Experiment 0 ⇒ Experiment 1 ⇒ (for $p = 1,\dots,d;\ j = 1,2;\ l = 1,2;$ Experiment 2-p-j-l)

For a probabilistic adversary $\mathcal{B}$, we define an experiment $\mathsf{Exp}^0_{\mathcal{B}}$ using Problem 1-ABE generator $\mathcal{G}^{\mathsf{P1\text{-}ABE}}_{\beta}(1^\lambda, d)$ in Definition 18 as follows:

1. $\mathcal{B}$ is given $\varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1\text{-}ABE}}_0(1^\lambda, d)$.

2. Output $\beta' \xleftarrow{\mathsf{R}} \mathcal{B}(1^\lambda, \varrho)$.

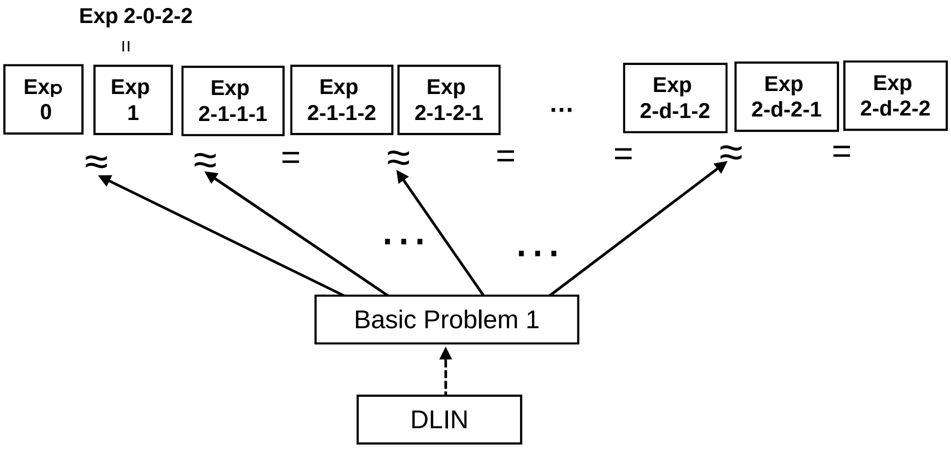


Figure 3: Structure of Reductions for the Proof of Lemma 23

Experiment 0 ($\mathsf{Exp}^0_{\mathcal{B}}$) **:** $\beta = 0$ case of Problem 1-ABE. That is,

$$\left.\begin{array}{l} \boldsymbol{e}_0 := (\omega, \boxed{0}, 0, 0, \varphi_0)_{\mathbb{B}_0}, \\ \text{for } t = 1, \ldots, d;\ i = 1, 2; \\ \boldsymbol{e}_{t,i} := (\ \overbrace{\sigma_{t,i}(1,t),\ \omega\vec{e}_i,}^{4}\ \overbrace{\boxed{0^2},\ 0^2,\ \boxed{0^2},}^{6}\ \overbrace{0^2,}^{2}\ \overbrace{\vec{\varphi}_{t,i}}^{2}\ )_{\mathbb{B}} \end{array}\right\} \tag{28}$$

where all variables are generated as in Problem 1-ABE.

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

$$\left.\begin{array}{l} \boldsymbol{e}_0 := (\omega, \boxed{\tau}, 0, 0, \varphi_0)_{\mathbb{B}_0}, \\ \text{for } t = 1, \ldots, d;\ i = 1, 2; \\ \boldsymbol{e}_{t,i} := (\ \overbrace{\sigma_{t,i}(1,t),\ \omega\vec{e}_i,}^{4}\ \overbrace{\boxed{\tau\vec{e}_i},\ 0^2,\ 0^2,}^{6}\ \overbrace{0^2,}^{2}\ \overbrace{\vec{\varphi}_{t,i}}^{2}\ )_{\mathbb{B}} \end{array}\right\} \tag{29}$$

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

Experiment 2-p-j-1 ($\mathsf{Exp}^{2\text{-}p\text{-}j\text{-}1}_{\mathcal{B}}$**,** for $p = 1, \ldots, d;\ j = 1, 2$) : Experiment 2-0-2-2 is Experiment 1. Same as Experiment 2-($p-1$)-2-2 if $j = 1$, or Experiment 2-p-1-2 if $j = 2$ except that

$$\boldsymbol{e}_{p,j} := (\ \overbrace{\sigma_{p,j}(1,p),\ \omega\vec{e}_j,}^{4}\ \overbrace{\tau\vec{e}_j,\ 0^2,\ \boxed{\widetilde{\sigma}_{p,j}(1,p)},}^{6}\ \overbrace{0^2,}^{2}\ \overbrace{\vec{\varphi}_{p,j}}^{2}\ )_{\mathbb{B}} \tag{30}$$

where $\widetilde{\sigma}_{p,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and all the other variables are generated as in Experiment 2-($p-1$)-2-2 if $j = 1$, or Experiment 2-p-1-2 if $j = 2$.

Experiment 2-p-j-2 ($\mathsf{Exp}^{2\text{-}p\text{-}j\text{-}2}_{\mathcal{B}}$**,** for $p = 1, \ldots, d;\ j = 1, 2$) : Same as Experiment 2-p-j-1 except that

$$\boldsymbol{e}_{p,j} := (\ \overbrace{\sigma_{p,j}(1,p),\ \omega\vec{e}_j,}^{4}\ \overbrace{\tau\vec{e}_j,\ 0^2,\ \boxed{\tau(z_{p,j,1}, z_{p,j,2})},}^{6}\ \overbrace{0^2,}^{2}\ \overbrace{\vec{\varphi}_{p,j}}^{2}\ )_{\mathbb{B}} \tag{31}$$

where $z_{p,j,1}, z_{p,j,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and all the other variables are generated as in Experiment 2-p-j-1.

Let $Z_t := \begin{pmatrix} z_{t,1,1} & z_{t,1,2} \\ z_{t,2,1} & z_{t,2,2} \end{pmatrix}$ for $t = 1, \ldots, d$, then $\boldsymbol{e}_{t,j}$ in the final experiment (Experiment 2-d-2-2) are expressed as

$$\text{for } t = 1, \ldots, d; \; j = 1, 2;$$

$$\boldsymbol{e}_{t,j} := (\overbrace{\sigma_{t,j}(1,t), \; \omega\vec{e}_j,}^{4} \quad \overbrace{\tau\vec{e}_j, \; 0^2, \; \tau\vec{e}_j Z_t,}^{6} \quad \overbrace{0^2,}^{2} \quad \overbrace{\vec{\varphi}_{t,j}}^{2} \quad)_{\mathbb{B}}$$

where $Z_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2\times 2}$. Therefore, the distribution in Experiment 2-d-2-2 and that in the $\beta = 1$ case of Problem 1-ABE are equivalent except for the case that $\det(Z_t) = 0$ for some t, i.e., except with probability d/q.

Lemmas In the following, we consider canonical (monomial) linear order in $\mathbb{N}^2$. For $(t_1, i_1), (t_2, i_2) \in \mathbb{N}^2$,

$$(t_1, i_1) < (t_2, i_2) \iff (t_1 < t_2) \;\text{ or }\; (t_1 = t_2 \;\text{ and }\; i_1 < i_2),$$
$$(t_1, i_1) > (t_2, i_2) \iff (t_2, i_2) < (t_1, i_1).$$

Lemma 45 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_1$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\Pr[\mathsf{Exp}^{(0)}_{\mathcal{B}}(\lambda) \to 1] - \Pr[\mathsf{Exp}^{(1)}_{\mathcal{B}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{C}_1}(\lambda)$.*

Proof. Given a BP1 instance $(\mathsf{param}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,i}\}_{i=1,2})$, $\mathcal{C}_1$ calculates

$$\boldsymbol{g}_{t,i} := \sigma_{t,i}(\boldsymbol{b}_1 + t\boldsymbol{b}_2) + \boldsymbol{e}_{\beta,i} + \varphi_{t,i,1}\boldsymbol{b}_{13} + \varphi_{t,i,2}\boldsymbol{b}_{14},$$

where $\sigma_{t,i}, \varphi_{t,i,1}, \varphi_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\mathcal{C}_1$ then sets $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}), \widehat{\mathbb{B}}'^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}), \widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14}), \widehat{\mathbb{B}}'^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_4, \boldsymbol{b}^*_{11}, \boldsymbol{b}^*_{12})$.

$\mathcal{C}_1$ then gives $\varrho := (\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}'^*_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}'^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{g}_{t,i}\}_{t=1,\ldots,d; i=1,2})$ to $\mathcal{B}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{B}$ outputs β'. If $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances in Experiment 0 (resp. Experiment 1). □

Lemma 46 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_2$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\Pr[\mathsf{Exp}^{(2\text{-}(p-1)\text{-}2\text{-}2)}_{\mathcal{B}}(\lambda) \to 1] - \Pr[\mathsf{Exp}^{(2\text{-}p\text{-}1\text{-}1)}_{\mathcal{B}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{C}_{2\text{-}p\text{-}j}}(\lambda)$ $(j = 1)$, or $|\Pr[\mathsf{Exp}^{(2\text{-}p\text{-}1\text{-}2)}_{\mathcal{B}}(\lambda) \to 1] - \Pr[\mathsf{Exp}^{(2\text{-}p\text{-}2\text{-}1)}_{\mathcal{B}}(\lambda) \to 1]| \leq \mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{C}_{2\text{-}p\text{-}j}}(\lambda)$ $(j = 2)$, where $\mathcal{C}_{2\text{-}p\text{-}j}(\cdot) := \mathcal{C}_2(p, j, \cdot)$.*

Proof. Given integers (p, j) and a BP1 instance $(\mathsf{param}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,i}\}_{i=1,2})$, $\mathcal{C}_2$ sets new dual orthonormal bases $\mathbb{D} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{14}) := (\boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_9, \boldsymbol{b}_{10}, \boldsymbol{b}_7, \boldsymbol{b}_8, \boldsymbol{b}_5, \boldsymbol{b}_6, \boldsymbol{b}_{11}, \ldots, \boldsymbol{b}_{14})$ and $\mathbb{D}^* := (\boldsymbol{d}^*_1, \ldots, \boldsymbol{d}^*_{14}) := (\boldsymbol{b}^*_3, \boldsymbol{b}^*_4, \boldsymbol{b}^*_1, \boldsymbol{b}^*_2, \boldsymbol{b}^*_9, \boldsymbol{b}^*_{10}, \boldsymbol{b}^*_7, \boldsymbol{b}^*_8, \boldsymbol{b}^*_5, \boldsymbol{b}^*_6, \boldsymbol{b}^*_{11}, \ldots, \boldsymbol{b}^*_{14})$.

$\mathcal{C}_2$ then sets $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}), \widehat{\mathbb{B}}'^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}), \widehat{\mathbb{D}} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_4, \boldsymbol{d}_{13}, \boldsymbol{d}_{14}), \widehat{\mathbb{D}}^* := (\boldsymbol{d}^*_1, \ldots, \boldsymbol{d}^*_4, \boldsymbol{d}^*_{11}, \boldsymbol{d}^*_{12})$. $\mathcal{C}_2$ can calculate $(\widehat{\mathbb{D}}, \widehat{\mathbb{D}}^*)$ from $(\mathbb{B}, \widehat{\mathbb{B}}^*)$ in the BP1 instance.

$\mathcal{C}_2$ then calculates $\boldsymbol{e}_{t,i}$ for $(t,i) < (p,j)$ as in Eq. (31) and $\boldsymbol{e}_{t,i}$ for $(t,i) > (p,j)$ as in Eq. (29), using $\mathbb{D}$ and $\widetilde{\omega}, \widetilde{\tau}, \sigma_{t,i}, z_{t,i,1}, z_{t,i,2}, \varphi_{t,i,1}, \varphi_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$. Using $\widetilde{\omega}, \widetilde{\tau}$, $\mathcal{C}_2$ calculates

$$\boldsymbol{g}_0 := (\widetilde{\omega}, \widetilde{\tau}, 0, 0, \varphi_0)_{\mathbb{D}_0},$$
$$\boldsymbol{g}_{p,j} := \boldsymbol{e}_{\beta,1} + p\boldsymbol{e}_{\beta,2} + \widetilde{\omega}\boldsymbol{d}_{2+j} + \widetilde{\tau}\boldsymbol{d}_{4+j},$$

where $\varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\mathcal{C}_2$ then gives $\varrho := (\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0'^*, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}'^*, \boldsymbol{g}_0, \{\boldsymbol{e}_{t,i}\}_{(t,i)\neq(p,j)}, \boldsymbol{g}_{p,j})$ to $\mathcal{B}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{B}$ outputs β'. When $j = 1$, if $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances in Experiment 2-$(p-1)$-2-2 (resp. Experiment 2-p-1-1). When $j = 2$, if $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances in Experiment 2-p-1-2 (resp. Experiment 2-p-2-1). □

Lemma 47 *For any adversary $\mathcal{B}$, for any security parameter λ,* $\Pr[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}j\text{-}1)}(\lambda) \to 1] = \Pr[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}j\text{-}2)}(\lambda) \to 1]$.

Proof. We generate $Z \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$, and set $\begin{pmatrix} \boldsymbol{d}_9 \\ \boldsymbol{d}_{10} \end{pmatrix} := U^{\mathrm{T}} \cdot \begin{pmatrix} \boldsymbol{b}_9 \\ \boldsymbol{b}_{10} \end{pmatrix}$ and $\mathbb{D} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_8, \boldsymbol{d}_9, \boldsymbol{d}_{10}, \boldsymbol{b}_{11}, \ldots, \boldsymbol{b}_{14})$ (and its dual $\mathbb{D}^*$). $(\mathbb{D}, \mathbb{D}^*)$ are consistent with $(\widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$. Since

$$\begin{array}{rrcccccl}
 & & & \overbrace{\hphantom{\sigma_{p,j}(1,p),\ \omega\vec{e}_j,}}^{4} & \overbrace{\hphantom{\tau\vec{e}_j,\ 0^2,\ \widetilde{\sigma}_{p,j}(1,p),}}^{6} & \overbrace{\hphantom{0^2,}}^{2} & \overbrace{\hphantom{\vec{\varphi}_{t,i}}}^{2} & \\
\text{for } (t,i) < (p,j), & \boldsymbol{e}_{t,i} = & (& \sigma_{t,i}(1,t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ \tau\vec{z}_{t,i}, & 0^2, & \vec{\varphi}_{t,i} &)_{\mathbb{B}}, \\
 & = & (& \sigma_{t,i}(1,t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ \tau\vec{z}'_{t,i}, & 0^2, & \vec{\varphi}_{t,i} &)_{\mathbb{D}}, \\
\text{for } (t,i) = (p,j), & \boldsymbol{e}_{t,i} = & (& \sigma_{p,j}(1,p),\ \omega\vec{e}_j, & \tau\vec{e}_j,\ 0^2,\ \widetilde{\sigma}_{p,j}(1,p), & 0^2, & \vec{\varphi}_{p,j} &)_{\mathbb{B}}, \\
 & = & (& \sigma_{p,j}(1,p),\ \omega\vec{e}_j, & \tau\vec{e}_j,\ 0^2,\ \tau\vec{z}_{p,j}, & 0^2, & \vec{\varphi}_{p,j} &)_{\mathbb{D}}, \\
\text{for } (t,i) > (p,j), & \boldsymbol{e}_{t,i} = & (& \sigma_{t,i}(1,t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ 0^2, & 0^2, & \vec{\varphi}_{t,i} &)_{\mathbb{B}}, \\
 & = & (& \sigma_{t,i}(1,t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ 0^2, & 0^2, & \vec{\varphi}_{t,i} &)_{\mathbb{D}},
\end{array}$$

where $\vec{z}_{p,j} := \tau^{-1}\widetilde{\sigma}_{p,j}(1,p) \cdot Z$ and $\vec{z}_{t,i} := (z_{t,i,1}, z_{t,i,2}), \vec{z}'_{t,i} := \vec{z}_{t,i} \cdot Z$ for $(t,i) < (p,j)$. Therefore, $\vec{z}_{p,j}$ and $\vec{z}'_{t,i}$ for $(t,i) < (p,j)$ are uniformly and independently distributed, and the joint distribution for Experiment 2-p-j-1 and that for Experiment 2-p-j-2 are equivalent. □

A.4.4 Proof of Lemma 24

Lemma 24. *Problem 2-ABE is computationally intractable under the DLIN assumption.*

For any adversary $\mathcal{B}$, there exist probabilistic machines $\mathcal{F}_1, \mathcal{F}_{2\text{-}1}, \ldots, \mathcal{F}_{2\text{-}5}$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2\text{-}ABE}}(\lambda) \leq \mathsf{Adv}_{\mathcal{F}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{p=1}^{d} \sum_{j=1}^{2} \Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}2\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \sum_{l=1,\ldots,d;\ l\neq p} \Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}}^{\mathsf{DLIN}}(\lambda) \Big) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}5\text{-}j}}^{\mathsf{DLIN}}(\lambda) \Big) + \epsilon$, *where* $\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}1}(p, j, \cdot), \mathcal{F}_{2\text{-}p\text{-}2\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}2}(p, j, \cdot)$, $\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}3}(p, j, l, \cdot), \mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}(\cdot) := \mathcal{F}_{2\text{-}4}(p, j, l, \cdot), \mathcal{F}_{2\text{-}p\text{-}5\text{-}j}(\cdot) := \mathcal{F}_{2\text{-}5}(p, j, \cdot)$ *and* $\epsilon := (20d^2 + 10d + 5)/q$.

Proof. To prove Lemma 24, we consider the following experiments. Problem 2-ABE is the hybrid of the following Experiment $0, 1, \ldots, 2$-d-8, i.e., $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2\text{-}ABE}}(\lambda) = \big| \Pr\big[\mathsf{Exp}_{\mathcal{B}}^{0}(\lambda) \to 1\big] - \Pr\big[\mathsf{Exp}_{\mathcal{B}}^{2\text{-}d\text{-}8}(\lambda) \to 1\big] \big|$ (Figure 4). Therefore, from Lemmas 48–56, and Lemmas in Appendix A.4.2, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2\text{-}ABE}}(\lambda) = \big| \Pr\big[\mathsf{Exp}_{\mathcal{B}}^{0}(\lambda) \to 1\big] - \Pr\big[\mathsf{Exp}_{\mathcal{B}}^{2\text{-}d\text{-}8}(\lambda) \to 1\big] \big|$
$\leq \mathsf{Adv}_{\mathcal{C}_1}^{\mathsf{BP2}}(\lambda) + \sum_{p=1}^{d} \Big(\mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}1}}^{\mathsf{BP3\text{-}p}}(\lambda) + \mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}2}}^{\mathsf{BP3\text{-}p}}(\lambda) + \mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}3}}^{\mathsf{BP5\text{-}p}}(\lambda) + \mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}4}}^{\mathsf{BP5\text{-}p}}(\lambda) + \mathsf{Adv}_{\mathcal{D}_{2\text{-}p\text{-}5}}^{\mathsf{BP4\text{-}p}}(\lambda) \Big)$
$\leq \mathsf{Adv}_{\mathcal{F}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{p=1}^{d} \sum_{j=1}^{2} \Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}1\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}2\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \sum_{l=1,\ldots,d;\ l\neq p} \Big(\mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}3\text{-}j\text{-}l}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}4\text{-}j\text{-}l}}^{\mathsf{DLIN}}(\lambda) \Big) + \mathsf{Adv}_{\mathcal{F}_{2\text{-}p\text{-}5\text{-}j}}^{\mathsf{DLIN}}(\lambda) \Big) + (20d^2 + 10d + 5)/q$, we obtain Lemma 24. □

Experiments In Experiment 0, a part framed by a box indicates positions of coefficients to be changed in a subsequent game. In the other experiments, a part framed by a box indicates coefficients which were changed in an experiment from the previous experiment. Experiments proceed as follows:

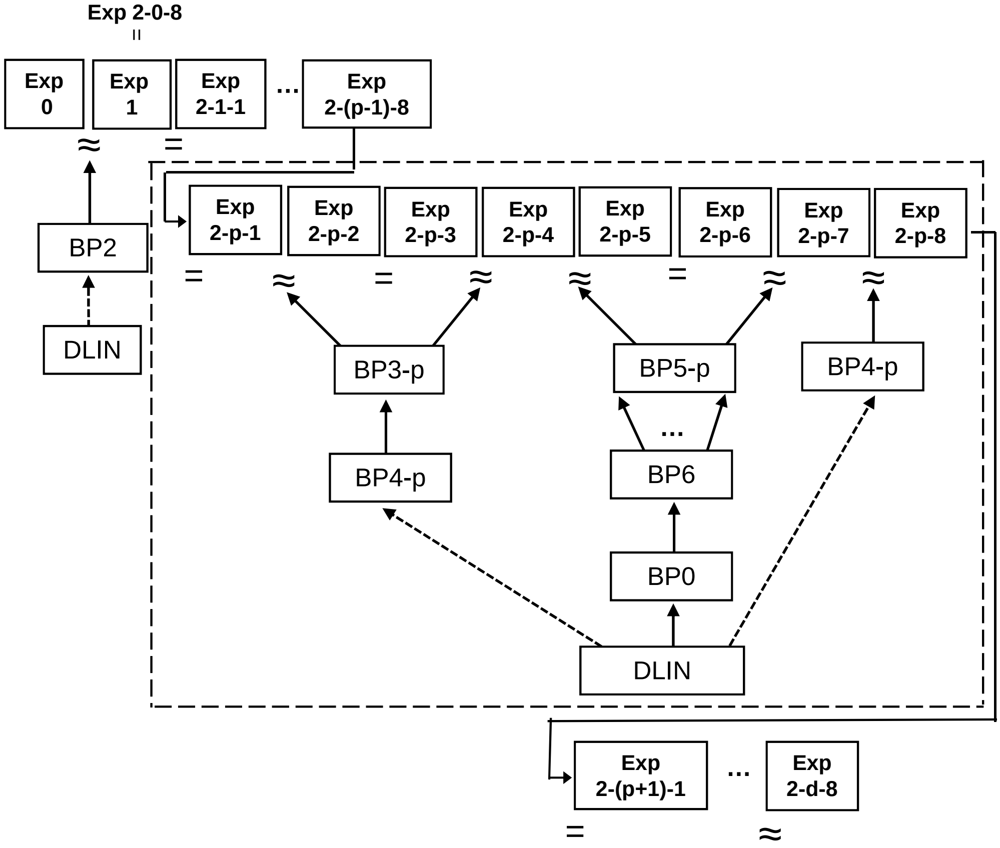


Figure 4: Structure of Reductions for the Proof of Lemma 24

Experiment 0 ⇒ Experiment 1 ⇒

for $p = 1, \dots, d$;   Experiment 2-p-1 ⇒ $\cdots$ ⇒ Experiment 2-p-8

For a probabilistic adversary $\mathcal{B}$, we define an experiment $\mathsf{Exp}^0_{\mathcal{B}}$ using Problem 2-ABE generator $\mathcal{G}^{\mathsf{P2\text{-}ABE}}_{\beta}(1^\lambda, d)$ in Definition 19 as follows:

1. $\mathcal{B}$ is given $\varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2\text{-}ABE}}_{0}(1^\lambda, d)$.

2. Output $\beta' \xleftarrow{\mathsf{R}} \mathcal{B}(1^\lambda, \varrho)$.

Experiment 0 ($\mathsf{Exp}^0_{\mathcal{B}}$) **:** $\beta = 0$ case of Problem 2-ABE. That is,

$$\boldsymbol{h}^*_0 := (\delta, \boxed{0}, 0, \eta_0, 0)_{\mathbb{B}^*_0},$$

for $t = 1, \dots, d;\ i = 1, 2;$

$$\boldsymbol{h}^*_{t,i} := (\quad \overbrace{\mu_{t,i}(t,-1),\ \delta\vec{e}_i,}^{4} \quad \overbrace{\boxed{0^6},}^{6} \quad \overbrace{\vec{\eta}_{t,i},}^{2} \quad \overbrace{0^2}^{2} \quad)_{\mathbb{B}^*}$$

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

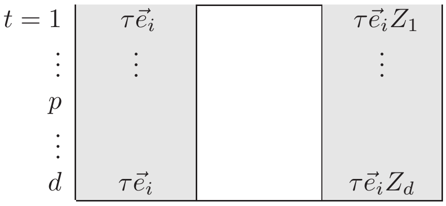
for $t = 1, \dots, d;\ i = 1, 2,$

$$\boldsymbol{e}_{t,i} := (\quad \overbrace{\sigma_{t,i}(1,t),\ \omega\vec{e}_i,}^{4} \quad \overbrace{\tau\vec{e}_i,\ \boxed{0^2},\ \tau\vec{e}_i Z_t,}^{6} \quad \overbrace{0^2,}^{2} \quad \overbrace{\vec{\varphi}_{t,i}}^{2} \quad)_{\mathbb{B}},$$

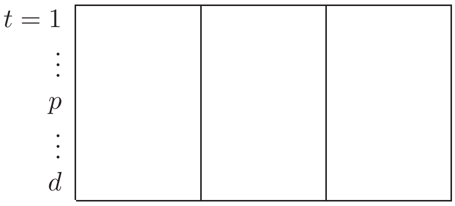
where all variables are generated as in Problem 2-ABE.

Below, we describe coefficients of the hidden part, i.e., $\mathsf{span}\langle \boldsymbol{b}_5, \ldots, \boldsymbol{b}_{10}\rangle$ (resp. $\mathsf{span}\langle \boldsymbol{b}^*_5, \ldots, \boldsymbol{b}^*_{10}\rangle$) of $\boldsymbol{e}_{t,i}$ (resp. $\boldsymbol{h}^*_{t,i}$) w.r.t. these bases vectors for $t = 1, \ldots, d$. 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 $\boldsymbol{e}_{t,i}$ in Experiment 0



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

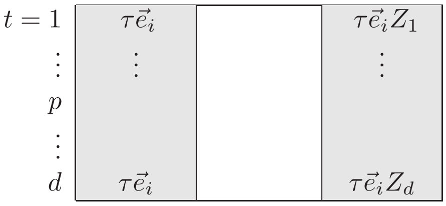


Experiment 1 ($\mathsf{Exp}^1_{\mathcal{B}}$) **:** Same as Experiment 0 except that

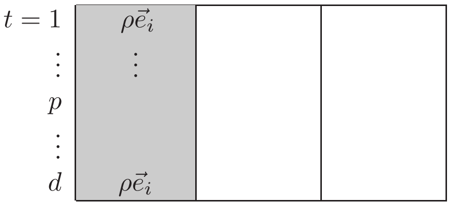
$$\left.\begin{array}{l} \boldsymbol{h}^*_0 := (\delta, \boxed{\rho}, 0, \eta_0, 0)_{\mathbb{B}^*_0}, \\ \text{for } t = 1, \ldots, d;\ i = 1, 2; \\ \boldsymbol{h}^*_{t,i} := (\ \overbrace{\mu_{t,i}(t, -1),\ \delta\vec{e}_i,}^{4}\ \ \overbrace{\boxed{\rho\vec{e}_i},\ 0^4,}^{6}\ \ \overbrace{\vec{\eta}_{t,i},}^{2}\ \ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*} \end{array}\right\} \tag{32}$$

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

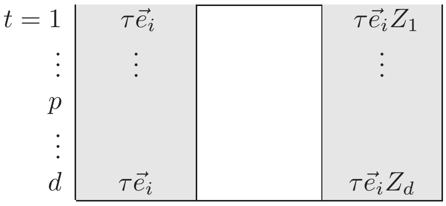
Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 1



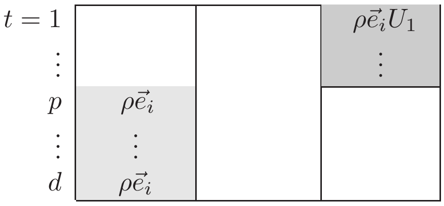
Coefficients of the hidden part of $\boldsymbol{h}^*_{t,i}$ in Experiment 1



Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 2-$(p-1)$-8



Coefficients of the hidden part of $\boldsymbol{h}^*_{t,i}$ in Experiment 2-$(p-1)$-8

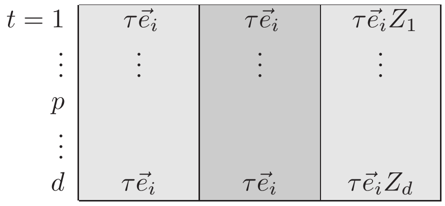


Experiment 2-p-1 ($\mathsf{Exp}^{2\text{-}p\text{-}1}_{\mathcal{B}}$**,** for $p = 1, \ldots, d$) : Experiment 2-0-8 is Experiment 1. Same as Experiment 2-$(p-1)$-8 except that

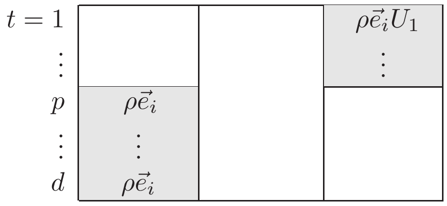
$$\left.\begin{array}{l} \text{for } t = 1, \ldots, d;\ i = 1, 2, \\ \boldsymbol{e}_{t,i} := (\ \overbrace{\sigma_{t,i}(1, t),\ \omega\vec{e}_i,}^{4}\ \ \overbrace{\tau\vec{e}_i,\ \boxed{\tau\vec{e}_i},\ \tau\vec{e}_i Z_t,}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_{t,i}}^{2}\ )_{\mathbb{B}}, \end{array}\right\} \tag{33}$$

where all the variables are generated as in Experiment 2-$(p-1)$-8.

Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 2-p-1



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



Experiment 2-p-2 $(\mathsf{Exp}_{\mathcal{B}}^{2\text{-}p\text{-}2}$**,** for $p=1,\ldots,d)$: Same as Experiment 2-p-1 except that

for $i=1,2$;

$$\boldsymbol{h}^*_{p,i} := (\ \overbrace{\mu_{p,i}(p,-1),\ \delta\vec{e}_i,}^{4}\ \overbrace{\boxed{(\rho-\theta_{p,i})\vec{e}_i,\ \theta_{p,i}\vec{e}_i},\ 0^2,}^{6}\ \overbrace{\vec{\eta}_{p,i},}^{2}\ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*}$$

where $\theta_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and all the other variables are generated as in Experiment 2-p-1.

Experiment 2-p-3 $(\mathsf{Exp}_{\mathcal{B}}^{2\text{-}p\text{-}3}$**,** for $p=1,\ldots,d)$: Same as Experiment 2-p-2 except that

for $i=1,2$;

$$\boldsymbol{h}^*_{p,i} := (\ \overbrace{\mu_{p,i}(p,-1),\ \delta\vec{e}_i,}^{4}\ \overbrace{\boxed{\theta_{p,i}\vec{e}_i,\ (\rho-\theta_{p,i})\vec{e}_i},\ 0^2,}^{6}\ \overbrace{\vec{\eta}_{p,i},}^{2}\ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*}$$

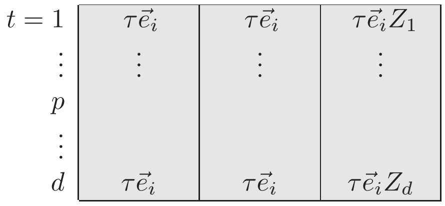
where all the variables are generated as in Experiment 2-p-2.

Experiment 2-p-4 $(\mathsf{Exp}_{\mathcal{B}}^{2\text{-}p\text{-}4}$**,** for $p=1,\ldots,d)$: Same as Experiment 2-p-3 except that

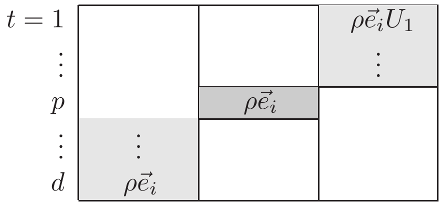
$$\text{for } i=1,2,\ \ \boldsymbol{h}^*_{p,i} := (\ \overbrace{\mu_{p,i}(p,-1),\ \delta\vec{e}_i,}^{4}\ \overbrace{\boxed{0^2,\ \rho\vec{e}_i},\ 0^2,}^{6}\ \overbrace{\vec{\eta}_{p,i},}^{2}\ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*},$$

where all the variables are generated as in Experiment 2-p-3.

Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 2-p-4



Coefficients of the hidden part of $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-4



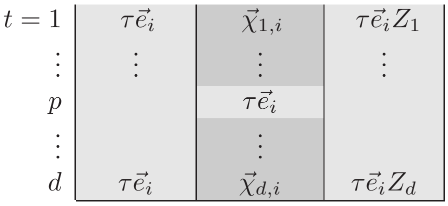
Experiment 2-p-5 $(\mathsf{Exp}_{\mathcal{B}}^{2\text{-}p\text{-}5}$**,** for $p=1,\ldots,d)$: Same as Experiment 2-p-4 except that

for $l=1,\ldots,p-1,p+1,\ldots,d$; $i=1,2$,

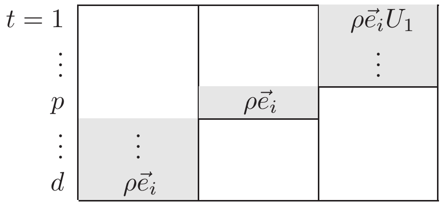
$$\boldsymbol{e}_{l,i} := (\ \overbrace{\sigma_{l,i}(1,l),\ \omega\vec{e}_i,}^{4}\ \overbrace{\tau\vec{e}_i,\ \boxed{\vec{\chi}_{l,i}},\ \tau\vec{e}_i Z_l,}^{6}\ \overbrace{0^2,}^{2}\ \overbrace{\vec{\varphi}_{l,i}}^{2}\ )_{\mathbb{B}}, \tag{34}$$

where $\vec{\chi}_{l,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, and all the other variables are generated as in Experiment 2-p-4.

Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 2-p-5



Coefficients of the hidden part of $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-5

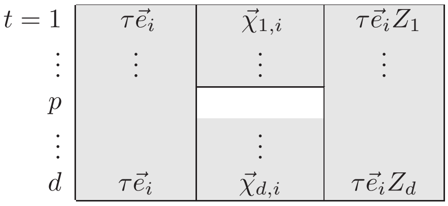


Experiment 2-p-6 ($\mathsf{Exp}^{2\text{-}p\text{-}6}_{\mathcal{B}}$**,** for $p = 1,\ldots,d$) : Same as Experiment 2-p-5 except that

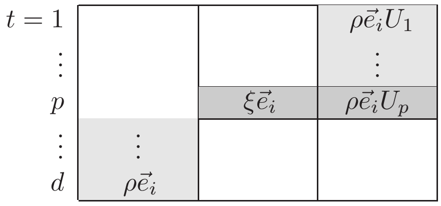
$$\begin{aligned}\text{for } i=1,2,\quad \boldsymbol{h}^*_{p,i} &:= (\overbrace{\mu_{p,i}(p,-1),\ \delta\vec{e}_i,}^{4}\ \overbrace{0^2,\ \boxed{\xi\vec{e}_i,\ \rho\vec{e}_iU_p},}^{6}\ \overbrace{\vec{\eta}_{p,i},}^{2}\ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*} \\ \boldsymbol{e}_{p,i} &:= (\sigma_{p,i}(1,p),\ \omega\vec{e}_i,\ \tau\vec{e}_i,\ \boxed{0^2},\ \tau\vec{e}_iZ_p,\ 0^2,\ \vec{\varphi}_{p,i}\ )_{\mathbb{B}},\end{aligned}$$

where $\xi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $Z_p \xleftarrow{\mathsf{U}} GL(2,\mathbb{F}_q)$, $U_p := (Z_p^{-1})^{\mathrm{T}}$, and all the other variables are generated as in Experiment 2-p-5.

Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 2-p-6



Coefficients of the hidden part of $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-6

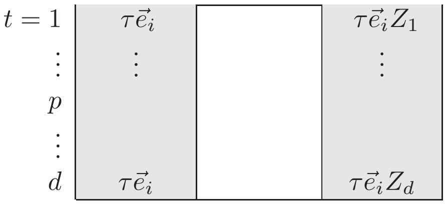


Experiment 2-p-7 ($\mathsf{Exp}^{2\text{-}p\text{-}7}_{\mathcal{B}}$**,** for $p = 1,\ldots,d$) : Same as Experiment 2-p-6 except that

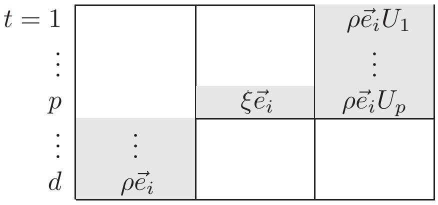
$$\text{for } l=1,\ldots,p-1,p+1,\ldots,d,\ i=1,2,$$
$$\boldsymbol{e}_{l,i} := (\overbrace{\sigma_{l,i}(1,l),\ \omega\vec{e}_i,}^{4}\ \overbrace{\tau\vec{e}_i,\ \boxed{0^2},\ \tau\vec{e}_iZ_l,}^{6}\ \overbrace{0^2,}^{2}\ \overbrace{\vec{\varphi}_{l,i}}^{2}\ )_{\mathbb{B}},$$

where all the variables are generated as in Experiment 2-p-6.

Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 2-p-7



Coefficients of the hidden part of $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-7



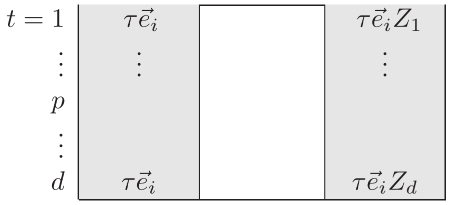
Experiment 2-p-8 ($\mathsf{Exp}^{2\text{-}p\text{-}8}_{\mathcal{B}}$**,** for $p = 1,\ldots,d$) : Same as Experiment 2-p-7 except that

$$\text{for } i=1,2,\quad \boldsymbol{h}^*_{p,i} := \ (\overbrace{\mu_{p,i}(p,-1),\ \delta\vec{e}_i,}^{4}\ \overbrace{0^2,\ \boxed{0^2},\ \rho\vec{e}_iU_p,}^{6}\ \overbrace{\vec{\eta}_{p,i},}^{2}\ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*}, \tag{35}$$

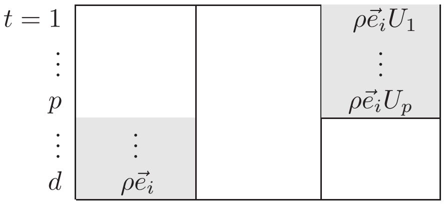
where all the variables are generated as in Experiment 2-p-7.

Experiment 2-8-d is the $\beta = 1$ case of Problem 2-ABE.

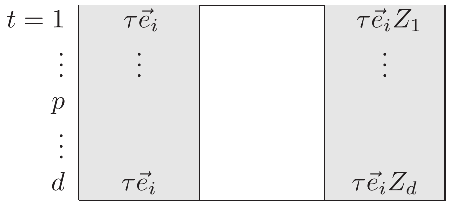
Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 2-p-8



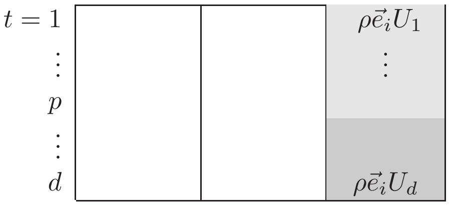
Coefficients of the hidden part of $\boldsymbol{h}^*_{t,i}$ in Experiment 2-p-8



Coefficients of the hidden part of $\boldsymbol{e}_{t,i}$ in Experiment 2-d-8



Coefficients of the hidden part of $\boldsymbol{h}^*_{t,i}$ in Experiment 2-d-8



Lemmas

Lemma 48 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_1$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\mathsf{Pr}[\mathsf{Exp}^{(0)}_{\mathcal{B}}(\lambda) \to 1] - \mathsf{Pr}[\mathsf{Exp}^{(1)}_{\mathcal{B}}(\lambda) \to 1]| \le \mathsf{Adv}^{\mathsf{BP2}}_{\mathcal{C}_1}(\lambda)$.*

Proof. Given a BP2 instance $(\mathsf{param}, \widehat{\mathbb{B}}_0, \mathbb{B}^*_0, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,2})$, $\mathcal{C}_1$ calculates

$$\begin{aligned}
&\boldsymbol{p}^*_{t,i} := \mu_{t,i}(t\boldsymbol{b}^*_1 - \boldsymbol{b}^*_2) + \boldsymbol{h}^*_{\beta,i} + \textstyle\sum_{j=1}^{2} \eta_{t,i,j}\boldsymbol{b}^*_{10+j},\\
&\boldsymbol{g}_0 := \boldsymbol{e}_0 + \varphi_0\boldsymbol{b}_{0,5}, \quad \boldsymbol{g}_{t,i} := \boldsymbol{e}_{t,i} + \tau\textstyle\sum_{j=1}^{2} z_{t,i,j}\boldsymbol{b}_{8+j} + \textstyle\sum_{j=1}^{2} \varphi_{t,i,j}\boldsymbol{b}_{12+j},\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{for } t = 1,\ldots,d,\ i = 1,2,
\end{aligned}$$

where $\mu_{t,i}, \eta_{t,i,1}, \eta_{t,i,2}, \varphi_0, \varphi_{t,i,1}, \varphi_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $(z_{t,i,j})_{i,j=1,2} := Z_t \xleftarrow{\mathsf{U}} GL(2,\mathbb{F}_q)$. $\mathcal{C}_1$ then sets $\widehat{\mathbb{B}}'_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}), \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \ldots, \boldsymbol{b}^*_{0,4}), \widehat{\mathbb{B}}' := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14}), \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_4, \boldsymbol{b}^*_{11}, \boldsymbol{b}^*_{12})$.

$\mathcal{C}_1$ then gives $\varrho := (\mathsf{param}, \widehat{\mathbb{B}}'_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}', \widehat{\mathbb{B}}^*, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{g}_0, \{\boldsymbol{p}^*_{t,i}, \boldsymbol{g}_{t,i}\}_{t=1,\ldots,d; i=1,2})$ to $\mathcal{B}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{B}$ outputs β'. If $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances in Experiment 0 (resp. Experiment 1). □

Lemma 49 *For any adversary $\mathcal{B}$, for any security parameter λ, $\mathsf{Pr}[\mathsf{Exp}^{(2\text{-}(p-1)\text{-}8)}_{\mathcal{B}}(\lambda) \to 1] = \mathsf{Pr}[\mathsf{Exp}^{(2\text{-}p\text{-}1)}_{\mathcal{B}}(\lambda) \to 1]$.*

Proof. If we set $\boldsymbol{d}_7 := \boldsymbol{b}_7 - \boldsymbol{b}_9$, $\boldsymbol{d}_8 := \boldsymbol{b}_8 - \boldsymbol{b}_{10}$, $\boldsymbol{d}^*_9 := \boldsymbol{b}^*_9 + \boldsymbol{b}^*_7$, $\boldsymbol{d}^*_{10} := \boldsymbol{b}^*_{10} + \boldsymbol{b}^*_8$, then $\mathbb{D} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6, \boldsymbol{d}_7, \boldsymbol{d}_8, \boldsymbol{b}_9, \ldots, \boldsymbol{b}_{14})$ and $\mathbb{D}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_8, \boldsymbol{d}^*_9, \boldsymbol{d}^*_{10}, \boldsymbol{b}^*_{11}, \ldots, \boldsymbol{b}^*_{14})$ are dual orthonormal bases. Moreover, $(\mathbb{D}, \mathbb{D}^*)$ are consistent with $(\widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$. Since

for $t = 1, \ldots, d;\ i = 1, 2,$

$$\begin{array}{rcccccl}
 & & \overbrace{\hphantom{\mu_{t,i}(t,-1),\ \delta\vec{e}_i,}}^{4} & \overbrace{\hphantom{\tau\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i Z_t,}}^{6} & \overbrace{\hphantom{\vec{\eta}_{t,i},}}^{2} & \overbrace{\hphantom{\vec{\varphi}_{t,i}}}^{2} & \\
\boldsymbol{h}^*_{t,i} = & (& \mu_{t,i}(t,-1),\ \delta\vec{e}_i, & \rho\vec{e}_i,\ 0^2,\ 0^2, & \vec{\eta}_{t,i}, & 0^2 &)_{\mathbb{B}^*} \\
= & (& \mu_{t,i}(t,-1),\ \delta\vec{e}_i, & \rho\vec{e}_i,\ 0^2,\ 0^2, & \vec{\eta}_{t,i}, & 0^2 &)_{\mathbb{D}^*} \\
\boldsymbol{e}_{t,i} = & (& \sigma_{t,i}(1,t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i Z_t, & 0^2, & \vec{\varphi}_{t,i} &)_{\mathbb{B}}, \\
= & (& \sigma_{t,i}(1,t),\ \omega\vec{e}_i, & \tau\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i Z_t, & 0^2, & \vec{\varphi}_{t,i} &)_{\mathbb{D}},
\end{array}$$

the distribution of the adversary's view for Experiment 2-($p-1$)-9 and that for Experiment 2-p-1 are equivalent. □

Lemma 50 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_{2\text{-}1}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\mathsf{Pr}[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}1)}(\lambda) \rightarrow 1] - \mathsf{Pr}[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}2)}(\lambda) \rightarrow 1]| \leq \mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}1}}^{\mathsf{BP3}\text{-}p}(\lambda)$, where $\mathcal{C}_{2\text{-}p\text{-}1}(\cdot) := \mathcal{C}_{2\text{-}1}(p, \cdot)$.*

Proof. Given an integer p and a BP3-p instance $(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{\beta,p,i}^*, \boldsymbol{e}_i, \boldsymbol{g}_i\}_{i=1,2})$, $\mathcal{C}_{2\text{-}1}$ generates $(z_{t,i,j})_{i,j=1,2} := Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $t = 1, \ldots, d$ and calculates $\boldsymbol{h}_0^*, \boldsymbol{h}_{t,i}^*$ $(t < p)$ as in Eq. (35) $\boldsymbol{h}_{t,i}^*$ $(t > p)$ as in Eq. (32) using $\mathbb{B}_0^*, \mathbb{B}^*$ and $\rho, \delta, \mu_{t,i}, \eta_{t,i,1}, \eta_{t,i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and (Z_t, U_t) for $t \neq p$. $\mathcal{C}_{2\text{-}1}$ then calculates

$$\boldsymbol{g}_0 := \boldsymbol{e}_0 + \omega \boldsymbol{b}_{0,1} + \varphi_0 \boldsymbol{b}_{0,5},$$
$$\boldsymbol{g}_{t,i} := \sigma_{t,i}(\boldsymbol{b}_1 + t\boldsymbol{b}_2) + \omega \boldsymbol{b}_{2+i} + \boldsymbol{e}_i + \textstyle\sum_{j=1}^{2} z_{t,i,j} \boldsymbol{g}_j + \sum_{j=1}^{2} \varphi_{t,i,j} \boldsymbol{b}_{12+j} \text{ for } t = 1, \ldots, d; i = 1, 2,$$
$$\boldsymbol{p}_{p,i}^* := \boldsymbol{h}_{\beta,p,i}^* + \delta \boldsymbol{b}_{2+i}^* + \rho \boldsymbol{b}_{6+i}^* \text{ for } i = 1, 2,$$

where $\omega, \varphi_0, \sigma_{t,i}, \varphi_{t,i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\mathcal{C}_{2\text{-}1}$ then sets $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$, $\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \ldots, \boldsymbol{b}_{0,4}^*)$, $\widehat{\mathbb{B}}' := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14})$, $\widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_4^*, \boldsymbol{b}_{11}^*, \boldsymbol{b}_{12}^*)$.

$\mathcal{C}_{2\text{-}1}$ then gives $\varrho := (\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}', \widehat{\mathbb{B}}^*, \boldsymbol{h}_0^*, \boldsymbol{g}_0, \{\boldsymbol{h}_{t,i}^*, \boldsymbol{p}_{p,i}^*\}_{t=1,\ldots,p-1,p+1,\ldots,d; i=1,2}, \{\boldsymbol{g}_{t,i}\}_{t=1,\ldots,d; i=1,2})$ to $\mathcal{B}$, and outputs $\beta' \in \{0, 1\}$ if $\mathcal{B}$ outputs β'. If $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances in Experiment 2-p-1 (resp. Experiment 2-p-2). □

Lemma 51 *For any adversary $\mathcal{B}$, for any security parameter λ,*
$\mathsf{Pr}[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}2)}(\lambda) \rightarrow 1] = \mathsf{Pr}[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}3)}(\lambda) \rightarrow 1]$.

Proof. Because the distribution $(\rho - \theta_{p,i}, \theta_{p,i})$, where $\rho, \theta_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, is equivalent to the distribution $(\theta_{p,i}, \rho - \theta_{p,i})$, where $\rho, \theta_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$. □

Lemma 52 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_{2\text{-}2}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\mathsf{Pr}[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}3)}(\lambda) \rightarrow 1] - |\mathsf{Pr}[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}4)}(\lambda) \rightarrow 1]| \leq \mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}2}}^{\mathsf{BP3}\text{-}p}(\lambda)$, where $\mathcal{C}_{2\text{-}p\text{-}2}(\cdot) := \mathcal{C}_{2\text{-}2}(p, \cdot)$.*

Lemma 52 is proven in a similar manner to Lemma 50.

Lemma 53 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_{2\text{-}3}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\mathsf{Pr}[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}4)}(\lambda) \rightarrow 1] - \mathsf{Pr}[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}5)}(\lambda) \rightarrow 1]| \leq \mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}3}}^{\mathsf{BP5}\text{-}p}(\lambda)$, where $\mathcal{C}_{2\text{-}p\text{-}3}(\cdot) := \mathcal{C}_{2\text{-}3}(p, \cdot)$.*

Proof. Given an integer p and a BP5-p instance

$$(\mathsf{param}, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \widetilde{\mathbb{B}}^*, \boldsymbol{h}_0^*, \{\boldsymbol{h}_{p,i}^*, \boldsymbol{e}_{\beta,l,i}\}_{l=1,\ldots,p-1,p+1,\ldots,d;\; i=1,2}, \{\widetilde{\boldsymbol{h}}_j\}_{j=5,6,9,10}),$$

$\mathcal{C}_{2\text{-}3}$ calculates $\boldsymbol{e}_0 := (\omega, \tau, 0, 0, \varphi_0)_{\mathbb{B}_0}$ using $\mathbb{B}_0$ and $\omega, \tau, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\mathcal{C}_{2\text{-}3}$ then calculates

$$\text{for } t = 1, \ldots, d; i = 1, 2; \quad \delta, \tau, \eta_0, \mu_{t,i}, \sigma_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\eta}_{t,i}, \vec{\varphi}_{p,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2,$$
$$U_t := (u_{t,i,j})_{i,j=1,2} \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q), \quad Z_t := (z_{t,i,j})_{i,j=1,2} := (U_t^{-1})^{\mathrm{T}},$$
$$\boldsymbol{p}_0^* := \boldsymbol{h}_0^* + (\ \delta,\ 0,\ 0,\ \eta_0,\ 0\ )_{\mathbb{B}_0^*},$$
$$\text{if } t < p, \quad \boldsymbol{p}_{t,i}^* := \textstyle\sum_{j=1,2} u_{t,i,j} \widetilde{\boldsymbol{h}}_{4+j}^* + (\ \mu_{t,i}(t,\ -1),\ \delta\vec{e}_i,\ 0^6,\ \vec{\eta}_{t,i},\ 0^2\ )_{\mathbb{B}^*},$$
$$\text{if } t = p, \quad \boldsymbol{p}_{p,i}^* := \textstyle\sum_{j=1,2} u_{p,i,j} \boldsymbol{h}_{p,j}^* + (\ 0^2,\ \delta\vec{e}_i,\ 0^{10}\ )_{\mathbb{B}^*},$$
$$\text{if } t > p, \quad \boldsymbol{p}_{t,i}^* := \textstyle\sum_{j=1,2} u_{t,i,j} \widetilde{\boldsymbol{h}}_{8+j}^* + (\ \mu_{t,i}(t,\ -1),\ \delta\vec{e}_i,\ 0^6,\ \vec{\eta}_{t,i},\ 0^2\ )_{\mathbb{B}^*},$$

$$\begin{aligned} &\text{if } t \neq p,\ \ \boldsymbol{g}_{t,i} := \boldsymbol{e}_{\beta,t,i} + (\ 0^2,\ \delta\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i Z_t,\ 0^4\ )_{\mathbb{B}}, \\ &\text{if } t = p,\ \ \boldsymbol{g}_{p,i} := (\ \sigma_{p,i}(1,\ p),\ \delta\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i Z_p,\ 0^2,\ \vec{\varphi}_{p,i}\ )_{\mathbb{B}}. \end{aligned}$$

$\mathcal{C}_{2\text{-}3}$ then sets $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}), \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \ldots, \boldsymbol{b}^*_{0,4}), \widehat{\mathbb{B}}' := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14}), \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_4, \boldsymbol{b}^*_{11}, \boldsymbol{b}^*_{12})$.

$\mathcal{C}_{2\text{-}3}$ then gives $\varrho := (\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}', \widehat{\mathbb{B}}^*, \boldsymbol{p}^*_0, \boldsymbol{e}_0, \{\boldsymbol{p}^*_{t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=1,2})$ to $\mathcal{B}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{B}$ outputs β'. If $\beta = 0$ (resp. $\beta = 1$), the distribution of ϱ is exactly same as that of instances in Experiment 2-p-4 (resp. Experiment 2-p-5). □

Lemma 54 *For any adversary $\mathcal{B}$, for any security parameter λ,* $\Pr[\mathsf{Exp}^{(2\text{-}p\text{-}5)}_{\mathcal{B}}(\lambda) \to 1] = \Pr[\mathsf{Exp}^{(2\text{-}p\text{-}6)}_{\mathcal{B}}(\lambda) \to 1]$.

Proof. To prove Lemma 54, we will show distribution $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{e}_{t,j}, \boldsymbol{h}^*_{t,j}\}_{t=1,\ldots,d;j=1,2})$ in Experiment 2-p-5 and that in Experiment 2-p-6 are equivalent. For that purpose, we define new dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ as follows: We generate $\widetilde{\xi} \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, Z_p \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q), U_p := (Z_p^{-1})^{\mathrm{T}}$ and set

$$\begin{pmatrix} \boldsymbol{d}^*_7 \\ \boldsymbol{d}^*_8 \\ \boldsymbol{d}^*_9 \\ \boldsymbol{d}^*_{10} \end{pmatrix} := \begin{pmatrix} \widetilde{\xi} I_2 & -U_p \\ 0_2 & I_2 \end{pmatrix} \begin{pmatrix} \boldsymbol{b}^*_7 \\ \boldsymbol{b}^*_8 \\ \boldsymbol{b}^*_9 \\ \boldsymbol{b}^*_{10} \end{pmatrix}, \quad \begin{pmatrix} \boldsymbol{d}_7 \\ \boldsymbol{d}_8 \\ \boldsymbol{d}_9 \\ \boldsymbol{d}_{10} \end{pmatrix} := \begin{pmatrix} \widetilde{\xi}^{-1} I_2 & 0_2 \\ \widetilde{\xi}^{-1} Z_p^{-1} & I_2 \end{pmatrix} \begin{pmatrix} \boldsymbol{b}_7 \\ \boldsymbol{b}_8 \\ \boldsymbol{b}_9 \\ \boldsymbol{b}_{10} \end{pmatrix},$$

$$\begin{aligned} \mathbb{D} &:= (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6, \boldsymbol{d}_7, \ldots, \boldsymbol{d}_{10}, \boldsymbol{b}_{11}, \ldots, \boldsymbol{b}_{14}), \\ \mathbb{D}^* &:= (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_6, \boldsymbol{d}^*_7, \ldots, \boldsymbol{d}^*_{10}, \boldsymbol{b}^*_{11}, \ldots, \boldsymbol{b}^*_{14}), \end{aligned}$$

where I_2 is the 2×2 identity matrix. We then easily verify that $\mathbb{D}$ and $\mathbb{D}^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}$ and $\mathbb{B}^*$. Keys and ciphertexts $(\{\boldsymbol{e}_{t,j}, \boldsymbol{h}^*_{t,j}\}_{t=1,\ldots,d;j=1,2})$ in Experiment 2-p-5 are expressed over bases $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ as

for $t = 1, \ldots, p-1; j = 1, 2,$

$$\begin{aligned} \boldsymbol{h}^*_{t,j} &= (\ \overbrace{\mu_{t,j}(t,-1),\ \delta\vec{e}_j,}^{4}\ \ \overbrace{0^4,\ \rho\vec{e}_j U_t,}^{6}\ \ \overbrace{\vec{\eta}_{t,j},}^{2}\ \ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*} \\ &= (\ \mu_{t,j}(t,-1),\ \delta\vec{e}_j,\ \ 0^4,\ \rho\vec{e}_j U_t,\ \ \vec{\eta}_{t,j},\ \ 0^2\ )_{\mathbb{D}^*} \end{aligned}$$

for $t = p;\ j = 1, 2,$

$$\begin{aligned} \boldsymbol{h}^*_{p,j} &= (\ \overbrace{\mu_{p,j}(p,-1),\ \delta\vec{e}_j,}^{4}\ \ \overbrace{0^2,\ \rho\vec{e}_j,\ 0^2,}^{6}\ \ \overbrace{\vec{\eta}_{p,j},}^{2}\ \ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*} \\ &= (\ \mu_{p,j}(p,-1),\ \delta\vec{e}_j,\ \ 0^2,\ \xi\vec{e}_j,\ \rho\vec{e}_j U_p,\ \ \vec{\eta}_{p,j},\ \ 0^2\ )_{\mathbb{D}^*} \end{aligned}$$

where $\xi := \widetilde{\xi}\rho$,

for $t = p+1, \ldots, d; j = 1, 2,$

$$\begin{aligned} \boldsymbol{h}^*_{t,j} &= (\ \overbrace{\mu_{t,j}(t,-1),\ \delta\vec{e}_j,}^{4}\ \ \overbrace{\rho\vec{e}_j,\ \ 0^4,}^{6}\ \ \overbrace{\vec{\eta}_{t,j},}^{2}\ \ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*} \\ &= (\ \mu_{t,j}(t,-1),\ \delta\vec{e}_j,\ \ \rho\vec{e}_j,\ \ 0^4,\ \ \vec{\eta}_{t,j},\ \ 0^2\ )_{\mathbb{D}^*} \end{aligned}$$

for $t = 1, \ldots, p-1, p+1, \ldots, d;\ j = 1, 2,$

$$\begin{aligned} \boldsymbol{e}_{t,j} &= (\ \overbrace{\sigma_{t,j}(1,t),\ \omega\vec{e}_j,}^{4}\ \ \overbrace{\tau\vec{e}_j,\ \vec{\chi}_{t,j},\ \tau\vec{e}_j Z_t,}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\vec{\varphi}_{t,j}}^{2}\ )_{\mathbb{B}}, \\ &= (\ \sigma_{t,j}(1,t),\ \omega\vec{e}_j,\ \ \tau\vec{e}_j,\ \vec{\chi}'_{t,j},\ \tau\vec{e}_j Z_t,\ \ 0^2,\ \ \vec{\varphi}_{t,j}\ )_{\mathbb{D}}, \end{aligned}$$

where $\vec{\chi}'_{t,j} := \widetilde{\xi}^{-1}\left(\vec{\chi}_{t,j} - \tau\vec{e}_j \cdot Z_t Z_p^{-1}\right)$, for $t = p$; $j = 1, 2$,

$$\begin{array}{rlllll} \boldsymbol{e}_{p,j} = (& \overbrace{\sigma_{p,j}(1,p),\ \omega\vec{e}_j,}^{4} & \overbrace{\tau\vec{e}_j,\ \tau\vec{e}_j,\ \tau\vec{e}_j Z_p,}^{6} & \overbrace{0^2,}^{2} & \overbrace{\vec{\varphi}_{p,j}}^{2} &)_{\mathbb{B}}, \\ = (& \sigma_{p,j}(1,p),\ \omega\vec{e}_j, & \tau\vec{e}_j,\ 0^2,\ \tau\vec{e}_j U_p, & 0^2, & \vec{\varphi}_{p,j} &)_{\mathbb{D}}, \end{array}$$

where $\vec{\chi}'_{t,j}$ are uniformly, independently distributed since $\vec{\chi}_{t,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ $(t \neq p)$.

In the light of the adversary's view, both $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ are consistent with public key $\mathsf{pk} := (\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$. Therefore, $\{\boldsymbol{e}_{t,j}, \boldsymbol{h}^*_{t,j}\}_{t=1,\ldots,d;\ j=1,2}$ can be expressed as keys and ciphertext in two ways, in Experiment 2-p-5 over bases $(\mathbb{B}, \mathbb{B}^*)$ and in Experiment 2-p-6 over bases $(\mathbb{D}, \mathbb{D}^*)$. Thus, Experiment 2-$p$-5 can be conceptually changed to Experiment 2-p-6. □

Lemma 55 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_{2\text{-}4}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\Pr[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}6)}(\lambda) \to 1] - \Pr[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}7)}(\lambda) \to 1]| \leq \mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}4}}^{\mathsf{BP5}\text{-}p}(\lambda)$, where $\mathcal{C}_{2\text{-}p\text{-}4}(\cdot) := \mathcal{C}_{2\text{-}4}(p, \cdot)$.*

Lemma 55 is proven in a similar manner to Lemma 53.

Lemma 56 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{C}_{2\text{-}5}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $|\Pr[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}7)}(\lambda) \to 1] - \Pr[\mathsf{Exp}_{\mathcal{B}}^{(2\text{-}p\text{-}8)}(\lambda) \to 1]| \leq \mathsf{Adv}_{\mathcal{C}_{2\text{-}p\text{-}5}}^{\mathsf{BP4}\text{-}p}(\lambda)$, where $\mathcal{C}_{2\text{-}p\text{-}5}(\cdot) := \mathcal{C}_{2\text{-}5}(p, \cdot)$.*

Lemma 56 is proven in a similar manner to Lemma 53.

A.5 Proofs of Lemmas 25–29 in Section 6.1.4

Lemma 25 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1\text{-}ABE}}(\lambda)$.*

Proof. In order to prove Lemma 25, we construct a probabilistic machine $\mathcal{B}_1$ against Problem 1-ABE using an adversary $\mathcal{A}$ in a security game (Game 0 or 1) as a black box as follows:

1. $\mathcal{B}_1$ is given a Problem 1-ABE instance, $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,j}\}_{t=1,\ldots,d;j=1,2})$.

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

3. At the first step of the game, $\mathcal{B}_1$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$ of Game 0 (and 1), where $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14})$ for $t = 1, .., d$.

4. When a key query is issued for access structure $\mathbb{S} := (M, \rho)$, $\mathcal{B}_1$ answers normal key $(\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_\ell^*)$ with Eq. (18), that is computed using $\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*$ of the Problem 1-ABE instance.

5. When $\mathcal{B}_1$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{(t, x_t) \mid 1 \leq t \leq d\}$ from $\mathcal{A}$, $\mathcal{B}_1$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}, c_{d+1})$ such that

$$\boldsymbol{c}_0 := \boldsymbol{e}_{\beta,0} + \zeta \boldsymbol{b}_{0,3}, \qquad \boldsymbol{c}_t := \boldsymbol{e}_{\beta,t,1} + x_t \boldsymbol{e}_{\beta,t,2}, \qquad c_{d+1} := g_T^{\zeta} m^{(b)},$$

   where $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\boldsymbol{b}_{0,3}, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,j}\}_{t=1,\ldots,d;j=1,2})$ is a part of the Problem 1-ABE instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_1$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_1$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_1$ outputs $\beta' := 0$.

It is straightforward that the distribution by $\mathcal{B}_1$'s simulation given a Problem 1-ABE instance with β is equivalent to that in Game 0 (resp. Game 1), when $\beta = 0$ (resp. $\beta = 1$). □

Lemma 26 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}1}}^{\mathsf{P2\text{-}ABE}}(\lambda) + 2/q$, where $\mathcal{B}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{2\text{-}1}(h, \cdot)$.*

Proof. In order to prove Lemma 26, we construct a probabilistic machine $\mathcal{B}_{2\text{-}1}$ against Problem 2-ABE using an adversary $\mathcal{A}$ in a security game (Game 2-$(h-1)$-3 or 2-h-1) as a black box as follows:

1. $\mathcal{B}_{2\text{-}1}$ is given an integer h and a Problem 2-ABE instance, $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\boldsymbol{h}_{\beta,t,j}^*, \boldsymbol{e}_{t,j}\}_{t=1,\dots,d; j=1,2})$.

2. $\mathcal{B}_{2\text{-}1}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. At the first step of the game, $\mathcal{B}_{2\text{-}1}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$ of Game 2-$(h-1)$-3 (and 2-h-1), where $\widehat{\mathbb{B}}_0$ and $\widehat{\mathbb{B}}$ are obtained from the Problem 2-ABE instance.

4. When the ι-th key query is issued for access structure $\mathbb{S} := (M, \rho)$, $\mathcal{B}_{2\text{-}1}$ answers as follows:

   (a) When $1 \leq \iota \leq h-1$, $\mathcal{B}_{2\text{-}1}$ answers semi-functional key $(\boldsymbol{k}_0^*, \dots, \boldsymbol{k}_\ell^*)$ with Eq. (23), that is computed using $\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*$ of the Problem 2-ABE instance.

   (b) When $\iota = h$, $\mathcal{B}_{2\text{-}1}$ calculates $(\boldsymbol{k}_0^*, \dots, \boldsymbol{k}_\ell^*)$ using $(\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{h}_{\beta,0}^*, \{\boldsymbol{b}_j^*, \boldsymbol{h}_{\beta,t,j}^*\}_{t=1,\dots,d; j=1,2})$ of the Problem 2-ABE instance as follows:

$$\begin{aligned}
&\widetilde{\pi}_t, \xi_t, \widetilde{g}_k, \widetilde{\xi}_k \xleftarrow{\mathsf{U}} \mathbb{F}_q \quad \text{for } t = 1, \dots, d;\ k = 1, \dots, r, \\
&\text{for } k = 1, \dots, r, \quad \widetilde{\boldsymbol{p}}_{\beta,0,k}^* := \widetilde{g}_k \boldsymbol{h}_{\beta,0}^* + \widetilde{\xi}_k \boldsymbol{b}_{0,1}^*, \\
&\text{for } t = 1, \dots, d;\ k = 1, \dots, r;\ j = 1, 2; \\
&\quad \boldsymbol{p}_{\beta,t,j}^* := \widetilde{\pi}_t \boldsymbol{h}_{\beta,t,j}^* + \xi_t \boldsymbol{b}_{2+j}^*, \qquad \widetilde{\boldsymbol{p}}_{\beta,t,k,j}^* := \widetilde{g}_k \boldsymbol{h}_{\beta,t,j}^* + \widetilde{\xi}_k \boldsymbol{b}_{2+j}^*, \\
&\boldsymbol{k}_0^* := -\textstyle\sum_{k=1}^r \widetilde{\boldsymbol{p}}_{\beta,0,k}^* + \boldsymbol{b}_{0,3}^*, \\
&\text{for } i = 1, \dots, \ell, \\
&\quad \text{if } \rho(i) = (t, v_i), \quad \boldsymbol{k}_i^* := v_i \boldsymbol{p}_{\beta,t,1}^* - \boldsymbol{p}_{\beta,t,2}^* + \textstyle\sum_{k=1}^r M_{i,k} \widetilde{\boldsymbol{p}}_{\beta,t,k,1}^*, \\
&\quad \text{if } \rho(i) = \neg(t, v_i), \quad \boldsymbol{k}_i^* := \textstyle\sum_{k=1}^r M_{i,k} (v_i \widetilde{\boldsymbol{p}}_{\beta,t,k,1}^* - \widetilde{\boldsymbol{p}}_{\beta,t,k,2}^*),
\end{aligned}$$

   where $(M_{i,k})_{i=1,\dots,\ell; k=1,\dots,r} := M$.

   (c) When $\iota \geq h+1$, $\mathcal{B}_{2\text{-}1}$ answers normal key $(\boldsymbol{k}_0^*, \dots, \boldsymbol{k}_\ell^*)$ with Eq. (18), that is computed using $\widehat{\mathbb{B}}_0^*, \widehat{\mathbb{B}}^*$ of the Problem 2-ABE instance.

5. When $\mathcal{B}_{2\text{-}1}$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{(t, x_t) \mid 1 \leq t \leq d\}$ from $\mathcal{A}$, $\mathcal{B}_{2\text{-}1}$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,x_t) \in \Gamma}, c_{d+1})$ such that for $(t, x_t) \in \Gamma$,

$$\boldsymbol{c}_0 := \boldsymbol{e}_0 + \zeta \boldsymbol{b}_{0,3} + \boldsymbol{q}_0, \qquad \boldsymbol{c}_t := \boldsymbol{e}_{t,1} + x_t \boldsymbol{e}_{t,2} + \boldsymbol{q}_t, \qquad c_{d+1} := g_T^\zeta m^{(b)},$$

where $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, $\boldsymbol{q}_0 \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{0,5}\rangle$, $\boldsymbol{q}_t \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{13}, \boldsymbol{b}_{14}\rangle$, and $(\boldsymbol{b}_{0,3}, \boldsymbol{e}_0, \{\boldsymbol{e}_{t,j}\}_{t=1,..,d;j=1,2})$ is a part of the Problem 2-ABE instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_{2\text{-}1}$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{2\text{-}1}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{2\text{-}1}$ outputs $\beta' := 0$.

Claim 7 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_{2\text{-}1}$ given a Problem 2-ABE instance with $\beta \in \{0,1\}$ is the same as that in Game 2-$(h-1)$-3 (resp. Game 2-h-1) if $\beta = 0$ (resp. $\beta = 1$) except with probability $1/q$ (resp. $1/q$).*

Proof. It is straightforward that the distribution by $\mathcal{B}_{2\text{-}1}$'s simulation given a Problem 2-ABE instance with $\beta = 0$ is equivalent to that in Game 2-$(h-1)$-3 except that δ defined in Problem 2-ABE is zero, i.e., except with probability $1/q$.

When $\beta = 1$, the challenge ciphertext in the above simulation is given as:

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

for $(t, x_t) \in \Gamma$,

$$\boldsymbol{c}_t := (\ \overbrace{\widetilde{\sigma}_t(1,\ t),\ \omega(1,\ x_t),}^{4}\ \ \overbrace{\tau(1,x_t),\ 0^2,\ \tau(1,\ x_t)\cdot Z_t,}^{6}\ \ \overbrace{0^2,}^{2}\ \ \overbrace{\widetilde{\varphi}_{t,1}, \widetilde{\varphi}_{t,2}}^{2}\ \ )_{\mathbb{B}},$$

where $\widetilde{\sigma}_t := \sigma_{t,1} + x_t\sigma_{t,2}, \widetilde{\varphi}_{t,j} := \varphi_{t,1,j} + x_t\varphi_{t,2,j}$ for $j = 1,2$, $\omega, \tau, \{\sigma_{t,j}, \varphi_{t,i,j}\}_{(t,x_t)\in\Gamma, i,j=1,2}$ are defined in Problem 2-ABE.

$\widetilde{\boldsymbol{p}}^*_{\beta,0}, \boldsymbol{p}^*_{\beta,t,j}, \widetilde{\boldsymbol{p}}^*_{\beta,t,k,j}$ for $t = 1,\ldots,d; k = 1,\ldots,r; j = 1,2$ calculated in case (b) of steps 4 and 6 in the above simulation are expressed as:

$$\theta_t := \widetilde{\pi}_t\delta + \xi_t, \quad f_k := \widetilde{g}_k\delta + \widetilde{\xi}_k, \quad \pi_t := \widetilde{\pi}_t\rho, \quad g_k := \widetilde{g}_k\rho,$$
$$\widetilde{\boldsymbol{p}}^*_{0,0,k} = (f_k, 0, 0, \widetilde{g}_k\eta_0, 0)_{\mathbb{B}_0^*}, \quad \widetilde{\boldsymbol{p}}^*_{1,0,k} = (f_k, g_k, 0, \widetilde{g}_k\eta_0, 0)_{\mathbb{B}_0^*},$$

$$\begin{array}{lcccccc}
 & & \overbrace{\hphantom{\widetilde{\pi}_t\mu_{t,j}(t,\ -1),\ \theta_t\vec{e}_j,}}^{4} & \overbrace{\hphantom{0^4,\ g_k\vec{e}_jU_t,}}^{6} & \overbrace{\hphantom{\widetilde{g}_k(\eta_{t,j,1}, \eta_{t,j,2}),}}^{2} & \overbrace{\hphantom{0^2}}^{2} & \\
\boldsymbol{p}^*_{0,t,j} := & (& \widetilde{\pi}_t\mu_{t,j}(t,\ -1),\ \theta_t\vec{e}_j, & 0^6, & \widetilde{\pi}_t(\eta_{t,j,1}, \eta_{t,j,2}), & 0^2 &)_{\mathbb{B}_t^*}, \\
\widetilde{\boldsymbol{p}}^*_{0,t,k,j} := & (& \widetilde{g}_k\mu_{t,j}(t,\ -1),\ f_k\vec{e}_j, & 0^6, & \widetilde{g}_k(\eta_{t,j,1}, \eta_{t,j,2}), & 0^2 &)_{\mathbb{B}_t^*}, \\
\boldsymbol{p}^*_{1,t,j} := & (& \widetilde{\pi}_t\mu_{t,j}(t,\ -1),\ \theta_t\vec{e}_j, & 0^4,\ \pi_t\vec{e}_jU_t & \widetilde{\pi}_t(\eta_{t,j,1}, \eta_{t,j,2}), & 0^2 &)_{\mathbb{B}_t^*}, \\
\widetilde{\boldsymbol{p}}^*_{1,t,k,j} := & (& \widetilde{g}_k\mu_{t,j}(t,\ -1),\ f_k\vec{e}_j, & 0^4,\ g_k\vec{e}_jU_t, & \widetilde{g}_k(\eta_{t,j,1}, \eta_{t,j,2}), & 0^2 &)_{\mathbb{B}_t^*},
\end{array}$$

where $\delta, \rho, \eta_0, \{\mu_{t,j}, U_t, \eta_{t,j,1}, \eta_{t,j,2}\}_{t=1,\ldots,d;j=1,2}$ are defined in Problem 2-ABE and $\vec{e}_1 := (1,0), \vec{e}_2 := (0,1)$. Therefore, $\{\boldsymbol{k}^*_i\}_{i=0,\ldots,\ell}$ are expressed as:

$$\vec{f} := (f_1,\ldots,f_r), \quad s_0 := \vec{1}\cdot\vec{f}^{\mathrm{T}}, \quad (s_1,\ldots,s_\ell)^{\mathrm{T}} := M\cdot\vec{f}^{\mathrm{T}},$$
$$\vec{g} := (g_1,\ldots,g_r), \quad a_0 := \vec{1}\cdot\vec{g}^{\mathrm{T}}, \quad (a_1,\ldots,a_\ell)^{\mathrm{T}} := M\cdot\vec{g}^{\mathrm{T}},$$
if $\beta = 0$, $\widetilde{\boldsymbol{k}}^*_0 = (-s_0, 0, 1, -a_0\eta_0, 0)_{\mathbb{B}_0^*}$, if $\beta = 1$, $\widetilde{\boldsymbol{k}}^*_0 = (-s_0, -a_0, 1, -a_0\eta_0, 0)_{\mathbb{B}_0^*}$,

if $\beta = 0$,

if $\rho(i) = (t, v_i)$,

$$\boldsymbol{k}^*_i := (\ \overbrace{\widetilde{\mu}_i(t,\ -1),\ s_i + \theta_t v_i, -\theta_t,}^{4}\ \ \overbrace{0^6,}^{6}\ \ \overbrace{\kappa_{i,1}, \kappa_{i,2},}^{2}\ \ \overbrace{0^2}^{2}\ \ )_{\mathbb{B}_t^*},$$

if $\rho(i) = \neg(t, v_i)$,

$$\boldsymbol{k}^*_i := (\ \widetilde{\mu}_i(t,\ -1),\ s_i(v_i, -1),\ \ 0^6,\ \ \kappa_{i,1}, \kappa_{i,2},\ \ 0^2\ \ )_{\mathbb{B}_t^*},$$

if $\beta = 1$,
if $\rho(i) = (t, v_i)$,
$\boldsymbol{k}_i^* := (\ \widetilde{\mu}_i(t, \ -1), \ s_i + \theta_t v_i, -\theta_t, \ \ 0^4, \ (a_i + \pi_t v_i, -\pi_t) \cdot U_t, \ \ \kappa_{i,1}, \kappa_{i,2}, \ \ 0^2 \ \ )_{\mathbb{B}_t^*}$,
if $\rho(i) = \neg(t, v_i)$,
$\boldsymbol{k}_i^* := (\ \ \widetilde{\mu}_i(t, \ -1), \ s_i(v_i, -1), \ \ \ \ 0^4, \ a_i(v_i, -1) \cdot U_t, \ \ \ \kappa_{i,1}, \kappa_{i,2}, \ \ 0^2 \ \ )_{\mathbb{B}_t^*}$,

where $\widetilde{\mu}_i := (v_i \widetilde{\pi}_t + \sum_{k=1}^{r} M_{i,k} \widetilde{g}_k)\mu_{t,1} - \widetilde{\pi}_t \mu_{t,2}, \kappa_{i,j} := (v_i \widetilde{\pi}_t + \sum_{k=1}^{r} M_{i,k} \widetilde{g}_k)\eta_{t,1,j} - \widetilde{\pi}_t \eta_{t,1,j}$ for $j = 1, 2$ if $\rho(i) = (t, v_i)$, $\widetilde{\mu}_i := (\sum_{k=1}^{r} M_{i,k} \widetilde{g}_k)(v_i \mu_{t,1} - \mu_{t,2}), \kappa_{i,j} := (\sum_{k=1}^{r} M_{i,k} \widetilde{g}_k)(v_i \eta_{t,1,j} - \mu_{t,2,j})$ for $j = 1, 2$ if $\rho(i) = \neg(t, v_i)$. Therefore, variables $\{\theta_t, \pi_t\}_{t=1,\ldots,d}, \{f_k, g_k\}_{k=1,\ldots,r}, \{\widetilde{\mu}_i, \kappa_{i,j}\}_{i=1,\ldots,\ell; j=1,2}$ are independently and uniformly distributed. Therefore, $\{\boldsymbol{k}_i^*\}_{i=0,\ldots,\ell}$ and $\{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}$ are distributed as in Eqs. (20), (21) and (19). Therefore, when $\beta = 1$, the distribution by $\mathcal{B}_{2\text{-}1}$'s simulation is equivalent to that in Game 2-h-1 except that δ defined in Problem 2-ABE is zero, i.e., except with probability $1/q$. □

This completes the proof of Lemma 26. □

Lemma 27 *For any adversary $\mathcal{A}$, for any security parameter λ,* $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)$.

Proof. It is clear that the distribution of the public-key and the ι-th key query's answer for $\iota \neq h$ in Game 2-h-1 and Game 2-h-2 are exactly the same. Therefore, to prove this lemma we will show that the joint distribution of the h-th key query's answer and the challenge ciphertext in Game 2-h-1 and Game 2-h-2 are equivalent.

Therefore, we will show that a_0 in Eq. (20) is uniformly and independently distributed from the other variables in the joint distribution of adversary $\mathcal{A}$'s view. Since $a_0 := \vec{1} \cdot \vec{g}^{\mathrm{T}}$ is only related to $(a_1, \ldots, a_\ell)^{\mathrm{T}} := M \cdot \vec{g}^{\mathrm{T}}$ and $U_t = (Z_t^{-1})^{\mathrm{T}}$ holds, a_0 is only related to $\{\vec{w}_i\}_{i=1,\ldots,\ell}$, $\{\vec{\vec{w}}_i\}_{i=1,\ldots,\ell}$ and $\{\vec{r}_t\}_{t=1,\ldots,d}$, where $\vec{w}_i := (a_i + \pi_i v_i, -\pi_i) \cdot U_t$ and $\vec{\vec{w}}_i := a_i(v_i, -1) \cdot U_t$ in Eq. (21) for $i = 1, \ldots, \ell$, and $\vec{r}_t := \tau(1, x_t) \cdot Z_t$ in Eq. (19) for $t = 1, \ldots, d$ with $t := \widetilde{\rho}(i)$. ($\widetilde{\rho}$ is defined at the start of Section 6.1.) With respect to the joint distribution of these variables, there are five cases for each $i \in \{1, \ldots, \ell\}$. Note that for any $i \in \{1, \ldots, \ell\}$, (Z_t, U_t) with $t := \widetilde{\rho}(i)$ is independent from the other variables, since $\widetilde{\rho}$ is injective:

1. $\gamma(i) = 1$ and $[\rho(i) = (t, v_i) \ \wedge \ (t, x_t) \in \Gamma \ \wedge \ v_i = x_t]$.

   Then, from Lemma 8, the joint distribution of $(\vec{w}_i, \vec{r}_t)$ is uniformly and independently distributed on $C_{\tau a_i} := \{(\vec{w}, \vec{r}) | \vec{w} \cdot \vec{r} = \tau a_i\}$ (over $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$).

2. $\gamma(i) = 1$ and $[\rho(i) = \neg(t, v_i) \ \wedge \ (t, x_t) \in \Gamma \ \wedge \ v_i \neq x_t]$.

   Then, from Lemma 8, the joint distribution of $(\vec{\vec{w}}_i, \vec{r}_t)$ is uniformly and independently distributed on $C_{(v_i - x_t)\cdot \tau a_i}$ (over $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$).

3. $\gamma(i) = 0$ and $[\rho(i) = (t, v_i) \ \wedge \ (t, x_t) \in \Gamma]$ (i.e., $v_i \neq x_t$).

   Then, from Lemma 8, the joint distribution of $(\vec{w}_i, \vec{r}_t)$ is uniformly and independently distributed on $C_{\tau((v_i - x_t)\cdot \pi_t + a_i)}$ (over $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$). Since π_t is uniformly and independently distributed on $\mathbb{F}_q$, the joint distribution of $(\vec{w}_i, \vec{r}_t)$ is uniformly and independently distributed over $\mathbb{F}_q^4$.

4. $\gamma(i) = 0$ and $[\rho(i) = \neg(t, v_i) \ \wedge \ (t, x_t) \in \Gamma]$ (i.e., $v_i = x_t$).

   Then, from Lemma 8, the joint distribution of $(\vec{\vec{w}}_i, \vec{r}_t)$ is uniformly and independently distributed on C_0 (over $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$).

5. $[\rho(i) = (t, v_i) \ \wedge \ (t, x_t) \notin \Gamma]$ or $[\rho(i) = \neg(t, v_i) \ \wedge \ (t, x_t) \notin \Gamma]$.
   Then, the distribution of $\vec{w}_i$ or $\vec{\vec{w}}_i$ is uniformly and independently distributed on $\mathbb{F}_q^2$ (over $Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q)$).

We then observe the joint distribution (or relation) of a_0, τ, $\{\vec{w}_i\}_{i=1,\dots,\ell}$, $\{\vec{\vec{w}}_i\}_{i=1,\dots,\ell}$ and $\{\vec{r}_t\}_{t=1,\dots,d}$. Those in cases 3-5 are obviously independent from a_0. Due to the restriction of adversary $\mathcal{A}$'s key queries, $\vec{1} \notin \mathsf{span}\langle (M_i)_{\gamma(i)=1} \rangle$. Therefore, $a_0 := \vec{1} \cdot \vec{g}^{\mathrm{T}}$ is independent from the joint distribution of τ and $\{\tau a_i := \tau M_i \cdot \vec{g}^{\mathrm{T}} \mid \gamma(i) = 1\}$ (over the random selection of $\vec{g}$), which can be given by $(\vec{w}_i, \vec{r}_t)$ in case 1 and $(\vec{\vec{w}}_i, \vec{r}_t)$ in case 2. Thus, a_0 is uniformly and independently distributed from the other variables in the joint distribution. Therefore, the view of adversary $\mathcal{A}$ in the Game 2-h-1 is the same as that in Game 2-h-2.

This completes the proof of Lemma 27. □

Lemma 28 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}2}}^{\mathsf{P2\text{-}ABE}}(\lambda) + 2/q$, where $\mathcal{B}_{2\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{2\text{-}2}(h, \cdot)$.*

Proof. In order to prove Lemma 28, we construct a probabilistic machine $\mathcal{B}_{2\text{-}2}$ against Problem 2-ABE using an adversary $\mathcal{A}$ in a security game (Game 2-h-2 or 2-h-3) as a black box. $\mathcal{B}_{2\text{-}2}$ acts in the same way as $\mathcal{B}_{2\text{-}1}$ in the proof of Lemma 26 except the following two points:

1. In case (b) of step 4; $\boldsymbol{k}_0^*$ is calculated as
$$\boldsymbol{k}_0^* := -\textstyle\sum_{k=1}^{r} \widetilde{\boldsymbol{p}}_{\beta,0,k}^* + r_0' \boldsymbol{b}_{0,2}^* + \boldsymbol{b}_{0,3}^*,$$
   where $r_0' \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\widetilde{\boldsymbol{p}}_{\beta,0,k}^*$ is calculated from $\boldsymbol{h}_{\beta,0}^*$ and $\boldsymbol{b}_{0,1}^*$ as in the proof of Lemma 26, and $\boldsymbol{b}_{0,2}^*$ and $\boldsymbol{b}_{0,3}^*$ are obtained from the Problem 2-ABE instance.
2. In the last step; if $b = b'$, $\mathcal{B}_{2\text{-}2}$ outputs $\beta' := 0$. Otherwise, $\mathcal{B}_{2\text{-}2}$ outputs $\beta' := 1$.

When $\beta = 0$, it is straightforward that the distribution by $\mathcal{B}_{2\text{-}2}$'s simulation is equivalent to that in Game 2-h-2 except that δ defined in Problem 2-ABE is zero, i.e., except with probability $1/q$. When $\beta = 1$, the distribution by $\mathcal{B}_{2\text{-}2}$'s simulation is equivalent to that in Game 2-h-3 except that δ defined in Problem 2-ABE is zero i.e., except with probability $1/q$. □

Lemma 29 *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu\text{-}3)}(\lambda)| \leq 1/q$.*

Proof. To prove Lemma 29, we will show distribution $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}, \{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\dots,\nu}, \boldsymbol{c})$ in Game 2-ν-3 and that in Game 3 are equivalent, where $\mathsf{sk}_{\mathbb{S}}^{(j)*}$ is the answer to the j-th key query, and $\boldsymbol{c}$ 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

$$\boldsymbol{d}_{0,2} := (0, 1, -\theta, 0, 0)_{\mathbb{B}} = \boldsymbol{b}_{0,2} - \theta \boldsymbol{b}_{0,3}, \quad \boldsymbol{d}_{0,3}^* := (0, \theta, 1, 0, 0)_{\mathbb{B}} = \boldsymbol{b}_{0,3}^* + \theta \boldsymbol{b}_{0,2}^*.$$

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 $(\{\boldsymbol{k}_0^{(j)*}\}_{j=1,\dots,\nu}, \boldsymbol{c}_0)$ in keys and challenge ciphertext $(\{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\dots,\nu}, \mathsf{ct}_\Gamma)$ in Game 2-ν-3 are expressed over bases $\mathbb{B}_0$ and $\mathbb{B}_0^*$ as $\boldsymbol{k}_0^{(j)*} = (-s_0^{(j)}, w_0^{(j)}, 1, \eta_0^{(j)}, 0)_{\mathbb{B}_0^*}$, $\boldsymbol{c}_0 = (\delta, r_0, \zeta, 0, \varphi_0)_{\mathbb{B}_0}$. Then,

$$\boldsymbol{k}_0^{(j)*} = (-s_0^{(j)}, w_0^{(j)}, 1, \eta_0^{(j)}, 0)_{\mathbb{B}_0^*} = (-s_0^{(j)}, w_0^{(j)} + \theta, 1, \eta_0^{(j)}, 0)_{\mathbb{D}_0^*} = (-s_0^{(j)}, \vartheta_0^{(j)}, 1, \eta_0^{(j)}, 0)_{\mathbb{D}_0^*},$$

where $\vartheta_0^{(j)} := w_0^{(j)} + \theta$ which are uniformly, independently distributed since $w_0^{(j)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

$$\boldsymbol{c}_0 = (\delta, \tau, \zeta, 0, \varphi_0)_{\mathbb{B}_0} = (\delta, \tau, \zeta + \tau\theta, 0, \varphi_0)_{\mathbb{D}_0} = (\delta, \tau, \zeta', 0, \varphi_0)_{\mathbb{D}_0}$$

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 $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}})$. Therefore, $\{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\dots,\nu}$ and ct_Γ can be expressed as keys and ciphertext in two ways, in Game 2-ν-3 over bases $(\mathbb{B}_0, \mathbb{B}_0^*)$ and in Game 3 over bases $(\mathbb{D}_0, \mathbb{D}_0^*)$. Thus, Game 2-$\nu$-3 can be conceptually changed to Game 3 if $\tau \neq 0$, i.e., except with probability $1/q$. □

B Proposed Fully Secure Unbounded Anonymous HIBE Scheme

Lewko-Waters [11] constructed fully secure unbounded HIBE scheme. The scheme is payload-hiding, but not attribute-hiding, i.e., non-anonymous. We propose the first fully (adaptively) secure and attribute-hiding unbounded HIBE scheme based on the techniques given in the previous sections. The security is proven under the DLIN assumption in the standard model.

Here, we employ standard definitions of anonymous HIBE scheme and its adaptively attribute-hiding security. For example, those for (anonymous) HPE, i.e., a general version of anonymous HIBE, are given in Appendix B.5 [8]. Our definitions are specialized to two-dimensional vectors for the equality relation, i.e., $\vec{x}_t := (1, x_t)$ (in ciphertexts) and $\vec{v}_t := (v_t, -1)$ (in secret-keys), where $\vec{x}_t \cdot \vec{v}_t = 0$ iff $x_t = v_t$.

Our scheme is constructed based on the (weakly) attribute-hiding HIPE scheme given in Appendix H.4 of [14]. The HIPE scheme employs $d+1$ DPVSs $\mathbb{V}_0, \mathbb{V}_1, \dots, \mathbb{V}_d$, where basis generation matrices are $X_0 \xleftarrow{\mathsf{U}} GL(5, \mathbb{F}_q)$ and $X_t \xleftarrow{\mathsf{U}} GL(3n_t + 1, \mathbb{F}_q)$ for $t = 1, \dots, d$. By arranging the matrices $X_0, X_1, \dots X_d$ diagonally and other off-diagonal parts are zero, in [14], we consider a special from of basis generation matrix $X \in \mathbb{F}_q^{N \times N}$ with $N := 5 + \sum_{t=1}^{d}(3n_t + 1)$, where

$$X := \begin{pmatrix} X_0 & & & \\ & X_1 & & \\ & & \ddots & \\ & & & X_d \end{pmatrix},$$

and the HIPE in [14] is constructed on the one vector space $\mathbb{V}$ ($\cong \mathbb{G}^N$) with special bases induced by X.

Here, since we use dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_t)_{t=0,1})$ given in Section 2, we only use two spaces $\mathbb{V}_0, \mathbb{V}_1$ and matrices X_0, X_1, where $X_0 \xleftarrow{\mathsf{U}} GL(5, \mathbb{F}_q)$ and $X_1 \xleftarrow{\mathsf{U}} GL(14, \mathbb{F}_q)$. Therefore, the corresponding bases generation matrix $X \in \mathbb{F}_q^{N \times N}$ with $N := 5 + 14d$ is given as

$$X := \begin{pmatrix} X_0 & & & \\ & X_1 & & \\ & & \ddots & \\ & & & X_1 \end{pmatrix},$$

where off-diagonal parts are zero. In other words, the matrix X gives direct sum decomposition $\mathbb{V} \cong \mathbb{V}_0 \oplus \overbrace{\mathbb{V}_1 \oplus \cdots \oplus \mathbb{V}_1}^{d}$ (resp. $\mathbb{V}^* \cong \mathbb{V}_0^* \oplus \overbrace{\mathbb{V}_1^* \oplus \cdots \oplus \mathbb{V}_1^*}^{d}$), where $\mathbb{V}_\iota := \mathsf{span}\langle \mathbb{B}_\iota \rangle$ (resp. $\mathbb{V}_\iota^* :=$

$\mathsf{span}\langle \mathbb{B}_\iota^* \rangle$) for $\iota = 0, 1$. Based on this isomorphism, i.e., embedding of $\mathbb{V}_0$ and $d\ \mathbb{V}_1$ (resp. $\mathbb{V}_0^*$ and $d\ \mathbb{V}_1^*$) in $\mathbb{V}$ (resp. $\mathbb{V}^*$), we define the following notations as:

$$
\begin{aligned}
&((\vec{x}_0)_{\mathbb{B}_0}, (\sigma_1(1,1), \vec{x}_1)_{\mathbb{B}_1}, \ldots, (\sigma_d(1,d), \vec{x}_d)_{\mathbb{B}_1}) + ((\vec{y}_0)_{\mathbb{B}_0}, (\widetilde{\sigma}_1(1,1), \vec{y}_1)_{\mathbb{B}_1}, \ldots, (\widetilde{\sigma}_d(1,d), \vec{y}_d)_{\mathbb{B}_1}) \\
&\ := ((\vec{x}_0 + \vec{y}_0)_{\mathbb{B}_0}, ((\sigma_1 + \widetilde{\sigma}_1)(1,1), \vec{x}_1 + \vec{y}_1)_{\mathbb{B}_1} \ldots, ((\sigma_d + \widetilde{\sigma}_d)(1,d), \vec{x}_d + \vec{y}_d)_{\mathbb{B}_1}) \\
&\quad \text{where } ((\vec{x}_0)_{\mathbb{B}_0}, (\sigma_1(1,1), \vec{x}_1)_{\mathbb{B}_1}, \ldots, (\sigma_d(1,d), \vec{x}_d)_{\mathbb{B}_1}), \\
&\qquad ((\vec{y}_0)_{\mathbb{B}_0}, (\widetilde{\sigma}_1(1,1), \vec{y}_1)_{\mathbb{B}_1}, \ldots, (\widetilde{\sigma}_d(1,d), \vec{y}_d)_{\mathbb{B}_1}) \in \mathbb{V} \cong \mathbb{V}_0 \oplus \overbrace{\mathbb{V}_1 \oplus \cdots \oplus \mathbb{V}_1}^{d},
\end{aligned}
$$

$$
\begin{aligned}
&(\vec{x})_{\mathbb{B}_0} := ((\vec{x})_{\mathbb{B}_0}, \overbrace{(\vec{0})_{\mathbb{B}_1}, \cdots, (\vec{0})_{\mathbb{B}_1}}^{d}) \in \mathbb{V}, \\
&(\vec{x})_{\mathbb{B}_1}^{\langle t \rangle} := ((\vec{0})_{\mathbb{B}_0}, \overbrace{(\vec{0})_{\mathbb{B}_1}, \cdots, (\vec{0})_{\mathbb{B}_1}}^{t-1}, (\vec{x})_{\mathbb{B}_1}, \overbrace{(\vec{0})_{\mathbb{B}_1}, \cdots, (\vec{0})_{\mathbb{B}_1}}^{d-t}) \in \mathbb{V} \ \text{ for } t = 1, \ldots, d, \\
&((\vec{x}_0)_{\mathbb{B}_0}, (\sigma_t(1,t), \vec{x}_t)_{\mathbb{B}} : t = 1, \ldots, \ell) := (\vec{x}_0)_{\mathbb{B}_0} + \textstyle\sum_{t=1}^{\ell} (\sigma_t(1,t), \vec{x}_t)_{\mathbb{B}_1}^{\langle t \rangle} \in \mathbb{V} \ \text{ for } 1 \leq \ell \leq d, \\
&((\vec{x}_0)_{\mathbb{B}_0}, (\sigma_t(1,t), \vec{x}_t)_{\mathbb{B}} : t = 1, \ldots, \ell, (\sigma_t(1,t), \vec{x}_\tau)_{\mathbb{B}}) \\
&\quad := (\vec{x}_0)_{\mathbb{B}_0} + \textstyle\sum_{t=1,\ldots,\ell,\tau} (\sigma_t(1,t), \vec{x}_t)_{\mathbb{B}_1}^{\langle t \rangle} \in \mathbb{V} \ \text{ for } 1 \leq \ell < \tau \leq d
\end{aligned}
$$

$$
\begin{aligned}
e(\boldsymbol{c}, \boldsymbol{k}^*) := \textstyle\prod_{t=0}^{d} e(\boldsymbol{c}_t, \boldsymbol{k}_t^*) \quad \text{where } &\boldsymbol{c} := (\boldsymbol{c}_0, \ldots, \boldsymbol{c}_d) \in \mathbb{V}_0 \oplus \overbrace{\mathbb{V}_1 \oplus \cdots \oplus \mathbb{V}_1}^{d}, \\
&\boldsymbol{k}^* := (\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_d^*) \in \mathbb{V}_0^* \oplus \overbrace{\mathbb{V}_1^* \oplus \cdots \oplus \mathbb{V}_1^*}^{d},
\end{aligned}
$$

where position is indicated by the 2-dimensional $\sigma_t(1,t)$ for $t = 1, \ldots, \ell$, and all the above notations are applied to the case with $\{\mathbb{B}_\iota^*\}_{\iota=0,1}$ instead of $\{\mathbb{B}_\iota\}_{\iota=0,1}$ with using $\mu_t(t, -1)$ instead of $\sigma_t(1,t)$.

B.1 Construction

Let $d := poly(\lambda)$, where $poly(\cdot)$ is an arbitrary polynomial. Random dual basis generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_t)_{t=0,1})$ is defined at the end of Section 2. We refer to Section 1.4 for notations on DPVS.

```
$\mathsf{Setup}(1^\lambda):\quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 14))$,
  $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$,  $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{13}, \boldsymbol{b}_{14})$,  $\widehat{\mathbb{B}}_{0,\mathsf{pk}}^* := \boldsymbol{b}_{0,4}^*$,  $\widehat{\mathbb{B}}_{0,\mathsf{sk}}^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*)$,
  $\widehat{\mathbb{B}}_{\mathsf{pk}}^* := (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \boldsymbol{b}_{11}^*, \boldsymbol{b}_{12}^*)$,  $\widehat{\mathbb{B}}_{\mathsf{sk}}^* := (\boldsymbol{b}_3^*, \boldsymbol{b}_4^*)$,
  return  $\mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}_{0,\mathsf{pk}}^*, \widehat{\mathbb{B}}_{\mathsf{pk}}^*)$,  $\mathsf{sk} := (\widehat{\mathbb{B}}_{0,\mathsf{sk}}^*, \widehat{\mathbb{B}}_{\mathsf{sk}}^*)$.
$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, (v_1, \ldots, v_\ell) \in \mathbb{F}_q^\ell)$ :
  for $j = 1, \ldots, 2\ell$;  $\tau = \ell + 1, \ldots, d$;  $\iota = 1, 2$;
    $\psi, \mu_{\mathsf{dec},t}, \mu_{\mathsf{ran},1,j,t}, s_{\mathsf{dec},t}, s_{\mathsf{ran},1,j,t}, \theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},1,j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q$  for $t = 1, \ldots, \ell$,
    $\mu_{\mathsf{del},(\tau,\iota),t}, \mu_{\mathsf{ran},2,\tau,t}, s_{\mathsf{del},(\tau,\iota),t}, s_{\mathsf{ran},2,\tau,t}, \theta_{\mathsf{del},(\tau,\iota),t}, \theta_{\mathsf{ran},2,\tau,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q$  for $t = 1, \ldots, \ell + 1$,
    $s_{\mathsf{dec},0} := \sum_{t=1}^{\ell} s_{\mathsf{dec},t}$,  $s_{\mathsf{del},(\tau,\iota),0} := \sum_{t=1}^{\ell+1} s_{\mathsf{del},(\tau,\iota),t}$,
    $s_{\mathsf{ran},1,j,0} := \sum_{t=1}^{\ell} s_{\mathsf{ran},1,j,t}$,  $s_{\mathsf{ran},2,\tau,0} := \sum_{t=1}^{\ell+1} s_{\mathsf{ran},2,\tau,t}$,
    $\vec{\eta}_{\mathsf{dec},t}, \ \vec{\eta}_{\mathsf{ran},1,j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ for $t = 0, \ldots, \ell$,  $\vec{\eta}_{\mathsf{del},(\tau,\iota),t}, \ \vec{\eta}_{\mathsf{ran},2,\tau,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ for $t = 0, \ldots, \ell + 1$,
    $\boldsymbol{k}_{\ell,\mathsf{dec}}^* := \ ( \ ( \ -s_{\mathsf{dec},0}, \ 0, \ 1, \ \eta_{\mathsf{dec},0}, \ 0 \ )_{\mathbb{B}_0^*}$,
            $( \ \mu_{\mathsf{dec},t}(t, -1), \ s_{\mathsf{dec},t} + \theta_{\mathsf{dec},t} v_t, \ -\theta_{\mathsf{dec},t}, \ 0^6, \ \vec{\eta}_{\mathsf{dec},t}, \ 0^2 \ )_{\mathbb{B}^*} : t = 1, \ldots, \ell)$,
```

$$\begin{aligned}
\boldsymbol{k}^*_{\ell,\mathsf{del},(\tau,\iota)} :=\ & (\ (\ -s_{\mathsf{del},(\tau,\iota),0},\ 0,\ 0,\ \eta_{\mathsf{del},(\tau,\iota),0},\ 0\ )_{\mathbb{B}_0^*},\\
& (\ \mu_{\mathsf{del},(\tau,\iota),t}(t,-1),\ s_{\mathsf{del},(\tau,\iota),t}+\theta_{\mathsf{del},(\tau,\iota),t}v_t,\ -\theta_{\mathsf{del},(\tau,\iota),t},\ 0^6,\ \vec{\eta}_{\mathsf{del},(\tau,\iota),t},\ 0^2\ )_{\mathbb{B}^*}:\\
& \qquad\qquad t=1,\dots,\ell,\\
& (\ \mu_{\mathsf{del},(\tau,\iota),\ell+1}(\tau,-1),\ \pi_{\mathsf{del},(\tau,\iota),\ell+1,1},\ \pi_{\mathsf{del},(\tau,\iota),\ell+1,2}\ \ 0^6,\ \vec{\eta}_{\mathsf{del},(\tau,2),\ell+1},\ 0^2\ )_{\mathbb{B}^*})\\
& \text{where,}\ (\ \pi_{\mathsf{del},(\tau,1),\ell+1,\iota},\ \pi_{\mathsf{del},(\tau,\iota),\ell+1,2}\ ) := \begin{cases} (\ s_{\mathsf{del},(\tau,1),\ell+1}+\psi,\ \ 0\ ) & \text{if } \iota=1,\\ (\ s_{\mathsf{del},(\tau,2),\ell+1},\ \ \psi\ ) & \text{if } \iota=2,\end{cases}\\
\boldsymbol{k}^*_{\ell,\mathsf{ran},1,j} :=\ & (\ (\ -s_{\mathsf{ran},1,j,0},\ 0,\ 0,\ \eta_{\mathsf{ran},1,j,0},\ 0\ )_{\mathbb{B}_0^*},\\
& (\ \mu_{\mathsf{ran},1,j,t}(t,-1),\ s_{\mathsf{ran},1,j,t}+\theta_{\mathsf{ran},1,j,t}v_t,\ -\theta_{\mathsf{ran},1,j,t},\ 0^6,\ \vec{\eta}_{\mathsf{ran},1,j,t},\ 0^2\ )_{\mathbb{B}^*}:\\
& \qquad\qquad t=1,\dots,\ell),\\
\boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau} :=\ & (\ (\ -s_{\mathsf{ran},2,\tau,0},\ 0,\ 0,\ \eta_{\mathsf{ran},2,\tau,0},\ 0\ )_{\mathbb{B}_0^*},\\
& (\ \mu_{\mathsf{ran},2,\tau,t}(t,-1),\ s_{\mathsf{ran},2,\tau,t}+\theta_{\mathsf{ran},2,\tau,t}v_t,\ -\theta_{\mathsf{ran},2,\tau,t}\ 0^6,\ \vec{\eta}_{\mathsf{ran},2,\tau,t},\ 0^2\ )_{\mathbb{B}^*}:\\
& \qquad\qquad t=1,\dots,\ell,\\
& (\ \mu_{\mathsf{ran},2,\tau,\ell+1}(\tau,-1),\ s_{\mathsf{ran},2,\tau,\ell+1},\ 0,\ 0^6,\ \vec{\eta}_{\mathsf{ran},2,\tau,\ell+1},\ 0^2\ )_{\mathbb{B}^*}),
\end{aligned}$$

$\mathsf{sk}_\ell := (\boldsymbol{k}^*_{\ell,\mathsf{dec}}, \{\boldsymbol{k}^*_{\ell,\mathsf{del},(\tau,\iota)}\}_{\tau=\ell+1,\dots,d;\ \iota=1,2}, \{\boldsymbol{k}^*_{\ell,\mathsf{ran},1,j},\ \boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau}\}_{j=1,\dots,2\ell;\ \tau=\ell+1,\dots,d}),$

return sk_ℓ.

$\mathsf{Enc}(\mathsf{pk}, m\in\mathbb{G}_T, (x_1,\dots,x_\ell)\in\mathbb{F}_q^\ell)$:

$\omega,\zeta,\varphi_0,\varphi_{t,1},\varphi_{t,2},\sigma_t \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t=1,\dots,\ell$,

$\boldsymbol{c}_1 := (\ (\omega,0,\zeta,0,\varphi_0)_{\mathbb{B}_0},\ (\ \sigma_t(1,t),\ \omega(1,x_t),\ 0^6,\ 0^2,\ \varphi_{t,1},\varphi_{t,2}\ )_{\mathbb{B}} : t=1,\dots,\ell),$

$c_2 := g_T^\zeta m,\qquad \mathsf{ct} := (\boldsymbol{c}_1, c_2),\quad$ return ct.

$\mathsf{Dec}(\mathsf{pk}, \boldsymbol{k}^*_{\ell,\mathsf{dec}}, \mathsf{ct})$: $m' := c_2/e(\boldsymbol{c}_1, \boldsymbol{k}^*_{\ell,\mathsf{dec}}),\quad$ return m'.

$\mathsf{Delegate}_\ell(\mathsf{pk}, \mathsf{sk}_\ell, v_{\ell+1})$:

for $j'=1,\dots,2(\ell+1);\ \tau=\ell+2,\dots,d;\ \iota=1,2;$

$\mu'_{\mathsf{del},(\tau,\iota)},\ \mu'_{\mathsf{ran},2,\tau},\ \phi_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{ran},2,\tau},\ \psi' \xleftarrow{\mathsf{U}} \mathbb{F}_q,$

$\boldsymbol{p}^*_{\mathsf{dec}}, \boldsymbol{p}^*_{\mathsf{del},(\tau,\iota)}, \boldsymbol{p}^*_{\mathsf{ran},1,j'}, \boldsymbol{p}^*_{\mathsf{ran},2,\tau} \xleftarrow{\mathsf{R}} \mathsf{CoreDel}_\ell(\mathsf{pk}, \mathsf{sk}_\ell, v_{\ell+1}),$

where $\mathsf{CoreDel}_\ell(\mathsf{pk}, \mathsf{sk}_\ell, v_{\ell+1})$: $\mu'_t, \xi, \alpha_j \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t=1,\dots,\ell+1; j=1,\dots,2\ell+1,$

$$\begin{aligned}
\text{return } \boldsymbol{p}^* := & \textstyle\sum_{t=1}^{\ell+1} \mu'_t(t\boldsymbol{b}^*_1-\boldsymbol{b}^*_2)^{\langle t\rangle} + \xi\left(v_{\ell+1}\boldsymbol{k}^*_{\ell,\mathsf{del},(\ell+1,1)} - \boldsymbol{k}^*_{\ell,\mathsf{del},(\ell+1,2)}\right)\\
& + \textstyle\sum_{j=1}^{2\ell} \alpha_j \boldsymbol{k}^*_{\ell,\mathsf{ran},1,j} + \alpha_{2\ell+1}\boldsymbol{k}^*_{\ell,\mathsf{ran},2,\ell+1},
\end{aligned}$$

$\boldsymbol{r}^*_{\mathsf{dec}}, \boldsymbol{r}^*_{\mathsf{ran},1,j'} \xleftarrow{\mathsf{U}} \mathsf{span}\langle\left(\boldsymbol{b}^*_{0,4}\right)^{\langle 0\rangle}, \{(\boldsymbol{b}^*_{11})^{\langle t\rangle}, (\boldsymbol{b}^*_{12})^{\langle t\rangle}\}_{t=1,\dots,\ell+1}\rangle,$

$\boldsymbol{r}^*_{\mathsf{del},(\tau,\iota)}, \boldsymbol{r}^*_{\mathsf{ran},2,\tau} \xleftarrow{\mathsf{U}} \mathsf{span}\langle\left(\boldsymbol{b}^*_{0,4}\right)^{\langle 0\rangle}, \{(\boldsymbol{b}^*_{11})^{\langle t\rangle}, (\boldsymbol{b}^*_{12})^{\langle t\rangle}\}_{t=1,\dots,\ell+1,\tau}\rangle,$

$\boldsymbol{k}^*_{\ell+1,\mathsf{dec}} := \boldsymbol{k}^*_{\ell,\mathsf{dec}} + \boldsymbol{p}^*_{\mathsf{dec}} + \boldsymbol{r}^*_{\mathsf{dec}},$

$$\begin{aligned}
\boldsymbol{k}^*_{\ell+1,\mathsf{del},(\tau,\iota)} := & \boldsymbol{p}^*_{\mathsf{del},(\tau,\iota)} + \mu'_{\mathsf{del},(\tau,\iota)}(\tau\boldsymbol{b}^*_1-\boldsymbol{b}^*_2)^{\langle\tau\rangle} + \phi_{\mathsf{del},(\tau,\iota)}\boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau}\\
& +\psi'\boldsymbol{k}^*_{\ell,\mathsf{del},(\tau,\iota)} + \boldsymbol{r}^*_{\mathsf{del},(\tau,\iota)},
\end{aligned}$$

$\boldsymbol{k}^*_{\ell+1,\mathsf{ran},1,j'} := \boldsymbol{p}^*_{\mathsf{ran},1,j'} + \boldsymbol{r}^*_{\mathsf{ran},1,j'},$

$\boldsymbol{k}^*_{\ell+1,\mathsf{ran},2,\tau} := \boldsymbol{p}^*_{\mathsf{ran},2,\tau} + \mu'_{\mathsf{ran},2,\tau}(\tau\boldsymbol{b}^*_1-\boldsymbol{b}^*_2)^{\langle\tau\rangle} + \phi_{\mathsf{ran},2,\tau}\boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau} + \boldsymbol{r}^*_{\mathsf{ran},2,\tau},$

$$\begin{aligned}
\mathsf{sk}_{\ell+1} := (& \boldsymbol{k}^*_{\ell+1,\mathsf{dec}}, \{\boldsymbol{k}^*_{\ell+1,\mathsf{del},(\tau,\iota)}\}_{\tau=\ell+2,\dots,d;\ \iota=1,2},\\
& \{\boldsymbol{k}^*_{\ell,\mathsf{ran},1,j'},\ \boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau}\}_{j'=1,\dots,2(\ell+1);\ \tau=\ell+2,\dots,d}),
\end{aligned}$$

return $\mathsf{sk}_{\ell+1}$.

B.2 Security

Theorem 7 *The proposed HIBE scheme is adaptively attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

The proof of Theorem 7 is obtained in a similar manner to Theorem 4.