Predicate- and Attribute-Hiding Inner Product Encryption in a Public Key Setting [*]

Yutaka Kawai
Mitsubishi Electric
Kawai.Yutaka@da.MitsubishiElectric.co.jp

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

November 18, 2013

Abstract

In this paper, we propose a *reasonable* definition of *predicate-hiding* inner product encryption (IPE) *in a public key setting*, which we call inner product encryption with ciphertext conversion (IPE-CC), where original ciphertexts are converted to predicate-searchable ones by an helper in possession of a conversion key. We then define a notion of *full* security for IPE-CC, which comprises three security properties of being adaptively *predicate-* and attribute-hiding in the public key setting, adaptively *(fully-)attribute-hiding against the helper*, and usefully secure even *against the private-key generator (PKG)*. We then present *the first fully secure IPE-CC* scheme, and convert it into the *first fully secure symmetric-key IPE (SIPE)* scheme, where the security is defined in the sense of Shen, Shi, Waters. All the security properties are proven under the decisional linear assumption in the standard model. The IPE-CC scheme is comparably as efficient as existing attribute-hiding (not predicate-hiding) IPE schemes. We also present a variant of the proposed IPE-CC scheme with the same security that achieves shorter public and secret keys. We employ two key techniques, *trapdoor basis setup*, in which a new trapdoor is embedded in a public key, and *multi-system proof technique*, which further generalizes an extended dual system approach given by Okamoto and Takashima recently.

[*] This is the full version of a paper appearing in Pairing 2013, the 6th International Conference on Pairing-Based Cryptography, November 22–24, 2013, Beijing, China.

Contents

1 Introduction

1.1 Background

The notion of *predicate encryption* (PE) was explicitly presented by Katz, Sahai and Waters [14] for achieving fine-grained control over revealed information on encrypted data for various predicate-searchable token key owners. In the encryption system, the owner of a (master) secret key can create and issue tokens to system users. Informally, tokens in a predicate encryption scheme correspond to predicates in some class $\mathcal{F}$, and a sender associates a ciphertext with an attribute in a set Σ; a ciphertext ct_x associated with the attribute (or plaintext) $x \in \Sigma$ can be evaluated by token tk_f corresponding to the predicate $f \in \mathcal{F}$ to learn whether $f(x) = 1$. In this paper, we only consider this *predicate-only* PE [14, 24], in which attribute x can be treated as a plaintext in a general functional encryption framework [9]. (However, we treat x as an attribute hereafter.)

In addition, a security notion for PE, *attribute-hiding*, was defined in [14], where, roughly speaking, a ciphertext conceals the associated attribute. More specifically, it requires that an adversary in possession of tokens $\mathsf{tk}_{f_1}, \ldots, \mathsf{tk}_{f_h}$ for predicates $f_1, \ldots, f_h$ cannot derive any information on attribute x from ciphertext ct_x other than the values of $f_1(x), \ldots, f_h(x)$.

Katz, Sahai and Waters [14] also presented a concrete construction of PE for a class of predicates called *inner product* predicates, which represents a wide class of predicates that includes an equality test (for IBE [2, 3, 5, 11] and HVE [10]), range queries [25], disjunctions or conjunctions of equality tests, and, more generally, arbitrary CNF or DNF formulas. Informally, an attribute of inner product predicates is expressed as vector $\vec{x}$ and predicate $f_{\vec{v}}$ is associated with vector $\vec{v}$, where $f_{\vec{v}}(\vec{x}) = 1$ iff $\vec{v} \cdot \vec{x} = 0$. (Here, $\vec{v} \cdot \vec{x}$ denotes the standard inner product.)

The attribute-hiding security achieved in [16, 17, 18] is more limited or weaker than that achieved in [14, 20]. The former is called weakly-attribute-hiding, and the latter *fully-attribute-hiding.* Although the IPE scheme [14] achieved fully-attribute-hiding, it is *selectively* secure under non-standard assumptions. Subsequently, several attribute-hiding IPE schemes have been proposed [16, 17, 18, 19, 23], for aiming at an IPE scheme with better security, e.g., adaptive security, fully-attribute-hiding and weaker (standard) assumptions. This research direction culminated in *adaptively secure* and *fully-attribute-hiding* IPE scheme under the *decisional linear (DLIN)* assumption [20]. The basic scheme in [20] has a variant with shorter public and tokens based on the technique in [19]. A hierarchical IPE (HIPE) scheme can be realized with the same security. (For a practical variant of the schemes, refer to [22].)

However, all previous public key IPE schemes have a problem to be applied in a practical system, that is, *predicate token queries may leak some sensitive information*, e.g., medical personal history, patent strategy, or corporate sensitive data. This is unavoidable in a *plain public key IPE* system, since anyone can generate a ciphertext associated with any attribute, and then, by using it, check the predicate associated in (target) token. In order to avoid this problem, Shen-Shi-Waters [24] proposed a *symmetric*-key IPE (SIPE) scheme, where predicate in a token is hidden from any malicious users [24, 26]. The property is called *predicate-hiding.* They [24] defined a strong security notion "full security", which implies predicate- and attribute-hiding, however, only constructed a weakly secure (selectively secure, single challenge) SIPE scheme since it is based on a weakly secure public key IPE given in [14]. Therefore, to construct a fully secure SIPE remains an interesting open problem.

Moreover, we require such an IPE functionality in a *public key setting.* To see the importance of *predicate- and attribute-hiding* IPE in a *public key setting*, let us consider an example on electronic medical record (EMR) storing and managing system that allows multiple hospitals to export EMRs to a remote server. By sharing EMRs among the hospitals, patient care and cost savings are greatly improved. Moreover, the database system provides a large source of medical research for physicians, biologists, and pharmacists, etc. For example, pharmaceutical companies use it for developing a new medicine.

Here, it is desirable that such a sensitive data be treated as encrypted data even for data processing and retrievals, which protects privacy of data provider. In addition, in the above example, multiple competitors, e.g., pharmaceutical companies, like to hide their access histories from each other. Hence, to apply PE technology to the remote EMR server setting, we require

1. For providing and sharing EMRs among multiple medical institutes, PE should be realized in a public key setting.

2. Attribute-hiding (for data-provider's privacy) and predicate-hiding (for data-retriever's privacy) must be assured.

In other applications with remote storage servers, a PE-encrypted file system with the above properties also highly improves user availability and removes privacy concerns. Recently, Boneh et al.[7, 8] proposed function-private PE (including IPE) schemes, which assure predicate-hiding only when used predicates are sampled from any *sufficiently unpredictable* distribution. The schemes does not guarantee predicate-hiding in the above setting, in general. Hence, to give a *reasonable and useful definition* of predicate-hiding IPE in a public key setting which is applicable in the above, is also an interesting open problem from a practical and theoretical point of view.[1]

1.2 Our Results

1. This paper introduces a reasonable and useful definition of (a variant of) IPE for achieving predicate-hiding in a public-key setting, i.e., *IPE with ciphertext conversion (IPE-CC).*

   Here, two types of ciphertexts, original and converted, are introduced, and a new type of key, conversion key, is used as well as public and secret keys: Each user encrypts an attribute $\vec{x}$ by using public key, and the generated ciphertext $\mathsf{ct}_{\vec{x}}$ is called original. The ciphertext is converted to a predicate-searchable one $\mathsf{CT}_{\vec{x}}$ by a helper in possession of the conversion key ck.

   IPE-CC has two types of secret (or trapdoor) keys, sk and ck. Depending on which key an adversary has, we have three security requirements:

   (a) predicate-hiding of token key $\mathsf{tk}_{\vec{v}}$ and attribute-hiding of ciphertexts ($\mathsf{ct}_{\vec{x}}$, $\mathsf{CT}_{\vec{x}}$) against any malicious user with no secret key sk nor conversion key ck,

   (b) (fully-)attribute-hiding of ciphertexts $(\mathsf{ct}_{\vec{x}}, \mathsf{CT}_{\vec{x}})$ against any malicious helper with no secret key sk,

   (c) predicate-hiding of token key $\mathsf{tk}_{\vec{v}}$ and attribute-hiding of ciphertext $\mathsf{ct}_{\vec{x}}$ against any malicious PKG with no conversion key ck.

   An IPE-CC scheme is called *fully secure* iff it satisfies all the above three security requirements.

2. This paper proposes *the first fully-secure* IPE-CC scheme, where all the security properties are proven under the DLIN assumption in the standard model (Section 3).

   Remark: Our IPE-CC scheme addresses privacy concerns given in the above remote server system, which is illustrated in Figure 1. Every data-provider, e.g., Hospital A, B,.., can put his encrypted data $\mathsf{ct}_{\vec{x}}$ for data $\vec{x}$ on the shared server, and each data-retriever, e.g., Pharmaceutical Company X, Y,.., obtains his own token $\mathsf{tk}_{\vec{v}}$ associated with a predicate category $\vec{v}$ from PKG. Here, a predicate category indicates an available range for specific predicate searches, e.g., Company X is assigned for accessing patient-data in the south of the U.S., and Y is assigned for accessing patient-data in the north. (The predicate category may be empty condition.) The data-retriever delegates the (high-level) token $\mathsf{tk}_{\vec{v}}$ to a specific predicate token $\mathsf{tk}_{\vec{v}\wedge\vec{w}}$, where $\vec{w}$ indicates some medical predicate, e.g., records for cardiac patients aged 60 and above. (Refer to Section 3.3 for the 2-level hierarchical IPE-CC scheme.) Helper converts original encrypted data $\mathsf{ct}_{\vec{x}}$ to searchable ones, $\mathsf{CT}_{\vec{x}}$, using conversion key ck (in some extra time). Note that the converted ciphertexts are not made public (while original encrypted data on the database are publicly accessible). In the figure, Company X sends a search query with delegated token $\mathsf{tk}_{\vec{v}\wedge\vec{w}}$, and he obtains search result, $f_{\vec{v}\wedge\vec{w}}(\vec{x}) \in \{0,1\}$. The basic security (a) protects privacy for both data-providers and data-retrievers from dishonest users, e.g., competing companies. The security condition (b) assures no information leakage to the server administrator (i.e.,

[1] Boneh et al. [6] approached the problem based on PIR, which is a communication protocol, while our solution is provided just by an encryption scheme (with much more efficient communication).

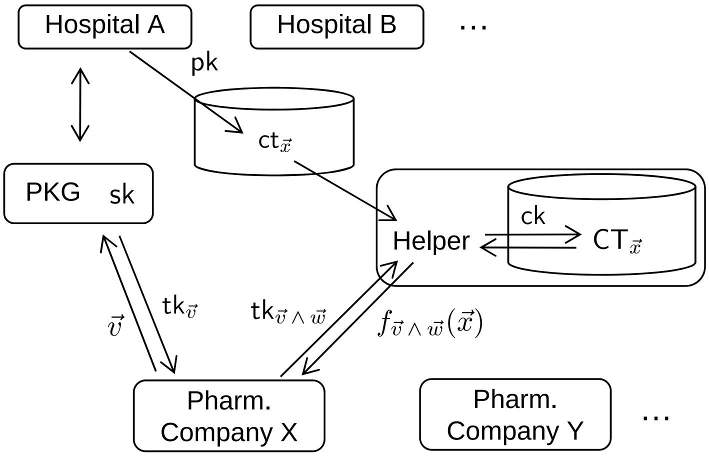


Figure 1: Application to EMR storing and managing system, in which original encrypted data $\mathsf{ct}_{\vec{x}}$ are publicly accessible but converted ciphertexts $\mathsf{CT}_{\vec{x}}$ are not made public. Pharmaceutical Company X retrieves medical data with some medical predicate $\vec{w}$ as well as a predetermined condition $\vec{v}$.

helper) from ciphertexts on the server. Moreover, since converted ciphertexts are not public, security (c) assures both predicate-hiding in tokens and attribute-hiding in ciphertexts *against PKG*. Since to mitigate the power of PKG is important in PE systems, this security against PKG is useful and interesting. Thus, to summarize, the proposed scheme provides attribute-hiding for ciphertexts as in [20] and predicate-hiding for tokens from any malicious users but the helper. The technique can be applied to unbounded IPE in [21].

3. We propose *the first fully secure* symmetric-key IPE (SIPE) scheme in the sense of the definition by Shen, Shi and Waters [24] (Section 4). The scheme is (generically) converted from our public key setting IPE-CC by including public key and conversion key into (master) secret key. The security is also proven under the DLIN assumption in the standard model.

4. We also present a variant of the proposed IPE-CC scheme with the same security that achieves shorter public key and shorter (master) secret key (Section 5). Table 1 in Section 6 compares the proposed IPE-CC scheme (resp. SIPE scheme) with existing attribute-hiding IPE schemes in the public key setting (resp. the existing SIPE scheme).

1.3 Key Techniques

Trapdoor Basis Setup: A full security notion of IPE-CC (in the public key setting) consists of three types of hiding properties against various type adversaries, i.e., malicious users, helper, or PKG. For achieving such a rich security property, we employ a new trapdoor embedded in a public key. See Figure 2. The setup algorithm produces a pair of random dual bases $(\mathbb{B}, \mathbb{B}^*)$ on a dual pairing vector space (DPVS), and by using random matrix $\mathsf{ck} := W$, linearly transforms a part of the basis, $\widehat{\mathbb{B}}$ $(\subset \mathbb{B})$, to a new basis $\widehat{\mathbb{D}} := \widehat{\mathbb{B}} \cdot W$, which is uniformly and independently distributed from $\mathbb{B}$. It outputs $\widehat{\mathsf{pk}} := \widehat{\mathbb{D}}$ as a part of a public key and the corresponding $\mathsf{sk} := \widehat{\mathbb{B}}^*$ as a secret key, where the bases are independent from each other if W is not considered. Original ciphrtexts and tokens inherit this independence property from the

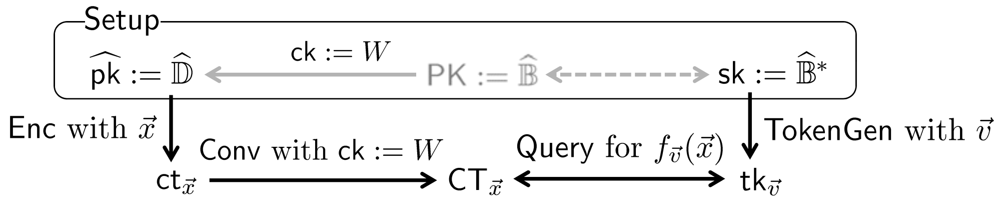

Setup
$\widehat{\mathsf{pk}} := \widehat{\mathbb{D}}$
$\mathsf{ck} := W$
$\mathsf{PK} := \widehat{\mathbb{B}}$
$\mathsf{sk} := \widehat{\mathbb{B}}^*$
Enc with $\vec{x}$
TokenGen with $\vec{v}$
Conv with $\mathsf{ck} := W$
Query for $f_{\vec{v}}(\vec{x})$
$\mathsf{ct}_{\vec{x}}$
$\mathsf{CT}_{\vec{x}}$
$\mathsf{tk}_{\vec{v}}$

Figure 2: Trapdoor basis setup with conversion key ck for public key $\widehat{\mathsf{pk}}$ and (master) secret key sk, in which $\mathsf{PK} := \widehat{\mathbb{B}}$ is not directly used (with Enc, $\mathsf{TokenGen}$, Conv, Query)

master key pair. The trapdoor (i.e., conversion key) W transforms the original ciphertexts to searchable ones, which are related to tokens through the dual orthonormal property of $(\mathbb{B}, \mathbb{B}^*)$. We establish security properties against various level adversaries based on this *trapdoor basis setup* construction.

In a subsequent work [15], we extend our trapdoor basis approach for achieving fully-anonymous functional encryption schemes, where two trapdoor matrices, W_1 and W_2, are used in re-encryption key generation and re-encrypted ciphertext generation, respectively.

Multi-System Proof Technique: As we observed, our IPE-CC scheme implies the *first* fully secure SIPE scheme. Since no previous SIPE schemes are fully secure, we develop a new technique to obtain the scheme, we call *multi-system proof technique*, which extends the approach given in [20].

Based on Waters' dual system encryption methodology, in the previous work [20], a large hidden subspace was used for achieving *fully*-attribute-hiding of IPE, where the subspace was $2n$-dimensional for n-dimensional attribute vectors and the two n-dimensional blocks played different roles in the proof. Moreover, to hide a challenge bit b from adversary, *unbiased* ciphertexts with $\omega_0 \vec{x}^{(0)} + \omega_1 \vec{x}^{(1)}$ for challenge $\vec{x}^{(0)}, \vec{x}^{(1)} \in \mathbb{F}_q^n$ (and $\omega_0, \omega_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$) played a key role in the security proof.

In this work, for achieving both *fully* predicate- and attribute-hiding security of our schemes, a simulator must deal with two types of challenges $(\vec{x}^{(0)}, \vec{x}^{(1)})$ and $(\vec{v}^{(0)}, \vec{v}^{(1)})$ simultaneously. Since the above unbiased ciphertext (or token) construction is not enough for this purpose, we use larger, $3n$-dimensional, multi-system hidden subspace, and refined game hopping.[2] See Appendix A for the details.

1.4 Notations

When A is a random variable or distribution, $y \xleftarrow{\mathsf{R}} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \xleftarrow{\mathsf{U}} A$ denotes that y is uniformly selected from A. We denote the finite field of order q by $\mathbb{F}_q$, and $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^\times$. A vector symbol denotes a vector representation over $\mathbb{F}_q$, e.g., $\vec{x}$ denotes $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. For two vectors $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{v} = (v_1, \ldots, v_n)$, $\vec{x} \cdot \vec{v}$ denotes the inner product $\sum_{i=1}^n x_i v_i$. The vector $\vec{0}$ is abused as the zero vector in $\mathbb{F}_q^n$ for any n. X^{T} denotes the transpose of matrix X. 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 $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^N y_i \boldsymbol{b}_i^*$. For a

[2] In [24], a generic conversion from an adaptively secure single-challenge SIPE to a fully secure (multi-challenge) SIPE is given. By using the conversion, we may take an approach to fully secure SIPE via single challenge secure SIPE based on IPE in [20]. However, since the conversion loses efficiency, our SIPE in Section 4 is better.

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

2 Definitions

2.1 Dual Pairing Vector Spaces (DPVS)

In this paper, for simplicity of description, we will present the proposed schemes on the symmetric version of dual pairing vector spaces (DPVS) [17, 16, 18] constructed using symmetric bilinear pairing groups given in Definition 1. Owing to the abstraction of DPVS, the presentation and the security proof of the proposed schemes are essentially the same as those on the asymmetric version of DPVS, $(q,\mathbb{V},\mathbb{V}^*,\mathbb{G}_T,\mathbb{A},\mathbb{A}^*,e)$, for which see Appendix A.2 in the full version of [18]. The symmetric version is a specific (self-dual) case of the asymmetric version, where $\mathbb{V} = \mathbb{V}^*$ and $\mathbb{A} = \mathbb{A}^*$.

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 $\boldsymbol{a}_i := (\overbrace{0,..,0}^{i-1},G,\overbrace{0,..,0}^{N-i})$, 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 $\boldsymbol{x} := (G_1,..,G_N) \in \mathbb{V}$ and $\boldsymbol{y} := (H_1,..,H_N) \in \mathbb{V}$. 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 $\mathcal{G}_{\mathsf{bpg}}$.*

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

2.3 Inner Product Encryption with Ciphertext Conversion (IPE-CC)

This section defines inner product encryption with ciphertext conversion (IPE-CC) and its security. An attribute (or plaintext) of inner product predicates is expressed as a vector $\vec{x} \in$

$\mathbb{F}_q^n \setminus \{\vec{0}\}$ and a predicate $f_{\vec{v}}$ is associated with a vector $\vec{v}$, where $f_{\vec{v}}(\vec{x}) = 1$ iff $\vec{v} \cdot \vec{x} = 0$. Let $\Sigma := \mathbb{F}_q^n \setminus \{\vec{0}\}$, i.e., the set of the attributes, and $\mathcal{F} := \{f_{\vec{v}} | \vec{v} \in \mathbb{F}_q^n \setminus \{\vec{0}\}\}$ i.e., the set of the predicates.

Definition 4 *An inner product encryption with ciphertext conversion (IPE-CC) scheme (for predicates $\mathcal{F}$ and attributes Σ) consists of probabilistic polynomial-time algorithms* $\mathsf{Setup}, \mathsf{TokenGen}, \mathsf{Enc}, \mathsf{Conv}$ *and* Query. *They are given as follows:*

- Setup *takes as input security parameter 1^λ, and it outputs a public key* pk, *a conversion key* ck, *and a (master) secret key* sk.

- $\mathsf{TokenGen}$ *takes as input a public key* pk, *a (master) secret key* sk, *and a predicate vector $\vec{v}$. It outputs a corresponding token* $\mathsf{tk}_{\vec{v}}$.

- Enc *takes as input a public key* pk *and an attribute (or plaintext) vector $\vec{x}$. It returns an original ciphertext* $\mathsf{ct}_{\vec{x}}$.

- Conv *takes as input a public key* pk, *a conversion key* ck, *and an original ciphertext* $\mathsf{ct}_{\vec{x}}$. *It returns a converted ciphertext* $\mathsf{CT}_{\vec{x}}$.

- Query *takes as input a public key* pk, *a token* $\mathsf{tk}_{\vec{v}}$ *and a converted ciphertext* $\mathsf{CT}_{\vec{x}}$. *It outputs either 0 or 1, indicating the value of the predicate $f_{\vec{v}}$ evaluated on the underlying attribute $\vec{x}$.*

Remark 1 In the introduction, we give an application example using a delegation from $\mathsf{tk}_{\vec{v}}$ to $\mathsf{tk}_{\vec{v} \wedge \vec{w}} (:= \mathsf{tk}_{(\vec{v},\vec{w})})$. While we can add this functionality, the explicit description of the delegation is not included here for simple presentation. Refer to Section 3.3 for the 2-level hierarchical IPE-CC scheme.

An IPE-CC scheme should have the following correctness property: for all $(\mathsf{pk}, \mathsf{ck}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n)$, all $f_{\vec{v}} \in \mathcal{F}$ and $\vec{x} \in \Sigma$, all $\mathsf{tk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{TokenGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$, all original ciphertexts $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, \vec{x})$ and converted ciphertexts $\mathsf{CT}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Conv}(\mathsf{pk}, \mathsf{ck}, \mathsf{ct}_{\vec{x}})$, it holds that $1 = \mathsf{Query}(\mathsf{tk}_{\vec{v}}, \mathsf{CT}_{\vec{x}})$ if $f_{\vec{v}}(\vec{x}) = 1$. Otherwise, it holds only with negligible probability.

We then define the *full* security notion of IPE-CC, which consists of three security notions, i.e., security against *malicious users*, *malicious helper*, and *malicious PKG*.

Definition 5 (Full Security of IPE-CC) *An IPE-CC scheme is* fully secure *if for all probabilistic polynomial-time adversaries $\mathcal{A}$, all $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisU}}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisH}}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisPKG}}(\lambda)$ are negligible.*

[Dishonest-User Game] *The model for defining the adaptively predicate-hiding and adaptively attribute-hiding security of IPE-CC against malicious user $\mathcal{A}$ is given as follows:*

1. *The challenger runs* Setup *to generate keys* pk, ck *and* sk, *and* pk *is given to $\mathcal{A}$. The challenger picks a random bit b.*

2. *$\mathcal{A}$ may adaptively make a polynomial number of queries, where each query is one of two types:*

   - *On the ℓ-th ciphertext query, $\mathcal{A}$ outputs two attribute vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$. The challenger responds with $(\mathsf{ct}_\ell, \mathsf{CT}_\ell)$, where $\mathsf{ct}_\ell \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, \vec{x}_\ell^{(b)})$ and $\mathsf{CT}_\ell \xleftarrow{\mathsf{R}} \mathsf{Conv}(\mathsf{pk}, \mathsf{ck}, \mathsf{ct}_\ell)$.*

- *On the h-th token query, $\mathcal{A}$ outputs two predicate vectors, $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$. The challenger responds with* $\mathsf{tk}_h \xleftarrow{\mathsf{R}} \mathsf{TokenGen}(\mathsf{pk}, \mathsf{sk}, \vec{v}_h^{(b)})$.

$\mathcal{A}$'s queries are subject to the restriction that, for all ciphertext queries $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ and all token queries $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$, $f_{\vec{v}_h^{(0)}}(\vec{x}_\ell^{(0)}) = f_{\vec{v}_h^{(1)}}(\vec{x}_\ell^{(1)})$.

3. *$\mathcal{A}$ outputs a guess b' of b.*

The success experiment in the above game, i.e., $b' = b$, is denoted by $\mathsf{Succ}_{\mathcal{A}}^{\mathsf{DisU}}(\lambda)$, and the advantage of $\mathcal{A}$ is defined as $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisU}}(\lambda) := \Pr[\,\mathsf{Succ}_{\mathcal{A}}^{\mathsf{DisU}}(\lambda)\,] - 1/2$ for any security parameter λ.

[Dishonest-Helper Game] *The model for defining the adaptively (fully-)attribute-hiding security of IPE-CC against malicious helper $\mathcal{A}$ is given as follows:*

1. *The challenger runs* Setup *to generate keys* pk, ck *and* sk, *and* pk *and* ck *are given to $\mathcal{A}$. The challenger picks a random bit b.*

2. *$\mathcal{A}$ may adaptively make a polynomial number of queries, where each query is one of two types:*

   - *On the ℓ-th ciphertext query, $\mathcal{A}$ outputs two attribute vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$. The challenger responds with* $\mathsf{ct}_\ell \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, \vec{x}_\ell^{(b)})$.
   - *On the h-th token query, $\mathcal{A}$ outputs a predicate vector, $\vec{v}_h$. The challenger responds with* $\mathsf{tk}_h \xleftarrow{\mathsf{R}} \mathsf{TokenGen}(\mathsf{pk}, \mathsf{sk}, \vec{v}_h)$.

   $\mathcal{A}$'s queries are subject to the restriction that, for all ciphertext queries $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ and all token queries $\vec{v}_h$, $f_{\vec{v}_h}(\vec{x}_\ell^{(0)}) = f_{\vec{v}_h}(\vec{x}_\ell^{(1)})$.

3. *$\mathcal{A}$ outputs a guess b' of b.*

The success experiment in the above game, i.e., $b' = b$, is denoted by $\mathsf{Succ}_{\mathcal{A}}^{\mathsf{DisH}}(\lambda)$, and the advantage of $\mathcal{A}$ is defined as $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisH}}(\lambda) := \Pr[\,\mathsf{Succ}_{\mathcal{A}}^{\mathsf{DisH}}(\lambda)\,] - 1/2$ for any security parameter λ.

[Dishonest-PKG Game] *The model for defining the adaptively attribute-hiding and predicate-hiding security of IPE-CC against malicious-PKG $\mathcal{A}$ is given as follows:*

1. *The challenger runs* Setup *to generate keys* pk, ck *and* sk, *and* pk *and* sk *are given to $\mathcal{A}$. The challenger picks a random bit b.*

2. *$\mathcal{A}$ may adaptively make a polynomial number of queries, where each query is one of two types:*

   - *On the ℓ-th ciphertext query, $\mathcal{A}$ outputs two attribute vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$. The challenger responds with* $\mathsf{ct}_\ell \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, \vec{x}_\ell^{(b)})$.
   - *On the h-th token query, $\mathcal{A}$ outputs two predicate vectors, $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$. The challenger responds with* $\mathsf{tk}_h \xleftarrow{\mathsf{R}} \mathsf{TokenGen}(\mathsf{pk}, \mathsf{sk}, \vec{v}_h^{(b)})$.

   $\mathcal{A}$'s queries are subject to no restrictions.

3. *$\mathcal{A}$ outputs a guess b' of b.*

The success experiment in the above, i.e., $b' = b$*, is denoted by* $\mathsf{Succ}_{\mathcal{A}}^{\mathsf{DisPKG}}(\lambda)$*, and the advantage of* $\mathcal{A}$ *is defined as* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisPKG}}(\lambda) := \mathsf{Pr}[\,\mathsf{Succ}_{\mathcal{A}}^{\mathsf{DisPKG}}(\lambda)\,] - 1/2$ *for any security parameter* λ*.*

Since a converted ciphertext is not publicly available, it is not given to the adversary in the above Dishonest-PKG game.

2.4 Symmetric-Key Inner Product Encryption (SIPE)

This section defines symmetric-key inner product encryption (SIPE) and its security.

An attribute (or plaintext) of inner product predicates is expressed as a vector $\vec{x} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$ and a predicate $f_{\vec{v}}$ is associated with a vector $\vec{v}$, where $f_{\vec{v}}(\vec{x}) = 1$ iff $\vec{v} \cdot \vec{x} = 0$. Let $\Sigma := \mathbb{F}_q^n \setminus \{\vec{0}\}$, i.e., the set of the attributes, and $\mathcal{F} := \{f_{\vec{v}} | \vec{v} \in \mathbb{F}_q^n \setminus \{\vec{0}\}\}$ i.e., the set of the predicates.

Definition 6 *A symmetric-key inner product encryption scheme (SIPE) for predicates* $\mathcal{F}$ *and attributes* Σ *consists of probabilistic polynomial-time algorithms* $\mathsf{Setup}, \mathsf{TokenGen}, \mathsf{Enc}$ *and* Query*. They are given as follows:*

- Setup *takes as input security parameter* 1^λ*, and it outputs a secret key* sk*.*
- $\mathsf{TokenGen}$ *takes as input a secret key* sk*, and a predicate vector* $\vec{v}$*. It outputs a corresponding token* $\mathsf{tk}_{\vec{v}}$*.*
- Enc *takes as input a secret key* sk *and an attribute (or plaintext) vector* $\vec{x}$*. It returns a ciphertext* $\mathsf{ct}_{\vec{x}}$*.*
- Query *takes as input a token* $\mathsf{tk}_{\vec{v}}$ *and a ciphertext* $\mathsf{ct}_{\vec{x}}$*. It outputs either 0 or 1, indicating the value of the predicate* $f_{\vec{v}}$ *evaluated on the underlying attribute* $\vec{x}$*.*

An SIPE scheme should have the following correctness property: for all $\mathsf{sk} \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n)$, all $f_{\vec{v}} \in \mathcal{F}$ and $\vec{x} \in \Sigma$, all $\mathsf{tk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{TokenGen}(\mathsf{sk}, \vec{v})$, all ciphertext $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{sk}, \vec{x})$, it holds that $1 = \mathsf{Query}(\mathsf{tk}_{\vec{v}}, \mathsf{ct}_{\vec{x}})$ if $f_{\vec{v}}(\vec{x}) = 1$. Otherwise, it holds with negligible probability.

We then define the *full* security notion of SIPE, which is the same as that given by Shen, Shi, and Waters [24].

Definition 7 (Full Security of SIPE) *The model for defining the full security of SIPE against adversary* $\mathcal{A}$ *is given as follows:*

1. *The challenger runs* Setup *to generate secret key* sk*, and picks a random bit* b*.*
2. $\mathcal{A}$ *may adaptively make a polynomial number of queries, where each query is one of two types:*
   - *On the* ℓ*-th ciphertext query,* $\mathcal{A}$ *outputs two attribute vectors* $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$*. The challenger responds with* $\mathsf{ct}_\ell \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{sk}, \vec{x}_\ell^{(b)})$*.*
   - *On the* h*-th token query,* $\mathcal{A}$ *outputs two predicate vectors,* $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$*. The challenger responds with* $\mathsf{tk}_h \xleftarrow{\mathsf{R}} \mathsf{TokenGen}(\mathsf{sk}, \vec{v}_h^{(b)})$*.*

   $\mathcal{A}$*'s queries are subject to the restriction that, for all ciphertext queries* $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ *and all token queries* $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$*,* $f_{\vec{v}_h^{(0)}}(\vec{x}_\ell^{(0)}) = f_{\vec{v}_h^{(1)}}(\vec{x}_\ell^{(1)})$*.*
3. $\mathcal{A}$ *outputs a guess* b' *of* b*.*

The success experiment in the above game, i.e., $b' = b$, is denoted by $\mathsf{Succ}_{\mathcal{A}}(\lambda)$*, and the advantage of* $\mathcal{A}$ *is defined as* $\mathsf{Adv}^{\mathsf{SIPE}}_{\mathcal{A}}(\lambda) := \Pr[\,\mathsf{Succ}_{\mathcal{A}}(\lambda)\,] - 1/2$ *for any security parameter* λ*. An SIPE scheme is* fully secure *if all probabilistic polynomial-time adversaries* $\mathcal{A}$ *have at most negligible advantage in the above game.*

3 Proposed (Basic) IPE-CC Scheme

3.1 Construction

We describe random dual orthonormal basis generator $\mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}$ below, which is used as a subroutine in the proposed IPE-CC and SIPE schemes.

$$\begin{aligned}
&\mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda, N): \ \mathsf{param}'_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N), \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, g_T := e(G,G)^\psi,\\
&\quad X := (\chi_{i,j}) \xleftarrow{\mathsf{U}} GL(N, \mathbb{F}_q), \ (\vartheta_{i,j}) := \psi \cdot (X^{\mathrm{T}})^{-1}, \ \mathsf{param}_{\mathbb{V}} := (\mathsf{param}'_{\mathbb{V}}, g_T),\\
&\quad \boldsymbol{b}_i := \textstyle\sum_{j=1}^N \chi_{i,j}\boldsymbol{a}_j, \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N), \ \boldsymbol{b}^*_i := \sum_{j=1}^N \vartheta_{i,j}\boldsymbol{a}_j, \mathbb{B}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_N),\\
&\quad \text{return} \ \ (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*).
\end{aligned}$$

We refer to Section 1.4 for notations on DPVS. For matrix $W := (w_{i,j})_{i,j=1,\ldots,N} \in \mathbb{F}_q^{N\times N}$ and element $\boldsymbol{g} := (G_1, \ldots, G_N)$ in N-dimensional $\mathbb{V}$, $\boldsymbol{g}W$ 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 like $(\boldsymbol{g}W)W^{-1} = \boldsymbol{g}(WW^{-1}) = \boldsymbol{g}$. The proposed scheme is given as:

$$\begin{aligned}
&\mathsf{Setup}(1^\lambda, \ n): \ (\mathsf{param}_{\mathbb{V}}, \mathbb{B} := (\boldsymbol{b}_1, .., \boldsymbol{b}_{6n}), \mathbb{B}^* := (\boldsymbol{b}^*_1, .., \boldsymbol{b}^*_{6n})) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda, N := 6n),\\
&\quad W \xleftarrow{\mathsf{U}} GL(N, \mathbb{F}_q), \ \ \boldsymbol{d}_i := \boldsymbol{b}_i W \text{ for } i = 1, \ldots, 6n, \ \ \mathbb{D} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{6n}),\\
&\quad \widehat{\mathbb{D}} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n, \boldsymbol{d}_{5n+1}, \ldots, \boldsymbol{d}_{6n}), \ \ \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{4n+1}, \ldots, \boldsymbol{b}^*_{5n}),\\
&\quad \text{return} \ \ \mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}}), \ \ \mathsf{ck} := W, \ \ \mathsf{sk} := \widehat{\mathbb{B}}^*.\\
&\mathsf{TokenGen}(\mathsf{pk}, \ \mathsf{sk}, \ \vec{v} \in \mathbb{F}_q^n \setminus \{\vec{0}\}): \ \ \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\\
&\quad \boldsymbol{k}^* := \ (\ \overbrace{\sigma\vec{v},}^{n} \ \ \overbrace{0^{3n},}^{3n} \ \ \overbrace{\vec{\eta},}^{n} \ \ \overbrace{0^n}^{n} \ )_{\mathbb{B}^*}, \ \ \text{return} \ \ \mathsf{tk}_{\vec{v}} := \boldsymbol{k}^*.\\
&\mathsf{Enc}(\mathsf{pk}, \ \vec{x} \in \mathbb{F}_q^n \setminus \{\vec{0}\}): \ \ \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \vec{\xi} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\\
&\quad \boldsymbol{f} := \ (\ \overbrace{\tau\vec{x},}^{n} \ \ \overbrace{0^{3n},}^{3n} \ \ \overbrace{0^n,}^{n} \ \ \overbrace{\vec{\xi}}^{n} \ )_{\mathbb{D}}, \ \ \ \text{return} \ \ \mathsf{ct}_{\vec{x}} := \boldsymbol{f}.\\
&\mathsf{Conv}(\mathsf{pk}, \ \mathsf{ck} := W, \ \mathsf{ct}_{\vec{x}} := \boldsymbol{f}): \ \ \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \ \boldsymbol{y} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{d}_{5n+1}, \ldots, \boldsymbol{d}_{6n}\rangle,\\
&\quad \boldsymbol{c} := (\rho\boldsymbol{f} + \boldsymbol{y})\,W^{-1}, \ \ \text{return} \ \ \mathsf{CT}_{\vec{x}} := \boldsymbol{c}.\\
&\mathsf{Query}(\mathsf{pk}, \ \mathsf{tk}_{\vec{v}} := \boldsymbol{k}^*, \ \mathsf{CT}_{\vec{x}} := \boldsymbol{c}):\\
&\quad \text{if } e(\boldsymbol{c}, \boldsymbol{k}^*) = 1, \ \text{output } 1, \quad \text{otherwise, output } 0.
\end{aligned}$$

Remark 2 To realize a delegation from $\mathsf{tk}_{\vec{v}}$ to $\mathsf{tk}_{\vec{v}\wedge\vec{w}}(:= \mathsf{tk}_{(\vec{v},\vec{w})})$ given in the introduction, we can construct a natural delegation algorithm in a similar manner to [17, 18, 19, 20]. We give the 2-level hierarchical IPE-CC (HIPE-CC) scheme in Section 3.3.

[Correctness] Since $\mathbb{D} \cdot W^{-1} := (\boldsymbol{d}_1 W^{-1}, \ldots, \boldsymbol{d}_{6n} W^{-1})$ is equal to $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{6n})$, $\boldsymbol{c} := (\rho\boldsymbol{f} + \boldsymbol{u})\,W^{-1} = (\ \omega\vec{x}, \ 0^{3n}, \ 0^n, \ \vec{\varphi}\ )_{\mathbb{D}} \cdot W^{-1} = (\ \omega\vec{x}, \ 0^{3n}, \ 0^n, \ \vec{\varphi}\ )_{\mathbb{D}\cdot W^{-1}} = (\ \omega\vec{x}, \ 0^{3n}, \ 0^n, \ \vec{\varphi}\ )_{\mathbb{B}}$, where $\omega \in \mathbb{F}_q$ and $\vec{\varphi} \in \mathbb{F}_q^n$ are uniformly and independently distributed. Therefore, if $\vec{v} \cdot \vec{x} = 0$, then $e(\boldsymbol{c}, \boldsymbol{k}^*) = g_T^{\omega\sigma\vec{v}\cdot\vec{x}} = 1$.

3.2 Security

The DLIN assumption is standard [18, 19, 20] and given in Definition 3.

Theorem 1 *The proposed IPE-CC scheme is fully secure under the DLIN assumption, i.e., for any adversary $\mathcal{A}$, all $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisU}}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisH}}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisPKG}}(\lambda)$ are negligible under the DLIN assumption.*

Proof. The proof of Theorem 1 is reduced to those of Lemmas 1–3. □

Lemma 1 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisU}}(\lambda)$ is negligible under the DLIN assumption.*

Lemma 2 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisH}}(\lambda)$ is negligible under the DLIN assumption.*

Lemma 3 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisPKG}}(\lambda)$ is negligible under the DLIN assumption.*

The proofs of Lemmas 1–3 are given in Appendix B.

3.3 Proposed (Basic 2-Level) Hierarchical IPE-CC Scheme

We refer to Section 1.4 for notations on DPVS. For matrix $W := (w_{i,j})_{i,j=1,\dots,N} \in \mathbb{F}_q^{N\times N}$ and element $\boldsymbol{g} := (G_1,\dots,G_N)$ in N-dimensional $\mathbb{V}$, for notation $\boldsymbol{g}W$, refer to Section 3.1. The hierarchical IPE-CC (HIPE-CC) below is based on the (basic) construction idea given in [16], however, since the scheme has enough hidden subspace and randomness spaces, the security is proven from the DLIN assumption.

$\mathsf{Setup}(1^\lambda,\ (n_1,\ n_2)\ ):\ n := n_1 + n_2,$

$(\mathsf{param}_{\mathbb{V}}, \mathbb{B} := (\boldsymbol{b}_1,\dots,\boldsymbol{b}_{6n}), \mathbb{B}^* := (\boldsymbol{b}_1^*,\dots,\boldsymbol{b}_{6n}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{IPE}}(1^\lambda, N := 6n),$

$W \xleftarrow{\mathsf{U}} GL(N,\mathbb{F}_q),\ \ \boldsymbol{d}_i := \boldsymbol{b}_i W \text{ for } i = 1,\dots,6n,\ \ \mathbb{D} := (\boldsymbol{d}_1,\dots,\boldsymbol{d}_{6n}),$

$\widehat{\mathbb{D}} := (\boldsymbol{d}_1,\dots,\boldsymbol{d}_n,\boldsymbol{d}_{5n+1},\dots,\boldsymbol{d}_{6n}),\ \ \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*,\dots,\boldsymbol{b}_n^*,\boldsymbol{b}_{4n+1}^*,\dots,\boldsymbol{b}_{5n}^*),$

$\text{return}\ \ \mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}}),\ \ \mathsf{ck} := W,\ \ \mathsf{sk} := \widehat{\mathbb{B}}^*.$

$\mathsf{TokenGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v}_1 \in \mathbb{F}_q^{n_1} \setminus \{\vec{0}\}):\ \ \sigma,\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}_0,\vec{\eta}_1,\dots,\vec{\eta}_{n_2} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,$

$$\begin{array}{rcl} \boldsymbol{k}_0^* &:=& (\ \overbrace{\sigma\vec{v}_1,\ 0^{n_2},}^{n}\ \ \overbrace{0^{3n},}^{3n}\ \ \overbrace{\vec{\eta}_0,}^{n}\ \ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*}, \\ \boldsymbol{k}_i^* &:=& (\ \sigma\vec{v}_1,\ \psi\vec{e}_i,\ \ 0^{3n},\ \ \vec{\eta}_i,\ \ 0^n\ )_{\mathbb{B}^*} \ \text{ for } i = 1,\dots,n_2, \end{array}$$

$$\text{where } \vec{e}_i := (\ 0^{i-1},\ 1,\ 0^{n_2-i}\ ),$$

$\text{return}\ \ \mathsf{tk}_{\vec{v}_1} := (\ \boldsymbol{k}_0^*,\ \boldsymbol{k}_1^*,\dots,\boldsymbol{k}_{n_2}^*\ ).$

$\mathsf{Enc}(\mathsf{pk},\ \vec{x}_1 \in \mathbb{F}_q^{n_1} \setminus \{\vec{0}\},\ \vec{x}_2 \in \mathbb{F}_q^{n_2}):\ \ \tau_1,\tau_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\xi} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,$

$\text{if } \vec{x}_2 = \vec{0},\ \vec{x}_2' \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_2},\ \ \text{else } \vec{x}_2' := \vec{x}_2,$

$$\boldsymbol{f} := (\ \overbrace{\tau_1\vec{x}_1,\ \tau_2\vec{x}_2',}^{n}\ \ \overbrace{0^{3n},}^{3n}\ \ \overbrace{0^n,}^{n}\ \ \overbrace{\vec{\xi}}^{n}\ )_{\mathbb{D}}, \qquad \text{return}\ \ \mathsf{ct}_{\vec{x}} := \boldsymbol{f}.$$

$\mathsf{Conv}(\mathsf{pk},\ \mathsf{ck} := W,\ \mathsf{ct}_{\vec{x}} := \boldsymbol{f}):\ \ \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \ \boldsymbol{y} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{d}_{5n+1},\dots,\boldsymbol{d}_{6n}\rangle,$

$\boldsymbol{c} := (\rho\boldsymbol{f} + \boldsymbol{y})\, W^{-1},\ \ \text{return}\ \ \mathsf{CT}_{\vec{x}} := \boldsymbol{c}.$

$\mathsf{Query}(\mathsf{pk},\ \mathsf{tk} := \mathsf{tk}_{\vec{v}_1} \text{ or } \mathsf{tk}_{(\vec{v}_1,\vec{v}_2)},\ \mathsf{CT}_{\vec{x}} := \boldsymbol{c}):$

$\text{if } \mathsf{tk} = \mathsf{tk}_{\vec{v}_1} = (\ \boldsymbol{k}_0^*,\ \boldsymbol{k}_1^*,\dots,\boldsymbol{k}_{n_2}^*\ ),$

$\text{if } e(\boldsymbol{c},\boldsymbol{k}_0^*) = 1,\ \text{output } 1,\ \ \text{otherwise, output } 0.$

$\text{if } \mathsf{tk} = \mathsf{tk}_{(\vec{v}_1,\vec{v}_2)} = \widetilde{\boldsymbol{k}}^*,\ \ \text{if } e(\boldsymbol{c},\widetilde{\boldsymbol{k}}^*) = 1,\ \text{output } 1,\ \ \text{otherwise, output } 0.$

```
Delegate(pk, $\mathsf{tk}_{\vec{v}_1} := (\ \boldsymbol{k}_0^*,\ \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_{n_2}^*\ ),\ \vec{v}_2 := (v_{2,1}, \ldots, v_{2,n_2}) \in \mathbb{F}_q^{n_2} \setminus \{\vec{0}\})$ :
    $\xi, \delta \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}' := (\eta'_1, \ldots, \eta'_n) \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,$
    $\widetilde{\boldsymbol{k}}^* := \xi \boldsymbol{k}_0^* + \delta(\sum_{i=1}^{n_2} v_{2,i} \boldsymbol{k}_i^*) + \sum_{i=1}^{n} \eta'_i \boldsymbol{b}_{4n+i}^*,$
    return $\mathsf{tk}_{(\vec{v}_1, \vec{v}_2)} (= \mathsf{tk}_{\vec{v}_1 \wedge \vec{v}_2}) := \widetilde{\boldsymbol{k}}^*.$
```

The full security notion of IPE-CC is extended to that for (2-level) HIPE-CC schemes in a usual way.

Theorem 2 *The proposed (2-level) HIPE-CC scheme is fully secure under the DLIN assumption.*

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

Remark:

1. While we present a 2-level HIPE-CC scheme here, clearly, the construction can be extended to an arbitrary level HIPE-CC scheme.
2. While the above basic HIPE-CC scheme is built based on [16], if we apply several techniques given in [18, 19], efficiency of the HIPE scheme is greatly improved.

4 Proposed SIPE Scheme (Conversion from IPE-CC to SIPE)

The definitions of symmetric-key IPE (SIPE) and full security of SIPE are given in Section 2.4.

From the above IPE-CC scheme, we obtain the first fully secure SIPE scheme. Namely, using the IPE-CC scheme, $\Pi_{\mathsf{IPE\text{-}CC}} := (\mathsf{Setup}, \mathsf{TokenGen}, \mathsf{Enc}, \mathsf{Conv}, \mathsf{Query})$, a modified setup algorithm $\mathsf{Setup}'(1^\lambda,\ n)$ outputs a (master) secret key $\mathsf{sk}' := (\mathsf{pk}, \mathsf{ck}, \mathsf{sk})$, where $(\mathsf{pk}, \mathsf{ck}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda,\ n)$, and a modified encryption algorithm $\mathsf{Enc}'(\mathsf{sk}',\ \vec{x})$ outputs a ciphertext $\mathsf{CT}'_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Conv}(\mathsf{pk}, \mathsf{ck}, \mathsf{ct}_{\vec{x}})$, where $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk},\ \vec{x})$, and the rest of algorithms, $\mathsf{TokenGen}$ and Query are the same as those of the IPE-CC scheme since an input sk' of $\mathsf{TokenGen}$ includes $(\mathsf{pk}, \mathsf{sk})$. Hence, we obtain a (converted) SIPE, $\Pi_{\mathsf{SIPE}} := (\mathsf{Setup}', \mathsf{TokenGen}, \mathsf{Enc}', \mathsf{Query})$.

Theorem 3 *The proposed SIPE scheme is fully secure under the DLIN assumption.*

Proof. By the construction, the full security for SIPE Π_{SIPE} is reduced from the Dishonest-User Game security for IPE-CC $\Pi_{\mathsf{IPE\text{-}CC}}$, i.e., for any adversary $\mathcal{A}$, we can construct $\mathcal{A}'$ from $\mathcal{A}$ s.t. $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{SIPE}}(\lambda)$ for Π_{SIPE} in Def. 7 is less than or equal to $\mathsf{Adv}_{\mathcal{A}'}^{\mathsf{DisU}}(\lambda)$ for $\Pi_{\mathsf{IPE\text{-}CC}}$ in Def. 5. Hence, Lemma 1 implies Theorem 3. □

5 A Variant for Achieving Shorter Public and Secret Keys

A variant of the proposed (basic) IPE-CC scheme with the same security, that achieves a shorter ($O(n)$-size) public key and secret key, can be constructed by combining with the techniques in [19], where n is the dimension of vectors of the IPE-CC scheme. Here, we show this variant.

5.1 Construction and Security

Let $N := 6n$ and

$$\mathcal{H}(n,\mathbb{F}_q) := \left\{ \begin{pmatrix} \mu''_1 & \mu''_2 & \cdots & \mu''_{n-1} & \mu''' \\ & \mu & & & \mu'_2 \\ & & \ddots & & \vdots \\ & & & \mu & \mu'_{n-1} \\ & & & & \mu'_n \end{pmatrix} \middle| \begin{array}{l} \mu, \mu'_2, \ldots, \mu'_n, \\ \mu''_1, \ldots, \mu''_{n-1}, \mu''' \in \mathbb{F}_q, \\ \text{a blank element in the matrix} \\ \text{denotes } 0 \in \mathbb{F}_q \end{array} \right\},$$

$$\mathcal{L}(6,n,\mathbb{F}_q) := \left\{ X := \begin{pmatrix} X_{1,1} & \cdots & X_{1,6} \\ \vdots & & \vdots \\ X_{6,1} & \cdots & X_{6,6} \end{pmatrix} \middle| \begin{array}{l} X_{i,j} \in \mathcal{H}(n,\mathbb{F}_q) \\ \text{for } i,j = 1,\ldots,6 \end{array} \right\} \bigcap GL(N,\mathbb{F}_q).$$

We note that $\mathcal{L}(6,n,\mathbb{F}_q)$ is a subgroup of $GL(N,\mathbb{F}_q)$ (Lemma 4). For $X \in \mathcal{L}(6,n,\mathbb{F}_q)$, we denote ($\psi$-times) its adjoint matrix $(X^{-1})^{\mathrm{T}}$ as a sparse form

$$(X^{-1})^{\mathrm{T}} := \begin{pmatrix} Y_{1,1} & \cdots & Y_{1,6} \\ \vdots & & \vdots \\ Y_{6,1} & \cdots & Y_{6,6} \end{pmatrix}, \text{ where } Y_{i,j} := \begin{pmatrix} \vartheta''_{i,j,1} & & & & \\ \vartheta''_{i,j,2} & \vartheta_{i,j} & & & \\ \vdots & & \ddots & & \\ \vartheta''_{i,j,n-1} & & & \vartheta_{i,j} & \\ \vartheta'''_{i,j} & \vartheta'_{i,j,2} & \cdots & & \vartheta'_{i,j,n} \end{pmatrix}$$

for $i,j = 1,\ldots,6$. Here, a blank element in the above matrix denotes $0 \in \mathbb{F}_q$. That is, $X \in \mathcal{L}(6,n,\mathbb{F}_q)$ is represented by $72n$ non-zero entries $\{\mu_{i,j}, \mu'_{i,j,2}, \ldots, \mu'_{i,j,n}, \mu''_{i,j,1}, \ldots, \mu''_{i,j,n-1}, \mu'''_{i,j}\}_{i,j=1,\ldots 6}$, and $\psi(X^{-1})^{\mathrm{T}}$ is represented by $72n$ non-zero entries $\{\vartheta_{i,j}, \vartheta'_{i,j,2}, \ldots, \vartheta'_{i,j,n}, \vartheta''_{i,j,1}, \ldots, \vartheta''_{i,j,n-1}, \vartheta'''_{i,j}\}_{i,j=1,\ldots 6}$.

Random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{ZIPE,SK}}$ with *sparse* matrices below is used as a subroutine in the proposed variants of IPE-CC and SIPE schemes.

$$\begin{array}{l}
\mathcal{G}_{\mathsf{ob}}^{\mathsf{ZIPE,SK}}(1^\lambda, 6, n): \quad \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),\ N := 6n, \\
\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ g_T := e(G,G)^\psi,\ \mathsf{param}'_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N, \mathsf{param}_{\mathbb{G}}), \\
\mathsf{param}_{\mathbb{V}} := (\mathsf{param}'_{\mathbb{V}},\ g_T),\ X \xleftarrow{\mathsf{U}} \mathcal{L}(6,n,\mathbb{F}_q), \\
\text{hereafter, } \{\mu_{i,j}, \mu'_{i,j,2}, .., \mu'_{i,j,n}, \mu''_{i,j,1}, .., \mu''_{i,j,n-1}, \mu'''_{i,j}\}_{i,j=1,\ldots 6} \text{ denotes} \\
\text{non-zero entries of } X, \text{ and } \{\vartheta_{i,j}, \vartheta'_{i,j,2}, .., \vartheta'_{i,j,n}, \vartheta''_{i,j,1}, .., \vartheta''_{i,j,n-1}, \vartheta'''_{i,j}\}_{i,j=1,\ldots 6} \\
\text{denotes non-zero entries of } \psi(X^{-1})^{\mathrm{T}}, \\
\{B_{i,j} := \mu_{i,j}G, B'_{i,j,2} := \mu'_{i,j,2}G, \ldots, B'_{i,j,n} := \mu'_{i,j,n}G, \\
\quad B''_{i,j,1} := \mu''_{i,j,1}G, \ldots, B''_{i,j,n-1} := \mu''_{i,j,n-1}G, B'''_{i,j} := \mu'''_{i,j}G\}_{i,j=1,\ldots 6}, \\
\{B^*_{i,j} := \vartheta_{i,j}G, B'^*_{i,j,2} := \vartheta'_{i,j,2}G, \ldots, B'^*_{i,j,n} := \vartheta'_{i,j,n}G, \\
\quad B''^*_{i,j,1} := \vartheta''_{i,j,1}G, \ldots, B''^*_{i,j,n-1} := \vartheta''_{i,j,n-1}G, B'''^*_{i,j} := \vartheta'''_{i,j}G\}_{i,j=1,\ldots 6}, \\
\text{return } \ (\mathsf{param}_{\mathbb{V}}, \{B_{i,j}, B'_{i,j,2}, \ldots, B'_{i,j,n}, B''_{i,j,1}, \ldots, B''_{i,j,n-1}, B'''_{i,j}\}_{i,j=1,\ldots 6}, \\
\quad \{B^*_{i,j}, B'^*_{i,j,2}, \ldots, B'^*_{i,j,n}, B''^*_{i,j,1}, \ldots, B''^*_{i,j,n-1}, B'''^*_{i,j}\}_{i,j=1,\ldots 6}).
\end{array}$$

Remark 3 Let

$$\begin{pmatrix} \boldsymbol{b}_{(i-1)n+1} \\ \vdots \\ \boldsymbol{b}_{in} \end{pmatrix} := \begin{pmatrix} B''_{i,1,1} & B''_{i,1,2} & \cdots & B'''_{i,1} & & B''_{i,6,1} & B''_{i,6,2} & \cdots & B'''_{i,6} \\ & B_{i,1} & & B'_{i,1,2} & & & B_{i,6} & & B'_{i,6,2} \\ & & \ddots & \vdots & \cdots & & & \ddots & \vdots \\ & & & B'_{i,1,n} & & & & & B'_{i,6,n} \end{pmatrix} \tag{1}$$

$$\begin{pmatrix} \boldsymbol{b}^*_{(i-1)n+1} \\ \vdots \\ \boldsymbol{b}^*_{in} \end{pmatrix} := \begin{pmatrix} B''^*_{i,1,1} & & & & & B''^*_{i,6,1} & & & \\ B''^*_{i,1,2} & B^*_{i,1} & & & \cdots & B''^*_{i,6,2} & B^*_{i,6} & & \\ \vdots & & \ddots & & & \vdots & & \ddots & \\ B'''^*_{i,1} & B'^*_{i,1,2} & \ldots & B'^*_{i,1,n} & & B'''^*_{i,6} & B'^*_{i,6,2} & \ldots & B'^*_{i,6,n} \end{pmatrix}$$

for $i = 1, \ldots, 6$, and $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{6n}), \mathbb{B}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_{6n})$, where a blank element in the matrices denotes $0 \in \mathbb{G}$. $(\mathbb{B}, \mathbb{B}^*)$ are the dual orthonormal bases, i.e., $e(\boldsymbol{b}_i, \boldsymbol{b}^*_i) = g_T$ and $e(\boldsymbol{b}_i, \boldsymbol{b}^*_j) = 1$ for $1 \le i \ne j \le 6n$.

Here, we assume that input vectors, $\vec{x} := (x_1, \ldots, x_n)$ and $\vec{v} := (v_1, \ldots, v_n)$, satisfies $x_1 \ne 0$ and $v_n \ne 0$. The proposed scheme is given as:

```
$\mathsf{Setup}(1^\lambda,\ n)$ :
  $(\mathsf{param}_{\mathbb{V}}, \{B_{i,j}, B'_{i,j,2}, \ldots, B'_{i,j,n}, B''_{i,j,1}, \ldots, B''_{i,j,n-1}, B'''_{i,j}\}_{i,j=1,\ldots 6},$
   $\{B^*_{i,j}, B'^*_{i,j,2}, \ldots, B'^*_{i,j,n}, B''^*_{i,j,1}, \ldots, B''^*_{i,j,n-1}, B'''^*_{i,j}\}_{i,j=1,\ldots 6}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{ZIPE,SK}}_{\mathsf{ob}}(1^\lambda, 6, n),$
  $W \xleftarrow{\mathsf{U}} \mathcal{L}(6, n, \mathbb{F}_q), \quad \begin{pmatrix} \boldsymbol{d}_1 \\ \vdots \\ \boldsymbol{d}_{6n} \end{pmatrix} := \begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_{6n} \end{pmatrix} \cdot W,$ where $(\boldsymbol{b}_i)_{i=1,\ldots,6n}$ is given in Eq. (1), and $(\boldsymbol{d}_i)_{i=1,\ldots,6n}$ is represented as in Eq. (1) using
  $\{D_{i,j}, D'_{i,j,2}, \ldots, D'_{i,j,n}, D''_{i,j,1}, \ldots, D''_{i,j,n-1}, D'''_{i,j}\}_{i,j=1,\ldots 6},$
  return $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \{D_{i,j}, D'_{i,j,2}, .., D'_{i,j,n}, D''_{i,j,1}, .., D''_{i,j,n-1}, D'''_{i,j}\}_{i=1,6;\, j=1,..,6}),$
   $\mathsf{ck} := W, \quad \mathsf{sk} := \{B^*_{i,j}, B'^*_{i,j,2}, .., B'^*_{i,j,n}, B''^*_{i,j,1}, .., B''^*_{i,j,n-1}, B'''^*_{i,j}\}_{i=1,5;\, j=1,..,6}.$
$\mathsf{TokenGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v})$ :   $\sigma, \eta_1, \ldots, \eta_n \xleftarrow{\mathsf{U}} \mathbb{F}_q,$
  for $j = 1, .., 6,$   $K^*_{j,1} := \sum_{l=1}^{n-1} (\sigma v_l B''^*_{1,j,l} + \eta_l B''^*_{5,j,l}) + \sigma v_n B'''^*_{1,j} + \eta_n B'''^*_{5,j},$
    $K^*_{j,l} := \sigma(v_l B^*_{1,j} + v_n B'^*_{1,j,l}) + \eta_l B^*_{5,j} + \eta_n B'^*_{5,j,l}$ for $l = 2, \ldots, n-1,$
    $K^*_{j,n} := \sigma v_n B'^*_{1,j,n} + \eta_n B'^*_{5,j,n},$
  $\boldsymbol{k}^* := (K^*_{1,1}, \ldots, K^*_{1,n}, \ldots \quad , K^*_{6,1}, \ldots, K^*_{6,n}) \in \mathbb{G}^{6n},$   return $\mathsf{tk}_{\vec{v}} := \boldsymbol{k}^*.$
$\mathsf{Enc}(\mathsf{pk},\ \vec{x})$ :   $\omega, \varphi_1, \ldots, \varphi_n \xleftarrow{\mathsf{U}} \mathbb{F}_q,$
  for $j = 1, .., 6,$   $F_{j,1} := \omega x_1 D''_{1,j,1} + \varphi_1 D''_{6,j,1},$
    $F_{j,l} := \omega(x_1 D''_{1,j,l} + x_l D_{1,j}) + \varphi_1 D''_{6,j,l} + \varphi_l D_{6,j}$ for $l = 2, \ldots, n-1,$
    $F_{j,n} := \omega x_1 D'''_{1,j} + \varphi_1 D'''_{6,j} + \sum_{l=2}^{n} (\omega x_l D''_{1,j,l} + \varphi_l D''_{6,j,l}),$
  $\boldsymbol{f} := (F_{1,1}, \ldots, F_{1,n}, \ldots \quad , F_{6,1}, \ldots, F_{6,n}) \in \mathbb{G}^{6n},$   return $\mathsf{ct}_{\vec{x}} := \boldsymbol{f}.$
$\mathsf{Conv}(\mathsf{pk},\ \mathsf{ck} := W,\ \mathsf{ct}_{\vec{x}} := \boldsymbol{f})$ :   $\rho \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{y} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{d}_{5n+1}, \ldots, \boldsymbol{d}_{6n} \rangle,$
  $\boldsymbol{c} := (\rho \boldsymbol{f} + \boldsymbol{y})\, W^{-1},$   return $\mathsf{CT}_{\vec{x}} := \boldsymbol{c}.$
$\mathsf{Query}(\mathsf{pk},\ \mathsf{tk}_{\vec{v}} := \boldsymbol{k}^*,\ \mathsf{CT}_{\vec{x}} := \boldsymbol{c})$ :
  if $e(\boldsymbol{c}, \boldsymbol{k}^*) = 1,$   return 1,   otherwise,   return 0.
```

Remark 4 A part of output of $\mathsf{Setup}(1^\lambda, n)$, $\{D_{i,j}, D'_{i,j,2}, \ldots, D'_{i,j,n}, D''_{i,j,1}, \ldots, D''_{i,j,n-1}, D'''_{i,j}\}_{i=1,6;\ j=1,\ldots 6}$, can be identified with $\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n, \boldsymbol{d}_{5n+1}, \ldots,\ \boldsymbol{d}_{6n})$, while $\mathbb{D} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{6n})$ is identified with $\{D_{i,j}, D'_{i,j,2}, \ldots, D'_{i,j,n}, D''_{i,j,1},\ \ldots, D''_{i,j,n-1}, D'''_{i,j}\}_{i,j=1,\ldots 6}$ as in Remark 3. Also, $\{B^*_{i,j}, B'^*_{i,j,2}, \ldots, B'^*_{i,j,n}, B''^*_{i,j,1}, \ldots, B''^*_{i,j,n-1}, B'''^*_{i,j}\}_{i=1,5;\ j=1,\ldots 6}$ can be identified with $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{4n+1}, \ldots, \boldsymbol{b}^*_{5n})$, while $\mathbb{B}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_{6n})$ is identified with $\{B^*_{i,j}, B'^*_{i,j,2}, \ldots, B'^*_{i,j,n},\ B''^*_{i,j,1}, \ldots, B''^*_{i,j,n-1}, B'''^*_{i,j}\}_{i,j=1,\ldots 6}$ in Remark 3. In Query, $\boldsymbol{c}$ and $\boldsymbol{k}^*$ can be alternatively described as

Table 1: Comparison with pairing-based IPE schemes in [14, 20, 24], where $|\mathbb{G}|$ represents size of an element of $\mathbb{G}$. PH, AH, PK, SK, TK, CT, GSD, and C3DH stand for predicate-hiding, attribute-hiding, public key, secret key, token, ciphertext, general subgroup decision [1], and composite 3-party (decisional) Diffie-Hellman [24], respectively.

	KSW08	OT12 IPE [20]		Proposed IPE-CC		SSW09	Proposed SIPE	
	IPE [14]	(basic)	(variant)	(basic)	(variant)	SIPE [24]	(basic)	(variant)
Setting	public key	public key		public key		secret key	secret key	
Security	selective & fully-AH	adaptive & fully-AH		adaptive & fully-secure (PH & AH)		selective & single-chal. PH & AH	adaptive & fully-secure (PH & AH)	
Order of $\mathbb{G}$	composite	prime		prime		composite	prime	
Assump.	2 variants of GSD	DLIN		DLIN		A variant of GSD, C3DH,DLIN	DLIN	
PK size	$O(n)\vert\mathbb{G}\vert$	$O(n^2)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$	$O(n^2)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$	–	–	–
SK size	$O(n)\vert\mathbb{G}\vert$	$O(n^2)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$	$O(n^2)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$	$O(n^2)\vert\mathbb{G}\vert$	$O(n)\vert\mathbb{G}\vert$
TK size	$(2n{+}1)\vert\mathbb{G}\vert$	$(4n{+}1)\vert\mathbb{G}\vert$	$10\vert\mathbb{G}\vert$	$6n\vert\mathbb{G}\vert$		$(2n+2)\vert\mathbb{G}\vert$	$6n\vert\mathbb{G}\vert$	
CT size	$(2n{+}1)\vert\mathbb{G}\vert$	$(4n{+}1)\vert\mathbb{G}\vert$	$5n\vert\mathbb{G}\vert$	$6n\vert\mathbb{G}\vert$		$(2n+2)\vert\mathbb{G}\vert$	$6n\vert\mathbb{G}\vert$	

$\boldsymbol{c} = (\overbrace{\omega\vec{x},}^{n}\ \overbrace{0^{3n},}^{3n}\ \overbrace{0^{n},}^{n}\ \overbrace{\vec{\varphi}}^{n}\ )_{\mathbb{B}}$, $\boldsymbol{k}^* = (\overbrace{\sigma\vec{v},}^{n}\ \overbrace{0^{3n},}^{3n}\ \overbrace{\vec{\eta},}^{n}\ \overbrace{0^{n}}^{n}\ )_{\mathbb{B}^*}$, where $\vec{\varphi} := (\varphi_1, \ldots, \varphi_n), \vec{\eta} := (\eta_1, \ldots, \eta_n) \in \mathbb{F}_q^n$.

Theorem 4 *The proposed IPE-CC scheme (with short public and secret keys) is fully secure under the DLIN assumption.*

Theorem 4 is proven in a similar manner to Theorem 3 (and 4) in [19]. For achieving dual system encryption proof for IPE-CC with employing a sparse matrix, $X \xleftarrow{\mathsf{U}} \mathcal{L}(6, n, \mathbb{F}_q)$, for base change, the matrix set $\mathcal{L}(6, n, \mathbb{F}_q)$ should form a (matrix) group. (For the reason, refer to [19].) Therefore, proofs of Theorem 1 and Theorem 4 have the same high-level structure using the full matrix group $GL(6n, \mathbb{F}_q)$ and a subgroup $\mathcal{L}(6, n, \mathbb{F}_q)$ based on Lemma 4, respectively.

Lemma 4 $\mathcal{L}(6, n, \mathbb{F}_q)$ *is a subgroup of* $GL(6n, \mathbb{F}_q)$.

Lemma 4 is proven in a similar manner to Lemma 2 in the full version of [19].

6 Efficiency Comparisons

Table 1 compares the proposed IPE-CC schemes in Sections 3 and 5 with pairing-based attribute-hiding IPE schemes in [14, 20], and compares the proposed SIPE schemes in Sections 4 (and 5) with pairing-based predicate- and attribute-hiding SIPE scheme in [24].

Acknowledgments. The authors would like to thank anonymous reviewers for their valuable comments.

References

[1] Mihir Bellare, Brent Waters, and Scott Yilek. Identity-based encryption secure against selective opening attack. In Ishai [13], pages 235–252.

[2] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238. Springer, 2004.

[3] Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Franklin [12], pages 443–459.

[4] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Franklin [12], pages 41–55.

[5] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, 2001.

[6] Dan Boneh, Eyal Kushilevitz, Rafail Ostrovsky, and William E. Skeith III. Public key encryption that allows PIR queries. In Alfred Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 50–67. Springer, 2007.

[7] Dan Boneh, Ananth Raghunathan, and Gil Segev. Function-private identity-based encryption: Hiding the function in functional encryption. In Ran Canetti and Juan A. Garay, editors, *CRYPTO (2)*, volume 8043 of *LNCS*, pages 461–478. Springer, 2013.

[8] Dan Boneh, Ananth Raghunathan, and Gil Segev. Function-private subspace-membership encryption and its applications. *IACR Cryptology ePrint Archive*, 2013:403, 2013.

[9] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Ishai [13], pages 253–273.

[10] 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.

[11] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *IMA Int. Conf. 2001*, volume 2260 of *LNCS*, pages 360–363. Springer, 2001.

[12] Matthew K. Franklin, editor. *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *LNCS*. Springer, 2004.

[13] Yuval Ishai, editor. *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*, volume 6597 of *LNCS*. Springer, 2011.

[14] 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.

[15] Yutaka Kawai and Katsuyuki Takashima. Fully-anonymous functional proxy-re-encryption. *IACR Cryptology ePrint Archive*, 2013:318, 2013.

[16] 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`.

[17] 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.

[18] 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`.

[19] 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`.

[20] 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`.

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

[22] Tatsuaki Okamoto and Katsuyuki Takashima. Efficient (hierarchical) inner-product encryption tightly reduced from the decisional linear assumption. *IEICE Transactions*, 96-A(1):42–52, 2013.

[23] Jong Hwan Park. Inner-product encryption under standard assumptions. *Des. Codes Cryptography*, 58(3):235–257, 2011.

[24] Emily Shen, Elaine Shi, and Brent Waters. Predicate privacy in encryption systems. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 457–473. Springer, 2009.

[25] Elaine Shi, John Bethencourt, Hubert T.-H. Chan, Dawn Xiaodong Song, and Adrian Perrig. Multi-dimensional range query over encrypted data. In *IEEE Symposium on Security and Privacy*, pages 350–364. IEEE Computer Society, 2007.

[26] Masayuki Yoshino, Noboru Kunihiro, Ken Naganuma, and Hisayoshi Sato. Symmetric inner-product predicate encryption based on three groups. In Tsuyoshi Takagi, Guilin Wang, Zhiguang Qin, Shaoquan Jiang, and Yong Yu, editors, *ProvSec*, volume 7496 of *LNCS*, pages 215–234. Springer, 2012.

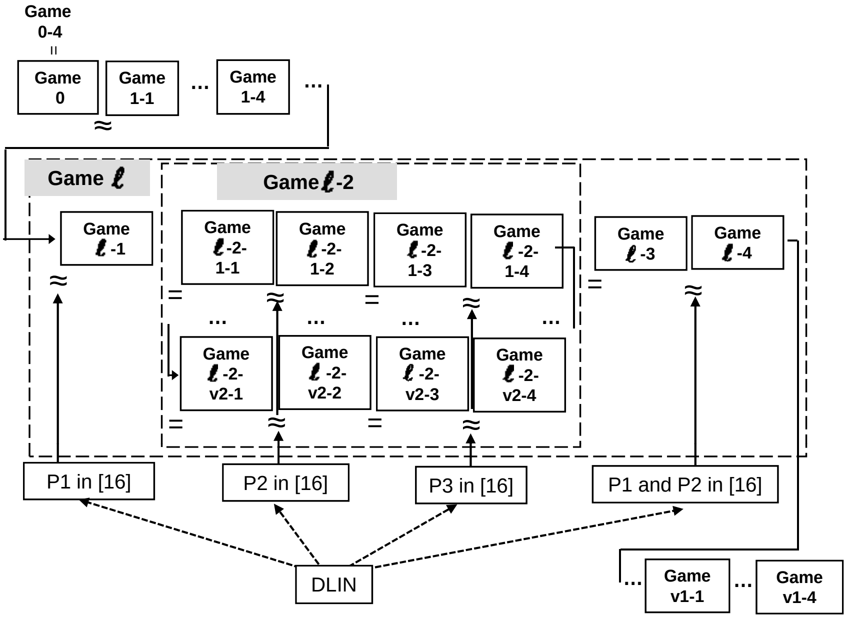


Figure 3: Structure of Reductions in the proof of Lemma 2

A Multi-System Proof Technique

A.1 Structural Comparison of our IPE-CC Scheme with the IPE in [20]

Since our security proofs (in particular, for Lemma 1) are extensions of the proof given in [20], we begin to compare our predicate-hiding IPE-CC with the existing attribute-hiding (not predicate-hiding) IPE [20].

Okamoto-Takashima [20] gave an attribute-hiding IPE scheme on DPVS framework. Ciphertexts (CT) and (secret-key) token (TK) of the scheme have dimension $4n+2 = 1+n+2n+n+1$, where the first one dimension is for encryption of plaintext (not attribute), the second is the real-encoding part (real part, for short) for CT and TK vectors, the third is the hidden part for achieving various forms of CT and TK, the fourth is the TK randomness part, and the fifth is the CT randomness part. Here, because we do not treat a plaintext other than attribute, CT and TK of the scheme are considered as composed of four parts, as indicated below, where the dimension structure is given by $4n + 1 = n + 2n + n + 1$. CT and TK of our IPE-CC have the same form, but dimension of each part is different, with $6n = n + 3n + n + n$ inner-structure. Particularly, $3n$ dimensional hidden part is crucial for our elaborated security proof of Lemma 1, where three blocks of n dimensional subspaces have different roles in the proof. We call it the *multi-system proof technique*, and the details are explained in Appendix A.2.

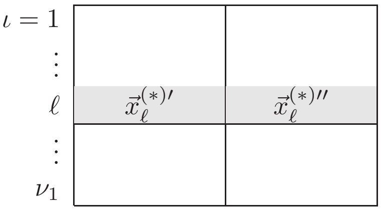
$$\text{CT \& TK in [20] IPE} \;:\; (\;\overbrace{\quad\text{real}\quad}^{n}\; \overbrace{\qquad\text{hidden}\qquad}^{2n}\; \overbrace{\;\text{TK ran.}\;}^{n}\; \overbrace{\;\text{CT ran.}\;}^{1}\;),$$

$$\text{CT \& TK in our IPE-CC} \;:\; (\;\overbrace{\quad\text{real}\quad}^{n}\; \overbrace{\qquad\qquad\text{hidden}\qquad\qquad}^{3n}\; \overbrace{\;\text{TK ran.}\;}^{n}\; \overbrace{\;\text{CT ran.}\;}^{n}\;).$$

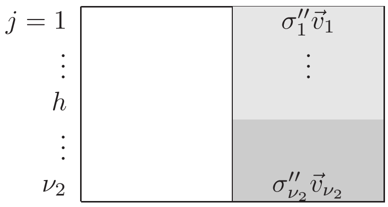
A.2 Intuitions for Proofs of Lemmas 1–3

First, we consider the proof of Lemma 2, where malicious helper $\mathcal{A}$, i.e., adversary has the conversion key W. By computing $\widehat{\mathbb{B}} := \widehat{\mathbb{D}} \cdot W^{-1}$, he knows $\widehat{\mathbb{B}}$. Then, the view of the adversary and the security definition (for the malicious helper) are the equivalent to those given in [20] for fully-attribute-hiding of IPE, except that multiple ciphertext challenges are considered in this paper, while single challenge is treated in [20]. Therefore, we can take a standard hybrid argument to achieve multiple challenge security from single challenge security, which is described in Figure 3. (In the figure, P1, P2, P3 stand for Problem 1, 2, 3, respectively.) Let ν_1 be the maximum number of $\mathcal{A}$'s challenge ciphertext queries and ν_2 the maximum number of $\mathcal{A}$'s challenge token queries. The reduction starts Game 0, and repeat Game ℓ sequences for $\ell = 1, \ldots, \nu_1$, where each sequence transform the ℓ-th queried ciphertext to an unbiased one for $b \in \{0, 1\}$. The ℓ-th sequence consists of four parts, Game ℓ-1, Game ℓ-2 sequence, Game ℓ-3, Game ℓ-4, where the main ℓ-2 sequence has another loop structure parametrized by $h = 1, \ldots, \nu_2$. The Game ℓ-2 sequence repeats four Games, Game ℓ-2-h-1,..., Game ℓ-2-h-4, for $h = 1, \ldots, \nu_2$. In the last ℓ-2-ν_2-4 in the sequence, coefficients of the $2n$-dimensional hidden part, i.e., $\mathsf{span}\langle \boldsymbol{d}_{n+1}, \ldots, \boldsymbol{d}_{3n} \rangle$ (resp. $\mathsf{span}\langle \boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{3n} \rangle$) of the ι-th queried $\boldsymbol{f}_\iota$ for $\iota = 1, \ldots, \nu_1$ (resp. the j-th queried $\boldsymbol{k}^*_j$ for $j = 1, \ldots, \nu_2$) w.r.t. these bases vectors are given as:

Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game ℓ-2-ν_2-4



Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game ℓ-2-ν_2-4



where $\vec{x}_\ell^{(*)\prime} := \tau'_{\ell,0} \vec{x}_\ell^{(0)} + \tau'_{\ell,1} \vec{x}_\ell^{(1)}$, $\vec{x}_\ell^{(*)\prime\prime} := \tau''_{\ell,0} \vec{x}_\ell^{(0)} + \tau''_{\ell,1} \vec{x}_\ell^{(1)}$ (unbiased form). In the second block of the hidden part, an unbiased vector $\vec{x}_\ell^{(*)\prime\prime}$ for the ℓ-th query (and zero for the rest of the $\iota (\neq \ell)$-th queries) in ciphertexts and (normal) $\vec{v}$-vectors, $\sigma''_1 \vec{v}_1, \ldots, \sigma''_{\nu_2} \vec{v}_{\nu_2}$, in tokens are placed. Therefore, the unbiased coefficient $\vec{x}_\ell^{(*)\prime\prime}$ is reflected to the real encoding part since the addition of b-biased $\tau \vec{x}_\ell^{(b)}$ and unbiased $\theta \vec{x}_\ell^{(*)\prime\prime}$ ($\theta \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_q$) is also unbiased, i.e., transforms $\boldsymbol{f}_\ell$ to an unbiased one. See [20] for the details.

Next, we consider the proof of Lemma 1, where malicious user has no secret keys, sk nor W, but he can ask two types of challenges, $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ for $\ell = 1, \ldots, \nu_1$ and $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ for $h = 1, \ldots, \nu_2$. The condition on the challenges is given by $f_{\vec{v}_h^{(0)}}(\vec{x}_\ell^{(0)}) = f_{\vec{v}_h^{(1)}}(\vec{x}_\ell^{(1)})$. In general, an unbiased form $\vec{x}_\ell^{(*)} := \omega_0 \vec{x}_\ell^{(0)} + \omega_1 \vec{x}_\ell^{(1)}$ does not preserve the value of the predicate, e.g., neither $f_{\vec{v}_h^{(0)}}(\vec{x}_\ell^{(*)})$ nor $f_{\vec{v}_h^{(1)}}(\vec{x}_\ell^{(*)})$ is determined from the value of $f_{\vec{v}_h^{(0)}}(\vec{x}_\ell^{(0)}) = f_{\vec{v}_h^{(1)}}(\vec{x}_\ell^{(1)})$. Since the unbiased form is not useful for reflecting the condition to the security proof, we must take another strategy. Through several game hoppings, we change the view of the adversary with challenge bit b to that with $1 - b$. The structure of the reduction is given in Figure 4. (In the figure, P1,..., P6 stand for Problem 1,..., 6, respectively.) The reduction starts Game 0, and after repeating Game 1-ℓ sequences for $\ell = 1, \ldots, \nu_1$, repeat Game 2-h sequences for $h = 1, \ldots, \nu_2$, where each sequence transform the h-th queried token to another kind of unbiased form for $b \in \{0, 1\}$ in the sense that forms of Eqs. (15) and (16) in Game 3 are equivalent: The h-th sequence consists of three parts, Game 2-h-1, Game 2-h-2 sequence, and Game 2-h-3, where the main 2-h-2 sequence has another loop structure parametrized by $\ell = 1, \ldots, \nu_1$. The Game 2-h-2 sequence repeats four Games, Game 2-h-2-ℓ-1,..., Game 2-h-2-ℓ-4, for $\ell = 1, \ldots, \nu_1$. In the last 2-h-2-ℓ-4 in the sequence, coefficients of the $3n$-dimensional hidden part, i.e., $\mathsf{span}\langle \boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{4n} \rangle$ (resp. $\mathsf{span}\langle \boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{4n} \rangle$) of the ι-th queried $\boldsymbol{c}_\iota$ for $\iota = 1, \ldots, \nu_1$ (resp. the j-th queried $\boldsymbol{k}^*_j$ for

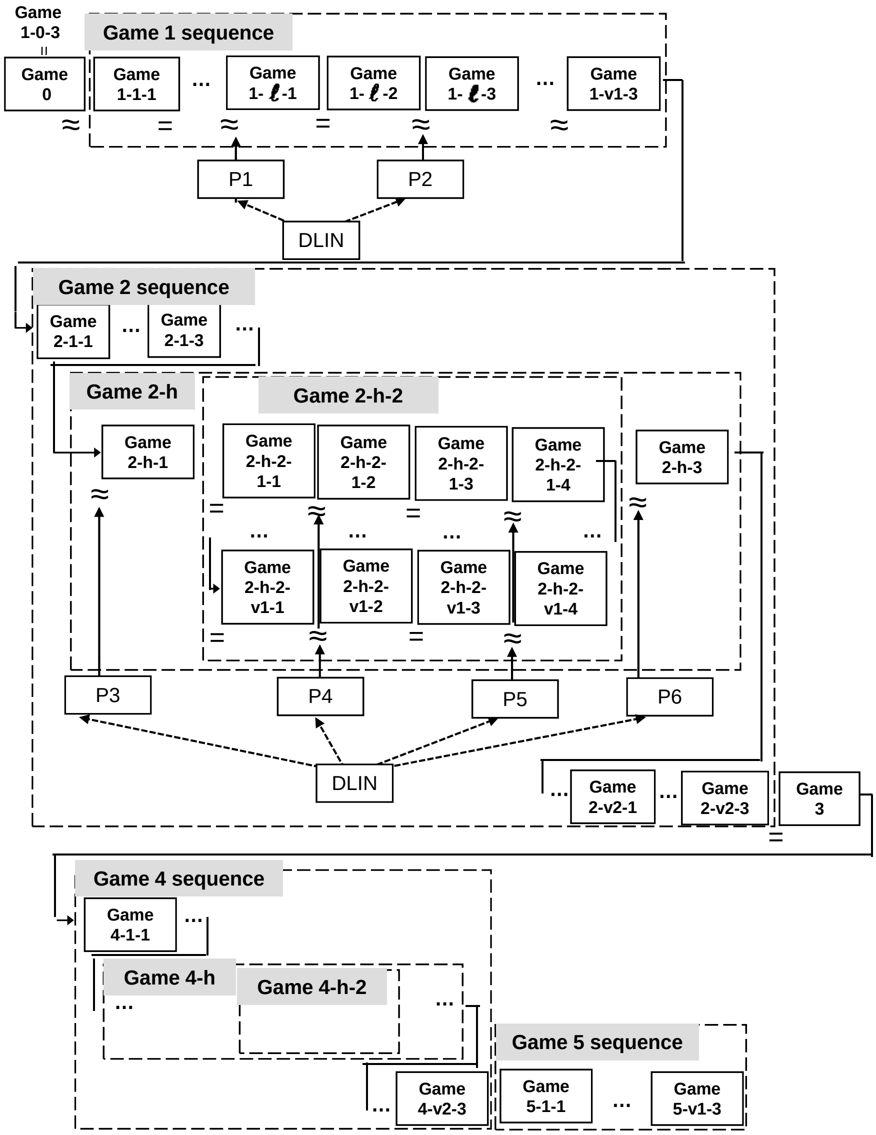


Figure 4: Structure of Reductions in the proof of Lemma 1

$j = 1, \dots, \nu_2$) w.r.t. these bases vectors are given as:

Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-2-ν_1-4

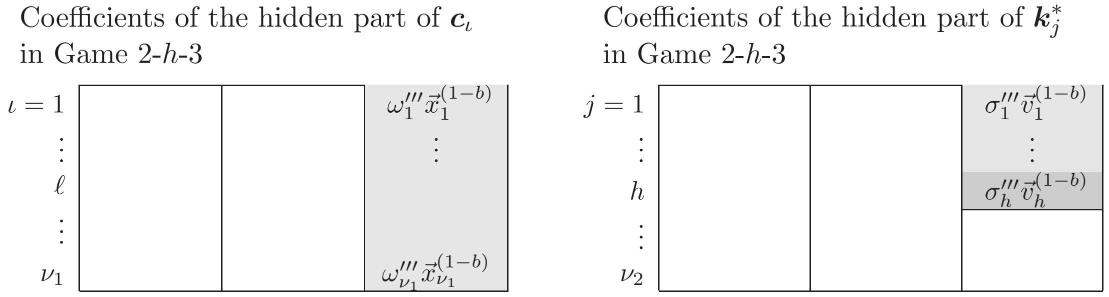
$\iota = 1$		$\omega''_1 \vec{x}_1^{(1-b)}$	$\omega'''_1 \vec{x}_1^{(1-b)}$
$\vdots$		$\vdots$	$\vdots$
ℓ			
$\vdots$			
ν_1		$\omega''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$	$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 2-h-2-ν_1-4

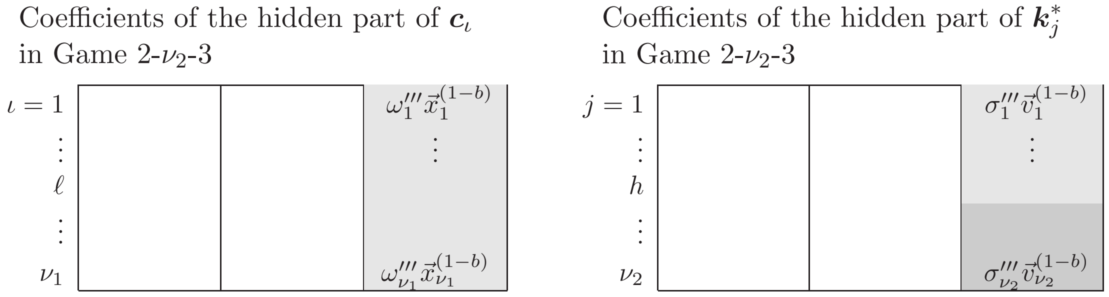
$j = 1$			$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\vdots$			$\vdots$
h	$\sigma'_h \vec{v}_h^{(1-b)}$	$\sigma''_h \vec{v}_h^{(1-b)}$	
$\vdots$			
ν_2			

In the second block of the hidden part, an *opposite* vector $\sigma''_h \vec{v}_h^{(1-b)}$ for the ℓ-th query (and zero for the rest of the $j (\neq h)$-th queries) in tokens and *opposite* vectors, $\omega''_1 \vec{x}_1^{(1-b)}, \dots, \omega''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$, in ciphertexts are placed. Different from Lemma 2 case, the result $(\sigma''_h \vec{v}_h^{(1-b)}; \omega''_1 \vec{x}_1^{(1-b)}, \dots, \omega''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)})$

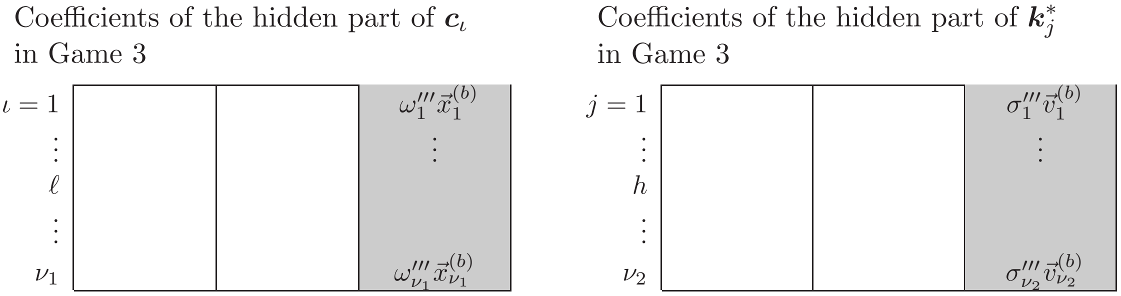
cannot be added to the real encoding part coefficients $(\sigma_h \vec{v}_h^{(b)}; \omega_1 \vec{x}_1^{(b)}, \ldots, \omega_{\nu_1} \vec{x}_{\nu_1}^{(b)})$ by a conceptual change, since the unbiased form is not useful as mentioned above. Instead, we store the result in *the third block of the hidden part* in the next Game 2-h-3 as:


Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-3
$\iota = 1$
$\vdots$
ℓ
$\vdots$
ν_1
$\omega_1''' \vec{x}_1^{(1-b)}$
$\vdots$
$\omega_{\nu_1}''' \vec{x}_{\nu_1}^{(1-b)}$
Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 2-h-3
$j = 1$
$\vdots$
h
$\vdots$
ν_2
$\sigma_1''' \vec{v}_1^{(1-b)}$
$\vdots$
$\sigma_h''' \vec{v}_h^{(1-b)}$

where all the coefficients in the first and second blocks become zero vectors preparing for the next Game 2-$(h+1)$ sequence. At the end of Game 2 sequence, we have


Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-ν_2-3
$\iota = 1$
$\vdots$
ℓ
$\vdots$
ν_1
$\omega_1''' \vec{x}_1^{(1-b)}$
$\vdots$
$\omega_{\nu_1}''' \vec{x}_{\nu_1}^{(1-b)}$
Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 2-ν_2-3
$j = 1$
$\vdots$
h
$\vdots$
ν_2
$\sigma_1''' \vec{v}_1^{(1-b)}$
$\vdots$
$\sigma_{\nu_2}''' \vec{v}_{\nu_2}^{(1-b)}$

where the third block is filled with *opposite* vectors with bit $1-b$. We note that the view of the adversary (malicious user) do not include $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ as well as $(\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*)$. Therefore, we can conceptually change between subspaces $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle$ and $\mathsf{span}\langle \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{4n} \rangle$ (resp. $\mathsf{span}\langle \boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^* \rangle$ and $\mathsf{span}\langle \boldsymbol{b}_{3n+1}^*, \ldots, \boldsymbol{b}_{4n}^* \rangle$), and tokens and ciphertexts are given as Eqs. (16) and (17) in Game 3. In particular, coefficients in the hidden part are given as:


Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 3
$\iota = 1$
$\vdots$
ℓ
$\vdots$
ν_1
$\omega_1''' \vec{x}_1^{(b)}$
$\vdots$
$\omega_{\nu_1}''' \vec{x}_{\nu_1}^{(b)}$
Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 3
$j = 1$
$\vdots$
h
$\vdots$
ν_2
$\sigma_1''' \vec{v}_1^{(b)}$
$\vdots$
$\sigma_{\nu_2}''' \vec{v}_{\nu_2}^{(b)}$

Through the reverse process, Game 4 and Game 5 sequences, we reach the final Game 5-ν_1-3, where all queried tokens and ciphertext are normal one for opposite bit $1-b$. Thus, Lemma 1 is proven.

Therefore, essentially, the reduction in Figure 4 is a combination of that in Figure 3 and a reverse of that in Figure 3, with a switch of subspace blocks in Game 3 for bit change from b to $1-b$. However, since we cannot make use of unbiased coefficients in this case, we need one more n-dimensional block in the hidden subspace. The total hidden subspace is $3n$-dimensional. We call it *multi-system proof technique*, which is an extension of the technique in [20] as we see in the above.

Finally, we consider the proof of Lemma 3, where malicious PKG has a secret key $\mathsf{sk} := \widehat{\mathbb{B}}^*$. The adversary cannot derive (useful) information from original ciphertexts $\mathsf{ct}_{\vec{x}}$ on $\mathbb{D}$ and tokens $\mathsf{tk}_{\vec{v}}$ on $\mathbb{B}^*$, since he has no $\mathbb{D}^*$ and $\mathbb{B}$ for checking them. The independent property of $\mathbb{B}$ and $\mathbb{D}$ makes the security proof rather simple.

B Proofs of Lemmas 1–3

B.1 Proof of Lemma 1

Lemma 1. *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{DisU}}_{\mathcal{A}}(\lambda)$ is negligible under the DLIN assumption.*

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

$$\mathsf{Adv}^{\mathsf{DisU}}_{\mathcal{A}}(\lambda) \leq \sum_{\ell=1}^{\nu_1} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}\ell\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}\ell\text{-}2}}(\lambda) \Big) +$$

$$\sum_{h=1}^{\nu_2} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}1}}(\lambda) + \sum_{\ell=1}^{\nu_1} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}2\text{-}\ell}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}3\text{-}\ell}}(\lambda) \Big) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}4}}(\lambda) \right) + \epsilon,$$

where $\mathcal{E}_{1\text{-}\ell\text{-}1}(\cdot) := \mathcal{E}_{1\text{-}1}(\ell, \cdot), \mathcal{E}_{1\text{-}\ell\text{-}2}(\cdot) := \mathcal{E}_{1\text{-}2}(\ell, \cdot), \mathcal{E}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{2\text{-}1}(h, \cdot), \mathcal{E}_{2\text{-}h\text{-}2\text{-}\ell}(\cdot) := \mathcal{E}_{2\text{-}2}(h, \ell, \cdot)$, $\mathcal{E}_{2\text{-}h\text{-}3\text{-}\ell}(\cdot) := \mathcal{E}_{2\text{-}3}(h, \ell, \cdot), \mathcal{E}_{2\text{-}h\text{-}4}(\cdot) := \mathcal{E}_{2\text{-}4}(h, \cdot)$, ν_1 (resp. ν_2) is the maximum number of $\mathcal{A}$'s challenge ciphertext (resp. key) queries and $\epsilon := (23\nu_1\nu_2 + (n+17)\nu_1 + 18\nu_2)/q$.

We give (intermediate) games for the proof of Lemma 1 below.

B.1.1 Games for the proof of Lemma 1

Let ν_1 be the maximum number of $\mathcal{A}$'s challenge ciphertext queries and ν_2 the maximum number of $\mathcal{A}$'s challenge token queries. To prove Lemma 1, we consider the following $8\nu_1\nu_2 + 6\nu_1 + 4\nu_2 + 2$ games. In Game 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0 : For $j = 1, \ldots, \nu_2$, the reply to the j-th token query for $(\vec{v}^{(0)}_j, \vec{v}^{(1)}_j)$ is:

$$\boldsymbol{k}^*_j := (\boxed{\sigma_j \vec{v}^{(b)}_j}, \boxed{0^n}, \boxed{0^n}, \boxed{0^n}, \vec{\eta}_j, 0^n)_{\mathbb{B}^*}, \tag{2}$$

where $b \xleftarrow{\mathsf{U}} \{0,1\}$, $\sigma_j \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\eta}_j \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$. For $\iota = 1, \ldots, \nu_1$, the reply to the ι-th ciphertext query for vectors $(\vec{x}^{(0)}_\iota, \vec{x}^{(1)}_\iota)$ is:

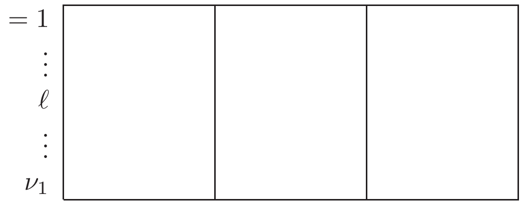
$$\boldsymbol{f}_\iota := (\boxed{\tau_\iota \vec{x}^{(b)}_\iota}, 0^n, \boxed{0^n}, \boxed{0^n}, 0^n, \vec{\xi}_\iota)_{\mathbb{D}}, \tag{3}$$

$$\boldsymbol{c}_\iota := (\boxed{\omega_\iota \vec{x}^{(b)}_\iota}, \boxed{0^n}, \boxed{0^n}, \boxed{0^n}, 0^n, \vec{\varphi}_\iota)_{\mathbb{B}}, \tag{4}$$

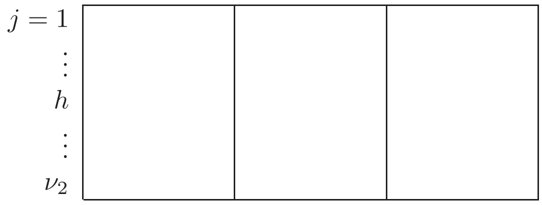
where $\tau_\iota, \omega_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\xi}_\iota, \vec{\varphi}_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$.

Below, we describe coefficients of the hidden part, i.e., $\mathsf{span}\langle \boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{4n} \rangle$ (resp. $\mathsf{span}\langle \boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{4n} \rangle$) of the ι-th queried $\boldsymbol{c}_\iota$ for $\iota = 1, \ldots, \nu_1$ (resp. the j-th queried $\boldsymbol{k}^*_j$ for $j = 1, \ldots, \nu_2$) w.r.t. these bases vectors. Non-zero coefficients are colored by light gray, and those which were changed from the previous game are colored by dark gray.

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



Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game 0



Game 1-ℓ-1 ($\ell = 1, \ldots, \nu_1$) : Game 1-0-3 is Game 0. Game 1-ℓ-1 is the same as Game 1-($\ell - 1$)-3 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\begin{aligned} \boldsymbol{f}_\ell &:= (\ \tau_\ell \vec{x}_\ell^{(b)},\ 0^n,\ \boxed{\tau''_\ell \vec{x}_\ell^{(b)}},\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}}, \\ \boldsymbol{c}_\ell &:= (\ \omega \vec{x}_\ell^{(b)},\ 0^n,\ \boxed{\omega''_\ell \vec{x}_\ell^{(b)}},\ 0^n,\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}}, \end{aligned} \tag{5}$$

where $\tau''_\ell, \omega''_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 1-($\ell - 1$)-3.

Game 1-ℓ-2 ($\ell = 1, \ldots, \nu_1$) : Game 1-ℓ-2 is the same as Game 1-ℓ-1 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\boldsymbol{f}_\ell := (\ \vec{r}_{f,\ell}\ )_{\mathbb{D}} \text{ with } \vec{r}_{f,\ell} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{6n}, \quad \text{i.e., } \boldsymbol{f}_\ell \xleftarrow{\mathsf{U}} \mathbb{V}, \tag{6}$$

$$\boldsymbol{c}_\ell := (\ \omega \vec{x}_\ell^{(b)},\ 0^n,\ \boxed{\omega''_\ell \vec{x}_\ell^{(1-b)}},\ 0^n,\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}}, \tag{7}$$

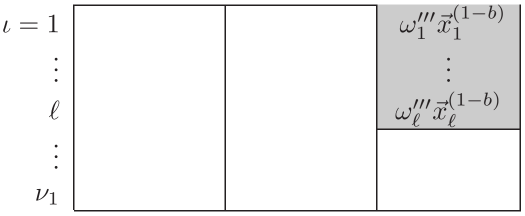
where all the variables are generated as in Game 1-ℓ-1.

Game 1-ℓ-3 ($\ell = 1, \ldots, \nu_1$) : Game 1-ℓ-3 is the same as Game 1-ℓ-2 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\boldsymbol{c}_\ell := (\ \omega_\ell \vec{x}_\ell^{(b)},\ 0^n,\ \boxed{0^n},\ \boxed{\omega'''_\ell \vec{x}_\ell^{(1-b)}},\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}}, \tag{8}$$

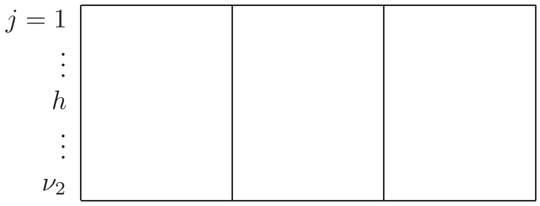
where $\tau'''_\ell, \omega'''_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 1-ℓ-2.

Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 1-ℓ-3

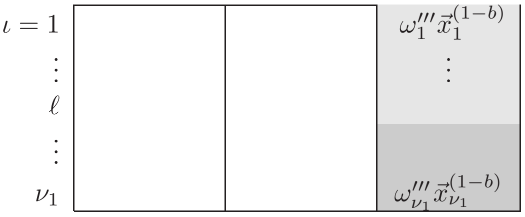


$\iota = 1$
$\vdots$
ℓ
$\vdots$
ν_1
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\vdots$
$\omega'''_\ell \vec{x}_\ell^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 1-ℓ-3

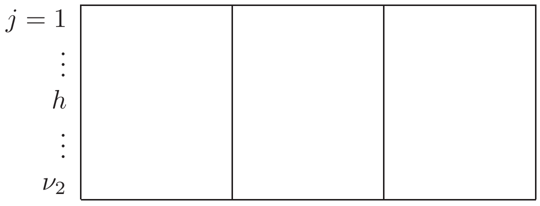


Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 1-ν_1-3 (= Game 2-0-3)



$\iota = 1$
$\vdots$
ℓ
$\vdots$
ν_1
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\vdots$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 1-ν_1-3 (= Game 2-0-3)

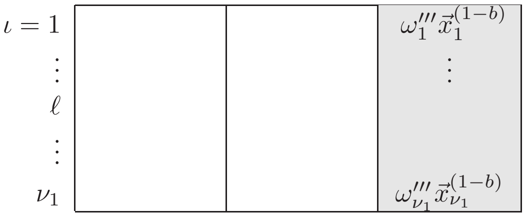


Game 2-h-1 ($h = 1, \ldots, \nu_2$) : Game 2-0-3 is Game 1-ν_1-3. Game 2-h-1 is the same as Game 2-($h - 1$)-3 except that the reply to the h-th token query for $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ is:

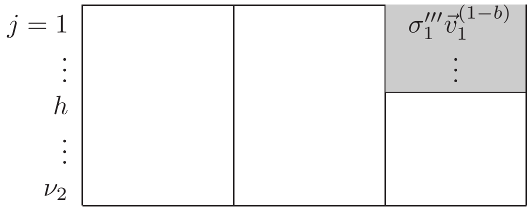
$$\boldsymbol{k}_h^* := (\ \sigma_h \vec{v}_h^{(b)},\ \boxed{\sigma'_h \vec{v}_h^{(b)}},\ \boxed{\sigma''_h \vec{v}_h^{(b)}},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*}, \tag{9}$$

where $\sigma'_h, \sigma''_h \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-$(h-1)$-3.

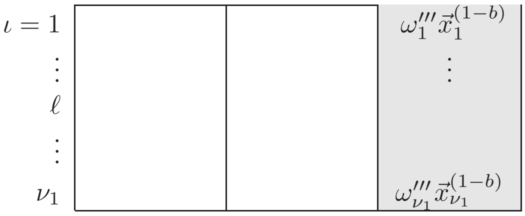
Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-$(h-1)$-3


$\iota = 1$
ℓ
ν_1
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

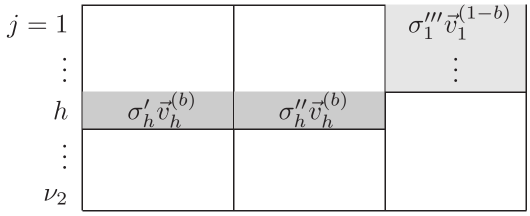
Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game 2-$(h-1)$-3



Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-1 (= Game 2-h-2-0-4)


$\iota = 1$
ℓ
ν_1
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game 2-h-1 (= Game 2-h-2-0-4)

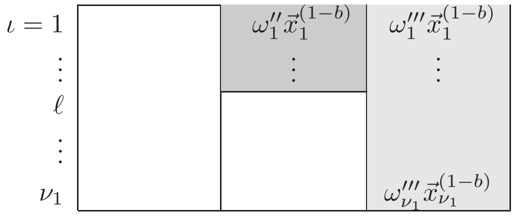

$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'_h \vec{v}_h^{(b)}$
$\sigma''_h \vec{v}_h^{(b)}$

Game 2-h-2-ℓ-1 ($h = 1, \ldots, \nu_2; \ell = 1, \ldots, \nu_1$) : Game 2-$h$-2-0-4 is Game 2-$h$-1. Game 2-$h$-2-$\ell$-1 is the same as Game 2-h-2-$(\ell-1)$-4 except that the reply to the h-th token query for $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ is:

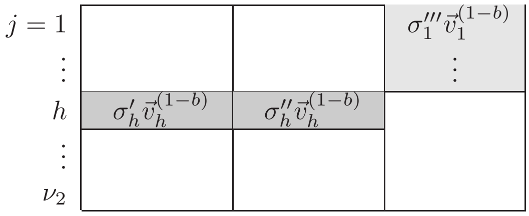
$$\boldsymbol{k}^*_h := (\ \sigma_h \vec{v}_h^{(b)},\ \boxed{\sigma'_h \vec{v}_h^{(b)}},\ \boxed{\sigma''_h \vec{v}_h^{(1-b)}},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*}, \tag{10}$$

where all the variables are generated as in Game 2-h-2-$(\ell-1)$-4. Here, a part framed by a box (resp. dashed box) indicates coefficients which were changed from the previous game when $\ell \geq 2$ (resp. $\ell = 1$).

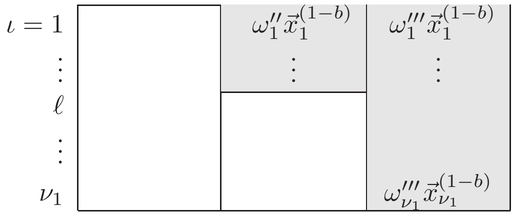
Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-2-$(\ell-1)$-4 for $\ell \geq 2$


$\iota = 1$
ℓ
ν_1
$\omega''_1 \vec{x}_1^{(1-b)}$
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

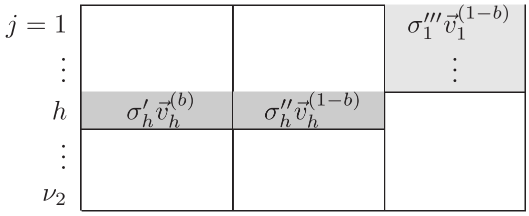
Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game 2-h-2-$(\ell-1)$-4 for $\ell \geq 2$


$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'_h \vec{v}_h^{(1-b)}$
$\sigma''_h \vec{v}_h^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-2-ℓ-1


$\iota = 1$
ℓ
ν_1
$\omega''_1 \vec{x}_1^{(1-b)}$
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game 2-h-2-ℓ-1

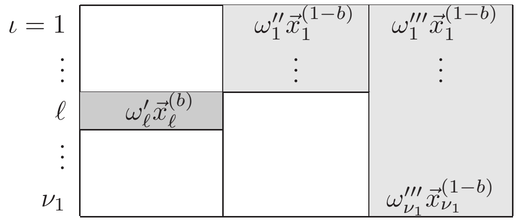

$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'_h \vec{v}_h^{(b)}$
$\sigma''_h \vec{v}_h^{(1-b)}$

Game 2-h-2-ℓ-2 ($h = 1, \ldots, \nu_2; \ell = 1, \ldots, \nu_1$) : Game 2-$h$-2-$\ell$-2 is the same as Game 2-h-2-ℓ-1 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

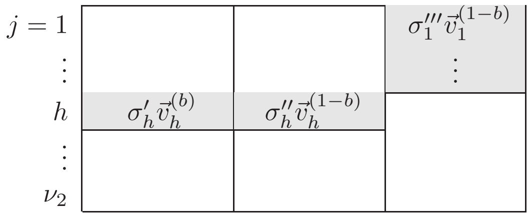
$$\boldsymbol{c}_\ell := (\ \omega_\ell \vec{x}_\ell^{(b)},\ \boxed{\omega'_\ell \vec{x}_\ell^{(b)}},\ 0^n,\ \omega'''_\ell \vec{x}_\ell^{(1-b)},\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}}, \tag{11}$$

where $\omega'_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-h-2-ℓ-1.

Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-2-ℓ-2


$\iota = 1$
ℓ
ν_1
$\omega''_1 \vec{x}_1^{(1-b)}$
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega'_\ell \vec{x}_\ell^{(b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 2-h-2-ℓ-2


$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'_h \vec{v}_h^{(b)}$
$\sigma''_h \vec{v}_h^{(1-b)}$

Game 2-h-2-ℓ-3 ($h = 1, \ldots, \nu_2; \ell = 1, \ldots, \nu_1$) : Game 2-$h$-2-$\ell$-3 is the same as Game 2-h-2-ℓ-2 except the reply to the h-th token query for $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ is:

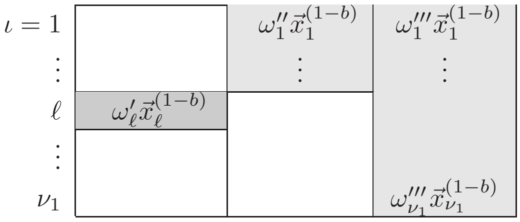
$$\boldsymbol{k}_h^* := (\ \sigma_h \vec{v}_h^{(b)},\ \boxed{\sigma'_h \vec{v}_h^{(1-b)}},\ \sigma''_h \vec{v}_h^{(1-b)},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*}, \tag{12}$$

and the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

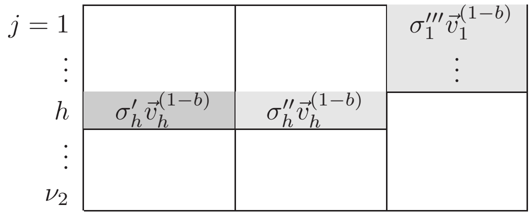
$$\boldsymbol{c}_\ell := (\ \omega_\ell \vec{x}_\ell^{(b)},\ \boxed{\omega'_\ell \vec{x}_\ell^{(1-b)}},\ 0^n,\ \omega'''_\ell \vec{x}_\ell^{(1-b)},\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}}, \tag{13}$$

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

Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-2-ℓ-3


$\iota = 1$
ℓ
ν_1
$\omega''_1 \vec{x}_1^{(1-b)}$
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega'_\ell \vec{x}_\ell^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 2-h-2-ℓ-3

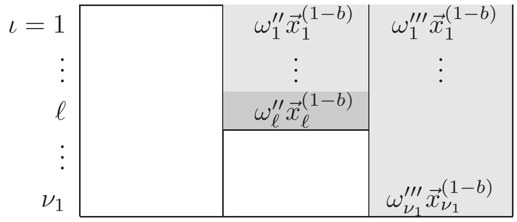

$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'_h \vec{v}_h^{(1-b)}$
$\sigma''_h \vec{v}_h^{(1-b)}$

Game 2-h-2-ℓ-4 ($h = 1, \ldots, \nu_2; \ell = 1, \ldots, \nu_1$) : Game 2-$h$-2-$\ell$-4 is the same as Game 2-h-2-ℓ-3 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

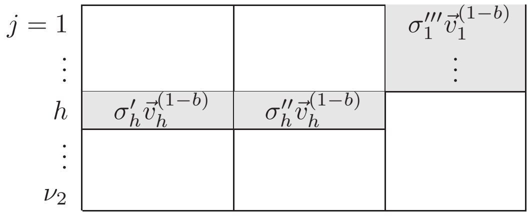
$$\boldsymbol{c}_\ell := (\ \omega_\ell \vec{x}_\ell^{(b)},\ \boxed{0^n},\ \boxed{\omega''_\ell \vec{x}_\ell^{(1-b)}},\ \omega'''_\ell \vec{x}_\ell^{(1-b)},\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}}, \tag{14}$$

where $\omega''_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-h-2-ℓ-3.

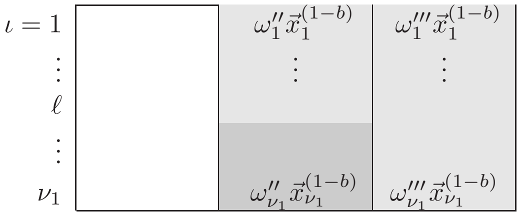
Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-2-ℓ-4


$\iota = 1$
ℓ
ν_1
$\omega''_1 \vec{x}_1^{(1-b)}$
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega''_\ell \vec{x}_\ell^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 2-h-2-ℓ-4

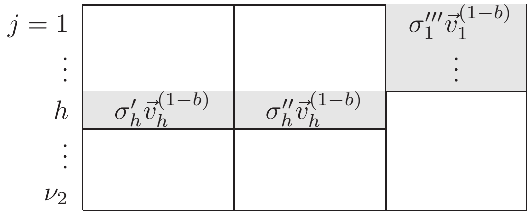

$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'_h \vec{v}_h^{(1-b)}$
$\sigma''_h \vec{v}_h^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-2-ν_1-4



$\iota = 1$
ℓ
ν_1
$\omega''_1 \vec{x}_1^{(1-b)}$
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game 2-h-2-ν_1-4



$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'_h \vec{v}_h^{(1-b)}$
$\sigma''_h \vec{v}_h^{(1-b)}$

Game 2-h-3 ($h = 1, \ldots, \nu_2$) : Game 2-h-3 is the same as Game 2-h-2-ν_1-4 except that the reply to the h-th token query for $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ is:

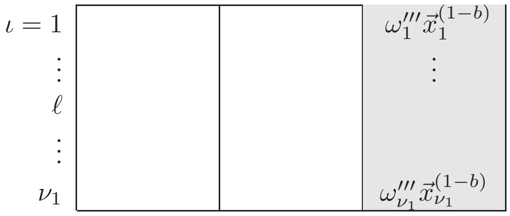
$$\boldsymbol{k}^*_h := (\ \sigma_h \vec{v}_h^{(b)},\ \boxed{0^n}, \boxed{0^n},\ \boxed{\sigma'''_h \vec{v}_h^{(1-b)}},\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*}, \tag{15}$$

where $\sigma'''_h \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and for all $\iota = 1, \ldots, \nu_1$, the reply to the ι-th ciphertext query for vectors $(\vec{x}_\iota^{(0)}, \vec{x}_\iota^{(1)})$ is:

$$\boldsymbol{c}_\iota := (\ \omega_\iota \vec{x}_\iota^{(b)},\ 0^n,\ \boxed{0^n},\ \omega'''_\iota \vec{x}_\iota^{(1-b)},\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{B}} \quad \text{for } \iota = 1, \ldots, \nu_1,$$

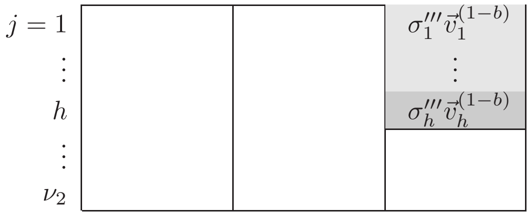
where $\omega_\iota, \omega'''_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\varphi}_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 2-h-2-ν_1-4.

Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-h-3



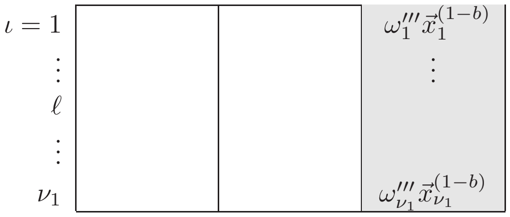
$\iota = 1$
ℓ
ν_1
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game 2-h-3



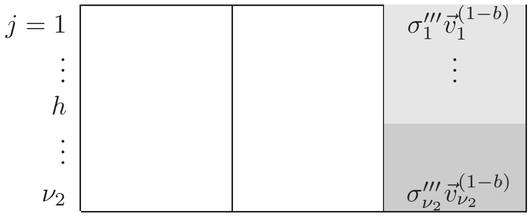
$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'''_h \vec{v}_h^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{c}_\iota$ in Game 2-ν_2-3



$\iota = 1$
ℓ
ν_1
$\omega'''_1 \vec{x}_1^{(1-b)}$
$\omega'''_{\nu_1} \vec{x}_{\nu_1}^{(1-b)}$

Coefficients of the hidden part of $\boldsymbol{k}^*_j$ in Game 2-ν_2-3



$j = 1$
h
ν_2
$\sigma'''_1 \vec{v}_1^{(1-b)}$
$\sigma'''_{\nu_2} \vec{v}_{\nu_2}^{(1-b)}$

Game 3 : Game 3 is the same as Game 2-ν_2-3 except that, for all $j = 1, \ldots, \nu_2$, the reply to the j-th token query for $(\vec{v}_j^{(0)}, \vec{v}_j^{(1)})$ is:

$$\boldsymbol{k}^*_j := (\ \boxed{\sigma_j \vec{v}_j^{(1-b)}},\ 0^n,\ 0^n,\ \boxed{\sigma'''_j \vec{v}_j^{(b)}},\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*} \quad \text{for } j = 1, \ldots, \nu_2, \tag{16}$$

where $\sigma_j, \sigma'''_j \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\eta}_j \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, and, for all $\iota = 1, \ldots, \nu_1$, the reply to the ι-th ciphertext query for vectors $(\vec{x}_\iota^{(0)}, \vec{x}_\iota^{(1)})$ is:

$$\boldsymbol{c}_\iota := (\ \boxed{\omega_\iota \vec{x}_\iota^{(1-b)}},\ 0^n,\ 0^n,\ \boxed{\omega'''_\iota \vec{x}_\iota^{(b)}},\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{B}} \quad \text{for } \iota = 1, \ldots, \nu_1, \tag{17}$$

where all the variables are generated as in Game 2-ν_2-3.

From here on, the reverse game transformations proceed, i.e., **Game 4-*h*-1; Game 4-*h*-2-*ℓ*-*i*** for i=1,. . . ,4; **Game 4-*h*-3;** and **Game 5-*ℓ*-*i*** for i=1,2,3.

The final game, **Game 5-$\boldsymbol{\nu_1}$-3** is given as below.

Game 5-$\boldsymbol{\nu_1}$-3 : Game 5-ν_1-3 is the same as Game 3 except that, for all $j = 1, \ldots, \nu_2$, the reply to the j-th token query for $(\vec{v}_j^{(0)}, \vec{v}_j^{(1)})$ is:

$$\boldsymbol{k}_j^* := (\ \sigma_j \vec{v}_j^{(1-b)},\ 0^n,\ 0^n,\ \boxed{0^n},\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*} \quad \text{for } j = 1, \ldots, \nu_2,$$

where all the variables are generated as in Game 3, and, for all $\iota = 1, \ldots, \nu_1$, the reply to the ι-th ciphertext query for vectors $(\vec{x}_\iota^{(0)}, \vec{x}_\iota^{(1)})$ is:

$$\begin{aligned} \boldsymbol{f}_\iota &:= (\ \tau_\iota \vec{x}_\iota^{(1-b)},\ 0^n,\ 0^n,\ \boxed{0^n},\ 0^n,\ \vec{\xi}_\iota\ )_{\mathbb{D}} \quad \text{for } \iota = 1, \ldots, \nu_1, \\ \boldsymbol{c}_\iota &:= (\ \omega_\iota \vec{x}_\iota^{(1-b)},\ 0^n,\ 0^n,\ \boxed{0^n},\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{B}} \quad \text{for } \iota = 1, \ldots, \nu_1, \end{aligned}$$

where all the variables are generated as in Game 3. Note that all $\boldsymbol{k}_j^*$ and $(\boldsymbol{c}_\iota, \boldsymbol{f}_\iota)$ are normal tokens and ciphertexts for the opposite bit $1 - b$ to the challenge bit b. The game hopping structure is described by Figure 4.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}i)}(\lambda)$ for $i = 1,2,3$; $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}i)}(\lambda)$ for $i = 1,3$; $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}\kappa)}(\lambda)$ for $\kappa = 1, \ldots, 4$ and $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0, 1\text{-}\ell\text{-}i (i = 1,2,3), 2\text{-}h\text{-}i (i = 1,3), 2\text{-}h\text{-}2\text{-}\ell\text{-}\kappa\ (\kappa = 1, \ldots, 4)$ and 3, respectively. We will show ten lemmas (Lemmas 12–21) that evaluate the gaps between pairs of neighboring games. From these lemmas and Lemmas 5–10, we obtain $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) \leq \mathsf{Adv}_{\mathcal{A}}^{(5\text{-}\nu_1\text{-}3)}(\lambda) + \delta$, where $\delta = 2\Big(\sum_{\ell=1}^{\nu_1}\Big(\Big|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}(\ell-1)\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}1)}(\lambda)\Big| + \sum_{i=2}^{3}\Big|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}(i-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}i)}(\lambda)\Big|\Big) + \sum_{h=1}^{\nu_2}\Big(\Big|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)\Big| + \sum_{\ell=1}^{\nu_1}\Big(\Big|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}(\ell-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}1)}(\lambda)\Big| + \sum_{i=2}^{4}\Big|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}(i-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}i)}(\lambda)\Big|\Big) + \Big|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda)\Big|\Big) \leq 2\,(\sum_{\ell=1}^{\nu_1}(\mathsf{Adv}_{\mathcal{B}_{1\text{-}\ell\text{-}1}}^{\mathsf{P1}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{1\text{-}\ell\text{-}2}}^{\mathsf{P2}}(\lambda)) + \sum_{h=1}^{\nu_2}(\mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}1}}^{\mathsf{P3}}(\lambda) + \sum_{\ell=1}^{\nu_1}(\mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}2\text{-}\ell}}^{\mathsf{P4}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}3\text{-}\ell}}^{\mathsf{P5}}(\lambda)) + \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}4}}^{\mathsf{P6}}(\lambda)) + 10\nu_1\nu_2 + (n+6)\nu_1) \leq 2\,(\sum_{\ell=1}^{\nu_1}(\mathsf{Adv}_{\mathcal{E}_{1\text{-}\ell\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{1\text{-}\ell\text{-}2}}^{\mathsf{DLIN}}(\lambda)) + \sum_{h=1}^{\nu_2}(\mathsf{Adv}_{\mathcal{E}_{2\text{-}h\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \sum_{\ell=1}^{\nu_1}(\mathsf{Adv}_{\mathcal{E}_{2\text{-}h\text{-}2\text{-}\ell}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{2\text{-}h\text{-}3\text{-}\ell}}^{\mathsf{DLIN}}(\lambda)) + \mathsf{Adv}_{\mathcal{E}_{2\text{-}h\text{-}4}}^{\mathsf{DLIN}}(\lambda)) + 23\nu_1\nu_2 + (n+17)\nu_1 + 18\nu_2\big)$. From Lemma 22, $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) \leq \delta/2$. This completes the proof of Lemma 1. □

B.1.2 Lemmas 5–22

Definition 8 (Problem 1) *Problem 1 is to guess* β, *given* $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P1}}(1^\lambda, n)$, *where*

$$\begin{aligned} &\mathcal{G}_\beta^{\mathsf{P1}}(1^\lambda, n) : \ (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{IPE}}(1^\lambda, 6n), \\ &\quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_{2n}^*, \boldsymbol{b}_{3n+1}^*, \ldots, \boldsymbol{b}_{6n}^*), \quad \omega, \omega'' \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\ &\quad \text{for } i = 1, \ldots, n; \quad \vec{\gamma}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n, \\ &\quad \boldsymbol{e}_{0,i} := (\ \overbrace{\omega \vec{e}_i,}^{n}\ \overbrace{0^{3n},}^{3n}\ \overbrace{0^n,}^{n}\ \overbrace{\vec{\gamma}_i}^{n}\ )_{\mathbb{B}}, \\ &\quad \boldsymbol{e}_{1,i} := (\ \omega \vec{e}_i,\ 0^n,\ \omega'' \vec{e}_i,\ 0^n,\ 0^n,\ \vec{\gamma}_i\ )_{\mathbb{B}}, \\ &\quad \text{return } (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}), \end{aligned}$$

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

Lemma 5 *For any adversary* $\mathcal{B}$, *there is a probabilistic machine* $\mathcal{E}$, *whose running time is essentially the same as that of* $\mathcal{B}$, *such that for any security parameter* λ, $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 6/q$.

Proof. Problem 1 is essentially the same as Basic Problem 1 in [18], where the intractability of the problem is reduced to that of DLIN. Therefore, Lemma 5 is proven in a similar manner as the reduction lemmas in [18]. □

Definition 9 (Problem 2) *Problem 2 is to guess* β, *given* $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2}}_{\beta}(1^\lambda,n)$, *where*

$$
\begin{array}{l}
\mathcal{G}^{\mathsf{P2}}_{\beta}(1^\lambda,n):\ (\mathsf{param}_{\mathbb{V}},\mathbb{B},\mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda,6n),\\
\quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1,\ldots,\boldsymbol{b}^*_{2n},\boldsymbol{b}^*_{4n+1},\ldots,\boldsymbol{b}^*_{6n}), \quad \omega'',\omega''' \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
\quad \text{for } i=1,\ldots,n; \quad \vec{\gamma}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\\
\quad \begin{array}{rcccccl}
 & & \overbrace{\hphantom{\ 0^n,\ }}^{n} & \overbrace{\hphantom{0^n,\ \omega''\vec{e}_i,\ 0^n,\quad}}^{3n} & \overbrace{\hphantom{\ 0^n,\ }}^{n} & \overbrace{\hphantom{\ \vec{\gamma}_i\ }}^{n} & \\
\boldsymbol{e}_{0,i} := & (& 0^n, & 0^n,\ \omega''\vec{e}_i,\ 0^n, & 0^n, & \vec{\gamma}_i &)_{\mathbb{B}},\\
\boldsymbol{e}_{1,i} := & (& 0^n, & 0^{2n},\quad \omega'''\vec{e}_i, & 0^n, & \vec{\gamma}_i &)_{\mathbb{B}},
\end{array}\\
\quad \text{return } (\mathsf{param}_{\mathbb{V}},\mathbb{B},\widehat{\mathbb{B}}^*,\{\boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}),
\end{array}
$$

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

Lemma 6 *For any adversary* $\mathcal{B}$, *there is a probabilistic machine* $\mathcal{E}$, *whose running time is essentially the same as that of* $\mathcal{B}$, *such that for any security parameter* λ, $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.

Proof. Problem 2 is reduced from Problem 1 in [18], where the intractability of the problem is reduced to that of DLIN. Therefore, Lemma 6 is proven in a similar manner as the reduction lemmas in [18]. □

Definition 10 (Problem 3) *Problem 3 is to guess* β, *given* $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P3}}_{\beta}(1^\lambda,n)$, *where*

$$
\begin{array}{l}
\mathcal{G}^{\mathsf{P3}}_{\beta}(1^\lambda,n):\ (\mathsf{param}_{\mathbb{V}},\mathbb{B},\mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda,6n),\\
\quad \widehat{\mathbb{B}} := (\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{n},\boldsymbol{b}_{3n+1},\ldots,\boldsymbol{b}_{6n}), \quad \sigma,\sigma',\sigma'' \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
\quad \text{for } i=1,\ldots,n; \quad \vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\\
\quad \begin{array}{rcccccl}
 & & \overbrace{\hphantom{\ \sigma\vec{e}_i,\ }}^{n} & \overbrace{\hphantom{\sigma'\vec{e}_i,\ \sigma''\vec{e}_i,\ 0^n,\quad}}^{3n} & \overbrace{\hphantom{\ \vec{\eta}_i,\ }}^{n} & \overbrace{\hphantom{\ 0^n\ }}^{n} & \\
\boldsymbol{h}^*_{0,i} := & (& \sigma\vec{e}_i, & 0^{3n}, & \vec{\eta}_i, & 0^n &)_{\mathbb{B}^*},\\
\boldsymbol{h}^*_{1,i} := & (& \sigma\vec{e}_i, & \sigma'\vec{e}_i,\ \sigma''\vec{e}_i,\ 0^n, & \vec{\eta}_i, & 0^n &)_{\mathbb{B}^*},
\end{array}\\
\quad \text{return } (\mathsf{param}_{\mathbb{V}},\widehat{\mathbb{B}},\mathbb{B}^*,\{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\ldots,n}),
\end{array}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{B}$, *the advantage of* $\mathcal{B}$ *for Problem 3,* $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda)$, *is similarly defined as in Definition 8.*

Lemma 7 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

Proof. Problem 3 is essentially the same as Basic Problem 1 in [18], where the intractability of the problem is reduced to that of DLIN. Therefore, Lemma 7 is proven in a similar manner as the reduction lemmas in [18]. □

Definition 11 (Problem 4) *Problem 4 is to guess β, given $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_i, \boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P4}}_{\beta}(1^\lambda, n)$, where*

$$\mathcal{G}^{\mathsf{P4}}_{\beta}(1^\lambda, n): \quad (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda, 6n),$$

$$\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{2n+1}, \ldots, \boldsymbol{b}^*_{6n}), \quad \sigma, \sigma', \omega, \omega' \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\text{for } i = 1, \ldots, n; \quad \vec{\eta}_i, \vec{\gamma}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,$$

$$\begin{array}{rccccccl}
 & & \overbrace{\hphantom{\omega\vec{e}_i,}}^{n} & \overbrace{\hphantom{\sigma'\vec{e}_i,\ 0^{2n},}}^{3n} & \overbrace{\hphantom{\vec{\eta}_i,}}^{n} & \overbrace{\hphantom{0^n}}^{n} & \\
\boldsymbol{h}^*_i := & (& \sigma\vec{e}_i, & \sigma'\vec{e}_i,\ 0^{2n}, & \vec{\eta}_i, & 0^n &)_{\mathbb{B}^*} \\
\boldsymbol{e}_{0,i} := & (& \omega\vec{e}_i, & 0^{3n}, & 0^n, & \vec{\gamma}_i &)_{\mathbb{B}}, \\
\boldsymbol{e}_{1,i} := & (& \omega\vec{e}_i, & \omega'\vec{e}_i,\ 0^{2n}, & 0^n, & \vec{\gamma}_i &)_{\mathbb{B}},
\end{array}$$

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

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

Lemma 8 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

Proof. Problem 4 is essentially the same as Basic Problem 2 in [18], where the intractability of the problem is reduced to that of DLIN. Therefore, Lemma 8 is proven in a similar manner as the reduction lemmas in [18]. □

Definition 12 (Problem 5) *Problem 5 is to guess β, given $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_i, \boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P5}}_{\beta}(1^\lambda, n)$, where*

$$\mathcal{G}^{\mathsf{P5}}_{\beta}(1^\lambda, n): \quad (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda, 6n),$$

$$\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{6n}), \quad \sigma', \sigma'', \omega', \omega'' \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\text{for } i = 1, \ldots, n; \quad \vec{\eta}_i, \vec{\gamma}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,$$

$$\begin{array}{rccccccl}
 & & \overbrace{\hphantom{0^n,}}^{n} & \overbrace{\hphantom{\sigma'\vec{e}_i,\ \sigma''\vec{e}_i,\ 0^n,}}^{3n} & \overbrace{\hphantom{\vec{\eta}_i,}}^{n} & \overbrace{\hphantom{0^n}}^{n} & \\
\boldsymbol{h}^*_i := & (& 0^n, & \sigma'\vec{e}_i,\ \sigma''\vec{e}_i,\ 0^n, & \vec{\eta}_i, & 0^n &)_{\mathbb{B}^*} \\
\boldsymbol{e}_{0,i} := & (& 0^n, & \omega'\vec{e}_i,\quad 0^{2n}, & 0^n, & \vec{\gamma}_i &)_{\mathbb{B}}, \\
\boldsymbol{e}_{1,i} := & (& 0^n, & 0^n,\ \ \omega''\vec{e}_i,\ 0^n, & 0^n, & \vec{\gamma}_i &)_{\mathbb{B}},
\end{array}$$

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 5, $\mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 9 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 8/q$.*

Proof. Problem 5 is essentially the same as Problem 3 in [20], where the intractability of the problem is reduced to that of DLIN. Therefore, Lemma 9 is proven in a similar manner as the reduction lemmas in [18] and [20]. □

Definition 13 (Problem 6) *Problem 6 is to guess β, given $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_{\beta,i}, \widetilde{\boldsymbol{h}}^*_{\beta,i}, \boldsymbol{e}_{\beta,i,j}\}_{i=1,\ldots,n;\ j=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P6}}_{\beta}(1^\lambda, n)$, where*

$$
\begin{array}{l}
\mathcal{G}^{\mathsf{P6}}_{\beta}(1^\lambda, n): \quad (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda, 6n), \\
\quad \widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1}, \ldots, \boldsymbol{b}_{6n}), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_{2n}, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{6n}), \\
\quad \sigma', \sigma'', \sigma''', \omega''_j, \omega'''_j \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ for } j = 1,2, \\
\quad \text{for } i = 1, \ldots, n;\ j = 1,2; \qquad \vec{\eta}_i, \vec{\vec{\eta}}_i, \vec{\gamma}_{i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n, \\
\qquad \begin{array}{rcccccl}
 & & \overbrace{\qquad\qquad}^{n} & \overbrace{\qquad\qquad\qquad\qquad}^{3n} & \overbrace{\qquad\qquad}^{n} & \overbrace{\qquad\qquad}^{n} & \\
\boldsymbol{h}^*_{0,i} := & (& 0^n, & \sigma'\vec{e}_i,\ \ \sigma''\vec{e}_i,\ \ 0^n, & \vec{\eta}_i, & 0^n &)_{\mathbb{B}^*} \\
\boldsymbol{h}^*_{1,i} := & (& 0^n, & 0^{2n}, \quad \sigma'''\vec{e}_i, & \vec{\eta}_i, & 0^n &)_{\mathbb{B}^*} \\
\boldsymbol{e}_{0,i,j} := & (& 0^n, & 0^n,\ \omega''_j\vec{e}_i,\ \omega'''_j\vec{e}_i, & 0^n, & \vec{\gamma}_{i,j} &)_{\mathbb{B}}, \\
\boldsymbol{e}_{1,i,j} := & (& 0^n, & 0^{2n}, \quad \omega'''_j\vec{e}_i, & 0^n, & \vec{\gamma}_{i,j} &)_{\mathbb{B}},
\end{array} \\
\quad \text{return}\, (\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_{\beta,i}, \widetilde{\boldsymbol{h}}^*_{\beta,i}, \boldsymbol{e}_{\beta,i,j}\}_{i=1,\ldots,n;\ j=1,2}),
\end{array}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 6, $\mathsf{Adv}^{\mathsf{P6}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 10 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P6}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_2}(\lambda) + 13/q$.*

Proof. Problem 6 is essentially the same as a combination of Problem 3 in [20] and Problem 2 in [18], where the intractability of the problem is reduced to that of DLIN. Therefore, Lemma 10 is proven in a similar manner as the reduction lemmas in [18] and [20]. □

Lemma 11 (Lemma 3 in [18]) *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 $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$.*

Lemma 12 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}(\ell-1)\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}\ell\text{-}1)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_{1\text{-}\ell\text{-}1}}(\lambda)$, where $\mathcal{B}_{1\text{-}\ell\text{-}1}(\cdot) := \mathcal{B}_{1\text{-}1}(\ell, \cdot)$.*

Proof. In order to prove Lemma 12, we construct a probabilistic machine $\mathcal{B}_{1\text{-}1}$ against Problem 1 using an adversary $\mathcal{A}$ in a security game (Game 1-$(\ell-1)$-3 or 1-ℓ-1) as a black box as follows:

1. $\mathcal{B}_{1\text{-}1}$ is given an integer ℓ and a Problem 1 instance, $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n})$.

2. $\mathcal{B}_{1\text{-}1}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. At the first step of the game, $\mathcal{B}_{1\text{-}1}$ picks a challenge bit $b \xleftarrow{\mathsf{U}} \{0,1\}$, and generates a random matrix $W \xleftarrow{\mathsf{U}} GL(6n, \mathbb{F}_q)$. $\mathcal{B}_{1\text{-}1}$ calculates $\boldsymbol{d}_i := \boldsymbol{b}_i W$ for $i = 1, \ldots, 6n$, $\mathbb{D} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{6n})$ and $\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n, \boldsymbol{d}_{5n+1}, \ldots, \boldsymbol{d}_{6n})$. $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1_\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}})$.

4. When the ι-th ciphertext query is issued for vectors $(\vec{x}_\iota^{(0)} := (x_{\iota,1}^{(0)}, \ldots, x_{\iota,n}^{(0)}), \vec{x}_\iota^{(1)} := (x_{\iota,1}^{(1)}, \ldots, x_{\iota,n}^{(1)}))$, $\mathcal{B}_{1\text{-}1}$ answers as follows:

   (a) When $\iota < \ell$, $\mathcal{B}_{1\text{-}1}$ answers ciphertexts of the form Eqs. (6) and (8), that are computed using $\mathbb{B}$ of the Problem 1 instance and $\mathbb{D}$ calculated above.

   (b) When $\iota = \ell$, $\mathcal{B}_{1\text{-}1}$ answers ciphertexts $\boldsymbol{c}_\ell := \sum_{i=1}^n x_{\ell,i}^{(b)} \boldsymbol{e}_{\beta,i}$ and $\boldsymbol{f}_\ell := (\rho' \sum_{i=1}^n x_{\ell,i}^{(b)} \boldsymbol{b}_i + \rho'' \boldsymbol{c}_\ell + \boldsymbol{z})W$ where $\rho', \rho'' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\boldsymbol{z} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{5n+1}, \ldots, \boldsymbol{b}_{6n} \rangle$, that are computed using $\mathbb{B}, \{\boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}$ of the Problem 1 instance and matrix W.

   (c) When $\iota > \ell$, $\mathcal{B}_{1\text{-}1}$ answers ciphertexts of the form Eqs. (3) and (4), that are computed using $\mathbb{B}$ of the Problem 1 instance and $\mathbb{D}$ calculated above.

5. When a token query is issued for vectors $(\vec{v}^{(0)}, \vec{v}^{(1)})$, $\mathcal{B}_{1\text{-}1}$ answers normal token $\boldsymbol{k}^*$ with Eq. (2) for $\vec{v}^{(b)}$, that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 1 instance.

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

Since the ℓ-th answered ciphertext is of the form (4) (resp. of the form (5)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{1\text{-}1}$ is distributed as in Game 1-$(\ell-1)$-3 (resp. 1-ℓ-1) if $\beta = 0$ (resp. $\beta = 1$). Then, $\left| \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}(\ell-1)\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}1)}(\lambda) \right| = \left| \mathsf{Pr}\left[\mathcal{B}_{1\text{-}1}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P1}}(1^\lambda, n) \right] - \mathsf{Pr}\left[\mathcal{B}_{1\text{-}1}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P1}}(1^\lambda, n) \right] \right| = \mathsf{Adv}_{\mathcal{B}_{1\text{-}1}}^{\mathsf{P1}}(\lambda)$. This completes the proof of Lemma 12. □

Lemma 13 *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}2)}(\lambda)| \leq (n+6)/q$.*

Proof. In order to prove Lemma 13, we define an intermediate game, Game 1-ℓ-1', and will show the equivalence of the distribution of the views of $\mathcal{A}$ in Game 1-ℓ-1 and that in Game 1-ℓ-1' (Claim 1) and those in Game 1-ℓ-2 and in Game 1-ℓ-1' (Claim 2).

Game 1-ℓ-1' : Game 1-ℓ-1' is the same as Game 1-ℓ-1 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\left.\begin{array}{l} \boldsymbol{f}_\ell := (\ \vec{r}_{f,\ell}\ )_{\mathbb{D}} \text{ with } \vec{r}_{f,\ell} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{6n}, \quad \text{i.e., } \boldsymbol{f}_\ell \xleftarrow{\mathsf{U}} \mathbb{V}, \\ \boldsymbol{c}_\ell := (\ \omega_\ell \vec{x}_\ell^{(b)},\ 0^n,\ \boxed{\vec{r}_{c,\ell}},\ 0^n,\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}}, \end{array}\right\} \tag{18}$$

where $\vec{r}_{c,\ell} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n \setminus \{\vec{0}\}$, and all the other variables are generated as in Game 1-ℓ-1.

Claim 1 *The distribution of the view of adversary $\mathcal{A}$ in Game 1-ℓ-1 and that in Game 1-ℓ-1' are equivalent except with negligible probability $(n+3)/q$.*

Proof. We will consider the distribution in Game 1-ℓ-1. We define new (dual orthonormal) bases $(\mathbb{U},\mathbb{U}^*)$ and a basis $\mathbb{W}$ of DPVS $\mathbb{V}$ below. First, we generate $F \xleftarrow{\mathsf{U}} GL(n,\mathbb{F}_q)$, and set

$$\left.\begin{array}{l}
\begin{pmatrix} \boldsymbol{u}_{2n+1}\\ \vdots \\ \boldsymbol{u}_{3n}\end{pmatrix} := F^{-1}\cdot \begin{pmatrix}\boldsymbol{b}_{2n+1}\\ \vdots\\ \boldsymbol{b}_{3n}\end{pmatrix}, \quad \begin{pmatrix}\boldsymbol{u}^*_{2n+1}\\ \vdots\\ \boldsymbol{u}^*_{3n}\end{pmatrix} := F^{\mathrm{T}}\cdot \begin{pmatrix}\boldsymbol{b}^*_{2n+1}\\ \vdots \\ \boldsymbol{b}^*_{3n}\end{pmatrix},\\
\boldsymbol{w}_{2n+i} \xleftarrow{\mathsf{U}} \mathbb{V} = \mathsf{span}\langle \boldsymbol{d}_1,\ldots,\boldsymbol{d}_{6n}\rangle \ \text{ for } i=1,\ldots,n,\\
\mathbb{U} := (\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{2n},\boldsymbol{u}_{2n+1},\ldots,\boldsymbol{u}_{3n},\boldsymbol{b}_{3n+1},\ldots,\boldsymbol{b}_{6n}),\\
\mathbb{U}^* := (\boldsymbol{b}^*_1,\ldots,\boldsymbol{b}^*_{2n},\boldsymbol{u}^*_{2n+1},\ldots,\boldsymbol{u}^*_{3n},\boldsymbol{b}^*_{3n+1},\ldots,\boldsymbol{b}^*_{6n}).\\
\mathbb{W} := (\boldsymbol{d}_1,\ldots,\boldsymbol{d}_{2n},\boldsymbol{w}_{2n+1},\ldots,\boldsymbol{w}_{3n},\boldsymbol{d}_{3n+1},\ldots,\boldsymbol{d}_{6n}),
\end{array}\right\} \tag{19}$$

except for negligible probability n/q. Then, $\mathbb{U}$ and $\mathbb{U}^*$ are dual orthonormal bases. The ℓ-th queried ciphertexts $(\boldsymbol{f}_\ell,\boldsymbol{c}_\ell)$ are expressed as

$$\left.\begin{array}{l}
\boldsymbol{f}_\ell = (\ \tau_\ell\vec{x}^{(b)}_\ell,\ 0^n,\ \tau''_\ell\vec{x}^{(b)}_\ell,\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}} = (\ \vec{r}_{f,\ell}\ )_{\mathbb{W}} \text{ with } \vec{r}_{f,\ell} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{6n}, \ \text{ i.e., } \boldsymbol{f}_\ell \xleftarrow{\mathsf{U}} \mathbb{V},\\
\boldsymbol{c}_\ell = (\ \omega_\ell\vec{x}^{(b)}_\ell,\ 0^n,\ \omega''_\ell\vec{x}^{(b)}_\ell,\ 0^n,\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}} = (\ \omega_\ell\vec{x}^{(b)}_\ell,\ 0^n,\ \vec{r}_{c,\ell},\ 0^n,\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{U}},
\end{array}\right\} \tag{20}$$

where $\tau_\ell,\tau''_\ell,\omega_\ell,\omega''_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\xi}_\ell,\vec{\varphi}_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, and $\vec{r}_{c,\ell} := \omega''\vec{x}^{(b)}_\ell \cdot F$. Since $\vec{x}^{(b)}_\ell \neq \vec{0}$, coefficient vectors $\tau''_\ell\vec{x}^{(b)}_\ell \neq \vec{0}, \omega''_\ell\vec{x}^{(b)}_\ell \neq \vec{0}$ except for probability $2/q$, i.e., except that $\tau''_\ell \neq 0$ or $\omega''_\ell \neq 0$. Then, vectors $\vec{r}_{f,\ell}$ and $\vec{r}_{c,\ell}$ are uniformly distributed in $\mathbb{F}_q^{6n}$ and $\mathbb{F}_q^n \setminus \{\vec{0}\}$, respectively, except for probability $1/q$, and they are independent from all the other variables.

Any other (ι-th) queried ciphertexts $\boldsymbol{f}$, $\boldsymbol{c}$ and queried token $\boldsymbol{k}^*$ in Game 1-ℓ-1 are:

$$\begin{array}{l}
\text{if } \iota < \ell,\ \boldsymbol{f}_\iota \xleftarrow{\mathsf{U}} \mathbb{V},\\
\qquad\qquad \boldsymbol{c}_\iota = (\ \omega_\iota\vec{x}^{(b)}_\iota,\ 0^n,\ 0^n,\ \omega'''_\iota\vec{x}^{(1-b)}_\iota,\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{B}} = (\ \omega_\iota\vec{x}^{(b)}_\iota,\ 0^n,\ 0^n,\ \omega'''_\iota\vec{x}^{(1-b)}_\iota,\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{U}},\\
\text{if } \iota > \ell,\ \boldsymbol{f}_\iota = (\ \tau_\iota\vec{x}^{(b)}_\iota,\ 0^n,\ 0^n,\ 0^n,\ 0^n,\ \vec{\xi}_\iota\ )_{\mathbb{D}} = (\ \tau_\iota\vec{x}^{(b)}_\iota,\ 0^n,\ 0^n,\ 0^n,\ 0^n,\ \vec{\xi}_\iota\ )_{\mathbb{W}},\\
\qquad\qquad \boldsymbol{c}_\iota = (\ \omega_\iota\vec{x}^{(b)}_\iota,\ 0^n,\ 0^n,\ 0^n,\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{B}} = (\ \omega_\iota\vec{x}^{(b)}_\iota,\ 0^n,\ 0^n,\ 0^n,\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{U}},\\
\boldsymbol{k}^* = (\ \sigma\vec{v}^{(b)},\ 0^n,\ 0^n,\ 0^n,\ \vec{\eta},\ 0^n\ )_{\mathbb{B}^*} = (\ \sigma\vec{v}^{(b)},\ 0^n,\ 0^n,\ 0^n,\ \vec{\eta},\ 0^n\ )_{\mathbb{U}^*},
\end{array}$$

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

In the light of the adversary's view, $(\mathbb{U},\mathbb{U}^*,\mathbb{W})$ are consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}})$. Moreover, since the RHS of Eq. (20) and that of Eq. (18) are the same form, the challenge ciphertexts $\boldsymbol{f}$, $\boldsymbol{c}$ in Game 1-ℓ-1 can be conceptually changed to that in Game 1-ℓ-1' except with probability $(n+3)/q$. □

Claim 2 *The distribution of the view of adversary $\mathcal{A}$ in Game 1-ℓ-2 and that in Game 1-ℓ-1' are equivalent except with probability $3/q$.*

Proof. Claim 2 is proven in a similar manner to Claim 1, using new orthonormal bases $(\mathbb{U},\mathbb{U}^*)$ as in Eq. (19). □

From Claims 1 and 2, adversary $\mathcal{A}$'s view in Game 1-ℓ-1 can be conceptually changed to that in Game 1-ℓ-2 except with probability $(n+6)/q$. This completes the proof of Lemma 13. □

Lemma 14 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}\ell\text{-}2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}\ell\text{-}3)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}\ell\text{-}2}}(\lambda)$, where $\mathcal{B}_{1\text{-}\ell\text{-}2}(\cdot) := \mathcal{B}_{1\text{-}2}(\ell,\cdot)$.*

Proof. In order to prove Lemma 14, we construct a probabilistic machine $\mathcal{B}_{1\text{-}2}$ against Problem 2 using an adversary $\mathcal{A}$ in a security game (Game 1-ℓ-2 or 1-ℓ-3) as a black box as follows:

1. $\mathcal{B}_{1\text{-}2}$ is given an integer ℓ and a Problem 2 instance, $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{e}_{\beta,i}\}_{i=1,\dots,n})$.

2. $\mathcal{B}_{1\text{-}2}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. At the first step of the game, $\mathcal{B}_{1\text{-}2}$ picks a challenge bit $b \xleftarrow{\mathsf{U}} \{0,1\}$, and generates a random basis $\mathbb{D} := (\boldsymbol{d}_i)_{i=1,\dots,6n}$ and set $\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \dots, \boldsymbol{d}_n, \boldsymbol{d}_{5n+1}, \dots, \boldsymbol{d}_{6n})$. $\mathcal{B}_{1\text{-}2}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1_\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}})$.

4. When the ι-th ciphertext query is issued for vectors $(\vec{x}_\iota^{(0)} := (x_{\iota,1}^{(0)}, \dots, x_{\iota,n}^{(0)}), \vec{x}_\iota^{(1)} := (x_{\iota,1}^{(1)}, \dots, x_{\iota,n}^{(1)}))$, $\mathcal{B}_{1\text{-}2}$ answers as follows:

   (a) When $\iota < \ell$, $\mathcal{B}_{1\text{-}2}$ answers ciphertexts of the form Eqs. (6) and (8), that are computed using $\mathbb{B}$ of the Problem 2 instance and $\mathbb{D}$ generated above.

   (b) When $\iota = \ell$, $\mathcal{B}_{1\text{-}2}$ answers ciphertexts $\boldsymbol{c}_\ell := \sum_{i=1}^{n}(\omega x_{\iota,i}^{(b)} \boldsymbol{b}_i + x_{\iota,i}^{(1-b)} \boldsymbol{e}_{\beta,i})$, $\boldsymbol{f}_\ell \xleftarrow{\mathsf{U}} \mathbb{V}$ where $\omega \xleftarrow{\mathsf{U}} \mathbb{F}_q$ that are computed using $\mathbb{B}$ and $\{\boldsymbol{e}_{\beta,i}\}_{i=1,\dots,n}$ of the Problem 2 instance.

   (c) When $\iota > \ell$, $\mathcal{B}_{1\text{-}2}$ answers ciphertexts of the form Eqs. (3) and (4), that are computed using $\mathbb{B}$ of the Problem 2 instance and $\mathbb{D}$ generated above.

5. When a token query is issued for vectors $(\vec{v}^{(0)}, \vec{v}^{(1)})$, $\mathcal{B}_{1\text{-}2}$ answers normal token $\boldsymbol{k}^*$ with Eq. (2) for $\vec{v}^{(b)}$, that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 2 instance.

6. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{1\text{-}2}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{1\text{-}2}$ outputs $\beta' := 0$.

Since the ℓ-th answered ciphertext is of the form Eqs. (6) and (7) (resp. of the form Eqs. (6) and (8)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{1\text{-}2}$ is distributed as in Game 1-ℓ-2 (resp. 1-ℓ-3) if $\beta = 0$ (resp. $\beta = 1$). Then, $\left|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}3)}(\lambda)\right| =$ $\left|\mathsf{Pr}\left[\mathcal{B}_{1\text{-}2}(1^\lambda, \varrho) \rightarrow 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P2}}(1^\lambda, n)\right] - \mathsf{Pr}\left[\mathcal{B}_{1\text{-}2}(1^\lambda, \varrho) \rightarrow 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P2}}(1^\lambda, n)\right]\right| = \mathsf{Adv}_{\mathcal{B}_{1\text{-}2}}^{\mathsf{P2}}(\lambda)$. This completes the proof of Lemma 14. □

Lemma 15 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}1}}^{\mathsf{P3}}(\lambda)$, where $\mathcal{B}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{2\text{-}1}(h, \cdot)$.*

Proof. In order to prove Lemma 15, we construct a probabilistic machine $\mathcal{B}_{2\text{-}1}$ against Problem 3 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 3 instance, $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}_{\beta,i}^*\}_{i=1,\dots,n})$.

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, $\mathcal{B}_{2\text{-}1}$ picks a challenge bit $b \xleftarrow{\mathsf{U}} \{0,1\}$, and generates a random basis $\mathbb{D} := (\boldsymbol{d}_i)_{i=1,\dots,6n}$ and set $\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \dots, \boldsymbol{d}_n, \boldsymbol{d}_{5n+1}, \dots, \boldsymbol{d}_{6n})$. $\mathcal{B}_{2\text{-}1}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1_\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}})$.

4. When a ciphertext query is issued for vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$, $\mathcal{B}_{2\text{-}1}$ answers ciphertexts $\boldsymbol{f}, \boldsymbol{c}$ with the form Eq. (6) and (8) for $\vec{x}^{(b)}$, that are computed using $\widehat{\mathbb{B}}$ of the Problem 3 instance and $\mathbb{D}$ generated above.

5. When the j-th token query is issued for vectors $(\vec{v}_j^{(0)} := (v_{j,1}^{(0)}, \ldots, v_{j,n}^{(0)}), \vec{v}_j^{(1)} := (v_{j,1}^{(1)}, \ldots, v_{j,n}^{(1)}))$, $\mathcal{B}_{2\text{-}1}$ answers as follows:
   (a) When $j < h$, $\mathcal{B}_{2\text{-}1}$ answers a token of the form Eq. (15), that is computed using $\mathbb{B}^*$ of the Problem 3 instance.
   (b) When $j = h$, $\mathcal{B}_{2\text{-}1}$ answers a token $\boldsymbol{k}_h^* := \sum_{i=1}^{n} v_{h,i}^{(b)} \boldsymbol{h}_{\beta,i}^*$ that is computed using $\{\boldsymbol{h}_{\beta,i}^*\}_{i=1,\ldots,n}$ of the Problem 3 instance.
   (c) When $j > h$, $\mathcal{B}_{2\text{-}1}$ answers a token of the form Eq. (2), that is computed using $\mathbb{B}^*$ of the Problem 3 instance.

6. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{2\text{-}1}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{2\text{-}1}$ outputs $\beta' := 0$.

Since the h-th answered token is of the form Eq. (2) (resp. of the form Eq. (9)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{2\text{-}1}$ is distributed as in Game 2-$(h-1)$-3 (resp. 2-h-1) if $\beta = 0$ (resp. $\beta = 1$). Then, $\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)\right| = \left|\Pr\left[\mathcal{B}_{2\text{-}1}(1^\lambda, \varrho) \rightarrow 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P3}}(1^\lambda, n)\right] - \Pr\left[\mathcal{B}_{2\text{-}1}(1^\lambda, \varrho) \rightarrow 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P3}}(1^\lambda, n)\right]\right| = \mathsf{Adv}_{\mathcal{B}_{2\text{-}1}}^{\mathsf{P3}}(\lambda)$. This completes the proof of Lemma 15. □

Lemma 16 *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}(\ell-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}1)}(\lambda)| \leq 2/q$.*

Proof. We first consider the case $\ell = 1$.

Then, Game 2-h-2-0-4 is Game 2-h-1. In order to prove Lemma 16, we define an intermediate game, Game 2-h-1', and will show the equivalence of the distribution of the views of $\mathcal{A}$ in Game 2-h-1 and that in Game 2-h-1' (Claim 3) and those in Game 2-h-2-1-1 and in Game 2-h-1' (Claim 4).

Game 2-h-1' : Game 2-h-1' is the same as Game 2-h-1 except that the reply to the h-th token query for vectors $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ is:

$$\boldsymbol{k}_h^* := (\ \sigma_h \vec{v}_h^{(b)},\ \sigma'_h \vec{v}_h^{(b)},\ \boxed{\vec{r}_h},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*}, \tag{21}$$

where $\vec{r}_h \xleftarrow{\mathsf{U}} \mathbb{F}_q^n \setminus \{\vec{0}\}$, and all the other variables are generated as in Game 2-h-1.

Claim 3 *The distribution of the view of adversary $\mathcal{A}$ in Game 2-h-1 and that in Game 2-h-1' are equivalent except with probability $1/q$.*

Proof. We will consider the distribution in Game 2-h-1. We define new (dual orthonormal) bases $(\mathbb{U}, \mathbb{U}^*)$ of DPVS $\mathbb{V}$ below. First, we generate $F \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q)$, and set orthonormal bases $\mathbb{U} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{2n}, \boldsymbol{u}_{2n+1}, \ldots, \boldsymbol{u}_{3n}, \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{6n})$ and $\mathbb{U}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_{2n}^*, \boldsymbol{u}_{2n+1}^*, \ldots, \boldsymbol{u}_{3n}^*, \boldsymbol{b}_{3n+1}^*, \ldots, \boldsymbol{b}_{6n}^*)$ as in Eq. (19). The h-th queried token $\boldsymbol{k}^*$ is expressed as

$$\boldsymbol{k}_h^* = (\ \sigma_h \vec{v}_h^{(b)},\ \sigma'_h \vec{v}_h^{(b)},\ \sigma''_h \vec{v}_h^{(b)},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*} = (\ \sigma_h \vec{v}_h^{(b)},\ \sigma'_h \vec{v}_h^{(b)},\ \vec{r}_h,\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{U}^*}, \tag{22}$$

where $\sigma_h, \sigma'_h, \sigma''_h \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\eta}_h \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, and $\vec{r}_h := \sigma''_h \vec{v}_h^{(b)} \cdot (F^{-1})^{\mathrm{T}}$. Since $\vec{v}_h^{(b)} \neq \vec{0}$, coefficient vector $\sigma''_h \vec{v}_h^{(b)} \neq \vec{0}$ except for probability $1/q$, i.e., except that $\sigma''_h \neq 0$. Then, vector $\vec{r}_h := \sigma''_h \vec{v}_h^{(b)} \cdot (F^{-1})^{\mathrm{T}}$ is uniformly distributed in $\mathbb{F}_q^n \setminus \{\vec{0}\}$ except for probability $1/q$ and independent from all the other variables.

Any other (j-th) queried token $\boldsymbol{k}^*$ and queried ciphertext $\boldsymbol{c}$ in Game 2-h-1 are:

$$\begin{aligned} \text{if } j < h,\ \boldsymbol{k}^*_j &= (\ \sigma_j \vec{v}^{(b)}_j,\ 0^n,\ 0^n,\ \sigma'''_j \vec{v}^{(1-b)}_j,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*} \\ &= (\ \sigma_j \vec{v}^{(b)}_j,\ 0^n,\ 0^n,\ \sigma'''_j \vec{v}^{(1-b)}_j,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{U}^*}, \\ \text{if } j > h,\ \boldsymbol{k}^*_j &= (\ \sigma_j \vec{v}^{(b)}_j,\ 0^n,\ 0^n,\ 0^n,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*} = (\ \sigma_j \vec{v}^{(b)}_j,\ 0^n,\ 0^n,\ 0^n,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{U}^*}, \\ \boldsymbol{c} &= (\ \omega \vec{x}^{(b)},\ 0^n,\ 0^n,\ \omega''' \vec{x}^{(1-b)},\ 0^n,\ \vec{\varphi}\ )_{\mathbb{B}} = (\ \omega \vec{x}^{(b)},\ 0^n,\ 0^n,\ \omega''' \vec{x}^{(1-b)},\ 0^n,\ \vec{\varphi}\ )_{\mathbb{U}}, \end{aligned}$$

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

In the light of the adversary's view, $(\mathbb{U}, \mathbb{U}^*)$ is consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}})$. Moreover, since the RHS of Eq. (22) and that of Eq. (21) are the same form, the view of $\mathcal{A}$ in Game 2-h-1 can be conceptually changed to that in Game 2-h-1' except with probability $1/q$. □

Claim 4 *The distribution of the view of adversary $\mathcal{A}$ in Game 2-h-2-1-1 and that in Game 2-h-1' are equivalent except with probability $1/q$.*

Proof. Claim 4 is proven in a similar manner to Claim 3, using new orthonormal bases $(\mathbb{U}, \mathbb{U}^*)$ and $\mathbb{W}$ as in Eq. (19). □

From Claims 3 and 4, adversary $\mathcal{A}$'s view in Game 2-h-1 can be conceptually changed to that in Game 2-h-2-1-1 except with probability $2/q$.

When $\ell \geq 2$, the above proof can be applied to the the first block of the hidden part instead of the second block of the hidden part. Therefore, when $\ell \geq 2$, Lemma 16 is proven in a similar way to the case $\ell = 1$.

This completes the proof of Lemma 16. □

Lemma 17 *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, $|\mathsf{Adv}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}2)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{2\text{-}h\text{-}2\text{-}\ell}}(\lambda)$, where $\mathcal{B}_{2\text{-}h\text{-}2\text{-}\ell}(\cdot) := \mathcal{B}_{2\text{-}2}(h, \ell, \cdot)$.*

Proof. In order to prove Lemma 17, we construct a probabilistic machine $\mathcal{B}_{2\text{-}2}$ against Problem 4 using an adversary $\mathcal{A}$ in a security game (Game 2-h-2-ℓ-1 or 2-h-2-ℓ-2) as a black box as follows:

1. $\mathcal{B}_{2\text{-}2}$ is given integers h, ℓ and a Problem 4 instance, $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_i, \boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n})$.

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

3. At the first step of the game, $\mathcal{B}_{2\text{-}2}$ picks a challenge bit $b \xleftarrow{\mathsf{U}} \{0, 1\}$, and generates a random basis $\mathbb{D} := (\boldsymbol{d}_i)_{i=1,\ldots,6n}$ and set $\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n, \boldsymbol{d}_{5n+1}, \ldots, \boldsymbol{d}_{6n})$. $\mathcal{B}_{2\text{-}2}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1_\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}})$.

4. When the ι-th ciphertext query is issued for vectors $(\vec{x}^{(0)}_\iota := (x^{(0)}_{\iota,1}, \ldots, x^{(0)}_{\iota,n}), \vec{x}^{(1)}_\iota := (x^{(1)}_{\iota,1}, \ldots, x^{(1)}_{\iota,n}))$, $\mathcal{B}_{2\text{-}2}$ calculates a ciphertext $\boldsymbol{f}_\iota$ of the form Eq. (6), and answers as follows:

   (a) When $\iota < \ell$, $\mathcal{B}_{2\text{-}2}$ calculates a ciphertext $\boldsymbol{c}_\iota$ of the form Eq. (14) that is computed using $\mathbb{B}$ of the Problem 4 instance, and answers $\boldsymbol{f}_\iota$ and $\boldsymbol{c}_\iota$.

   (b) When $\iota = \ell$, $\mathcal{B}_{2\text{-}2}$ calculates a ciphertext $\boldsymbol{c}_\ell := \sum_{i=1}^{n}(x^{(b)}_{\ell,i} \boldsymbol{e}_{\beta,i} + \omega''' x^{(1-b)}_{\ell,i} \boldsymbol{b}_{3n+i})$ where $\omega''' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ that is computed using $\{\boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}$ and $\mathbb{B}$ of the Problem 4 instance. $\mathcal{B}_{2\text{-}2}$ answers $\boldsymbol{f}_\ell$ and $\boldsymbol{c}_\ell$.

    (c) When $\iota > \ell$, $\mathcal{B}_{2\text{-}2}$ calculates a ciphertext of the form Eq. (8), that is computed using $\mathbb{B}$ of the Problem 4 instance. $\mathcal{B}_{2\text{-}2}$ answers $\boldsymbol{f}$ and $\boldsymbol{c}$.

5. When the j-th token query is issued for vectors $(\vec{v}_j^{(0)} := (v_{j,1}^{(0)}, \ldots, v_{j,n}^{(0)}), \vec{v}_j^{(1)} := (v_{j,1}^{(1)}, \ldots, v_{j,n}^{(1)}))$, $\mathcal{B}_{2\text{-}2}$ answers as follows:
    (a) When $j < h$, $\mathcal{B}_{2\text{-}2}$ answers a token of the form Eq. (15), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 4 instance.
    (b) When $j = h$, $\mathcal{B}_{2\text{-}2}$ answers a token $\boldsymbol{k}_h^* := \sum_{i=1}^{n}(v_{h,i}^{(b)}\boldsymbol{h}_i^* + \sigma'' v_{h,i}^{(1-b)}\boldsymbol{b}_{2n+i}^*)$ where $\sigma'' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ that is computed using $\{\boldsymbol{h}_i^*\}_{i=1,\ldots,n}$ and $\widehat{\mathbb{B}}^*$ of the Problem 4 instance.
    (c) When $j > h$, $\mathcal{B}_{2\text{-}2}$ answers a token of the form Eq. (2), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 4 instance.

6. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{2\text{-}2}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{2\text{-}2}$ outputs $\beta' := 0$.

The h-th answered token is of the form Eq. (10). Since the ℓ-th answered ciphertext is of the form Eq. (8) (resp. of the form Eq. (11)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{2\text{-}2}$ is distributed as in Game 2-h-2-ℓ-1 (resp. 2-h-2-ℓ-2) if $\beta = 0$ (resp. $\beta = 1$). Then, $\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}2)}(\lambda)\right| = \left|\Pr\left[\mathcal{B}_{2\text{-}2}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P4}}(1^\lambda, n)\right] - \Pr\left[\mathcal{B}_{2\text{-}2}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P4}}(1^\lambda, n)\right]\right| = \mathsf{Adv}_{\mathcal{B}_{2\text{-}2}}^{\mathsf{P4}}(\lambda)$. This completes the proof of Lemma 17. □

Lemma 18 *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}3)}(\lambda)| \le 8/q$.*

Proof. In order to prove Lemma 18, we define an intermediate game, Game 2-h-2-ℓ-2', and will show the equivalence of the distribution of the views of $\mathcal{A}$ in Game 2-h-2-ℓ-2 and that in Game 2-h-2-ℓ-2' (Claim 5) and those in Game 2-h-2-ℓ-3 and in Game 2-h-2-ℓ-2' (Claim 6).

Game 2-h-2-ℓ-2' : Game 2-h-2-ℓ-2' is the same as Game 2-h-2-ℓ-2 except the reply to the h-th token query for $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ is:

$$\boldsymbol{k}_h^* := (\ \sigma_h \vec{v}_h^{(b)},\ \boxed{\vec{w}_h},\ \sigma_h'' \vec{v}_h^{(1-b)},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*}, \tag{23}$$

and the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\boldsymbol{c}_\ell := (\ \omega_\ell \vec{x}_\ell^{(b)},\ \boxed{\vec{r}_\ell},\ 0^n,\ \omega_\ell''' \vec{x}_\ell^{(1-b)},\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}}, \tag{24}$$

where, if $\vec{x}_\ell^{(b)} \cdot \vec{v}_h^{(b)} = 0$ (and $\vec{x}_\ell^{(1-b)} \cdot \vec{v}_h^{(1-b)} = 0$), then $(\vec{r}_\ell, \vec{w}_h) \xleftarrow{\mathsf{U}} W_0 := \{(\vec{r}, \vec{w}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n | \vec{r} \cdot \vec{w} = 0\}$, and if $\vec{x}_\ell^{(b)} \cdot \vec{v}_h^{(b)} \neq 0$ (and $\vec{x}_\ell^{(1-b)} \cdot \vec{v}_h^{(1-b)} \neq 0$), then $(\vec{r}_\ell, \vec{w}_h) \xleftarrow{\mathsf{U}} \mathbb{F}_q^n \times \mathbb{F}_q^n \setminus W_0$, and all the variables are generated as in Game 2-h-2-ℓ-2.

Claim 5 *The distribution of the view of adversary $\mathcal{A}$ in Game 2-h-2-ℓ-2 and that in Game 2-h-2-ℓ-2' are equivalent except with probability $4/q$.*

Proof. We will consider the distribution in Game 2-h-2-ℓ-2. We define new (dual orthonormal) bases $(\mathbb{U}, \mathbb{U}^*)$ of DPVS $\mathbb{V}$ below. First, we generate $U \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q)$, and set

$$\left.\begin{array}{l}
\begin{pmatrix} \boldsymbol{u}_{n+1} \\ \vdots \\ \boldsymbol{u}_{2n} \end{pmatrix} := U^{-1} \cdot \begin{pmatrix} \boldsymbol{b}_{n+1} \\ \vdots \\ \boldsymbol{b}_{2n} \end{pmatrix}, \quad \begin{pmatrix} \boldsymbol{u}_{n+1}^* \\ \vdots \\ \boldsymbol{u}_{2n}^* \end{pmatrix} := U^{\mathrm{T}} \cdot \begin{pmatrix} \boldsymbol{b}_{n+1}^* \\ \vdots \\ \boldsymbol{b}_{2n}^* \end{pmatrix}, \\
\mathbb{U} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n, \boldsymbol{u}_{n+1}, \ldots, \boldsymbol{u}_{2n}, \boldsymbol{b}_{2n+1}, \ldots, \boldsymbol{b}_{6n}), \\
\mathbb{U}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*, \boldsymbol{u}_{n+1}^*, \ldots, \boldsymbol{u}_{2n}^*, \boldsymbol{b}_{2n+1}^*, \ldots, \boldsymbol{b}_{6n}^*).
\end{array}\right\} \tag{25}$$

Then, $\mathbb{U}$ and $\mathbb{U}^*$ are dual orthonormal bases. The ℓ-th queried ciphertext $\boldsymbol{c}_\ell$ and the h-th queried token $\boldsymbol{k}_h^*$ are expressed as

$$\boldsymbol{c}_\ell = (\ \omega_\ell \vec{x}_\ell^{(b)},\ \omega'_\ell \vec{x}_\ell^{(b)},\ 0^n,\ \omega'''_\ell \vec{x}_\ell^{(1-b)},\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{B}} = (\ \omega_\ell \vec{x}_\ell^{(b)},\ \vec{r}_\ell,\ 0^n,\ \omega'''_\ell \vec{x}_\ell^{(1-b)},\ 0^n,\ \vec{\varphi}_\ell\ )_{\mathbb{U}}, \quad (26)$$

$$\boldsymbol{k}_h^* = (\ \sigma_h \vec{v}_h^{(b)},\ \sigma'_h \vec{v}_h^{(b)},\ \sigma''_h \vec{v}_h^{(1-b)},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*} = (\ \sigma_h \vec{v}_h^{(b)},\ \vec{w}_h,\ \sigma''_h \vec{v}_h^{(1-b)},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{U}^*}, \ (27)$$

where $\omega_\ell, \omega'_\ell, \omega'''_\ell, \sigma_h, \sigma'_h, \sigma''_h \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\varphi}_\ell, \vec{\eta}_h \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, and $\vec{r}_\ell := \omega'_\ell \vec{x}_\ell^{(b)} \cdot U,\ \vec{w}_h := \sigma' \vec{v}_h^{(b)} \cdot (U^{-1})^{\mathrm{T}}$.

From Lemma 11, if $\vec{x}_\ell^{(b)} \cdot \vec{v}_h^{(b)} \neq 0$, the pair of coefficients $(\omega'_\ell \vec{x}_\ell^{(b)} U, \sigma'_h \vec{v}_h (U^{-1})^{\mathrm{T}})$ are uniformly distributed in $\mathbb{F}_q^n \times \mathbb{F}_q^n \setminus W_0$ and independent from all the other variables except for the case $\omega'_\ell = 0$ or $\sigma'_h = 0$, i.e., except with probability $2/q$.

Also, from Lemma 11, if $\vec{x}_\ell^{(b)} \cdot \vec{v}_h^{(b)} = 0$, the pair of coefficients $(\omega'_\ell \vec{x}_\ell^{(b)} U, \sigma'_h \vec{v}_h (U^{-1})^{\mathrm{T}})$ are uniformly distributed in W_0 and independent from all the other variables except for the case $\omega'_\ell = 0$ or $\sigma'_h = 0$, i.e., except with probability $2/q$.

Any other (ι-th) queried ciphertext $\boldsymbol{c}_\iota$ and (j-th) queried token $\boldsymbol{k}_j^*$ in Game 2-h-2-ℓ-2 are:

$$\begin{aligned}
&\text{if } \iota < \ell,\ \boldsymbol{c}_\iota = (\ \omega_\iota \vec{x}_\iota^{(b)},\ 0^n,\ \omega''_\iota \vec{x}_\iota^{(1-b)},\ \omega'''_\iota \vec{x}_\iota^{(1-b)},\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{B}} \\
&\qquad\qquad = (\ \omega_\iota \vec{x}_\iota^{(b)},\ 0^n,\ \omega''_\iota \vec{x}_\iota^{(1-b)},\ \omega'''_\iota \vec{x}_\iota^{(1-b)},\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{U}}, \\
&\text{if } \iota > \ell,\ \boldsymbol{c} = (\ \omega_\iota \vec{x}_\iota^{(b)},\ 0^n,\ 0^n,\ \omega'''_\iota \vec{x}_\iota^{(1-b)},\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{B}} = (\ \omega_\iota \vec{x}_\iota^{(b)},\ 0^n,\ 0^n,\ \omega'''_\iota \vec{x}_\iota^{(1-b)},\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{U}}, \\
&\text{if } j < h,\ \boldsymbol{k}_j^* = (\ \sigma_j \vec{v}_j^{(b)},\ 0^n,\ 0^n,\ \sigma'''_j \vec{v}_j^{(b)},\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*} = (\ \sigma_j \vec{v}_j^{(b)},\ 0^n,\ 0^n,\ \sigma'''_j \vec{v}_j^{(b)},\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{U}^*}, \\
&\text{if } j > h,\ \boldsymbol{k}_j^* = (\ \sigma_j \vec{v}_j^{(b)},\ 0^n,\ 0^n,\ 0^n,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*} = (\ \sigma_j \vec{v}_j^{(b)},\ 0^n,\ 0^n,\ 0^n,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{U}^*},
\end{aligned}$$

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

In the light of the adversary's view, $(\mathbb{U}, \mathbb{U}^*)$ is consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$. Moreover, since the RHS of Eq. (26) (resp. the RHS of Eq. (27)) and that of Eq. (24) (resp. that of Eq. (23) are the same form, the view of $\mathcal{A}$ in Game 2-h-2-ℓ-2 can be conceptually changed to that in Game 2-h-2-ℓ-2' except with probability $4/q$. □

Claim 6 *The distribution of the view of adversary $\mathcal{A}$ in Game 2-h-2-ℓ-3 and that in Game 2-h-2-ℓ-2' are equivalent except with probability $4/q$.*

Proof. Claim 6 is proven in a similar manner to Claim 5, using new orthonormal bases $(\mathbb{U}, \mathbb{U}^*)$ as in Eq. (25). □

From Claims 5 and 6, adversary $\mathcal{A}$'s view in Game 2-h-2-ℓ-2 can be conceptually changed to that in Game 2-h-2-ℓ-3 except with probability $8/q$. This completes the proof of Lemma 18. □

Lemma 19 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}3}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}4)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}3\text{-}\ell}}^{\mathsf{P5}}(\lambda)$, where $\mathcal{B}_{2\text{-}h\text{-}3\text{-}\ell}(\cdot) := \mathcal{B}_{2\text{-}3}(h, \ell, \cdot)$.*

Proof. In order to prove Lemma 19, we construct a probabilistic machine $\mathcal{B}_{2\text{-}3}$ against Problem 5 using an adversary $\mathcal{A}$ in a security game (Game 2-h-2-ℓ-3 or 2-h-2-ℓ-4) as a black box as follows:

1. $\mathcal{B}_{2\text{-}3}$ is given integers h, ℓ and a Problem 5 instance, $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}_i^*, \boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n})$.

2. $\mathcal{B}_{2\text{-}3}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. At the first step of the game, $\mathcal{B}_{2\text{-}3}$ picks a challenge bit $b \xleftarrow{\mathsf{U}} \{0,1\}$, and generates a random basis $\mathbb{D} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{6n})$, and calculates $\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n, \boldsymbol{d}_{5n+1}, \ldots, \boldsymbol{d}_{6n})$. $\mathcal{B}_{2\text{-}3}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1_\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}})$.

4. When the ι-th ciphertext query is issued for vectors $(\vec{x}_\iota^{(0)} := (x_{\iota,1}^{(0)}, \ldots, x_{\iota,n}^{(0)}), \vec{x}_\iota^{(1)} := (x_{\iota,1}^{(1)}, \ldots, x_{\iota,n}^{(1)}))$, $\mathcal{B}_{2\text{-}3}$ calculates a ciphertext $\boldsymbol{f}_\iota$ of the form Eq. (6), and answers as follows:

   (a) When $\iota < \ell$, $\mathcal{B}_{2\text{-}3}$ calculates a ciphertext $\boldsymbol{c}_\iota$ of the form Eq. (14), that is computed using $\mathbb{B}$ of the Problem 5 instance. $\mathcal{B}_{2\text{-}3}$ answers $\boldsymbol{f}_\iota$ and $\boldsymbol{c}_\iota$.

   (b) When $\iota = \ell$, $\mathcal{B}_{2\text{-}3}$ calculates a ciphertext $\boldsymbol{c}_\ell := \sum_{i=1}^{n}(\omega x_{\ell,i}^{(b)} \boldsymbol{b}_i + x_{\ell,i}^{(1-b)} \boldsymbol{e}_{\beta,i} + \omega''' x_{\ell,i}^{(1-b)} \boldsymbol{b}_{3n+i})$ where $\omega, \omega''' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ that is computed using $\{\boldsymbol{e}_{\beta,i}\}_{i=1,\ldots,n}$ and $\mathbb{B}$ of the Problem 5 instance. $\mathcal{B}_{2\text{-}3}$ answers $\boldsymbol{f}_\ell$ and $\boldsymbol{c}_\ell$.

   (c) When $\iota > \ell$, $\mathcal{B}_{2\text{-}3}$ calculates a ciphertext $\boldsymbol{c}_\iota$ of the form Eq. (8), that is computed using $\mathbb{B}$ of the Problem 5 instance. $\mathcal{B}_{2\text{-}3}$ answers $\boldsymbol{f}_\iota$ and $\boldsymbol{c}_\iota$.

5. When the j-th token query is issued for vectors $(\vec{v}_j^{(0)} := (v_{j,1}^{(0)}, \ldots, v_{j,n}^{(0)}), \vec{v}_j^{(1)} := (v_{j,1}^{(1)}, \ldots, v_{j,n}^{(1)}))$, $\mathcal{B}_{2\text{-}3}$ answers as follows:

   (a) When $j < h$, $\mathcal{B}_{2\text{-}3}$ answers a token of the form Eq. (15), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 5 instance.

   (b) When $j = h$, $\mathcal{B}_{2\text{-}3}$ answers a token $\boldsymbol{k}_j^* := \sum_{i=1}^{n}(\sigma v_{j,i}^{(b)} \boldsymbol{b}_i^* + v_{j,i}^{(1-b)} \boldsymbol{h}_i^*)$ where $\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q$ that is computed using $\{\boldsymbol{h}_i^*\}_{i=1,\ldots,n}$ and $\widehat{\mathbb{B}}^*$ of the Problem 5 instance.

   (c) When $j > h$, $\mathcal{B}_{2\text{-}3}$ answers a token of the form Eq. (2), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 5 instance.

6. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{2\text{-}3}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{2\text{-}3}$ outputs $\beta' := 0$.

The h-th answered token is of the form Eq. (12). Since the ℓ-th answered ciphertext is of the form Eq. (13) (resp. of the form Eq. (14)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{2\text{-}3}$ is distributed as in Game 2-h-2-ℓ-3 (resp. 2-h-2-ℓ-4) if $\beta = 0$ (resp. $\beta = 1$). Then, $\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\ell\text{-}4)}(\lambda)\right| = \left|\mathsf{Pr}\left[\mathcal{B}_{2\text{-}3}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P5}}(1^\lambda, n)\right] - \mathsf{Pr}\left[\mathcal{B}_{2\text{-}3}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P5}}(1^\lambda, n)\right]\right| = \mathsf{Adv}_{\mathcal{B}_{2\text{-}3}}^{\mathsf{P5}}(\lambda)$. This completes the proof of Lemma 19. □

Lemma 20 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}4}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\nu_1\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}4}}^{\mathsf{P6}}(\lambda)$, where $\mathcal{B}_{2\text{-}h\text{-}4}(\cdot) := \mathcal{B}_{2\text{-}4}(h, \cdot)$.*

Proof. In order to prove Lemma 20, we construct a probabilistic machine $\mathcal{B}_{2\text{-}4}$ against Problem 6 using an adversary $\mathcal{A}$ in a security game (Game 2-h-2-ν_1-4 or 2-h-3) as a black box as follows:

1. $\mathcal{B}_{2\text{-}4}$ is given integers h and a Problem 6 instance, $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_{\beta,i,\kappa}\}_{i=1,\ldots,n;\ \kappa=1,2})$.

2. $\mathcal{B}_{2\text{-}4}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. At the first step of the game, $\mathcal{B}_{2\text{-}4}$ picks a challenge bit $b \xleftarrow{\mathsf{U}} \{0,1\}$, and generates a random basis $\mathbb{D} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{6n})$, and calculates $\widehat{\mathbb{D}} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n, \boldsymbol{d}_{5n+1}, \ldots, \boldsymbol{d}_{6n})$. $\mathcal{B}_{2\text{-}4}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1_\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}})$.

4. When the ι-th ciphertext query is issued for vectors $(\vec{x}_\iota^{(0)} := (x_{\iota,1}^{(0)}, \ldots, x_{\iota,n}^{(0)}), \vec{x}_\iota^{(1)} := (x_{\iota,1}^{(1)}, \ldots, x_{\iota,n}^{(1)}))$, $\mathcal{B}_{2\text{-}4}$ answers a ciphertext $\boldsymbol{f}$ of the form Eq. (6), and $\boldsymbol{c}_\iota := \sum_{i=1}^{n}(\omega_\iota x_{\iota,i}^{(b)}\boldsymbol{b}_i + x_{\iota,i}^{(1-b)}(\delta_{\iota,1}\boldsymbol{e}_{\beta,i,1} + \delta_{\iota,2}\boldsymbol{e}_{\beta,i,2}) + \widetilde{\gamma}_{\iota,i}\boldsymbol{b}_{5n+i})$ where $\omega_\iota, \delta_{\iota,1}, \delta_{\iota,2}, \widetilde{\gamma}_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ that is computed using $\{\boldsymbol{e}_{\beta,i,\kappa}\}_{i=1,\ldots,n;\ \kappa=1,2}$ and $\widehat{\mathbb{B}}$ of the Problem 6 instance.

5. When the j-th token query is issued for vectors $(\vec{v}_j^{(0)} := (v_{j,1}^{(0)}, \ldots, v_{j,n}^{(0)}), \vec{v}_j^{(1)} := (v_{j,1}^{(1)}, \ldots, v_{j,n}^{(1)}))$, $\mathcal{B}_{2\text{-}4}$ answers as follows:

   (a) When $j < h$, $\mathcal{B}_{2\text{-}4}$ answers a token of the form Eq. (15), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 6 instance.

   (b) When $j = h$, $\mathcal{B}_{2\text{-}4}$ answers a token $\boldsymbol{k}_h^* := \sum_{i=1}^{n}(\sigma v_{h,i}^{(b)}\boldsymbol{b}_i^* + v_{h,i}^{(1-b)}\boldsymbol{h}_{\beta,i}^*)$ where $\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q$ that is computed using $\{\boldsymbol{h}_{\beta,i}^*\}_{i=1,\ldots,n}$ and $\widehat{\mathbb{B}}^*$ of the Problem 6 instance.

   (c) When $j > h$, $\mathcal{B}_{2\text{-}4}$ answers a token of the form Eq. (2), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 6 instance.

6. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{2\text{-}4}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{2\text{-}4}$ outputs $\beta' := 0$.

Claim 7 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_{2\text{-}4}$ given a Problem 6 instance with $\beta \in \{0,1\}$ is the same as that in Game 2-h-2-ν_1-4 (resp. Game 2-h-3) if $\beta = 0$ (resp. $\beta = 1$).*

Proof. We will consider the joint distribution of $\{\boldsymbol{c}_\iota\}_{\iota=1}^{\nu_1}$ and $\{\boldsymbol{k}_j^*\}_{j=1}^{\nu_2}$. We note that if $j \neq h$, each secret key $\boldsymbol{k}_j^*$ is generated independently from other queries. Therefore, we only consider the distribution of the h-th token $\boldsymbol{k}_h^*$ below.

When $\beta = 0$, ciphertext $\boldsymbol{c}_\iota$ generated in step 4 is

$$\begin{aligned} \boldsymbol{c}_\iota &:= \textstyle\sum_{i=1}^{n}(\omega_\iota x_{\iota,i}^{(b)}\boldsymbol{b}_i + x_{\iota,i}^{(1-b)}(\delta_{\iota,1}\boldsymbol{e}_{0,i,1} + \delta_{\iota,2}\boldsymbol{e}_{0,i,2}) + \widetilde{\gamma}_{\iota,i}\boldsymbol{b}_{5n+i}) \\ &= (\ \omega_\iota\vec{x}_\iota^{(b)},\ 0^n,\ (\delta_{\iota,1}\omega_1'' + \delta_{\iota,2}\omega_2'')\vec{x}_\iota^{(1-b)},\ (\delta_{\iota,1}\omega_1''' + \delta_{\iota,2}\omega_2''')\vec{x}_\iota^{(1-b)},\ 0^n,\ \vec{\gamma}_\iota'\ )_{\mathbb{B}} \end{aligned}$$

where $\omega_\iota, \delta_{\iota,1}\omega_1'' + \delta_{\iota,2}\omega_2'', \delta_{\iota,1}\omega_1''' + \delta_{\iota,2}\omega_2''' \in \mathbb{F}_q$ and $\vec{\gamma}_\iota' \in \mathbb{F}_q^n$ for $\iota = 1, \ldots, \nu_1$ are uniformly and independently distributed.

When $\beta = 1$, ciphertext $\boldsymbol{c}_\iota$ generated in step 4 is

$$\begin{aligned} \boldsymbol{c}_\iota &:= \textstyle\sum_{i=1}^{n}(\omega_\iota x_{\iota,i}^{(b)}\boldsymbol{b}_i + x_{\iota,i}^{(1-b)}(\delta_{\iota,1}\boldsymbol{e}_{1,i,1} + \delta_{\iota,2}\boldsymbol{e}_{1,i,2}) + \widetilde{\gamma}_{\iota,i}\boldsymbol{b}_{5n+i}) \\ &= (\ \omega_\iota\vec{x}_\iota^{(b)},\ 0^n,\ 0^n,\ (\delta_{\iota,1}\omega_1''' + \delta_{\iota,2}\omega_2''')\vec{x}_\iota^{(1-b)},\ 0^n,\ \vec{\gamma}_\iota'\ )_{\mathbb{B}} \end{aligned}$$

where $\omega_\iota, \delta_{\iota,1}\omega_1''' + \delta_{\iota,2}\omega_2''' \in \mathbb{F}_q$ and $\vec{\gamma}_\iota' \in \mathbb{F}_q^n$ for $\iota = 1, \ldots, \nu_1$ are uniformly and independently distributed.

When $\beta = 0$, the h-th token $\boldsymbol{k}_h^*$ generated in step (b) is

$$\boldsymbol{k}_h^* \ := \ \textstyle\sum_{i=1}^{n}(\sigma v_{h,i}^{(b)}\boldsymbol{b}_i^* + v_{h,i}^{(1-b)}\boldsymbol{h}_{0,i}^*) = (\ \sigma\vec{v}_h^{(b)},\ \sigma'\vec{v}_h^{(1-b)},\ \sigma''\vec{v}_h^{(1-b)},\ 0^n,\ \vec{\eta}',\ 0^n\ )_{\mathbb{B}^*},$$

where $\sigma, \sigma', \sigma'' \in \mathbb{F}_q$ and $\vec{\eta}' \in \mathbb{F}_q^n$ are uniformly and independently distributed.

When $\beta = 1$, the h-th token $\boldsymbol{k}_h^*$ generated in step (b) is

$$\boldsymbol{k}_h^* \ := \ \textstyle\sum_{i=1}^{n}(\sigma v_{h,i}^{(b)}\boldsymbol{b}_i^* + v_{h,i}^{(1-b)}\boldsymbol{h}_{1,i}^*) = (\ \sigma\vec{v}_h^{(b)},\ 0^n,\ 0^n,\ \sigma'''\vec{v}_h^{(1-b)},\ \vec{\eta}',\ 0^n\ )_{\mathbb{B}^*},$$

where $\sigma, \sigma''' \in \mathbb{F}_q$ and $\vec{\eta}' \in \mathbb{F}_q^n$ are uniformly and independently distributed.

Therefore, generated $\{\boldsymbol{c}_\iota\}_{\iota=1}^{\nu_1}$ and $\{\boldsymbol{k}^*_j\}_{j=1}^{\nu_2}$ have the same joint distribution as in Game 2-h-2-ν_1-4 (resp. Game 2-h-3) if $\beta = 0$ (resp. $\beta = 1$). □

From Claim 7, $\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2\text{-}\nu_1\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda)\right| = \left|\mathsf{Pr}\left[\mathcal{B}_{2\text{-}4}(1^\lambda, \varrho) \rightarrow 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P6}}(1^\lambda, n)\right] - \mathsf{Pr}\left[\mathcal{B}_{2\text{-}4}(1^\lambda, \varrho) \rightarrow 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P6}}(1^\lambda, n)\right]\right| = \mathsf{Adv}_{\mathcal{B}_{2\text{-}4}}^{\mathsf{P6}}(\lambda)$. This completes the proof of Lemma 20. □

Lemma 21 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu_2\text{-}3)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)$.*

Proof. In Game 2-ν_2-3, for $j = 1, \ldots, \nu_2$, the reply to the j-th token query for $(\vec{v}_j^{(0)}, \vec{v}_j^{(1)})$ are given as

$$\boldsymbol{k}^*_j := (\ \sigma_j \vec{v}_j^{(b)},\ 0^n,\ 0^n,\ \sigma_j''' \vec{v}_j^{(1-b)},\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*} \quad \text{for } j = 1, \ldots, \nu_2,$$

where $\sigma_j, \sigma_j''' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\eta}_j \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, and for $j = 1, \ldots, \nu_2$, the ι-th reply to a ciphertext query for vectors $(\vec{x}_\iota^{(0)}, \vec{x}_\iota^{(1)})$ are given as

$$\begin{aligned} &\boldsymbol{f}_\iota \xleftarrow{\mathsf{U}} \mathbb{V} \quad \text{for } \iota = 1, \ldots, \nu_1, \\ &\boldsymbol{c}_\iota := (\ \omega_\iota \vec{x}_\iota^{(b)},\ 0^n,\ 0^n,\ \omega_\iota''' \vec{x}_\iota^{(1-b)},\ 0^n,\ \vec{\varphi}_\iota\ )_{\mathbb{B}} \quad \text{for } \iota = 1, \ldots, \nu_1, \end{aligned}$$

where $\omega_\iota, \omega_\iota''' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\varphi}_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$.

Therefore, by swapping basis vectors in the first block and the fourth block, we obtain the distribution in Game 3. That is, we define new dual orthonormal bases $(\mathbb{U}, \mathbb{U}^*)$ of DPVS $\mathbb{V}$ as

$$\begin{aligned} &\boldsymbol{u}_i := \boldsymbol{b}_{3n+i}, \quad \boldsymbol{u}_{3n+i} := \boldsymbol{b}_i, \quad \boldsymbol{u}^*_i := \boldsymbol{b}^*_{3n+i}, \quad \boldsymbol{u}^*_{3n+i} := \boldsymbol{b}^*_i \quad \text{for } i = 1, \ldots, n, \\ &\mathbb{U} := (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, \boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{3n}, \boldsymbol{u}_{3n+1}, \ldots, \boldsymbol{u}_{4n}, \boldsymbol{b}_{4n+1}, \ldots, \boldsymbol{b}_{6n}), \\ &\mathbb{U}^* := (\boldsymbol{u}^*_1, \ldots, \boldsymbol{u}^*_n, \boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{3n}, \boldsymbol{u}^*_{3n+1}, \ldots, \boldsymbol{u}^*_{4n}, \boldsymbol{b}^*_{4n+1}, \ldots, \boldsymbol{b}^*_{6n}). \end{aligned}$$

We then easily verify that $\mathbb{U}$ and $\mathbb{U}^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}$ and $\mathbb{B}^*$. Tokens and ciphertexts in Game 2-ν_2-3 over bases $(\mathbb{B}, \mathbb{B}^*)$ are expressed those in Game 3 over bases $(\mathbb{U}, \mathbb{U}^*)$. This completes the proof of Lemma 21. □

Lemma 22 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(5\text{-}\nu_1\text{-}3)}(\lambda) = -\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$.*

Proof. All $\boldsymbol{k}^*_j$ and $\boldsymbol{c}_\iota$ are normal tokens and ciphertexts for the opposite bit $1 - b$ to the challenge bit b in Game 5-ν_1-3. Hence, success probability $\mathsf{Pr}[\,\mathsf{Succ}_{\mathcal{A}}^{(5\text{-}\nu_1\text{-}3)}(\lambda)\,]$ in Game 5-ν_1-3 is $1 - \mathsf{Pr}[\,\mathsf{Succ}_{\mathcal{A}}^{(0)}(\lambda)\,]$, where $\mathsf{Pr}[\,\mathsf{Succ}_{\mathcal{A}}^{(0)}(\lambda)\,]$ is success probability in Game 0. Therefore, we have $\mathsf{Adv}_{\mathcal{A}}^{(5\text{-}\nu_1\text{-}3)}(\lambda) = -\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$. □

B.2 Proof of Lemma 2

Lemma 2. *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisH}}(\lambda)$ is negligible under the DLIN assumption.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_1, \mathcal{E}_{2\text{-}1}, \mathcal{E}_{2\text{-}2}, \mathcal{E}_{3\text{-}1}, \mathcal{E}_{3\text{-}2}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\begin{aligned} \mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisH}}(\lambda) \leq \sum_{\ell=1}^{\nu_1} \Bigg(&\mathsf{Adv}_{\mathcal{E}_{\ell\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \sum_{h=1}^{\nu_2} \Big(\mathsf{Adv}_{\mathcal{E}_{\ell\text{-}2\text{-}h\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{\ell\text{-}2\text{-}h\text{-}2}}^{\mathsf{DLIN}}(\lambda) \Big) \\ &+ \mathsf{Adv}_{\mathcal{E}_{\ell\text{-}3\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{\ell\text{-}3\text{-}2}}^{\mathsf{DLIN}}(\lambda) \Bigg) + \epsilon, \end{aligned}$$

where $\mathcal{E}_{\ell\text{-}1}(\cdot) := \mathcal{E}_1(\ell,\cdot), \mathcal{E}_{\ell\text{-}2\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{2\text{-}1}(\ell,h,\cdot), \mathcal{E}_{\ell\text{-}2\text{-}h\text{-}2}(\cdot) := \mathcal{E}_{2\text{-}2}(\ell,h,\cdot), \mathcal{E}_{\ell\text{-}3\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{3\text{-}1}(\ell,h,\cdot)$, $\mathcal{E}_{\ell\text{-}3\text{-}h\text{-}2}(\cdot) := \mathcal{E}_{3\text{-}2}(\ell,h,\cdot)$, ν_1 *(resp.* ν_2*) is the maximum number of* $\mathcal{A}$*'s challenge ciphertext (resp. key) queries and* $\epsilon := \nu_1(23\nu_2+22)/q$.

Note that Lemma 2 is proven in a similar manner to the basic IPE scheme in [20]. For completeness, we give game transformations for the proof of Lemma 2.

Let ν_1 be the maximum number of $\mathcal{A}$'s challenge ciphertext queries and ν_2 the maximum number of $\mathcal{A}$'s challenge token queries. To prove Lemma 2, we consider the following $4\nu_1\nu_2 + 3\nu_1 + 1$ games. In Game 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0 : For $j = 1,\dots,\nu_2$, the reply to the j-th token query for $\vec{v}_j$ is:

$$\boldsymbol{k}_j^* := (\ \sigma_j\vec{v}_j,\ \boxed{0^n},\ \boxed{0^n},\ 0^n,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*},$$

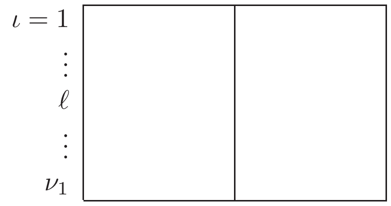
where $\sigma_j \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\eta}_j \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$. For $\iota = 1,\dots,\nu_1$, the reply to the ι-th ciphertext query for vectors $(\vec{x}_\iota^{(0)}, \vec{x}_\iota^{(1)})$ is:

$$\boldsymbol{f}_\iota := (\ \boxed{\tau_\iota\vec{x}_\iota^{(b)}},\ \boxed{0^n},\ \boxed{0^n},\ 0^n,\ 0^n,\ \vec{\xi}_\iota\ )_{\mathbb{D}},$$

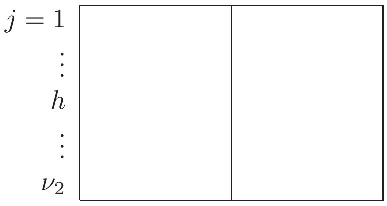
where $b \xleftarrow{\mathsf{U}} \{0,1\}$ and $\tau_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\xi}_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$.

Below, we describe coefficients of the hidden part, i.e., $\mathsf{span}\langle \boldsymbol{d}_{n+1},\dots,\boldsymbol{d}_{3n}\rangle$ (resp. $\mathsf{span}\langle \boldsymbol{b}_{n+1}^*,\dots,\boldsymbol{b}_{3n}^*\rangle$) of the ι-th queried $\boldsymbol{f}_\iota$ for $\iota = 1,\dots,\nu_1$ (resp. the j-th queried $\boldsymbol{k}_j^*$ for $j = 1,\dots,\nu_2$) w.r.t. these bases vectors. Non-zero coefficients are colored by light gray, and those which were changed from the previous game are colored by dark gray.

Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game 0



Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game 0

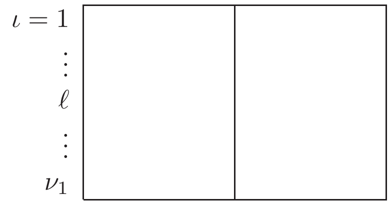


Game $\boldsymbol{\ell}$-1 ($\boldsymbol{\ell = 1,\dots,\nu_1}$) : Game 0-4 is Game 0. Game ℓ-1 is the same as Game $(\ell-1)$-4 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

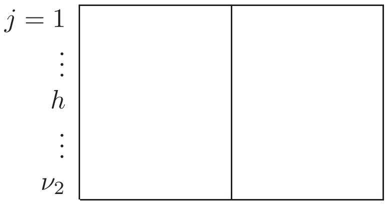
$$\boldsymbol{f}_\ell := (\ \tau_\ell\vec{x}_\ell^{(b)},\ \boxed{\tau'_\ell\vec{x}_\ell^{(b)}},\ \boxed{\tau''_\ell\vec{x}_\ell^{(b)}},\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}},$$

where $\tau'_\ell, \tau''_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game $(\ell-1)$-4.

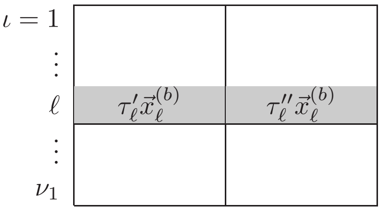
Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game $(\ell-1)$-4



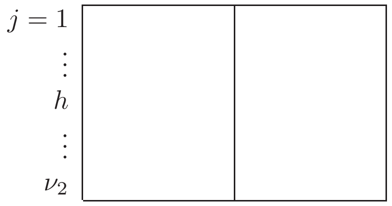
Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game $(\ell-1)$-4



Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game ℓ-1 (= Game ℓ-2-0-4)


$\iota = 1$
$\vdots$
ℓ
$\vdots$
ν_1
$\tau'_\ell \vec{x}_\ell^{(b)}$
$\tau''_\ell \vec{x}_\ell^{(b)}$

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game ℓ-1 (= Game ℓ-2-0-4)

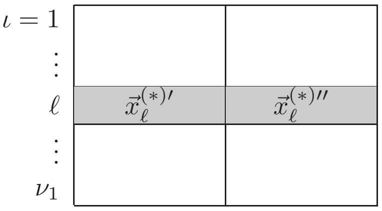


Game $\boldsymbol{\ell}$-2-$\boldsymbol{h}$-1 ($\boldsymbol{\ell = 1, \ldots, \nu_1;\ h = 1, \ldots, \nu_2}$) : Game ℓ-2-0-4 is Game ℓ-1. Game ℓ-2-h-1 is the same as Game ℓ-2-$(h-1)$-4 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

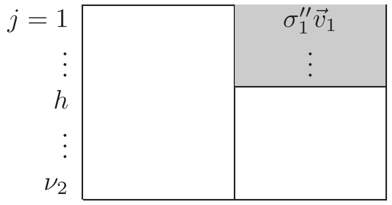
$$\boldsymbol{f}_\ell := (\ \tau_\ell \vec{x}_\ell^{(b)},\ \boxed{\tau'_\ell \vec{x}_\ell^{(b)}},\ \boxed{\tau''_{\ell,0} \vec{x}_\ell^{(0)} + \tau''_{\ell,1} \vec{x}_\ell^{(1)}},\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}},$$

where $\tau''_{\ell,0}, \tau''_{\ell,1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game ℓ-2-$(h-1)$-4. Here, a part framed by a box (resp. dashed box) indicates coefficients which were changed from the previous game when $h \geq 2$ (resp. $h = 1$).

Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game ℓ-2-$(h-1)$-4 for $h \geq 2$

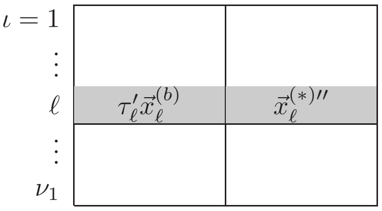


Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game ℓ-2-$(h-1)$-4 for $h \geq 2$

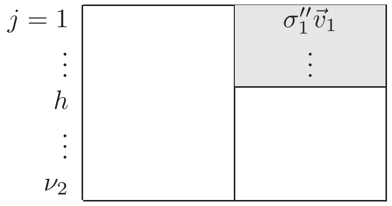


where $\vec{x}_\ell^{(*)\prime} := \tau'_{\ell,0} \vec{x}_\ell^{(0)} + \tau'_{\ell,1} \vec{x}_\ell^{(1)}$, $\vec{x}_\ell^{(*)\prime\prime} := \tau''_{\ell,0} \vec{x}_\ell^{(0)} + \tau''_{\ell,1} \vec{x}_\ell^{(1)}$ (unbiased form).

Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game ℓ-2-h-1


$\iota = 1$
$\vdots$
ℓ
$\vdots$
ν_1
$\tau'_\ell \vec{x}_\ell^{(b)}$
$\vec{x}_\ell^{(*)\prime\prime}$

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game ℓ-2-h-1



where $\vec{x}_\ell^{(*)\prime\prime} := \tau''_{\ell,0} \vec{x}_\ell^{(0)} + \tau''_{\ell,1} \vec{x}_\ell^{(1)}$ (unbiased form).

Game $\boldsymbol{\ell}$-2-$\boldsymbol{h}$-2 ($\boldsymbol{\ell = 1, \ldots, \nu_1;\ h = 1, \ldots, \nu_2}$) : Game ℓ-2-h-2 is the same as Game ℓ-2-h-1 except that the reply to the h-th token query for $\vec{v}_h$ is:

$$\boldsymbol{k}_h^* := (\ \sigma_h \vec{v}_h,\ \boxed{\sigma'_h \vec{v}_h},\ 0^n,\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*},$$

where $\sigma'_h \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game ℓ-2-h-1.

Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game ℓ-2-h-2

$\iota = 1$		
$\vdots$		
ℓ	$\tau'_\ell \vec{x}_\ell^{(b)}$	$\vec{x}_\ell^{(*)''}$
$\vdots$		
ν_1		

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game ℓ-2-h-2

$j = 1$		$\sigma''_1 \vec{v}_1$
$\vdots$		$\vdots$
h	$\sigma'_h \vec{v}_h$	
$\vdots$		
ν_2		

where $\vec{x}_\ell^{(*)''} := \tau''_{\ell,0}\vec{x}_\ell^{(0)} + \tau''_{\ell,1}\vec{x}_\ell^{(1)}$ (unbiased form).

Game $\boldsymbol{\ell}$-2-$\boldsymbol{h}$-3 ($\boldsymbol{\ell = 1, \ldots, \nu_1;\ h = 1, \ldots, \nu_2}$) : Game ℓ-2-h-3 is the same as Game ℓ-2-h-2 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\boldsymbol{f}_\ell := (\ \tau_\ell \vec{x}_\ell^{(b)},\ \boxed{\tau'_{\ell,0}\vec{x}_\ell^{(0)} + \tau'_{\ell,1}\vec{x}_\ell^{(1)}},\ \boxed{\tau''_{\ell,0}\vec{x}_\ell^{(0)} + \tau''_{\ell,1}\vec{x}_\ell^{(1)}},\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}},$$

where $\tau'_{\ell,0}, \tau'_{\ell,1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game ℓ-2-h-2.

Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game ℓ-2-h-3

$\iota = 1$		
$\vdots$		
ℓ	$\vec{x}_\ell^{(*)'}$	$\vec{x}_\ell^{(*)''}$
$\vdots$		
ν_1		

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game ℓ-2-h-3

$j = 1$		$\sigma''_1 \vec{v}_1$
$\vdots$		$\vdots$
h	$\sigma'_h \vec{v}_h$	
$\vdots$		
ν_2		

where $\vec{x}_\ell^{(*)'} := \tau'_{\ell,0}\vec{x}_\ell^{(0)} + \tau'_{\ell,1}\vec{x}_\ell^{(1)}$, $\vec{x}_\ell^{(*)''} := \tau''_{\ell,0}\vec{x}_\ell^{(0)} + \tau''_{\ell,1}\vec{x}_\ell^{(1)}$ (unbiased form).

Game $\boldsymbol{\ell}$-2-$\boldsymbol{h}$-4 ($\boldsymbol{\ell = 1, \ldots, \nu_1;\ h = 1, \ldots, \nu_2}$) : Game ℓ-2-h-4 is the same as Game ℓ-2-h-3 except that the reply to the h-th token query for $\vec{v}_h$ is:

$$\boldsymbol{k}_h^* := (\ \sigma_h \vec{v}_h,\ \boxed{0^n},\ \boxed{\sigma''_h \vec{v}_h},\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*},$$

where $\sigma''_h \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game ℓ-2-h-3.

Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game ℓ-2-h-4

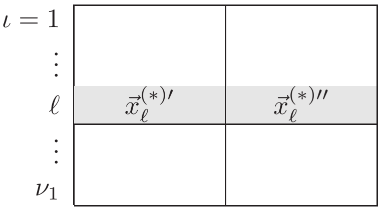
$\iota = 1$		
$\vdots$		
ℓ	$\vec{x}_\ell^{(*)'}$	$\vec{x}_\ell^{(*)''}$
$\vdots$		
ν_1		

Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game ℓ-2-h-4

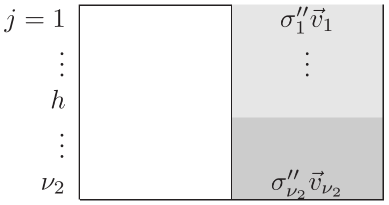
$j = 1$		$\sigma''_1 \vec{v}_1$
$\vdots$		$\vdots$
h		$\sigma''_h \vec{v}_h$
$\vdots$		
ν_2		

where $\vec{x}_\ell^{(*)\prime} := \tau'_{\ell,0}\vec{x}_\ell^{(0)} + \tau'_{\ell,1}\vec{x}_\ell^{(1)}$, $\vec{x}_\ell^{(*)\prime\prime} := \tau''_{\ell,0}\vec{x}_\ell^{(0)} + \tau''_{\ell,1}\vec{x}_\ell^{(1)}$ (unbiased form).

Coefficients of the hidden part of $\boldsymbol{f}_\iota$ in Game ℓ-2-ν_2-4



Coefficients of the hidden part of $\boldsymbol{k}_j^*$ in Game ℓ-2-ν_2-4



where $\vec{x}_\ell^{(*)\prime} := \tau'_{\ell,0}\vec{x}_\ell^{(0)} + \tau'_{\ell,1}\vec{x}_\ell^{(1)}$, $\vec{x}_\ell^{(*)\prime\prime} := \tau''_{\ell,0}\vec{x}_\ell^{(0)} + \tau''_{\ell,1}\vec{x}_\ell^{(1)}$ (unbiased form).

Game $\boldsymbol{\ell}$-3 ($\boldsymbol{\ell = 1, \ldots, \nu_1}$) : Game ℓ-3 is the same as Game ℓ-2-ν_2-4 except that except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\boldsymbol{f}_\ell := (\ \boxed{\tau_{\ell,0}\vec{x}^{(0)} + \tau_{\ell,1}\vec{x}^{(1)}},\ \tau'_{\ell,0}\vec{x}^{(0)} + \tau'_{\ell,1}\vec{x}_\ell^{(1)},\ \tau''_{\ell,0}\vec{x}_\ell^{(0)} + \tau''_{\ell,1}\vec{x}_\ell^{(1)},\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}},$$

where $\tau_{\ell,0}, \tau_{\ell,1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game ℓ-2-ν_2-4.

Game $\boldsymbol{\ell}$-4 ($\boldsymbol{\ell = 1, \ldots, \nu_1}$) : Game ℓ-4 is the same as Game ℓ-3 except that, for all $j = 1, \ldots, \nu_2$, the j-th token query for $\vec{v}_j$ is:

$$\boldsymbol{k}_j^* := (\ \sigma_j\vec{v}_j,\ 0^n,\ \boxed{0^n},\ 0^n,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*} \quad \text{for } j = 1, \ldots, \nu_2,$$

The reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\boldsymbol{f}_\ell := (\ \tau_{\ell,0}\vec{x}_\ell^{(0)} + \tau_{\ell,1}\vec{x}_\ell^{(1)},\ \boxed{0^n},\ \boxed{0^n},\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}},$$

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

Note that at the final game, Game ν_1-4, all challenge ciphertexts are independent from bit $b \xleftarrow{\mathsf{U}} \{0, 1\}$.

We note This game hopping is very similar to that used in [20] for the basic IPE scheme. Therefore, we can evaluate the gaps between pairs of neighboring games in a similar way to that in [20]. □

B.3 Proof of Lemma 3

Lemma 3. *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisPKG}}(\lambda)$ is negligible under the DLIN assumption.*

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

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DisPKG}}(\lambda) \le \sum_{\ell=1}^{\nu_1} \mathsf{Adv}_{\mathcal{E}_{1\text{-}\ell}}^{\mathsf{DLIN}}(\lambda) + \sum_{h=1}^{\nu_2} \mathsf{Adv}_{\mathcal{E}_{2\text{-}h}}^{\mathsf{DLIN}}(\lambda) + \epsilon,$$

where $\mathcal{E}_{1\text{-}\ell}(\cdot) := \mathcal{E}_1(\ell, \cdot), \mathcal{E}_{2\text{-}h}(\cdot) := \mathcal{E}_2(h, \cdot)$, ν_1 (resp. ν_2) is the maximum number of $\mathcal{A}$'s challenge ciphertext (resp. key) queries and $\epsilon := 6(\nu_1 + \nu_2)/q$.

Let ν_1 be the maximum number of $\mathcal{A}$'s challenge ciphertext queries and ν_2 the maximum number of $\mathcal{A}$'s challenge token queries. To prove Lemma 3, we consider the following $2\nu_1+2\nu_2+1$ games. In Game 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0 : For all $j = 1, \ldots, \nu_2$, the reply to the j-th token query for vectors $(\vec{v}_j^{(0)}, \vec{v}_j^{(1)})$ is:

$$\boldsymbol{k}_j^* := (\ \boxed{\sigma_j \vec{v}_j^{(b)}},\ \boxed{0^n},\ 0^n,\ 0^n,\ \vec{\eta}_j,\ 0^n\ )_{\mathbb{B}^*},$$

where $b \xleftarrow{\mathsf{U}} \{0,1\}, \sigma_j \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\eta}_j \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$. For all $\iota = 1, \ldots, \nu_1$, the reply to the ι-th ciphertext query for vectors $(\vec{x}_\iota^{(0)}, \vec{x}_\iota^{(1)})$ is:

$$\boldsymbol{f}_\iota := (\ \boxed{\tau_\iota \vec{x}_\iota^{(b)}},\ \boxed{0^n},\ 0^n,\ 0^n,\ 0^n,\ \vec{\xi}_\iota\ )_{\mathbb{D}},$$

where $\tau_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\xi}_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$.

Game 1-$\boldsymbol{\ell}$-1 ($\boldsymbol{\ell = 1, \ldots, \nu_1}$) : Game 1-0-2 is Game 0. Game 1-ℓ-1 is the same as Game 1-$(\ell-1)$-2 except that the reply to the ℓ-th ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\boldsymbol{f}_\ell := (\ \tau_\ell \vec{x}_\ell^{(b)},\ \boxed{\tau'_\ell \vec{x}_\ell^{(b)}},\ 0^n,\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}},$$

where $\tau'_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 1-$(\ell-1)$-2.

Game 1-$\boldsymbol{\ell}$-2 ($\boldsymbol{\ell = 1, \ldots, \nu_1}$) : Game 1-$\ell$-2 is the same as Game 1-ℓ-1 except that the reply to a ciphertext query for vectors $(\vec{x}_\ell^{(0)}, \vec{x}_\ell^{(1)})$ is:

$$\boldsymbol{f}_\ell := (\ \boxed{\vec{r}_{\ell,1}},\ \boxed{\vec{r}_{\ell,2}},\ 0^n,\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}},$$

where $\vec{r}_{\ell,1}, \vec{r}_{\ell,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 1-ℓ-1.

Game 2-$\boldsymbol{h}$-1 ($\boldsymbol{h = 1, \ldots, \nu_2}$) : Game 2-0-2 is Game 1-ν_1-2. Game 2-h-1 is the same as Game 2-$(h-1)$-2 except that the reply to the h-th token query for $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ is:

$$\boldsymbol{k}_h^* := (\ \sigma_h \vec{v}_h^{(b)},\ \boxed{\sigma'_h \vec{v}_h^{(b)}},\ 0^n,\ 0^n,\ \vec{\eta}_h,\ 0^n\ )_{\mathbb{B}^*},$$

where $\sigma'_h \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-$(h-1)$-2.

Game 2-$\boldsymbol{h}$-2 ($\boldsymbol{h = 1, \ldots, \nu_2}$) : Game 2-$h$-2 is the same as Game 2-h-1 except that the reply to the h-th token query for $(\vec{v}_h^{(0)}, \vec{v}_h^{(1)})$ is:

$$\boldsymbol{k}^* := (\ \boxed{\vec{w}_{h,1}},\ \boxed{\vec{w}_{h,2}},\ 0^n,\ 0^n,\ \vec{\eta},\ 0^n\ )_{\mathbb{B}^*},$$

where $\vec{w}_{h,1}, \vec{w}_{h,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 2-h-1.

Note that at the final game, Game 2-ν_2-2, all challenge ciphertexts and keys are independent from bit $b \xleftarrow{\mathsf{U}} \{0,1\}$.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}\iota)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}\iota)}(\lambda)$ for $\iota = 1, 2$ be the advantage of $\mathcal{A}$ in Game 0, 1-ℓ-ι, 2-h-ι, respectively. We will show four lemmas that evaluate the gaps between pairs of neighboring games. From these lemmas and Lemma 5, we obtain $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) \le \sum_{\ell=1}^{\nu_1} \left(\left| \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}(\ell-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}1)}(\lambda) \right| + \left| \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}2)}(\lambda) \right| \right) + \sum_{h=1}^{\nu_2} \left(\left| \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) \right| + \left| \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda) \right| \right) \le \sum_{\ell=1}^{\nu_1} \mathsf{Adv}_{\mathcal{B}_{1\text{-}\ell}}^{\mathsf{P1}}(\lambda) + \sum_{h=1}^{\nu_2} \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P1}}(\lambda) \le \sum_{\ell=1}^{\nu_1} \mathsf{Adv}_{\mathcal{E}_{1\text{-}\ell}}^{\mathsf{DLIN}}(\lambda) + \sum_{h=1}^{\nu_2} \mathsf{Adv}_{\mathcal{E}_{2\text{-}h}}^{\mathsf{DLIN}}(\lambda) + 6(\nu_1 + \nu_2)/q$. □

Lemma 23 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}(\ell-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{1\text{-}\ell}}^{\mathsf{P1}}(\lambda)$, where $\mathcal{B}_{1\text{-}\ell}(\cdot) := \mathcal{B}_1(\ell, \cdot)$.*

Proof. Lemma 23 is proven in a simillar manner to Lemma 12 since $\mathbb{D}$ and $\mathbb{B}^*$ are independent from malicious PKG not in possesion of a conversion matrix W. □

Lemma 24 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}1)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}\ell\text{-}2)}(\lambda)$.*

Proof. We will consider the distribution in Game 1-ℓ-1.

First, we note that since public key $\widehat{\mathbb{D}}$ and (master) secret key $\widehat{\mathbb{B}}^*$ are independent from malicious PKG not in possesion of a conversion matrix W, we only consider vector elements over basis $\mathbb{D}$, here.

We define new (dual orthonormal) bases $(\mathbb{W}, \mathbb{W}^*)$ of DPVS $\mathbb{V}$ below. First, we generate $U_1, U_2 \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q)$, and set

$$\begin{pmatrix} \boldsymbol{w}_1 \\ \vdots \\ \boldsymbol{w}_{2n} \end{pmatrix} := \begin{pmatrix} I_n & 0_n \\ U_1 & U_2 \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{d}_1 \\ \vdots \\ \boldsymbol{d}_{2n} \end{pmatrix}, \text{ i.e., } \begin{array}{c} \boldsymbol{w}_i := \boldsymbol{d}_i,\ \boldsymbol{w}_{n+i} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{d}_1, \ldots, \boldsymbol{d}_{2n} \rangle \\ \text{for } i = 1, \ldots, n, \\ \text{except for negligible probability,} \end{array}$$

$$\mathbb{W} := (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n, \boldsymbol{w}_{n+1}, \ldots, \boldsymbol{w}_{2n}, \boldsymbol{d}_{2n+1}, \ldots, \boldsymbol{d}_{6n}).$$

Since ℓ-th queried $\vec{x}_\ell^{(b)} \neq \vec{0}$ and $\boldsymbol{w}_{n+i} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{d}_1, \ldots, \boldsymbol{d}_{2n} \rangle$ for $i = 1, \ldots, n$,

$$\boldsymbol{f}_\ell := (\ \tau_\ell \vec{x}_\ell^{(b)},\ \tau'_\ell \vec{x}_\ell^{(b)},\ 0^n,\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{D}} = (\ \vec{r}_{\ell,1},\ \vec{r}_{\ell,2},\ 0^n,\ 0^n,\ 0^n,\ \vec{\xi}_\ell\ )_{\mathbb{W}},$$

where $\vec{r}_{\ell,1}, \vec{r}_{\ell,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$.

In the light of the adversary's view, $\mathbb{W}$ is consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$. Therefore, the view of $\mathcal{A}$ in Game 1-ℓ-1 can be conceptually changed to that in Game 1-ℓ-2. □

Lemma 25 *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, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P1}}(\lambda)$, where $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.*

Proof. Lemma 25 is proven in a simillar manner to Lemma 12 since $\mathbb{D}$ and $\mathbb{B}^*$ are independent from malicious PKG not in possesion of a conversion matrix W. □

Lemma 26 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)$.*

Lemma 26 is proven in a similar manner to Lemma 24.