Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption*

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

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

November 5, 2010

Abstract

This paper presents a fully secure functional encryption scheme for a wide class of relations, that are specified by non-monotone access structures combined with inner-product relations. The security is proven under a standard assumption, the decisional linear (DLIN) assumption, in the standard model. The proposed functional encryption scheme covers, as special cases, (1) key-policy and ciphertext-policy attribute-based encryption with non-monotone access structures, and (2) (hierarchical) predicate encryption with inner-product relations and functional encryption with non-zero inner-product relations.

*An extended abstract was presented at Advances in Cryptology – CRYPTO 2010, LNCS 6223, pages 191-208. This is the full paper.

Contents

1 Introduction

1.1 Background

Although numerous encryption systems have been developed over several thousand years, any traditional encryption system before the 1970's had a great restriction on the relation between a ciphertext encrypted by an encryption-key and the decryption-key such that these keys should be equivalent. The innovative notion of public-key cryptosystems in the 1970's relaxed this restriction, where these keys differ and the encryption-key can be published.

Recently, a new innovative class of encryption systems, *functional encryption* (FE), has been extensively studied. FE provides more sophisticated and flexible relations between the keys where a secret key, sk_Ψ, is associated with a parameter, Ψ, and message m is encrypted to a ciphertext $\mathsf{Enc}(m, \mathsf{pk}, \Upsilon)$ using system public key pk along with another parameter Υ. Ciphertext $\mathsf{Enc}(m, \mathsf{pk}, \Upsilon)$ can be decrypted by secret sk_Ψ if and only if a relation $R(\Psi, \Upsilon)$ holds. FE has various applications in the areas of access control for databases, mail services, and contents distribution [2, 7, 9, 16, 17, 22, 23, 24, 25, 27].

When R is the simplest relation or equality relation, i.e., $R(\Psi, \Upsilon)$ holds iff $\Psi = \Upsilon$, it is *identity-based encryption* (IBE) [3, 4, 5, 6, 10, 12, 13, 15].

As a more general class of FE, *attribute-based encryption* (ABE) schemes have been proposed [2, 7, 9, 16, 17, 22, 23, 24, 25, 27], where either one of the parameters for encryption and secret key is a tuple of attributes, and the other is an access structure or (monotone) span program along with a tuple of attributes, e.g., Υ is a general access structure $(\hat{M}, (v_1, \ldots, v_i))$ (or a tuple of attributes $(x_1, \ldots, x_i)$, resp.) for encryption and $\Psi := (x_1, \ldots, x_i)$ (or $\Psi := (\hat{M}, (v_1, \ldots, v_i))$, resp.) for a secret key. Here, some elements of the tuple may be empty. $R(\Psi, \Upsilon)$ holds iff the truth-value vector of $(\mathsf{T}(x_1 = v_1), \ldots, \mathsf{T}(x_i = v_i))$ is accepted by $\hat{M}$, where $\mathsf{T}(\psi) := 1$ if ψ is true, and $\mathsf{T}(\psi) := 0$ if ψ is false (For example, $\mathsf{T}(x = v) := 1$ if $x = v$, and $\mathsf{T}(x = v) := 0$ if $x \neq v$).

If Ψ is $(\hat{M}, (v_1, \ldots, v_i))$ for a secret key, it is called key-policy ABE (KP-ABE). If Υ $(\hat{M}, (v_1, \ldots, v_i))$ for encryption, it is ciphertext-policy ABE (CP-ABE).

Inner-product encryption (IPE) [17] is also a class of FE, where each parameter for encryption and secret key is a vector over a field or ring (e.g., $\overrightarrow{x} := (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ and $\overrightarrow{v} := (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ for encryption and secret key, respectively), and $R(\overrightarrow{x}, \overrightarrow{v})$ holds iff $\overrightarrow{x} \cdot \overrightarrow{v} = 0$, where $\overrightarrow{x} \cdot \overrightarrow{v}$ is the inner-product of $\overrightarrow{x}$ and $\overrightarrow{v}$. The inner-product relation represents a wide class of relations including equality, conjunction and disjunction (more generally, CNF and DNF) of equality relations and polynomial relations.

There are two types of secrecy in FE, *attribute-hiding* and *payload-hiding* [17]. Roughly speaking, attribute-hiding requires that a ciphertext conceal the associated attribute as well as the plaintext, while payload-hiding only requires that a ciphertext conceal the plaintext. Attribute-hiding FE is called *predicate encryption* (PE) [17]. *Anonymous* IBE and *hidden-vector encryption* (HVE) [9] are a class of PE and covered by predicate IPE, or PE with inner-product relations.

Although many ABE and IPE schemes have been presented over the last several years, no adaptively-secure (or fully-secure) scheme has been proposed in the standard model except [18]. The ABE scheme in [18] supports monotone access structures with equality relations and is secure under non-standard assumptions over composite order pairing groups. The IPE scheme

in [18] supports inner-product relations and is secure under a non-standard assumption, whose size depends on some parameter that is not the security parameter.

No adaptively-secure (or fully-secure) ABE (even for monotone access structures) or IPE scheme has been proposed under a standard assumption in the standard model, and no adaptively-secure (or fully-secure) ABE scheme with *non-monotone* access structures has been proposed (even under non-standard assumptions) in the standard model. In addition, to the best of our knowledge, no FE scheme (even with selective security) has been presented that supports more general relations than those for ABE, i.e., access structures with equality relations, and those for IPE, i.e., inner-product relations.

1.2 Our Result

- This paper proposes an adaptively secure functional encryption (FE) scheme for a wide class of relations, that are specified by non-monotone access structures combined with inner-product relations. More precisely, either one of the parameters for encryption and a secret key is a tuple of attribute vectors and the other is a non-monotone access structure or span program $\hat{M} := (M, \rho)$ along with a tuple of attribute vectors, e.g., $\Upsilon := (\overrightarrow{x}_1, \ldots, \overrightarrow{x}_i) \in \mathbb{F}_q^{n_1+\cdots+n_i}$ for encryption, and $\Psi := (\hat{M}, (\overrightarrow{v}_1, \ldots, \overrightarrow{v}_i) \in \mathbb{F}_q^{n_1+\cdots+n_i})$ for a secret key. The component-wise inner-product relations for attribute vector components, e.g., $\{\overrightarrow{x}_t \cdot \overrightarrow{v}_t = 0 \text{ or not }\}_{t\in\{1,\ldots,i\}}$, are input to span program $\hat{M}$, and $R(\Psi, \Upsilon)$ holds iff the truth-value vector of $(\mathsf{T}(\overrightarrow{x}_1 \cdot \overrightarrow{v}_1 = 0), \ldots, \mathsf{T}(\overrightarrow{x}_i \cdot \overrightarrow{v}_i = 0))$ is accepted by span program $\hat{M}$.

  Similarly to ABE, we propose two types of FE schemes, the KP-FE and CP-FE schemes.

  Note that in Section 6, parameter x for encryption is expressed by $\Gamma := \{(t, \overrightarrow{x}_t) \mid 1 \leq t \leq d\}$ in place of a tuple of vectors $(\overrightarrow{x}_1, \ldots, \overrightarrow{x}_i)$, where $1 \leq t \leq d$ means that t is an element of some subset of $\{1, \ldots, d\}$, and parameter Ψ for the secret key is expressed by $\mathbb{S} := (M, \rho)$ (not by $\hat{M} := (M, \rho)$ along with $(\overrightarrow{v}_1, \ldots, \overrightarrow{v}_i)$ as described above), where ρ in $\mathbb{S}$ is abused as ρ in $\hat{M}$ combined with $(\overrightarrow{v}_1, \ldots, \overrightarrow{v}_i)$ (see Definition 4).

  Since the class of relations supported by the proposed FE scheme is more general than that for ABE and IPE, the proposed FE scheme includes the following schemes as special cases:

  1. The (KP and CP)-ABE schemes for non-monotone access structures with equality relations. Here, the underlying attribute vectors of the FE scheme, $\{\overrightarrow{x}_t\}_{t\in\{1,\ldots,d\}}$ and $\{\overrightarrow{v}_t\}_{t\in\{1,\ldots,d\}}$, are specialized to two-dimensional vectors for the equality relation, e.g., $\overrightarrow{x}_t := (1, x_t)$ and $\overrightarrow{v}_t := (v_t, -1)$, where $\overrightarrow{x}_t \cdot \overrightarrow{v}_t = 0$ iff $x_t = v_t$ (see Section G).
  2. The IPE and non-zero-IPE schemes, where a non-zero-IPE scheme is a class of FE with $R(\overrightarrow{x}, \overrightarrow{v})$ iff $\overrightarrow{x} \cdot \overrightarrow{v} \neq 0$. Here, the underlying access structure $\mathbb{S}$ of the FE scheme is specialized to the 1-out-of-1 secret sharing. The IPE scheme is 'attribute-hiding,' i.e., it is the PE scheme for the inner-product relations.

     In addition, if the underlying access structure is specialized to the d-out-of-d secret sharing, our FE scheme can be specialized to a *hierarchical* zero/non-zero IPE scheme by adding delegation and rerandomization mechanisms.

- The proposed FE scheme with such a wide class of relations is proven to be *adaptively secure* (adaptively payload-hiding against CPA) under a standard assumption, the *decisional linear (DLIN)* assumption (over prime order pairing groups), in the standard model.

Note that even for FE with the simplest relations or the equality relations, i.e., IBE, only a few IBE schemes are known to be adaptively secure under standard assumptions; the Waters IBE scheme [26] under the DBDH assumption, and the Waters IBE scheme [28] under the DBDH and DLIN assumptions.

- To prove the security, this paper elaborately combines the dual system encryption methodology proposed by Waters [28] and the concept of dual pairing vector spaces (DPVS) proposed by Okamoto and Takashima [20, 21], in a manner similar to that in [18]. See Section 2 for the concept and actual construction of DPVS.

  This paper also develops a new technique to prove the security based on the DLIN assumption. This provides a new methodology of employing a simple assumption defined on primitive groups to prove a complicated scheme that is designed on a higher level concept, DPVS.

  In our methodology, the top level of the security proof (based on the dual system encryption methodology) directly employs only top level assumptions (assumptions by Problems 1 and 2), that are defined on DPVS. The methodology bridges the top level assumptions and the primitive one, the DLIN assumption, in a hierarchical manner, where several levels of assumptions are constructed hierarchically. Such a modular way of proof greatly clarifies the logic of a complicated security proof.

- The efficiency of the proposed FE scheme is comparable to that of the existing ABE and IPE schemes. For example, if the proposed FE scheme is specialized to the IPE scheme, the key and ciphertext sizes are $(3n + 6) \cdot |G|$, while they are $(2n + 3) \cdot |G|$ for the IPE scheme in [18], where n is the dimension of the attribute vectors, and $|G|$ denotes the size of an element of prime order pairing group $\mathbb{G}$, e.g., 256 bits.

- It is easy to convert the (CPA-secure) proposed FE scheme to a CCA-secure FE scheme by employing an existing general conversion such as that by Canetti, Halevi and Katz [11] or that by Boneh and Katz [8] (using additional 7-dimensional dual spaces $(\mathbb{B}_{d+1}, \mathbb{B}^*_{d+1})$ with $n_{d+1} := 2$ on the proposed FE scheme, and a strongly unforgeable one-time signature scheme or message authentication code with encapsulation). That is, we can present a *fully secure* (adaptively payload-hiding against CCA) FE scheme for the same class of relations in the *standard model* under the DLIN assumption as well as a strongly unforgeable one-time signature scheme or message authentication code with encapsulation (see Section 8).

1.3 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. $y := z$ denotes that y is set, defined or substituted by z. When a is a fixed value, $A(x) \to a$ (e.g., $A(x) \to 1$) denotes the event that machine (algorithm) A outputs a on input x. A function $f : \mathbb{N} \to \mathbb{R}$ is *negligible* in λ, if for every constant $c > 0$, there exists an integer n such that $f(\lambda) < \lambda^{-c}$ for all $\lambda > n$.

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., $\overrightarrow{x}$ denotes $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. For two vectors $\overrightarrow{x} = (x_1, \ldots, x_n)$ and $\overrightarrow{v} = (v_1, \ldots, v_n)$, $\overrightarrow{x} \cdot \overrightarrow{v}$ denotes the inner-product $\sum_{i=1}^n x_i v_i$. The vector $\overrightarrow{0}$ 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. $\mathsf{span}\langle \overrightarrow{x}_1, \ldots, \overrightarrow{x}_n \rangle$) denotes the subspace generated by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ (resp. $\overrightarrow{x}_1, \ldots, \overrightarrow{x}_n$). For vectors $\overrightarrow{x} := (x_1, \ldots, x_N)$, $\overrightarrow{y} := (y_1, \ldots, y_N) \in \mathbb{F}_q^N$ and bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N), \mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$, $(\overrightarrow{x})_{\mathbb{B}}$ $(= (x_1, \ldots, x_N)_{\mathbb{B}})$ denotes linear combination $\sum_{i=1}^N x_i \boldsymbol{b}_i$, and $(\overrightarrow{y})_{\mathbb{B}^*}$ $(= (y_1, \ldots, y_N)_{\mathbb{B}^*})$ denotes $\sum_{i=1}^N y_i \boldsymbol{b}_i^*$. For a format of attribute vectors $\overrightarrow{n} := (d; n_1, \ldots, n_d)$ that indicates dimensions of vector spaces, $\overrightarrow{e}_{t,j}$ denotes the canonical basis vector $(\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n_t - j}) \in \mathbb{F}_q^{n_t}$ for $t = 1, \ldots, d$ and $j = 1, \ldots, n_t$.

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

Definition 1 *"Symmetric bilinear pairing groups"* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *are a tuple of a prime* q*, cyclic additive group* $\mathbb{G}$ *and multiplicative group* $\mathbb{G}_T$ *of order* q*,* $G \neq 0 \in \mathbb{G}$*, and a polynomial-time computable nondegenerate bilinear pairing* $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ *i.e.,* $e(sG, tG) = e(G, G)^{st}$ *and* $e(G, G) \neq 1$*.*

Let $\mathcal{G}_{\mathsf{bpg}}$ *be an algorithm that takes input* 1^λ *and outputs a description of bilinear pairing groups* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *with security parameter* λ*.*

In this paper, we concentrate on the symmetric version of dual pairing vector spaces [20, 21] constructed using symmetric bilinear pairing groups given in Definition 1.

Definition 2 *"Dual pairing vector spaces (DPVS)"* $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ *by a direct product of symmetric pairing groups* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *are a tuple of prime* q*,* N*-dimensional vector space* $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$ *over* $\mathbb{F}_q$*, cyclic group* $\mathbb{G}_T$ *of order* q*, canonical basis* $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$ *of* $\mathbb{V}$*, where* $\boldsymbol{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G, \overbrace{0, \ldots, 0}^{N-i})$*, and pairing* $e : \mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$*.*

The pairing is defined by $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^N e(G_i, H_i) \in \mathbb{G}_T$ *where* $\boldsymbol{x} := (G_1, \ldots, G_N) \in \mathbb{V}$ *and* $\boldsymbol{y} := (H_1, \ldots, H_N) \in \mathbb{V}$*. This is nondegenerate bilinear i.e.,* $e(s\boldsymbol{x}, t\boldsymbol{y}) = e(\boldsymbol{x}, \boldsymbol{y})^{st}$ *and if* $e(\boldsymbol{x}, \boldsymbol{y}) = 1$ *for all* $\boldsymbol{y} \in \mathbb{V}$*, then* $\boldsymbol{x} = \boldsymbol{0}$*. For all* i *and* j*,* $e(\boldsymbol{a}_i, \boldsymbol{a}_j) = e(G, G)^{\delta_{i,j}}$ *where* $\delta_{i,j} = 1$ *if* $i = j$*, and* 0 *otherwise, and* $e(G, G) \neq 1 \in \mathbb{G}_T$*.*

DPVS also has linear transformations $\phi_{i,j}$ *on* $\mathbb{V}$ *s.t.* $\phi_{i,j}(\boldsymbol{a}_j) = \boldsymbol{a}_i$ *and* $\phi_{i,j}(\boldsymbol{a}_k) = \boldsymbol{0}$ *if* $k \neq j$*, which can be easily achieved by* $\phi_{i,j}(\boldsymbol{x}) := (\overbrace{0, \ldots, 0}^{i-1}, G_j, \overbrace{0, \ldots, 0}^{N-i})$ *where* $\boldsymbol{x} := (G_1, \ldots, G_N)$*. We call* $\phi_{i,j}$ *"distortion maps".*

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 using* $\mathcal{G}_{\mathsf{bpg}}$*.*

For the asymmetric version of DPVS, $(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*, e)$, see Appendix A.2. The above symmetric version is obtained by identifying $\mathbb{V} = \mathbb{V}^*$ and $\mathbb{A} = \mathbb{A}^*$ in the asymmetric version.

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

$$
\begin{aligned}
&\mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n} := (d; n_1, \ldots, n_d)) : \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \quad \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \\
&\quad N_0 := 5, \quad N_t := 3n_t + 1 \ \text{ for } t = 1, \ldots, d, \\
&\quad \text{for } t = 0, \ldots, d, \\
&\qquad \mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t, \mathsf{param}_{\mathbb{G}}),
\end{aligned}
$$

$$X_t := \begin{pmatrix} \overrightarrow{\chi}_{t,1} \\ \vdots \\ \overrightarrow{\chi}_{t,N_t} \end{pmatrix} := (\chi_{t,i,j})_{i,j} \xleftarrow{\cup} GL(N_t, \mathbb{F}_q), \quad \begin{pmatrix} \overrightarrow{\vartheta}_{t,1} \\ \vdots \\ \overrightarrow{\vartheta}_{t,N_t} \end{pmatrix} := (\vartheta_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1},$$

$$\boldsymbol{b}_{t,i} := (\overrightarrow{\chi}_{t,i})_{\mathbb{A}_t} = \textstyle\sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j} \quad \text{for } i = 1, \ldots, N_t, \quad \mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,N_t}),$$

$$\boldsymbol{b}^*_{t,i} := (\overrightarrow{\vartheta}_{t,i})_{\mathbb{A}_t} = \textstyle\sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j} \quad \text{for } i = 1, \ldots, N_t, \quad \mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,N_t}),$$

$$g_T := e(G, G)^{\psi}, \quad \mathsf{param}_{\overrightarrow{n}} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,\ldots,d}, \ g_T)$$

return $(\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d})$.

We note that $g_T = e(\boldsymbol{b}_{t,i}, \boldsymbol{b}^*_{t,i})$ for $t = 0, \ldots, d; i = 1, \ldots, N_t$.

3 Functional Encryption with General Relations

3.1 Span Programs and Non-Monotone Access Structures

Definition 3 (Span Programs [1]) *Let $\{p_1, \ldots, p_n\}$ be a set of variables. A span program over $\mathbb{F}_q$ is a labeled matrix $\hat{M} := (M, \rho)$ where M is a $(\ell \times r)$ matrix over $\mathbb{F}_q$ and ρ is a labeling of the rows of M by literals from $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ (every row is labeled by one literal), i.e., $\rho : \{1, \ldots, \ell\} \to \{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$.*

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

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

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

We assume that the matrix M satisfies the condition: $M_i \neq \overrightarrow{0}$ for $i = 1, \ldots, \ell$.

We now introduce a non-monotone access structure with evaluating map γ by using the inner-product of attribute vectors, that is employed in the proposed functional encryption schemes.

Definition 4 (Inner-Products of Attribute Vectors and Access Structures) *$\mathcal{U}_t$ ($t = 1, \ldots, d$ and $\mathcal{U}_t \subset \{0,1\}^*$) is a sub-universe, a set of attributes, each of which is expressed by a pair of sub-universe id and n_t-dimensional vector, i.e., $(t, \overrightarrow{v})$, where $t \in \{1, \ldots, d\}$ and $\overrightarrow{v} \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}$.*

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

Let Γ be a set of attributes, i.e., $\Gamma := \{(t, \overrightarrow{x}_t) \mid \overrightarrow{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}, 1 \leq t \leq d\}$, where $1 \leq t \leq d$ means that t is an element of some subset of $\{1, \ldots, d\}$.

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

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

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

Definition 5 *A secret-sharing scheme for span program* $\hat{M} := (M, \rho)$ *is:*

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

3.2 Key-Policy Functional Encryption with General Relations

Definition 6 (Key-Policy Functional Encryption : KP-FE) *A key-policy functional encryption scheme consists of four algorithms.*

Setup *This is a randomized algorithm that takes as input security parameter and format* $\overrightarrow{n} := (d; n_1, \ldots, n_d)$ *of attributes. It outputs public parameters* pk *and master secret key* sk*.*

KeyGen *This is a randomized algorithm that takes as input access structure* $\mathbb{S} := (M, \rho)$*,* pk *and* sk*. It outputs a decryption key* $\mathsf{sk}_{\mathbb{S}}$*.*

Enc *This is a randomized algorithm that takes as input message* m*, a set of attributes,* $\Gamma := \{(t, \overrightarrow{x}_t) | \overrightarrow{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}, 1 \leq t \leq d\}$*, and public parameters* pk*. It outputs a ciphertext* ct_Γ*.*

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

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

Definition 7 *The model for proving the adaptively payload-hiding security of KP-FE under chosen plaintext attack is:*

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

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

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

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

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

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

We note that the model can easily be extended to handle chosen-ciphertext attacks (CCA) by allowing for decryption queries in Phases 1 and 2. The advantage of adversary $\mathcal{A}$ *in the CCA game is defined as* $\mathsf{Adv}_\mathcal{A}^{\mathsf{KP\text{-}FE,CCA\text{-}PH}}(\lambda) := \Pr[b' = b] - 1/2$ *for any security parameter* λ*.*

3.3 Ciphertext-Policy Functional Encryption with General Relations

Definition 8 (Ciphertext-Policy Functional Encryption : CP-FE) *A ciphertext-policy functional encryption scheme consists of four algorithms.*

Setup *This is a randomized algorithm that takes as input security parameter and format* $\overrightarrow{n} := (d; n_1, \ldots, n_d)$ *of attributes. It outputs the public parameters* pk *and a master key* sk*.*

KeyGen *This is a randomized algorithm that takes as input a set of attributes,* $\Gamma := \{(t, \overrightarrow{x}_t) | \overrightarrow{x}_t \in \mathbb{F}_q^{n_t}, 1 \leq t \leq d\}$*,* pk *and* sk*. It outputs a decryption key.*

Enc *This is a randomized algorithm that takes as input message* m*, access structure* $\mathbb{S} := (M, \rho)$*, and the public parameters* pk*. It outputs the ciphertext.*

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

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

Definition 9 *The model for proving the adaptively payload-hiding security of CP-FE under chosen plaintext attack is:*

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

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

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

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

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

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

We note that the model can easily be extended to handle chosen-ciphertext attacks (CCA) by allowing for decryption queries in Phase 1 and 2. The advantage of an adversary $\mathcal{A}$ *in the CCA game is defined as* $\mathsf{Adv}^{\mathsf{CP\text{-}FE,CCA\text{-}PH}}_{\mathcal{A}}(\lambda) := \Pr[b' = b] - 1/2$ *for any security parameter* λ*.*

4 Decisional Linear (DLIN) Assumption

Definition 10 (DLIN: Decisional Linear Assumption) *The DLIN problem is to guess* $\beta \in \{0,1\}$*, given* $(\mathsf{param}_{\mathbb{G}},\ G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{DLIN}}_\beta(1^\lambda)$*, where*

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$*. For a probabilistic machine* $\mathcal{E}$*, we define the advantage of* $\mathcal{E}$ *for the DLIN problem as:*

$$\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) := \left|\mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{DLIN}}_0(1^\lambda)\right] - \mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{DLIN}}_1(1^\lambda)\right]\right|.$$

The DLIN assumption is: For any probabilistic polynomial-time adversary $\mathcal{E}$*, the advantage* $\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda)$ *is negligible in* λ*.*

5 Lemmas for the Proofs of Main Theorems

We will show three lemmas for the proof of Theorems 1 and 2.

Definition 11 (Problem 1) *Problem 1 is to guess* β*, given* $(\mathsf{param}_{\overrightarrow{n}}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \overrightarrow{n})$*, where*

$$\begin{aligned}
&\mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \overrightarrow{n}) : \quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),\\
&\quad \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, .., \boldsymbol{b}^*_{0,5}),\ \widehat{\mathbb{B}}^*_t := (\boldsymbol{b}^*_{t,1}, .., \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,2n_t+1}, .., \boldsymbol{b}^*_{t,3n_t+1}) \ \text{ for } t = 1, .., d,\\
&\quad \omega, z_0, \gamma_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{e}_{0,0} := (\omega, 0, 0, 0, \gamma_0)_{\mathbb{B}_0}, \quad \boldsymbol{e}_{1,0} := (\omega, z_0, 0, 0, \gamma_0)_{\mathbb{B}_0},\\
&\quad \text{for } t = 1, \ldots, d;\\
&\qquad \overrightarrow{e}_{t,1} := (1, 0^{n_t-1}) \in \mathbb{F}_q^{n_t},\ \overrightarrow{z}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},\ \gamma_t \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\qquad\qquad\qquad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\ }^{1}\\
&\qquad \boldsymbol{e}_{0,t,1} := \ (\ \omega\overrightarrow{e}_{t,1},\ \ 0^{n_t},\ \ 0^{n_t},\ \ \gamma_t\ )_{\mathbb{B}_t},\\
&\qquad \boldsymbol{e}_{1,t,1} := \ (\ \omega\overrightarrow{e}_{t,1},\ \ \overrightarrow{z}_t,\ \ 0^{n_t},\ \ \gamma_t\ )_{\mathbb{B}_t},\\
&\qquad \boldsymbol{e}_{t,i} := \omega\boldsymbol{b}_{t,i} \ \text{ for } i = 2, \ldots, n_t,\\
&\quad \text{return}\ \ (\mathsf{param}_{\overrightarrow{n}}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t}),
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic machine* $\mathcal{B}$, *we define the advantage of* $\mathcal{B}$ *as the quantity*

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

Lemma 1 *For any adversary* $\mathcal{B}$, *there exist probabilistic machines* $\mathcal{E}$, *whose running times are essentially the same as that of* $\mathcal{B}$, *such that for any security parameter* λ, $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + (d+6)/q$.

Definition 12 (Problem 2) *Problem 2 is to guess* β, *given* $(\mathsf{param}_{\overrightarrow{n}}, \widehat{\mathbb{B}}_0, \mathbb{B}^*_0, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=1,\ldots,n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, \overrightarrow{n})$, *where*

$$\begin{aligned}
&\mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, \overrightarrow{n}): \quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),\\
&\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, .., \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,2n_t+1}, .., \boldsymbol{b}_{t,3n_t+1}) \quad \text{for } t = 1, .., d,\\
&\delta, \delta_0, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \tau, u_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ z_0 := u_0^{-1},\\
&\begin{pmatrix} \overrightarrow{z}_{t,1} \\ \vdots \\ \overrightarrow{z}_{t,n_t} \end{pmatrix} := Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q),\ \begin{pmatrix} \overrightarrow{u}_{t,1} \\ \vdots \\ \overrightarrow{u}_{t,n_t} \end{pmatrix} := (Z_t^{-1})^{\mathrm{T}} \text{ for } t = 1, .., d,\\
&\boldsymbol{h}^*_{0,0} := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}^*_0},\ \boldsymbol{h}^*_{1,0} := (\delta, u_0, 0, \delta_0, 0)_{\mathbb{B}^*_0},\ \boldsymbol{e}_0 := (\omega, \tau z_0, 0, 0, 0)_{\mathbb{B}_0},\\
&\text{for } t = 1, \ldots, d;\ i = 1, \ldots, n_t;\\
&\quad \overrightarrow{e}_{t,i} := (0^{i-1}, 1, 0^{n_t - i}) \in \mathbb{F}_q^{n_t},\quad \overrightarrow{\delta}_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},\\
&\qquad\qquad \overbrace{\phantom{\delta \overrightarrow{e}_{t,i},}}^{n_t}\ \overbrace{\phantom{0^{n_t},}}^{n_t}\ \overbrace{\phantom{\overrightarrow{\delta}_{t,i},}}^{n_t}\ \overbrace{}^{1}\\
&\quad \boldsymbol{h}^*_{0,t,i} := (\ \delta \overrightarrow{e}_{t,i},\ 0^{n_t},\ \overrightarrow{\delta}_{t,i},\ 0\ )_{\mathbb{B}^*_t}\\
&\quad \boldsymbol{h}^*_{1,t,i} := (\ \delta \overrightarrow{e}_{t,i},\ \overrightarrow{u}_{t,i},\ \overrightarrow{\delta}_{t,i},\ 0\ )_{\mathbb{B}^*_t}\\
&\quad \boldsymbol{e}_{t,i} := (\ \omega \overrightarrow{e}_{t,i},\ \tau \overrightarrow{z}_{t,i},\ 0^{n_t},\ 0\ )_{\mathbb{B}_t},\\
&\text{return } (\mathsf{param}_{\overrightarrow{n}}, \widehat{\mathbb{B}}_0, \mathbb{B}^*_0, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}),
\end{aligned}$$

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 11.*

Lemma 2 *For any adversary* $\mathcal{B}$, *there exists a probabilistic machine* $\mathcal{E}$, *whose running time is essentially the same as that of* $\mathcal{B}$, *such that for any security parameter* λ, $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.

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

6 Proposed KP-FE Scheme

6.1 Construction

We define function $\widetilde{\rho} : \{1, \ldots, \ell\} \to \{1, \ldots, d\}$ by $\widetilde{\rho}(i) := t$ if $\rho(i) = (t, \overrightarrow{v})$ or $\rho(i) = \neg(t, \overrightarrow{v})$, where ρ is given in access structure $\mathbb{S} := (M, \rho)$. In the proposed scheme, we assume that $\widetilde{\rho}$ is injective for $\mathbb{S} := (M, \rho)$ with decryption key $\mathsf{sk}_{\mathbb{S}}$. We will show how to relax the restriction in Appendix F.

In the description of the scheme, we assume that input vector, $\overrightarrow{x}_t := (x_{t,1}, \ldots, x_{t,n_t})$, is normalized such that $x_{t,1} := 1$. (If $\overrightarrow{x}_t$ is not normalized, change it to a normalized one by $(1/x_{t,1}) \cdot \overrightarrow{x}_t$, assuming that $x_{t,1}$ is non-zero).

Random dual bases generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n})$ is defined at the end of Section 2. We refer to Section 1.3 for notations on DPVS.

$\mathsf{Setup}(1^\lambda,\ \overrightarrow{n} := (d; n_1, \ldots, n_d)) :\quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),$

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \ \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1})\quad$ for $t = 1, .., d,$

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*),\ \ \widehat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, .., \boldsymbol{b}_{t,n_t}^*, \boldsymbol{b}_{t,2n_t+1}^*, .., \boldsymbol{b}_{t,3n_t}^*)\quad$ for $t = 1, .., d,$

$\mathsf{pk} := (1^\lambda, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d}),\ \ \mathsf{sk} := \{\widehat{\mathbb{B}}_t^*\}_{t=0,\ldots,d},$

return pk, sk.

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (M, \rho)) :$

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

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

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

if $\rho(i) = (t, \overrightarrow{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}),\qquad \theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \ \overrightarrow{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},$

$$\boldsymbol{k}_i^* := \quad (\ \overbrace{s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i}^{n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{\overrightarrow{\eta}_i}^{n_t},\ \overbrace{0}^{1}\ )_{\mathbb{B}_t^*},$$

if $\rho(i) = \neg(t, \overrightarrow{v}_i),\qquad \overrightarrow{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},$

$$\boldsymbol{k}_i^* := \quad (\ \overbrace{s_i \overrightarrow{v}_i}^{n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{\overrightarrow{\eta}_i}^{n_t},\ \overbrace{0}^{1}\ )_{\mathbb{B}_t^*},$$

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

$\mathsf{Enc}(\mathsf{pk},\ m,\ \Gamma := \{(t, \overrightarrow{x}_t := (x_{t,1}, .., x_{t,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}) \mid 1 \le t \le d, x_{t,1} := 1\}) :$

$\omega, \varphi_0, \varphi_t, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $(t, \overrightarrow{x}_t) \in \Gamma,$

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

$$\boldsymbol{c}_t := \quad (\ \overbrace{\omega \overrightarrow{x}_t}^{n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{\varphi_t}^{1}\ )_{\mathbb{B}_t} \quad \text{for } (t, \overrightarrow{x}_t) \in \Gamma,$$

$c_{d+1} := g_T^\zeta m,\ \ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, c_{d+1}).$

return ct_Γ.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*),\ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, c_{d+1})) :$

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \overrightarrow{x}_t)\}$, then compute I and $\{\alpha_i\}_{i\in I}$ such that

$\overrightarrow{1} = \sum_{i\in I} \alpha_i M_i,$ where M_i is the i-th row of $M,$ and

$I \subseteq \{i \in \{1, \ldots, \ell\} \ \mid\ [\rho(i) = (t, \overrightarrow{v}_i)\ \wedge\ (t, \overrightarrow{x}_t) \in \Gamma\ \wedge\ \overrightarrow{v}_i \cdot \overrightarrow{x}_t = 0]$

$\qquad\qquad \vee\ [\rho(i) = \neg(t, \overrightarrow{v}_i)\ \wedge\ (t, \overrightarrow{x}_t) \in \Gamma\ \wedge\ \overrightarrow{v}_i \cdot \overrightarrow{x}_t \neq 0]\ \}.$

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i\in I\ \wedge\ \rho(i)=(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i} \prod_{i\in I\ \wedge\ \rho(i)=\neg(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)}$$

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

[Correctness] If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \overrightarrow{x}_t)\}$,

$$e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \textstyle\prod_{i\in I\ \wedge\ \rho(i)=(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i} \cdot \prod_{i\in I\ \wedge\ \rho(i)=\neg(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)}$$

$$= g_T^{-\delta s_0+\zeta} \prod_{i\in I \ \wedge \ \rho(i)=(t,\overrightarrow{v}_i)} g_T^{\delta\alpha_i s_i} \prod_{i\in I \ \wedge \ \rho(i)=\neg(t,\overrightarrow{v}_i)} g_T^{\delta\alpha_i s_i(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)}$$
$$= g_T^{\delta(-s_0+\sum_{i\in I}\alpha_i s_i)+\zeta} = g_T^{\zeta}.$$

6.2 Security

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

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_1, \mathcal{E}_{2,h}^+, \mathcal{E}_{2,h+1}$ $(h = 0, \ldots, \nu-1)$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KP\text{-}FE,PH}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{h=0}^{\nu-1}\left(\mathsf{Adv}_{\mathcal{E}_{2,h}^+}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{2,h+1}}^{\mathsf{DLIN}}(\lambda)\right) + \epsilon,$$

where ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (2d\nu + 16\nu + d + 7)/q$.

Proof Outline of Theorem 1: At the top level of strategy of the security proof, we follow the dual system encryption methodology proposed by Waters [28]. In the methodology, ciphertexts and secret keys have two forms, *normal* and *semi-functional*. In the proof herein, we also introduce another form called *pre-semi-functional*. The real system uses only normal ciphertexts and normal secret keys, and semi-functional/pre-semi-functional ciphertexts and keys are used only in a sequence of security games for the security proof.

To prove this theorem, we employ Game 0 (original adaptive-security game) through Game 3. In Game 1, the challenge ciphertext is changed to semi-functional. When at most ν secret key queries are issued by an adversary, there are 2ν game changes from Game 1 (Game 2-0), Game 2-0^+, Game 2-1 through Game 2-$(\nu-1)^+$ and Game 2-ν. In Game 2-h, the first h keys are semi-functional while the remaining keys are normal, and the challenge ciphertext is semi-functional. In Game 2-h^+, the first h keys are semi-functional and the $(h+1)$-th key is *pre-semi-functional* while the remaining keys are normal, and the challenge ciphertext is *pre-semi-functional*. The final game with advantage 0 is changed from Game 2-ν. As usual, we prove that the advantage gaps between neighboring games are negligible.

For $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*)$ and $\mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, c_{d+1})$, we focus on $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^* := (\boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*)$ and $\overrightarrow{\boldsymbol{c}}_\Gamma := (\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma})$, and ignore the other part of $\mathsf{sk}_{\mathbb{S}}$ and ct_Γ (and call them secret key and ciphertext, respectively) in this proof outline. In addition, we ignore a negligible factor in the (informal) descriptions of this proof outline. For example, we say "A is bounded by B" when $A \le B + \epsilon(\lambda)$ where $\epsilon(\lambda)$ is negligible in security parameter λ.

A *normal* secret key, $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{norm}}$ (with access structure $\mathbb{S}$), is the correct form of the secret key of the proposed FE scheme, and is expressed by Eq. (1). Similarly, a *normal* ciphertext (with attribute set Γ), $\overrightarrow{\boldsymbol{c}}_\Gamma^{\mathsf{norm}}$, is expressed by Eq. (2). A *semi-functional* secret key, $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{semi}}$, is expressed by Eq. (8), and a *semi-functional* ciphertext, $\overrightarrow{\boldsymbol{c}}_\Gamma^{\mathsf{semi}}$, is expressed by Eqs. (3)-(5). A *pre-semi-functional* secret key, $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{pre\text{-}semi}}$, and *pre-semi-functional* ciphertext, $\overrightarrow{\boldsymbol{c}}_\Gamma^{\mathsf{pre\text{-}semi}}$, are expressed by Eq. (6) and Eqs. (3), (7) and (5), respectively.

To prove that the advantage gap between Games 0 and 1 is bounded by the advantage of Problem 1 (to guess $\beta \in \{0,1\}$), we construct a simulator of the challenger of Game 0 (or 1) (against an adversary $\mathcal{A}$) by using an instance with $\beta \xleftarrow{\mathsf{U}} \{0,1\}$ of Problem 1. We then show that the distribution of the secret keys and challenge ciphertext replied by the simulator is equivalent to those of Game 0 when $\beta = 0$ and those of Game 1 when $\beta = 1$. That is, the advantage of Problem 1 is equivalent to the advantage gap between Games 0 and 1 (Lemma

4). The advantage of Problem 1 is proven to be equivalent to that of the DLIN assumption (Lemma 1).

The advantage gap between Games 2-h and 2-h^+ is similarly shown to be bounded by the advantage of Problem 2 (i.e., advantage of the DLIN assumption) (Lemmas 5 and 2). Here, we introduce *special forms of pre-semi-functional* keys and ciphertexts, $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{spec.pre\text{-}semi}}$ and $\overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{spec.pre\text{-}semi}}$, respectively, such that they are equivalent to pre-semi-functional keys and ciphertexts, $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{pre\text{-}semi}}$ and $\overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{pre\text{-}semi}}$, respectively, except that $w_0 r_0 = a_0 := \sum_{k=1}^{r} g_k$ and $r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ (note that $r_0, w_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{pre\text{-}semi}}$ and $\overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{pre\text{-}semi}}$). These forms of keys and ciphertexts, $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{spec.pre\text{-}semi}}$ and $\overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{spec.pre\text{-}semi}}$, are simulated using Problem 2 with $\beta = 1$. ¿From the definition of these forms, $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{spec.pre\text{-}semi}}$ can decrypt $\overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{spec.pre\text{-}semi}}$ for any Γ when $\mathbb{S}$ accepts Γ, i.e., it is hard for simulator $\mathcal{B}_{2,h}^{+}$ to tell $(\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{spec.pre\text{-}semi}}, \overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{spec.pre\text{-}semi}})$ for Game 2-h^+ from $(\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{norm}}, \overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{semi}})$ for Game 2-h under the assumption of Problem 2. On the other hand, $a_0 (= w_0 r_0)$ is independently distributed from the other variables when $\mathbb{S}$ does not accept Γ (shown in Proof of Claim 1 by using Lemma 3). That is, the joint distribution of $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{pre\text{-}semi}}$ and $\overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{pre\text{-}semi}}$ is equivalent to that of $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{spec.pre\text{-}semi}}$ and $\overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{spec.pre\text{-}semi}}$, when $\mathbb{S}$ does not accept Γ (i.e., $\mathcal{B}_{2,h}^{+}$'s simulation using Problem 2 with $\beta = 1$ is the same distribution as that of Game 2-h^+ from the adversary's view). In other words, w_0 and r_0 in $\overrightarrow{\boldsymbol{k}}_{\mathbb{S}}^{*\,\mathsf{spec.pre\text{-}semi}}$ and $\overrightarrow{\boldsymbol{c}}_{\Gamma}^{\mathsf{spec.pre\text{-}semi}}$ (given by $\mathcal{B}_{2,h}^{+}$'s simulation using Problem 2 with $\beta = 1$) are correlated for the case that $\mathbb{S}$ accepts Γ or for simulator $\mathcal{B}_{2,h}^{+}$'s view, but adversary $\mathcal{A}$ cannot notice the correlation since $\mathcal{A}$'s queries should satisfy the condition that $\mathbb{S}$ does not accept Γ.

The advantage gap between Games 2-h^+ and 2-$(h+1)$ is similarly shown to be bounded by the advantage of Problem 2, i.e., advantage of the DLIN assumption (Lemmas 6 and 2).

Finally we show that Game 2-ν can be conceptually changed to Game 3 (Lemma 7).

Proof of Theorem 1 : To prove Theorem 1, we consider the following $(2\nu + 3)$ games. In Game 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

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

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (-s_0,\ \boxed{0},\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}, \\ \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \quad \boldsymbol{k}_i^* := (s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i,\ \boxed{0^{n_t}},\ \overrightarrow{\eta}_i,\ 0)_{\mathbb{B}_t^*}, \\ \quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \quad \boldsymbol{k}_i^* := (s_i \overrightarrow{v}_i,\ \boxed{0^{n_t}},\ \overrightarrow{\eta}_i,\ 0)_{\mathbb{B}_t^*}, \end{array}\right\} \tag{1}$$

where $\overrightarrow{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\overrightarrow{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{f}^{\mathrm{T}}, s_0 := \overrightarrow{1} \cdot \overrightarrow{f}^{\mathrm{T}}$, $\theta_i, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$, $\overrightarrow{e}_{t,1} = (1, 0, \ldots, 0) \in \mathbb{F}_q^{n_t}$, and $\overrightarrow{v}_i \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}$. The challenge ciphertext for challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{(t, \overrightarrow{x}_t) \mid 1 \le t \le d\}$ is:

$$\left.\begin{array}{l} \boldsymbol{c}_0 := (\delta,\ \boxed{0},\ \boxed{\zeta},\ 0,\ \varphi_0)_{\mathbb{B}_0}, \\ \boldsymbol{c}_t := (\delta \overrightarrow{x}_t,\ \boxed{0^{n_t}},\ 0^{n_t},\ \varphi_t)_{\mathbb{B}_t} \text{ for } (t, \overrightarrow{x}_t) \in \Gamma, \\ c_{d+1} := g_T^{\zeta} m^{(b)}, \end{array}\right\} \tag{2}$$

where $b \xleftarrow{\mathsf{U}} \{0,1\}; \delta, \zeta, \varphi_0, \varphi_t \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $\overrightarrow{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}$.

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

$$\boldsymbol{c}_0 := (\delta,\ \boxed{r_0},\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0}, \tag{3}$$

$$\boldsymbol{c}_t := (\delta \overrightarrow{x}_t,\ \boxed{\overrightarrow{r}_t},\ 0^{n_t},\ \varphi_t)_{\mathbb{B}_t} \text{ for } (t, \overrightarrow{x}_t) \in \Gamma, \tag{4}$$

$$c_{d+1} := g_T^{\zeta} m^{(b)}, \tag{5}$$

where $r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{r}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$, and all the other variables are generated as in Game 0.

Game 2-h^+ ($h = 0, \ldots, \nu - 1$) : Game 2-0 is Game 1. Game 2-h^+ is the same as Game 2-h except the reply to the $(h+1)$-th key query for $\mathbb{S} := (M, \rho)$ with $\ell \times r$ matrix M, and $\boldsymbol{c}_t$ of the challenge ciphertext are:

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (-s_0,\ \boxed{w_0},\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}, \\ \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \\ \quad\quad \boldsymbol{k}_i^* := (s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i,\ \boxed{(a_i \overrightarrow{e}_{t,1} + \pi_i \overrightarrow{v}_i) \cdot Z_t},\ \overrightarrow{\eta}_i,\ 0)_{\mathbb{B}_t^*}, \\ \quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \\ \quad\quad \boldsymbol{k}_i^* := (s_i \overrightarrow{v}_i,\ \boxed{a_i \overrightarrow{v}_i \cdot Z_t},\ \overrightarrow{\eta}_i,\ 0)_{\mathbb{B}_t^*}, \end{array}\right\} \tag{6}$$

$$\boldsymbol{c}_t := (\delta \overrightarrow{x}_t,\ \boxed{\overrightarrow{x}_t \cdot U_t},\ 0^{n_t},\ \varphi_t)_{\mathbb{B}_t} \text{ for } (t, \overrightarrow{x}_t) \in \Gamma, \tag{7}$$

where $w_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\overrightarrow{a}^{\mathrm{T}} := (a_1, \ldots, a_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{g}^{\mathrm{T}}$, $\pi_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ $(i = 1, \ldots, \ell)$, $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $t = 1, \ldots, d$, and all the other variables are generated as in Game 2-h.

Game 2-$(h+1)$ ($h = 0, \ldots, \nu - 1$) : Game 2-$(h+1)$ is the same as Game 2-h^+ except the reply to the $(h+1)$-th key query for $\mathbb{S} := (M, \rho)$ with $\ell \times r$ matrix M, and $\boldsymbol{c}_t$ of the challenge ciphertext are:

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (-s_0,\ w_0,\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}, \\ \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \quad \boldsymbol{k}_i^* := (s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i,\ \boxed{0^{n_t}},\ \overrightarrow{\eta}_i,\ 0)_{\mathbb{B}_t^*}, \\ \quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \quad \boldsymbol{k}_i^* := (s_i \overrightarrow{v}_i,\ \boxed{0^{n_t}},\ \overrightarrow{\eta}_i,\ 0)_{\mathbb{B}_t^*}, \end{array}\right\} \tag{8}$$

$$\boldsymbol{c}_t := (\delta \overrightarrow{x}_t,\ \boxed{\overrightarrow{r}_t},\ 0^{n_t},\ \varphi_t)_{\mathbb{B}_t} \text{ for } (t, \overrightarrow{x}_t) \in \Gamma,$$

where $\overrightarrow{r}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$, and all the other variables are generated as in Game 2-h^+.

Game 3 : Same as Game 2-ν except that $\boldsymbol{c}_0$ and c_{d+1} of the challenge ciphertext are

$$\boldsymbol{c}_0 := (\delta,\ r_0,\ \boxed{\zeta'},\ 0,\ \varphi_0)_{\mathbb{B}_0}, \quad c_{d+1} := g_T^{\zeta} m^{(b)},$$

where $\zeta' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ (i.e., independent from $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$), and all the other variables are generated as in Game 2-ν.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0, 1, 2\text{-}h, 2\text{-}h^+$ and 3, respectively. $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$ is equivalent to $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KP\text{-}FE,PH}}(\lambda)$ and it is clear that $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$ by Lemma 8.

We will show four lemmas (Lemmas 4-7) that evaluate the gaps between pairs of $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h+1))}(\lambda)$ for $h = 0, \ldots, \nu - 1$ and $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)$. From

these lemmas and Lemmas 1 and 2, we obtain $\mathsf{Adv}^{\mathsf{KP\text{-}FE,PH}}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) \leq \left|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)\right| + \sum_{h=0}^{\nu-1}\left|\mathsf{Adv}^{(2\text{-}h)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h^+)}_{\mathcal{A}}(\lambda)\right| + \sum_{h=0}^{\nu-1}\left|\mathsf{Adv}^{(2\text{-}h^+)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}(h+1))}_{\mathcal{A}}(\lambda)\right| + \left|\mathsf{Adv}^{(2\text{-}\nu)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)\right| + \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + \sum_{h=0}^{\nu-1}\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}^+_{2,h}}(\lambda) + \sum_{h=0}^{\nu-1}\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2,h+1}}(\lambda) + (2d\nu + 6\nu + 1)/q \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \sum_{h=0}^{\nu-1}\left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}^+_{2,h}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2,h+1}}(\lambda)\right) + (2d\nu + 16\nu + d + 7)/q$. This completes the proof of Theorem 1. □

Lemma 4 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda)$.*

Proof. In order to prove Lemma 4, we construct a probabilistic machine $\mathcal{B}_1$ against Problem 1 using an adversary $\mathcal{A}$ in a security game (Game 0 or 1) as a black box as follows:

1. $\mathcal{B}_1$ is given a Problem 1 instance, $(\mathsf{param}_{\overrightarrow{n}}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,j}\}_{t=1,\ldots,d;j=2,\ldots,n_t})$.
2. $\mathcal{B}_1$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_1$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d})$ of Game 0 (and 1), where $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1})$ for $t = 1, .., d$, that are obtained from the Problem 1 instance.
4. When a key query is issued for access structure $\mathbb{S} := (M, \rho)$, $\mathcal{B}_1$ answers normal key $(\boldsymbol{k}^*_0, \ldots, \boldsymbol{k}^*_\ell)$ with Eq. (1), that is computed using $\{\widehat{\mathbb{B}}^*_t\}_{t=0,\ldots,d}$ of the Problem 1 instance.
5. When $\mathcal{B}_1$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{(t, \overrightarrow{x}_t) \mid 1 \leq t \leq d\}$ from $\mathcal{A}$, $\mathcal{B}_1$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, c_{d+1})$ such that
$$\boldsymbol{c}_0 := \boldsymbol{e}_{\beta,0} + \zeta \boldsymbol{b}_{0,3}, \qquad \boldsymbol{c}_t := x_{t,1}\boldsymbol{e}_{\beta,t,1} + \sum_{j=2}^{n_t} x_{t,j}\boldsymbol{e}_{t,j}, \qquad c_{d+1} := g_T^{\zeta} m^{(b)},$$
where $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\boldsymbol{b}_{0,3}, \boldsymbol{e}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,j}\}_{t=1,\ldots,d;j=2,\ldots,n_t})$ is a part of the Problem 1 instance.
6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_1$ executes the same procedure as that of step 4.
7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_1$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_1$ outputs $\beta' := 0$.

It is straightforward that the distribution by $\mathcal{B}_1$'s simulation given a Problem 1 instance with β is equivalent to that in Game 0 (resp. Game 1), when $\beta = 0$ (resp. $\beta = 1$) since $x_{t,1} = 1$. □

Lemma 5 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}^+_{2,h}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}h)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h^+)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}^+_{2,h}}(\lambda) + (d+3)/q$.*

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

1. $\mathcal{B}^+_{2,h}$ is given a Problem 2 instance, $(\mathsf{param}_{\overrightarrow{n}}, \widehat{\mathbb{B}}_0, \mathbb{B}^*_0, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,j}, \boldsymbol{e}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,n_t})$.

2. $\mathcal{B}_{2,h}^{+}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. At the first step of the game, $\mathcal{B}_{2,h}^{+}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^{\lambda}, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}'_t\}_{t=0,\ldots,d})$ of Game 2-h (and 2-h^{+}), where $\widehat{\mathbb{B}}'_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}}'_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1})$ for $t = 1, .., d$, that are obtained from the Problem 2 instance.

4. When the ι-th key query is issued for access structure $\mathbb{S} := (M, \rho)$, $\mathcal{B}_{2,h}^{+}$ answers as follows:

   (a) When $1 \leq \iota \leq h$, $\mathcal{B}_{2,h}^{+}$ answers semi-functional key $(\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_\ell^*)$ with Eq. (8), that is computed using $\{\mathbb{B}_t^*\}_{t=0,\ldots,d}$ of the Problem 2 instance.

   (b) When $\iota = h+1$, $\mathcal{B}_{2,h}^{+}$ calculates $(\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_\ell^*)$ using $(\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{h}_{\beta,0}^*, \{\boldsymbol{b}_{t,j}^*, \boldsymbol{h}_{\beta,t,j}^*\}_{t=1,\ldots,d;j=1,\ldots,n_t})$ of the Problem 2 instance as follows:

$$
\begin{array}{l}
\pi_t, \mu_t, g_k, \widetilde{\mu}_k \xleftarrow{\cup} \mathbb{F}_q \ \text{ for } t = 1, \ldots, d;\ k = 1, \ldots, r, \\
\widetilde{\boldsymbol{p}}_{\beta,0}^* := \sum_{k=1}^{r} \left(g_k \boldsymbol{h}_{\beta,0}^* + \widetilde{\mu}_k \boldsymbol{b}_{0,1}^* \right), \\
\text{for } t = 1, \ldots, d;\ k = 1, \ldots, r;\ j = 1, \ldots, n_t; \\
\quad \boldsymbol{p}_{\beta,t,j}^* := \pi_t \boldsymbol{h}_{\beta,t,j}^* + \mu_t \boldsymbol{b}_{t,j}^*, \qquad \widetilde{\boldsymbol{p}}_{\beta,t,k,j}^* := g_k \boldsymbol{h}_{\beta,t,j}^* + \widetilde{\mu}_k \boldsymbol{b}_{t,j}^*, \\
\boldsymbol{k}_0^* := -\widetilde{\boldsymbol{p}}_{\beta,0}^* + \boldsymbol{b}_{0,3}^*, \\
\text{for } i = 1, \ldots, \ell, \\
\quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \quad \boldsymbol{k}_i^* := \sum_{j=1}^{n_t} v_{i,j} \boldsymbol{p}_{\beta,t,j}^* + \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{p}}_{\beta,t,k,1}^*, \\
\quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \quad \boldsymbol{k}_i^* := \sum_{j=1}^{n_t} v_{i,j} (\sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{p}}_{\beta,t,k,j}^*),
\end{array}
$$

   where $(M_{i,k})_{i=1,\ldots,\ell;k=1,\ldots,r} := M$.

   (c) When $\iota \geq h+2$, $\mathcal{B}_{2,h}^{+}$ answers normal key $(\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_\ell^*)$ with Eq. (1), that is computed using $\{\mathbb{B}_t^*\}_{t=0,\ldots,d}$ of the Problem 2 instance.

5. When $\mathcal{B}_{2,h}^{+}$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{(t, \overrightarrow{x}_t) \mid 1 \leq t \leq d\}$ from $\mathcal{A}$, $\mathcal{B}_{2,h}^{+}$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, c_{d+1})$ such that for $(t, \overrightarrow{x}_t) \in \Gamma$,

$$
\boldsymbol{c}_0 := \boldsymbol{e}_0 + \zeta \boldsymbol{b}_{0,3} + \boldsymbol{q}_0, \qquad \boldsymbol{c}_t := \sum_{j=1}^{n_t} x_{t,j} \boldsymbol{e}_{t,j} + \boldsymbol{q}_t, \qquad c_{d+1} := g_T^{\zeta} m^{(b)},
$$

   where $\zeta \xleftarrow{\cup} \mathbb{F}_q$, $b \xleftarrow{\cup} \{0,1\}$, $\boldsymbol{q}_0 \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}_{0,5} \rangle$, $\boldsymbol{q}_t \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}_{t,3n_t+1} \rangle$, and $(\boldsymbol{b}_{0,3}, \boldsymbol{e}_0, \{\boldsymbol{e}_{t,j}\}_{t=1,..,d;j=1,..,n_t})$ is a part of the Problem 2 instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_{2,h}^{+}$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{2,h}^{+}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{2,h}^{+}$ outputs $\beta' := 0$.

Remark 1 $\widetilde{\boldsymbol{p}}_{\beta,0}^*, \boldsymbol{p}_{\beta,t,j}^*, \widetilde{\boldsymbol{p}}_{\beta,t,k,j}^*$ for $t = 1, \ldots, d; k = 1, \ldots, r; j = 1, \ldots, n_t$ calculated in case (b) of steps 4 and 6 in the above simulation are expressed as:

$$
\begin{array}{l}
\theta_t := \pi_t \delta + \mu_t, \quad f_k := g_k \delta + \widetilde{\mu}_k, \quad s_0 := \sum_{k=1}^{r} f_k, \quad a_0 := \sum_{k=1}^{r} g_k, \quad w_0 := a_0 / z_0 \ (= a_0 u_0), \\
\widetilde{\boldsymbol{p}}_{0,0}^* = (s_0, 0, 0, a_0 \delta_0, 0)_{\mathbb{B}_0^*}, \quad \widetilde{\boldsymbol{p}}_{1,0}^* = (s_0, w_0, 0, a_0 \delta_0, 0)_{\mathbb{B}_0^*},
\end{array}
$$

$$
\begin{array}{lcccccccc}
 & & \overbrace{\phantom{\theta_t \overrightarrow{e}_{t,j},}}^{n_t} & & \overbrace{\phantom{0^{n_t},}}^{n_t} & & \overbrace{\phantom{\pi_t \overrightarrow{\delta}_{t,j},}}^{n_t} & \overbrace{}^{1} & \\
\boldsymbol{p}_{0,t,j}^* := & (& \theta_t \overrightarrow{e}_{t,j}, & & 0^{n_t}, & & \pi_t \overrightarrow{\delta}_{t,j}, & 0 &)_{\mathbb{B}_t^*}, \\
\widetilde{\boldsymbol{p}}_{0,t,k,j}^* := & (& f_k \overrightarrow{e}_{t,j}, & & 0^{n_t}, & & g_k \overrightarrow{\delta}_{t,j}, & 0 &)_{\mathbb{B}_t^*}, \\
\boldsymbol{p}_{1,t,j}^* := & (& \theta_t \overrightarrow{e}_{t,j}, & & \pi_t \overrightarrow{u}_{t,j}, & & \pi_t \overrightarrow{\delta}_{t,j}, & 0 &)_{\mathbb{B}_t^*}, \\
\widetilde{\boldsymbol{p}}_{1,t,k,j}^* := & (& f_k \overrightarrow{e}_{t,j}, & & g_k \overrightarrow{u}_{t,j}, & & g_k \overrightarrow{\delta}_{t,j}, & 0 &)_{\mathbb{B}_t^*},
\end{array}
$$

where $\delta, z_0, \delta_0, \{\overrightarrow{e}_{t,j}, \overrightarrow{u}_{t,j}, \overrightarrow{\delta}_{t,j}\}_{t=1,\ldots,d;j=1,..,n_t}$ are defined in Problem 2. Note that variables $\{\theta_t, \pi_t\}_{t=1,\ldots,d}$, $\{f_k, g_k\}_{k=1,\ldots,r}$ are independently and uniformly distributed. Therefore, $\{\boldsymbol{k}_i^*\}_{i=0,\ldots,\ell}$ are distributed as Eq. (6) except $w_0 := a_0/r_0$, i.e., $w_0 r_0 = a_0$, using a_0 and $r_0 := z_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ in $\boldsymbol{c}_0$ (Eq. (3)).

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

Proof. It is clear that $\mathcal{B}_{2,h}^{+}$'s simulation of the public-key generation (step 2) and the ι-th key query's answer for $\iota \neq h+1$ (cases (a) and (c) of steps 4 and 6) is perfect, i.e., exactly the same as the Setup and the KeyGen oracle in Game 2-h and Game 2-h^+.

Therefore, to prove this lemma we will show that the joint distribution of the $(h+1)$-the key query's answer and the challenge ciphertext by $\mathcal{B}_{2,h}^{+}$'s simulation given a Problem 2 instance with β is equivalent to that in Game 2-h (resp. Game 2-h^+), when $\beta = 0$ (resp. $\beta = 1$).

When $\beta = 0$, it is straightforward to show that they are equivalent except that δ defined in Problem 2 is zero or there exists $t \in \{0, \ldots, d\}$ such that $\overrightarrow{r}_t = \overrightarrow{0}$, where $\overrightarrow{r}_t$ are defined in Eqs. (3) and (4), i.e., except with probability $(d+2)/q$.

When $\beta = 1$, the distribution by $\mathcal{B}_{2,h}^{+}$'s simulation is Eq. (6) for the key and Eqs. (3), (5), and (7) for the challenge ciphertext, where the distribution is the same as that defined in these equations except $w_0 := a_0/r_0$, i.e., $w_0 r_0 = a_0$, using $a_0 := \overrightarrow{1} \cdot \overrightarrow{g}^{\mathrm{T}}$ and $r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ in $\boldsymbol{c}_0$ (Eq. (3)) from Remark 1. The corresponding distribution in Game 2-h^+ is Eq. (6) and Eqs. (3), (5), and (7) where $r_0, w_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ as defined in the equations.

Therefore, we will show that a_0 is uniformly and independently distributed from the other variables in the joint distribution of $\mathcal{B}_{2,h}^{+}$'s simulation. Since $a_0 := \overrightarrow{1} \cdot \overrightarrow{g}^{\mathrm{T}}$ is only related to $(a_1, \ldots, a_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{g}^{\mathrm{T}}$ and $U_t = (Z_t^{-1})^{\mathrm{T}}$ holds, a_0 is only related to $\{\overrightarrow{w}_i\}_{i=1,\ldots,\ell}, \{\overrightarrow{\overrightarrow{w}}_i\}_{i=1,\ldots,\ell}$ and $\{\overrightarrow{r}_t\}_{t=1,\ldots,d}$, where $\overrightarrow{w}_i := (a_i \overrightarrow{e}_{t,1} + \pi_i \overrightarrow{v}_i) \cdot Z_t := ((a_i, 0, \ldots, 0) + \pi_i \overrightarrow{v}_i) \cdot Z_t$ and $\overrightarrow{\overrightarrow{w}}_i := a_i \overrightarrow{v}_i \cdot Z_t$ in Eq. (6) for $i = 1, \ldots, \ell$, and $\overrightarrow{r}_t := \overrightarrow{x}_t \cdot U_t$ in Eq. (7) for $t = 1, \ldots, d$ with $t := \widetilde{\rho}(i)$. ($\widetilde{\rho}$ is defined at the start of Section 6.) With respect to the joint distribution of these variables, there are five cases for each $i \in \{1, \ldots, \ell\}$. Note that for any $i \in \{1, \ldots, \ell\}$, (Z_t, U_t) with $t := \widetilde{\rho}(i)$ is independent from the other variables, since $\widetilde{\rho}$ is injective:

1. $\gamma(i) = 1$ and $[\rho(i) = (t, \overrightarrow{v}_i) \ \wedge \ (t, \overrightarrow{x}_t) \in \Gamma \ \wedge \ \overrightarrow{v}_i \cdot \overrightarrow{x}_t = 0]$.

   Then, from Lemma 3, the joint distribution of $(\overrightarrow{w}_i, \overrightarrow{r}_t)$ is uniformly and independently distributed on $C_{a_i} := \{(\overrightarrow{w}, \overrightarrow{r}) | \overrightarrow{w} \cdot \overrightarrow{r} = a_i\}$ (over $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$).

2. $\gamma(i) = 1$ and $[\rho(i) = \neg(t, \overrightarrow{v}_i) \ \wedge \ (t, \overrightarrow{x}_t) \in \Gamma \ \wedge \ \overrightarrow{v}_i \cdot \overrightarrow{x}_t \neq 0]$.

   Then, from Lemma 3, the joint distribution of $(\overrightarrow{\overrightarrow{w}}_i, \overrightarrow{r}_t)$ is uniformly and independently distributed on $C_{(\overrightarrow{v}_i \cdot \overrightarrow{x}_t) \cdot a_i}$ (over $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$).

3. $\gamma(i) = 0$ and $[\rho(i) = (t, \overrightarrow{v}_i) \ \wedge \ (t, \overrightarrow{x}_t) \in \Gamma]$ (i.e., $\overrightarrow{v}_i \cdot \overrightarrow{x}_t \neq 0$).

   Then, from Lemma 3, the joint distribution of $(\overrightarrow{w}_i, \overrightarrow{r}_t)$ is uniformly and independently distributed on $C_{(\overrightarrow{v}_i \cdot \overrightarrow{x}_t) \cdot \pi_t + a_i}$ (over $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$) where π_t is defined in Remark 1. Since π_t is uniformly and independently distributed on $\mathbb{F}_q$, the joint distribution of $(\overrightarrow{w}_i, \overrightarrow{r}_t)$ is uniformly and independently distributed over $\mathbb{F}_q^{2n_t}$.

4. $\gamma(i) = 0$ and $[\rho(i) = \neg(t, \overrightarrow{v}_i) \ \wedge \ (t, \overrightarrow{x}_t) \in \Gamma]$ (i.e., $\overrightarrow{v}_i \cdot \overrightarrow{x}_t = 0$).

Then, from Lemma 3, the joint distribution of $(\overrightarrow{\overline{w}}_i, \overrightarrow{r}_t)$ is uniformly and independently distributed on C_0 (over $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$).

5. $[\rho(i) = (t, \overrightarrow{v}_i) \ \wedge \ (t, \overrightarrow{x}_t) \notin \Gamma]$ or $[\rho(i) = \neg(t, \overrightarrow{v}_i) \ \wedge \ (t, \overrightarrow{x}_t) \notin \Gamma]$.
   Then, the distribution of $\overrightarrow{w}_i$ is uniformly and independently distributed on $\mathbb{F}_q^{n_t}$ (over $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$).

We then observe the joint distribution (or relation) of a_0, $\{\overrightarrow{w}_i\}_{i=1,\ldots,\ell}$, $\{\overrightarrow{\overline{w}}_i\}_{i=1,\ldots,\ell}$ and $\{\overrightarrow{r}_t\}_{t=1,\ldots,d}$. Those in cases 3-5 are obviously independent from a_0. Due to the restriction of adversary $\mathcal{A}$'s key queries, $\overrightarrow{1} \notin \mathsf{span}\langle(M_i)_{\gamma(i)=1}\rangle$. Therefore, $a_0 := \overrightarrow{1} \cdot \overrightarrow{g}^{\mathrm{T}}$ is independent from the joint distribution of $\{a_i := M_i \cdot \overrightarrow{g}^{\mathrm{T}} \mid \gamma(i) = 1\}$ (over the random selection of $\overrightarrow{g}$), which can be given by $(\overrightarrow{w}_i, \overrightarrow{r}_t)$ in case 1 and $(\overrightarrow{\overline{w}}_i, \overrightarrow{r}_t)$ in case 2. Thus, a_0 is uniformly and independently distributed from the other variables in the joint distribution of $\mathcal{B}_{2,h}^{+}$'s simulation.

Therefore, the view of adversary $\mathcal{A}$ in the game simulated by $\mathcal{B}_{2,h}^{+}$ given a Problem 2 instance with $\beta = 1$ is the same as that in Game 2-h^+ except that δ defined in Problem 2 is zero i.e., except with probability $1/q$. □

This completes the proof of Lemma 5. □

Lemma 6 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2,h+1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h+1))}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2,h+1}}^{\mathsf{P2}}(\lambda) + (d+3)/q$.*

Proof. In order to prove Lemma 6, we construct a probabilistic machine $\mathcal{B}_{2,h+1}$ against Problem 2 using an adversary $\mathcal{A}$ in a security game (Game 2-h^+ or 2-$(h+1)$) as a black box. $\mathcal{B}_{2,h+1}$ acts in the same way as $\mathcal{B}_{2,h}^{+}$ in the proof of Lemma 5 except the following two points:

1. In case (b) of step 4; $\boldsymbol{k}_0^*$ is calculated as
$$\boldsymbol{k}_0^* := -\widetilde{\boldsymbol{p}}_{\beta,0}^* + r_0' \boldsymbol{b}_{0,2}^* + \boldsymbol{b}_{0,3}^*,$$
   where $r_0' \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\widetilde{\boldsymbol{p}}_{\beta,0}^*$ is calculated from $\boldsymbol{h}_{\beta,0}^*$ and $\boldsymbol{b}_{0,1}^*$ as in the proof of Lemma 5, and $\mathbb{B}^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,2}^*, \boldsymbol{b}_{0,3}^*)$ is in the Problem 2 instance.

2. In the last step; if $b = b'$, $\mathcal{B}_{2,h+1}$ outputs $\beta' := 0$. Otherwise, $\mathcal{B}_{2,h+1}$ outputs $\beta' := 1$.

When $\beta = 0$, it is straightforward that the distribution by $\mathcal{B}_{2,h+1}$'s simulation is equivalent to that in Game 2-$(h+1)$ except that δ defined in Problem 2 is zero, i.e., except with probability $1/q$. When $\beta = 1$, the distribution by $\mathcal{B}_{2,h+1}$'s simulation is equivalent to that in Game 2-h^+ except that δ defined in Problem 2 is zero or there exists $t \in \{0, \ldots, d\}$ such that $\overrightarrow{r}_t = \overrightarrow{0}$ are defined in Eqs. (3) and (4), i.e., except with probability $(d+2)/q$. □

Lemma 7 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) \leq \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu)}(\lambda) + 1/q$.*

Proof. To prove Lemma 7, we will show distribution $(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c})$ in Game 2-ν and that in Game 3 are equivalent, where $\mathsf{sk}_{\mathbb{S}}^{(j)*}$ is the answer to the j-th key query, and $\boldsymbol{c}$ is the challenge ciphertext. By definition, we only need to consider elements on $\mathbb{V}_0$ or $\mathbb{V}_0^*$. We define new bases $\mathbb{D}_0$ of $\mathbb{V}_0$ and $\mathbb{D}_0^*$ of $\mathbb{V}_0^*$ as follows: We generate $\theta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and set
$$\boldsymbol{d}_{0,2} := (0, 1, -\theta, 0, 0)_{\mathbb{B}} = \boldsymbol{b}_{0,2} - \theta \boldsymbol{b}_{0,3}, \quad \boldsymbol{d}_{0,3}^* := (0, \theta, 1, 0, 0)_{\mathbb{B}} = \boldsymbol{b}_{0,3}^* + \theta \boldsymbol{b}_{0,2}^*.$$

We set $\mathbb{D}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{d}_{0,2}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4}, \boldsymbol{b}_{0,5})$, $\mathbb{D}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,2}^*, \boldsymbol{d}_{0,3}^*, \boldsymbol{b}_{0,4}^*, \boldsymbol{b}_{0,5}^*)$. We then easily verify that $\mathbb{D}_0$ and $\mathbb{D}_0^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}_0$ and $\mathbb{B}_0^*$.

The $\mathbb{V}_0$ components $(\{\boldsymbol{k}_0^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_0)$ in keys and challenge ciphertext $(\{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\ldots,\nu}, \mathsf{ct}_\Gamma)$ in Game 2-ν are expressed over bases $\mathbb{B}_0$ and $\mathbb{B}_0^*$ as $\boldsymbol{k}_0^{(j)*} = (-s_0^{(j)}, w_0^{(j)}, 1, \eta_0^{(j)}, 0)_{\mathbb{B}_0^*}$, $\boldsymbol{c}_0 = (\delta, r_0, \zeta, 0, \varphi_0)_{\mathbb{B}_0}$. Then,

$$\boldsymbol{k}_0^{(j)*} = (-s_0^{(j)}, w_0^{(j)}, 1, \eta_0^{(j)}, 0)_{\mathbb{B}_0^*} = (-s_0^{(j)}, w_0^{(j)} + \theta, 1, \eta_0^{(j)}, 0)_{\mathbb{D}_0^*} = (-s_0^{(j)}, \vartheta_0^{(j)}, 1, \eta_0^{(j)}, 0)_{\mathbb{D}_0^*},$$

where $\vartheta_0^{(j)} := w_0^{(j)} + \theta$ which are uniformly, independently distributed since $w_0^{(j)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

$$\boldsymbol{c}_0 = (\delta, r_0, \zeta, 0, \varphi_0)_{\mathbb{B}_0} = (\delta, r_0, \zeta + r_0\theta, 0, \varphi_0)_{\mathbb{D}_0} = (\delta, r_0, \zeta', 0, \varphi_0)_{\mathbb{D}_0}$$

where $\zeta' := \zeta + r_0\theta$ which is uniformly, independently distributed since $\theta \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

In the light of the adversary's view, both $(\mathbb{B}_0, \mathbb{B}_0^*)$ and $(\mathbb{D}_0, \mathbb{D}_0^*)$ are consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d})$. Therefore, $\{\mathsf{sk}_{\mathbb{S}}^{(j)*}\}_{j=1,\ldots,\nu}$ and ct_Γ can be expressed as keys and ciphertext in two ways, in Game 2-ν over bases $(\mathbb{B}_0, \mathbb{B}_0^*)$ and in Game 3 over bases $(\mathbb{D}_0, \mathbb{D}_0^*)$. Thus, Game 2-$\nu$ can be conceptually changed to Game 3 if $r_0 \neq 0$, i.e., except with probability $1/q$. □

Lemma 8 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$.*

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

7 Proposed CP-FE Scheme

7.1 Construction

$\widetilde{\rho} : \{1, \ldots, \ell\} \to \{1, \ldots, d\}$ is defined at the start of Section 6. In the proposed scheme, we assume that $\widetilde{\rho}$ is injective for $\mathbb{S} := (M, \rho)$ with ciphertext $\mathsf{ct}_{\mathbb{S}}$. We will show how to relax the restriction in Appendix F.

In the description of the scheme, we assume that input vector $\overrightarrow{x}_t := (x_{t,1}, \ldots, x_{t,n_t})$ is normalized such that $x_{t,1} := 1$. (If $\overrightarrow{x}_t$ is not normalized, change it to a normalized one by $(1/x_{t,1}) \cdot \overrightarrow{x}_t$ assuming that $x_{t,1}$ is non-zero). In addition, we assume that input vector $\overrightarrow{v}_i := (v_{i,1}, \ldots, v_{i,n_t})$ satisfies that $v_{i,n_t} \neq 0$.

Random dual bases generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n})$ is defined at the end of Section 2. We refer to Section 1.3 for notations on DPVS.

$\mathsf{Setup}(1^\lambda, \overrightarrow{n} := (d; n_1, \ldots, n_d))$: $(\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n})$,

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$, $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1})$ for $t = 1, \ldots, d$,

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*)$, $\widehat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, \ldots, \boldsymbol{b}_{t,n_t}^*, \boldsymbol{b}_{t,2n_t+1}^*, \ldots, \boldsymbol{b}_{t,3n_t}^*)$ for $t = 1, \ldots, d$,

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

return pk, sk.

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma := \{(t, \overrightarrow{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}) \mid 1 \leq t \leq d,\ x_{t,1} := 1\})$:

$\delta, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ such that $(t, \overrightarrow{x}_t) \in \Gamma$,

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

$$\boldsymbol{k}_t^* := \Big(\overbrace{\delta \overrightarrow{x}_t,}^{n_t} \quad \overbrace{0^{n_t},}^{n_t} \quad \overbrace{\overrightarrow{\varphi}_t,}^{n_t} \quad \overbrace{0}^{1} \Big)_{\mathbb{B}_t^*} \text{ for } (t, \overrightarrow{x}_t) \in \Gamma,$$

$\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\overrightarrow{x}_t)\in\Gamma})$

return sk_Γ.

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

$\overrightarrow{f} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r,\ \overrightarrow{s}^{\mathrm{T}} := (s_1,\ldots,s_\ell)^{\mathrm{T}} := M\cdot\overrightarrow{f}^{\mathrm{T}},\ s_0 := \overrightarrow{1}\cdot\overrightarrow{f}^{\mathrm{T}},\ \eta_0,\eta_i,\theta_i,\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q\ (i=1,..,\ell),$

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

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

if $\rho(i) = (t,\overrightarrow{v}_i := (v_{i,1},\ldots,v_{i,n_t}) \in \mathbb{F}_q^{n_t}\setminus\{\overrightarrow{0}\})\ (v_{i,n_t}\neq 0)$,

$$\boldsymbol{c}_i := (\ \overbrace{s_i\overrightarrow{e}_{t,1}+\theta_i\overrightarrow{v}_i,}^{n_t}\ \overbrace{0^{n_t},}^{n_t}\ \overbrace{0^{n_t},}^{n_t}\ \overbrace{\eta_i}^{1}\ )_{\mathbb{B}_t},$$

if $\rho(i) = \neg(t,\overrightarrow{v}_i)$,

$$\boldsymbol{c}_i := (\ \overbrace{s_i\overrightarrow{v}_i,}^{n_t}\ \overbrace{0^{n_t},}^{n_t}\ \overbrace{0^{n_t},}^{n_t}\ \overbrace{\eta_i}^{1}\ )_{\mathbb{B}_t},$$

$c_{d+1} := g_T^{\zeta} m,\quad \mathsf{ct}_{\mathbb{S}} := (\mathbb{S},\boldsymbol{c}_0,\boldsymbol{c}_1,\ldots,\boldsymbol{c}_\ell,c_{d+1}).$

return $\mathsf{ct}_{\mathbb{S}}$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_\Gamma := (\Gamma,\boldsymbol{k}_0^*,\{\boldsymbol{k}_t^*\}_{(t,\overrightarrow{x}_t)\in\Gamma}),\ \mathsf{ct}_{\mathbb{S}} := (\mathbb{S},\boldsymbol{c}_0,\boldsymbol{c}_1,\ldots,\boldsymbol{c}_\ell,c_{d+1}))$:

If $\mathbb{S} := (M,\rho)$ accepts $\Gamma := \{(t,\overrightarrow{x}_t)\}$, then compute I and $\{\alpha_i\}_{i\in I}$ such that

$\overrightarrow{1} = \sum_{i\in I}\alpha_i M_i,$ where M_i is the i-th row of M, and

$I \subseteq \{i\in\{1,\ldots,\ell\}|\ [\rho(i) = (t,\overrightarrow{v}_i)\ \wedge\ (t,\overrightarrow{x}_t)\in\Gamma\ \wedge\ \overrightarrow{v}_i\cdot\overrightarrow{x}_t = 0]$

$\qquad\qquad \vee\ \ [\rho(i) = \neg(t,\overrightarrow{v}_i)\ \wedge\ (t,\overrightarrow{x}_t)\in\Gamma\ \wedge\ \overrightarrow{v}_i\cdot\overrightarrow{x}_t\neq 0]\ \}.$

$$K := e(\boldsymbol{c}_0,\boldsymbol{k}_0^*) \prod_{i\in I\ \wedge\ \rho(i)=(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_i,\boldsymbol{k}_t^*)^{\alpha_i} \cdot \prod_{i\in I\ \wedge\ \rho(i)=\neg(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_i,\boldsymbol{k}_t^*)^{\alpha_i/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)}$$

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

[Correctness] If $\mathbb{S} := (M,\rho)$ accepts $\Gamma := \{(t,\overrightarrow{x}_t)\}$,

$$\begin{aligned}
&e(\boldsymbol{c}_0,\boldsymbol{k}_0^*)\textstyle\prod_{i\in I\ \wedge\ \rho(i)=(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_i,\boldsymbol{k}_t^*)^{\alpha_i}\cdot\prod_{i\in I\ \wedge\ \rho(i)=\neg(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_i,\boldsymbol{k}_t^*)^{\alpha_i/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)}\\
&= g_T^{-\delta s_0+\zeta}\textstyle\prod_{i\in I\ \wedge\ \rho(i)=(t,\overrightarrow{v}_i)} g_T^{\delta\alpha_i s_i}\prod_{i\in I\ \wedge\ \rho(i)=\neg(t,\overrightarrow{v}_i)} g_T^{\delta\alpha_i s_i(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)}\\
&= g_T^{\delta(-s_0+\sum_{i\in I}\alpha_i s_i)+\zeta} = g_T^{\zeta}.
\end{aligned}$$

7.2 Security

We can prove adaptively payload-hiding security for the CP-FE scheme similarly as the proposed KP-FE case (Theorem 1).

Theorem 2 *The proposed CP-FE scheme is adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_1,\mathcal{E}_{2,h}^+,\mathcal{E}_{2,h+1}$ $(h=0,\ldots,\nu-1)$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CP\text{-}FE,PH}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{h=0}^{\nu-1}\left(\mathsf{Adv}_{\mathcal{E}_{2,h}^+}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{2,h+1}}^{\mathsf{DLIN}}(\lambda)\right) + \epsilon,$$

where ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (2d\nu+16\nu+2d+8)/q$.

Proof Outline of Theorem 2: As in the proof of Theorem 1, we follow the dual system encryption methodology proposed by Waters [28], at the top level of strategy of the security proof. In addition, the description of the game transformation is very similar to that of Theorem 1, and the three forms of ciphertexts and secret keys, *normal*, *semi-functional*, and *pre-semi-functional*, are also used as before. Therefore, here, we only describe these forms of ciphertexts and secret keys for the proof of Theorem 2.

For $\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\overrightarrow{x}_t)\in\Gamma})$ and $\mathsf{ct}_\mathbb{S} := (\mathbb{S}, \boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$, we focus on $\overrightarrow{\boldsymbol{k}}_\Gamma^* := (\boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\overrightarrow{x}_t)\in\Gamma})$ and $\overrightarrow{\boldsymbol{c}}_\mathbb{S} := (\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell)$, and ignore the other part of sk_Γ and $\mathsf{ct}_\mathbb{S}$ (and call them secret key and ciphertext, respectively) in this proof outline.

A *normal* secret key, $\overrightarrow{\boldsymbol{k}}_\Gamma^{*\,\mathsf{norm}}$ (with attribute set Γ), is a correct form of the secret key of the proposed CP-FE scheme, and is expressed by Eq. (9). Similarly, a *normal* ciphertext $\overrightarrow{\boldsymbol{c}}_\mathbb{S}^{\mathsf{norm}} := (\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\ell)$ (with access structure $\mathbb{S}$) is Eq. (10). A *semi-functional* secret key, $\overrightarrow{\boldsymbol{k}}_\Gamma^{*\,\mathsf{semi}}$, is Eq. (16), and a *semi-functional* ciphertext, $\overrightarrow{\boldsymbol{c}}_\mathbb{S}^{\mathsf{semi}}$, is Eqs. (11)-(13). A *pre-semi-functional* secret key, $\overrightarrow{\boldsymbol{k}}_\Gamma^{*\,\mathsf{pre\text{-}semi}}$, and *pre-semi-functional* ciphertext, $\overrightarrow{\boldsymbol{c}}_\mathbb{S}^{\mathsf{pre\text{-}semi}}$, are Eq. (14) and Eqs. (11),(15) and (13), respectively.

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

Game 0 : Original game. That is, the reply to a KeyGen query for $\Gamma := \{(t, \overrightarrow{x}_t)\}$ are:

$$\left.\begin{aligned} \boldsymbol{k}_0^* &:= (\delta,\ \boxed{0},\ 1,\ \varphi_0,\ 0)_{\mathbb{B}_0^*}, \\ \boldsymbol{k}_t^* &:= (\delta\overrightarrow{x}_t,\ \boxed{0^{n_t}},\ \overrightarrow{\varphi}_t,\ 0)_{\mathbb{B}_t} \ \text{ for } (t, \overrightarrow{x}_t) \in \Gamma, \end{aligned}\right\} \tag{9}$$

where $\delta \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times$, $\varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $(t, \overrightarrow{x}_t) \in \Gamma$. The challenge ciphertext for challenge plaintexts $(m^{(0)}, m^{(1)})$ and access structure $\mathbb{S} := (M, \rho)$ is:

$$\left.\begin{aligned} &\boldsymbol{c}_0 := (-s_0,\ \boxed{0},\ \boxed{\zeta},\ 0,\ \eta_0)_{\mathbb{B}_0}, \\ &\text{for } i = 1, \ldots, \ell, \\ &\quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \quad \boldsymbol{c}_i := (s_i\overrightarrow{e}_{t,1} + \theta_i\overrightarrow{v}_i,\ \boxed{0^{n_t}},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t}, \\ &\quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \quad \boldsymbol{c}_i := (s_i\overrightarrow{v}_i,\ \boxed{0^{n_t}},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t}, \\ &c_{d+1} := g_T^\zeta m^{(b)}, \end{aligned}\right\} \tag{10}$$

where $\overrightarrow{f} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$, $\overrightarrow{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{f}^{\mathrm{T}}$, $s_0 := \overrightarrow{1} \cdot \overrightarrow{f}^{\mathrm{T}}$, $\eta_0, \theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ $\overrightarrow{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $i = 1, \ldots, \ell$, and $\overrightarrow{e}_{t,1} := (1, 0, \ldots, 0) \in \mathbb{F}_q^{n_t}$.

Game 1 : Same as Game 0 except that the challenge ciphertext $(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\ell, c_{d+1})$ is:

$$\boldsymbol{c}_0 := (-s_0,\ \boxed{w_0},\ \zeta,\ 0,\ \eta_0)_{\mathbb{B}_0}, \tag{11}$$

$$\left.\begin{aligned} &\text{for } i = 1, \ldots, \ell, \\ &\quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \quad \boldsymbol{c}_i := (s_i\overrightarrow{e}_{t,1} + \theta_i\overrightarrow{v}_i,\ \boxed{\overrightarrow{w}_i},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t}, \\ &\quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \quad \boldsymbol{c}_i := (s_i\overrightarrow{v}_i,\ \boxed{\overrightarrow{\overrightarrow{w}}_i},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t}, \end{aligned}\right\} \tag{12}$$

$$c_{d+1} := g_T^\zeta m^{(b)}, \tag{13}$$

where $w_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{w}_i, \overrightarrow{\overrightarrow{w}}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $i = 1, \ldots, \ell$, and all the other variables are generated as in Game 0.

Game 2-h^+ ($h = 0, \ldots, \nu-1$) : Game 2-0 is Game 1. Game 2-h^+ is the same as Game 2-h except that $\boldsymbol{k}_t^*$ for $t = 0$ and $(t, \overrightarrow{x}_t) \in \Gamma$ of the reply to the $(h+1)$-th KeyGen query, and $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell)$ of the challenge ciphertext are:

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (\delta,\ \boxed{r_0},\ 1,\ \varphi_0,\ 0)_{\mathbb{B}_0^*}, \\ \boldsymbol{k}_t^* := (\delta \overrightarrow{x}_t,\ \boxed{\overrightarrow{x}_t \cdot U_t},\ \overrightarrow{\varphi}_t,\ 0)_{\mathbb{B}_t} \ \text{ for } (t, \overrightarrow{x}_t) \in \Gamma, \end{array}\right\} \tag{14}$$

$$\left.\begin{array}{l} \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \ \ \boldsymbol{c}_i := (s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i,\ \boxed{(a_i \overrightarrow{e}_{t,1} + \pi_i \overrightarrow{v}_i) \cdot Z_t},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t}, \\ \quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \ \ \boldsymbol{c}_i := (s_i \overrightarrow{v}_i,\ \boxed{a_i \overrightarrow{v}_i \cdot Z_t},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t}, \end{array}\right\} \tag{15}$$

where $r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\overrightarrow{a}^{\mathrm{T}} := (a_1, \ldots, a_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{g}^{\mathrm{T}}$, $\pi_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, \ell$, $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $t = 1, \ldots, d$, and all the other variables are generated as in Game 2-h.

Game 2-($h+1$) ($h = 0, \ldots, \nu-1$) : Game 2-($h+1$) is the same as Game 2-h^+ except that $\boldsymbol{k}_t^*$ for $(t, \overrightarrow{x}_t) \in \Gamma$ of the reply to the $(h+1)$-th KeyGen query, and $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell)$ of the challenge ciphertext are:

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (\delta,\ r_0,\ 1,\ \varphi_0,\ 0)_{\mathbb{B}_0^*}, \\ \boldsymbol{k}_t^* := (\delta \overrightarrow{x}_t,\ \boxed{0^{n_t}},\ \overrightarrow{\varphi}_t,\ 0)_{\mathbb{B}_t} \ \text{ for } (t, \overrightarrow{x}_t) \in \Gamma, \end{array}\right\} \tag{16}$$

$$\begin{array}{l} \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \quad \boldsymbol{c}_i := (s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i,\ \boxed{\overrightarrow{w}_i},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t}, \\ \quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \quad \boldsymbol{c}_i := (s_i \overrightarrow{v}_i,\ \boxed{\overrightarrow{\overrightarrow{w}}_i},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t}, \end{array}$$

where $\overrightarrow{w}_i, \overrightarrow{\overrightarrow{w}}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $i = 1, \ldots, \ell$, and all the other variables are generated as in Game 2-h^+.

Game 3 : Same as Game 2-ν except that $\boldsymbol{c}_0$ and c_{d+1} of the challenge ciphertext are

$$\boldsymbol{c}_0 := (-s_0,\ w_0,\ \boxed{\zeta'},\ 0,\ \eta_0)_{\mathbb{B}_0}, \quad c_{d+1} := g_T^{\zeta} m^{(b)},$$

where $\zeta' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ (i.e., independent from $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$), and all the other variables are generated as in Game 2-ν.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$ be $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CP\text{-}FE,PH}}(\lambda)$ in Game 0, and $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $1, 2\text{-}h, 2\text{-}h^+, 3$, respectively. It is clear that $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$ by Lemma 13.

We will show four lemmas (Lemmas 9-12) that evaluate the gaps between pairs of $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h+1))}(\lambda)$ for $h = 0, \ldots, \nu-1$. From these lemmas and Lemmas 1 and 2, we obtain $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CP\text{-}FE,PH}}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) \leq \left|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| + \sum_{h=0}^{\nu-1} \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda)\right| + \sum_{h=0}^{\nu-1} \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h+1))}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)\right| + \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1}}(\lambda) + \sum_{h=0}^{\nu-1} \mathsf{Adv}_{\mathcal{B}_{2,h}^+}^{\mathsf{P2}}(\lambda) + \sum_{h=0}^{\nu-1} \mathsf{Adv}_{\mathcal{B}_{2,h+1}}^{\mathsf{P2}}(\lambda) + (2d\nu + 6\nu + d + 2)/q \leq \mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{h=0}^{\nu-1} \left(\mathsf{Adv}_{\mathcal{E}_{2,h}^+}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{2,h+1}}^{\mathsf{DLIN}}(\lambda)\right) + (2d\nu + 16\nu + d + 10)/q$. This completes the proof of Theorem 2. □

Lemma 9 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1}}(\lambda) + (d+1)/q$.*

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

1. $\mathcal{B}_1$ is given Problem 1 instance $(\mathsf{param}_{\overrightarrow{n}}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,j}\}_{t=1,\ldots,d;j=2,\ldots,n_t})$.
2. $\mathcal{B}_1$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_1$ sets

$$\begin{aligned}
&\mathbb{D}_0 := \mathbb{B}_0,\ \mathbb{D}^*_0 := \mathbb{B}^*_0,\ \widehat{\mathbb{D}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{D}}^*_0 := \widehat{\mathbb{B}}^*_0,\\
&\mathbb{D}_t := (\boldsymbol{d}_{t,j})_{j=1,\ldots,3n_t+1} := (\boldsymbol{b}_{t,2}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,1}, \boldsymbol{b}_{t,n_t+1}, \ldots, \boldsymbol{b}_{t,3n_t+1}),\\
&\mathbb{D}^*_t := (\boldsymbol{d}^*_{t,j})_{j=1,\ldots,3n_t+1} := (\boldsymbol{b}^*_{t,2}, \ldots, \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,1}, \boldsymbol{b}^*_{t,n_t+1}, \ldots, \boldsymbol{b}^*_{t,3n_t+1}),\\
&\widehat{\mathbb{D}}_t := (\boldsymbol{d}_{t,1}, \ldots, \boldsymbol{d}_{t,n_t}, \boldsymbol{d}_{t,3n_t+1}), \quad \widehat{\mathbb{D}}^*_t := (\boldsymbol{d}^*_{t,1}, \ldots, \boldsymbol{d}^*_{t,n_t}, \boldsymbol{d}^*_{t,2n_t+1}, \ldots, \boldsymbol{d}^*_{t,3n_t}),
\end{aligned}$$

   for $t = 1, \ldots, d$. $\mathcal{B}_1$ obtains $\widehat{\mathbb{D}}_t$ and $\widehat{\mathbb{D}}^*_t$ from $\mathbb{B}_t$ and $\widehat{\mathbb{B}}^*_t$ in the Problem 1 instance, and returns $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{D}}_t\}_{t=0,..,d})$ to $\mathcal{A}$.
4. When a KeyGen query is issued for attribute sets Γ, $\mathcal{B}_1$ answers normal key sk_Γ computed using $\{\widehat{\mathbb{D}}^*_t\}_{t=0,..,d}$.
5. When $\mathcal{B}_1$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\mathbb{S} := (M, \rho)$ from $\mathcal{A}$, $\mathcal{B}_1$ calculates the challenge ciphertext $(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\ell, c_{d+1})$ as follows:

$$\boldsymbol{c}_0 := -s_0 \boldsymbol{e}_{\beta,0} + \zeta \boldsymbol{b}_{0,3},\ \ \boldsymbol{c}_i := \textstyle\sum_{j=1}^{n_t-1} c_{i,j} \boldsymbol{e}_{t,j+1} + c_{i,n_t} \boldsymbol{e}_{\beta,t,1} \ \text{ for } i = 1, \ldots, \ell,\ \ c_{d+1} := g_T^{\zeta} m^{(b)},$$

   where $b \xleftarrow{\mathsf{U}} \{0,1\}$, $\overrightarrow{f} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$, $\overrightarrow{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{f}^{\mathrm{T}}$, $s_0 := \overrightarrow{1} \cdot \overrightarrow{f}^{\mathrm{T}}$, $\theta_i, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, \ell$, $\overrightarrow{c}_i := s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i$ if $\rho(i) = (t, \overrightarrow{v}_i)$ or $\overrightarrow{c}_i := s_i \overrightarrow{v}_i$ if $\rho(i) = (t, \overrightarrow{v}_i)$ for $i = 1, \ldots, \ell$, and $\boldsymbol{e}_{\beta,0}, \boldsymbol{b}_{0,3}, \boldsymbol{e}_{\beta,t,1}, \{\boldsymbol{e}_{t,j}\}_{j=2,\ldots,n_t}$ are from the Problem 1 instance. $\mathcal{B}_1$ gives the challenge ciphertext to $\mathcal{A}$.
6. When a KeyGen query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_1$ executes the same procedure as that of step 4.
7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_1$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_1$ outputs $\beta' := 0$.

When $\beta = 0$, it is straightforward that the distribution by $\mathcal{B}_1$'s simulation is equivalent to that in Game 0. When $\beta = 1$, the distribution by $\mathcal{B}_1$'s simulation is equivalent to that in Game 1 except for the case that $s_0 = 0$ or there exists an $i \in \{1, \ldots, \ell\}$ such that $c_{i,n_t} = 0$, i.e., except with probability $(\ell + 1)/q \leq (d + 1)/q$ since $\ell \leq d$. □

Lemma 10 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}^+_{2,h}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}h)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h^+)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}^+_{2,h}}(\lambda) + (d + 3)/q$.*

Proof. In order to prove Lemma 10, we construct a probabilistic machine $\mathcal{B}^+_{2,h}$ against Problem 2 using an adversary $\mathcal{A}$ in a security game (Game 2-h or 2-h^+) as a black box as follows:

1. $\mathcal{B}^+_{2,h}$ is given a Problem 2 instance, $(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,..,d}, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,j}, \boldsymbol{e}_{t,j}\}_{t=1,..,d;j=1,..,n_t})$.
2. $\mathcal{B}^+_{2,h}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.

3. At the first step of the game, $\mathcal{B}^+_{2,h}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}'_t\}_{t=0,..,d})$ of Game 2-h (and 2-h^+), where $\widehat{\mathbb{B}}'_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}}'_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1})$ for $t = 1, .., d$, that are obtained from the Problem 2 instance.

4. When the ι-th key query is issued for attribute $\Gamma := \{(t, \overrightarrow{x}_t)\}$, $\mathcal{B}^+_{2,h}$ answers as follows:

   (a) When $1 \le \iota \le h$, $\mathcal{B}^+_{2,h}$ answers semi-functional key $(\boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\overrightarrow{x}_t)\in\Gamma})$ with Eq. (16), that is computed using $\{\mathbb{B}^*_t\}_{t=0,...,d}$ of the Problem 2 instance.

   (b) When $\iota = h+1$, $\mathcal{B}^+_{2,h}$ calculates $(\boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\overrightarrow{x}_t)\in\Gamma})$ using $\boldsymbol{b}^*_{0,3}, \boldsymbol{h}^*_{\beta,0}, \{\boldsymbol{h}^*_{\beta,t,j}\}_{t=1,..,d;j=1,..,n_t}$ of the Problem 2 instance as follows:

$$\boldsymbol{k}^*_0 := \boldsymbol{h}^*_{\beta,0} + \boldsymbol{b}^*_{0,3}, \quad \boldsymbol{k}^*_t := \textstyle\sum_{j=1}^{n_t} x_{t,j} \boldsymbol{h}^*_{\beta,t,j} \ \text{ for } (t, \overrightarrow{x}_t) \in \Gamma.$$

   (c) When $\iota \ge h+2$, $\mathcal{B}^+_{2,h}$ answers normal key $(\boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\overrightarrow{x}_t)\in\Gamma})$ with Eq. (9), that is computed using $\{\mathbb{B}^*_t\}_{t=0,...,d}$ of the Problem 2 instance.

5. When $\mathcal{B}^+_{2,h}$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\mathbb{S} := (M, \rho)$ from $\mathcal{A}$, $\mathcal{B}^+_{2,h}$ computes challenge ciphertext $(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_\ell, c_{d+1})$ as follows:

$$\begin{aligned}
&\pi'_t, \mu_t, g'_k, \widetilde{\mu}_k \xleftarrow{\cup} \mathbb{F}_q \ \text{ for } t = 1, \ldots, d;\ k = 1, \ldots, r,\\
&\widetilde{\boldsymbol{f}}_0 := \textstyle\sum_{k=1}^{r} (g'_k \boldsymbol{e}_0 + \widetilde{\mu}_k \boldsymbol{b}_{0,1}),\\
&\text{for } t = 1, \ldots, d;\ k = 1, \ldots, r;\ j = 1, \ldots, n_t;\\
&\quad \boldsymbol{f}_{t,j} := \pi'_t \boldsymbol{e}_{t,j} + \mu_t \boldsymbol{b}_{t,j}, \quad \widetilde{\boldsymbol{f}}_{t,k,j} := g'_k \boldsymbol{e}_{t,j} + \widetilde{\mu}_k \boldsymbol{b}_{t,j},\\
&\zeta \xleftarrow{\cup} \mathbb{F}_q, \quad \boldsymbol{c}_0 := -\widetilde{\boldsymbol{f}}_0 + \zeta \boldsymbol{b}_{0,3} + \boldsymbol{q}_0,\\
&\text{for } i = 1 \ldots, \ell,\\
&\quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \ \ \boldsymbol{c}_i := \textstyle\sum_{j=1}^{n_t} v_{i,j} \boldsymbol{f}_{t,j} + \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,1} + \boldsymbol{q}_i,\\
&\quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \ \ \boldsymbol{c}_i := \textstyle\sum_{j=1}^{n_t} v_{i,j} (\sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,j}) + \boldsymbol{q}_i,\\
&c_{d+1} := g_T^{\zeta} m^{(b)},
\end{aligned}$$

   where $(M_{i,k})_{i=1,...,\ell;k=1,...,r} := M$, $\boldsymbol{q}_0 \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}_{0,5} \rangle$, and $\boldsymbol{q}_i \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}_{t,3n_t+1} \rangle$ and $(\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{e}_0, \{\boldsymbol{e}_{t,j}\}_{t=1,...,d;j=1,...,n_t})$ is a part of the Problem 2 instance. $\mathcal{B}^+_{2,h}$ gives the challenge ciphertext to $\mathcal{A}$.

6. When a KeyGen query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}^+_{2,h}$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}^+_{2,h}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}^+_{2,h}$ outputs $\beta' := 0$.

Remark 2 $\widetilde{\boldsymbol{f}}_0, \boldsymbol{f}_{t,j}, \widetilde{\boldsymbol{f}}_{t,k,j}$ for $t = 1, \ldots, d; k = 1, \ldots, r; j = 1, \ldots, n_t$ calculated in the step 5 in the above simulation are expressed as:

$$\begin{aligned}
&\pi_t := \tau \pi'_t, \ \ \theta_t := \pi_t \omega + \mu_t, \ \ g_k := \tau g'_k, \ \ f_k := g_k \omega + \widetilde{\mu}_k,\\
&s_0 := \textstyle\sum_{k=1}^{r} f_k, \ \ a_0 := \sum_{k=1}^{r} g_k, \ \ w_0 := a_0 / u_0 \ (= a_0 z_0),\\
&\widetilde{\boldsymbol{f}}_0 = (s_0, w_0, 0, 0, 0)_{\mathbb{B}_0},
\end{aligned}$$

$$\begin{array}{lcccccc}
 & & \overbrace{\qquad}^{n_t} & \overbrace{\qquad}^{n_t} & \overbrace{\qquad}^{n_t} & \overbrace{\ }^{1} & \\
\boldsymbol{f}_{t,j} := & (& \theta_t \overrightarrow{e}_{t,j}, & \pi_t \overrightarrow{z}_{t,j}, & 0^{n_t}, & 0 &)_{\mathbb{B}_t},\\
\widetilde{\boldsymbol{f}}_{t,k,j} := & (& f_k \overrightarrow{e}_{t,j}, & g_k \overrightarrow{z}_{t,j}, & 0^{n_t}, & 0 &)_{\mathbb{B}_t},
\end{array}$$

where $\tau, \omega, u_0, \{\overrightarrow{e}_{t,j}, \overrightarrow{z}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,n_t}$ are defined in Problem 2. Note that variables $\{\theta_t, \pi_t\}_{t=1,\ldots,d}$, $\{f_k, g_k\}_{k=1,\ldots,r}$ are independently and uniformly distributed. Therefore, $\{\boldsymbol{c}_i\}_{i=0,\ldots,\ell}$ are distributed as (11) and (15) except $w_0 := a_0/r_0$, i.e., $w_0 r_0 = a_0$, using a_0 and $r_0 := u_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ in $\boldsymbol{k}_0^*$ (Eq. (14)).

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

Proof. It is clear that $\mathcal{B}_{2,h}^+$'s simulation of the public-key generation (step 3) and the ι-th key query's answer for $\iota \neq h+1$ (cases (a) and (c) of step 4) is perfect, i.e., exactly the same as the Setup and the KeyGen oracle in Game 2-h and Game 2-h^+.

Therefore, to prove this lemma we will show that the joint distribution of the $(h+1)$-th key query's answer and the challenge ciphertext by $\mathcal{B}_{2,h}^+$'s simulation given a Problem 2 instance with β is equivalent to that in Game 2-h (resp. Game 2-h^+), when $\beta = 0$ (resp. $\beta = 1$).

When $\beta = 0$, it is straightforward to show that they are equivalent except that δ defined in Problem 2 is zero or there exists $i \in \{0, \ldots, \ell\}$ such that $\overrightarrow{w}_i = \overrightarrow{0}$ with $\rho(i) = (t, \overrightarrow{v}_i)$ or $\overrightarrow{\overline{w}}_i = \overrightarrow{0}$ with $\rho(i) = \neg(t, \overrightarrow{v}_i)$, where $\overrightarrow{w}_i$ and $\overrightarrow{\overline{w}}_i$ are defined in Eqs. (11) and (12), i.e., except with probability $(\ell+2)/q \leq (d+2)/q$ since $\ell \leq d$.

When $\beta = 1$, the distribution by $\mathcal{B}_{2,h}^+$'s simulation is Eq. (14) for the key and Eqs. (11), (13), and (15) for the challenge ciphertext, where the distribution is the same as that defined in these equations except $w_0 := a_0/r_0$, i.e., $w_0 r_0 = a_0$, using $a_0 := \overrightarrow{1} \cdot \overrightarrow{g}^{\mathrm{T}}$ and $r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ in $\boldsymbol{k}_0^*$ (Eq. (14)) from Remark 2. The corresponding distribution in Game 2-h^+ is Eq. (14) and Eqs. (11), (13), and (15) where $r_0, w_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ as defined in the equations.

Moreover, similarly as in the proof of Claim 1, we can show that a_0 is uniformly and independently distributed from the other variables in the joint distribution of $\mathcal{B}_{2,h}^+$'s simulation.

Therefore, the view of adversary $\mathcal{A}$ in the game simulated by $\mathcal{B}_{2,h}^+$ given a Problem 2 instance with $\beta = 1$ is the same as that in Game 2-h^+ except that δ defined in Problem 2 is zero i.e., except with probability $1/q$. □

This completes the proof of Lemma 10. □

Lemma 11 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2,h+1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h+1))}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2,h+1}}^{\mathsf{P2}}(\lambda) + (d+3)/q$.*

Proof. The proof of Lemma 11 is similar to that of Lemma 6. □

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

Proof. The proof of Lemma 12 is similar to that of Lemma 7. □

Lemma 13 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$.*

8 Fully Secure (CCA Secure) CP-FE Scheme

We can transform the proposed KP-FE and CP-FE schemes to CCA secure KP-FE and CP-FE schemes, respectively, by using the Canetti-Halevi-Katz (CHK) transformation [11] or the Boneh-Katz (BK) transformation [8].

This section shows a CCA secure CP-FE scheme, that is modified from the CP-FE scheme in Section 7 through the CHK transformation, in which a strongly unforgeable one-time signature scheme $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ is employed.

We can similarly apply the CHK transformation to our KP-FE scheme and the BK transformation to the FE schemes.

8.1 Strongly Unforgeable One-Time Signatures

Definition 13 (Signatures) *A signature scheme consists of three algorithms.*

Gen *This is a randomized algorithm that takes as input the security parameter* 1^λ*. It outputs a verification key* verk *and a signing key* sigk*.*

Sig *This is a randomized algorithm that takes as input a signing key* sigk *and a message* m *(in some implicit message space). It outputs a signature* σ*.*

Ver *This takes as input a verification key* verk*, a message* m*, and a signature* σ*, and outputs a boolean value* $\mathsf{accept} := 1$ *or* $\mathsf{reject} := 0$*.*

A signature scheme should have the following correctness property: for all $(\mathsf{verk}, \mathsf{sigk}) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^\lambda)$, all messages m, and all signatures $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}, m)$, it holds that $1 = \mathsf{Ver}(\mathsf{verk}, m, \sigma)$ with probability 1.

Definition 14 (Strongly Unforgeable One-Time Signatures) *For an adversary, we define* $\mathsf{Adv}^{\mathsf{OS},\mathsf{SUF}}_{\mathcal{A}}(\lambda)$ *to be the success probability in the following experiment for any security parameter* λ*. A signature scheme is a strongly unforgeable one-time signature scheme if the success probability of any polynomial-time adversary is negligible:*

1. *Run* $(\mathsf{verk}, \mathsf{sigk}) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^\lambda)$ *and give* verk *to the adversary.*
2. *The adversary is given access to signing oracle* $\mathsf{Sig}(\mathsf{sigk}, \cdot)$ *at most once. We denote the pair of message and signature by* (m, σ) *if the signing oracle is queried.*
3. *At the end, the adversary outputs* (m', σ')*.*

We say the adversary succeeds if $\mathsf{Ver}(\mathsf{verk}, m', \sigma') = 1$ *and* $(m', \sigma') \neq (m, \sigma)$ *(assuming the signing oracle is queried).*

8.2 Construction

$\widetilde{\rho} : \{1, \ldots, \ell\} \to \{1, \ldots, d\}$ is defined at the start of Section 6. In the proposed scheme, we assume that $\widetilde{\rho}$ is injective for $\mathbb{S} := (M, \rho)$.

In the description of the scheme, we assume that an input vector, $\overrightarrow{x}_t := (x_{t,1}, \ldots, x_{t,n_t})$, is normalized such that $x_{t,1} := 1$. (If $\overrightarrow{x}_t$ is not normalized, change it to a normalized one by $(1/x_{t,1}) \cdot \overrightarrow{x}_t$, assuming that $x_{t,1}$ is non-zero). In addition, we assume that input vector $\overrightarrow{v}_t := (v_{i,1}, \ldots, v_{i,n_t})$ satisfies that $v_{i,n_t} \neq 0$.

Random dual bases generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n})$ is defined at the end of Section 2. We refer to Section 1.3 for notations on DPVS, e.g., $(x_1, \ldots, x_N)_{\mathbb{B}}, (y_1, \ldots, y_N)_{\mathbb{B}^*}$ for $x_i, y_i \in \mathbb{F}_q$, and $\overrightarrow{e}_{t,j}$.

For simplicity, we assume verification key verk is an element in $\mathbb{F}_q$. (We can extend the construction to verification key over any distribution D by first hashing verk using a collision resistant hash $H : \mathsf{D} \to \mathbb{F}_q$.)

$\mathsf{Setup}(1^\lambda,\ \overrightarrow{n} := (d; n_1, \ldots, n_d))$

$n_{d+1} := 2, \quad \overrightarrow{n}' := (d+1; \{n_t\}_{t=1,\ldots,d+1}), \quad (\mathsf{param}_{\overrightarrow{n}'}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d+1}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}'),$

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$, $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1})$ for $t = 1, \ldots, d+1$,

$\widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4})$, $\widehat{\mathbb{B}}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,2n_t+1}, \ldots, \boldsymbol{b}^*_{t,3n_t})$ for $t = 1, \ldots, d+1$,

$\mathsf{pk} := (1^\lambda, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d+1})$, $\mathsf{sk} := \{\widehat{\mathbb{B}}^*_t\}_{t=0,\ldots,d+1}$.

return pk, sk.

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma := \{(t, \overrightarrow{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}) \mid 1 \le t \le d,\ x_{t,1} := 1\})$

$\delta, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ such that $(t, \overrightarrow{x}_t) \in \Gamma$, $\overrightarrow{\varphi}_{d+1,1}, \overrightarrow{\varphi}_{d+1,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$

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

$\boldsymbol{k}^*_t := (\overbrace{\delta \overrightarrow{x}_t,}^{n_t} \overbrace{0^{n_t},}^{n_t} \overbrace{\overrightarrow{\varphi}_t,}^{n_t} \overbrace{0}^{1})_{\mathbb{B}^*_t}$ for $(t, \overrightarrow{x}_t) \in \Gamma$,

$\boldsymbol{k}^*_{d+1,1} := (\delta(1,0),\ 0^2,\ \overrightarrow{\varphi}_{d+1,1},\ 0)_{\mathbb{B}^*_{d+1}}$, $\boldsymbol{k}^*_{d+1,2} := (\delta(0,1),\ 0^2,\ \overrightarrow{\varphi}_{d+1,2},\ 0)_{\mathbb{B}^*_{d+1}}$,

$\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, \boldsymbol{k}^*_{d+1,1}, \boldsymbol{k}^*_{d+1,2})$

return sk_Γ.

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

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

$s_{\ell+1}, \eta_0, \eta_i, \theta_i, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, \ell+1$, $(\mathsf{sigk}, \mathsf{verk}) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^\lambda)$,

$\boldsymbol{c}_0 := (-s_0 - s_{\ell+1},\ 0,\ \zeta,\ 0,\ \eta_0)_{\mathbb{B}_0}$,

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

if $\rho(i) = (t, \overrightarrow{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\})$ $(v_{i,n_t} \neq 0)$,

$\boldsymbol{c}_i := (\overbrace{s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i,}^{n_t} \overbrace{0^{n_t},}^{n_t} \overbrace{0^{n_t},}^{n_t} \overbrace{\eta_i}^{1})_{\mathbb{B}_t}$,

if $\rho(i) = \neg(t, \overrightarrow{v}_i)$,

$\boldsymbol{c}_i := (\overbrace{s_i \overrightarrow{v}_i,}^{n_t} \overbrace{0^{n_t},}^{n_t} \overbrace{0^{n_t},}^{n_t} \overbrace{\eta_i}^{1})_{\mathbb{B}_t}$,

$\boldsymbol{c}_{\ell+1} := (s_{\ell+1} - \theta_{\ell+1} \cdot \mathsf{verk},\ \theta_{\ell+1},\ 0^2,\ 0^2,\ \eta_{\ell+1})_{\mathbb{B}_{d+1}}$,

$c_{d+2} := g_T^\zeta m$, $C := (\mathbb{S}, \boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1}, c_{d+2})$, $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}, C)$,

return $\mathsf{ct}_\mathbb{S} := (\mathsf{verk}, C, \sigma)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, \boldsymbol{k}^*_{d+1,1}, \boldsymbol{k}^*_{d+1,2}),\ \mathsf{ct}_\mathbb{S} := (\mathsf{verk}, (\mathbb{S}, \boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1}, c_{d+2}), \sigma))$

if $\mathsf{Ver}(\mathsf{verk}, C, \sigma) \neq 1$, return $\perp$, where $C := (\mathbb{S}, \boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1}, c_{d+2})$,

if $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \overrightarrow{x}_t)\}$, then compute I and $\{\alpha_i\}_{i\in I}$ such that

$\overrightarrow{1} = \sum_{i\in I} \alpha_i M_i$, where M_i is the i-th row of M, and

$I \subseteq \{i \in \{1, \ldots, \ell\} \mid [\rho(i) = (t, \overrightarrow{v}_i) \ \wedge\ (t, \overrightarrow{x}_t) \in \Gamma \ \wedge\ \overrightarrow{v}_i \cdot \overrightarrow{x}_t = 0]$

$\vee\ [\rho(i) = \neg(t, \overrightarrow{v}_i) \ \wedge\ (t, \overrightarrow{x}_t) \in \Gamma \ \wedge\ \overrightarrow{v}_i \cdot \overrightarrow{x}_t \neq 0]\ \}$.

$\boldsymbol{s}^*_{d+1} := \boldsymbol{k}^*_{d+1,1} + \mathsf{verk} \cdot \boldsymbol{k}^*_{d+1,2}$,

$K := e(\boldsymbol{c}_0, \boldsymbol{k}^*_0) \prod_{i\in I \ \wedge\ \rho(i)=(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i} \cdot \prod_{i\in I \ \wedge\ \rho(i)=\neg(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)} \cdot e(\boldsymbol{c}_{\ell+1}, \boldsymbol{s}^*_{d+1})$,

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

[Correctness] If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \overrightarrow{x}_t)\}$,

$$e(\boldsymbol{c}_0, \boldsymbol{k}^*_0) \textstyle\prod_{i\in I \ \wedge\ \rho(i)=(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i} \cdot \prod_{i\in I \ \wedge\ \rho(i)=\neg(t,\overrightarrow{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)} \cdot e(\boldsymbol{c}_{\ell+1}, \boldsymbol{s}^*_{d+1})$$

$$= g_T^{\delta(-s_0-s_{\ell+1})+\zeta} \prod_{i\in I \ \wedge \ \rho(i)=(t,\overrightarrow{v}_i)} g_T^{\delta\alpha_i s_i} \prod_{i\in I \ \wedge \ \rho(i)=\neg(t,\overrightarrow{v}_i)} g_T^{\delta\alpha_i s_i(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)/(\overrightarrow{v}_i\cdot\overrightarrow{x}_t)} g_T^{\delta s_{\ell+1}}$$
$$= g_T^{\delta(-s_0-s_{\ell+1}+\sum_{i\in I}\alpha_i s_i+s_{\ell+1})+\zeta} = g_T^{\zeta}.$$

8.3 Security

Theorem 3 *The proposed CP-FE scheme is adaptively payload-hiding against chosen-ciphertext attacks under the DLIN assumption provided that the underlying signature scheme* $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ *is a strongly unforgeable one-time signature scheme.*

For any adversary $\mathcal{A}$*, there exist probabilistic machines* $\mathcal{E}_1, \mathcal{E}_{2,h}^+, \mathcal{E}_{2,h+1}$ $(h = 0, \ldots, \nu_1 - 1)$, $\mathcal{E}_{3,h}, \mathcal{E}_{4,h}$ $(h = 1, \ldots, \nu_2)$*, whose running times are essentially the same as that of* $\mathcal{A}$*, such that for any security parameter* λ*,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CP\text{-}FE,CCA\text{-}PH}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{h=0}^{\nu_1-1}\left(\mathsf{Adv}_{\mathcal{E}_{2,h}^+}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{2,h+1}}^{\mathsf{DLIN}}(\lambda)\right)$$
$$+ \sum_{h=1}^{\nu_2}\left(\mathsf{Adv}_{\mathcal{E}_{3,h}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{4,h}}^{\mathsf{OS,SUF}}(\lambda)\right) + \epsilon,$$

where ν_1 *is the maximum number of* $\mathcal{A}$*'s* KeyGen *queries,* ν_2 *is the maximum number of* $\mathcal{A}$*'s* Dec *queries, and* $\epsilon := (2d\nu_1 + 16\nu_1 + 8\nu_2 + d + 10)/q$*.*

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

Game 0 : Original game. That is, the reply to a KeyGen query for $\Gamma := \{(t, \overrightarrow{x}_t)\}$ are:

$$\boldsymbol{k}_0^* := (\delta,\ \boxed{0},\ 1,\ \varphi_0,\ 0)_{\mathbb{B}_0^*},$$
$$\boldsymbol{k}_t^* := (\delta\overrightarrow{x}_t,\ \boxed{0^{n_t}},\ \overrightarrow{\varphi}_t,\ 0)_{\mathbb{B}_t} \ \text{ for } (t, \overrightarrow{x}_t) \in \Gamma,$$
$$\boldsymbol{k}_{d+1,1}^* := (\delta(1,0),\ 0^2,\ \overrightarrow{\varphi}_{d+1,1},\ 0)_{\mathbb{B}_{d+1}^*}, \quad \boldsymbol{k}_{d+1,2}^* := (\delta(0,1),\ 0^2,\ \overrightarrow{\varphi}_{d+1,2},\ 0)_{\mathbb{B}_{d+1}^*},$$

where $\delta \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times$, $\varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $(t, \overrightarrow{x}_t) \in \Gamma$, $\overrightarrow{\varphi}_{d+1,1}, \overrightarrow{\varphi}_{d+1,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$. In answering Dec query for $\mathsf{ct}_{\mathbb{S}} := (\mathsf{verk}, (\mathbb{S}, \boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1}, c_{d+2}), \sigma)$ when $\mathsf{Ver}(\mathsf{verk}, C, \sigma) = 1$, where $C := (\mathbb{S}, \boldsymbol{c}_0, \ldots, \boldsymbol{c}_{\ell+1}, c_{d+2})$, the used key for $\Gamma := \{(t, \overrightarrow{x}_t)\}$ such that $\mathbb{S}$ accepts Γ are:

$$\boldsymbol{k}_0^* := (\widetilde{\delta},\ \boxed{0},\ 1,\ \widetilde{\varphi}_0,\ 0)_{\mathbb{B}_0^*},$$
$$\boldsymbol{k}_t^* := (\widetilde{\delta}\overrightarrow{x}_t,\ 0^{n_t},\ \overrightarrow{\widetilde{\varphi}}_t,\ 0)_{\mathbb{B}_t} \ \text{ for } (t, \overrightarrow{x}_t) \in \Gamma,$$
$$\boldsymbol{s}_{d+1}^* := (\widetilde{\delta}(1, \mathsf{verk}),\ \boxed{0^2},\ \overrightarrow{\widetilde{\varphi}}_{d+1},\ 0)_{\mathbb{B}_{d+1}^*},$$

where $\widetilde{\delta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times$, $\widetilde{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{\widetilde{\varphi}}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $(t, \overrightarrow{x}_t) \in \Gamma$, $\overrightarrow{\widetilde{\varphi}}_{d+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$.

The challenge ciphertext for challenge plaintexts $(m^{(0)}, m^{(1)})$ and access structure $\mathbb{S} := (M, \rho)$ is:

$$\boldsymbol{c}_0 := (-s_0 - s_{\ell+1},\ \boxed{0},\ \boxed{\zeta},\ 0,\ \eta_0)_{\mathbb{B}_0},$$
$$\text{for } i = 1, \ldots, \ell,$$
$$\quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \quad \boldsymbol{c}_i := (s_i\overrightarrow{e}_{t,1} + \theta_i\overrightarrow{v}_i,\ \boxed{0^{n_t}},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t},$$
$$\quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \quad \boldsymbol{c}_i := (s_i\overrightarrow{v}_i,\ \boxed{0^{n_t}},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t},$$
$$\boldsymbol{c}_{\ell+1} := (s_{\ell+1} - \theta_{\ell+1}\cdot\mathsf{verk},\ \theta_{\ell+1},\ \boxed{0^2},\ 0^2,\ \eta_{\ell+1})_{\mathbb{B}_{d+1}},$$
$$c_{d+2} := g_T^{\zeta} m^{(b)},$$

where $\overrightarrow{f} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$, $\overrightarrow{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{f}^{\mathrm{T}}$, $s_0 := \overrightarrow{1} \cdot \overrightarrow{f}^{\mathrm{T}}$, $s_{\ell+1}, \zeta, \eta_0, \eta_i, \theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, \ell+1$, and $\overrightarrow{e}_{t,1} := (1, 0, \ldots, 0) \in \mathbb{F}_q^{n_t}$.

Game 1 : Same as Game 0 except that the challenge ciphertext for challenge plaintexts $(m^{(0)}, m^{(1)})$ and access structure $\mathbb{S} := (M, \rho)$ is:

$$\begin{aligned}
&\boldsymbol{c}_0 := (-s_0 - s_{\ell+1},\ \boxed{w_0},\ \zeta,\ 0,\ \eta_0)_{\mathbb{B}_0},\\
&\text{for } i = 1, \ldots, \ell+1,\\
&\quad \text{if } \rho(i) = (t, \overrightarrow{v}_i),\ \ \boldsymbol{c}_i := (s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i,\ \boxed{\overrightarrow{w}_i},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t},\\
&\quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i),\ \ \boldsymbol{c}_i := (s_i \overrightarrow{v}_i,\ \boxed{\overrightarrow{\overrightarrow{w}}_i},\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t},\\
&\boldsymbol{c}_{\ell+1} := (s_{\ell+1} - \theta_{\ell+1} \cdot \mathsf{verk},\ \theta_{\ell+1},\ \boxed{\overrightarrow{w}_{\ell+1}},\ 0^2,\ \eta_{\ell+1})_{\mathbb{B}_{d+1}},
\end{aligned}$$

where $w_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{w}_i, \overrightarrow{\overrightarrow{w}}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $i = 1, \ldots, \ell$, $\overrightarrow{w}_{\ell+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, and all the other variables are generated as in Game 0.

Game 2-h^+ ($h = 0, \ldots, \nu_1 - 1$) and **Game 2-$(h+1)$ ($h = 0, \ldots, \nu_1 - 1$)** are the same as **Game 2-h^+** and **Game 2-$(h+1)$** in the proof of Theorem 2, respectively.

Game 3-h ($h = 1, \ldots, \nu_2$) : Game 3-0 is Game 2-ν_1. Game 3-h is the same as Game 3-$(h-1)$ except that $\boldsymbol{k}_0^*, \boldsymbol{s}_{d+1}^*$ of the key used in answering the h-th Dec query when $\mathsf{Ver}(\mathsf{verk}, C, \sigma) = 1$ are:

$$\begin{aligned}
&\boldsymbol{k}_0^* := (\widetilde{\delta},\ \boxed{\widetilde{r}_0},\ 1,\ \widetilde{\varphi}_0,\ 0)_{\mathbb{B}_0^*},\\
&\boldsymbol{s}_{d+1}^* := (\widetilde{\delta}(1, \mathsf{verk}),\ \boxed{\overrightarrow{\widetilde{r}}_{d+1}},\ \overrightarrow{\widetilde{\varphi}}_{d+1},\ 0)_{\mathbb{B}_{d+1}^*},
\end{aligned}$$

where $\widetilde{r}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{\widetilde{r}}_{d+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, and all the other variables are generated as in Game 3-$(h-1)$.

Game 4 : Same as Game 3-ν_2 except that $\boldsymbol{c}_0$ in the challenge ciphertext is:

$$\boldsymbol{c}_0 := (-s_0 - s_{\ell+1},\ w_0,\ \boxed{\zeta'},\ 0,\ \eta_0)_{\mathbb{B}_0},$$

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

We follow the argument in [11] used for the chosen ciphertext security, and the rest of the proof of Theorem 3 is similar to that of Theorem 2.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$ be $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CP\text{-}FE,CCA\text{-}PH}}(\lambda)$ in Game 0, and $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $1, 2\text{-}h, 2\text{-}h^+, 3\text{-}h, 4$, respectively. ($\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda) = 0$.) We can evaluate the gaps between pairs of $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h+1))}(\lambda)$ for $h = 0, \ldots, \nu_1 - 1$ using Problems 3 and 4 (given in Appendix D) as in the proof of Theorem 2.

Moreover, we can evaluate the gaps between pairs of $\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h)}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h+1))}(\lambda)$ for $h = 0, \ldots, \nu_2 - 1$ using Problem 5 in Appendix D. □

References

[1] Beimel, A., Secure schemes for secret sharing and key distribution. PhD Thesis, Israel Institute of Technology, Technion, Haifa, Israel, (1996)

[2] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Press, Los Alamitos (2007)

[3] Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)

[4] Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)

[5] Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005)

[6] Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)

[7] Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption scheme. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455–470. Springer, Heidelberg (2008)

[8] Boneh, D., Katz, J., Improved efficiency for CCA-secure cryptosystems built using identity based encryption. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 87–103. Springer, Heidelberg (2005)

[9] Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007)

[10] Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer, Heidelberg (2006)

[11] Canetti, R., Halevi S., Katz J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004)

[12] Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) IMA Int. Conf. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001)

[13] Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)

[14] Gentry, C., Halevi, S.: Hierarchical identity-based encryption with polynomially many levels. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 437–456. Springer, Heidelberg (2009)

[15] Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002)

[16] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communication Security 2006, pp. 89–98, ACM, New York (2006)

[17] Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)

[18] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010)

[19] Lewko, A.B., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010)

[20] Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 57–74. Springer, Heidelberg (2008)

[21] Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products, In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Heidelberg (2009)

[22] Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: ACM Conference on Computer and Communication Security 2007, pp. 195–203, ACM, New York (2007)

[23] Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. In: ACM Conference on Computer and Communication Security 2006, pp. 99–112, ACM, New York (2006)

[24] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)

[25] Shi, E., Waters, B.: Delegating capability in predicate encryption systems. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldørsson, M.M., Ingølfsdøttir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, pp. 560–578. Springer, Heidelberg (2008)

[26] Waters, B.: Efficient identity based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)

[27] Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. ePrint, IACR, `http://eprint.iacr.org/2008/290`

[28] Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)

A Dual Pairing Vector Spaces (DPVS)

A.1 Summary

We now briefly explain our approach, DPVS, constructed on symmetric pairing groups $(q, \mathbb{G}, \mathbb{G}_T, G, e)$, where q is a prime, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order q, G is a generator of $\mathbb{G}$, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerate bilinear pairing operation, and $e(G, G) \neq 1$. Here we denote the group operation of $\mathbb{G}$ by addition and $\mathbb{G}_T$ by multiplication, respectively. Note that this construction also works on *asymmetric* pairing groups (in this paper, we use symmetric pairing groups for simplicity of description).

Vector space $\mathbb{V}$: $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$, whose element is expressed by N-dimensional vector, $\boldsymbol{x} := (x_1 G, \ldots, x_N G)$ ($x_i \in \mathbb{F}_q$ for $i = 1, \ldots, N$).

Canonical base $\mathbb{A}$: $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$ of $\mathbb{V}$, where $\boldsymbol{a}_1 := (G, 0, \ldots, 0), \boldsymbol{a}_2 := (0, G, 0, \ldots, 0)$, $\ldots, \boldsymbol{a}_N := (0, \ldots, 0, G)$.

Pairing operation: $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(x_i G, y_i G) = e(G, G)^{\sum_{i=1}^{N} x_i y_i} = e(G, G)^{\overrightarrow{x} \cdot \overrightarrow{y}} \in \mathbb{G}_T$, where $\boldsymbol{x} := (x_1 G, \ldots, x_N G) = x_1 \boldsymbol{a}_1 + \cdots + x_N \boldsymbol{a}_N \in \mathbb{V}$, $\boldsymbol{y} := (y_1 G, \ldots, y_N G) = y_1 \boldsymbol{a}_1 + \cdots + y_N \boldsymbol{a}_N \in \mathbb{V}$, $\overrightarrow{x} := (x_1, \ldots, x_N)$ and $\overrightarrow{y} := (y_1, \ldots, y_N)$. Here, $\boldsymbol{x}$ and $\boldsymbol{y}$ can be expressed by coefficient vector over basis $\mathbb{A}$ such that $(x_1, \ldots, x_N)_{\mathbb{A}} = (\overrightarrow{x})_{\mathbb{A}} := \boldsymbol{x}$ and $(y_1, \ldots, y_N)_{\mathbb{A}} = (\overrightarrow{y})_{\mathbb{A}} := \boldsymbol{y}$.

Base change: Canonical basis $\mathbb{A}$ is changed to basis $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ of $\mathbb{V}$ using a uniformly chosen (regular) linear transformation, $X := (\chi_{i,j}) \xleftarrow{\cup} GL(N, \mathbb{F}_q)$, such that $\boldsymbol{b}_i = \sum_{j=1}^{N} \chi_{i,j} \boldsymbol{a}_j$, $(i = 1, \ldots, N)$. $\mathbb{A}$ is also changed to basis $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$ of $\mathbb{V}$, such that $(\vartheta_{i,j}) := (X^T)^{-1}$, $\boldsymbol{b}_i^* = \sum_{j=1}^{N} \vartheta_{i,j} \boldsymbol{a}_j$, $(i = 1, \ldots, N)$. We see that $e(\boldsymbol{b}_i, \boldsymbol{b}_j^*) = e(G, G)^{\delta_{i,j}}$, ($\delta_{i,j} = 1$ if $i = j$, and $\delta_{i,j} = 0$ if $i \neq j$) i.e., $\mathbb{B}$ and $\mathbb{B}^*$ are dual orthonormal bases of $\mathbb{V}$.

Here, $\boldsymbol{x} := x_1 \boldsymbol{b}_1 + \cdots + x_N \boldsymbol{b}_N \in \mathbb{V}$ and $\boldsymbol{y} := y_1 \boldsymbol{b}_1^* + \cdots + y_N \boldsymbol{b}_N^* \in \mathbb{V}$ can be expressed by coefficient vectors over $\mathbb{B}$ and $\mathbb{B}^*$ such that $(x_1, \ldots, x_N)_{\mathbb{B}} = (\overrightarrow{x})_{\mathbb{B}} := \boldsymbol{x}$ and $(y_1, \ldots, y_N)_{\mathbb{B}^*} = (\overrightarrow{y})_{\mathbb{B}^*} := \boldsymbol{y}$, and $e(\boldsymbol{x}, \boldsymbol{y}) = e(G, G)^{\sum_{i=1}^{N} x_i y_i} = e(G, G)^{\overrightarrow{x} \cdot \overrightarrow{y}} \in \mathbb{G}_T$.

Intractable problem: One of the most natural decisional problems in this approach is the decisional subspace problem [20]. It is to tell $\boldsymbol{v} := v_{N_2+1} \boldsymbol{b}_{N_2+1} + \cdots + v_{N_1} \boldsymbol{b}_{N_1}$ $(= (0, \ldots, 0, v_{N_2+1}, \ldots, v_{N_1})_{\mathbb{B}})$, from $\boldsymbol{u} := v_1 \boldsymbol{b}_1 + \cdots + v_{N_1} \boldsymbol{b}_{N_1}$ $(= (v_1, \ldots, v_{N_1})_{\mathbb{B}})$, where $(v_1, \ldots, v_{N_1}) \xleftarrow{\cup} \mathbb{F}_q^{N_1}$ and $N_2 + 1 < N_1$.

Trapdoor: Although the decisional subspace problem is assumed to be intractable, it can be efficiently solved using *trapdoor* $\boldsymbol{t}^* \in \mathsf{span}\langle \boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_{N_2}^* \rangle$. Given $\boldsymbol{v} := v_{N_2+1} \boldsymbol{b}_{N_2+1} + \cdots + v_{N_1} \boldsymbol{b}_{N_1}$ or $\boldsymbol{u} := v_1 \boldsymbol{b}_1 + \cdots + v_{N_1} \boldsymbol{b}_{N_1}$, we can tell $\boldsymbol{v}$ from $\boldsymbol{u}$ using $\boldsymbol{t}^*$ since $e(\boldsymbol{v}, \boldsymbol{t}^*) = 1$ and $e(\boldsymbol{u}, \boldsymbol{t}^*) \neq 1$ with high probability.

Advantage of this approach: Higher dimensional vector treatment of bilinear pairing groups have been already employed in literature especially in the areas of IBE, ABE and BE (e.g., [5, 2, 7, 10, 16, 24]). For example, in a typical vector treatment, two vector forms of $P := (x_1 G, \ldots, x_N G)$ and $Q := (y_1 G, \ldots, y_N G)$ are set and pairing for P and Q is operated as $e(P, Q) := \prod_{i=1}^{N} e(x_i G, y_i G)$. Such treatment can be rephrased in this approach such that $P = x_1 \boldsymbol{a}_1 + \cdots + x_N \boldsymbol{a}_N$ $(= (x_1, \ldots, x_N)_{\mathbb{A}})$, and $Q = y_1 \boldsymbol{a}_1 + \cdots + y_N \boldsymbol{a}_N$ $(= (y_1, \ldots, y_N)_{\mathbb{A}})$ over canonical basis $\mathbb{A}$.

The major drawback of this approach is the easily *decomposable* property over $\mathbb{A}$ (i.e., the decisional subspace problem is easily solved). That is, it is easy to decompose $x_i \boldsymbol{a}_i = (0, \ldots, 0, x_i G, 0, \ldots, 0)$ from $P := x_1 \boldsymbol{a}_1 + \cdots x_N \boldsymbol{a}_N = (x_1 G, \ldots, x_N G)$.

In contrast, our approach employs basis $\mathbb{B}$, which is linearly transformed from $\mathbb{A}$ using a secret random matrix $X \in \mathbb{F}_q^{n \times n}$. A remarkable property over $\mathbb{B}$ is that it seems hard to decompose $x_i \boldsymbol{b}_i$ from $P' := x_1 \boldsymbol{b}_1 + \cdots x_N \boldsymbol{b}_N$ (and the decisional subspace problem seems intractable). In addition, the secret matrix X (and the dual orthonormal basis $\mathbb{B}^*$ of $\mathbb{V}$) can be used as a source of the trapdoors to the decomposability (and distinguishability for the decisional subspace problem through the pairing operation over $\mathbb{B}$ and $\mathbb{B}^*$ as mentioned

above). The hard decomposability (and indistinguishability) and its trapdoors are ones of the key tricks in this paper. Note that composite order pairing groups are often employed with similar tricks such as hard decomposability (and indistinguishability) of a composite order group to the prime order subgroups and its trapdoors through factoring (e.g., [17, 25]).

A.2 Dual Pairing Vector Spaces by Direct Product of Asymmetric Pairing Groups

Definition 15 *"Asymmetric bilinear pairing groups"* $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, e)$ *are a tuple of a prime* q*, cyclic additive groups* $\mathbb{G}_1, \mathbb{G}_2$ *and multiplicative group* $\mathbb{G}_T$ *of order* q*,* $G_1 \neq 0 \in \mathbb{G}_1, G_2 \neq 0 \in \mathbb{G}_2$*, and a polynomial-time computable nondegenerate bilinear pairing* $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ *i.e.,* $e(sG_1, tG_2) = e(G_1, G_2)^{st}$ *and* $e(G_1, G_2) \neq 1$*.*

Let $\mathcal{G}_{\mathsf{bpg}}$ *be an algorithm that takes input* 1^λ *and outputs a description of bilinear pairing groups* $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, e)$ *with security parameter* λ*.*

Definition 16 *"Dual pairing vector spaces (DPVS)"* $(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*, e)$ *by direct product of asymmetric pairing groups* $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, e)$ *are a tuple of a prime* q*, two* N*-dimensional vector spaces* $\mathbb{V} := \overbrace{\mathbb{G}_1 \times \cdots \times \mathbb{G}_1}^{N}$ *and* $\mathbb{V}^* := \overbrace{\mathbb{G}_2 \times \cdots \times \mathbb{G}_2}^{N}$ *over* $\mathbb{F}_q$*, a cyclic group* $\mathbb{G}_T$ *of order* q*, and their canonical bases i.e.,* $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$ *of* $\mathbb{V}$ *and* $\mathbb{A}^* := (\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_N^*)$ *of* $\mathbb{V}^*$*, where* $\boldsymbol{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G_1, \overbrace{0, \ldots, 0}^{N-i})$ *and* $\boldsymbol{a}_i^* := (\overbrace{0, \ldots, 0}^{i-1}, G_2, \overbrace{0, \ldots, 0}^{N-i})$*, and pairing* $e : \mathbb{V} \times \mathbb{V}^* \to \mathbb{G}_T$*.*

The pairing is defined by $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(D_i, H_i) \in \mathbb{G}_T$ *where* $\boldsymbol{x} := (D_1, \ldots, D_N) \in \mathbb{V}$ *and* $\boldsymbol{y} := (H_1, \ldots, H_N) \in \mathbb{V}^*$*. This is nondegenerate bilinear i.e.,* $e(s\boldsymbol{x}, t\boldsymbol{y}) = e(\boldsymbol{x}, \boldsymbol{y})^{st}$ *and if* $e(\boldsymbol{x}, \boldsymbol{y}) = 1$ *for all* $\boldsymbol{y} \in \mathbb{V}$*, then* $\boldsymbol{x} = \boldsymbol{0}$*. For all* i *and* j*,* $e(\boldsymbol{a}_i, \boldsymbol{a}_j^*) = g_T^{\delta_{i,j}}$ *where* $\delta_{i,j} = 1$ *if* $i = j$*, and* 0 *otherwise, and* $e(G_1, G_2) \neq 1 \in \mathbb{G}_T$*.*

DPVS also has linear transformations $\phi_{i,j}$ *on* $\mathbb{V}$ *s.t.* $\phi_{i,j}(\boldsymbol{a}_j) = \boldsymbol{a}_i$ *and* $\phi_{i,j}(\boldsymbol{a}_k) = \boldsymbol{0}$ *if* $k \neq j$*, which can be easily achieved by* $\phi_{i,j}(\boldsymbol{x}) := (\overbrace{0, \ldots, 0}^{i-1}, D_j, \overbrace{0, \ldots, 0}^{N-i})$ *where* $\boldsymbol{x} := (D_1, \ldots, D_N)$*. Moreover, linear transformation* $\phi_{i,j}^*$ *on* $\mathbb{V}^*$ *s.t.* $\phi_{i,j}^*(\boldsymbol{a}_j^*) = \boldsymbol{a}_i^*$ *and* $\phi_{i,j}^*(\boldsymbol{a}_k^*) = \boldsymbol{0}$ *if* $k \neq j$ *can be easily achieved by* $\phi_{i,j}^*(\boldsymbol{y}) := (\overbrace{0, \ldots, 0}^{i-1}, H_j, \overbrace{0, \ldots, 0}^{N-i})$ *where* $\boldsymbol{y} := (H_1, \ldots, H_N)$*. We call* $\phi_{i,j}$ *and* $\phi_{i,j}^*$ *"distortion maps".*

DPVS generation algorithm $\mathcal{G}_{\mathsf{dpvs}}$ *takes input* 1^λ *(*$\lambda \in \mathbb{N}$*),* $N \in \mathbb{N}$ *and a description of bilinear pairing groups* $\mathsf{param}_{\mathbb{G}}$*, and outputs a description of* $\mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*, e)$ *constructed above with security parameter* λ *and* N*-dimensional* $(\mathbb{V}, \mathbb{V}^*)$*.*

B Proofs of Lemmas 1 and 2

B.1 Outline

The DLIN Problem is reduced to (complicated) Problems 1 and 2 through several intermediate steps, or intermediate problems, as indicated below (See Figure 1):

1. DLIN Problem (in Definition 10)
2. Basic Problem 0 with three-dimensional DPVS (in Definition 17)
3. Basic Problems 1 and 2 with $\overrightarrow{n} := (d; n_1, \ldots, n_d)$ (in Definitions 18 and 19)

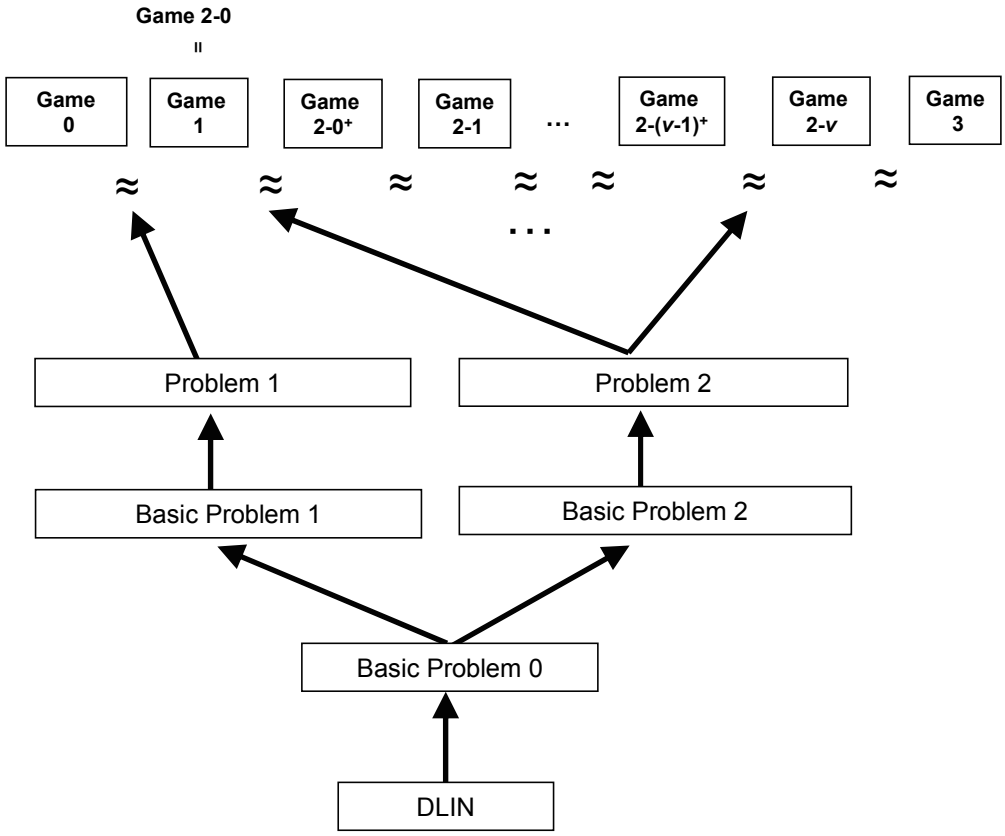

Figure 1: Structure of Reductions for the Proposed KP-FE (in Section 6) and CP-FE (in Section 7) Schemes

4. Problems 1 and 2 with $\overrightarrow{n}$ (in Definitions 11 and 12)

We will explain how the simplest problem, DLIN, is sequentially transformed to more complicated ones according to parameter $\overrightarrow{n}$, which indicates degree of complexity.

DLIN → Basic Problem 0 : Basic Problem 0 uses three-dimensional DPVS. In this first reduction step, a DLIN instance on (symmetric) pairing group is transformed to a Basic Problem 0 instance on the DPVS, i.e., higher level concept. It is proven in Lemma 15.

Basic Problem 0 → Basic Problems 1 and 2 : Format $\overrightarrow{n} := (d; n_1, \ldots, n_d)$ corresponds to $d+1$ DPVSs, $\mathbb{V}_t$ $(t = 0, \ldots, d)$. The dimension of $\mathbb{V}_0$ is 5, and the dimensions of $\mathbb{V}_t$ are $3n_t + 1$ for $t = 1, \ldots, d$. In this reduction step, vector elements (and additional group elements) in a Basic Problem 0 instance are transformed to the corresponding elements in $\mathbb{V}_t$ for $t = 0, \ldots, d$. They are proven in Lemmas 16 and 18.

Basic Problem 1 → Problem 1 : The proof is given in Lemmas 17.

Basic Problem 2 → Problem 2 : The proof is given in Lemma 19.

B.2 Preliminary Lemmas

We will use the following two lemmas (Lemmas 14 and 15) in the proofs of Lemmas 1 and 2.

Lemma 14 *Let $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ be dual pairing vector spaces by direct product of symmetric pairing groups. Using $\{\phi_{i,j}\}$, we can efficiently sample a random linear transformation*

$$W := \sum_{i=1,j=1}^{N,N} r_{i,j}\phi_{i,j}$$

of $\mathbb{V}$ with random coefficients $\{r_{i,j}\}_{i,j\in\{1,\ldots,N\}} \xleftarrow{\mathsf{U}} GL(N, \mathbb{F}_q)$. At that time, the matrix $(r^*_{i,j}) := (\{r_{i,j}\}^{-1})^T$ defines the adjoint action on $\mathbb{V}$ for pairing e, i.e., $e(W(\boldsymbol{x}), (W^{-1})^T(\boldsymbol{y})) = e(\boldsymbol{x}, \boldsymbol{y})$ for any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{V}$, via

$$(W^{-1})^T := \sum_{i=1,j=1}^{N,N} r^*_{i,j}\phi_{i,j}.$$

Definition 17 (Basic Problem 0) *Basic Problem 0 is to guess $\beta \in \{0, 1\}$, given $(\mathsf{param}_{\mathsf{BP0}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{y}^*_\beta, \boldsymbol{f}, \kappa G, \xi G, \delta\xi G) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP0}}_\beta(1^\lambda)$, where*

$$\begin{aligned}
&\mathcal{G}^{\mathsf{BP0}}_\beta(1^\lambda): \quad \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),\\
&\quad \mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 3, \mathsf{param}_{\mathbb{G}}),\\
&\quad X := \begin{pmatrix} \overrightarrow{\chi}_1 \\ \overrightarrow{\chi}_2 \\ \overrightarrow{\chi}_3 \end{pmatrix} := (\chi_{i,j})_{i,j} \xleftarrow{\mathsf{U}} GL(3, \mathbb{F}_q),\ (\vartheta_{i,j})_{i,j} := \begin{pmatrix} \overrightarrow{\vartheta}_1 \\ \overrightarrow{\vartheta}_2 \\ \overrightarrow{\vartheta}_3 \end{pmatrix} := (X^T)^{-1}, \quad \kappa, \xi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\\
&\quad \boldsymbol{b}_i := \kappa(\overrightarrow{\chi}_i)_{\mathbb{A}} = \kappa\textstyle\sum_{j=1}^3 \chi_{i,j}\boldsymbol{a}_j \ \text{ for } i = 1, 3, \quad \widehat{\mathbb{B}} := (\boldsymbol{b}_1, \boldsymbol{b}_3),\\
&\quad \boldsymbol{b}^*_i := \xi(\overrightarrow{\vartheta}_i)_{\mathbb{A}} = \xi\textstyle\sum_{j=1}^3 \vartheta_{i,j}\boldsymbol{a}_{t,j} \ \text{ for } i = 1, 2, 3, \quad \mathbb{B}^* := (\boldsymbol{b}^*_1, \boldsymbol{b}^*_2, \boldsymbol{b}^*_3),\\
&\quad g_T := e(G, G)^{\kappa\xi}, \quad \mathsf{param}_{\mathsf{BP0}} := (\mathsf{param}_{\mathbb{V}},\ g_T)\\
&\quad \delta, \sigma, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \rho, \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\\
&\quad \boldsymbol{y}^*_0 := (\delta, 0, \sigma)_{\mathbb{B}^*}, \quad \boldsymbol{y}^*_1 := (\delta, \rho, \sigma)_{\mathbb{B}^*}, \quad \boldsymbol{f} := (\omega, \tau, 0)_{\mathbb{B}},\\
&\quad \text{return} \ \ (\mathsf{param}_{\mathsf{BP0}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{y}^*_\beta, \boldsymbol{f}, \kappa G, \xi G, \delta\xi G).
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic machine $\mathcal{D}$, we define the advantage of $\mathcal{D}$ for Basic Problem 0, $\mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{D}}(\lambda)$, is similarly defined as in Definition 11.

Lemma 15 *For any adversary $\mathcal{D}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{E}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{D}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

Proof. Given a DLIN instance

$$(\mathsf{param}_{\mathbb{G}},\ G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta),$$

$\mathcal{E}$ calculates

$$\begin{aligned}
&\mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 3, \mathsf{param}_{\mathbb{G}}),\\
&g_T := e(\kappa G, \xi G) \ \ \left(= e(G, G)^{\kappa\xi}\right), \quad \mathsf{param}_{\mathsf{BP0}} := (\mathsf{param}_{\mathbb{V}},\ g_T).
\end{aligned}$$

$\mathcal{E}$ sets 3×3 matrices Π^*, Π as follows:

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

Then, $\Pi \cdot (\Pi^*)^{\mathrm{T}} = \kappa\xi \cdot I_3$. By using matrices Π and Π^*, $\mathcal{E}$ sets

$$\begin{aligned}
&\boldsymbol{u}_1^* := (\xi, 0, 1)_{\mathbb{A}}, \quad \boldsymbol{u}_2^* := (0, 0, 1)_{\mathbb{A}}, \quad \boldsymbol{u}_3^* := (0, \kappa, 1)_{\mathbb{A}}, \\
&\boldsymbol{u}_1 := (\kappa, 0, 0)_{\mathbb{A}}, \quad \boldsymbol{u}_2 := (-\kappa, -\xi, \kappa\xi)_{\mathbb{A}}, \quad \boldsymbol{u}_3 := (0, \xi, 0)_{\mathbb{A}},
\end{aligned}$$

$\mathcal{E}$ can compute $\boldsymbol{u}_i^*$ for $i = 1, 2, 3$ and $\boldsymbol{u}_i$ for $i = 1, 3$ from the above DLIN instance. Let bases $\mathbb{U} := (\boldsymbol{u}_i)_{i=1,2,3}$, $\mathbb{U}^* := (\boldsymbol{u}_i^*)_{i=1,2,3}$ of $\mathbb{V}$. $\mathcal{E}$ then generates $\eta, \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q$ such that $\eta \neq 0$, and sets

$$\boldsymbol{v} := (\varphi G, -\eta G, \eta(\kappa G)) \quad (= (\varphi, -\eta, \eta\kappa)_{\mathbb{A}}) \quad \text{and} \quad \boldsymbol{w}_\beta^* := (\delta\xi G, \sigma\kappa G, Y_\beta).$$

$\mathcal{E}$ generates random linear transformation W on $\mathbb{V}$ given in Lemma 14, then calculates

$$\begin{aligned}
&\boldsymbol{b}_i := W(\boldsymbol{u}_i) \ \text{ for } i = 1, 3, \quad \boldsymbol{b}_i^* := (W^{-1})^{\mathrm{T}}(\boldsymbol{u}_i^*) \ \text{ for } i = 1, 2, 3, \\
&\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \boldsymbol{b}_3). \quad \mathbb{B}^* := (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \boldsymbol{b}_3^*), \\
&\boldsymbol{f} = W(\boldsymbol{v}), \quad \boldsymbol{y}_\beta^* = (W^{-1})^{\mathrm{T}}(\boldsymbol{w}_\beta^*)
\end{aligned}$$

$\mathcal{E}$ then gives $(\mathsf{param}_{\mathsf{BP0}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{y}_\beta^*, \boldsymbol{f}, \kappa G, \xi G, \delta\xi G)$ to $\mathcal{D}$, where $\delta\xi G$ is contained in the DLIN instance, and outputs $\beta' \in \{0, 1\}$ if $\mathcal{D}$ outputs β'.

If we set

$$\tau := \xi^{-1}\eta, \quad \omega := \tau + \kappa^{-1}\varphi,$$

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

$$\begin{aligned}
&\boldsymbol{v} = (\varphi, -\eta, \eta\kappa)_{\mathbb{A}} = ((\omega - \tau)\kappa, -\tau\xi, \tau\kappa\xi)_{\mathbb{A}} = \omega\boldsymbol{u}_1 + \tau\boldsymbol{u}_2 = (\omega, \tau, 0)_{\mathbb{U}}, \ \text{ and} \\
&\boldsymbol{f} = W(\boldsymbol{v}) = W((\omega, \tau, 0)_{\mathbb{U}}) = (\omega, \tau, 0)_{\mathbb{B}}.
\end{aligned}$$

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

$$\begin{aligned}
&\boldsymbol{w}_0^* = (\delta\xi G, \sigma\kappa G, (\delta + \sigma)G) = (\delta\xi, \sigma\kappa, \delta + \sigma)_{\mathbb{A}} = \delta\boldsymbol{u}_1^* + \sigma\boldsymbol{u}_3^* = (\delta, 0, \sigma)_{\mathbb{U}^*} \ \text{ and} \\
&\boldsymbol{y}_0^* = (W^{-1})^{\mathrm{T}}(\boldsymbol{w}_0^*) = (W^{-1})^{\mathrm{T}}((\delta, 0, \sigma)_{\mathbb{U}^*}) = (\delta, 0, \sigma)_{\mathbb{B}^*}.
\end{aligned}$$

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

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

$$\begin{aligned}
\boldsymbol{w}_1^* &= (\delta\xi G, \sigma\kappa G, (\delta + \rho + \sigma)G) = (\delta\xi, \sigma\kappa, \delta + \rho + \sigma)_{\mathbb{A}} \\
&= \delta\boldsymbol{u}_1^* + \rho\boldsymbol{u}_2^* + \sigma\boldsymbol{u}_3^* = (\delta, \rho, \sigma)_{\mathbb{U}^*}, \ \text{ and} \\
\boldsymbol{y}_1^* &= (W^{-1})^{\mathrm{T}}(\boldsymbol{w}_1^*) = (W^{-1})^{\mathrm{T}}((\delta, \rho, \sigma)_{\mathbb{U}^*}) = (\delta, \rho, \sigma)_{\mathbb{B}^*},
\end{aligned}$$

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

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

B.3 Proof of Lemma 1

Combining Lemmas 15, 16 and 17, we obtain Lemma 1.

Definition 18 (Basic Problem 1) *Basic Problem 1 is to guess* $\beta \in \{0,1\}$*, given* $(\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t\}_{t=0,\ldots,d}, \boldsymbol{f}_{\beta,0}, \{\boldsymbol{f}_{\beta,t,1}, \boldsymbol{f}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP1}}_{\beta}(1^\lambda, \overrightarrow{n})$*, where*

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{BP1}}_{\beta}(1^\lambda, \overrightarrow{n} := (d; n_1, \ldots, n_d)) : \quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),\\
&\quad \omega, \gamma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\\
&\quad \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, .., \boldsymbol{b}^*_{0,5}),\quad \boldsymbol{f}_{0,0} := (\omega, 0, 0, 0, \gamma)_{\mathbb{B}_0},\quad \boldsymbol{f}_{1,0} := (\omega, \tau, 0, 0, \gamma)_{\mathbb{B}_0},\\
&\quad \text{for } t = 1, \ldots, d,\\
&\qquad \overrightarrow{e}_{t,1} := (1, 0^{n_t-1}) \in \mathbb{F}_q^{n_t},\quad \widehat{\mathbb{B}}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,n_t+2}, \ldots, \boldsymbol{b}^*_{t,3n_t+1}),\\
&\qquad\qquad\qquad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\ }^{1}\\
&\qquad \boldsymbol{f}_{0,t,1} := \ (\quad \omega \overrightarrow{e}_{t,1}, \quad 0^{n_t}, \quad 0^{n_t}, \quad \gamma \quad)_{\mathbb{B}_t},\\
&\qquad \boldsymbol{f}_{1,t,1} := \ (\quad \omega \overrightarrow{e}_{t,1}, \quad \tau \overrightarrow{e}_{t,1}, \quad 0^{n_t}, \quad \gamma \quad)_{\mathbb{B}_t},\\
&\qquad \boldsymbol{f}_{t,i} := \omega \boldsymbol{b}_{t,i} \quad i = 2, \ldots, n_t,\\
&\quad \text{return} \quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t\}_{t=0,\ldots,d}, \boldsymbol{f}_{\beta,0}, \{\boldsymbol{f}_{\beta,t,1}, \boldsymbol{f}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t}).
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$*. For a probabilistic adversary* $\mathcal{C}$*, the advantage of* $\mathcal{C}$ *for Basic Problem 1,* $\mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{C}}(\lambda)$*, is similarly defined as in Definition 11.*

Lemma 16 *For any adversary* $\mathcal{C}$*, there is a probabilistic machine* $\mathcal{D}$*, whose running time is essentially the same as that of* $\mathcal{C}$*, such that for any security parameter* λ*,* $\mathsf{Adv}^{\mathsf{BP1}}_{\mathcal{C}}(\lambda) \leq \mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{D}}(\lambda)$ *for any* $\overrightarrow{n} := (d; \{n_t\}) := (d; n_1, \ldots, n_d)$*.*

Proof. $\mathcal{D}$ is given a Basic Problem 0 instance

$$(\mathsf{param}_{\mathsf{BP0}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{y}^*_\beta, \boldsymbol{f}, \kappa G, \xi G, \delta\xi G).$$

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

$$
\begin{aligned}
&\mathsf{param}_0 := (q, \mathbb{V}_0, \mathbb{G}_T, \mathbb{A}_0, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 5, \mathsf{param}_{\mathbb{G}}),\\
&\mathsf{param}_t := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 3n_t + 1, \mathsf{param}_{\mathbb{G}}) \quad \text{for } t = 1, \ldots, d,\\
&\mathsf{param}_{\overrightarrow{n}} := (\{\mathsf{param}_t\}_{t=0,\ldots,d}, g_T),
\end{aligned}
$$

where g_T is contained in $\mathsf{param}_{\mathsf{BP0}}$. $\mathcal{D}$ generates random linear transformation W_t on $\mathbb{V}_t$ ($t = 0, \ldots, d$) given in Lemma 14, then sets

$$
\begin{aligned}
&\boldsymbol{d}_{0,\iota} := W_0(\boldsymbol{b}^*_\iota, 0, 0) \quad \text{for } \iota = 1, 2, \quad \boldsymbol{d}_{0,3} := W_0(0, 0, 0, \xi G, 0),\\
&\boldsymbol{d}_{0,4} := W_0(\boldsymbol{b}^*_3, 0, 0), \quad \boldsymbol{d}_{0,5} := W_0(0, 0, 0, 0, \xi G),\\
&\boldsymbol{d}^*_\iota := (W_0^{-1})^{\mathrm{T}}(\boldsymbol{b}_\iota, 0, 0) \quad \text{for } \iota = 1, 2, \quad \boldsymbol{d}^*_{0,3} := (W_0^{-1})^{\mathrm{T}}(0, 0, 0, \kappa G, 0),\\
&\boldsymbol{d}^*_{0,4} := (W_0^{-1})^{\mathrm{T}}(\boldsymbol{b}_3, 0, 0) \quad \boldsymbol{d}^*_{0,5} := (W_0^{-1})^{\mathrm{T}}(0, 0, 0, 0, \kappa G),\\
&\boldsymbol{g}_{\beta,0} := W_0(\boldsymbol{y}^*_\beta, 0, 0),\\
&\text{for } t = 1, \ldots, d,\\
&\quad \boldsymbol{d}_{t,1} := W_t(\boldsymbol{b}^*_1, 0^{N_t-3}),\ \boldsymbol{d}_{t,n_t+1} := W_t(\boldsymbol{b}^*_2, 0^{N_t-3}),\ \boldsymbol{d}_{t,N_t} := W_t(\boldsymbol{b}^*_3, 0^{N_t-3}),\\
&\quad \text{otherwise, } \boldsymbol{d}_{t,i} := W_t(0^\iota, \xi G, 0^{N_t-\iota-1}) \ \text{ where } \begin{cases} \iota := i+1 \text{ if } i \in \{2, \ldots, n_t\}, \\ \iota := i \text{ if } i \in \{n_t+2, \ldots, N_t-1\}, \end{cases}\\
&\quad \boldsymbol{d}^*_{t,1} := (W_t^{-1})^{\mathrm{T}}(\boldsymbol{b}_1, 0^{N_t-3}),\ \boldsymbol{d}^*_{t,n_t+1} := (W_t^{-1})^{\mathrm{T}}(\boldsymbol{b}_2, 0^{N_t-3}),\ \boldsymbol{d}^*_{t,N_t} := (W_t^{-1})^{\mathrm{T}}(\boldsymbol{b}_3, 0^{N_t-3}),\\
&\quad \text{otherwise, } \boldsymbol{d}^*_{t,i} := (W_t^{-1})^{\mathrm{T}}(0^\iota, \kappa G, 0^{N_t-\iota-1}) \ \text{ where } \begin{cases} \iota := i+1 \text{ if } i \in \{2, \ldots, n_t\}, \\ \iota := i \text{ if } i \in \{n_t+2, \ldots, N_t-1\}, \end{cases}\\
&\quad \boldsymbol{g}_{\beta,t,1} := W_t(\boldsymbol{y}^*_\beta, 0^{N_t-3}),\ \boldsymbol{g}_{t,i} := W_t(0^{i+1}, \delta\xi G, 0^{N_t-i-2}) \ \text{ for } i = 2, \ldots, n_t,
\end{aligned}
$$

where $(\boldsymbol{v}, 0^{N_t-3}) := (\widetilde{G}_1, \widetilde{G}_2, \widetilde{G}_3, , 0^{N_t-3})$ for any $\boldsymbol{v} := (\widetilde{G}_1, \widetilde{G}_2, \widetilde{G}_3) \in \mathbb{V} = \mathbb{G}^3$. Then, $\mathbb{D}_0 := (\boldsymbol{d}_{0,i})_{i=1,\ldots,5}$ and $\mathbb{D}_0^* := (\boldsymbol{d}_{0,i}^*)_{i=1,\ldots,5}$, $\mathbb{D}_t := (\boldsymbol{d}_{t,i})_{i=1,\ldots,3n_t+1}$ and $\mathbb{D}_t^* := (\boldsymbol{d}_{t,i}^*)_{i=1,\ldots,3n_t+1}$ are dual orthonormal bases. $\mathcal{D}$ can compute $\mathbb{D}_t$ for $t = 0, \ldots, d$, $\widehat{\mathbb{D}}_0^* := (\boldsymbol{d}_{0,1}^*, \boldsymbol{d}_{0,3}^*, \ldots, \boldsymbol{d}_{0,5}^*)$, $\widehat{\mathbb{D}}_t^* := (\boldsymbol{d}_{t,1}^*, \ldots, \boldsymbol{d}_{t,n_t}^*, \boldsymbol{d}_{t,n_t+2}^*, \ldots, \boldsymbol{d}_{t,3n_t+1}^*)$ for $t = 1, \ldots, d$ from $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \boldsymbol{b}_3)$, $\mathbb{B}^*$, κG, and ξG. $\mathcal{D}$ then gives $(\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{D}_t, \widehat{\mathbb{D}}_t^*\}_{t=0,\ldots,d}, \boldsymbol{g}_{\beta,0}, \{\boldsymbol{g}_{\beta,t,1}, \boldsymbol{g}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t})$ to $\mathcal{C}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{C}$ outputs β'.

We can see that

$$
\begin{aligned}
&\boldsymbol{g}_{0,0} := (\omega', 0, 0, 0, \gamma')_{\mathbb{D}_0}, \quad \boldsymbol{g}_{1,0} := (\omega', \tau', 0, 0, \gamma')_{\mathbb{D}_0},\\
&\text{for } t = 1, \ldots, d,\\
&\qquad\qquad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{1}\\
&\boldsymbol{g}_{0,t,1} := \quad (\quad \omega' \overrightarrow{e}_{t,1}, \quad 0^{n_t}, \quad 0^{n_t}, \quad \gamma' \quad)_{\mathbb{D}_t},\\
&\boldsymbol{g}_{1,t,1} := \quad (\quad \omega' \overrightarrow{e}_{t,1}, \quad \tau' \overrightarrow{e}_{t,1}, \quad 0^{n_t}, \quad \gamma' \quad)_{\mathbb{D}_t},\\
&\boldsymbol{g}_{t,i} := \omega' \boldsymbol{d}_{t,i} \quad \text{for } i = 2, \ldots, n_t,
\end{aligned}
$$

where $\omega' := \delta$, $\gamma' := \sigma$, and $\tau' := \rho$ which are distributed uniformly in $\mathbb{F}_q$. Therefore, the distribution of $(\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{D}_t, \widehat{\mathbb{D}}_t^*\}_{t=0,\ldots,d}, \boldsymbol{g}_{\beta,0}, \{\boldsymbol{g}_{\beta,t,1}, \boldsymbol{g}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t})$ is exactly the same as $\left\{ \varrho \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{BP1}}(1^\lambda, \overrightarrow{n}) \right\}$. □

Lemma 17 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{C}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P1}}(\lambda) \leq \mathsf{Adv}_{\mathcal{C}}^{\mathsf{BP1}}(\lambda) + (d+1)/q$.*

Proof. Given a Basic Problem 1 instance

$$(\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \widehat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}, \boldsymbol{f}_{\beta,0}, \{\boldsymbol{f}_{\beta,t,1}, \boldsymbol{f}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t}),$$

$\mathcal{C}$ calculates

$$\boldsymbol{r}_t \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{t,3n_t+1} \rangle, \quad \boldsymbol{e}_{\beta,t,1} := \boldsymbol{f}_{\beta,t,1} + \boldsymbol{r}_t \quad \text{for } t = 1, \ldots, d.$$

$\mathcal{C}$ generates $u_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times$, $\begin{pmatrix} \overrightarrow{u}_{t,1} \\ \vdots \\ \overrightarrow{u}_{t,n_t} \end{pmatrix} := U_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$ for $t = 1, \ldots, d$. $\mathcal{C}$ then calculates

$$
\begin{aligned}
&\boldsymbol{d}_{0,2} := (0, u_0, 0, 0, 0)_{\mathbb{B}_0},\\
&\qquad\qquad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{1}\\
&\boldsymbol{d}_{t,n_t+i} := (\quad 0^{n_t}, \quad \overrightarrow{u}_{t,i}, \quad 0^{n_t}, \quad 0 \quad)_{\mathbb{B}_t} \quad \text{for } t = 1, \ldots, d;\ i = 1, \ldots, n_t,
\end{aligned}
$$

$\mathcal{C}$ then sets dual orthonormal basis vectors

$$
\begin{aligned}
&\boldsymbol{d}_{0,2}^* := (0, u_0^{-1}, 0, 0, 0)_{\mathbb{B}_0^*},\\
&\qquad\qquad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{1}\\
&\boldsymbol{d}_{t,n_t+i}^* := (\quad 0^{n_t}, \quad \overrightarrow{z}_{t,i}, \quad 0^{n_t}, \quad 0 \quad)_{\mathbb{B}_t^*} \quad \text{for } t = 1, \ldots, d;\ i = 1 \ldots, n_t,
\end{aligned}
$$

where $\begin{pmatrix} \overrightarrow{z}_{t,1} \\ \vdots \\ \overrightarrow{z}_{t,n_t} \end{pmatrix} := (U_t^{-1})^{\mathrm{T}}$. $\mathcal{C}$ cannot calculate above $\boldsymbol{d}^*_{0,2}$ and $\boldsymbol{d}^*_{t,i}$ for $i = n_t+1, \ldots, 2n_t$ because of lack of $\boldsymbol{b}^*_{0,2}$ and $\boldsymbol{b}^*_{t,n_t+1}$. $\mathcal{C}$ then sets

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

$\mathcal{C}$ gives $(\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{D}_t, \widehat{\mathbb{D}}^*_t\}_{t=0,..,d}, \boldsymbol{f}_{\beta,0}, \{\boldsymbol{e}_{\beta,t,1}, \boldsymbol{f}_{t,i}\}_{t=1,...,d;i=2,...,n_t})$ to $\mathcal{B}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{B}$ outputs β'.

Then, with respect to $\mathbb{D}_t, \mathbb{D}^*_t$ (instead of $\mathbb{B}_t, \mathbb{B}^*_t$, respectively), the above answer to $\mathcal{B}$ has the same distribution as the Problem 1 instance, i.e., the above instance has the same distribution as the one given by generator $\mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \overrightarrow{n})$ if z_0 in Problem 1 is not equal to 0 and $(z_{t,1}, \ldots, z_{t,n_t})$ in Problem 1 is not equal to $\overrightarrow{0}$ for any $t = 1, \ldots, d$, i.e., except with probability $(d+1)/q$ for $\beta = 1$. □

B.4 Proof of Lemma 2

Combining Lemmas 15, 18 and 19, we obtain Lemma 2.

Definition 19 (Basic Problem 2) *Basic Problem 2 is to guess $\beta \in \{0,1\}$, given $(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,..,d}, \boldsymbol{y}^*_{\beta,0}, \boldsymbol{f}_0, \{\boldsymbol{y}^*_{\beta,t,i}, \boldsymbol{f}_{t,i}\}_{t=1,..,d;i=1,..,n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP2}}_\beta(1^\lambda, \overrightarrow{n})$, where*

$$\begin{aligned}
&\mathcal{G}^{\mathsf{BP2}}_\beta(1^\lambda, \overrightarrow{n} := (d; n_1, \ldots, n_d)) : \quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,...,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),\\
&\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \ldots, \boldsymbol{b}_{0,5}),\\
&\quad \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,2n_t+1}, \ldots, \boldsymbol{b}_{t,3n_t+1}) \text{ for } t = 1, \ldots, d,\\
&\quad \delta, \delta_0, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \rho, \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\\
&\quad \boldsymbol{y}^*_{0,0} := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{y}^*_{1,0} := (\delta, \rho, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{f}_0 := (\omega, \tau, 0, 0, 0)_{\mathbb{B}_0},\\
&\quad \text{for } t = 1, \ldots, d, \quad i = 1, \ldots, n_t;\\
&\qquad \overrightarrow{e}_{t,i} := (0^{i-1}, 1, 0^{n_t-i}) \in \mathbb{F}_q^{n_t},\\
&\qquad\qquad\qquad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\ }^{1}\\
&\qquad \boldsymbol{y}^*_{0,t,i} := \ (\ \delta \overrightarrow{e}_{t,i}, \quad 0^{n_t}, \quad \delta_0 \overrightarrow{e}_{t,i}, \quad 0\ )_{\mathbb{B}^*_t}\\
&\qquad \boldsymbol{y}^*_{1,t,i} := \ (\ \delta \overrightarrow{e}_{t,i}, \quad \rho \overrightarrow{e}_{t,i}, \quad \delta_0 \overrightarrow{e}_{t,i}, \quad 0\ )_{\mathbb{B}^*_t}\\
&\qquad \boldsymbol{f}_{t,i} := \ (\ \omega \overrightarrow{e}_{t,i}, \quad \tau \overrightarrow{e}_{t,i}, \quad 0^{n_t}, \quad 0\ )_{\mathbb{B}_t},\\
&\quad \text{return } \ (\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,..,d}, \boldsymbol{y}^*_{\beta,0}, \boldsymbol{f}_0, \{\boldsymbol{y}^*_{\beta,t,i}, \boldsymbol{f}_{t,i}\}_{t=1,..,d;i=1,..,n_t}).
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic machine $\mathcal{C}$, we define the advantage of $\mathcal{C}$ for Basic Problem 2, $\mathsf{Adv}^{\mathsf{BP2}}_{\mathcal{C}}(\lambda)$, as in Definition 11.

Lemma 18 *For any adversary $\mathcal{C}$, there is a probabilistic machine $\mathcal{D}$, whose running time is essentially the same as that of $\mathcal{C}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{BP2}}_{\mathcal{C}}(\lambda) = \mathsf{Adv}^{\mathsf{BP0}}_{\mathcal{D}}(\lambda)$ for any $\overrightarrow{n} := (d; \{n_t\}) := (d; n_1, \ldots, n_d)$.*

Proof. $\mathcal{D}$ is given a Basic Problem 0 instance

$$(\mathsf{param}_{\mathsf{BP0}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \boldsymbol{y}^*_\beta, \boldsymbol{f}, \kappa G, \xi G, \delta\xi G).$$

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

$$\begin{aligned}
&\mathsf{param}_0 := (q, \mathbb{V}_0, \mathbb{G}_T, \mathbb{A}_0, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 5, \mathsf{param}_{\mathbb{G}}),\\
&\mathsf{param}_t := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 3n_t+1, \mathsf{param}_{\mathbb{G}}) \quad \text{for } t = 1, \ldots, d,\\
&\mathsf{param}_{\overrightarrow{n}} := (\{\mathsf{param}_t\}_{t=0,\ldots,d}, g_T),
\end{aligned}$$

where g_T is contained in $\mathsf{param}_{\mathsf{BP0}}$. $\mathcal{D}$ generates random linear transformation W_t on $\mathbb{V}_t$ ($t = 0, \ldots, d$) given in Lemma 14, then sets

$$\begin{aligned}
&\boldsymbol{d}_{0,\iota} := W_0(\boldsymbol{b}_\iota, 0, 0) \quad \text{for } \iota = 1, 2, \quad \boldsymbol{d}_{0,3} := W_0(0, 0, 0, \kappa G, 0),\\
&\boldsymbol{d}_{0,4} := W_0(\boldsymbol{b}_3, 0, 0), \quad \boldsymbol{d}_{0,5} := W_0(0, 0, 0, 0, \kappa G),\\
&\boldsymbol{d}^*_\iota := (W_0^{-1})^{\mathrm{T}}(\boldsymbol{b}^*_\iota, 0, 0) \quad \text{for } \iota = 1, 2, \quad \boldsymbol{d}^*_{0,3} := (W_0^{-1})^{\mathrm{T}}(0, 0, 0, \xi G, 0),\\
&\boldsymbol{d}^*_{0,4} := (W_0^{-1})^{\mathrm{T}}(\boldsymbol{b}^*_3, 0, 0) \quad \boldsymbol{d}^*_{0,5} := (W_0^{-1})^{\mathrm{T}}(0, 0, 0, 0, \xi G),\\
&\boldsymbol{p}^*_{\beta,0} := (W_0^{-1})^{\mathrm{T}}(\boldsymbol{y}^*_\beta, 0, 0), \qquad \boldsymbol{g}_0 := W_0(\boldsymbol{f}, 0, 0),\\
&\text{for } t = 1, \ldots, d,\\
&\quad \boldsymbol{d}_{t,(\iota-1)n_t+i} := W_t(0^{3(i-1)}, \boldsymbol{b}_\iota, 0^{3(n_t-i)}, 0) \quad \text{for } \iota = 1, 2, 3;\ i = 1, \ldots, n_t,\\
&\quad \boldsymbol{d}_{t,3n_t+1} := W_t(0^{3n_t}, \kappa G),\\
&\quad \boldsymbol{d}^*_{t,(\iota-1)n_t+i} := (W_t^{-1})^{\mathrm{T}}(0^{3(i-1)}, \boldsymbol{b}^*_\iota, 0^{3(n_t-i)}, 0) \quad \text{for } \iota = 1, 2, 3;\ i = 1, \ldots, n_t,\\
&\quad \boldsymbol{d}^*_{t,3n_t+1} := (W_t^{-1})^{\mathrm{T}}(0^{3n_t}, \xi G),\\
&\quad \boldsymbol{p}^*_{\beta,t,i} := (W_t^{-1})^{\mathrm{T}}(0^{3(i-1)}, \boldsymbol{y}^*_\beta, 0^{3(n_t-i)}, 0) \quad \text{for } i = 1, \ldots, n_t,\\
&\quad \boldsymbol{g}_{t,i} := W_t(0^{3(i-1)}, \boldsymbol{f}, 0^{3(n_t-i)}, 0) \quad \text{for } i = 1, \ldots, n_t.
\end{aligned}$$

where $(0^{l_1}, \boldsymbol{v}, 0^{l_2}) := (0^{l_1}, \widetilde{G}_1, \widetilde{G}_2, \widetilde{G}_3, 0^{l_2})$ for any $\boldsymbol{v} := (\widetilde{G}_1, \widetilde{G}_2, \widetilde{G}_3) \in \mathbb{V} = \mathbb{G}^3$ and $l_1, l_2 \in \mathbb{Z}_{\geq 0}$. Then, $\mathbb{D}_0 := (\boldsymbol{d}_{0,i})_{i=1,\ldots,5}$ and $\mathbb{D}^*_0 := (\boldsymbol{d}^*_{0,i})_{i=1,\ldots,5}$, $\mathbb{D}_t := (\boldsymbol{d}_{t,i})_{i=1,\ldots,3n_t+1}$ and $\mathbb{D}^*_t := (\boldsymbol{d}^*_{t,i})_{i=1,\ldots,3n_t+1}$ for $t = 1, \ldots, d$ are dual orthonormal bases. $\mathcal{D}$ can compute

$$\begin{aligned}
&\widehat{\mathbb{D}}_0 := (\boldsymbol{d}_{0,1}, \boldsymbol{d}_{0,3}, \ldots, \boldsymbol{d}_{0,5}), \quad \mathbb{D}^*_0 := (\boldsymbol{d}^*_{0,1}, \ldots, \boldsymbol{d}^*_{0,5}),\\
&\text{for } t = 1, \ldots, d, \quad \widehat{\mathbb{D}}_t := (\boldsymbol{d}_{t,1}, \ldots, \boldsymbol{d}_{t,n_t}, \boldsymbol{d}_{t,2n_t+1}, \ldots, \boldsymbol{d}_{t,3n_t+1}), \quad \mathbb{D}^*_t := (\boldsymbol{d}^*_{t,1}, \ldots, \boldsymbol{d}^*_{t,3n_t+1}),
\end{aligned}$$

from $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \boldsymbol{b}_3), \mathbb{B}^*, \kappa G$, and ξG. $\mathcal{D}$ then gives $(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{D}}_t, \mathbb{D}^*_t\}_{t=0,\ldots,d}, \boldsymbol{p}^*_{\beta,0}, \boldsymbol{g}_0, \{\boldsymbol{p}^*_{\beta,t,i}, \boldsymbol{g}_{t,i}\}_{t=1,\ldots,d;i=1,\ldots,n_t})$ to $\mathcal{C}$, and outputs $\beta' \in \{0, 1\}$ if $\mathcal{C}$ outputs β'.

We can see that

$$\begin{aligned}
&\boldsymbol{p}^*_{0,0} = (\delta, 0, 0, \delta_0, 0)_{\mathbb{D}^*_0}, \quad \boldsymbol{p}^*_{1,0} = (\delta, \rho, 0, \delta_0, 0)_{\mathbb{D}^*_0}, \quad \boldsymbol{g}_0 = (\omega, \tau, 0, 0, 0)_{\mathbb{D}_0},\\
&\qquad\qquad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\qquad}^{n_t} \quad \overbrace{\ }^{1}\\
&\boldsymbol{p}^*_{0,t,i} = (\ \delta \overrightarrow{e}_{t,i}, \quad 0^{n_t}, \quad \delta_0 \overrightarrow{e}_{t,i}, \quad 0\ )_{\mathbb{D}^*_t}\\
&\boldsymbol{p}^*_{1,t,i} = (\ \delta \overrightarrow{e}_{t,i}, \quad \rho \overrightarrow{e}_{t,i}, \quad \delta_0 \overrightarrow{e}_{t,i}, \quad 0\ )_{\mathbb{D}^*_t}\\
&\boldsymbol{g}_{t,i} = (\ \omega \overrightarrow{e}_{t,i}, \quad \tau \overrightarrow{e}_{t,i}, \quad 0^{n_t}, \quad 0\ )_{\mathbb{D}_t},\\
&\qquad\qquad\qquad\qquad\qquad\qquad t = 1, \ldots, d; i = 1, \ldots, n_t,
\end{aligned}$$

Therefore, the distribution of $(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{D}}_t, \mathbb{D}^*_t\}_{t=0,\ldots,d}, \boldsymbol{p}^*_{\beta,0}, \boldsymbol{g}_0, \{\boldsymbol{p}^*_{\beta,t,i}, \boldsymbol{g}_{t,i}\}_{t=1,\ldots,d;i=1,\ldots,n_t})$ is exactly the same as $\left\{\varrho \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{BP2}}_\beta(1^\lambda, (d, \{n_t\}))\right\}$. □

Lemma 19 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{C}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}}(\lambda) = \mathsf{Adv}^{\mathsf{BP2}}_{\mathcal{C}}(\lambda)$.*

Proof. Given a Basic Problem 2 instance

$$(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,..,d}, \boldsymbol{y}^*_{\beta,0}, \boldsymbol{f}_0, \{\boldsymbol{y}^*_{\beta,t,i}, \boldsymbol{f}_{t,i}\}_{t=1,..,d;i=1,..,n_t}),$$

$\mathcal{C}$ calculates

$$\boldsymbol{r}^*_{t,i} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}^*_{t,2n_t+1}, \ldots, \boldsymbol{b}^*_{t,3n_t}\rangle, \quad \boldsymbol{h}^*_{\beta,t,i} := \boldsymbol{y}^*_{\beta,t,i} + \boldsymbol{r}^*_{t,i}.$$

$\mathcal{C}$ then generates $z'_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times$ and $\begin{pmatrix} \overrightarrow{z}'_{t,1} \\ \vdots \\ \overrightarrow{z}'_{t,n_t} \end{pmatrix} := Z'_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$, for $t = 1, \ldots, d$, and calculates

$$\boldsymbol{d}^*_{0,2} := (0, z'_0, 0, 0, 0)_{\mathbb{B}^*_0},$$
$$\boldsymbol{d}^*_{t,n_t+i} := (\overbrace{0^{n_t}}^{n_t}, \overbrace{\overrightarrow{z}'_{t,i}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t} \quad \text{for } t = 1, \ldots, d;\ i = 1 \ldots, n_t.$$

$\mathcal{C}$ then sets $z_0 := \rho^{-1} z'_0, u_0 := z_0^{-1}$, $\begin{pmatrix} \overrightarrow{z}_{t,1} \\ \vdots \\ \overrightarrow{z}_{t,n_t} \end{pmatrix} := Z_t := \rho^{-1} Z'_t$ and $\begin{pmatrix} \overrightarrow{u}_{t,1} \\ \vdots \\ \overrightarrow{u}_{t,n_t} \end{pmatrix} := (Z_t^{-1})^{\mathrm{T}}$, where ρ is defined in Basic Problem 2. Then,

$$\boldsymbol{d}^*_{0,2} = (0, \rho z_0, 0, 0, 0)_{\mathbb{B}^*_0},$$
$$\boldsymbol{d}^*_{t,n_t+i} = (\overbrace{0^{n_t}}^{n_t}, \overbrace{\rho\overrightarrow{z}_{t,i}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t} \quad \text{for } t = 1, \ldots, d;\ i = 1 \ldots, n_t.$$

$\mathcal{C}$ then sets dual orthonormal basis vectors

$$\boldsymbol{d}_{0,2} := (0, \rho^{-1} u_0, 0, 0, 0)_{\mathbb{B}_0},$$
$$\boldsymbol{d}_{t,n_t+i} := (\overbrace{0^{n_t}}^{n_t}, \overbrace{\rho^{-1}\overrightarrow{u}_{t,i}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t} \quad \text{for } t = 1, \ldots, d;\ i = 1 \ldots, n_t.$$

$\mathcal{C}$ cannot calculate above $\boldsymbol{d}_{0,2}$ and $\boldsymbol{d}_{t,i}$ for $i = n_t + 1, \ldots, 2n_t$. $\mathcal{C}$ then sets

$$\mathbb{D}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{d}_{0,2}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{D}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,4}, \boldsymbol{b}_{0,5}),\ \mathbb{D}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{d}^*_{0,2}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}, \boldsymbol{b}^*_{0,5}),$$
$$\mathbb{D}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{d}_{t,n_t+1}, \ldots, \boldsymbol{d}_{t,2n_t}, \boldsymbol{b}_{t,2n_t+1}, \ldots, \boldsymbol{b}_{t,3n_t+1}),$$
$$\widehat{\mathbb{D}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,2n_t+1}, \ldots, \boldsymbol{b}_{t,3n_t+1}),$$
$$\mathbb{D}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t}, \boldsymbol{d}^*_{t,n_t+1}, \ldots, \boldsymbol{d}^*_{t,2n_t}, \boldsymbol{b}^*_{t,2n_t+1}, \ldots, \boldsymbol{b}^*_{t,3n_t+1}).$$

$\mathcal{C}$ gives $(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{D}}_t, \mathbb{D}^*_t\}_{t=0,..,d}, \boldsymbol{y}^*_{\beta,0}, \boldsymbol{f}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{f}_{t,i}\}_{t=1,..,d;i=1,..,n_t})$ to $\mathcal{B}$, and outputs $\beta' \in \{0,1\}$ if $\mathcal{B}$ outputs β'.

For τ in Basic Problem 2, let $\tau' := \rho\tau$. Then, with respect to $\tau', \mathbb{D}_t, \mathbb{D}^*_t$ (instead of $\tau, \mathbb{B}_t, \mathbb{B}^*_t$), the above answer to $\mathcal{B}$ has the same distribution as the Problem 2 instance, i.e., the above instance has the same distribution as the one given by generator $\mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, \overrightarrow{n})$. □

C Proof of Lemma 3

Proof. We first remind the definition of cofactor (and cofactor matrix). When $n \geq 2$, for $n \times n$ matrix $Z := (z_{i,j})$, let $\Delta_{i,j}$ the minor obtained by removing the i-th row and the j-th column from Z. Cofactors $\widetilde{z}_{i,j}$ are defined by $(-1)^{i+j}\Delta_{i,j}$. The determinant of Z is given as $\det Z = \sum_{j=1}^{n} z_{i,j}\widetilde{z}_{i,j}$. In particular, when $i = 1$, we obtain

$$\det Z = \sum_{j=1}^{n} z_{1,j}\widetilde{z}_{1,j}. \tag{17}$$

In addition, when $\det Z \neq 0$, we have

$$U := (Z^{-1})^{\mathrm{T}} = \frac{1}{\det Z}\begin{pmatrix} \widetilde{z}_{1,1} & \dots & \widetilde{z}_{1,n} \\ \vdots & & \vdots \\ \widetilde{z}_{n,1} & \dots & \widetilde{z}_{n,n} \end{pmatrix}. \tag{18}$$

Case that $\overrightarrow{x} \cdot \overrightarrow{v} = p \neq 0$: For normalized pair of vectors

$$\overrightarrow{x} := (p, 0, \dots, 0), \quad \overrightarrow{v} := (1, 0, \dots, 0), \tag{19}$$

we will show that $(\overrightarrow{x}U, \overrightarrow{v}Z)$ is uniformly distributed on C_p for $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$. By that, for any pair $(\overrightarrow{x}, \overrightarrow{v}) \in C_p$, we see that $(\overrightarrow{x}U, \overrightarrow{v}Z)$ is uniformly distributed on C_p for $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$. Therefore, we consider $(\overrightarrow{x}, \overrightarrow{v})$ given by (19) in the following.

Since $Z = (z_{i,j})$ and (18) holds,

$$\overrightarrow{x}U = \frac{p}{\det Z}(\widetilde{z}_{1,1}, \dots, \widetilde{z}_{1,n}), \quad \overrightarrow{v}Z = (z_{1,1}, \dots, z_{1,n}).$$

Cofactors $\widetilde{z}_{1,j}$ are determined by $n-1$ rows, from the second to the n-th rows of Z. Hence, from formula (17), we see that $(\overrightarrow{x}U, \overrightarrow{v}Z)$ is uniformly distributed on C_p when $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q)$.

Case that $\overrightarrow{x} \cdot \overrightarrow{v} = 0$: For normalized pair

$$\overrightarrow{x} := (0, 1, \dots, 0), \quad \overrightarrow{v} := (1, 0, \dots, 0),$$

we will show that $(\overrightarrow{x}U, \overrightarrow{v}Z)$ is uniformly distributed on C_0 for $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$ because of the similar reason as above.

Since $Z = (z_{i,j})$ and (18) holds,

$$\overrightarrow{x}U = \frac{1}{\det Z}(\widetilde{z}_{2,1}, \dots, \widetilde{z}_{2,n}), \quad \overrightarrow{v}Z = (z_{1,1}, \dots, z_{1,n}).$$

Cofactors $\widetilde{z}_{2,j}$ are determined by $n-1$ rows except for the second one, that is, the first, and from the third to the n-th rows of Z. In particular, only term $\det Z$ in $(\overrightarrow{x}U, \overrightarrow{v}Z)$ is related to the second row of Z.

First, since $\widetilde{z}_{2,1}$ are determined by the rows of Z except for the second one, we see that $\overrightarrow{x}U$ are distributed uniformly on the space orthogonal to $\overrightarrow{v}Z$ up to scalar multiplication. Moreover, $\det Z$ is uniformly distributed in $\mathbb{F}_q^{\times}$ (non-zero scalar values), when the second row of Z is uniformly distributed in $\mathbb{F}_q^n$ such that $\det Z \neq 0$.

Combining these two facts, we see that $(\overrightarrow{x}U, \overrightarrow{v}Z)$ is uniformly distributed on C_0 when $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q)$. □

D Problems 3, 4 and 5 for CCA-Secure CP-FE

We will show Problems 3–5 and Lemmas 20–22 for the proof of Theorem 3. The proofs of Lemmas 20–22 are similar to those of Lemmas 1 and 2

Definition 20 (Problem 3) *Problem 3 is to guess $\beta \in \{0,1\}$, given* $(\mathsf{param}_{\overrightarrow{n}}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d+1;i=2,\ldots,n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P3}}_\beta(1^\lambda, \overrightarrow{n})$*, where*

$$\begin{aligned}
&\mathcal{G}^{\mathsf{P3}}_\beta(1^\lambda, \overrightarrow{n}): \quad n_{d+1} := 2, \quad \overrightarrow{n}' := (d+1; \{n_t\}_{t=1,\ldots,d+1}),\\
&\quad (\mathsf{param}_{\overrightarrow{n}'}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d+1;i=2,\ldots,n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \overrightarrow{n}'),\\
&\quad \text{return} \quad (\mathsf{param}_{\overrightarrow{n}}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d+1;i=2,\ldots,n_t}).
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic machine $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 3, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 11.

Lemma 20 *For any adversary $\mathcal{B}$, there exist probabilistic machine $\mathcal{E}$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + (d+7)/q$.*

Definition 21 (Problem 4) *Problem 4 is to guess $\beta \in \{0,1\}$, given* $(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,..,d}, \mathbb{B}_{d+1}, \mathbb{B}^*_{d+1}, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, \{\boldsymbol{h}^*_{d+1,i}\}_{i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P4}}_\beta(1^\lambda, \overrightarrow{n})$*, where*

$$\begin{aligned}
&\mathcal{G}^{\mathsf{P4}}_\beta(1^\lambda, \overrightarrow{n}): \quad n_{d+1} := 2, \quad \overrightarrow{n}' := (d+1; \{n_t\}_{t=1,\ldots,d+1}),\\
&\quad (\mathsf{param}_{\overrightarrow{n}'}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d+1}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}'),\\
&\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \ldots, \boldsymbol{b}_{0,5}), \quad \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,2n_t+1}, \ldots, \boldsymbol{b}_{t,3n_t+1}) \ \text{ for } t = 1, \ldots, d,\\
&\quad \delta, \delta_0, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ u_0, \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \ z_0 := u_0^{-1},\\
&\quad \begin{pmatrix} \overrightarrow{z}_{t,1} \\ \vdots \\ \overrightarrow{z}_{t,n_t} \end{pmatrix} := Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q), \quad \begin{pmatrix} \overrightarrow{u}_{t,1} \\ \vdots \\ \overrightarrow{u}_{t,n_t} \end{pmatrix} := (Z_t^{-1})^{\mathrm{T}} \quad \text{for } t = 1, \ldots, d,\\
&\quad \boldsymbol{h}^*_{0,0} := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{h}^*_{1,0} := (\delta, u_0, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{e}_0 := (\omega, \tau z_0, 0, 0, 0)_{\mathbb{B}_0},\\
&\quad \text{for } t = 1, \ldots, d; \ i = 1, \ldots, n_t;\\
&\qquad \overrightarrow{e}_{t,i} := (0^{i-1}, 1, 0^{n_t-i}) \in \mathbb{F}_q^{n_t}, \quad \overrightarrow{\delta}_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},\\
&\qquad\qquad \overbrace{}^{n_t} \quad \overbrace{}^{n_t} \quad \overbrace{}^{n_t} \quad \overbrace{}^{1}\\
&\qquad \boldsymbol{h}^*_{0,t,i} := \ (\ \delta\overrightarrow{e}_{t,i}, \quad 0^{n_t}, \quad \overrightarrow{\delta}_{t,i}, \quad 0\ )_{\mathbb{B}^*_t},\\
&\qquad \boldsymbol{h}^*_{1,t,i} := \ (\ \delta\overrightarrow{e}_{t,i}, \quad \overrightarrow{u}_{t,i}, \quad \overrightarrow{\delta}_{t,i}, \quad 0\ )_{\mathbb{B}^*_t},\\
&\qquad \boldsymbol{e}_{t,i} := \ (\ \omega\overrightarrow{e}_{t,i}, \quad \tau\overrightarrow{z}_{t,i}, \quad 0^{n_t}, \quad 0\ )_{\mathbb{B}_t}\\
&\quad \boldsymbol{h}^*_{d+1,i} := \delta \boldsymbol{b}^*_{d+1,i} \ \text{ for } i = 1, 2,\\
&\quad \text{return } (\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,..,d}, \mathbb{B}_{d+1}, \mathbb{B}^*_{d+1}, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, \{\boldsymbol{h}^*_{d+1,i}\}_{i=1,2}).
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic machine $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 4, $\mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 11.

Lemma 21 *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

Definition 22 (Problem 5) *Problem 5 is to guess $\beta \in \{0,1\}$, given* $(\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,d+1}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=1,..,d}, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{t,i}\}_{t=1,..,d;i=1,..,n_t}, \{\boldsymbol{h}^*_{\beta,d+1,i}, \boldsymbol{e}_{d+1,i}\}_{i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P5}}_\beta(1^\lambda, \overrightarrow{n})$, *where*

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{P5}}_\beta(1^\lambda, \overrightarrow{n}):\ n_{d+1} := 2, \quad \overrightarrow{n}' := (d+1; \{n_t\}_{t=1,\ldots,d+1}),\\
&\quad (\mathsf{param}_{\overrightarrow{n}'}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d+1}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}'),\\
&\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \ldots, \boldsymbol{b}_{0,5}), \quad \widehat{\mathbb{B}}_{d+1} := (\boldsymbol{b}_{d+1,1}, \boldsymbol{b}_{d+1,2}, \boldsymbol{b}_{d+1,5}, \ldots, \boldsymbol{b}_{d+1,7}),\\
&\quad \delta, \delta_0, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ u_0, \tau \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ z_0 := u_0^{-1},\\
&\quad \boldsymbol{h}^*_{0,0} := (\delta, 0, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{h}^*_{1,0} := (\delta, u_0, 0, \delta_0, 0)_{\mathbb{B}^*_0}, \quad \boldsymbol{e}_0 := (\omega, \tau z_0, 0, 0, 0)_{\mathbb{B}_0},\\
&\quad \boldsymbol{h}^*_{t,i} := \delta \boldsymbol{b}^*_{t,i} \ \text{ for } t = 1, \ldots, d;\ i = 1, \ldots, n_t,\\
&\quad \begin{pmatrix} \overrightarrow{z}_{d+1,1} \\ \overrightarrow{z}_{d+1,2} \end{pmatrix} := Z_{d+1} \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q), \quad \begin{pmatrix} \overrightarrow{u}_{d+1,1} \\ \overrightarrow{u}_{d+1,2} \end{pmatrix} := (Z^{-1}_{d+1})^{\mathrm{T}},\\
&\quad \text{for } i = 1, 2,\\
&\qquad \overrightarrow{e}_{d+1,i} := (0^{i-1}, 1, 0^{2-i}) \in \mathbb{F}_q^2, \quad \overrightarrow{\delta}_{d+1,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2,\\
&\qquad\qquad\qquad \overbrace{\phantom{\delta \overrightarrow{e}_{d+1,i},}}^{2} \ \overbrace{}^{2} \ \overbrace{\phantom{\overrightarrow{\delta}_{d+1,i},}}^{2} \ \overbrace{}^{1}\\
&\qquad \boldsymbol{h}^*_{0,d+1,i} := \ (\ \delta \overrightarrow{e}_{d+1,i}, \quad 0^2, \quad \overrightarrow{\delta}_{d+1,i}, \quad 0\ )_{\mathbb{B}^*_{d+1}},\\
&\qquad \boldsymbol{h}^*_{1,d+1,i} := \ (\ \delta \overrightarrow{e}_{d+1,i}, \quad \overrightarrow{u}_{d+1,i}, \quad \overrightarrow{\delta}_{d+1,i}, \quad 0\ )_{\mathbb{B}^*_{d+1}},\\
&\qquad \boldsymbol{e}_{d+1,i} := \ (\ \omega \overrightarrow{e}_{d+1,i}, \quad \tau \overrightarrow{z}_{d+1,i}, \quad 0^2, \quad 0\ )_{\mathbb{B}_{d+1}},\\
&\quad \text{return } \ (\mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t\}_{t=0,d+1}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=1,..,d},\\
&\qquad\qquad \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{t,i}\}_{t=1,..,d;i=1,..,n_t}, \{\boldsymbol{h}^*_{\beta,d+1,i}, \boldsymbol{e}_{d+1,i}\}_{i=1,2}),
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic machine $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 5, $\mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 11.

Lemma 22 *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, $\mathsf{Adv}^{\mathsf{P5}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

E Generalized Version of Lemma 3

Let V is n-dimensional vector space $\mathbb{F}_q^n$, and V^* its dual. For $\overrightarrow{p} := (p_1, \ldots, p_s) \in \mathbb{F}_q^s$, let

$$
C_{\overrightarrow{p}} := \left\{ (\overrightarrow{x}, \overrightarrow{v}_1, \ldots, \overrightarrow{v}_s) \;\middle|\; \begin{array}{l} \overrightarrow{x} \neq \overrightarrow{0},\ \overrightarrow{x} \cdot \overrightarrow{v}_i = p_i \text{ for } i = 1, \ldots, s \\ \{\overrightarrow{v}_i\}_{i=1,\ldots,s} \text{ are linearly independent over } \mathbb{F}_q, \end{array} \right\} \subset V \times (V^*)^s.
$$

Lemma 23 *For all $\overrightarrow{p}$ such that $C_{\overrightarrow{p}} \neq \emptyset$, for all $(\overrightarrow{x}, \overrightarrow{v}_1, \ldots, \overrightarrow{v}_s) \in C_{\overrightarrow{p}}$, and $(\overrightarrow{r}, \overrightarrow{w}_1, \ldots, \overrightarrow{w}_s) \in C_{\overrightarrow{p}}$,*

$$
\Pr_{Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q),} [\overrightarrow{x}U = \overrightarrow{r} \ \wedge\ \overrightarrow{v}_i Z = \overrightarrow{w}_i \text{ for } i = 1, \ldots, s] = \frac{1}{\sharp C_{\overrightarrow{p}}},
$$

where $U := (Z^{-1})^{\mathrm{T}}$.

Proof. Case that there exists an i such that $\overrightarrow{x} \cdot \overrightarrow{v}_i = p_i \neq 0$: We can assume that $p_i \neq 0$ for $i = 1, \ldots, t$, $p_i = 0$ for $i = t+1, \ldots, s$ through an appropriate change of order of coordinates. Then $t \geq 1$.

For normalized tuple of vectors

$$\overrightarrow{x} = (p_1, \ldots, p_t, 0, \ldots, 0), \qquad \overrightarrow{v}_i := (\overbrace{0, \ldots, 0}^{i-1}, 1, \overbrace{0, \ldots, 0}^{n-i}) \quad \text{for } i = 1, \ldots, s, \tag{20}$$

we will show that $(\overrightarrow{x}U, \overrightarrow{v}_1 Z, \ldots, \overrightarrow{v}_s Z)$ is uniformly distributed on $C_{\overrightarrow{p}}$ for $Z \xleftarrow{\cup} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$. By that, for any pair $(\overrightarrow{x}, \overrightarrow{v}_1, \ldots, \overrightarrow{v}_s) \in C_{\overrightarrow{p}}$, we see that $(\overrightarrow{x}U, \overrightarrow{v}_1 Z, \ldots, \overrightarrow{v}_s Z)$ is uniformly distributed on $C_{\overrightarrow{p}}$ for $Z \xleftarrow{\cup} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$. Therefore, we consider $(\overrightarrow{x}, \overrightarrow{v}_1, \ldots, \overrightarrow{v}_s)$ given by (20) in the following.

Since $Z = (z_{i,j})$ and (18) holds,

$$\overrightarrow{x}U = \frac{1}{\det Z} \sum_{i=1}^{t} p_i(\widetilde{z}_{i,1}, \ldots, \widetilde{z}_{i,n}), \qquad \overrightarrow{v}_i Z = (z_{i,1}, \ldots, z_{i,n}) \quad \text{for } i = 1, \ldots, s.$$

Cofactors $\widetilde{z}_{i,j}$ are determined by $n-1$ rows of Z except for the i-th one. Hence, from formula (17), we see that $(\overrightarrow{x}U, \overrightarrow{v}_1 Z, \ldots, \overrightarrow{v}_s Z)$ is uniformly distributed on $C_{\overrightarrow{p}}$ when $Z \xleftarrow{\cup} GL(n, \mathbb{F}_q)$.

Case that $p_i = \overrightarrow{x} \cdot \overrightarrow{v}_i = 0$ for all $1 \leq i \leq s$: For normalized tuple

$$\overrightarrow{x} = (\overbrace{0, \ldots, 0}^{s}, 1, \overbrace{0, \ldots, 0}^{n-s-1}), \qquad \overrightarrow{v}_i := (\overbrace{0, \ldots, 0}^{i-1}, 1, \overbrace{0, \ldots, 0}^{n-i}) \quad \text{for } i = 1, \ldots, s,$$

we will show that $(\overrightarrow{x}U, \overrightarrow{v}_1 Z, \ldots, \overrightarrow{v}_s Z)$ is uniformly distributed on $C_{\overrightarrow{0}}$ for $Z \xleftarrow{\cup} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$ because of the similar reason as above (where $\overrightarrow{0} := (0, \ldots, 0)$).

Since $Z = (z_{i,j})$ and (18) holds,

$$\overrightarrow{x}U = \frac{1}{\det Z}(\widetilde{z}_{s+1,1}, \ldots, \widetilde{z}_{s+1,n}), \qquad \overrightarrow{v}_i Z = (z_{i,1}, \ldots, z_{i,n}) \quad \text{for } i = 1, \ldots, s.$$

Cofactors $\widetilde{z}_{s+1,j}$ are determined by $n-1$ rows of Z except for the $(s+1)$-th one. In particular, only term $\det Z$ in $(\overrightarrow{x}U, \overrightarrow{v}_1 Z, \ldots, \overrightarrow{v}_s Z)$ is related to the $(s+1)$-th row of Z.

First, since $\widetilde{z}_{s+1,j}$ are determined by the rows of Z except for the $(s+1)$-th one, we see that $\overrightarrow{x}U$ is distributed uniformly on the space orthogonal to $\mathsf{span}\langle \overrightarrow{v}_1 Z, \ldots, \overrightarrow{v}_s Z \rangle$ up to scalar multiplication. Moreover, $\det Z$ is uniformly distributed in $\mathbb{F}_q^{\times}$ (non-zero scalar values), when the $(s+1)$-th row of Z is uniformly distributed in $\mathbb{F}_q^n$ such that $\det Z \neq 0$.

Combining these two facts, we see that $(\overrightarrow{x}U, \overrightarrow{v}_1 Z, \ldots, \overrightarrow{v}_s Z)$ is uniformly distributed on $C_{\overrightarrow{0}}$ when $Z \xleftarrow{\cup} GL(n, \mathbb{F}_q)$. □

F How to Relax the Restriction that $\widetilde{\rho}$ Is Injective

We assume that $\varphi \in \mathbb{N}$ is given in the system. For any access structure $\mathbb{S} := (M, \rho)$ for ciphertext in the CP-FE scheme, $\varphi \geq \max_{t=1}^{d} \#\{i \mid \widetilde{\rho}(i) = t\}$. (In the proposed CP-FE scheme in Section 7, we assume that $\varphi := 1$.)

We will show how to modify the CP-FE scheme to allow $\varphi > 1$ with preserving the security of the CP-FE scheme in Section 7.

We can also show the similar modification of the KP-FE scheme to allow $\varphi > 1$.

F.1 The Modified CP-FE Scheme

1. As for Setup, given $(1^\lambda,\ \overrightarrow{n} := (d; n_1, \ldots, n_d))$, execute $\mathsf{Setup}(1^\lambda,\ \overrightarrow{n}' := (d; n'_1, \ldots, n'_d))$ such that $n'_t := n_t + \varphi$ for $t = 1, \ldots, d$.

2. As for KeyGen, given $(\mathsf{pk},\ \mathsf{sk},\ \Gamma := \{(t, \overrightarrow{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{F}_q^{n_t}) \mid 1 \le t \le d\})$ execute the same procedure as KeyGen except that:

$$\boldsymbol{k}^*_t := \ (\overbrace{\quad \delta \overrightarrow{x}_t, 0^\varphi \quad}^{n'_t} \overbrace{\quad 0^{n'_t}, \quad}^{n'_t} \overbrace{\quad \overrightarrow{\varphi}_t, \quad}^{n'_t} \overbrace{\quad 0 \quad}^{1})_{\mathbb{B}^*_t} \qquad \text{for } (t, \overrightarrow{x}_t) \in \Gamma,$$

3. As for Enc, given $(\mathsf{pk},\ m,\ \mathbb{S} := (M, \rho))$, execute the same procedure as Enc except that:

$$\begin{aligned}
&\text{if } \rho(i) = (t, \overrightarrow{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{F}_q^{n_t}) \qquad \eta_i \xleftarrow{\cup} \mathbb{F}_q, \\
&\boldsymbol{c}_i := \ (\overbrace{\quad s_i \overrightarrow{e}_{t,1} + \theta_i \overrightarrow{v}_i, 0^\varphi, \quad}^{n'_t} \overbrace{\quad 0^{n'_t}, \quad}^{n'_t} \overbrace{\quad 0^{n'_t}, \quad}^{n'_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t} \\
&\text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \qquad \eta_i \xleftarrow{\cup} \mathbb{F}_q, \\
&\boldsymbol{c}_i := \ (\overbrace{\quad s_i \overrightarrow{v}_i, 0^\varphi, \quad}^{n'_t} \overbrace{\quad 0^{n'_t}, \quad}^{n'_t} \overbrace{\quad 0^{n'_t}, \quad}^{n'_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}
\end{aligned}$$

F.2 Security

We can prove the security of the modified CP-FE scheme in a manner similar to that of Theorem 2 except that Problem 2 is changed to Modified Problem 2, Lemma 10 is changed, where $\mathcal{B}^+_{2,h}$'s simulation is executed on Modified Problem 2, Game 2-h^+ is changed to Modified Game 2-h^+, and Claim 2 is proven based on Lemma 23 in place of Lemma 3.

Here we only show the essence of the change by using Modified Game 2-h^+. The Modified Game 2-h^+ is the same as Game 2-h^+ except that $Z_t \xleftarrow{\cup} GL(n'_t, \mathbb{F}_q)$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $t = 1, \ldots, d$, where for each t such that $\{i_\kappa \mid \widetilde{\rho}(i_\kappa) = t,\ 1 \le \kappa \le \varphi\}\}$ is not empty, and for $\kappa = 1, \ldots, \varphi$, the framed part by a box in $\boldsymbol{k}^*_t$ in Eq. (14) is $(\overrightarrow{x}_t, 0^\varphi) \cdot U_t$, and the framed parts by a box in $\boldsymbol{c}_i$ $(:= \boldsymbol{c}_{i_\kappa})$ in Eq. (15) are $(a_i \overrightarrow{e}_{t,1} + \pi_i \overrightarrow{v}_i, 0^{\kappa-1}, 1, 0^{\varphi-\kappa}) \cdot Z_t$ and $(a_i \overrightarrow{v}_i, 0^{\kappa-1}, 1, 0^{\varphi-\kappa}) \cdot Z_t$. By using Modified Problem 2, $\mathcal{B}^+_{2,h}$ can simulate the ciphertexts, $\boldsymbol{c}_{i_\kappa}$. By applying Lemma 23, we can prove Claim 2 for the changed simulation by $\mathcal{B}^+_{2,h}$ in a manner similar to the proof of Claim 2.

G Special Cases

This section describes special cases, KP-ABE and CP-ABE, of the proposed FE schemes given in Sections 6 and 7. Here, the underlying attribute vectors, $\{\overrightarrow{x}_t\}_{t \in \{1,\ldots,d\}}$ and $\{\overrightarrow{v}_i\}_{i \in \{1,\ldots,\ell\}}$, are specialized to two-dimensional vectors for the equality relation, e.g., $\overrightarrow{x}_t := (1, x_t)$ and $\overrightarrow{v}_i := (v_i, -1)$, where $\overrightarrow{x}_t \cdot \overrightarrow{v}_i = 0$ iff $x_t = v_i$. These schemes are also adaptively payload hiding under the DLIN assumption.

G.1 KP-ABE with Non-Monotone Access Structures

$\mathsf{Setup}(1^\lambda,\ \overrightarrow{n} := (d; 2, \ldots, 2)) :\quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),$

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\quad \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \boldsymbol{b}_{t,2}, \boldsymbol{b}_{t,7}) \quad \text{for } t = 1, .., d,$

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*),\quad \widehat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, \boldsymbol{b}_{t,2}^*, \boldsymbol{b}_{t,5}^*, \boldsymbol{b}_{t,6}^*) \quad \text{for } t = 1, .., d,$

$\mathsf{pk} := (1^\lambda, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d}),\quad \mathsf{sk} := \{\widehat{\mathbb{B}}_t^*\}_{t=0,\ldots,d},$

return $\mathsf{pk}, \mathsf{sk}.$

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (M, \rho)) :$

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

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

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

if $\rho(i) = (t, \overrightarrow{v}_i := (v_i, -1) \in \mathbb{F}_q^2 \setminus \{\overrightarrow{0}\}),\qquad \theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \overrightarrow{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^2,$

$$\boldsymbol{k}_i^* := \Big(\overbrace{s_i + \theta_i v_i,\quad -\theta_i}^{2},\ \overbrace{0,\quad 0}^{2},\ \overbrace{\overrightarrow{\eta}_i}^{2},\ \overbrace{0}^{1}\Big)_{\mathbb{B}_t^*},$$

if $\rho(i) = \neg(t, \overrightarrow{v}_i),\qquad \overrightarrow{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^2,$

$$\boldsymbol{k}_i^* := \Big(\overbrace{s_i v_i,\quad -s_i}^{2},\ \overbrace{0,\quad 0}^{2},\ \overbrace{\overrightarrow{\eta}_i}^{2},\ \overbrace{0}^{1}\Big)_{\mathbb{B}_t^*},$$

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

$\mathsf{Enc}(\mathsf{pk},\ m,\ \Gamma := \{(t, \overrightarrow{x}_t := (1, x_t) \in \mathbb{F}_q^2 \setminus \{\overrightarrow{0}\}) \mid 1 \le t \le d\}) :$

$\omega, \varphi_0, \varphi_t, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q \text{ for } (t, \overrightarrow{x}_t) \in \Gamma,$

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

$$\boldsymbol{c}_t := \Big(\overbrace{\omega,\quad \omega x_t}^{2},\ \overbrace{0,\quad 0}^{2},\ \overbrace{0,\quad 0}^{2},\ \overbrace{\varphi_t}^{1}\Big)_{\mathbb{B}_t} \quad \text{for } (t, \overrightarrow{x}_t) \in \Gamma,$$

$c_{d+1} := g_T^\zeta m,\quad \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, c_{d+1}).$

return $\mathsf{ct}_\Gamma.$

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_\ell^*),\ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, c_{d+1})) :$

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \overrightarrow{x}_t)\}$, then compute I and $\{\alpha_i\}_{i\in I}$ such that

$\overrightarrow{1} = \sum_{i\in I} \alpha_i M_i,$ where M_i is the i-th row of $M,$ and

$I \subseteq \{i \in \{1, \ldots, \ell\} \quad | \quad [\rho(i) = (t, \overrightarrow{v}_i) \ \wedge\ (t, \overrightarrow{x}_t) \in \Gamma \ \wedge\ v_i = x_t]$

$\qquad\qquad \vee\ [\rho(i) = \neg(t, \overrightarrow{v}_i) \ \wedge\ (t, \overrightarrow{x}_t) \in \Gamma \ \wedge\ v_i \neq x_t]\ \}.$

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

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

G.2 CP-ABE with Non-Monotone Access Structures

$\mathsf{Setup}(1^\lambda,\ \overrightarrow{n} := (d; 2, \ldots, 2)) :\quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),$

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\quad \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \boldsymbol{b}_{t,2}, \boldsymbol{b}_{t,7}) \quad \text{for } t = 1, \ldots, d,$

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*),\quad \widehat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, \boldsymbol{b}_{t,2}^*, \boldsymbol{b}_{t,5}^*, \boldsymbol{b}_{t,6}^*) \quad \text{for } t = 1, \ldots, d,$

$\mathsf{pk} := (1^\lambda, \mathsf{param}_{\overrightarrow{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d}),\quad \mathsf{sk} := \{\widehat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}.$

return pk, sk.

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \ \Gamma := \{(t, \overrightarrow{x}_t := (1, x_t) \in \mathbb{F}_q^2 \setminus \{\overrightarrow{0}\}) \mid 1 \le t \le d, \}) :$

$\delta, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \overrightarrow{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ such that $(t, \overrightarrow{x}_t) \in \Gamma,$

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

$$\boldsymbol{k}_t^* := (\overbrace{\delta,\quad \delta x_t,}^{2}\ \overbrace{0,\quad 0,}^{2}\ \overbrace{\overrightarrow{\varphi}_t,}^{2}\ \overbrace{0}^{1})_{\mathbb{B}_t^*} \quad \text{for } (t, \overrightarrow{x}_t) \in \Gamma,$$

$\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\overrightarrow{x}_t)\in\Gamma})$

return sk_Γ.

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

$\overrightarrow{f} \xleftarrow{\mathsf{R}} \mathbb{F}_q^r,\ \overrightarrow{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{f}^{\mathrm{T}},\ s_0 := \overrightarrow{1} \cdot \overrightarrow{f}^{\mathrm{T}},\ \eta_0, \eta_i, \theta_i, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q\ (i = 1, .., \ell),$

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

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

if $\rho(i) = (t, \overrightarrow{v}_i := (v_i, -1) \in \mathbb{F}_q^2 \setminus \{\overrightarrow{0}\})$,

$$\boldsymbol{c}_i := (\overbrace{s_i + \theta_i v_i,\quad -\theta_i,}^{2}\ \overbrace{0,\quad 0,}^{2}\ \overbrace{0,\quad 0,}^{2}\ \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

if $\rho(i) = \neg(t, \overrightarrow{v}_i)$,

$$\boldsymbol{c}_i := (\overbrace{s_i v_i,\quad -s_i,}^{2}\ \overbrace{0,\quad 0,}^{2}\ \overbrace{0,\quad 0,}^{2}\ \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

$c_{d+1} := g_T^\zeta m,\quad \mathsf{ct}_\mathbb{S} := (\mathbb{S}, \boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1}).$

return $\mathsf{ct}_\mathbb{S}$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\overrightarrow{x}_t)\in\Gamma}),\ \mathsf{ct}_\mathbb{S} := (\mathbb{S}, \boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})) :$

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \overrightarrow{x}_t)\}$, then compute I and $\{\alpha_i\}_{i\in I}$ such that

$\overrightarrow{1} = \sum_{i\in I} \alpha_i M_i,$ where M_i is the i-th row of $M,$ and

$I \subseteq \{i \in \{1, \ldots, \ell\} \mid [\rho(i) = (t, \overrightarrow{v}_i) \ \wedge\ (t, \overrightarrow{x}_t) \in \Gamma \ \wedge\ v_i = x_t]$

$\qquad\qquad \vee\ [\rho(i) = \neg(t, \overrightarrow{v}_i) \ \wedge\ (t, \overrightarrow{x}_t) \in \Gamma \ \wedge\ v_i \neq x_t]\ \}.$

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

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