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

Tatsuaki Okamoto[1] and Katsuyuki Takashima[2]

[1] NTT, 3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585, Japan
okamoto.tatsuaki@lab.ntt.co.jp
[2] Mitsubishi Electric, 5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

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 well-established 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.

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 (ek) and the decryption-key (dk) such that ek and dk should be equivalent. The innovative notion of public-key cryptosystems in the 1970's relaxed this restriction, where ek and dk differ and ek 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 ek and dk where the ek and dk are parameterized by x and v, respectively, and dk_v can decrypt a ciphertext encrypted with $\mathsf{ek}_x := (\mathsf{ek}, x)$ iff $R(x, v)$ holds for some relation R. FE has various applications in the areas of access control for databases, mail services, and contents distribution [2, 7, 9, 16, 17, 22–25, 27].

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

As a more general class of FE, *attribute-based encryption* (ABE) schemes have been proposed [2, 7, 9, 16, 17, 22–25, 27], where either one of the parameters for ek and dk is a tuple of attributes and the other is a access structure or (monotone) span program $\hat{M}$ along with a tuple of attributes, e.g.,

$x := (x_1, \ldots, x_d)$ for ek and $v := (\hat{M}, (v_1, \ldots, v_d))$ for dk, or $v := (v_1, \ldots, v_d)$ for dk and $x := (\hat{M}, (x_1, \ldots, x_d))$ for ek. Here, some elements of the tuple may be empty. The component-wise equality relations for (non-empty) attribute components, e.g., $\{x_t = v_t\}_{t \in \{1,\ldots,d\}}$, are input to (monotone) span program $\hat{M}$, and $R(x, v)$ holds iff the truth-value vector of $(\mathsf{T}(x_1 = v_1), \ldots, \mathsf{T}(x_d = v_d))$ 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 $\hat{M}$ is embedded into decryption-key dk_v (e.g., $v := (\hat{M}, (v_1, \ldots, v_d))$ for dk and $x := (x_1, \ldots, x_d)$ for ek), it is called key-policy ABE (KP-ABE). If $\hat{M}$ is embedded into a ciphertext (e.g., $x := (\hat{M}, (x_1, \ldots, x_d))$ for ek and $v := (v_1, \ldots, v_d)$ for dk), it is ciphertext-policy ABE (CP-ABE).

Inner-product encryption (IPE) [17] is also a class of FE, where each parameter for ek and dk 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 ek and dk, 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 *well-established* 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 ek and dk 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., $x := (\overrightarrow{x}_1, \ldots, \overrightarrow{x}_d) \in \mathbb{F}_q^{n_1+\cdots+n_d}$ for ek and $v := (\hat{M}, (\overrightarrow{v}_1, \ldots, \overrightarrow{v}_d) \in \mathbb{F}_q^{n_1+\cdots+n_d})$ for dk. The component-wise inner-product relations for attribute vector components, e.g., $\{\overrightarrow{x}_t \cdot \overrightarrow{v}_t = 0 \text{ or not }\}_{t\in\{1,\ldots,d\}}$, are input to span program $\hat{M}$, and $R(x, v)$ holds iff the truth-value vector of $(\mathsf{T}(\overrightarrow{x}_1 \cdot \overrightarrow{v}_1 = 0), \ldots, \mathsf{T}(\overrightarrow{x}_t \cdot \overrightarrow{v}_t = 0))$ is accepted by span program $\hat{M}$.

Similarly to ABE, we propose two types of FE schemes, the KP-FE and CP-FE schemes. Although this paper focuses on the KP-FE scheme, similar results are obtained for the CP-FE scheme (see the full version of this paper).

Note that in Section 5, 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 $(\overrightarrow{x}_1, \ldots, \overrightarrow{x}_d)$, where $1 \leq t \leq d$ means that t is an element of some subset of $\{1, \ldots, d\}$, and parameter v for the decryption key is expressed by $\mathbb{S} := (M, \rho)$ (not by $\hat{M} := (M, \rho)$ along with $(\overrightarrow{v}_1, \ldots, \overrightarrow{v}_d)$ as described above), where ρ in $\mathbb{S}$ is abused as ρ in $\hat{M}$ combined with $(\overrightarrow{v}_1, \ldots, \overrightarrow{v}_d)$ (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 $x_t = v_t$.
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 (see the full version for the proof).

   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 (see the full version for the construction and proof).

– The proposed FE scheme with such a wide class of relations is proven to be *adaptively secure* (adaptively payload-hiding against CPA) under a well-established 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 well-established assumptions; the Waters IBE scheme [26] under the DBDH assumption, and the Waters IBE scheme [28] under the DBDH and DLIN assumptions.

  The DLIN assumption is considered to be the simplest decisional assumption regarding pairing group $\mathbb{G}$, since the DLIN assumption is defined only over $\mathbb{G}$, the DDH assumption does not hold in $\mathbb{G}$, and the DBDH assumption is defined over two groups $\mathbb{G}$ and $\mathbb{G}_T$.

– 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 (and the full version of this paper) 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 $(4n+5)\cdot|G|$, 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 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 8-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 the full version of this paper for the construction and security proof).

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, $A(x) \rightarrow a$ (e.g., $A(x) \rightarrow 1$) denotes the event that machine (algorithm) A outputs a on input x. A function $f : \mathbb{N} \rightarrow \mathbb{R}$ 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 bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$, $(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^{N} x_i \boldsymbol{b}_i$ and $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^{N} y_i \boldsymbol{b}_i^*$.

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 by 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 by 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 the full version of this paper. 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.

$\mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n} := (d; n_1, \ldots, n_d)) : \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \quad \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,$
$N_0 := 5, \quad N_t := 4n_t \quad \text{for } t = 1, \ldots, d,$
for $t = 0, \ldots, d, \quad \mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t, \mathsf{param}_{\mathbb{G}}),$
$X_t := (\chi_{t,i,j})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t, \mathbb{F}_q), \ (\vartheta_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1},$
$\boldsymbol{b}_{t,i} := (\chi_{t,i,1}, \ldots, \chi_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j}, \ \mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,N_t}),$
$\boldsymbol{b}^*_{t,i} := (\vartheta_{t,i,1}, \ldots, \vartheta_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j}, \ \mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,N_t}),$
$g_T := e(G, G)^\psi, \quad \mathsf{param}_{\overrightarrow{n}} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,\ldots,d}, \ g_T)$
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*.*

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

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 secure if all polynomial time adversaries have at most a negligible advantage in the above game.*

Similarly we can define a *ciphertext-policy* FE (CP-FE) scheme (see the full version of this paper).

4 Assumption

Definition 8 (DLIN: Decisional Linear Assumption). *The DLIN problem is to guess* $\beta \in \{0,1\}$*, given* $(\mathsf{param}_\mathbb{G}, G, \xi G, \kappa G, \omega\xi G, \gamma\kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$*, where*

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

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 Proposed KP-FE Scheme

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 the full version of this paper.

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).

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

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \ \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1}, .., \boldsymbol{b}_{t,4n_t})\quad$ 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 $\mathsf{pk}, \mathsf{sk}.$

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

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

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

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

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

$$\boldsymbol{k}^*_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{t,2}, .., \theta_i v_{i,n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_{i,1}, .., \eta_{i,n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t})_{\mathbb{B}^*_t},$$

if $\rho(i) = \neg(t, \overrightarrow{v}_i),\qquad \eta_{i,1}, \ldots, \eta_{i,n_t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$

$$\boldsymbol{k}^*_i := (\overbrace{s_i(v_{i,1}, .., v_{i,n_t})}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_{i,1}, .., \eta_{i,n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t})_{\mathbb{B}^*_t},$$

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

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

$\delta, \varphi_0, \varphi_{t,1}, \ldots, \varphi_{t,n_t}, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $(t, \overrightarrow{x}_t) \in \Gamma,$

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

$\boldsymbol{c}_t := (\overbrace{\ \delta(x_{t,1},..,x_{t,n_t}),}^{n_t}\overbrace{\ 0^{n_t},}^{n_t}\overbrace{\ 0^{n_t},}^{n_t}\overbrace{\ \varphi_{t,1},..,\varphi_{t,n_t}\ }^{n_t})_{\mathbb{B}_t}$ 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

$s_0 = \sum_{i\in I} \alpha_i s_i$, 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]

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

6 Security

The proofs of Lemmas 1–4 and 6–8, and Claim 1 are given in the full version of this paper.

6.1 Theorem

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 $\mathcal{E}_0, \mathcal{E}_h^+, \mathcal{E}_{h+1}$ ($h = 0,\ldots,\nu-1$), whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KP\text{-}FE,PH}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}_0}^{\mathsf{DLIN}}(\lambda) + \sum_{h=0}^{\nu-1} \left(\mathsf{Adv}_{\mathcal{E}_h^+}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{h+1}}^{\mathsf{DLIN}}(\lambda)\right) + \epsilon,$$

where ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (2d\nu+12\nu+d+7)/q$.

6.2 Lemmas

We will show three lemmas for the proof of Theorem 1.

Definition 9 (Problem 1). *Problem 1 is to guess β, given* $(\mathsf{param}_{\overrightarrow{n}}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,i}\}_{t=1,\ldots,d;i=1,\ldots,n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \overrightarrow{n})$*, where*

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \overrightarrow{n}): \quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),\\
&\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1}, .., \boldsymbol{b}_{t,4n_t}) \ \text{ for } t = 1, .., d,\\
&\quad \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}),\ \widehat{\mathbb{B}}^*_t := (\boldsymbol{b}^*_{t,1}, .., \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,2n_t+1}, .., \boldsymbol{b}^*_{t,3n_t}) \ \text{ for } t = 1, .., d,\\
&\quad u_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ \delta, \delta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (u_{t,i,j})_{i,j=1,\ldots,n_t} \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q) \ \text{ for } t = 1, .., d,\\
&\quad \boldsymbol{e}_{0,0} := (\delta, 0, 0, 0, \delta_0)_{\mathbb{B}_0}, \quad \boldsymbol{e}_{1,0} := (\delta, u_0, 0, 0, \delta_0)_{\mathbb{B}_0},\\
&\quad \text{for } t = 1, \ldots, d; \quad i = 1, \ldots, n_t;\\
&\qquad \delta_{t,i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ for } j = 1, \ldots, n_t,\\
&\qquad \boldsymbol{e}_{0,t,i} := (\ \overbrace{0^{i-1}, \delta, 0^{n_t-i}}^{n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{\delta_{t,i,1}, .., \delta_{t,i,n_t}}^{n_t}\ )_{\mathbb{B}_t},\\
&\qquad \boldsymbol{e}_{1,t,i} := (\ 0^{i-1}, \delta, 0^{n_t-i},\ u_{t,i,1}, .., u_{t,i,n_t},\ 0^{n_t},\ \delta_{t,i,1}, .., \delta_{t,i,n_t}\ )_{\mathbb{B}_t},\\
&\quad \text{return } \ (\mathsf{param}_{\overrightarrow{n}}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{e}_{\beta,0}, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,i}\}_{t=1,\ldots,d;i=1,\ldots,n_t}),
\end{aligned}
$$

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 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, $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

Definition 10 (Problem 2). *Problem 2 is to guess β, given* $(\mathsf{param}_{\overrightarrow{n}}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \boldsymbol{h}^*_{\beta,0}, \boldsymbol{e}_0, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=1,\ldots,n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, \overrightarrow{n})$*, where*

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, \overrightarrow{n}): \quad (\mathsf{param}_{\overrightarrow{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \overrightarrow{n}),\\
&\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+1}, .., \boldsymbol{b}_{t,4n_t}) \quad \text{for } t = 1, .., d,\\
&\quad \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, .., \boldsymbol{b}^*_{0,4}),\ \widehat{\mathbb{B}}^*_t := (\boldsymbol{b}^*_{t,1}, .., \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,2n_t+1}, .., \boldsymbol{b}^*_{t,3n_t}) \quad \text{for } t = 1, .., d,\\
&\quad \tau, u_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ \omega, \delta, \gamma_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ w_0 := \tau / u_0,\\
&\quad (z_{t,i,j})_{i,j=1,..,n_t} := Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q),\ (u_{t,i,j})_{i,j=1,..,n_t} := (Z_t^{-1})^{\mathrm{T}} \text{ for } t = 1, .., d,\\
&\quad \boldsymbol{h}^*_{0,0} := (\omega, 0, 0, \gamma_0, 0)_{\mathbb{B}^*_0},\ \boldsymbol{h}^*_{1,0} := (\omega, w_0, 0, \gamma_0, 0)_{\mathbb{B}^*_0},\ \boldsymbol{e}_0 := (\delta, u_0, 0, 0, 0)_{\mathbb{B}_0},\\
&\quad \text{for } t = 1, \ldots, d;\ i = 1, \ldots, n_t;\\
&\qquad \left(w_{t,i,j}\right)_{i,j=1,\ldots,n_t} := \tau \cdot Z_t, \quad \gamma_{t,i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q \quad \text{for } j = 1, .., n_t,
\end{aligned}
$$

$$
\begin{array}{lcccccc}
 & \overbrace{\quad}^{n_t} & \overbrace{\quad}^{n_t} & \overbrace{\quad}^{n_t} & \overbrace{\quad}^{n_t} & \\
\boldsymbol{h}^*_{0,t,i} := (& 0^{i-1}, \omega, 0^{n_t-i}, & 0^{n_t}, & \gamma_{t,i,1}, .., \gamma_{t,i,n_t}, & 0^{n_t} &)_{\mathbb{B}^*_t} \\
\boldsymbol{h}^*_{1,t,i} := (& 0^{i-1}, \omega, 0^{n_t-i}, & w_{t,i,1}, .., w_{t,i,n_t}, & \gamma_{t,i,1}, .., \gamma_{t,i,n_t}, & 0^{n_t} &)_{\mathbb{B}^*_t} \\
\boldsymbol{e}_{t,i} := & (0^{i-1}, \delta, 0^{n_t-i}, & u_{t,i,1}, .., u_{t,i,n_t}, & 0^{n_t}, & 0^{n_t} &)_{\mathbb{B}_t},
\end{array}
$$

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

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 9.*

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* $(\overrightarrow{r}, \overrightarrow{w}) \in C_p$, $\Pr[\overrightarrow{x}U = \overrightarrow{r} \ \wedge \ \overrightarrow{v}Z = \overrightarrow{w}] = 1/\sharp C_p$, *where* $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$.

6.3 Proof of Theorem 1

Proof Outline : 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 target 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 target 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 target 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 $A \leq B + \epsilon(\lambda)$ 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 target ciphertext replied by the simulator is equivalent to those of Game 0 when $\beta = 0$ and Game 1 when $\beta = 1$. That is, the advantage 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 by 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 $\mathcal{B}_h^+$ 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., $\mathcal{B}_h^+$'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 $\mathcal{B}_h^+$'s simulation using Problem 2 with $\beta = 1$) are correlated for the case that $\mathbb{S}$ accepts Γ or for simulator $\mathcal{B}_h^+$'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:

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (-s_0, \boxed{0}, 1, \eta_0, 0)_{\mathbb{B}_0^*}, \\ \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \boldsymbol{k}_i^* := (s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, .., \theta_i v_{i,n_t}, \boxed{0^{n_t}}, \eta_{i,1}, .., \eta_{i,n_t}, 0^{n_t})_{\mathbb{B}_t^*}, \\ \quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \boldsymbol{k}_i^* := (s_i(v_{i,1}, .., v_{i,n_t}), \boxed{0^{n_t}}, \eta_{i,1}, .., \eta_{i,n_t}, 0^{n_t})_{\mathbb{B}_t^*}, \end{array}\right\} \quad (1)$$

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

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

where $b \xleftarrow{\cup} \{0,1\}; \delta, \zeta, \varphi_0, \varphi_{t,1}, \ldots, \varphi_{t,n_t} \xleftarrow{\cup} \mathbb{F}_q$, and $\overrightarrow{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\overrightarrow{0}\}$.

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

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

$$\boldsymbol{c}_t := (\delta(x_{t,1}, .., x_{t,n_t}), \boxed{r_{t,1}, .., r_{t,n_t}}, 0^{n_t}, \varphi_{t,1}, .., \varphi_{t,n_t})_{\mathbb{B}_t} \text{ for } (t, \overrightarrow{x}_t) \in \Gamma, \quad (4)$$

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

where $r_0, r_{t,1}, \ldots, r_{t,n_t} \xleftarrow{\cup} \mathbb{F}_q$.

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 target ciphertext are:

$$\left.\begin{array}{l} \boldsymbol{k}_0^* := (-s_0, \boxed{w_0}, 1, \eta_0, 0)_{\mathbb{B}_0^*}, \\ \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \overrightarrow{v}_i) \\ \quad\quad \boldsymbol{k}_i^* := (s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, .., \theta_i v_{i,n_t}, \boxed{w_{i,1}, .., w_{i,n_t}}, \eta_{i,1}, .., \eta_{i,n_t}, 0^{n_t})_{\mathbb{B}_t^*}, \\ \quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i) \\ \quad\quad \boldsymbol{k}_i^* := (s_i(v_{i,1}, .., v_{i,n_t}), \boxed{\overline{w}_{i,1}, .., \overline{w}_{i,n_t}}, \eta_{i,1}, .., \eta_{i,n_t}, 0^{n_t})_{\mathbb{B}_t^*}, \end{array}\right\} \quad (6)$$

$$\boldsymbol{c}_t := (\delta(x_{t,1}, .., x_{t,n_t}), \boxed{r_{t,1}, .., r_{t,n_t}}, 0^{n_t}, \varphi_{t,1}, , , , \varphi_{t,n_t})_{\mathbb{B}_t} \text{ for } (t, \overrightarrow{x}_t) \in \Gamma, \quad (7)$$

where $w_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\overrightarrow{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\overrightarrow{a}^{\mathrm{T}} := (a_1, \ldots, a_\ell)^{\mathrm{T}} := M \cdot \overrightarrow{g}^{\mathrm{T}}$, $\tau_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ $(i = 1, \ldots, \ell)$, $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $t = 1, \ldots, d$,

$$
\begin{aligned}
&(w_{i,1}, \ldots, w_{i,n_t}) := (a_i + \tau_i v_{i,1}, \tau_i v_{i,2}, \ldots, \tau_i v_{i,n_t}) \cdot Z_t, \\
&(\overline{w}_{i,1}, \ldots, \overline{w}_{i,n_t}) := a_i (v_{i,1}, \ldots, v_{i,n_t}) \cdot Z_t, \\
&(r_{t,1}, \ldots, r_{t,n_t}) := (x_{t,1}, \ldots, x_{t,n_t}) \cdot U_t.
\end{aligned}
$$

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 target ciphertext are:

$$
\left.
\begin{array}{l}
\boldsymbol{k}_0^* := (-s_0, w_0, 1, \eta_0, 0)_{\mathbb{B}_0^*}, \\
\text{for } i = 1, \ldots, \ell, \\
\text{if } \rho(i) = (t, \overrightarrow{v}_i), \boldsymbol{k}_i^* := (s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, .., \theta_i v_{i,n_t}, \boxed{0^{n_t}}, \eta_{i,1}, .., \eta_{i,n_t}, 0^{n_t})_{\mathbb{B}_t^*}, \\
\text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \boldsymbol{k}_i^* := (s_i(v_{i,1}, .., v_{i,n_t}), \boxed{0^{n_t}}, \eta_{i,1}, .., \eta_{i,n_t}, 0^{n_t})_{\mathbb{B}_t^*},
\end{array}
\right\} \quad (8)
$$

$$
\boldsymbol{c}_t := (\delta(x_{t,1}, \ldots, x_{t,n_t}), \boxed{r_{t,1}, \ldots, r_{t,n_t}}, 0^{n_t}, \varphi_{t,1}, \ldots, \varphi_{t,n_t})_{\mathbb{B}_t} \quad \text{for } (t, \overrightarrow{x}_t) \in \Gamma,
$$

where $r_{t,1}, \ldots, r_{t,n_t} \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

Game 3 : Same as Game 2-ν except that $\boldsymbol{c}_0$ and c_{d+1} of the target 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 $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$).

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 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KP\text{-}FE,PH}}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) \leq \left|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| + \sum_{h=0}^{\nu-1} \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda)\right| + \sum_{h=0}^{\nu-1} \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h+1))}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)\right| + \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}_0}^{\mathsf{P1}}(\lambda) + \sum_{h=0}^{\nu-1} \mathsf{Adv}_{\mathcal{B}_h^+}^{\mathsf{P2}}(\lambda) + \sum_{h=0}^{\nu-1} \mathsf{Adv}_{\mathcal{B}_{h+1}}^{\mathsf{P2}}(\lambda) + (2d\nu + 2\nu + d + 2)/q \leq \mathsf{Adv}_{\mathcal{E}_0}^{\mathsf{DLIN}}(\lambda) + \sum_{h=0}^{\nu-1} \left(\mathsf{Adv}_{\mathcal{E}_h^+}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{h+1}}^{\mathsf{DLIN}}(\lambda)\right) + (2d\nu + 12\nu + d + 7)/q.$ This completes the proof of Theorem 1. □

Lemma 4. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_0$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_0}^{\mathsf{P1}}(\lambda) + (d+1)/q$.*

Lemma 5. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_h^+$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h^+)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_h^+}^{\mathsf{P2}}(\lambda) + (d+1)/q$.*

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

1. $\mathcal{B}_h^+$ is given a Problem 2 instance, $(\mathsf{param}_{\overrightarrow{n}}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}_0^*, \boldsymbol{h}_{\beta,0}^*, \boldsymbol{e}_0, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}_t^*, \boldsymbol{h}_{\beta,t,j}^*, \boldsymbol{e}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,n_t})$.
2. $\mathcal{B}_h^+$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_h^+$ 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^+), that is a part of the Problem 2 instance.
4. When the ι-th key query is issued for access structure $\mathbb{S} := (M, \rho)$, $\mathcal{B}_h^+$ answers as follows:
   (a) When $1 \leq \iota \leq h$, $\mathcal{B}_h^+$ answers semi-functional key $(\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_\ell^*)$ with Eq. (8), that is computed by using $\{\widehat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}$ of the Problem 2 instance.
   (b) When $\iota = h+1$, $\mathcal{B}_h^+$ calculates $(\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_\ell^*)$ by using $(\boldsymbol{h}_{\beta,0}^*, \{\boldsymbol{h}_{\beta,t,j}^*\}_{t=1,\ldots,d;j=1,\ldots,n_t})$ of the Problem 2 instance as follows:

$$
\begin{aligned}
&\mu_{t,l}, \widetilde{\mu}_{k,l} \xleftarrow{\mathsf{U}} \mathbb{F}_q \quad \text{for } t = 1, \ldots, d;\ k = 1, \ldots, r;\ l = 1, 2,\\
&\boldsymbol{p}_{\beta,0}^* := \textstyle\sum_{k=1}^r \left(\widetilde{\mu}_{k,1} \boldsymbol{h}_{\beta,0}^* + \widetilde{\mu}_{k,2} \boldsymbol{b}_{0,1}^*\right),\\
&\text{for } t = 1, \ldots, d;\ k = 1, \ldots, r;\ j = 1, \ldots, n_t;\\
&\quad \boldsymbol{p}_{\beta,t,j}^* := \mu_{t,1} \boldsymbol{h}_{\beta,t,j}^* + \mu_{t,2} \boldsymbol{b}_{t,j}^*, \qquad \widetilde{\boldsymbol{p}}_{\beta,t,k,j}^* := \widetilde{\mu}_{k,1} \boldsymbol{h}_{\beta,t,j}^* + \widetilde{\mu}_{k,2} \boldsymbol{b}_{t,j}^*,\\
&\boldsymbol{k}_0^* := -\boldsymbol{p}_{\beta,0}^* + \boldsymbol{b}_{0,3}^*,\\
&\text{for } i = 1, \ldots, \ell,\\
&\quad \text{if } \rho(i) = (t, \overrightarrow{v}_i), \quad \boldsymbol{k}_i^* := \textstyle\sum_{j=1}^{n_t} v_{i,j} \boldsymbol{p}_{\beta,t,j}^* + \sum_{k=1}^r M_{i,k} \widetilde{\boldsymbol{p}}_{\beta,t,k,n_t}^*,\\
&\quad \text{if } \rho(i) = \neg(t, \overrightarrow{v}_i), \quad \boldsymbol{k}_i^* := \textstyle\sum_{j=1}^{n_t} v_{i,j} (\sum_{k=1}^r M_{i,k} \widetilde{\boldsymbol{p}}_{\beta,t,k,j}^*),
\end{aligned}
$$

   where $(M_{i,k})_{i=1,\ldots,\ell;k=1,\ldots,r} := M$.
   (c) When $\iota \geq h+2$, $\mathcal{B}_h^+$ answers normal key $(\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_\ell^*)$ with Eq. (1), that is computed by using $\{\widehat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}$ of the Problem 2 instance.
5. When $\mathcal{B}_h^+$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and $\Gamma := \{(t, \overrightarrow{x}_t) \mid 1 \leq t \leq d\}$ from $\mathcal{A}$, $\mathcal{B}_h^+$ computes the challenge ciphertext $(\boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\overrightarrow{x}_t)\in\Gamma}, c_{d+1})$ such that for $(t, \overrightarrow{x}_t) \in \Gamma$,

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

   where $\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, $\boldsymbol{q}_0 \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{0,5} \rangle$, $\boldsymbol{q}_t \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{t,3n_t+1}, \ldots, \boldsymbol{b}_{t,4n_t} \rangle$, 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, $\mathcal{B}_h^+$ executes the same procedure as that of step 4.

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

Claim 1. *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_h^+$ 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. $\beta = 1$).*

The proof of Claim 1 is given in the full version of this paper. This completes the proof of Lemma 5. □

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

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

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

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 (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. RSA-CT 2005, LNCS, Springer Verlag (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. EUROCRYPT 2004, LNCS, Springer-Verlag (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 (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, EUROCRYPT 2010. LNCS, 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: ASIACRYPT 2009, 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 (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, (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. Eurocrypt 2005, LNCS, vol. 3152, pp.443–459. Springer Verlag, (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)