Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption

Tatsuaki Okamoto[1] and Katsuyuki Takashima[2]

[1] NTT
okamoto.tatsuaki@lab.ntt.co.jp
[2] Mitsubishi Electric
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

Abstract. This paper proposes the first inner product encryption (IPE) scheme that is adaptively secure and fully attribute-hiding (attribute-hiding in the sense of the definition by Katz, Sahai and Waters), while the existing IPE schemes are either fully attribute-hiding but selectively secure or adaptively secure but weakly attribute-hiding. The proposed IPE scheme is proven to be adaptively secure and fully attribute-hiding under the decisional linear assumption in the standard model. The IPE scheme is comparably as efficient as the existing attribute-hiding IPE schemes. We also present a variant of the proposed IPE scheme with the same security that achieves shorter public and secret keys. A hierarchical IPE scheme can be constructed that is also adaptively secure and fully attribute-hiding under the same assumption. In this paper, we extend the dual system encryption technique by Waters into a more general manner, in which new forms of ciphertext and secret keys are employed and new types of information theoretical tricks are introduced along with several forms of computational reduction.

1 Introduction

1.1 Background

Functional encryption (FE) is an advanced class of encryption and it covers identity-based encryption (IBE)[3, 4, 7, 11], hidden-vector encryption (HVE) [8], inner-product encryption (IPE) [15], predicate encryption (PE) and attribute-based encryption (ABE) [2, 13, 23, 16, 22, 24, 19]. In FE, there is a relation $R(v, x)$ which determines what a secret key with parameter v can decrypt a ciphertext encrypted under parameter x. The enhanced functionality and flexibility provided by FE systems are very appealing for many practical applications.

For some applications, the parameters for encryption are required to be hidden from ciphertexts. One of such applications is an advanced notion of PKE with keyword search (PEKS) [6], which we call *PKE with functional search* (PEFS) in this paper. In PEFS, a parameter x (not just a keyword) embedded in a ciphertext is searched (checked) whether $R(v, x)$ holds or not by using a secret key with parameter v. Here, keyword search is a special case of functional

search $R(v, x)$ when $R(v, x) \Leftrightarrow [x = v]$. Parameter x of a ciphertext is often private information and should be hidden from ciphertexts in such applications.

To capture the security requirement, Katz, Sahai and Waters [15] introduced *attribute-hiding* (based on the same notion for HVE by Boneh and Waters [8]), a security notion for FE that is stronger than the basic security requirement, *payload-hiding*. Roughly speaking, attribute-hiding requires that a ciphertext conceal the associated parameter as well as the plaintext, while payload-hiding only requires that a ciphertext conceal the plaintext. Attribute-hiding FE is often called predicate encryption (PE).

The widest class of relations of a FE system in the literature is general non-monotone (span program) relations, which can be expressed using AND, OR, Threshold and NOT gates [19]. FE systems supporting such a wide class of relations, however, have one limitation in that the parameter x of the ciphertext should be revealed to users to decrypt. That is, such FE systems do not satisfy the attribute-hiding security.

To the best of our knowledge, the widest class of relations supported by attribute-hiding FE systems are *inner-product predicates* in [15, 16, 19], which we call the KSW08, LOS$^+$10 and OT10 schemes. Parameters of inner-product predicates are expressed as vectors $\vec{x}$ (for a ciphertext) and $\vec{v}$ (for a secret key), where $R(\vec{v}, \vec{x})$ holds iff $\vec{v} \cdot \vec{x} = 0$. (Here, $\vec{v} \cdot \vec{x}$ denotes the standard inner-product.) In this paper we call FE for inner-product predicates *inner product encryption* (IPE).

Inner-product predicates represent a fairly wide class of relations including equality tests as the simplest case (i.e., anonymous IBE and HVE are very special classes of attribute-hiding IPE), disjunctions or conjunctions of equality tests, and, more generally, CNF or DNF formulas. We note, however, that inner product predicates are less expressive than general (even monotone span program) relations of FE. To use inner product predicates for such general relations, formulas must be written in CNF or DNF form, which can cause a super-polynomial blowup in size for arbitrary formulas.

Among the existing attribute-hiding IPEs, the KSW08 IPE scheme [15] is proven to be only *selectively* secure. Although the LOS$^+$10 and OT10 IPE schemes [16, 19] are proven to be *adaptively* secure, the achieved attribute-hiding security is limited or weaker than that defined in [15]. Here, we call the attribute-hiding security defined in [15] *fully attribute-hiding* and that achieved in [16, 19] *weakly attribute-hiding*. In the fully attribute-hiding security definition [15], adversary $\mathcal{A}$ is allowed to ask a key-query for $\vec{v}$ such that $\vec{v} \cdot \vec{x}^{(0)} = \vec{v} \cdot \vec{x}^{(1)} = 0$ provided that $m^{(0)} = m^{(1)}$ ($\vec{x}^{(b)}$ and $m^{(b)}$ ($b = 0, 1$) are for the challenge ciphertext in the security definition), while in the weakly attribute-hiding security definition [16, 19], $\mathcal{A}$ is only allowed to ask a key-query for $\vec{v}$ such that $\vec{v} \cdot \vec{x}^{(b)} \neq 0$ for all $b \in \{0, 1\}$.

Let us explain the difference between the fully and weakly attribute-hiding definitions in a PEFS system. User Alice provides her secret key, $\mathsf{sk}_{\vec{v}}$, to proxy server Bob, who checks whether $\vec{v} \cdot \vec{x} = 0$ or not for an incoming ciphertext, $\mathsf{ct}_{\vec{x}}$, encrypted with parameter $\vec{x}$. In the weakly attribute-hiding security, privacy of

$\vec{x}$ from $\mathsf{ct}_{\vec{x}}$ is ensured only if $\vec{v}\cdot\vec{x}\neq 0$, but cannot be ensured or some privacy on $\vec{x}$ may be revealed if $\vec{v}\cdot\vec{x}=0$. Here note that there still exists $(n-1)$-dimensional freedom (or room of privacy) of n-dimensional vector $\vec{x}$, even if $\vec{v}$ and the fact that $\vec{v}\cdot\vec{x}=0$ is revealed. For example, let $\vec{v}$ express formula on an email message attributes, [[Subject $= X$] $\vee$ [Subject $= Y$]] $\wedge$ [[Receiver = Alice] $\vee$ [Receiver = Alice's secretary]], and $\vec{x}$ express ciphertext attribute (Subject $= X$, Receiver = Alice). In this case, $\vec{v}\cdot\vec{x}=0$, since the ciphertext attribute expressed by $\vec{x}$ satisfies the formula expressed by $\vec{v}$. Although Bob knows $\mathsf{sk}_{\vec{v}}$ and $\vec{v}$, Bob has no idea which attribute $\vec{x}$ is embedded in $\mathsf{ct}_{\vec{x}}$ except that the ciphertext attribute satisfies the formula, i.e., $\vec{v}\cdot\vec{x}=0$, if the fully attribute-hiding security is achieved. On the other hand, Bob may obtain some additional information on the attribute (e.g., Bob may know that the subject is X, not Y), if only the weakly attribute-hiding security is guaranteed.

The KSW08 IPE scheme is fully attribute-hiding but selectively secure, and the LOS$^+$10 and OT10 IPE schemes are adaptively secure but weakly attribute-hiding. Therefore, there is no IPE scheme that is adaptively secure and fully attribute-hiding simultaneously. As for a more limited class of schemes, HVE (as mentioned above, HVE is a very special class of attribute-hiding IPE), an adaptively secure and fully attribute-hiding HVE scheme has been proposed [10]. For hierarchical IPE (HIPE), the LOS$^+$10 and OT10 HIPE schemes [16, 19] are adaptively secure but weakly attribute-hiding, i.e., there is no HIPE scheme that is adaptively secure and fully attribute-hiding simultaneously.

It is a technically challenging task to achieve an adaptively secure and fully attribute-hiding (H)IPE scheme. Even if we use the powerful dual system encryption technique by Waters, the main difficulty resides in how to change a (normal) secret key queried with $\vec{v}$ to a semi-functional secret key, without knowing $\vec{x}^{(b)}$ $(b=0,1)$ for the challenge ciphertext, i.e., without knowing whether $\vec{v}\cdot\vec{x}^{(b)}=0$ or not, since an adversary may issue key queries with $\vec{v}$ before issuing the challenge ciphertext query with $\vec{x}^{(b)}$ $(b=0,1)$ and two possible cases, $\vec{v}\cdot\vec{x}^{(b)}=0$ (for all $b\in\{0,1\}$) and $\vec{v}\cdot\vec{x}^{(b)}\neq 0$ (for all $b\in\{0,1\}$), are allowed in *fully* attribute-hiding IPE. Note that in *weakly* attribute-hiding IPE, it is always required that $\vec{v}\cdot\vec{x}^{(b)}\neq 0$. At a first glance, it looks hard to achieve it, since the form of semi-functional secret key may be different (e.g., canceled or randomized) depending on whether $\vec{v}\cdot\vec{x}^{(b)}=0$ or not. Another technically challenging target in this paper is to prove the security under the decisional linear (DLIN) assumption (on prime order pairing groups) in the standard model.

1.2 Our Results

This paper proposes the first IPE scheme that is adaptively secure and fully attribute-hiding simultaneously. The proposed IPE scheme is proven to be adaptively secure and fully attribute-hiding under the DLIN assumption in the standard model (Section 4). We also present a variant of the proposed IPE scheme with the same security that achieves shorter master public keys and shorter secret keys (Section 5). A hierarchical IPE (HIPE) scheme can be realized that is also adaptively secure and fully attribute-hiding under the same assumption

(see the full version of this paper [21] for the HIPE scheme). Table 2 in Section 6 compares the proposed IPE schemes with several existing attribute-hiding IPE schemes.

1.3 Key Techniques

To overcome the above-mentioned difficulty, we extend the dual system encryption technique into a more general manner, in which various forms of ciphertext and secret keys are introduced ('normal', 'temporal 0', 'temporal 1', 'temporal 2' and 'unbiased' forms for a ciphertext, and 'normal', 'temporal 1' and 'temporal 2' forms for a secret key), and new types (Types 1, 2, 3) of information theoretical tricks are employed with several forms of computational reduction (the security of Problems 1, 2 and 3 to DLIN). See Table 1 and Figure 1 in Section 4.2 for the outline.

In our approach, all forms ('normal', 'temporal 1' and 'temporal 2') of a secret key do not depend on whether $\vec{v} \cdot \vec{x}^{(b)} = 0$ or not. Although the aim of a 'semi-functional' secret key in the original dual system encryption method is to randomize the semi-functional part, the aim of these forms of a secret-key in our approach is just to encode $\vec{v}$ in a (hidden) subspace for a secret-key.

Another key point in our approach is that we transform a challenge ciphertext to an 'unbiased' ciphertext whose advantage is 0 in the final game, and $\vec{x}^{(b)}$ is randomized to a random vector in a two-dimensional subspace, $\mathsf{span}\langle \vec{x}^{(0)}, \vec{x}^{(1)} \rangle$. In contrast, $\vec{x}^{(b)}$ is randomized to a random vector in the n-dimensional whole space, $\mathbb{F}_q^n$, in [16, 19] for weakly attribute-hiding IPE based on the original dual system encryption technique.

Therefore, in our approach, only $\vec{v}$ is encoded in a (hidden) subspace of the temporal forms of a secret-key, and a random vector in $\mathsf{span}\langle \vec{x}^{(0)}, \vec{x}^{(1)} \rangle$ is encoded in the corresponding (hidden) subspace for the temporal and unbiased forms of a ciphertext.

To realize this approach, our construction is based on the dual pairing vector spaces (DPVS) (Section 2) [16, 19]. A nice property of DPVS is that we can set a hidden linear subspace by concealing the basis of a subspace from the public key. Typically, a pair of dual (or orthonormal) bases, $\mathbb{B}$ and $\mathbb{B}^*$, are randomly generated using random linear transformation, and a part of $\mathbb{B}$ (say $\hat{\mathbb{B}}$) is used as a public key and the corresponding part of $\mathbb{B}^*$ (say $\hat{\mathbb{B}}^*$) is used as a secret key or trapdoor. Therefore, the basis, $\mathbb{B} - \hat{\mathbb{B}}$, is information theoretically concealed against an adversary, i.e., even an infinite power adversary has no idea on which basis is selected as $\mathbb{B} - \hat{\mathbb{B}}$ when $\hat{\mathbb{B}}$ is published. It provides a framework for information theoretical tricks in the public-key setting.

In the proposed (basic) IPE scheme, $\mathsf{span}\langle \mathbb{B} \rangle$ and $\mathsf{span}\langle \mathbb{B}^* \rangle$, are $(4n + 2)$-dimensional (where the dimension of inner-product vectors is n), and, as for public parameter $\hat{\mathbb{B}}$, $\mathsf{span}\langle \hat{\mathbb{B}} \rangle$ is $(2n + 2)$-dimensional, i.e., the basis for the remaining $2n$-dimensional space is information theoretically concealed (ambiguous). We use the $2n$-dimensional hidden subspace to realize the various forms of ciphertext and secret keys and make elaborate game transformations over these forms towards the final goal, the 'unbiased' ciphertext.

The game transformations are alternating over computational and conceptual (information theoretical), and the combinations of three types of information theoretical tricks and three computational tricks (Problems 1, 2 and 3) play a central role in our approach, as shown in Figure 1. Type 1 is a (conceptual) linear transformation inside a (hidden) subspace for a ciphertext, Type 2 is a (conceptual) linear transformation inside a (hidden) subspace for a ciphertext with preserving the corresponding secret key value, and Type 3 is a (conceptual) linear transformation across (hidden and partially public) subspaces. The security of Problems 1, 2 and 3 is reduced to the DLIN assumption.

See Section 4.2 for the details of our techniques, in which the game transformations as well as the form changes of ciphertext and secret keys are summarized in Table 1 and Figure 1.

1.4 Notations

When A is a random variable or distribution, $y \xleftarrow{\mathsf{R}} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \xleftarrow{\mathsf{U}} A$ denotes that y is uniformly selected from A. $y := z$ 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 $\mathbb{F}_q \backslash \{0\}$ by $\mathbb{F}_q^{\times}$. A vector symbol denotes a vector representation over $\mathbb{F}_q$, e.g., $\vec{x}$ denotes $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. For two vectors $\vec{v} = (v_1, \ldots, v_n)$ and $\vec{x} = (x_1, \ldots, x_n)$, $\vec{v} \cdot \vec{x}$ denotes the inner-product $\sum_{i=1}^{n} x_i v_i$. The vector $\vec{0}$ is abused as the zero vector in $\mathbb{F}_q^n$ for any n. X^{T} denotes the transpose of matrix X. I_ℓ denotes the $\ell \times \ell$ identity matrix. A bold face letter denotes an element of vector space $\mathbb{V}$, e.g., $\boldsymbol{x} \in \mathbb{V}$. When $\boldsymbol{b}_i \in \mathbb{V}$ $(i = 1, \ldots, n)$, $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle \subseteq \mathbb{V}$ (resp. $\mathsf{span}\langle \vec{x}_1, \ldots, \vec{x}_n \rangle$) denotes the subspace generated by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ (resp. $\vec{x}_1, \ldots, \vec{x}_n$). For bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$, $(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^{N} x_i \boldsymbol{b}_i$ and $(v_1, \ldots, v_N)_{\mathbb{B}^*} := \sum_{i=1}^{N} v_i \boldsymbol{b}_i^*$. $GL(n, \mathbb{F}_q)$ denotes the general linear group of degree n over $\mathbb{F}_q$.

2 Dual Pairing Vector Spaces (DPVS) and the Decisional Linear (DLIN) Assumption

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* $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ *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 [17, 18]. constructed by using symmetric bilinear pairing groups given in

Definition 1. 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 following symmetric version is obtained by identifying $\mathbb{V} = \mathbb{V}^*$ and $\mathbb{A} = \mathbb{A}^*$ in the asymmetric version.

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* $\phi_{i,j}$ *"canonical 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* $\mathcal{G}_{\mathsf{bpg}}$*.*

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

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

Definition 3 (DLIN: Decisional Linear Assumption [5]). *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* $\mathcal{G}^{\mathsf{DLIN}}_\beta(1^\lambda) : \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \kappa, \delta, \xi, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, Y_0 := (\delta + \sigma)G, Y_1 \xleftarrow{\mathsf{U}} \mathbb{G}, \text{return } (\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta)$*, 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*.*

3 Definition of Inner Product Encryption (IPE)

This section defines predicate encryption (PE) for the class of inner-product predicates, i.e., inner product encryption (IPE) and its security.

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

Definition 4. *An inner product encryption scheme (for predicates $\mathcal{F}$ and attributes Σ) consists of probabilistic polynomial-time algorithms* $\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}$ *and* Dec. *They are given as follows:*

- Setup *takes as input security parameter 1^λ outputs (master) public key* pk *and (master) secret key* sk.
- KeyGen *takes as input the master public key* pk*, secret key* sk*, and predicate vector $\vec{v}$. It outputs a corresponding secret key* $\mathsf{sk}_{\vec{v}}$.
- Enc *takes as input the master public key* pk*, plaintext m in some associated plaintext space,* msg*, and attribute vector $\vec{x}$. It returns ciphertext* $\mathsf{ct}_{\vec{x}}$.
- Dec *takes as input the master public key* pk*, secret key* $\mathsf{sk}_{\vec{v}}$ *and ciphertext* $\mathsf{ct}_{\vec{x}}$*. It outputs either plaintext m or the distinguished symbol $\perp$.*

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

We then define the security notion of IPE, that was called "*adaptively* secure and *fully attribute-hiding*" in Abstract and Section 1. Since we will deal with only this security notion hereafter, we shortly call it "*adaptively attribute-hiding.*"

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

1. Setup *is run to generate keys* pk *and* sk*, and* pk *is given to $\mathcal{A}$.*
2. *$\mathcal{A}$ may adaptively make a polynomial number of key queries for predicate vectors, $\vec{v}$. In response, $\mathcal{A}$ is given the corresponding key* $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$.
3. *$\mathcal{A}$ outputs challenge attribute vector $(\vec{x}^{(0)}, \vec{x}^{(1)})$ and challenge plaintexts $(m^{(0)}, m^{(1)})$, subject to the following restrictions:*
   - *$\vec{v} \cdot \vec{x}^{(0)} \neq 0$ and $\vec{v} \cdot \vec{x}^{(1)} \neq 0$ for all the key queried predicate vectors, $\vec{v}$.*
   - *Two challenge plaintexts are equal, i.e., $m^{(0)} = m^{(1)}$, and any key query $\vec{v}$ satisfies $f_{\vec{v}}(\vec{x}^{(0)}) = f_{\vec{v}}(\vec{x}^{(1)})$, i.e., one of the following conditions.*
     - *$\vec{v} \cdot \vec{x}^{(0)} = 0$ and $\vec{v} \cdot \vec{x}^{(1)} = 0$,*
     - *$\vec{v} \cdot \vec{x}^{(0)} \neq 0$ and $\vec{v} \cdot \vec{x}^{(1)} \neq 0$,*
4. *A random bit b is chosen. $\mathcal{A}$ is given* $\mathsf{ct}_{\vec{x}^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m^{(b)}, \vec{x}^{(b)})$.
5. *The adversary may continue to issue key queries for additional predicate vectors, $\vec{v}$, subject to the restriction given in step 3. $\mathcal{A}$ is given the corresponding key* $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$.
6. *$\mathcal{A}$ outputs a bit b', and wins if $b' = b$.*

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

For each run of the game, the variable s is defined as $s := 0$ if $m^{(0)} \neq m^{(1)}$ for challenge plaintexts $m^{(0)}$ and $m^{(1)}$, and $s := 1$ otherwise.

4 Proposed (Basic) IPE Scheme

4.1 Construction

In the description of the scheme, we assume that the first coordinate, x_1, of input vector, $\vec{x} := (x_1, \ldots, x_n)$, is nonzero. Random dual basis generator $\mathcal{G}_{\mathsf{ob}}(1^\lambda, N)$ is defined at the end of Section 2. We refer to Section 1.4 for notations on DPVS.

$\mathsf{Setup}(1^\lambda,\ n)$:

$(\mathsf{param}_{\mathbb{V}}, \mathbb{B} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{4n+1}), \mathbb{B}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_{4n+1})) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+2)$,

$\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1})$, $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{4n})$,

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

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v} \in \mathbb{F}_q^n \setminus \{\vec{0}\})$: $\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$,

$$\boldsymbol{k}^* := (\overbrace{1}^{1}, \overbrace{\sigma\vec{v}}^{n}, \overbrace{0^{2n}}^{2n}, \overbrace{\vec{\eta}}^{n}, \overbrace{0}^{1})_{\mathbb{B}^*},$$

return $\mathsf{sk}_{\vec{v}} := \boldsymbol{k}^*$.

$\mathsf{Enc}(\mathsf{pk},\ m, \vec{x} \in \mathbb{F}_q^n \setminus \{\vec{0}\})$: $\omega, \varphi, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{c}_1 := (\overbrace{\zeta}^{1}, \overbrace{\omega\vec{x}}^{n}, \overbrace{0^{2n}}^{2n}, \overbrace{0^n}^{n}, \overbrace{\varphi}^{1})_{\mathbb{B}}, \quad c_2 := g_T^{\zeta} m,$$

return $\mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := \boldsymbol{k}^*,\ \mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2))$: $m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*)$, return m'.

[**Correctness**] If $\vec{v} \cdot \vec{x} = 0$, then $e(\boldsymbol{c}_1, \boldsymbol{k}^*) = g_T^{\zeta + \omega\sigma\vec{v}\cdot\vec{x}} = g_T^{\zeta}$.

4.2 Security

Main Theorem (Theorem 1) and Main Lemma (Lemma 1)

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

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

$$\begin{aligned}\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{A}}(\lambda) \leq\ & \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}1}}(\lambda) \\ & + \textstyle\sum_{h=1}^{\nu} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}2\text{-}h}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}2}}(\lambda) \right) + \epsilon,\end{aligned}$$

where $\mathcal{E}_{0\text{-}2\text{-}h}(\cdot) := \mathcal{E}_{0\text{-}2}(h,\cdot)$, $\mathcal{E}_{1\text{-}2\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{1\text{-}2\text{-}1}(h,\cdot)$, $\mathcal{E}_{1\text{-}2\text{-}h\text{-}2}(\cdot) := \mathcal{E}_{1\text{-}2\text{-}2}(h,\cdot)$, ν *is the maximum number of* $\mathcal{A}$*'s key queries and* $\epsilon := (18\nu + 17)/q$.

Proof. First, we execute a preliminary game transformation from Game 0 (original security game in Definition 5) to Game 0', which is the same as Game 0 except that flip a coin $t \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted in step 3 if $t \neq s$. We define that $\mathcal{A}$ wins with probability $1/2$ when the game is aborted (and the advantage in Game 0' is $\mathsf{Pr}[\mathcal{A} \text{ wins }] - 1/2$ as well). Since t is independent from s, the game is aborted with probability $1/2$. Hence, the advantage in Game 0' is a half of that in Game 0, i.e., $\mathsf{Adv}^{\mathsf{IPE,AH},0'}_{\mathcal{A}}(\lambda) = 1/2 \cdot \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{A}}(\lambda)$. Moreover, $\Pr[\mathcal{A} \text{ wins}] = 1/2 \cdot (\Pr[\mathcal{A} \text{ wins} \mid t = 0] + \Pr[\mathcal{A} \text{ wins} \mid t = 1])$ in Game 0' since t is uniformly and independently generated.

As for the conditional probability with $t = 0$, it holds that, for any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_1$ and $\mathcal{E}_2$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, in Game 0',

$$\Pr[\mathcal{A} \text{ wins} \mid t = 0] - 1/2 \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \textstyle\sum_{h=1}^{\nu} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h}}(\lambda) + \epsilon,$$

where $\mathcal{E}_{2\text{-}h}(\cdot) := \mathcal{E}_2(h,\cdot)$ and ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (6\nu + 5)/q$. This is obtained in the same manner as the weakly attribute-hiding security of the OT10 IPE in the full version of [19]: Since the difference between our IPE and the OT10 IPE is only the dimension of the hidden subspaces, i.e., the former has $2n$ and the latter has n, the weakly attribute-hiding security of the OT10 IPE implies the security with $t = 0$ of our IPE.

As for the conditional probability with $t = 1$, i.e., $\Pr[\mathcal{A} \text{ wins} \mid t = 1]$, Lemma 1 (Eq. (1)) holds. Therefore,

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{A}}(\lambda) &= 2 \cdot \mathsf{Adv}^{\mathsf{IPE,AH},0'}_{\mathcal{A}}(\lambda) = \Pr[\mathcal{A} \text{ wins} \mid t = 0] + \Pr[\mathcal{A} \text{ wins} \mid t = 1] - 1 \\
&= (\Pr[\mathcal{A} \text{ wins} \mid t = 0] - 1/2) + (\Pr[\mathcal{A} \text{ wins} \mid t = 1] - 1/2) \\
&\leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}1}}(\lambda) + \textstyle\sum_{h=1}^{\nu} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}2\text{-}h}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}1}}(\lambda) \\
&\quad + \textstyle\sum_{h=1}^{\nu} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}2}}(\lambda) \right) + \epsilon, \text{ where } \epsilon := (18\nu + 17)/q. \quad \square
\end{aligned}$$

Lemma 1 (Main Lemma). *For any adversary* $\mathcal{A}$*, there exist probabilistic machines* $\mathcal{E}_1, \mathcal{E}_{2\text{-}1}$ *and* $\mathcal{E}_{2\text{-}2}$*, whose running times are essentially the same as that of* $\mathcal{A}$*, such that for any security parameter* λ*, in Game 0' (described in the proof of Theorem 1),*

$$\begin{aligned}
&\Pr[\mathcal{A} \text{ wins} \mid t = 1] - 1/2 \\
&\quad \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \textstyle\sum_{h=1}^{\nu} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}2}}(\lambda) \right) + \epsilon, \qquad (1)
\end{aligned}$$

where $\mathcal{E}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{2\text{-}1}(h,\cdot)$, $\mathcal{E}_{2\text{-}h\text{-}2}(\cdot) := \mathcal{E}_{2\text{-}2}(h,\cdot)$, ν *is the maximum number of* $\mathcal{A}$*'s key queries and* $\epsilon := (12\nu + 12)/q$.

Proof Outline of Lemma 1 At the top level strategy of the security proof, an extended form of the dual system encryption by Waters [25] is employed, where ciphertexts and secret keys have three forms, *normal*, *temporal 1* and *temporal 2*. The real system uses only normal ciphertexts and normal secret keys, and temporal 1 and 2 ciphertexts and keys are used only in a sequence of security games for the security proof. (Additionally, ciphertexts have temporal 0 and unbiased forms. See below.)

To prove this lemma, we only consider the $t = 1$ case. We employ Game 0' (described in the proof of Theorem 1) through Game 3. In Game 1, the challenge ciphertext is changed to temporal 0 form. When at most ν secret key queries are issued by an adversary, there are 4ν game changes from Game 1 (Game 2-0-4), Game 2-1-1, Game 2-1-2, Game 2-1-3, Game 2-1-4 through Game 2-ν-1, Game 2-ν-2, Game 2-ν-3, Game 2-ν-4.

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

We summarize these changes in Table 1, where shaded parts indicate the challenge ciphertext or queried key(s) which were changed in a game from the previous game

As usual, we prove that the advantage gaps between neighboring games are negligible.

For $\mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2)$, we focus on $\boldsymbol{c}_1$, and ignore the other part of $\mathsf{ct}_{\vec{x}}$, i.e., c_2, (and call $\boldsymbol{c}_1$ ciphertext) 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, $\boldsymbol{k}^{*\,\mathsf{norm}}$ (with vector $\vec{v}$), is the correct form of the secret key of the proposed IPE scheme, and is expressed by Eq. (2). Similarly, a normal ciphertext (with vector $\vec{x}$), $\boldsymbol{c}_1^{\mathsf{norm}}$, is expressed by Eq. (3). A temporal 0 ciphertext is expressed by Eq. (4). A temporal 1 ciphertext, $\boldsymbol{c}_1^{\mathsf{temp1}}$, is expressed by Eq. (5) and a temporal 1 secret key, $\boldsymbol{k}^{*\,\mathsf{temp1}}$, is expressed by Eq. (6). A temporal 2 ciphertext, $\boldsymbol{c}_1^{\mathsf{temp2}}$, is expressed by Eq. (7) and a temporal 2 secret key, $\boldsymbol{k}^{*\,\mathsf{temp2}}$, is expressed by Eq. (8). An unbiased ciphertext, $\boldsymbol{c}_1^{\mathsf{unbias}}$, is expressed by Eq. (9).

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

Table 1. Outline of Game Descriptions

Game	Challenge ciphertext	Queried keys				
		1	$\cdots$ $h-1$	h	$h+1$ $\cdots$	ν
0'	normal	normal				
1	temporal 0	normal				
2-1-1	temporal 1	normal				
2-1-2	temporal 1	temporal 1	normal			
2-1-3	temporal 2	temporal 1	normal			
2-1-4	temporal 2	temporal 2	normal			
		$\vdots$				
2-h-1	temporal 1	temporal 2		normal		
2-h-2	temporal 1	temporal 2		temporal 1	normal	
2-h-3	temporal 2	temporal 2		temporal 1	normal	
2-h-4	temporal 2	temporal 2		temporal 2	normal	
		$\vdots$				
2-ν-4	temporal 2	temporal 2				temporal 2
3	unbiased	temporal 2				

$\beta \xleftarrow{\mathsf{U}} \{0,1\}$ 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 6). The advantage of Problem 1 is proven to be equivalent to that of the DLIN assumption (Lemma 2).

We then show that Game 2-$(h-1)$-4 can be conceptually changed to Game 2-h-1 (Lemma 7), by using the fact that parts of bases, $(\boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{2n})$ and $(\boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{2n})$, are unknown to the adversary. In particular, when $h = 1$, it means that Game 1 can be conceptually changed to Game 2-1-1. When $h \geq 2$, we notice that temporal 2 key and temporal 1 challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{temp2}}, \boldsymbol{c}_1^{\mathsf{temp1}})$, are equivalent to temporal 2 key and temporal 2 challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{temp2}}, \boldsymbol{c}_1^{\mathsf{temp2}})$, except that $\vec{x}^{(b)}$ is used in $\boldsymbol{c}_1^{\mathsf{temp1}}$ instead of $\omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)}$ (with $\omega'_0, \omega'_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$) for some coefficient vector in $\boldsymbol{c}_1^{\mathsf{temp2}}$. This change of coefficient vectors can be done conceptually since zero vector 0^n is used for the corresponding part in $\boldsymbol{k}^{*\,\mathsf{temp2}}$.

The advantage gap between Games 2-h-1 and 2-h-2 is shown to be bounded by the advantage of Problem 2, i.e., advantage of the DLIN assumption (Lemmas 8 and 3).

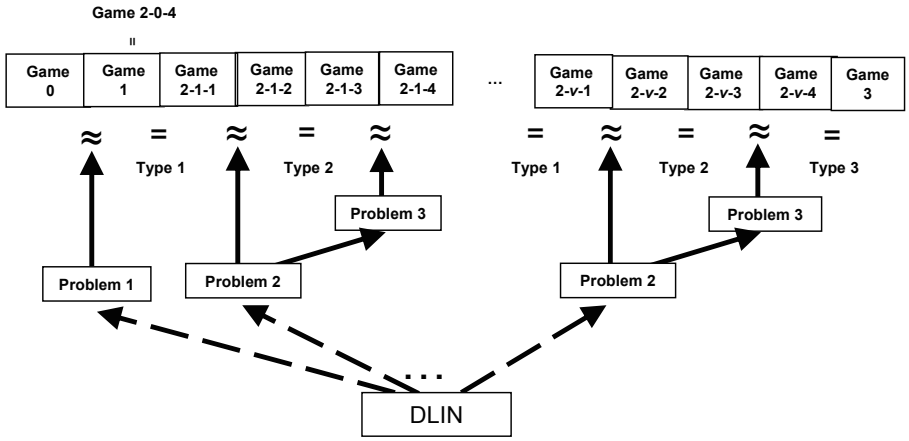

Fig. 1. Structure of Reductions

We then show that Game 2-h-2 can be conceptually changed to Game 2-h-3 (Lemma 9), again by using the fact that parts of bases, $(\boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{2n})$ and $(\boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{2n})$, are unknown to the adversary. In this conceptual change, we use the fact that all key queries $\vec{v}$ satisfy $\vec{v} \cdot \vec{x}^{(0)} = \vec{v} \cdot \vec{x}^{(1)} = 0$ or $\vec{v} \cdot \vec{x}^{(0)} \neq 0$ and $\vec{v} \cdot \vec{x}^{(1)} \neq 0$. Here, we notice that temporal 1 key and temporal 1 challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{temp1}}, \boldsymbol{c}_1^{\mathsf{temp1}})$, are equivalent to temporal 1 key and temporal 2 challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{temp1}}, \boldsymbol{c}_1^{\mathsf{temp2}})$, except that random linear combination $\omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)}$ (with $\omega'_0, \omega'_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$) is used in $\boldsymbol{c}_1^{\mathsf{temp2}}$ instead of $\vec{x}^{(b)}$ for some coefficient vector in $\boldsymbol{c}_1^{\mathsf{temp1}}$. This conceptual change is proved by using Lemma 5.

The advantage gap between Games 2-h-3 and 2-h-4 is similarly shown to be bounded by the advantage of Problem 3, i.e., advantage of the DLIN assumption (Lemmas 10 and 4).

We then show that Game 2-ν-4 can be conceptually changed to Game 3 (Lemma 11) by using the fact that parts of bases, $(\boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{3n})$ and $(\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_{2n})$, are unknown to the adversary.

Figure 1 shows the structure of the security reduction, where the security of the scheme is hierarchically reduced to the intractability of the DLIN problem. The reduction steps indicated by dotted arrows can be shown in the same manner as that in (the full version of) [19].

Proof of Lemma 1 To prove Lemma 1, we consider the following $4\nu+3$ games when $t = 1$. 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' : Same as Game 0 except that flip a coin $t \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted in step 3 if $t \neq s$. In order to prove Lemma 1, we

consider the case with $t = 1$. The reply to a key query for $\vec{v}$ is:

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

where $\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$. The challenge ciphertext for challenge plaintext $m := m^{(0)} = m^{(1)}$ and vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \boxed{\omega\vec{x}^{(b)}},\ \boxed{0^n},\ \boxed{0^n},\ 0^n,\ \varphi\ )_{\mathbb{B}},\quad c_2 := g_T^{\zeta} m, \tag{3}$$

where $b \xleftarrow{\mathsf{U}} \{0,1\}$ and $\zeta, \omega, \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q$. Here, we note that c_2 is independent from bit b.

Game 1 : Game 1 is the same as Game 0' except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintext $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega\vec{x}^{(b)},\ \boxed{zx_1^{(b)}, 0^{n-1}},\ 0^n,\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{4}$$

where $x_1^{(b)} \neq 0$ is the first coordinate of $\vec{x}^{(b)}$, $z \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 0'.

Game 2-h-1 ($h = 1, \ldots, \nu$) : Game 2-0-4 is Game 1. Game 2-h-1 is the same as Game 2-$(h-1)$-4 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintext $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega\vec{x}^{(b)},\ \boxed{\omega'\vec{x}^{(b)}},\ \boxed{\omega_0''\vec{x}^{(0)} + \omega_1''\vec{x}^{(1)}},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{5}$$

where $\omega', \omega_0'', \omega_1'' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-$(h-1)$-4.

Game 2-h-2 ($h = 1, \ldots, \nu$) : Game 2-h-2 is the same as Game 2-h-1 except that the reply to the h-th key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \sigma\vec{v},\ \boxed{\sigma'\vec{v}},\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \tag{6}$$

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

Game 2-h-3 ($h = 1, \ldots, \nu$) : Game 2-h-3 is the same as Game 2-h-2 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintexts $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega\vec{x}^{(b)},\ \boxed{\omega_0'\vec{x}^{(0)} + \omega_1'\vec{x}^{(1)}},\ \omega_0''\vec{x}^{(0)} + \omega_1''\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{7}$$

where $\omega_0', \omega_1' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-h-2.

Game 2-h-4 ($h = 1, \ldots, \nu$) : Game 2-h-4 is the same as Game 2-h-3 except that the reply to the h-th key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \sigma\vec{v},\ \boxed{0^n},\ \boxed{\sigma''\vec{v}},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \tag{8}$$

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

Game 3 : Game 3 is the same as Game 2-ν-4 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintexts $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\zeta, \boxed{\omega_0 \vec{x}^{(0)} + \omega_1 \vec{x}^{(1)}}, \omega'_0 \vec{x}^{(0)} + \omega'_1 \vec{x}^{(1)}, \omega''_0 \vec{x}^{(0)} + \omega''_1 \vec{x}^{(1)}, 0^n, \varphi)_{\mathbb{B}}, \quad (9)$$

where $\omega_0, \omega_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-ν-4. Here, we note that $\boldsymbol{c}_1$ is independent from bit $b \xleftarrow{\mathsf{U}} \{0,1\}$.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda), \ldots, \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}4)}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0', 1, 2\text{-}h\text{-}1, \ldots, 2\text{-}h\text{-}4$ and 3 when $t = 1$, respectively. $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda)$ is equivalent to the left-hand side of Eq. (1). We will show six lemmas (Lemmas 6–11) that evaluate the gaps between pairs of neighboring games. From these lemmas and Lemmas 2–4, we obtain $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) \leq \left|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| + \sum_{h=1}^{\nu}\sum_{\iota=1}^{4}\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}(\iota-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}\iota)}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)\right| + \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1}}(\lambda) + \sum_{h=1}^{\nu}\left(\mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}1}}^{\mathsf{P2}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}2}}^{\mathsf{P3}}(\lambda)\right) + (2\nu+1)/q \leq \mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{h=1}^{\nu}\left(\mathsf{Adv}_{\mathcal{E}_{2\text{-}h\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{2\text{-}h\text{-}2}}^{\mathsf{DLIN}}(\lambda)\right) + (12\nu+12)/q.$ □

The definitions of Problems 1–3 and the advantages ($\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P1}}(\lambda)$, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2}}(\lambda)$, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P3}}(\lambda)$), and the proofs of Lemmas 2–12 are given in the full version [21].

Lemma 2 (resp. 3, 4). *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, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P1}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 6/q$, (resp. $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P3}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$).*

Lemma 5 is the same as Lemma 3 in [19].

Lemma 6. *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, $|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1}}(\lambda)$.*

Lemma 7. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \leq 2/q$.*

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

Lemma 9. *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda)$.*

Lemma 10. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}4)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}2}}^{\mathsf{P3}}(\lambda)$, where $\mathcal{B}_{2\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{2\text{-}2}(h, \cdot)$.*

Lemma 11. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \leq 1/q$.*

Lemma 12. *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$.*

5 A Variant for Achieving Shorter Public and Secret Keys

A variant of the proposed (basic) IPE scheme with the same security, that achieves a shorter ($O(n)$-size) master public key and shorter ($O(1)$-size) secret keys (excluding the description of $\vec{v}$), can be constructed by combining with the techniques in [20], where n is the dimension of vectors of the IPE scheme. This variant also enjoys more efficient decryption. Here, we show this variant. See the key idea, performance and the security proof of this scheme in the full versions of this paper [21] and [20]. Let $N := 5n + 1$ and

$$\mathcal{H}(n, \mathbb{F}_q) := \left\{ \begin{pmatrix} \mu & & \mu'_1 \\ & \ddots & \vdots \\ & \mu & \mu'_{n-1} \\ & & \mu'_n \end{pmatrix} \middle| \begin{array}{l} \mu, \mu'_l \in \mathbb{F}_q \text{ for } l = 1, \ldots, n, \\ \text{a blank element in the matrix} \\ \text{denotes } 0 \in \mathbb{F}_q \end{array} \right\}, \quad (10)$$

$$\mathcal{L}^+(5, n, \mathbb{F}_q) := \left\{ X := \begin{pmatrix} \chi_{0,0} & \chi_{0,1}\vec{e}_n & \cdots & \chi_{0,5}\vec{e}_n \\ \vec{\chi}^{\mathrm{T}}_{1,0} & X_{1,1} & \cdots & X_{1,5} \\ \vdots & \vdots & & \vdots \\ \vec{\chi}^{\mathrm{T}}_{5,0} & X_{5,1} & \cdots & X_{5,5} \end{pmatrix} \middle| \begin{array}{l} X_{i,j} \in \mathcal{H}(n, \mathbb{F}_q), \\ \vec{\chi}_{i,0} := (\chi_{i,0,l})_{l=1,\ldots,n} \in \mathbb{F}_q^n, \\ \chi_{0,0}, \chi_{0,j} \in \mathbb{F}_q \\ \text{for } i, j = 1, \ldots, 5 \end{array} \right\} \bigcap GL(N, \mathbb{F}_q). \quad (11)$$

We note that $\mathcal{L}^+(5, n, \mathbb{F}_q)$ is a subgroup of $GL(N, \mathbb{F}_q)$. Random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{ZIPE,SK}}$ below is used as a subroutine in the proposed IPE.

$\mathcal{G}_{\mathsf{ob}}^{\mathsf{ZIPE,SK}}(1^\lambda, 5, n)$: $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda)$, $N := 5n + 1$,
$\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times$, $g_T := e(G, G)^\psi$, $\mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N, \mathsf{param}_{\mathbb{G}})$,
$\mathsf{param}_n := (\mathsf{param}_{\mathbb{V}}, g_T)$, $X \xleftarrow{\mathsf{U}} \mathcal{L}^+(5, n, \mathbb{F}_q)$, $(\vartheta_{i,j})_{i,j=0,\ldots,5n} := \psi \cdot (X^{\mathrm{T}})^{-1}$,
hereafter, $\{\chi_{0,0}, \chi_{0,j}, \chi_{i,0,l}, \mu_{i,j}, \mu'_{i,j,l}\}_{i,j=1,\ldots 5; l=1,\ldots,n}$ denotes non-zero entries of X, where $\{\mu_{i,j}, \mu'_{i,j,l}\}$ are non-zero entries of submatrices $X_{i,j}$ of X as given in Eqs. (11) and (10),
$\boldsymbol{b}_i := (\vartheta_{i,0}, \ldots, \vartheta_{i,5n})_{\mathbb{A}} = \sum_{j=0}^{5n} \vartheta_{i,j} \boldsymbol{a}_j$ for $i = 0, \ldots, 5n$, $\mathbb{B} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{5n})$,
$B^*_{0,0} := \chi_{0,0} G, B^*_{0,j} := \chi_{0,j} G, B^*_{i,0,l} := \chi_{i,0,l} G, B^*_{i,j} := \mu_{i,j} G, B'^*_{i,j,l} := \mu'_{i,j,l} G$
for $i, j = 1, \ldots, 5; l = 1, \ldots, n$,
return $(\mathsf{param}_n, \mathbb{B}, \{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,l}, B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,5; l=1,\ldots,n})$.

Remark 1 Let $\boldsymbol{b}^*_0 := (\ B^*_{0,0},\ 0^{n-1}, B^*_{0,1}, \ldots, 0^{n-1}, B^*_{0,5}\ )$,

$$\begin{pmatrix} \boldsymbol{b}^*_{(i-1)n+1} \\ \vdots \\ \boldsymbol{b}^*_{in} \end{pmatrix} := \begin{pmatrix} B^*_{i,0,1} & B^*_{i,1} & & B'^*_{i,1,1} & B^*_{i,5} & & B'^*_{i,5,1} \\ \vdots & & \ddots & \vdots & & \ddots & \vdots \\ B^*_{i,0,n-1} & & B^*_{i,1} & B'^*_{i,1,n-1} & & B^*_{i,5} & B'^*_{i,5,n-1} \\ B^*_{i,0,n} & & & B'^*_{i,1,n} & & & B'^*_{i,5,n} \end{pmatrix}$$

for $i = 1, \ldots, 5$, and $\mathbb{B}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_{5n}^*)$, where a blank element in the matrix denotes $0 \in \mathbb{G}$. $\mathbb{B}^*$ is the dual orthonormal basis of $\mathbb{B}$, i.e., $e(\boldsymbol{b}_i, \boldsymbol{b}_i^*) = g_T$ and $e(\boldsymbol{b}_i, \boldsymbol{b}_j^*) = 1$ for $0 \le i \ne j \le 5n$.

Here, we assume that input vector, $\vec{v} := (v_1, \ldots, v_n)$, has an index l ($1 \le l \le n-1$) with $v_l \ne 0$, and that input vector, $\vec{x} := (x_1, \ldots, x_n)$, satisfies $x_n \ne 0$.

$\mathsf{Setup}(1^\lambda,\ n)$:

$(\mathsf{param}_n, \mathbb{B},\ \{B_{0,0}^*, B_{0,j}^*, B_{i,0,l}^*, B_{i,j}^*, B_{i,j,l}'^*\}_{i,j=1,\ldots,5;l=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{ZIPE,SK}}(1^\lambda, 5, n)$,

$\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1}, \ldots, \boldsymbol{b}_{5n})$,

return $\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \widehat{\mathbb{B}}), \mathsf{sk} := \{B_{0,0}^*, B_{0,j}^*, B_{i,0,l}^*, B_{i,j}^*, B_{i,j,l}'^*\}_{i=1,4;j=1,..,5;l=1,..,n}$.

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v})$: $\sigma, \eta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $K_0^* := B_{0,0}^* + \sum_{l=1}^n v_l(\sigma B_{1,0,l}^* + \eta B_{4,0,l}^*)$,

$K_{1,j}^* := \sigma B_{1,j}^* + \eta B_{4,j}^*$, $K_{2,j}^* := B_{0,j}^* + \sum_{l=1}^n v_l(\sigma B_{1,j,l}'^* + \eta B_{4,j,l}'^*)$ for $j = 1, .., 5$,

return $\mathsf{sk}_{\vec{v}} := (\vec{v}, K_0^*, \{K_{1,j}^*, K_{2,j}^*\}_{j=1,\ldots,5})$.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \vec{x})$: $\omega, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\varphi} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $\boldsymbol{c}_1 := (\ \zeta,\ \overbrace{\omega\vec{x}}^{n},\ \overbrace{0^{2n}}^{2n},\ \overbrace{0^n}^{n},\ \overbrace{\vec{\varphi}}^{n}\ )_{\mathbb{B}}$,

$c_2 := g_T^\zeta m$, return $\mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := (\vec{v}, K_0^*, \{K_{1,j}^*, K_{2,j}^*\}_{j=1,\ldots,5}),\ \mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2))$:

Parse $\boldsymbol{c}_1$ as a $(5n+1)$-tuple $(C_0, \ldots, C_{5n}) \in \mathbb{G}^{5n+1}$,

$D_j := \sum_{l=1}^{n-1} v_l C_{(j-1)n+l}$ for $j = 1, \ldots, 5$,

$F := e(C_0, K_0^*) \cdot \prod_{j=1}^5 \left(e(D_j, K_{1,j}^*) \cdot e(C_{jn}, K_{2,j}^*)\right)$, return $m' := c_2/F$.

Remark 2 A part of output of $\mathsf{Setup}(1^\lambda, n)$, $\{B_{0,0}^*, B_{0,j}^*, B_{i,0,l}^*, B_{i,j}^*, B_{i,j,l}'^*\}_{i=1,4;j=1,\ldots,5;l=1,\ldots,n}$, can be identified with $\widehat{\mathbb{B}}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_n^*, \boldsymbol{b}_{3n+1}^*, \ldots, \boldsymbol{b}_{4n}^*)$, while $\mathbb{B}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_{5n}^*)$ is identified with $\{B_{0,0}^*, B_{0,j}^*, B_{i,0,l}^*, B_{i,j}^*, B_{i,j,l}'^*\}_{i=1,\ldots,5;j=1,\ldots,5;l=1,\ldots,n}$ in Remark 1. Decryption Dec can be alternatively described as:

$\mathsf{Dec}'(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := (\vec{v}, K_0^*, \{K_{1,j}^*, K_{2,j}^*\}_{j=1,\ldots,5}),\ \mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2))$:

$\boldsymbol{k}^* := (\overbrace{K_0^*, v_1K_{1,1}^*, .., v_{n-1}K_{1,1}^*, K_{2,1}^*,}^{n}\ \ldots,\ \overbrace{v_1K_{1,5}^*, .., v_{n-1}K_{1,5}^*, K_{2,5}^*}^{n})$,

that is, $\boldsymbol{k}^* = (1,\ \overbrace{\sigma\vec{v},}^{n}\ \overbrace{0^{2n},}^{2n}\ \overbrace{\eta\vec{v}}^{n}\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*}$, $F := e(\boldsymbol{c}_1, \boldsymbol{k}^*)$,

return $m' := c_2/F$.

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

6 Comparison

Table 2 compares the proposed IPE schemes in Sections 4 and 5 with existing attribute-hiding IPE schemes in [15, 18, 16, 19].

Table 2. Comparison with IPE schemes in [15, 18, 16, 19], where $|\mathbb{G}|$ and $|\mathbb{G}_T|$ represent size of an element of $\mathbb{G}$ and that of $\mathbb{G}_T$, respectively. AH, PK, SK, CT, GSD, DSP and eDDH stand for attribute-hiding, master public key, secret key, ciphertext, general subgroup decision [1], decisional subspace problem [18], and extended decisional Diffie-Hellman [16], respectively.

	KSW08 [15]	OT09 [18]	LOS$^+$10 [16]	OT10 [19]	Proposed (basic)	Proposed (variant)
Security	selective & fully-AH	selective & weakly-AH	adaptive & weakly-AH	adaptive & weakly-AH	adaptive & fully-AH	adaptive & fully-AH
Order of $\mathbb{G}$	composite	prime	prime	prime	prime	prime
Assump.	2 variants of GSD	2 variants of DSP	n-eDDH	DLIN	DLIN	DLIN
PK size	$O(n)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n)\|\mathbb{G}\|$
SK size	$(2n+1)\|\mathbb{G}\|$	$(n+3)\|\mathbb{G}\|$	$(2n+3)\|\mathbb{G}\|$	$(3n+2)\|\mathbb{G}\|$	$(4n+2)\|\mathbb{G}\|$	$11\|\mathbb{G}\|$
CT size	$(2n+1)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(n+3)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(2n+3)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(3n+2)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(4n+2)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(5n+1)\|\mathbb{G}\| + \|\mathbb{G}_T\|$

References

1. Bellare, M., Waters, B., Yilek, S.: Identity-based encryption secure against selective opening attack. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 235–252. Springer (2011)
2. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy. pp. 321–334. IEEE Computer Society (2007)
3. Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin and Camenisch [9], pp. 223–238
4. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin [12], pp. 443–459
5. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin [12], pp. 41–55
6. Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin and Camenisch [9], pp. 506–522
7. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer (2001)
8. 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 (2007)
9. Cachin, C., Camenisch, J. (eds.): Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, LNCS, vol. 3027. Springer (2004)
10. Caro, A.D., Iovino, V., Persiano, G.: Hidden vector encryption fully secure against unrestricted queries. IACR Cryptology ePrint Archive 2011, 546 (2011)
11. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) IMA Int. Conf. 2001. LNCS, vol. 2260, pp. 360–363. Springer (2001)

12. Franklin, M.K. (ed.): Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings, LNCS, vol. 3152. Springer (2004)
13. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Juels et al. [14], pp. 89–98
14. Juels, A., Wright, R.N., di Vimercati, S.D.C. (eds.): Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, October 30 - November 3, 2006. ACM (2006)
15. 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 (2008)
16. Lewko, A.B., 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 2008. LNCS, vol. 6110, pp. 62–91. Springer (2010), full version is available at `http://eprint.iacr.org/2010/110`
17. 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 (2008)
18. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer (2009)
19. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer (2010), full version is available at `http://eprint.iacr.org/2010/563`
20. Okamoto, T., Takashima, K.: Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 138–159. Springer (2011), full version is available at `http://eprint.iacr.org/2011/648`
21. Okamoto, T., Takashima, K.: Adaptively attribute-hiding (hierarchical) inner product encryption. IACR Cryptology ePrint Archive 2011, 543 (2011), the full version of this paper, `http://eprint.iacr.org/2011/543`
22. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: Ning, P., di Vimercati, S.D.C., Syverson, P.F. (eds.) ACM Conference on Computer and Communications Security. pp. 195–203. ACM (2007)
23. Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. In: Juels et al. [14], pp. 99–112
24. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer (2005)
25. 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 (2009)