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

1 Introduction

1.1 Background

IPE and ABE The notions of *inner-product encryption* (IPE) and *attribute-based encryption* (ABE) introduced by Katz, Sahai and Waters [6] and Sahai and Waters [18] constitute an advanced class of encryption, *functional encryption* (FE), and provide more flexible and fine-grained functionalities in sharing and distributing sensitive data than traditional symmetric and public-key encryption as well as identity-based encryption (IBE).

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

a set of attributes, and the other is an access policy (structure) or (monotone) span program over a universe of attributes, e.g., a secret key for a user is associated with an access policy and a ciphertext is associated with a set of attributes, where a secret key can decrypt a ciphertext, iff the attribute set satisfies the policy. If the access policy is for a secret key, it is called key-policy ABE (KP-ABE), and if the access policy is for encryption, it is ciphertext-policy ABE (CP-ABE).

For some applications, the parameters for encryption are required to be hidden from ciphertexts. To capture the security requirement, Katz, Sahai and Waters [6] introduced *attribute-hiding* (based on the same notion for hidden vector encryption (HVE) by Boneh and Waters [4]), a security notion for FE that is stronger than the basic security requirement, *payload-hiding*. Roughly speaking, attribute-hiding requires that a ciphertext conceal the associated parameter as well as the plaintext, while payload-hiding only requires that a ciphertext conceal the plaintext. A weaker notion of attribute-hiding than the original one [6] was given by [7]. The weaker notion is called *weakly attribute-hiding*, and the original one is *fully attribute-hiding*. Informally, in the fully attribute-hiding, the secrecy of attribute x is ensured even against an adversary having a secret key with v such that $R(v, x)$ holds (i.e., no information is released on x except $R(v, x)$ holds), while it is ensured only when $R(v, x)$ does not hold in the weakly attribute-hiding (see Definition 4 for the definition of the fully attribute-hiding).

To the best of our knowledge, the widest class of attribute-hiding FE is IPE [6, 7, 12, 14] (KSW08, LOS$^+$10, OT10 and OT12 schemes). Inner-products for IPE represent a fairly wide class of relations including equality tests as the simplest case (i.e., anonymous IBE and HVE are very special classes of attribute-hiding IPE), disjunctions or conjunctions of equality tests, and, more generally, CNF or DNF formulas. We note, however, that inner-product relations are less expressive than a class of relations (on span programs) for ABE, while existing ABE schemes for such a wider class of relations are not attribute-hiding but only payload-hiding.

Among the existing IPE schemes, only the OT12 IPE scheme [14] achieves the *full (adaptive)* security and *fully attribute-hiding* simultaneously, whereas other attribute-hiding IPE schemes [6, 11, 7, 12] are selectively secure or weakly attribute-hiding, and some IPE schemes [1, 13] only achieve payload-hiding. As for ABE, Lewko et.al. and Okamoto-Takashima ABE schemes [7, 12] are fully secure in the standard model, while ABE schemes [18, 5, 16, 20] before [7, 12] were *selectively* secure.

Unbounded IPE and ABE All previous constructions of IPE and ABE except the Lewko-Waters ABE scheme [9] have restriction, or are *bounded*, in the choice of the parameters for secret key and encryption once the public parameters have been set. The only *unbounded* ABE scheme [9], however, is *selectively* secure, while they presented an *unbounded* hierarchical identity-based encryption (HIBE) that is *fully secure* in the standard model. No *unbounded* IPE scheme has been presented. Therefore, no *fully secure* and *unbounded* scheme for an advanced class of encryption like IPE or ABE has been presented.

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

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

The only known technique to prove the full security of an (attribute-hiding) IPE or ABE system is the dual system encryption by Waters [19] and its extension [14]. In the techniques, information theoretical arguments (e.g., conceptual change due to the same distribution and the independent randomness of two distributions etc.) over some (hidden) parts of a secret-key and challenge ciphertext play a key role in the security proof, provided that the adversary follows the secret-key-query condition in the security games. To execute a security proof based on the information theoretical arguments, an appropriate distribution of randomness consistent with the key-query condition should be supplied in the proof games transformed from the original proof game.

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

In contrast, for *unbounded* IPE and ABE schemes, some (unbounded amount of) randomness whose distribution is consistent with the key-query condition should be supplied in addition to the randomness provided by the public parameters. For example, even when the dimension of vectors for IPE is required to be n, the size of the public parameters is $O(1)$ in *unbounded* IPE, i.e., the size of secret randomness to generate the public parameters is $O(1)$. Clearly, such a size of randomness is not sufficient for the information theoretical arguments over n-dimensional vectors. Therefore, any additional source of randomness should be provided, and the distribution of the randomness should be specific (i.e., consistent with the key-query condition). For the unbounded HIBE scheme [9], where the equality (un-)matching is the key-query condition, a simple compression technique works well to create such randomness since equality can be simply compressed with preserving the property. The key-query condition for IPE and ABE, however, is in general much more complicated than just the equality matching for (H)IBE, and no technique was known to create randomness consistent with such a complicated condition in some security proofs. This is a reason why [9] succeeds in realizing a fully secure unbounded HIBE but not for ABE (and not for IPE).

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

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

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

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

1.2 Our Results

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

Table 1. Comparison of *attribute-hiding IPE schemes*, where $|\mathbb{G}|$ and $|\mathbb{G}_T|$ represent size of an element of $\mathbb{G}$ and that of $\mathbb{G}_T$, respectively. AH, IP, PK, SK, CT, GSD and eDDH stand for attribute-hiding, inner-product, master public key (public parameters), secret key, ciphertext, general subgroup decision [3] and extended decisional Diffie-Hellman [7], respectively.

	KSW08 [6]	LOS+10 [7]	OT10 [12]	OT12 [14]		Proposed IPE	
				(basic)	(variant)	(type 1 or 2) Section 4.1	(type 0) Section 4.2
Bounded or Unbounded	bounded	bounded	bounded	bounded	bounded	unbounded	unbounded
Restriction on IP relation	restricted*	restricted	restricted	restricted	restricted	relaxed	restricted
Security	selective & fully-AH	adaptive & weakly-AH	adaptive & weakly-AH	adaptive & fully-AH	adaptive & fully-AH	adaptive & fully-AH	adaptive & fully-AH
Order of $\mathbb{G}$	composite	prime	prime	prime	prime	prime	prime
Assump.	2 variants of GSD	n-eDDH	DLIN	DLIN	DLIN	DLIN	DLIN
PK size	$O(n)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n)\|\mathbb{G}\|$	$O(1)\|\mathbb{G}\|$	$O(1)\|\mathbb{G}\|$
SK size	$(2n+1)\|\mathbb{G}\|$	$(2n+3)\|\mathbb{G}\|$	$(3n+2)\|\mathbb{G}\|$	$(4n+2)\|\mathbb{G}\|$	$11\|\mathbb{G}\|$	$(15n+5)\|\mathbb{G}\|$	$(21n+9)\|\mathbb{G}\|$
CT size	$(2n+1)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(2n+3)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(3n+2)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(4n+2)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(5n+1)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(15n'+5)\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$(21n'+9)\|\mathbb{G}\| + \|\mathbb{G}_T\|$

* It can be easily relaxed.

Remark: We now roughly explain the three types of inner-product relations. To relax the above-mentioned restriction on the inner-product relation, we introduce a new type of inner-product (generalized inner-product) for $\vec{v}$ and $\vec{x}$, where their dimensions can be different (say n and n' for the dimensions of $\vec{v}$ and $\vec{x}$). In this notion, vector $\vec{v}$ and $\vec{x}$ are expressed by $\{(t, v_t) \mid t \in I_{\vec{v}},\ \sharp I_{\vec{v}} = n\}$ and $\{(t, x_t) \mid t \in I_{\vec{x}},\ \sharp I_{\vec{x}} = n'\}$, respectively, where $t \in \mathbb{N}$ is an index for vectors, whose semantics is given by each application. Here note that we abuse the same vector notation, $\vec{v}$, for the new expression as well as for the conventional one, $(v_1, \ldots, v_n)$. In the above-mentioned example, $\vec{x} := \{(1,1), (2, x_1), \ldots, (101, x_{100}), (102, x_1^2), (103, x_1x_2), \ldots, (n', x_{100}^3)\}$ where $I_{\vec{x}} := \{1, 2, \ldots, n'\}$, and $\vec{v} := \{(1, r_1ab - r_2c), (6, -r_1b), (17, -r_1a), (58, r_2), (517, r_1)\}$ where $I_{\vec{v}} := \{1, 6, 17, 58, 517\}$. The generalized inner-product of $\vec{v}$ over $\vec{x}$ is defined by $\sum_{t \in I_{\vec{v}}} v_t x_t$ if $I_{\vec{v}} \subseteq I_{\vec{x}}$. Otherwise, it is undefined. By using the generalized inner-product notion, the secret key size can be in proportion to the effective dimension (e.g., 5 instead of around 10^6).

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

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

	LW11 [9]	LOS$^+$10 [7]		OT10 [12]		Proposed KP-ABE	
		(basic)	(modified)	(basic)	(modified)	(basic) Section 5	(modified) in full ver.
Bounded or Unbounded	unbounded	bounded	bounded	bounded	bounded	unbounded	unbounded
Security	selective	full	full	full	full	full	full
Order of $\mathbb{G}$	composite	composite	composite	prime	prime	prime	prime
Assump.	GSD	GSD	GSD	DLIN	DLIN	DLIN	DLIN
Degree of access policies	arbitrary	1	arbitrary	1	arbitrary	1	arbitrary
PK size	$O(1)\|\mathbb{G}\|$	$O(n_{\mathsf{max}})\|\mathbb{G}\|$	$O(n_{\mathsf{max}})\|\mathbb{G}\|$	$O(d)\|\mathbb{G}\|$	$O(d)\|\mathbb{G}\|$	$O(1)\|\mathbb{G}\|$	$O(1)\|\mathbb{G}\|$
SK size	$O(\ell)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$	$O(\ell)\|\mathbb{G}\|$
CT size	$O(n)\|\mathbb{G}\|$	$O(n)\|\mathbb{G}\|$	$O(k_{\mathsf{max}}n)\|\mathbb{G}\|$	$O(n)\|\mathbb{G}\|$	$O(k_{\mathsf{max}}n)\|\mathbb{G}\|$	$O(n)\|\mathbb{G}\|$	$O(k_{\mathsf{max}}n)\|\mathbb{G}\|$

(in other words, the inner-product for Type 0 is defined iff these dimensions are equivalent.)

2. We present the first *unbounded* inner-product encryption (IPE) schemes. The proposed unbounded IPE schemes are *fully (adaptively) secure and fully attribute-hiding* in the standard model under a standard assumption, the decisional linear (DLIN) assumption. The proposed unbounded IPE schemes consist of the above-mentioned types of generalized IPE, Types 0, 1 and 2, For comparison of attribute-hiding IPE schemes, see Table 1.
3. We present the first *unbounded* KP- and CP-ABE schemes that are *fully secure* (adaptively payload-hiding) in the standard model. The proposed unbounded ABE schemes are fully secure under the DLIN assumption, and are for a wide class of relations, non-monotone access structures (see the full version for the proposed CP-ABE scheme). See Table 2 for comparison of KP-ABE schemes.

   Remark: Similarly to the existing fully secure ABE schemes in the standard model [7, 12, 8] except [10], our basic ABE scheme (Section 5) has a restriction that the degree of access policies is 1 [3]. A modified KP-ABE scheme is shown in the full version of this paper to relax the restriction or to achieve an arbitrary degree k of access policies with preserving the fully

[3] Informally, the degree may imply the number of appearance of a variable in a formula, e.g., formula $((x = a) \vee (x = b)) \wedge (y = c)$ has degree 2 for variable x. For the definition of the degree of access policies in our schemes, see the full version. The degree should be a bit differently defined in [18, 5, 16, 20, 7, 8], where degree 1 is called *one-use*.

secure and unbounded property. It, however, shares a shortcoming of the existing fully secure (modified) ABE schemes [7, 12, 8] that the ciphertext size grows linearly with k. Here, a (maximum) value of k can be determined in each application of our ABE scheme, while the public parameters are fixed and commonly shared by all applications and users.

1.3 Key Techniques

As mentioned above, the difficulty of realizing a fully secure unbounded IPE or ABE scheme arises from the hardness of supplying an *unbounded amount of* randomness *consistent* with the complicated key-query condition for the (dual system encryption) security arguments on IPE or ABE. To overcome this difficulty, we develop novel techniques, *indexing* and *consistent randomness amplification*, on the dual system encryption and the dual pairing vector spaces (DPVS). Roughly speaking, the *indexing* technique is for supplying a source of unbounded amount of randomness and the *consistent randomness amplification* technique is for amplifying the randomness of the source through a computational assumption (e.g., the DLIN assumption in our case) and the randomness of hidden bases as well as for adjusting the distribution of the amplified randomness to be consistent with a condition. This methodology could provide a general framework for proving the security in unbounded situations.

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

In a typical construction of *bounded* IPE schemes [7, 12, 14] which are based on DPVS, once a basis of DPVS, a part of the basis of a N-dimensional space is published as public parameters, the dimension n of predicate and attribute vectors for secret key and encryption is bounded or fixed, e.g., $n \leq N/4$ (i.e., $N = O(n)$). The full security is proven through the information theoretical arguments, and the randomness of secret matrix X (e.g., the amount of the randomness is $O(n^2)$) supplies enough randomness for the arguments.

In contrast, the dimension, n, of the predicate and attribute vectors is not bounded by the public parameters in *unbounded* IPE. For example, in one of the proposed IPE schemes (Section 4), the public parameters consist of a constant number of elements, 9 elements of bases (or 105 pairing group elements), $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$ and $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15})$, where random matrices of constant sizes, $X_0 \xleftarrow{\cup} \mathbb{F}_q^{5\times 5}$ and $X_1 \xleftarrow{\cup} \mathbb{F}_q^{15\times 15}$, are employed to generate the public parameters. The randomness of the public parameters, just a constant amount with respect to n, is clearly insufficient for the (dual system encryption) arguments on the proof of full security.

To supply additional randomness for the purpose, in our IPE schemes, we introduce a technique called *indexing*, where two-dimensional index vectors,

$\sigma_t(1,t)$ and $\mu_t(t,-1)$ are embedded into ciphertext $\boldsymbol{c}_t$ and secret key $\boldsymbol{k}^*_t$, respectively, where σ_t and μ_t are freshly random for each t. In our IPE scheme (Section 4) where $n = n'$ for simplicity, for example, secret key $(\boldsymbol{k}^*_1, \ldots, \boldsymbol{k}^*_n)$ for $\vec{v} := (v_1, \ldots, v_n)$ can be expressed by a coefficient vector, $(\mu_t(t,-1), \delta v_t, \ldots)$, for $t = 1, \ldots, n$, over basis $\mathbb{B}^*$, i.e., $\boldsymbol{k}^*_t := (\mu_t(t,-1), \delta v_t, \ldots)_{\mathbb{B}^*}$ and ciphertext $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n)$ for $\vec{x} := (x_1, \ldots, x_n)$ can be expressed by $\boldsymbol{c}_t := (\sigma_t(1,t), \omega x_t, \ldots)_{\mathbb{B}}$ for $t = 1, \ldots, n$, where δ, ω are randomly selected. While the size of the public parameters or its randomness is constant in n, an unbounded amount of randomness, $\{\mu_t\}_{t=1,\ldots,n}, \{\sigma_t\}_{t=1,\ldots,n}$, can be supplied to secret key and ciphertext. This is a key idea of the *indexing* technique.

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

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

The consistent randomness amplification technique is composed of several computational and conceptual (information theoretical) transformations. One of the key tricks of the transformations is to amplify a source of randomness to

a hidden part by applying a computational assumption, the DLIN assumption. Another computational trick is to swap two vectors in different positions under DLIN. Information theoretical key tricks are inter-subspace and intra-subspace types of conceptual transformations (see the full version for more details).

The security proofs of our IPE and ABE schemes are hierarchically constructed in a modular manner. The very top level of the security proof is based on the dual system encryption and its extension. Several problems in the middle level support the top level arguments. Our key techniques, the indexing and consistent randomness amplification techniques, which are also constructed in a hierarchical manner, are employed in the lowest level to reduce the hardness of the middle level problems to the DLIN assumption.

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. We denote the finite field of order q by $\mathbb{F}_q$, $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^\times$, and the set of positive integers by $\mathbb{N}$. 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. A bold face letter denotes an element of vector space $\mathbb{V}$, e.g., $\boldsymbol{x} \in \mathbb{V}$. When $\boldsymbol{b}_i \in \mathbb{V}$ $(i = 1, \ldots, n)$, $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle \subseteq \mathbb{V}$ (resp. $\mathsf{span}\langle \vec{x}_1, \ldots, \vec{x}_n \rangle$) denotes the subspace generated by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ (resp. $\vec{x}_1, \ldots, \vec{x}_n$). For bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$, $(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^N x_i \boldsymbol{b}_i$ and $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^N y_i \boldsymbol{b}_i^*$. $\vec{e}_1$ and $\vec{e}_2$ denote the canonical basis vectors in $\mathbb{F}_q^2$, i.e., $\vec{e}_1 := (1, 0)$ and $\vec{e}_2 := (0, 1)$. $GL(n, \mathbb{F}_q)$ denotes the general linear group of degree n over $\mathbb{F}_q$.

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

Definition 1. *"Symmetric bilinear pairing groups"* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *are a tuple of a prime* q*, cyclic additive group* $\mathbb{G}$ *and multiplicative group* $\mathbb{G}_T$ *of order* q*,* $G \neq 0 \in \mathbb{G}$*, and a polynomial-time computable nondegenerate bilinear pairing* $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ *i.e.,* $e(sG, tG) = e(G, G)^{st}$ *and* $e(G, G) \neq 1$*. Let* $\mathcal{G}_{\mathsf{bpg}}$ *be an algorithm that takes input* 1^λ *and outputs a description of bilinear pairing groups* $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ *with security parameter* λ*.*

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

where $\boldsymbol{x} := (G_1, \ldots, G_N) \in \mathbb{V}$ *and* $\boldsymbol{y} := (H_1, \ldots, H_N) \in \mathbb{V}$. *This is nondegenerate bilinear i.e.,* $e(s\boldsymbol{x}, t\boldsymbol{y}) = e(\boldsymbol{x}, \boldsymbol{y})^{st}$ *and if* $e(\boldsymbol{x}, \boldsymbol{y}) = 1$ *for all* $\boldsymbol{y} \in \mathbb{V}$, *then* $\boldsymbol{x} = \boldsymbol{0}$. *For all* i *and* j, $e(\boldsymbol{a}_i, \boldsymbol{a}_j) = e(G, G)^{\delta_{i,j}}$ *where* $\delta_{i,j} = 1$ *if* $i = j$, *and* 0 *otherwise, and* $e(G, G) \neq 1 \in \mathbb{G}_T$. *DPVS generation algorithm* $\mathcal{G}_{\mathsf{dpvs}}$ *takes input* 1^λ *(*$\lambda \in \mathbb{N}$*) and* $N \in \mathbb{N}$, *and outputs a description of* $\mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ *with security parameter* λ *and* N*-dimensional* $\mathbb{V}$. *It can be constructed by using* $\mathcal{G}_{\mathsf{bpg}}$.

For the asymmetric version of DPVS, see Appendix A.2 in [12]. We describe random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}$, which is used as a subroutine in our IPE and ABE schemes.

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

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

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

3.1 Generalized Inner-Product Encryption

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

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

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

Definition 3. *An inner product encryption scheme (for generalized inner-product relation* $R(\vec{v}, \vec{x})$*) consists of probabilistic polynomial-time algorithms* Setup, KeyGen, Enc *and* Dec. *They are given as follows:*

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

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

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

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

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

Definition 4. *The model for defining the adaptively fully-attribute-hiding security of IPE against adversary* $\mathcal{A}$ *(under chosen plaintext attacks) is given by the following game:*

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

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

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

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

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

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

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

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

3.2 Attribute-Based Encryption with Non-Monotone Access Structures

Span Programs and Non-Monotone Access Structures

Definition 5 (Span Programs [2]). *Let $\{p_1, \ldots, p_n\}$ be a set of variables. A span program over $\mathbb{F}_q$ is a labeled matrix $\hat{M} := (M, \rho)$ where M is a $(\ell \times r)$ matrix over $\mathbb{F}_q$ and ρ is a labeling of the rows of M by literals from $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ (every row is labeled by one literal), i.e., $\rho : \{1, \ldots, \ell\} \to \{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$.*

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

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

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

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

Definition 6 (Access Structures). *$\mathcal{U}_t$ $(t = 1, \ldots, d$ and $\mathcal{U}_t \subset \{0,1\}^*)$ is a sub-universe, a set of attributes, each of which is expressed by a pair of sub-universe id and value of attribute, i.e., (t, v), where $t \in \{1, \ldots, d\}$ and $v \in \mathbb{F}_q$.*

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

Let Γ be a set of attributes, i.e., $\Gamma := \{(t, x_t) \mid x_t \in \mathbb{F}_q, 1 \leq t \leq d\}$, 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 $[\rho(i) = (t, v_i)] \wedge [(t, x_t) \in \Gamma] \wedge [v_i = x_t]$ or $[\rho(i) = \neg(t, v_i)] \wedge [(t, x_t) \in \Gamma] \wedge [v_i \neq x_t]$. Set $\gamma(i) = 0$ otherwise.

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

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

Definition 7. *A secret-sharing scheme for span program $\hat{M} := (M, \rho)$ is:*

1. *Let M be $\ell \times r$ matrix. Let column vector $\vec{f}^{\mathrm{T}} := (f_1, \ldots, f_r)^{\mathrm{T}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$. Then, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}} = \sum_{k=1}^{r} f_k$ is the secret to be shared, and $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$ is the vector of ℓ shares of the secret s_0 and the share s_i belongs to $\rho(i)$.*

2. *If span program* $\hat{M} := (M, \rho)$ *accept* δ*, or access structure* $\mathbb{S} := (M, \rho)$ *accepts* Γ*, i.e.,* $\vec{1} \in \mathsf{span}\langle (M_i)_{\gamma(i)=1} \rangle$ *with* $\gamma : \{1, \ldots, \ell\} \to \{0, 1\}$*, then there exist constants* $\{\alpha_i \in \mathbb{F}_q \mid i \in I\}$ *such that* $I \subseteq \{i \in \{1, \ldots, \ell\} \mid \gamma(i) = 1\}$ *and* $\sum_{i \in I} \alpha_i s_i = s_0$*. Furthermore, these constants* $\{\alpha_i\}$ *can be computed in time polynomial in the size of matrix* M*.*

Key-Policy Attribute-Based Encryption In key-policy attribute-based encryption (KP-ABE), encryption (resp. a secret key) is associated with attributes Γ (resp. access structure $\mathbb{S}$). Relation R for KP-ABE is defined as $R(\mathbb{S}, \Gamma) = 1$ iff access structure $\mathbb{S}$ accepts Γ.

Definition 8 (Key-Policy Attribute-Based Encryption: KP-ABE). *A key-policy attribute-based encryption scheme 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*. It outputs public parameters* pk *and master secret key* sk*.*
- KeyGen *takes as input public parameters* pk*, master secret key* sk*, and access structure* $\mathbb{S} := (M, \rho)$*. It outputs a corresponding secret key* $\mathsf{sk}_{\mathbb{S}}$*.*
- Enc *takes as input public parameters* pk*, message* m *in some associated message space* msg*, and a set of attributes,* $\Gamma := \{(t, x_t) | x_t \in \mathbb{F}_q, 1 \leq t \leq d\}$*. It outputs a ciphertext* ct_Γ*.*
- Dec *takes as input public parameters* pk*, secret key* $\mathsf{sk}_{\mathbb{S}}$ *for access structure* $\mathbb{S}$*, and ciphertext* ct_Γ *that was encrypted under a set of attributes* Γ*. It outputs either* $m' \in \mathsf{msg}$ *or the distinguished symbol* $\perp$*.*

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

Definition 9. *The model for defining the adaptively payload-hiding security of KP-ABE under chosen plaintext attack is given by the following game:*

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

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

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

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

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

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

4 Proposed IPE Schemes

4.1 Type 1 IPE Scheme

Construction Idea for Our Type 1 and 2 IPE Schemes In the existing constructions [11, 7, 12–15] of IPE on DPVS, around cn ($c \geq 1$) dimensional vector spaces are used for n-dimensional attribute and predicate vectors. Here, the vectors are encoded in an n-dimensional subspace. Although this is a typical strategy of constructing IPE on DPVS, we cannot employ this idea in the *unbounded* setting, where we can use only constant dimensional spaces. In our construction, each component x_t of $\vec{x}$ (resp. v_t of $\vec{v}$) is encoded in a constant dimensional space. In order to meet the decryption condition, we employ the *indexing* technique and n-out-of-n secret sharing trick. For example, in Type 1 construction, 4-dimensional vector $(\mu_t(t,-1), \delta v_t, s_t)$ is encoded in key $\boldsymbol{k}^*_t$, and $(\sigma_t(1,t), \omega x_t, \widetilde{\omega})$ is encoded in ciphertext $\boldsymbol{c}_t$. The first 2-dimension is used for indexes, and s_t in the fourth component of $\boldsymbol{k}^*_t$ is for the secret sharing. Informally, a ciphertext can be decrypted if all n pieces of shares s_t are recovered. A Type 2 IPE scheme can be constructed from our Type 1 scheme by setting the secret-sharing mechanism in the ciphertext side instead of the secret key side.

Construction of Type 1 IPE

$$
\begin{aligned}
&\mathsf{Setup}(1^\lambda): \quad (\mathsf{param}, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 5, N := 15)),\\
&\quad \widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \widehat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{14}, \boldsymbol{b}_{15}),\\
&\quad \widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}),\ \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_1, .., \boldsymbol{b}^*_4, \boldsymbol{b}^*_{12}, \boldsymbol{b}^*_{13}),\\
&\quad \text{return } \ \mathsf{pk} := (1^\lambda, \mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}),\ \mathsf{sk} := (\widehat{\mathbb{B}}^*_0, \widehat{\mathbb{B}}^*).\\
&\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v} := \{(t, v_t) \,|\, t \in I_{\vec{v}}\}): \ s_t, \delta, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q \text{ for } t \in I_{\vec{v}},\\
&\quad s_0 := \textstyle\sum_{(t,v_t)\in\vec{v}} s_t, \quad \boldsymbol{k}^*_0 := (\ -s_0,\ 0,\ 1,\ \eta_0,\ 0\ )_{\mathbb{B}^*_0},\\
&\quad \text{for } t \in I_{\vec{v}}, \quad \mu_t, \eta_{t,1}, \eta_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\quad\quad \boldsymbol{k}^*_t := (\ \overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t}^{4}\ \overbrace{0^7,}^{7}\ \overbrace{\eta_{t,1}, \eta_{t,2},}^{2}\ \overbrace{0^2}^{2}\ )_{\mathbb{B}^*},\\
&\quad \text{return } \ \mathsf{sk}_{\vec{v}} := (I_{\vec{v}}, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{t\in I_{\vec{v}}}).\\
&\mathsf{Enc}(\mathsf{pk},\ m,\ \vec{x} := \{(t, x_t) \,|\, t \in I_{\vec{x}}\}): \ \omega, \widetilde{\omega}, \zeta, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\quad \boldsymbol{c}_0 := (\ \widetilde{\omega},\ 0,\ \zeta,\ 0,\ \varphi_0\ )_{\mathbb{B}_0},\ c_T := g_T^{\zeta},
\end{aligned}
$$

for $t \in I_{\vec{x}}$, $\sigma_t, \varphi_{t,1}, \varphi_{t,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{c}_t := (\overbrace{\sigma_t(1,\ t),\ \omega x_t,\ \widetilde{\omega}}^{4}\ \overbrace{0^7,}^{7}\ \overbrace{0^2,}^{2}\ \overbrace{\varphi_{t,1}, \varphi_{t,2}}^{2}\ )_{\mathbb{B}},$$

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

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := (I_{\vec{v}}, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{t \in I_{\vec{v}}}),\ \mathsf{ct}_{\vec{x}} := (I_{\vec{x}}, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{t \in I_{\vec{x}}}, c_T))$:

if $I_{\vec{v}} \subseteq I_{\vec{x}}$, $K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot \prod_{t \in I_{\vec{v}}} e(\boldsymbol{c}_t, \boldsymbol{k}_t^*)$, return $m' := c_T / K$,

else return $\perp$.

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

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

The proof of Theorem 1 is given in the full version of this paper.

4.2 Type 0 IPE Scheme

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

Construction of Type 0 IPE

$\mathsf{Setup}(1^\lambda)$: $(\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, (N_0 := 9, N := 21))$,

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,2}, \boldsymbol{b}_{0,5}, \boldsymbol{b}_{0,8}, \boldsymbol{b}_{0,9})$, $\widehat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_5, \boldsymbol{b}_{19}, \ldots, \boldsymbol{b}_{21})$,

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,2}^*, \boldsymbol{b}_{0,5}^*, \ldots, \boldsymbol{b}_{0,7}^*)$, $\widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_5^*, \boldsymbol{b}_{16}^*, \ldots, \boldsymbol{b}_{18}^*)$,

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

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v} := (v_1, \ldots, v_n))$: $s_t, \delta, \widetilde{\delta}, \eta_{0,1}, \eta_{0,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t = 1, \ldots, n$,

$s_0 := \sum_{t=1}^n s_t$, $\boldsymbol{k}_0^* := (\ -s_0,\ \widetilde{\delta},\ 0^2,\ 1,\ \eta_{0,1}, \eta_{0,2},\ 0^2\ )_{\mathbb{B}_0^*}$,

for $t = 1, \ldots, n$, $\mu_t, \eta_{t,1}, .., \eta_{t,3} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{k}_t^* := (\overbrace{\mu_t(t,\ -1),\ \delta v_t,\ s_t,\ \widetilde{\delta},}^{5}\ \overbrace{0^{10},}^{10}\ \overbrace{\eta_{t,1}, .., \eta_{t,3},}^{3}\ \overbrace{0^3}^{3}\ )_{\mathbb{B}^*},$$

return $\mathsf{sk}_{\vec{v}} := \{\boldsymbol{k}_t^*\}_{t=0,\ldots,n}$.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \vec{x} := (x_1, \ldots, x_{n'})) :\quad f_t, \omega, \widetilde{\omega}, \zeta, \varphi_{0,1}, \varphi_{0,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t = 1, \ldots, n'$,

$f_0 := \sum_{t=1}^{n'} f_t, \quad \boldsymbol{c}_0 := (\ \widetilde{\omega},\ -f_0,\ 0^2,\ \zeta,\ 0^2,\ \varphi_{0,1},\ \varphi_{0,2}\ )_{\mathbb{B}_0}, \quad c_T := g_T^{\zeta}$,

for $t = 1, \ldots, n', \quad \sigma_t, \varphi_{t,1}, .., \varphi_{t,3} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{c}_t := (\ \overbrace{\sigma_t(1,\ t),\ \omega x_t,\ \widetilde{\omega},\ f_t}^{5},\ \overbrace{0^{10}}^{10},\ \overbrace{0^3}^{3},\ \overbrace{\varphi_{t,1}, .., \varphi_{t,3}}^{3}\ )_{\mathbb{B}},$$

return $\mathsf{ct}_{\vec{x}} := (\{\boldsymbol{c}_t\}_{t=0,\ldots,n'}, c_T)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := \{\boldsymbol{k}_t^*\}_{t=0,\ldots,n},\ \mathsf{ct}_{\vec{x}} := (\{\boldsymbol{c}_t\}_{t=0,\ldots,n'}, c_T)) :$

if $n = n',\ K := \prod_{t=0}^{n} e(\boldsymbol{c}_t, \boldsymbol{k}_t^*)$, return $m' := c_T/K$, else return $\perp$.

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

Theorem 2. *The proposed Type 0 IPE scheme is adaptively fully-attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

The proof of Theorem 2 is given in the full version of this paper.

5 Proposed KP-ABE Scheme (Basic)

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

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

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

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

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

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (M, \rho)) :\ \vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r,\ s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$,

$\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}},\ \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \boldsymbol{k}_0^* := (-s_0,\ 0,\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}$,

for $i = 1, \ldots, \ell, \quad \mu_i, \theta_i, \eta_{i,1}, \eta_{i,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

if $\rho(i) = (t, v_i)$,

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

if $\rho(i) = \neg(t, v_i)$,

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

return $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_i^*\}_{i=0,\ldots,\ell})$.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \Gamma := \{(t,x_t) \mid 1 \le t \le d\}) :\ \omega, \zeta, \varphi_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q,$

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

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

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

return $\mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}, c_{d+1})$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_i^*\}_{i=0,\ldots,\ell}),\ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}, c_{d+1})) :$

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

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

$I \subseteq \{i \in \{1,\ldots,\ell\} \mid [\rho(i) = (t,v_i) \wedge (t,v_i) \in \Gamma]$

$\qquad\qquad \vee\, [\rho(i) = \neg(t,v_i) \wedge (t,x_t) \in \Gamma \wedge v_i \neq x_t]\ \},$

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

return $m' := c_{d+1}/K,$ else return $\perp$.

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

Theorem 3. *The proposed KP-ABE scheme is adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption.*

The proof of Theorem 3 is given in the full version of this paper.

References

1. Attrapadung, N., Libert, B.: Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 384–402. Springer (2010)
2. Beimel, A.: Secure schemes for secret sharing and key distribution. PhD Thesis, Israel Institute of Technology, Technion, Haifa (1996)
3. 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)
4. 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)
5. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Juels, A., Wright, R.N., di Vimercati, S.D.C. (eds.) ACM CCS 2006. pp. 89–98. ACM (2006)
6. 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)

7. 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 2010. LNCS, vol. 6110, pp. 62–91. Springer (2010), full version is available at http://eprint.iacr.org/2010/110
8. Lewko, A.B., Waters, B.: Decentralizing attribute-based encryption. In: Paterson [17], pp. 568–588
9. Lewko, A.B., Waters, B.: Unbounded HIBE and attribute-based encryption. In: Paterson [17], pp. 547–567
10. Lewko, A.B., Waters, B.: New proof methods for attribute-based encryption: Achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer (2012)
11. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer (2009)
12. 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
13. 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
14. Okamoto, T., Takashima, K.: Adaptively attribute-hiding (hierarchical) inner product encryption. In: Pointcheval, D., Johansson, T. (eds.) Eurocrypt 2012. LNCS, vol. 7237, pp. 591–608. Springer (2012), full version is available at http://eprint.iacr.org/2011/543
15. Okamoto, T., Takashima, K.: Efficient (hierarchical) inner product encryption tightly reduced from the decisional linear assumption. To appear in IEICE Trans. Fundamentals vol.E96-A, no.1, Jan. 2013 (2013)
16. 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 CCS 2007. pp. 195–203. ACM (2007)
17. Paterson, K.G. (ed.): Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings, LNCS, vol. 6632. Springer (2011)
18. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer (2005)
19. 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)
20. Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer (2011)