Fully-Anonymous Functional Proxy-Re-Encryption

Yutaka Kawai and Katsuyuki Takashima

Mitsubishi Electric, 5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan,
Kawai.Yutaka@da.MitsubishiElectric.co.jp, Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

October 11, 2013

Abstract. In this paper, we introduce a general notion of functional proxy-re-encryption (F-PRE), where a wide class of functional encryption (FE) is combined with proxy-re-encryption (PRE) mechanism. The PRE encryption system should reveal *minimal* information to a proxy, in particular, hiding parameters of re-encryption keys and of original ciphertexts which he manipulate is highly desirable. We first formulate such a *fully-anonymous* security notion of F-PRE including usual payload-hiding properties. We then propose the first fully-anonymous inner-product PRE (IP-PRE) scheme, whose security is proven under the DLIN assumption and the existence of a strongly unforgeable one-time signature scheme in the standard model. Also, we propose the first ciphertext-policy F-PRE scheme with the access structures of Okamoto-Takashima (CRYPTO 2010), which also has an anonymity property for re-encryption keys as well as payload-hiding for original and re-encrypted ciphertexts. The security is proven under the same assumptions as the above IP-PRE scheme in the standard model. For these results, we develop novel *blind delegation* and *subspace insulation for re-enc key basis* techniques on the dual system encryption (DSE) paradigm and the dual pairing vector spaces (DPVS) approach. These techniques seem difficult to be realized by a *composite-order* bilinear group DSE approach.

1 Introduction

1.1 Background

The notions of *inner-product encryption* (IPE) and *attribute-based encryption* (ABE) introduced by Katz, Sahai and Waters [13] and Sahai and Waters [31] 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.

For some applications for FE, the parameters for encryption are required to be hidden from ciphertexts. To capture the security requirement, Katz, Sahai and Waters [13] introduced *attribute-hiding* (based on the same notion for hidden vector encryption (HVE) by Boneh and Waters [6]), 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. Informally, in the (fully) attribute-hiding, the secrecy of challenge attribute $x^{(0)}, x^{(1)}$ is ensured against an adversary having a secret key with v such that $R(v, x^{(0)}) = R(v, x^{(1)})$ holds (even if $R(v, x^{(b)}) = 1$), i.e., the adversary cannot guess bit b if the *compatibility* condition $R(v, x^{(0)}) = R(v, x^{(1)})$ for the challenge holds. (It is a maximal requirement since if the challenge is incompatible for some key query, an adversary easily guess the challenge bit.) Inner-products for IPE represent a fairly wide class of relations including equality tests as the simplest case, 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 [29] achieves the *full (adaptive)* security and *fully attribute-hiding* simultaneously. As for ABE, Lewko et.al. and Okamoto-Takashima ABE schemes [14, 27] are fully secure in the standard model.

Proxy-re-encryption (PRE) is an interesting extension of traditional public key encryption (PKE). In addition to the normal operations of PKE, with a dedicated re-encryption key (generated by an original receiver A), a proxy can turn ciphertexts originally destined for user A (called original ciphertexts) into those for user B. A remarkable property of PRE is that the proxy carrying out the transform is totally ignorant of the plaintext. PRE was first formalized by Blaze et al. [4] and has received much attention in recent years. There are many models as well as implementations; refer to [4, 2, 8, 20, 33, 19, 9, 34, 35, 12, 23, 22, 11, 17] for some examples.

Extending FE with PRE, i.e., functional PRE (F-PRE), improves various aspects of existing FE. For example, when Alice contacts a local government on tax and social security, she submits encrypted information to a man to contact (say, Bob) since she has *no knowledge on the inner structure* of the government, which is usually a confidential matter. Bob is given a re-encryption key from his manager, and then re-encrypts the encrypted message on tax to *an appropriate department X*, and that on social security to *another department Y*, while Bob learns *nothing on the contents* for the privacy of

Table 1. Comparison of our schemes with existing Ciphertext-Policy (CP)-AB-PRE schemes [19, 22, 18], where q, d, $|U|$, $|\Gamma|$, ℓ (resp. ℓ') and n represent the number of key queries, the number of sub-universes of attributes, the maximum size of a sub-universe, the number of attributes for the secret key, the number of rows in access matrix for the original ciphertext (resp. re-enc key or re-enc ciphertext) and the dimension for attribute vectors, respectively. STdM, ROM, CTDH, ADBDH, DBDH, BDHE, and sUF stand for standard model, random oracle model, complex triple Diffie-Hellman problem, augment decisional bilinear Diffie-Hellman problem, the decisional bilinear Diffie-Hellman problem, and the bilinear Diffie-Hellman exponent problem, strongly unforgeable, respectively. (PK, SK, RK, OCT and RCT stand for public key, secret key, re-encryption key, original ciphertext, re-encrypted ciphertext, respectively.)

	LCLS09 [19]	LHC10 [22]	LFWS13 [18] [a]	Proposed	
Primitive	CP-AB-PRE	CP-AB-PRE	CP-AB-PRE	IP-PRE [b]	CP-AB-PRE
Security model	selective in STdM	selective in STdM	selective in ROM	adaptive in STdM	adaptive in STdM
Access structures	non-monotonic AND gates	non-monotonic AND gates	(large-universe) monotonic span programs	inner-product relations	(large-universe) non-monotonic span programs
Assumptuion	CTDH & ADBDH	DBDH	q-parallel BDHE	DLIN & sUF sig.	DLIN & sUF sig.
Anonymity against Proxy	×	×	×	✓	✓
PK/SK/ RK size [c]	$O(d)/O(d)/$ $O(d)$	$O(d\|U\|)/O(d)/$ $O(d)$	$O(1)/O(\|\Gamma\|)/$ $O(\|\Gamma\|+\ell')$	$O(n)/O(n)/$ $O(n^2)$	$O(d)/O(\|\Gamma\|)/$ $O(d+\ell')$
OCT/RCT size [c]	$O(d)/O(d)$	$O(1)/O(1)$	$O(\ell)/O(\ell+\ell')$	$O(n)/O(n^2)$	$O(\ell)/O(d+\ell+\ell')$

[a] The *large-universe* CP-AB-PRE obtained from *small-universe* one in [17] has similar features as that of [18].
[b] An efficient version of our fully-anonymous IP-PRE scheme in Section 4.2 by applying the sparse matrix technique given in [28]
[c] The number of group elements is given with a common assumption in the ABE/IPE application that the description of the attribute or policy is not considered a part of SK/RK/OCT/RCT.

Alice. (By using our *fully anonymous* F-PRE, Bob need not know even the destinations, X or Y.) Such re-encryption by attributes also deals with personnel changes flexibly: When the department X (or some of the members) is changed to Y, Bob re-encrypts an encrypted message originally for X to that destined to Y. As the examples show, F-PRE realizes convenient private communication even among organizations with *unknown or changeable inner structures*.

Previously, various combinations of PRE and special classes of FE exist, that is, ID-based PRE (IB-PRE) [12, 23, 11], broadcast encryption based PRE [10, 38], attribute-based PRE (AB-PRE) [19, 24, 22, 17, 18]. While the notion of AB-PRE covers the existing F-PRE schemes above, the previous AB-PRE schemes [19, 22, 17, 18] only achieve a weak security, that is, security in the *selective model* (Table 1). Also, access structures which can be treated in the previous AB-PRE [19, 24, 22] are just conjunctive (AND) formulas, not disjunction (OR) or negation (NOT). Thus, these previous F-PRE schemes are insufficient from the view point of functionality or security, or both.

In recent applications, usually, the data is outsourced to an outside remote server. Then, since we do not trust on the server manager, or proxy, any more, another important requirement for PRE is *anonymity for a re-encryption key*: As well as an encrypted message, source and target parameters of a re-encryption key, i.e., v and x' of $\mathsf{rk}_{v,x'}$, should be concealed from *the proxy*. The security property ensures that we can *securely* outsource the re-encryption task to the proxy.

Surprisingly, many previous PRE schemes (even of traditional PKE-based) has no anonymity for a re-encryption key. The first anonymous (PKE-based) PRE scheme was proposed by Ateniese et al. [1], however, the security is only proven in a weak security model, where only a *restricted* adversary is considered. While the weak point was removed in a subsequent work by Shao et al. [36],

Table 2. Comparison of *anonymity* properties ("Anonimity" and "Unlinkability") between our schemes and existing several anonymous (F-)PRE schemes [1, 11, 36, 32, 21]. STdM, ROM, OCT, RCT, RK and AH-RK stand for standard model, random oracle model, original ciphertext, re-encrypted ciphertext, re-encryption key and attribute-hiding for re-encryption keys, respectively.

	ABH09 [1]	SLWL12 [36]	EMO11 [11]	Shao12 [32]	Proposed	
Primitive	(PK-)PRE		IB-PRE		IP-PRE	CP-AB-PRE
Security model	in STdM	in ROM	in ROM		in STdM	
Anonimity for OCT/RCT/RK	✓[a b]	✓[a]	✓	✓	✓	partial ✓ (only for AH-RK)
Unlinkability for RCT/RK	✓	partial ✓ (only for RK)	✓	partial ✓ (only for RK)	✓	✓

[a] An original ciphertext has an anonymity in the sense that it cannot be linked to the used public key.
[b] The anonymity for RK is only proven in a weak security model, where an adversary cannot query with the same parameter twice to the re-encryption key oracle.

the security of their scheme is proven only in the random oracle model. Moreover, *anonymous F-PRE* schemes were proposed in [11, 32], however, they are *less expressive ID-based* PRE and the security is claimed just in the *random oracle model*. No such kinds of anonymous (including key-private) *expressive inner-product* (IP-)PRE exists. Namely, existing anonymous F-PRE constructions are quite insufficient. See Table 2 for the comparison on anonymous F-PRE.

An *anonymous* F-PRE scheme should have usual anonymous FE security requirements, that is, payload-hiding and *(fully-)attribute-hiding security* for original and re-encrypted ciphertexts. And, as mentioned, parameters (v, x'), which we call predicate and attribute, respectively, in a re-encryption key $\mathsf{rk}_{v,x'}$ should be also concealed. The secrecy should be kept against a powerful adversary who can access a combination of decryption key, re-encryption key, and re-encryption queries. For example, even using the two types of keys, an original ciphertext should not reveal additional information on message or attributes. We will give a reasonable security definition including the above basic requirements (in Section 3) and call it *fully-anonymity*.

Our first target is an *adaptively secure* and *fully anonymous* IP-PRE scheme (Table 2). Among the above requirements, (full) attribute-hiding property for an original ciphertext is the most challenging since an adversary can apply queried decryption keys, re-encryption keys, and re-encryption oracle to the target ciphertext. Even if we use the dual system encryption (DSE) by Waters [37] and its extension in [29], the main difficulty resides in how to change a (normal) re-encryption key queried with $(\vec{v}, \vec{x}')$ to a semi-functional re-encryption key, *before seeing the challenge* $(\vec{x}^{(0)}, \vec{x}^{(1)})$, i.e., without knowing whether $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)})$ holds or not. We will explain it below: The previous fully attribute-hiding IPE security game allows a non-matching key query, and it requires that a decryption key query $\vec{v}$ is compatible with the challenge $(\vec{x}^{(0)}, \vec{x}^{(1)})$, i.e., $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)})$. (The case that $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = 0$ is a non-matching one.) While this condition for the challenge and decryption key queries is common for the previous FE systems, a (fully-anonymous) F-PRE scheme must also deal with a more complicated condition, i.e.,

$$R(\vec{v}, \vec{x}^{(0)}) \cdot R(\vec{v}', \vec{x}') = R(\vec{v}, \vec{x}^{(1)}) \cdot R(\vec{v}', \vec{x}') \tag{1}$$

for any re-encryption key query $(\vec{v}, \vec{x}')$ and decryption key query $\vec{v}'$. It reflects one attack strategy of the adversary, where he (or she) tries to convert the challenge ciphertext to a re-encrypted one by a queried re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'}$ and then decrypt it by a queried decryption key $\mathsf{sk}_{\vec{v}'}$. We consider some fixed re-encryption key query $(\vec{v}, \vec{x}')$ below. If $R(\vec{v}', \vec{x}') = 1$ for *some* decryption key query $\vec{v}'$,

Eq. (1) is equivalent to $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)})$. However, if $R(\vec{v}', \vec{x}') = 0$ for *any* decryption key query $\vec{v}'$, Eq. (1) holds unconditionally even in the incompatible case, i.e., $R(\vec{v}, \vec{x}^{(0)}) \neq R(\vec{v}, \vec{x}^{(1)})$. At a first glance, it looks hard to treat with both the cases simultaneously, since the form of semi-functional re-encryption key *may* be different depending on whether $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)})$ or not, and the simulator does not know the fact when the re-encryption key query occurs before the challenge.

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

1. This paper introduces a new notion of functional proxy-re-encryption (F-PRE). The system should reveal *minimal* information to a proxy, in particular, hiding parameters in re-encryption keys and in original ciphertexts which he manipulates is highly desirable. We first formulate such a *fully-anonymous* notion of F-PRE, which includes usual payload-hiding properties. It can be considered as a natural extension of *fully-attribute-hiding* FE. The notion consists of the following security requirements, which are informally described, and more formally defined by the games against an adversary with access to decryption, re-encrypted key, and re-encryption queries (see Section 3 for the formal definitions). Here, parameters x, x' and v are called attributes and a predicate, respectively.
   - **Attribute-Hiding Security for Original Ciphertexts:** An original ciphertext for plaintext m and attribute x releases no information regarding (m, x) against a user not in possession of a matching decryption key sk_v with $R(v, x) = 1$, or a matching key pair of a re-encryption key and a decryption key $(\mathsf{rk}_{v,x'}, \mathsf{sk}_{v'})$ with $R(v, x) = 1$ and $R(v', x') = 1$. It also releases no information regarding x against a user in possession of a matching decryption key sk_v except that $R(v, x) = 1$ or a matching key pair $(\mathsf{rk}_{v,x'}, \mathsf{sk}_{v'})$ except that $R(v, x) = 1$ and $R(v', x') = 1$.
   - **Predicate- and Attribute-Hiding Security for Re-encrypted Ciphertexts:** A re-encrypted ciphertext for plaintext m (and original attribute x) and re-encryption key $\mathsf{rk}_{v,x'}$ with attribute x' releases no information regarding $(m, x, v; x')$ against a user not in possession of a matching decryption key $\mathsf{sk}_{v'}$ for x', and no information regarding x' against a user in possession of a matching decryption key $\mathsf{sk}_{v'}$ except that $R(v', x') = 1$.
   - **Predicate- and Attribute-Hiding Security for Re-encryption Keys:** A re-encryption key for predicate and attribute (v, x') releases no information regarding (v, x') against a user not in possession of a matching key for x', and no information regarding x' against a user in possession of a matching decryption key $\mathsf{sk}_{v'}$ except that $R(v', x') = 1$.
   - **Unlinkability of Re-encryption Keys:** A re-encryption key generated from a decryption key cannot be linked to the decryption key by any means (unconditional unlinkability).
   - **Unlinkability of Re-encrypted Ciphertexts:** A re-encrypted ciphertext generated from a re-encryption key and an original ciphertext cannot be linked to the re-encryption key or the original ciphertext by any efficient adversary (computational unlinkability).
   - **Full Anonymity:** We say that an F-PRE scheme is *fully-anonymous* if it satisfies the above three hiding requirements given in three *adaptive* security games, and two unlinkability requirements.
2. This paper proposes the first *fully-anonymous* inner-product proxy-re-encryption (IP-PRE) scheme, whose security is proven under the DLIN assumption and the existence of a strongly unforgeable one-time signature scheme in the standard model (Tables 1 and 2, Theorem 1). The IP-PRE scheme uses an underlying fully attribute-hiding IPE scheme, which was proposed in [29]. It shows a new significant application of fully attribute-hiding property except for searchable encryption. For achieving the security properties, we use two key techniques, *blind delegation* and *hidden subspace insulation* for (extended) dual system encryption.

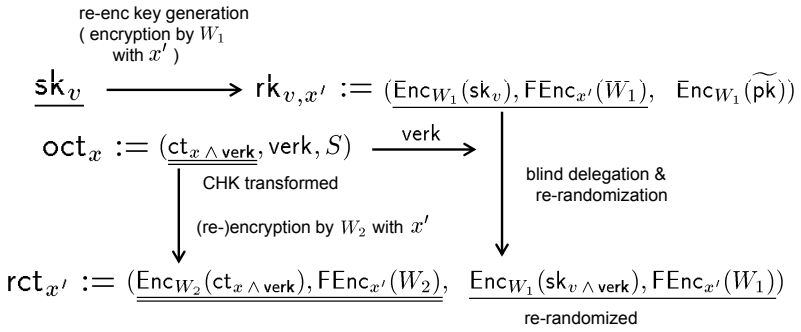

Fig. 1. Basic Conversions among secret key sk_v, re-encryption key $\mathsf{rk}_{v,x'}$, original ciphertext oct_x and re-encrypted ciphertext $\mathsf{rct}_{x'}$ in a high-level description

3. We also propose the first ciphertext-policy (CP-)F-PRE scheme with the access structure class given by Okamoto-Takashima [27], which includes non-monotone span program access structures. The construction is based on our IP-PRE schemes. The scheme is proven to be payload-hiding of original and re-encrypted ciphertexts, attribute-hiding of re-encryption keys, and unlinkable under the same assumptions as those of our IP-PRE schemes (Tables 1 and 2). Here, hiding attributes of re-encryption keys is an important requirement for anonymous re-encryption outsourcing. Refer to Appendix E.

1.3 Key Techniques

As we mentioned in Section 1.1, in our fully-anonymous F-PRE, while a decryption key query v should satisfy a simple compatibility condition ($R(v, x^{(0)}) = R(v, x^{(1)})$) with the challenge, a re-encryption key query (v, x') need satisfy a complicated condition in Eq. (1), which includes an incompatible case ($R(v, x^{(0)}) \neq R(v, x^{(1)})$). All the previous DSE proofs (including the fully-attribute-hiding one [29]) use the compatibility condition as an essential logical ingredient. Hence, we need to develop an extended DSE technique which allows the incompatible case for achieving *adaptively secure* and *fully-anonymous* F-PRE.

CHK Transform and Blind Delegation: As a first attempt, to conceal sk_v (including v) from a malicious proxy, we encrypt it as $(\mathsf{Enc}_{W_1}(\mathsf{sk}_v), \mathsf{FEnc}_{x'}(W_1))$ in a re-encryption key $\mathsf{rk}_{v,x'}$, where Enc is an ordinary (symmetric) encryption scheme with secret W_1, and FEnc is a functional encryption scheme with parameter x'. Then, if an adversary has no matching key for x', he has no information of sk_v nor v.

If these components are also embedded into a re-encrypted ciphertext $\mathsf{rct}_{x'}$ *without modification*, a user with a matching key for x' obtains the original sk_v. It is not desirable for (F-)PRE, therefore, modified forms of $\mathsf{Enc}_{W_1}(\mathsf{sk}_v)$ (and $\mathsf{FEnc}_{x'}(W_1)$)) should be embedded into a re-encrypted ciphertext $\mathsf{rct}_{x'}$. For achieving an appropriate modification, we use two ingredients, the Canetti-Halevi-Katz (CHK) transformation [7] and *blind delegation* (see Figure 1). The CHK transformation converts a ciphertext ct_x to $\mathsf{ct}_{x \wedge \mathsf{verk}}$, where verk is a verification key of a one-time signature scheme, and $x \wedge \mathsf{verk}$ is the conjunction of x (for relation R) and verk (for identity matching). An original ciphertext in our F-PRE schemes consists of $\mathsf{oct}_x := (\mathsf{ct}_{x \wedge \mathsf{verk}}, \mathsf{verk}, S)$ with S is a signature of $\mathsf{ct}_{x \wedge \mathsf{verk}}$ by a corresponding signature generation key. Then, a decryptor of oct_x first verifies if S is valid under verk, and if so, correctly decrypts $\mathsf{ct}_{x \wedge \mathsf{verk}}$ with a decryption key. By this mechanism, an adversary cannot modify the challenge ciphertext meaningfully. Using verk in input, a re-encryptor modifies

(or delegates) sk_v to $\mathsf{sk}_{v\wedge\mathsf{verk}}$, which is specialized to $\mathsf{ct}_{x\wedge\mathsf{verk}}$ in the input original ciphertext. Since $\mathsf{ct}_{x\wedge\mathsf{verk}}$ cannot be modified to another meaningful one, modified $\mathsf{sk}_{v\wedge\mathsf{verk}}$ is only effective to $\mathsf{ct}_{x\wedge\mathsf{verk}}$.

Here, we have a technical challenge: The re-encryptor should modify $\mathsf{Enc}_{W_1}(\mathsf{sk}_v)$ to $\mathsf{Enc}_{W_1}(\mathsf{sk}_{v\wedge\mathsf{verk}})$ without decrypting $\mathsf{Enc}_{W_1}(\mathsf{sk}_v)$, i.e., in an encrypted form. For achieving it, in our schemes, we will include $\mathsf{Enc}_{W_1}(\widetilde{\mathsf{pk}})$ in a re-encryption key $\mathsf{rk}_{v,x'}$, where $\widetilde{\mathsf{pk}}$ is a part of the public key. Namely, $\mathsf{rk}_{v,x'}$ essentially consists of $(\mathsf{Enc}_{W_1}(\mathsf{sk}_v), \mathsf{FEnc}_{x'}(W_1), \mathsf{Enc}_{W_1}(\widetilde{\mathsf{pk}}))$, and in re-encryption, a re-encryptor delegates $\mathsf{Enc}_{W_1}(\mathsf{sk}_v)$ to $\mathsf{Enc}_{W_1}(\mathsf{sk}_{v\wedge\mathsf{verk}})$ using $\mathsf{Enc}_{W_1}(\widetilde{\mathsf{pk}})$ in a blind manner. Hence, we call such a new technique *blind delegation*. We develop it based on the dual pairing vector spaces (DPVS) framework [26, 27, 29]. (See REnc algorithms in Sections 4.1 and 4.2.)

Moreover, in order not to allow a matching key holder for x to decrypt a re-encrypted ciphertext $\mathsf{rct}_{x'}$ (with $x' \neq x$), $\mathsf{ct}_{x\wedge\mathsf{verk}}$ in an input original ciphertext is encrypted with another secret W_2 in re-encryption. Hence, the re-encrypted ciphertext $\mathsf{rct}_{x'}$ essentially consists of $(\mathsf{Enc}_{W_2}(\mathsf{ct}_{x\wedge\mathsf{verk}}), \mathsf{FEnc}_{x'}(W_2), \mathsf{Enc}_{W_1}(\mathsf{sk}_{v\wedge\mathsf{verk}}), \mathsf{FEnc}_{x'}(W_1))$, where $\mathsf{FEnc}_{x'}(W_1)$ is re-randomized for an unlinkability requirement (Figure 1). A decryptor with a matching key for x' first obtains W_1 and W_2 and calculates $\mathsf{Dec}(\mathsf{sk}_{v\wedge\mathsf{verk}}, \mathsf{ct}_{x\wedge\mathsf{verk}})$ by using usual decryption.

Information-Theoretical Insulation of a Subspace for Re-Enc Key Basis: For formal security proof, we use a novel technique (*subspace insulation for re-enc key basis*) for realizing DSE with allowing an incompatible re-encryption key query. In an original DSE security game [37, 27], each queried decryption key is changed to semi-functional, one by one. In our F-PRE, we also change each queried re-encryption key to semi-functional, one by one. Since a simulator (challenger) does not know whether the query is compatible or incompatible to the challenge before seeing the challenge query, the semi-functional form should not depend on the compatibility type. Namely, we need to give *two (or more) different and consistent simulations* for the *same* semi-functional re-encryption key for (v, x') with the following requirements:

- If some matching decryption key for x' is queried, the adversary obtains the secret W_1 for the re-encryption key. The challenger must simulate a semi-functional form of a decryption key sk_v, which can be decrypted from $\mathsf{Enc}_{W_1}(\mathsf{sk}_v)$ by using W_1.
- If no matching decryption keys for x' are queried, the adversary has no W_1 for the re-encryption key. The challenger must simulate $\mathsf{Enc}_{W_1}(\mathsf{sk}_v)$ which is *consistent* with the above semi-functional form of sk_v. For the simulation, we use an *insulated subspace* since W_1 is hidden for the adversary.

To achieve the above simulations, we realize a nice trick based on the DPVS framework. That is, we can create a (hidden) subspace of a re-enc key basis $\mathbb{D}_1^* := \mathbb{B}^* \cdot W_1$, which is *information-theoretically insulated from* the master key bases $(\mathbb{B}, \mathbb{B}^*)$. We elaborately combine this trick for the second type of re-encryption key queries, and a similar game change as in the original (and extended) DSE in [27, 29] for the first type key queries based on a pairwise independent argument. For the details of the technique, refer to Appendix D.1 and Figure 2.

DPVS Framework: Both techniques, i.e., blind delegation and subspace insulation for re-enc key basis, are built on the DPVS framework, where a ciphertext $\boldsymbol{c}_x$ and a secret key $\boldsymbol{k}_v^*$ are encoded on a random basis $\mathbb{B} := (\boldsymbol{b}_i)$ and its dual $\mathbb{B}^* := (\boldsymbol{b}_i^*)$, respectively. For blind delegation, a random matrix W_1 in $\mathbb{F}_q^{N\times N}$ transforms $\boldsymbol{k}_v^*$ and $\boldsymbol{b}_i^* (\in \widetilde{\mathsf{pk}})$ to $\boldsymbol{k}_v^{*\mathsf{rk}} := \boldsymbol{k}_v^* W_1$ and $\boldsymbol{d}_i^* := \boldsymbol{b}_i^* W_1 (\in \mathsf{Enc}_{W_1}(\widetilde{\mathsf{pk}}))$ in a re-encryption key, then, REnc delegates $\boldsymbol{k}_v^{*\mathsf{rk}}$ to $\boldsymbol{k}_{v\wedge\mathsf{verk}}^{*\mathsf{rk}}$ by using $\boldsymbol{d}_i^*$ instead of $\boldsymbol{b}_i^*$. For the delegation, not all basis vectors $\boldsymbol{d}_i^*$ (in $\mathbb{D}^*$) are included in the re-encryption key, hence, an *insulated* hidden subspace from a subbasis of $\mathbb{D}^* := (\boldsymbol{d}_i^*)$ is used for proving adaptive security against an adversary, and the basis changing technique is crucial for our constructions. In composite-order DSE schemes, a hidden subspace (subgroup) is given by the order-q subgroup in order-pqr subgroup (with p, q, r primes), for example. Therefore, while the DPVS approach is suitable for the above subspace insulation, the composite-order bilinear group approach seems to be difficult to realize them.

1.4 Notations

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

2 Dual Pairing Vector Spaces (DPVS)

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

In this paper, we concentrate on the symmetric version of dual pairing vector spaces [25, 26]. 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 Appendix A.2 in the full version of [27].

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* $\boldsymbol{x} = \vec{0}$*. 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 matrix $W := (w_{i,j})_{i,j=1,\ldots,N} \in \mathbb{F}_q^{N \times N}$ and element $\boldsymbol{g} := (G_1, \ldots, G_N)$ in N-dimensional $\mathbb{V}$, $\boldsymbol{g}W$ denotes $(\sum_{i=1}^N G_i w_{i,1}, \ldots, \sum_{i=1}^N G_i w_{i,N}) = (\sum_{i=1}^N w_{i,1} G_i, \ldots, \sum_{i=1}^N w_{i,N} G_i)$ by a natural multiplication of a N-dim. row vector and a $N \times N$ matrix. Thus it holds an associative law like $(\boldsymbol{g}W)W^{-1} = \boldsymbol{g}(WW^{-1}) = \boldsymbol{g}$.

3 Functional Proxy-Re-Encryption

In this section, we define a notion of functional proxy-re-encryption, F-PRE, and its security. An attribute and a predicate are expressed as x and v, respectively. We denote $R(v, x) = 1$ that a

relation holds for v and x. Informally speaking, F-PRE is functional encryption with re-encryption mechanism, that is, an FE scheme with additional algorithms, re-encryption key generation (RKG) and re-encryption (REnc). RKG algorithm, which takes as input a decryption key of FE sk_v and an attribute x', generates a re-encryption key $\mathsf{rk}_{v,x'}$ which is associated with v and x'. A proxy who is given a re-encryption key $\mathsf{rk}_{v,x'}$ and an original ciphertext with x, can computes a *re-encrypted* ciphertext with attribute x' from a ciphertext with x using REnc algorithm if $R(v,x)=1$.

Definition 3 (Functional Proxy-Re-Encryption: F-PRE). *A functional proxy-re-encryption scheme consists of the following seven algorithms.*

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

KG**:** *takes as input the public key pk, the (master) secret key sk, and a predicate v. It outputs a corresponding decryption key sk_v.*

Enc**:** *takes as input the public key pk, an attribute x, and a plaintext m in some associated plaintext space. It outputs an original ciphertext oct_x.*

RKG**:** *takes as input the public key pk, a decryption key sk_v, and an attribute x'. It outputs a re-encryption key $\mathsf{rk}_{v,x'}$.*

REnc**:** *takes as input the public key pk, a re-encryption key $\mathsf{rk}_{v,x'}$, and an original ciphertext oct_x. It outputs a re-encrypted ciphertext $\mathsf{rct}_{x'}$.*

$\mathsf{Dec}_{\mathsf{oct}}$**:** *takes as input the public key pk, a decryption key sk_v, and an original ciphertext oct_x. It outputs either a plaintext m or the distinguished symbol $\perp$.*

$\mathsf{Dec}_{\mathsf{rct}}$**:** *takes as input the public key pk, a decryption key $\mathsf{sk}_{v'}$, and a re-encrypted ciphertext $\mathsf{rct}_{x'}$. It outputs either a plaintext m or the distinguished symbol $\perp$.*

The correctness for an F-PRE scheme is defined as:

1. For any plaintext m, any $(\mathsf{pk},\mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda)$, any v and x, any decryption key $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk},\mathsf{sk},v)$, and any original ciphertext $\mathsf{oct}_x \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk},x,m)$, we have $m=\mathsf{Dec}_{\mathsf{oct}}(\mathsf{pk},\mathsf{sk}_v,\mathsf{oct}_x)$ if $R(v,x)=1$. Otherwise, it holds with negligible probability.
2. For any plaintext m, any $(\mathsf{pk},\mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda)$, any v,v',x,x', any decryption key $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk},\mathsf{sk},v)$, any re-encryption key $\mathsf{rk}_{v,x'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk},\mathsf{sk}_v,x')$, any original ciphertext $\mathsf{oct}_x \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk},x,m)$, and re-encrypted ciphertext $\mathsf{rct}_{x'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk},\mathsf{rk}_{v,x'},\mathsf{oct}_x)$, we have $m=\mathsf{Dec}_{\mathsf{rct}}(\mathsf{pk},\mathsf{sk}_{v'},\mathsf{rct}_{x'})$ if $R(v,x)=1$ and $R(v',x')=1$. Otherwise, it holds with negligible probability.

Definition 4. *We introduce a useful (multiplicative) notation "$\bullet$" for describing our security definitions (Definitions 5–7) concisely. For any variable X,*

$$X \bullet R(v,x) := \begin{cases} X & \text{if } R(v,x)=1, \\ \perp & \text{if } R(v,x)=0. \end{cases}$$

Let $m \bullet R(v,x) \bullet R(v',x')$ mean $(m \bullet R(v,x)) \bullet R(v',x')$. Then, the results of items 1 and 2 in the above correctness are rephrased as $m \bullet R(v,x) = \mathsf{Dec}_{\mathsf{oct}}(\mathsf{pk},\mathsf{sk}_v,\mathsf{oct}_x)$ and $m \bullet R(v,x) \bullet R(v',x') = \mathsf{Dec}_{\mathsf{rct}}(\mathsf{pk},\mathsf{sk}_{v'},\mathsf{rct}_{x'})$, respectively.

Next, we define four security properties of F-PRE.

Definition 5 (Attribute-Hiding for Original Ciphertexts (AH-OC)). *The model for defining the (adaptively) attribute-hiding security for original ciphertexts of F-PRE against adversary $\mathcal{A}$ (under chosen plaintext attacks) is given by the following game:*

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

Phase 1. *The adversary* $\mathcal{A}$ *is allowed to adaptively issue a polynomial number of queries as follows.*

Decryption key query. *For a decryption key query* v*, the challenger gives* $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v)$ *to* $\mathcal{A}$*.*

Re-encryption key query. *For a re-encryption key query* (v, x')*, the challenger computes* $\mathsf{rk}_{v,x'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_v, x')$ *where* $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v)$*. It gives* $\mathsf{rk}_{v,x'}$ *to* $\mathcal{A}$*.*

Re-encryption query. *For a re-encryption query* (v, x', oct_x)*, the challenger computes* $\mathsf{rk}_{v,x'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_v, x')$ *where* $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v)$ *and* $\mathsf{rct}_{x'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{v,x'}, \mathsf{oct}_x)$*. It gives* $\mathsf{rct}_{x'}$ *to* $\mathcal{A}$*.*

Challenge. *For a challenge query* $(m^{(0)}, m^{(1)}, x^{(0)}, x^{(1)})$ *subjected to the following restrictions:*

- *Any decryption key query* v *and any re-encryption key query* (v_ℓ, x'_ℓ) *for* $\ell = 1, \ldots, \nu_2$ *satisfy* $m^{(0)} \bullet R(v, x^{(0)}) = m^{(1)} \bullet R(v, x^{(1)})$ *and* $m^{(0)} \bullet R(v_\ell, x^{(0)}) \bullet R(v, x'_\ell) = m^{(1)} \bullet R(v_\ell, x^{(1)}) \bullet R(v, x'_\ell)$*.*

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

Phase 2. *The adversary* $\mathcal{A}$ *may continue to issue decryption key queries, re-encryption key queries and re-encryption queries, subjected to the restriction in challenge phase and the following additional restriction for re-encryption queries.*

Re-encryption query. *For a re-encryption query* $(v_t, x'_t, \mathsf{oct}_t)$ *for* $t = 1, \ldots, \nu_3$*, subject to the following restrictions:*

- $m^{(0)} \bullet R(v_t, x^{(0)}) \bullet R(v', x'_t) = m^{(1)} \bullet R(v_t, x^{(1)}) \bullet R(v', x'_t)$ *for any decryption key query for* v' *if* $\mathsf{oct}_t = \mathsf{oct}_{x^{(b)}}$

The challenger computes $\mathsf{rk}_{v_t,x'_t} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v_t), x'_t)$ *and* $\mathsf{rct}_{x'_t} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{v_t,x'_t}, \mathsf{oct}_t)$*. It gives* $\mathsf{rct}_{x'_t}$ *to* $\mathcal{A}$*.*

Guess. $\mathcal{A}$ *outputs its guess* $b' \in \{0,1\}$ *for* b *and wins the game if* $b = b'$*.*

We define the advantage of $\mathcal{A}$ *as* $\mathsf{Adv}^{\mathsf{AH\text{-}OC}}_{\mathcal{A}}(\lambda) := \Pr[b = b'] - \frac{1}{2}$*. An F-PRE scheme is attribute-hiding for original ciphertexts if all polynomial time adversaries have at most negligible advantage in the above game. For each run of the game, we define three types of variables* $s_{\mathsf{m}}, s_{\mathsf{rk},\ell}, s_{\mathsf{renc},t}$ *(*$\ell = 1, \ldots, \nu_2, t = 1, \ldots, \nu_3$*) as follows:*

- *For challenge plaintexts* $m^{(0)}$ *and* $m^{(1)}$*,* $s_{\mathsf{m}} := 0$ *if* $m^{(0)} \neq m^{(1)}$ *and* $s_{\mathsf{m}} := 1$*, otherwise.*
- *For the* ℓ*-th re-encryption key query* (v_ℓ, x'_ℓ) *and challenge* $(m^{(0)}, x^{(0)})$ *and* $(m^{(1)}, x^{(1)})$*,* $s_{\mathsf{rk},\ell} := 0$ *if* $m^{(0)} \bullet R(v_\ell, x^{(0)}) \neq m^{(1)} \bullet R(v_\ell, x^{(1)})$ *and* $s_{\mathsf{rk},\ell} := 1$ *otherwise.*
- *For the* t*-th re-encryption query* $(v_t, x'_t, \mathsf{oct}_t)$ *and challenge* $(m^{(0)}, x^{(0)})$ *and* $(m^{(1)}, x^{(1)})$*,* $s_{\mathsf{renc},t} := 0$ *if* $\mathsf{oct}_t = \mathsf{oct}_{x^{(b)}} \wedge m^{(0)} \bullet R(v_t, x^{(0)}) \neq m^{(1)} \bullet R(v_t, x^{(1)})$*,* $s_{\mathsf{renc},t} := 1$ *if* $\mathsf{oct}_t = \mathsf{oct}_{x^{(b)}} \wedge m^{(0)} \bullet R(v_t, x^{(0)}) = m^{(1)} \bullet R(v_t, x^{(1)})$*, and* $s_{\mathsf{renc},t} := 2$ *if* $\mathsf{oct}_t \neq \mathsf{oct}_{x^{(b)}}$

The above variables, $s_{\mathsf{m}}, s_{\mathsf{rk},\ell}, s_{\mathsf{renc},t}$*, are used for defining cases in the proof of Theorem 2 in Appendix D.3.*

Definition 6 (Predicate- and Attribute-Hiding for Re-Encrypted Ciphertexts (PAH-RC)). *The model for defining the (adaptively) predicate- and attribute-hiding security for re-encrypted ciphertexts of F-PRE against adversary* $\mathcal{A}$ *(under chosen plaintext attacks) is given by the following game:*

Setup, Phase 1. *They are defined as the same as those in Definition 5, respectively.*

Challenge. *For a challenge query* $(m^{(0)}, m^{(1)}, x^{(0)}, x^{(1)}, v^{(0)}, v^{(1)}, x'^{(0)}, x'^{(1)})$ *subjected to the following restrictions:*

– $(m^{(0)}, x^{(0)}, v^{(0)}) \bullet R(v', x'^{(0)}) = (m^{(1)}, x^{(1)}, v^{(1)}) \bullet R(v', x'^{(1)})$ *for any decryption key query* v'.

The challenger flips a random bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ *and gives* $\mathsf{rct}_{x'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v^{(b)}), x'^{(b)}), \mathsf{Enc}(\mathsf{pk}, x^{(b)}, m^{(b)}))$. *Then it gives* $\mathsf{rct}_{x'^{(b)}}$ *to* $\mathcal{A}$.

Phase 2. *The adversary* $\mathcal{A}$ *may continue to issue decryption key queries, re-encryption key queries and re-encryption queries, subjected to the restriction in challenge phase.*

Guess. $\mathcal{A}$ *outputs its guess* $b' \in \{0,1\}$ *for* b *and wins the game if* $b = b'$.

We define the advantage of $\mathcal{A}$ *as* $\mathsf{Adv}^{\mathsf{PAH\text{-}RC}}_{\mathcal{A}}(\lambda) := \Pr[b = b'] - \frac{1}{2}$. *An F-PRE scheme is predicate- and attribute-hiding for re-encrypted ciphertexts if all polynomial time adversaries have at most negligible advantage in the above game. For each run of the game, the variable* $s_{\mathsf{m,x,v}}$ *is defined as* $s_{\mathsf{m,x,v}} := 0$ *if* $(m^{(0)}, x^{(0)}, v^{(0)}) \neq (m^{(1)}, x^{(1)}, v^{(1)})$ *for challenge* $(m^{(\iota)}, x^{(\iota)}, v^{(\iota)})$ *for* $\iota = 0, 1$, *and* $s_{\mathsf{m,x,v}} := 1$, *otherwise. The above variable,* $s_{\mathsf{m,x,v}}$, *is used for defining cases in the proof of Theorem 3 in Appendix D.4.*

Definition 7 (Predicate- and Attribute-Hiding for Re-Encryption Keys (PAH-RK)). *The model for defining the (adaptively) predicate- and attribute-hiding security for re-encryption keys of F-PRE against adversary* $\mathcal{A}$ *(under chosen plaintext attacks) is given by the following game:*

Setup, Phase 1. *They are defined as the same as those in Definition 5, respectively.*

Challenge. *For a challenge query* $(v^{(0)}, v^{(1)}, x'^{(0)}, x'^{(1)})$, *subject to the following restrictions:*

– $v^{(0)} \bullet R(v', x'^{(0)}) = v^{(1)} \bullet R(v', x'^{(1)})$ *for any decryption key query* v'.

The challenger flips a random bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ *and computes* $\mathsf{rk}_{v^{(b)}, x'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v^{(b)}), x'^{(b)})$. *Then it gives* $\mathsf{rk}_{v^{(b)}, x'^{(b)}}$ *to* $\mathcal{A}$.

Phase 2. *The adversary* $\mathcal{A}$ *may continue to issue decryption key queries, re-encryption key queries and re-encryption queries, subjected to the restriction in challenge phase.*

Guess. $\mathcal{A}$ *outputs its guess* $b' \in \{0,1\}$ *for* b *and wins the game if* $b = b'$.

We define the advantage of $\mathcal{A}$ *as* $\mathsf{Adv}^{\mathsf{PAH\text{-}RK}}_{\mathcal{A}}(\lambda) := \Pr[b = b'] - \frac{1}{2}$. *An F-PRE scheme is predicate- and attribute-hiding for re-encryption keys if all polynomial time adversaries have at most negligible advantage in the above game. For each run of the game, the variable* s_{v} *is defined as* $s_{\mathsf{v}} := 0$ *if* $v^{(0)} \neq v^{(1)}$ *for challenge predicates, and* $s_{\mathsf{v}} := 1$ *otherwise. The above variable* s_{v} *is used for defining cases in the proof of Theorem 4 in Appendix D.5.*

Definition 8 (Unlinkability). *An F-PRE scheme is unlinkable if the following two conditions hold:*

(Unconditional) Unlinkability of Re-encryption Keys *for all* $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n)$, *all predicates* v, *all attributes* x', *distributions* $(\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v),\ \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_v, x'))$ *and* $(\mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v),\ \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v), x'))$ *are equivalent except for negligible probability.*

(Computational) Unlinkability of Re-encrypted Ciphertexts *Any probabilistic polynomial-time adversary* $\mathcal{A}$ *has negligible success probability in the following game: The guessing game is defined between an adversary* $\mathcal{A}$ *and a challenger as in Definitions 5–7, and* **Setup, Phase 1, Guess** *phases are the same as those in the definitions. In* **Challenge** *phase,* $\mathcal{A}$ *submits a predicate* v, *attributes* x, x', *and a message* m, *where* $R(v', x') = 0$ *for any decryption key query* v' *in* **Phase 1**. *The challenger then calculates* $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v)$, *flips a coin* $b \xleftarrow{\mathsf{U}} \{0,1\}$, *and gives* $(\mathsf{rk}_{v,x'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_v, x'),\ \mathsf{oct}_x \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, x, m),\ \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{v,x'}, \mathsf{oct}_x))$ *if* $b = 0$, $(\mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_v, x'),\ \mathsf{Enc}(\mathsf{pk}, x, m),\ \mathsf{REnc}(\mathsf{pk}, \mathsf{RKG}(\mathsf{pk},\ \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, v), x'), \mathsf{Enc}(\mathsf{pk}, x, m))$ *if* $b = 1$, *to* $\mathcal{A}$. *(*$\mathcal{A}$ *outputs a guessed bit* b' *in* Guess *phase.) Here,* $\mathcal{A}$ *can ask the challenger to obtain any decryption key, re-encryption key, re-encrypted ciphertext in* **Phase 1** *and* **Phase 2** *under the condition that no decryption key query* v' *matches the challenge* x', *i.e.,* $R(v', x') = 0$.

4 Proposed Inner-Product Proxy-Re-Encryption (IP-PRE) Schemes

A special form of F-PRE formulated in Section 3 is IP-PRE, where decryption key parameter (predicate) v and ciphertext parameter (attribute) x are given by n-dimensional vectors over $\mathbb{F}_q$, i.e., $\vec{v}$ and $\vec{x}$, and $R(\vec{v},\vec{x})=1$ iff $\vec{v}\cdot\vec{x}=0$. We normalize that $x_1=1$ and $v_n=1$ for $\vec{x}:=(x_i)_n^{i=1}$ and $\vec{v}:=(v_i)_n^{i=1}$. In Section 4.1, we describe our basic IP-PRE scheme. Based on it, we propose a *fully-anonymous* IP-PRE scheme in Section 4.2. We describe ingredients used for both schemes below.

A Strongly Unforgeable One-Time Signature Scheme. Since the CHK transform is crucial for our schemes as is described in Section 1.3, we use a strongly unforgeable one-time signature scheme. Refer to Appendix B.1 for the details. For simplicity, we assume verification key verk is an element in $\mathbb{F}_q$. (We can extend the construction to verification key over any distribution D by first hashing verk using a collision resistant hash $H:\mathsf{D}\to\mathbb{F}_q$.)

Underlying IPE Schemes. We use a payload-hiding IPE scheme in our basic scheme, and a fully attribute-hiding (FAH) IPE scheme in our fully anonymous scheme, whose message space is a matrix space $\mathbb{F}_q^{N\times N}$ ($N:=3n+4, 4n+4$, respectively). In addition, we tweak the FAH-IPE for our purpose: An ordinary FAH-IPE scheme consists of four algorithms, $(\mathsf{Setup}_{\mathsf{IPE}},\mathsf{KG}_{\mathsf{IPE}},\mathsf{Enc}_{\mathsf{IPE}},\mathsf{Dec}_{\mathsf{IPE}})$. $\mathsf{Enc}_{\mathsf{IPE}}$ of a tweaked version is composed of two algorithms, $\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}$ and $\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}$, where $\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}$ encrypts only attribute vector $\vec{x}$ and outputs $\mathsf{prect}_{\vec{x}}$, and $\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}$ takes as input $\mathsf{prect}_{\vec{x}}$ and plaintext m and outputs $\mathsf{ct}_{\vec{x}}$ of m. Moreover, we add a re-randomization algorithm for ciphertexts, $\mathsf{RR}_{\mathsf{IPE}}$. Namely, it consists of seven algorithms, $(\mathsf{Setup}_{\mathsf{IPE}},\mathsf{KG}_{\mathsf{IPE}},\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}},\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}},\mathsf{Enc}_{\mathsf{IPE}},\mathsf{RR}_{\mathsf{IPE}},\mathsf{Dec}_{\mathsf{IPE}})$. Refer to Appendix B.2 for the details.

Random Dual Orthonormal Basis Generator. We describe random dual orthonormal basis generator $\mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}$ below, which is used as a subroutine in the proposed schemes.

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

4.1 Basic IP-PRE Scheme

We describe a construction idea of our basic IP-PRE for our full IP-PRE (in Section 4.2). For the formal description of the basic IP-PRE scheme and its security, refer to Appendix C.

Setup generates a key pair for the underlying IPE, $(\mathsf{pk}^{\mathsf{IPE}},\mathsf{sk}^{\mathsf{IPE}})$, and a dual basis pair, $(\mathbb{B},\mathbb{B}^*)$, of a $(3n+4)$-dimensional vector space. The master secret key sk is $(\boldsymbol{b}^*_0,\ \mathsf{sk}^{\mathsf{IPE}})$, and public key pk is $(\widehat{\mathbb{B}},\widehat{\mathbb{B}}^*)$, where $\widehat{\mathbb{B}}:=(\boldsymbol{b}_0,..,\boldsymbol{b}_{n+2},\boldsymbol{b}_{3n+3}),\widehat{\mathbb{B}}^*:=(\boldsymbol{b}^*_1,..,\boldsymbol{b}^*_{n+2},\boldsymbol{b}^*_{2n+2},..,\boldsymbol{b}^*_{3n+2})$. The first dimension is used for decryption, the next n-dimension for embedding $\vec{x}$ and $\vec{v}$, the next 2-dimension for CHK mechanism, the next n-dimension for security proof (hidden subspace), the rest for randomization.

KG takes $(\mathsf{pk},\mathsf{sk},\vec{v})$ as input, and generates $\boldsymbol{k}^*:=(\ 1,\ \delta\vec{v},\ 0^2,\ 0^n,\ \vec{\eta},\ 0)_{\mathbb{B}^*},\ \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}}\xleftarrow{\mathsf{R}}\mathsf{KG}^{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}},\mathsf{sk}^{\mathsf{IPE}},\vec{v})$, where $\delta\xleftarrow{\mathsf{U}}\mathbb{F}_q$, $\vec{\eta}\xleftarrow{\mathsf{U}}\mathbb{F}_q^n$, and returns $\mathsf{sk}_{\vec{v}}:=(\vec{v},\boldsymbol{k}^*,\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$.

Enc takes $(\mathsf{pk},\vec{x},m)$ as input, and generates $(\mathsf{sigk},\mathsf{verk})\xleftarrow{\mathsf{R}}\mathsf{SigKG}(1^\lambda)$, $\zeta,\omega,\rho,\varphi\xleftarrow{\mathsf{U}}\mathbb{F}_q$, and $\boldsymbol{c}:=(\ \zeta,\ \omega\vec{x},\ \rho(\mathsf{verk},1),\ \ 0^n,\ 0^n,\ \varphi)_{\mathbb{B}},\ c_T:=m\cdot g_T^\zeta,\ S\xleftarrow{\mathsf{R}}\mathsf{Sig}(\mathsf{sigk},C)$, where $C:=(\vec{x},\boldsymbol{c},c_T)$, and returns $\mathsf{oct}_{\vec{x}}:=(C,\mathsf{verk},S)$, i.e., a CHK converted ciphertext.

RKG takes $(\mathsf{pk},\mathsf{sk}_{\vec{v}},\vec{x}')$ as input, and generates $W_1\xleftarrow{\mathsf{U}}GL(3n+4,\mathbb{F}_q)$, $\boldsymbol{k}^{*\mathsf{rk}}:=(\boldsymbol{k}^*+(\ 0,\ \delta'\vec{v},\ 0^2,\ 0^n,\ \vec{\eta}\,',\ 0)_{\mathbb{B}^*})W_1,\ \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}\xleftarrow{\mathsf{R}}\mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}},\vec{x}',W_1)$, where $\delta'\xleftarrow{\mathsf{U}}\mathbb{F}_q,\vec{\eta}\,'\xleftarrow{\mathsf{U}}\mathbb{F}_q^n$, and $\widehat{\mathbb{D}}^*_1:=(\boldsymbol{d}^*_i:=\boldsymbol{b}^*_iW_1)_{i=1,\ldots,n+2,2n+2,\ldots,3n+3}$, and returns $\mathsf{rk}_{\vec{v},\vec{x}'}:=(\vec{v},\vec{x}',\boldsymbol{k}^{*\mathsf{rk}},\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'},\widehat{\mathbb{D}}^*_1)$. $\boldsymbol{k}^{*\mathsf{rk}}$ is

the product of (re-randomized) vector $\boldsymbol{k}^*$ by matrix W_1, and $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ is a ciphertext of W_1 with $\vec{x}'$. Here, $\boldsymbol{k}^{*\mathsf{rk}}$ is represented over basis $\mathbb{D}_1^* := (\boldsymbol{b}_i^* W_1)_{i=0,..,3n+3}$ as $\boldsymbol{k}^{*\mathsf{rk}} = (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ 0^n,\ \vec{\eta}^{\ \mathsf{rk}},\ 0)_{\mathbb{D}_1^*}$ where $\delta^{\mathsf{rk}}, \vec{\eta}^{\ \mathsf{rk}}$ are freshly random variables.

REnc takes $(\mathsf{pk}, \mathsf{rk}_{\vec{v},\vec{x}'} := (\vec{v}, \vec{x}', \boldsymbol{k}^{*\mathsf{rk}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \widehat{\mathbb{D}}_1^*), \mathsf{oct}_{\vec{x}} := (C := (\vec{x}, \boldsymbol{c}, c_T), \mathsf{verk}, S))$ as input, and first verify that $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$, and if so, generates $W_2 \xleftarrow{\mathsf{U}} GL(3n+4, \mathbb{F}_q)$ and $\boldsymbol{k}^{*\mathsf{renc}} := \boldsymbol{k}^{*\mathsf{rk}} + (\ 0,\ \delta''\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \vec{\eta}\,'',\ 0)_{\mathbb{D}_1^*}$, $\boldsymbol{c}^{\mathsf{renc}} := (\boldsymbol{c} + (\ \zeta', \omega'\vec{x}, \rho'(\mathsf{verk}, 1), 0^n, 0^n, \varphi')_{\mathbb{B}})W_2$, $c_T^{\mathsf{renc}} := c_T \cdot g_T^{\zeta'}$, $\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{RR}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'})$, $\mathsf{ct}^{\mathsf{renc}}_{2,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', W_2)$, where $\delta'', \sigma, \zeta', \omega', \rho', \varphi' \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}\,'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, and returns $\mathsf{rct}_{\vec{x}'} := (\vec{x}', \boldsymbol{c}^{\mathsf{renc}}, c_T^{\mathsf{renc}}, \boldsymbol{k}^{*\mathsf{renc}}, \{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2})$.

$\boldsymbol{k}^{*\mathsf{renc}}$ is obtained by converted from $\boldsymbol{k}^{*\mathsf{rk}}$ by embedding a CHK tag part $\sigma(-1, \mathsf{verk})$, then, is specialized for decrypting $\boldsymbol{c}^{\mathsf{renc}}$ only. $(\boldsymbol{c}^{\mathsf{renc}}, c_T^{\mathsf{renc}})$ are the products of (re-randomized) $(\boldsymbol{c}, c_T)$ by W_2, respectively, and $\{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2}$ are fresh ciphertexts of W_1 and W_2, respectively, with $\vec{x}'$. Here, $\boldsymbol{k}^{*\mathsf{renc}}$ is represented over basis $\mathbb{D}_1^*$ as $\boldsymbol{k}^{*\mathsf{renc}} = (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{D}_1^*}$, where $\delta^{\mathsf{renc}}, \vec{\eta}^{\ \mathsf{renc}}$ are freshly random, $\boldsymbol{c}^{\mathsf{renc}}$ and c_T^{renc} are represented over basis $\mathbb{D}_2 := (\boldsymbol{b}_i W_2)_{i=0,..,3n+3}$ as $\boldsymbol{c}^{\mathsf{renc}} = (\ \zeta^{\mathsf{renc}},\ \omega^{\mathsf{renc}}\vec{x},\ \rho^{\mathsf{renc}}(\mathsf{verk}, 1),\ 0^n,\ 0^n,\ \varphi^{\mathsf{renc}})_{\mathbb{D}_2}$ and $c_T^{\mathsf{renc}} := m \cdot g_T^{\zeta^{\mathsf{renc}}}$ where $\zeta^{\mathsf{renc}}, \omega^{\mathsf{renc}}, \varphi^{\mathsf{renc}}$ are freshly random.

$\mathsf{Dec}_{\mathsf{oct}}$ takes $(\mathsf{pk}, \mathsf{sk}_{\vec{v}} := (\vec{v}, \boldsymbol{k}^*, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}}), \mathsf{oct}_{\vec{x}} := (C := (\vec{x}, \boldsymbol{c}, c_T), \mathsf{verk}, S))$ as input, and first verify that $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$, and if so, calculates $K := e(\boldsymbol{c}, \boldsymbol{k}^*)$, and returns $\widetilde{m} := c_T / K$.

$\mathsf{Dec}_{\mathsf{rct}}$ takes $(\mathsf{pk}, \mathsf{sk}_{\vec{v}'} := (\vec{v}', \boldsymbol{k}^*, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}'}), \mathsf{rct}_{\vec{x}'} := (\vec{x}', \boldsymbol{c}^{\mathsf{renc}}, c_T^{\mathsf{renc}}, \boldsymbol{k}^{*\mathsf{renc}}, \{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2}))$ as input, and calculates $\widetilde{W}_i \xleftarrow{\mathsf{R}} \mathsf{Dec}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}'}, \mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'})$ for $i = 1, 2$, $\widetilde{K} := e(\boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1}, \boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1})$, and returns $\widetilde{m} := c_T^{\mathsf{renc}} / \widetilde{K}$. Here, $(\boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1}, \boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1})$ are represented over bases $(\mathbb{B}, \mathbb{B}^*)$ as $\boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1} = (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{B}^*}$ and $\boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1} = (\ \zeta^{\mathsf{renc}},\ \omega^{\mathsf{renc}}\vec{x},\ \rho^{\mathsf{renc}}(\mathsf{verk}, 1),\ 0^n,\ 0^n,\ \varphi^{\mathsf{renc}})_{\mathbb{B}}$.

4.2 Fully-Anonymous IP-PRE Scheme

The basic IP-PRE scheme does not have predicate- and attribute-hiding security for re-encryption keys because a predicate vector $\vec{v}$ and an attribute vector $\vec{x}'$ are included in re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'}$. $\vec{v}$ is needed to re-randomize $\boldsymbol{k}^{*\mathsf{rk}}$ and $\vec{x}'$ is needed to generate a ciphertext $\mathsf{ct}^{\mathsf{renc}}_{1.\vec{x}'}$ in REnc algorithm. In order to construct IP-PRE scheme with the predicate- and attribute-hiding for $\mathsf{rk}_{\vec{v},\vec{x}'}$, we modify the basic IP-PRE scheme as follows: In order to remove $\vec{v}$ from $\mathsf{rk}_{\vec{v},\vec{x}'}$ and re-randomize $\boldsymbol{k}^{*\mathsf{rk}}$ in REnc, RKG also outputs $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ which is generated on the basis $\mathbb{D}_1^* = \mathbb{B}^* W_1$ (instead of the vector $\vec{v}$). Then, the predicate vector $\vec{v}$ is embedded into $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ *in a hidden form* from an adversary who cannot decrypt $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ i.e., cannot obtain W_1. Similarly, in order to remove $\vec{x}'$ from $\mathsf{rk}_{\vec{v},\vec{x}'}$, RKG also outputs a pre-ciphertext $\mathsf{prect}_{\vec{x}'}$ instead of the attribute vector $\vec{x}'$. From the attribute-hiding security of the underlying IPE scheme, the vector $\vec{x}'$ is hidden from the adversary. In a similar manner, for attribute-hiding for original ciphertexts, Enc also outputs $\boldsymbol{c}_{\mathsf{ran}}$ instead of an attribute vector $\vec{x}$ which is included into $\mathsf{oct}_{\vec{x}}$. REnc re-randomizes $\boldsymbol{c}$ by using $\boldsymbol{c}_{\mathsf{ran}}$ (instead of using $\vec{x}$). Our fully anonymous IPE scheme is obtained by modifying our basic scheme as below including the above modifications.

1. The dimension of the vector space for $(\mathbb{B}, \mathbb{B}^*)$ is enlarged to $4n + 4$.
2. An underlying IPE scheme is fully attribute-hiding.
3. $\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*$ are included into sk as well as $\boldsymbol{b}_0^*$.
4. For re-randomization in RKG, an additional $\boldsymbol{k}^*_{\mathsf{ran}}$ is included into decryption key $\mathsf{sk}_{\vec{v}}$ as well as $\boldsymbol{k}^*$.
5. For re-randomization in REnc, an additional $\boldsymbol{c}_{\mathsf{ran}}$ (resp. $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$) is included into original ciphertext $\mathsf{oct}_{\vec{x}}$ as well as $\boldsymbol{c}$ (resp. re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'}$ as well as $\boldsymbol{k}^{*\mathsf{rk}}$). Moreover, $\mathsf{prect}_{\vec{x}'}$ is included into $\mathsf{rk}_{\vec{v},\vec{x}'}$.

We give our fully-anonymous IP-PRE scheme below.

$\mathsf{Setup}(1^\lambda, n)$**:** $(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$,
$(\mathsf{param}_n, \mathbb{B} = (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{4n+3}), \mathbb{B}^* = (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_{4n+3})) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4)$,
$\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n+2}, \boldsymbol{b}_{4n+3})$, $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_{n+1}, \boldsymbol{b}^*_{n+2}, \boldsymbol{b}^*_{3n+3}, \ldots, \boldsymbol{b}^*_{4n+2})$,
return $\mathsf{pk} := (1^\lambda, \mathsf{pk}^{\mathsf{IPE}}, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$, $\mathsf{sk} := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n\ \mathsf{sk}^{\mathsf{IPE}})$.

$\mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \vec{v})$**:** $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}^{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}, \vec{v})$, $\delta, \delta_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}, \vec{\eta}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$,
$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ 0^{2n},\ \vec{\eta},\ 0)_{\mathbb{B}^*}$, $\boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ 0^{2n},\ \vec{\eta}_{\mathsf{ran}},\ 0)_{\mathbb{B}^*}$,
return $\mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$.

$\mathsf{Enc}(\mathsf{pk}, \vec{x}, m)$**:** $\zeta, \omega, \omega_{\mathsf{ran}}, \rho, \rho_{\mathsf{ran}}, \varphi, \varphi_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $(\mathsf{sigk}, \mathsf{verk}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$,
$\boldsymbol{c} := (\ \zeta,\ \omega\vec{x},\ \rho(\mathsf{verk}, 1),\ 0^{2n},\ 0^n,\ \varphi)_{\mathbb{B}}$, $\boldsymbol{c}_{\mathsf{ran}} := (\ 0,\ \omega_{\mathsf{ran}}\vec{x},\ \rho_{\mathsf{ran}}(\mathsf{verk}, 1),\ 0^{2n},\ 0^n,\ \varphi_{\mathsf{ran}})_{\mathbb{B}}$,
$c_T := m \cdot g_T^{\zeta}$, $C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T)$, $S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}, C)$, return $\mathsf{oct}_{\vec{x}} := (C, \mathsf{verk}, S)$.

$\mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \vec{x}')$**:** $r, r_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}', \vec{\eta}'_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$,
$W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$, $\widehat{\mathbb{D}}^*_1 := (\boldsymbol{d}^*_i := \boldsymbol{b}^*_i W_1)_{i=n+1,n+2,3n+3,\ldots,4n+2}$,
$\boldsymbol{k}^{*\mathsf{rk}} := (\boldsymbol{k}^* + r\boldsymbol{k}^*_{\mathsf{ran}} + (\ 0,\ 0^n,\ 0^2,\ 0^{2n},\ \vec{\eta}',\ 0)_{\mathbb{B}^*}))W_1$,
$\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (r_{\mathsf{ran}}\boldsymbol{k}^*_{\mathsf{ran}} + (\ 0,\ 0^n,\ 0^2,\ 0^{2n},\ \vec{\eta}'_{\mathsf{ran}},\ 0)_{\mathbb{B}^*})W_1$,
$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', W_1)$, $\mathsf{prect}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}')$,
return $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1)$.

$\mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1), \mathsf{oct}_{\vec{x}} := (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}, S))$**:**
If $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, return $\perp$.
$r', \sigma, \zeta', \xi, \rho', \varphi' \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}\,'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $W_2 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$
$\boldsymbol{k}^{*\mathsf{renc}} := \boldsymbol{k}^{*\mathsf{rk}} + r'\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} + (\ 0,\ 0^n,\ \sigma(-1, \mathsf{verk}),\ 0^{2n},\ \vec{\eta}\,'',\ 0)_{\mathbb{D}^*_1}$,
$\boldsymbol{c}^{\mathsf{renc}} := (\boldsymbol{c} + \xi\boldsymbol{c}_{\mathsf{ran}} + (\ \zeta',\ 0^n,\ \rho'(\mathsf{verk}, 1),\ 0^{2n},\ 0^n,\ \varphi')_{\mathbb{B}})W_2$, $c^{\mathsf{renc}}_T := c_T \cdot g_T^{\zeta'}$,
$\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{RR}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'})$, $\mathsf{ct}^{\mathsf{renc}}_{2,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{prect}_{\vec{x}'}, W_2)$,
return $\mathsf{rct}_{\vec{x}'} := (\boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \boldsymbol{k}^{*\mathsf{renc}}, \{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2})$.

$\mathsf{Dec}_{\mathsf{oct}}(\mathsf{pk}, \mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}}), \mathsf{oct}_{\vec{x}} := (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}, S))$**:**
If $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, return $\perp$, $K := e(\boldsymbol{c}, \boldsymbol{k}^*)$, return $\widetilde{m} := c_T/K$.

$\mathsf{Dec}_{\mathsf{rct}}(\mathsf{pk}, \mathsf{sk}_{\vec{v}'} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}'}), \mathsf{rct}_{\vec{x}'} := (\boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \boldsymbol{k}^{*\mathsf{renc}}, \{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2}))$**:**
$\widetilde{W}_i \xleftarrow{\mathsf{R}} \mathsf{Dec}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}'}, \mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'})$ for $i = 1, 2$, $\widetilde{K} := e(\boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1}, \boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1})$, return $\widetilde{m} := c^{\mathsf{renc}}_T/\widetilde{K}$.

Remark 1 (Representations of $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$ and $(\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T)$).

1. Since components $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ in a re-encryption key are generated from $\boldsymbol{k}^*$ and $\boldsymbol{k}^*_{\mathsf{ran}}$ in a decryption key, we show $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ are uniformly and independently distributed from the decryption key components. $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ are represented over basis $\mathbb{D}^*_1 := (\boldsymbol{b}^*_i W_1)_{i=0,..,4n+3}$ as $\boldsymbol{k}^{*\mathsf{rk}} = (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ 0^{2n},\ \vec{\eta}^{\,\mathsf{rk}},\ 0)_{\mathbb{D}^*_1}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} = (\ 0,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ 0^{2n},\ \vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}},\ 0)_{\mathbb{D}^*_1}$ with $\delta^{\mathsf{rk}} := \delta + r\delta_{\mathsf{ran}}$, $\delta^{\mathsf{rk}}_{\mathsf{ran}} := r_{\mathsf{ran}}\delta_{\mathsf{ran}}$, $\vec{\eta}^{\,\mathsf{rk}} := \vec{\eta} + r\vec{\eta}_{\mathsf{ran}} + \vec{\eta}\,'$, and $\vec{\eta}_1{}^{\mathsf{rk}} := r_{\mathsf{ran}}\vec{\eta}_1 + \vec{\eta}\,'_{\mathsf{ran}}$ which are uniformly and independently distributed from $\mathsf{sk}_{\vec{v}}$ except when $\delta_{\mathsf{ran}} = 0$, i.e., except for probability $1/q$ since $r, r_{\mathsf{ran}}, \vec{\eta}\,', \vec{\eta}\,'_{\mathsf{ran}}$ are uniformly and independently distributed.
2. Components $\boldsymbol{k}^{*\mathsf{renc}}$ and $(\boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T)$ in a re-encrypted ciphertext are generated from $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$ in a re-encryption key and $(\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T)$ in a ciphertext, respectively. Hence, $\boldsymbol{k}^{*\mathsf{renc}}$ is represented over basis $\mathbb{D}^*_1$ as $\boldsymbol{k}^{*\mathsf{renc}} = (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^{2n},\ \vec{\eta}^{\,\mathsf{renc}},\ 0)_{\mathbb{D}^*_1}$ with $\delta^{\mathsf{renc}} := \delta^{\mathsf{rk}} + r'\delta^{\mathsf{rk}}_{\mathsf{ran}}$, $\vec{\eta}^{\,\mathsf{renc}} := \vec{\eta}^{\,\mathsf{rk}} + r'\vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}} + \vec{\eta}''$, which are uniformly and independently distributed from $\mathsf{rk}_{\vec{v},\vec{x}'}$ except when $\delta^{\mathsf{rk}}_{\mathsf{ran}} = 0$, i.e., except for probability $1/q$ since $r', \vec{\eta}''$ are uniformly and

independently distributed. $\boldsymbol{c}^{\mathsf{renc}}$ and c_T^{renc} are represented over basis $\mathbb{D}_2 := (\boldsymbol{b}_i W_2)_{i=0,..,4n+3}$ as $\boldsymbol{c}^{\mathsf{renc}} = (\ \zeta^{\mathsf{renc}},\ \omega^{\mathsf{renc}}\vec{x},\ \rho^{\mathsf{renc}}(\mathsf{verk}, 1),\ 0^{2n},\ 0^n,\ \varphi^{\mathsf{renc}})_{\mathbb{D}_2}$ and $c_T^{\mathsf{renc}} := m \cdot g_T^{\zeta^{\mathsf{renc}}}$ with $\zeta^{\mathsf{renc}} := \zeta + \zeta'$, $\omega^{\mathsf{renc}} := \omega + \xi\omega_{\mathsf{ran}}, \rho^{\mathsf{renc}} := \rho + \xi\rho_{\mathsf{ran}} + \rho', \varphi^{\mathsf{renc}} := \varphi + \xi\varphi_{\mathsf{ran}} + \varphi'$, which are uniformly and independently distributed from $\mathsf{oct}_{\vec{x}}$ except when $\omega_{\mathsf{ran}} = 0$, i.e., except for probability $1/q$ since $\zeta', \xi, \rho', \varphi'$ are uniformly and independently distributed.

[Correctness of $\mathsf{Dec}_{\mathsf{oct}}$] If $\vec{x} \cdot \vec{v} = 0$, $K = e(\boldsymbol{c}, \boldsymbol{k}^*) = g_T^{\zeta + \omega\delta\vec{x}\cdot\vec{v}} = g_T^{\zeta}$.

[Correctness of $\mathsf{Dec}_{\mathsf{rct}}$] $(\boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1}, \boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1})$ are represented over bases $(\mathbb{B}, \mathbb{B}^*)$ as $\boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1} = (\ 1,\ \delta^{\mathsf{renc}}\vec{v}, \sigma(-1, \mathsf{verk}),\ 0^{2n},\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{B}^*}$ and $\boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1} = (\ \zeta^{\mathsf{renc}},\ \omega^{\mathsf{renc}}\vec{x},\ \rho^{\mathsf{renc}}(\mathsf{verk}, 1),\ 0^{2n},\ 0^n,\ \varphi^{\mathsf{renc}})_{\mathbb{B}}$. Hence, if $\vec{x} \cdot \vec{v} = 0$, $\widetilde{K} = e(\boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1}, \boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1}) = g_T^{\zeta^{\mathsf{renc}} + \omega^{\mathsf{renc}}\delta^{\mathsf{renc}}\vec{x}\cdot\vec{v}} = g_T^{\zeta^{\mathsf{renc}}}$.

The DLIN assumption is given in Appendix A, and the OT12 IPE scheme is given in Definition 15 in Appendix B.2.

Theorem 1 (Main Theorem). *The proposed IP-PRE scheme is fully-anonymous under the DLIN assumption provided the underlying signature scheme is a strongly unforgeable one-time signature scheme and the underlying IPE scheme is given by the OT12 IPE scheme.*

Proof. From Corollary 1 (and Theorems 2–4) and Theorem 5, we obtain Theorem 1. □

The proofs of Theorems 2–5 are given in Appendices D.3–D.6 respectively. When the underlying IPE scheme is given by the OT12 IPE scheme, we have Corollary 1 below.

Theorem 2. *The proposed IP-PRE scheme is attribute-hiding for original ciphertexts against chosen plaintext attacks under the DLIN assumption provided the underlying signature scheme is a strongly unforgeable one-time signature scheme and the underlying IPE scheme is fully attribute-hiding.*

Theorem 3. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encrypted ciphertexts against chosen plaintext attacks provided the underlying IPE scheme is fully attribute-hiding.*

Theorem 4. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encryption keys against chosen plaintext attacks provided the underlying IPE scheme is fully attribute-hiding.*

Corollary 1 *The proposed IP-PRE scheme is attribute-hiding for original ciphertexts against chosen plaintext attacks under the DLIN assumption provided the underlying signature scheme is a strongly unforgeable one-time signature scheme and the underlying IPE scheme is given by the OT12 IPE scheme.*

It is predicate- and attribute-hiding for re-encrypted ciphertexts against chosen plaintext attacks under the DLIN assumption provided the underlying IPE scheme is given by the OT12 IPE scheme.

It is predicate- and attribute-hiding for re-encryption key against chosen plaintext attacks under the DLIN assumption provided the underlying IPE scheme is given by the OT12 IPE scheme.

Theorem 5. *The proposed IP-PRE scheme is unlinkable.*

5 Proposed Ciphertext Policy Functional Proxy-Re-Encryption (CP-F-PRE) Scheme

We propose a CP-F-PRE scheme with the access structure given by Okamoto-Takashima [27]. The scheme is payload-hiding for original ciphertexts, payload-hiding for re-encrypted ciphertexts, and attribute-hiding for re-encryption keys under the DLIN assumption and the existence of a strongly unforgeable one-time signature scheme (Corollary 3). In addition, the scheme is unlinkable (Theorem 11). For security definitions, the proposed scheme and its security theorems, refer to Appendix E.

References

1. G. Ateniese, K. Benson, and S. Hohenberger. Key-Private Proxy Re-encryption. In *Topics in Cryptology - CT-RSA 2009*, volume 5473 of *LNCS*, pages 279–294, 2009.
2. G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage. *ACM Trans. Inf. Syst. Secur.*, 9(1):1–30, 2006.
3. A. Beimel. Secure schemes for secret sharing and key distribution. *PhD Thesis, Israel Institute of Technology, Technion, Haifa*, 1996.
4. M. Blaze, G. Bleumer, and M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. In *Advances in Cryptology - EUROCRYPT'98*, volume 1403 of *LNCS*, pages 127–144, 1998.
5. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55, 2004.
6. D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC 2007*, pages 535–554, 2007.
7. R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In *Advances in Cryptology-Eurocrypt 2004*, volume 3027 of *LNCS*, pages 207–222, 2004.
8. R. Canetti and S. Hohenberger. Chosen-Ciphertext Secure Proxy Re-encryption. In *Proceedings of the 14th ACM conference on Computer and communications security - ACM CCS 2007*, pages 185–194, 2007.
9. S. Chow, J. Weng, Y. Yang, and R. Deng. Efficient Unidirectional Proxy Re-Encryption. In *Progress in Cryptology - AFRICACRYPT 2010*, volume 6055 of *LNCS*, pages 316–332, 2010.
10. C.-K. Chu, J. Weng, S. Chow, J. Zhou, and R. Deng. Conditional proxy broadcast re-encryption. In *Information Security and Privacy*, 2009.
11. K. Emura, A. Miyaji, and K. Omote. An Identity-Based Proxy Re-Encryption Scheme with Source Hiding Property, and its Application to a Mailing-List System. In *EuroPKI 2011*, volume 6711 of *LNCS*, pages 77–92, 2011.
12. M. Green and G. Ateniese. Identity-Based Proxy Re-encryption. In *Applied Cryptography and Network Security*, volume 4521 of *LNCS*, pages 288–306, 2007.
13. J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT 2008*, pages 146–162, 2008.
14. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91, 2010. Full version is available at http://eprint.iacr.org/2010/110.
15. A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In *TCC 2010*, pages 455–479, 2010.
16. A. B. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *CRYPTO 2012*, pages 180–198, 2012.
17. K. Li. Matrix Access structure Policy used in Attribute-Based Proxy Re-encryption. *International Journal of Computer Science Issues: IJCSI*, 9:119–127, 2012.
18. K. Liang, L. Fang, D. S. Wong, and W. Susilo. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. *IACR Cryptology ePrint Archive*, 2013:236, 2013.
19. X. Liang, Z. Cao, H. Lin, and J. Shao. Attribute based proxy re-encryption with delegating capabilities. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, ASIACCS '09, pages 276–286. ACM, 2009.
20. B. Libert and D. Vergnaud. Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption. In *Public Key Cryptography - PKC 2008*, volume 4939 of *LNCS*, pages 360–379, 2008.
21. Liming Fang and Willy Susilo and Chunpeng Ge and Jiandong Wang. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. *Theoretical Computer Science*, 462:39–58, 2012.
22. S. Luo, J. Hu, and Z. Chen. Ciphertext Policy Attribute-Based Proxy Re-encryption. In *Information and Communications Security - ICICS 2010*, LNCS, pages 401–415, 2010.
23. T. Matsuo. Proxy re-encryption systems for identity-based encryption. In *Pairing-Based Cryptography Pairing 2007*, volume 4575 of *LNCS*, pages 247–267, 2007.
24. T. Mizuno and H. Doi. Hybrid proxy re-encryption scheme for attribute-based encryption. In F. Bao, M. Yung, D. Lin, and J. Jing, editors, *Inscrypt*, volume 6151 of *Lecture Notes in Computer Science*, pages 288–302. Springer, 2009.
25. T. Okamoto and K. Takashima. Homomorphic encryption and signatures from vector decomposition. In *Pairing-Based Cryptography - Pairing 2008*, LNCS, pages 57–74, 2008.
26. T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In *Advances in Cryptology - ASIACRYPT 2009*, LNCS, pages 214–231, 2009.
27. T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208, 2010. Full version is available at http://eprint.iacr.org/2010/563.

28. T. Okamoto and K. Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In *Cryptology and Network Security - CANS 2011*, volume 7092 of *LNCS*, pages 138–159, 2011. Full version is available at http://eprint.iacr.org/2011/648.
29. T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In *Advances in Cryptology - Eurocrypt 2012*, volume 7237 of *LNCS*, pages 591–608, 2012. Full version is available at http://eprint.iacr.org/2011/543.
30. T. Okamoto and K. Takashima. Fully secure unbounded inner-product and attribute-based encryption. In *Advances in Cryptology - Asiacrypt 2012*, volume 7658 of *LNCS*, pages 349–366, 2012. Full version is available at http://eprint.iacr.org/2011/671.
31. A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473, 2005.
32. J. Shao. Anonymous id-based proxy re-encryption. In *ACISP*, pages 364–375, 2012.
33. J. Shao and Z. Cao. CCA-Secure Proxy Re-encryption without Pairings. In *Public Key Cryptography - PKC 2009*, volume 5443 of *LNCS*, pages 357–376, 2009.
34. J. Shao, Z. Cao, and P. Liu. CCA-Secure PRE Scheme without Random Oracles. Cryptology ePrint Archive, Report 2010/112, 2010. http://eprint.iacr.org/.
35. J. Shao and P. Liu. CCA-Secure PRE Scheme without Public Verifiability. Cryptology ePrint Archive, Report 2010/357, 2010. http://eprint.iacr.org/.
36. J. Shao, P. Liu, G. Wei, and Y. Ling. Anonymous proxy re-encryption. *Security and Communication Networks*, 5(5):439–449, 2012.
37. B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In *CRYPTO 2009*, pages 619–636, 2009.
38. J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai. Conditional proxy re-encryption secure against chosen-ciphertext attack,. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security - ASIACCS 2009*, pages 322–332. ACM, 2009.

A Decisional Linear (DLIN) Assumption

Definition 9 (DLIN: Decisional Linear Assumption [5]). *The DLIN problem is to guess* $\beta \in \{0,1\}$*, given* $(\mathsf{param}_{\mathbb{G}},\ G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$*, where* $\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$: $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \kappa, \delta, \xi, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, Y_0 := (\delta+\sigma)G, Y_1 \xleftarrow{\mathsf{U}} \mathbb{G}, \mathrm{return}\ (\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta)$*, for* $\beta \xleftarrow{\mathsf{U}} \{0,1\}$*. For a probabilistic machine* $\mathcal{E}$*, we define the advantage of* $\mathcal{E}$ *for the DLIN problem as:* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) := \left|\mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda)\right] - \mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)\right]\right|$*. The DLIN assumption is: For any probabilistic polynomial-time adversary* $\mathcal{E}$*, the advantage* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda)$ *is negligible in* λ*.*

B Building Blocks for the Proposed IP-PRE Schemes in Section 4

B.1 One-Time Signatures

Definition 10 (Signature Scheme). A signature scheme consists of the following three algorithms.

SigKG takes as input a security parameter 1^λ and outputs verification key verk and signing key sigk.
Sig takes as input a message m and a signing key sigk and outputs a signature S.
Ver takes as input a message m, a signature S, and a verification key sigk and outputs a boolean value $\mathsf{accept} = 1$ or $\mathsf{reject} = 0$

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

Definition 11 (Strong Unforgeability). For an adversary, we define $\mathsf{Adv}^{\mathsf{OS},\mathsf{SUF}}_{\mathcal{B}_4}(\lambda)$ to be the success probability in the following experiment for any security parameter λ. A signature scheme is a strongly unforgeable one-time signature scheme if the success probability of any polynomial-time adversary is negligible:

1. The challenger runs $(\mathsf{verk}, \mathsf{sigk}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$ and gives verk to the adversary.
2. The adversary makes signing query on a message m and receives $S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}, m)$ at most ones. We denote the pair of message and signature (m, S) if the sining oracle is queried.
3. At the end, the adversary outputs (m', S').

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

B.2 Underlying Fully Attribute-Hiding IPE

We tweak a usual fully attribute-hiding IPE to be used in our fully-anonymous IP-PRE.

In this subsection, we propose new concept of an IPE scheme. We define relation $R(\vec{v}, \vec{x}) = 1$ if and only if $\vec{v} \cdot \vec{x} = 0$. In ordinarily IPE scheme, there are four algorithms $(\mathsf{Setup}_{\mathsf{IPE}}, \mathsf{KG}_{\mathsf{IPE}}, \mathsf{Enc}_{\mathsf{IPE}}, \mathsf{Dec}_{\mathsf{IPE}})$. In order to construct secure IP-PRE scheme, we introduce new algorithms $\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}$ and $\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}$ to IPE scheme. Roughly speaking, $\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}$ encrypts only attribute vector $\vec{x}$ and $\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}$ encrypts only plaintext m by deriving attribute $\vec{x}$ from $\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}$ whereas Enc encrypts both an attribute and a plaintext. We consider IPE scheme that message space is matrix space $\mathbb{F}_q^{N \times N}$. That is, $\mathsf{Enc}_{\mathsf{IPE}}$ is a sequential composition of $\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}$ and $\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}$, which takes as input an attribute $\vec{x}$ and a plaintext $X \in \mathbb{F}_q^{N \times N}$, respectively.

Definition 12. *An inner-product encryption scheme consists of the following seven algorithms.*

$\mathsf{Setup}_{\mathsf{IPE}}$**:** *takes as input a security parameter* 1^λ *and a positive integer* n *outputs public key* pk *and (master) secret key* sk*.*

$\mathsf{KG}_{\mathsf{IPE}}$**:** *takes as input a public key* pk*, a (master) secret key* sk*, and a predicate vector* $\vec{v}$*. It outputs a corresponding decryption key* $\mathsf{sk}_{\vec{v}}$*.*

$\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}$**:** *takes as input a public key* pk *and an attribute vector* $\vec{x}$*. It outputs a pre-ciphertext* $\mathsf{prect}_{\vec{x}}$*.*

$\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}$**:** *takes as input a public key* pk*, a pre-ciphertext* $\mathsf{prect}_{\vec{x}}$*, a plaintext* $X \in \mathbb{F}_q^{N \times N}$ *in some associated plaintext space. It outputs a ciphertext* $\mathsf{ct}_{\vec{x}}$*.*

$\mathsf{Enc}_{\mathsf{IPE}}$**:** *takes as input a public key* pk*, a plaintext* $X \in \mathbb{F}_q^{N \times N}$ *in some associated plaintext space, and an attribute vector* $\vec{x}$*. It outputs a ciphertext* $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}), X)$*.*

$\mathsf{RR}_{\mathsf{IPE}}$**:** *takes as input a public key* pk*, a ciphertext* $\mathsf{ct}_{\vec{x}}$*. It outputs a (re-randomized) ciphertext* $\widetilde{\mathsf{ct}}_{\vec{x}}$*.*

$\mathsf{Dec}_{\mathsf{IPE}}$**:** *takes as input a public key* pk*, a decryption key* $\mathsf{sk}_{\vec{v}}$*, and an original ciphertext* $\mathsf{ct}_{\vec{x}}$*. It outputs either plaintext* $X \in \mathbb{F}_q^{N \times N}$ *or the distinguished symbol* $\perp$*.*

We require the correctnesses for an IPE scheme: (1) For any plaintext $X \in \mathbb{F}_q^{N \times N}$, any $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(\lambda)$, any $\vec{v}$ and $\vec{x}$, any decryption key $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{sk}, \vec{v})$, and any ciphertext $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}, X, \vec{x})$, we have $m = \mathsf{Dec}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \mathsf{ct}_{\vec{x}})$ if $R(\vec{v}, \vec{x}) = 1$. Otherwise it holds with negligible probability. (2) For any plaintext m, any $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(\lambda)$, any $\vec{v}$ and $\vec{x}$, any decryption key $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{sk}, \vec{v})$, any pre-ciphertext $\mathsf{prect}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x})$ and any ciphertext $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{prect}_{\vec{x}}, X)$, we have $m = \mathsf{Dec}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \mathsf{ct}_{\vec{x}})$ if $R(\vec{v}, \vec{x}) = 1$. Otherwise it holds with negligible probability. The above two conditions also hold for a re-randomized $\widetilde{\mathsf{ct}}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{RR}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{ct}_{\vec{x}})$ instead of an ordinary ciphertext $\mathsf{ct}_{\vec{x}}$.

We then define fully attribute-hiding security of IPE scheme.

Definition 13 (Attribute-Hiding Security). *The model for defining the fully attribute-hiding security of IPE against adversary $\mathcal{A}$ under chosen plaintext attacks is given as follows:*

Setup. *The challenger runs the setup algorithm* $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$*, and it gives the security parameter* λ *and the public key* pk *to the adversary* $\mathcal{A}$*.*

Phase 1. *The adversary* $\mathcal{A}$ *is allowed to adaptively issue a polynomial number of key queries. For a decryption key query* v*, the challenger gives* $\mathsf{sk}_v \xleftarrow{\mathsf{R}} \mathsf{KG}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{sk}, \vec{v})$ *to* $\mathcal{A}$*.*

Challenge. *For a challenge query* $(X^{(0)}, X^{(1)}, \vec{x}^{(0)}, \vec{x}^{(1)})$*, subject to the following restriction:*

1. $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)}) = 0$ *for all the decryption key queries* $\vec{v}$*, or*
2. *Two challenge plaintexts are equal, i.e.,* $X^{(0)} = X^{(1)}$*, and any decryption key query* $\vec{v}$ *satisfies* $R(\vec{v}, \vec{x}^{(0)}) = R(\vec{v}, \vec{x}^{(1)})$*.*

The challenger flips a random $b \in \{0, 1\}$ *and computes* $\mathsf{ct}_{\vec{x}^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x}^{(b)}, X^{(b)})$*. Then it gives* $\mathsf{ct}_{\vec{x}^{(b)}}$ *to* $\mathcal{A}$*.*

Phase 2. *The adversary* $\mathcal{A}$ *is allowed to adaptively issue a polynomial number of key queries. For a decryption key query* v*, subject to the restriction given it challenge phase.*

Finally, $\mathcal{A}$ *outputs its guess* $b' \in \{0, 1\}$ *for* b *and wins the game if* $b = b'$*. We define the advantage of* $\mathcal{A}$ *as* $Adv_{\mathcal{A}}^{\mathsf{IPE},\mathsf{AH}}(\lambda) = Pr[b = b'] - \frac{1}{2}$*. An IPE scheme is fully attribute-hiding if all polynomial time adversaries have at most negligible advantage in the above game. If item 1 in Challenge is allowed for* $\mathcal{A}$*, an IPE scheme is payload-hiding if all polynomial time adversaries have at most negligible advantage in the game.*

Definition 14 ((Unconditional) Unlinkability). *An IPE scheme is unconditionally unlinkable if the following two conditions hold:*

Unlinkability of Ciphertexts *for all* $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$*, all attribute vectors* $\vec{x}$*, all plaintexts* $X \in \mathbb{F}_q^{N \times N}$*, distributions* $(\mathsf{prect}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x}),\ \mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{prect}_{\vec{x}}, X))$ *and* $(\mathsf{prect}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x}),\ \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x}, X))$ *are equivalent except for negligible probability.*

Unlinkability of Re-randomized Ciphertexts *for all* $(\mathsf{sk}, \mathsf{pk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$*, all attribute vectors* $\vec{x}$*, all plaintexts* $X \in \mathbb{F}_q^{N \times N}$*, distributions* $(\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x}, X),\ \mathsf{RR}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{ct}_{\vec{x}}))$ *and* $(\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x}, X),\ \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x}, X))$ *are equivalent except for negligible probability.*

Fully attribute-hiding IPE scheme which is proposed in [29] is an instantiation of the above underlying IPE scheme. We give specific underlying IPE scheme $(\mathsf{Setup}_{\mathsf{IPE}}, \mathsf{KG}_{\mathsf{IPE}}, \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}, \mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}, \mathsf{Enc}_{\mathsf{IPE}}, \mathsf{RR}_{\mathsf{IPE}}, \mathsf{Dec}_{\mathsf{IPE}})$ based on fully attribute-hiding IPE scheme proposed in [29].

Definition 15 (The OT12 IPE Scheme). *Let* E *be an injective encoding function from* $\mathbb{F}_q$ *to* G_T*. Assume that the security parameter is chosen so that* E *is an injective function.*

$\mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$**:** $(\mathsf{param}_n, \mathbb{B}_{\mathsf{IPE}} = (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{4n+1}), \mathbb{B}^*_{\mathsf{IPE}} = (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_{4n+1})) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+2)$,
$\widehat{\mathbb{B}}_{\mathsf{IPE}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1})$, $\widehat{\mathbb{B}}^*_{\mathsf{IPE}} := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{4n})$,
return $\mathsf{pk}^{\mathsf{IPE}} := (1^\lambda, \mathsf{param}_n, \widehat{\mathbb{B}}_{\mathsf{IPE}})$, $\mathsf{sk}^{\mathsf{IPE}} := \widehat{\mathbb{B}}^*_{\mathsf{IPE}}$.

$\mathsf{KG}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}, \vec{v})$**:** $\delta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^{2n},\ \vec{\eta},\ 0)_{\mathbb{B}^*_{\mathsf{IPE}}}$, return $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}} := \boldsymbol{k}^*$.

$\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x})$**:** $\omega, \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\boldsymbol{c}' := (0,\ \omega\vec{x},\ 0^{2n},\ 0^n,\ \varphi)_{\mathbb{B}_{\mathsf{IPE}}}$, return $\mathsf{prect}_{\vec{x}} := \boldsymbol{c}'$.

$\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{prect}_{\vec{x}}, X := (X_{i,j})_{i,j=1,\ldots,n} \in \mathbb{F}_q^{N \times N})$**:** $\xi'_0, \varphi'_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\boldsymbol{c}_0 := \xi'_0 \boldsymbol{c}' + \varphi'_0 \boldsymbol{b}_{4n+1}$,
for $i, j = 1, \ldots, n$, $\zeta_{i,j}, \xi'_{i,j}, \varphi'_{i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,
$\boldsymbol{c}_{i,j} := \xi'_{i,j} \boldsymbol{c}' + (\ \zeta_{i,j},\ 0^n,\ 0^{2n},\ 0^n,\ \varphi'_{i,j})_{\mathbb{B}_{\mathsf{IPE}}}$, $c_{T,i,j} := E(X_{i,j}) \cdot g_T^{\zeta_{i,j}}$,
return $\mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_0, \{\boldsymbol{c}_{i,j}, c_{T,i,j}\}_{i,j=1,\ldots,n})$.

$\mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x}, X \in \mathbb{F}_q^{N\times N})$: $\mathsf{prect}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}, \vec{x})$, return $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{prect}_{\vec{x}}, X)$.

$\mathsf{RR}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_0, \{\boldsymbol{c}_{i,j}, c_{T,i,j}\}_{i,j=1,\dots,n}))$: $\widetilde{\xi}_0, \widetilde{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\widetilde{\boldsymbol{c}}_0 := \widetilde{\xi}_0\boldsymbol{c}_0 + \widetilde{\varphi}_0\boldsymbol{b}_{4n+1}$,
for $i,j = 1,\dots,n$, $\widetilde{\zeta}_{i,j}, \widetilde{\xi}_{i,j}, \widetilde{\varphi}_{i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q$,
$\widetilde{\boldsymbol{c}}_{i,j} := \widetilde{\xi}_{i,j}\boldsymbol{c}_0 + (\ \widetilde{\zeta}_{i,j},\ 0^n,\ 0^{2n},\ 0^n,\ \widetilde{\varphi}_{i,j})_{\mathbb{B}_{\mathsf{IPE}}}$, $\widetilde{c}_{T,i,j} := c_{T,i,j} \cdot g_T^{\widetilde{\zeta}_{i,j}}$,
return $\widetilde{\mathsf{ct}}_{\vec{x}} := (\widetilde{\boldsymbol{c}}_0, \{\widetilde{\boldsymbol{c}}_{i,j}, \widetilde{c}_{T,i,j}\}_{i,j=1,\dots,n})$.

$\mathsf{Dec}_{\mathsf{IPE}}(\mathsf{pk}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}}, \mathsf{ct}_{\vec{x}})$: $K_{i,j} := e(\boldsymbol{c}_{i,j}, \boldsymbol{k}^*)$, $E(\widetilde{X}_{i,j}) := c_{T,i,j}/K_{i,j}$,
return $\widetilde{X} := (\widetilde{X}_{i,j})_{i,j=1,\dots,n}$ by decoding of $E(\widetilde{X}_{i,j})$.

We obtain a fully attribute-hiding IPE scheme with the above message space based on a fully attribute-hiding IPE in [29]. We call it the OT12 IPE scheme.

Lemma 1. *The OT12 IPE scheme is fully-attribute-hiding under the DLIN assumption.*

Proof. The OT12 IPE scheme is equivalent fully-attribute-hiding IPE scheme which is proposed in [29] except that there exists $\mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}$ and $\mathsf{Enc}^{\mathsf{m}}_{\mathsf{IPE}}$. So, the security proof of fully-attribute-hiding is also similarly obtained to the security proof in [29]. □

Lemma 2. *The OT12 IPE scheme is unconditionally unlinkable.*

Proof. It holds $\boldsymbol{c}_0 = (0,\ \omega_0\vec{x},\ 0^{2n},\ 0^n,\ \varphi_0)_{\mathbb{B}_{\mathsf{IPE}}}$ with uniformly and independently distributed $\omega_0 := \xi_0'\omega, \varphi_0 := \xi_0'\varphi + \varphi_0'$ since $\xi_0', \varphi_0' \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $\boldsymbol{c}_{i,j} = (\ \zeta_{i,j},\ \omega_{i,j}\vec{x},\ 0^{2n},\ 0^n,\ \varphi_{i,j})_{\mathbb{B}_{\mathsf{IPE}}}$ with uniformly and independently distributed $\zeta_{i,j}, \omega_{i,j} := \xi_{i,j}'\omega, \varphi_{i,j} := \xi_{i,j}'\varphi + \varphi_{i,j}'$ except when $\omega = 0$, i.e., except for probability $1/q$ since $\zeta_{i,j}, \xi_{i,j}', \varphi_{i,j}' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i,j = 1,\dots,n$. This completes the unlinkability of ciphertexts $\mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_0, \{\boldsymbol{c}_{i,j}, c_{T,i,j}\}_{i,j=1,\dots,n})$. The unlinkability of re-randomized ciphertexts $\widetilde{\mathsf{ct}}_{\vec{x}} := (\widetilde{\boldsymbol{c}}_0, \{\widetilde{\boldsymbol{c}}_{i,j}, \widetilde{c}_{T,i,j}\}_{i,j=1,\dots,n})$ is similarly proven. □

C Basic IP-PRE

$\mathsf{Setup}(1^\lambda, n)$: $(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$,
$(\mathsf{param}_n, \mathbb{B} = (\boldsymbol{b}_0, \dots, \boldsymbol{b}_{3n+3}), \mathbb{B}^* = (\boldsymbol{b}_0^*, \dots, \boldsymbol{b}_{3n+3}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 3n+4)$,
$\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \dots, \boldsymbol{b}_{n+2}, \boldsymbol{b}_{3n+3})$, $\widehat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, \dots, \boldsymbol{b}_{n+2}^*, \boldsymbol{b}_{2n+2}^*, \dots, \boldsymbol{b}_{3n+2}^*)$,
return $\mathsf{pk} := (1^\lambda, \mathsf{pk}^{\mathsf{IPE}}, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$, $\mathsf{sk} := (\boldsymbol{b}_0^*, \mathsf{sk}^{\mathsf{IPE}})$.

$\mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \vec{v})$: $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}^{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}, \vec{v})$,
$\delta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ 0^n,\ \vec{\eta},\ 0)_{\mathbb{B}^*}$,
return $\mathsf{sk}_{\vec{v}} := (\vec{v}, \boldsymbol{k}^*, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$.

$\mathsf{Enc}(\mathsf{pk}, \vec{x}, m)$: $\zeta, \omega, \rho, \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $(\mathsf{sigk}, \mathsf{verk}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$,
$\boldsymbol{c} := (\ \zeta,\ \omega\vec{x},\ \rho(\mathsf{verk}, 1),\ 0^n,\ 0^n,\ \varphi)_{\mathbb{B}}$,
$c_T := m \cdot g_T^\zeta$, $C := (\vec{x}, \boldsymbol{c}, c_T)$, $S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}, C)$, return $\mathsf{oct}_{\vec{x}} := (C, \mathsf{verk}, S)$.

$\mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \vec{x}')$: $\delta' \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}\,' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $W_1 \xleftarrow{\mathsf{U}} GL(3n+4, \mathbb{F}_q)$,
$\boldsymbol{d}_i^* := \boldsymbol{b}_i^* W_1$ for $i = 1,\dots,n+2, 2n+3, \dots, 3n+3$, $\widehat{\mathbb{D}}_1^* := (\boldsymbol{d}_1^*, \dots, \boldsymbol{d}_{n+2}^*, \boldsymbol{d}_{2n+2}^*, \dots, \boldsymbol{d}_{3n+3}^*)$
$\boldsymbol{k}^{*\mathsf{rk}} := (\boldsymbol{k}^* + (\ 0,\ \delta'\vec{v},\ 0^2,\ 0^n,\ \vec{\eta}\,',\ 0)_{\mathbb{B}^*})W_1$,
$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', W_1)$, return $\mathsf{rk}_{\vec{v},\vec{x}'} := (\vec{v}, \vec{x}', \boldsymbol{k}^{*\mathsf{rk}}, \widehat{\mathbb{D}}_1^*, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'})$.

Remark $\boldsymbol{k}^{*\mathsf{rk}}$ is represented over basis $\mathbb{D}_1^* := (\boldsymbol{b}_i^* W_1)_{i=0,..,3n+3}$ as $\boldsymbol{k}^{*\mathsf{rk}} = (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ 0^n,\ \vec{\eta}^{\,\mathsf{rk}},\ 0)_{\mathbb{D}_1^*}$ with $\delta^{\mathsf{rk}} := \delta + \delta'$, $\vec{\eta}^{\,\mathsf{rk}} := \vec{\eta} + \vec{\eta}\,'$, which are uniformly and independently distributed from $\mathsf{sk}_{\vec{v}}$.

$\mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{\vec{v},\vec{x}'} := (\vec{v}, \vec{x}', \boldsymbol{k}^{*\mathsf{rk}}, \widehat{\mathbb{D}}_1^*, \mathsf{ct}_{\vec{x}'}^{\mathsf{rk}}),\ \mathsf{oct}_{\vec{x}} := (C := (\vec{x}, \boldsymbol{c}, c_T), \mathsf{verk}, S))$**:**
If $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, return $\perp$.
$\delta'', \sigma, \zeta', \omega', \rho', \varphi' \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}\,'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\ W_2 \xleftarrow{\mathsf{U}} GL(3n+4, \mathbb{F}_q)$
$\boldsymbol{k}^{*\mathsf{renc}} := \boldsymbol{k}^{*\mathsf{rk}} + (\ 0,\ \delta''\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \vec{\eta}\,'',\ 0)_{\mathbb{D}_1^*}$,
$\boldsymbol{c}^{\mathsf{renc}} := (\boldsymbol{c}_0 + (\ \zeta',\ \omega'\vec{x},\ \rho'(\mathsf{verk}, 1),\ 0^n,\ 0^n,\ \varphi')_{\mathbb{B}})W_2, \quad c_T^{\mathsf{renc}} := c_T \cdot g_T^{\zeta'}$
$\mathsf{ct}_{1,\vec{x}'}^{\mathsf{renc}} \xleftarrow{\mathsf{R}} \mathsf{RR}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{ct}_{\vec{x}'}^{\mathsf{rk}}),\ \mathsf{ct}_{\vec{x}'}^{\mathsf{renc}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', W_2)$,
return $\mathsf{rct}_{\vec{x}'} := (\vec{x}', \boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c_T^{\mathsf{renc}}, \{\mathsf{ct}_{i,\vec{x}'}^{\mathsf{renc}}\}_{i=1,2})$.
Remark $\boldsymbol{k}^{*\mathsf{renc}}$ is represented over basis $\mathbb{D}_1^*$ as $\boldsymbol{k}^{*\mathsf{renc}} = (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{D}_1^*}$ with $\delta^{\mathsf{renc}} := \delta^{\mathsf{rk}} + \delta''$, $\vec{\eta}^{\ \mathsf{renc}} := \vec{\eta}^{\ \mathsf{rk}} + \vec{\eta}''$, which are uniformly and independently distributed from $\mathsf{rk}_{\vec{v},\vec{x}'}$. $\boldsymbol{c}^{\mathsf{renc}}$ and c_T^{renc} are represented over basis $\mathbb{D}_2 := (\boldsymbol{b}_i W_2)_{i=0,..,3n+3}$ as $\boldsymbol{c}^{\mathsf{renc}} = (\ \zeta^{\mathsf{renc}},\ \omega^{\mathsf{renc}}\vec{x},\ \rho^{\mathsf{renc}}(\mathsf{verk}, 1),\ 0^n,\ 0^n,\ \varphi^{\mathsf{renc}})_{\mathbb{D}_2}$ and $c_T^{\mathsf{renc}} := m \cdot g_T^{\zeta^{\mathsf{renc}}}$ with $\zeta^{\mathsf{renc}} := \zeta + \zeta'$, $\omega^{\mathsf{renc}} := \omega + \omega'$, $\rho^{\mathsf{renc}} := \rho + \rho'$, $\varphi^{\mathsf{renc}} := \varphi + \varphi'$, which are uniformly and independently distributed from $\mathsf{oct}_{\vec{x}}$.

$\mathsf{Dec}_{\mathsf{oct}}(\mathsf{pk}, \mathsf{sk}_{\vec{v}} := (\vec{v}, \boldsymbol{k}^*, \mathsf{sk}_{\vec{v}}^{\mathsf{IPE}}), \mathsf{oct}_{\vec{x}} := (C := (\vec{x}, \boldsymbol{c}, c_T), \mathsf{verk}, S))$**:**
If $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, return $\perp$, $K := e(\boldsymbol{c}, \boldsymbol{k}^*)$, return $\widetilde{m} := c_T/K$.

$\mathsf{Dec}_{\mathsf{rct}}(\mathsf{pk}, \mathsf{sk}_{\vec{v}'} := (\vec{v}', \boldsymbol{k}^*, \mathsf{sk}_{\vec{v}'}^{\mathsf{IPE}}), \mathsf{rct}_{\vec{x}'} := (\vec{x}', \boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}_0^{\mathsf{renc}}, c_1^{\mathsf{renc}}, \{\mathsf{ct}_{i,\vec{x}'}^{\mathsf{renc}}\}_{i=1,2}))$**:**
$\widetilde{W}_i \xleftarrow{\mathsf{R}} \mathsf{Dec}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}_{\vec{v}'}^{\mathsf{IPE}}, \mathsf{ct}_{i,\vec{x}'}^{\mathsf{renc}})$ for $i = 1, 2$, $\quad \widetilde{K} := e(\boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1}, \boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1})$,
return $\widetilde{m} := c_T^{\mathsf{renc}}/\widetilde{K}$.
Remark $(\boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1}, \boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1})$ are represented over bases $(\mathbb{B}, \mathbb{B}^*)$ as $\boldsymbol{k}^{*\mathsf{renc}}\widetilde{W}_1^{-1} = (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{B}^*}$ and $\boldsymbol{c}^{\mathsf{renc}}\widetilde{W}_2^{-1} = (\ \zeta^{\mathsf{renc}},\ \omega^{\mathsf{renc}}\vec{x},\ \rho^{\mathsf{renc}}(\mathsf{verk}, 1),\ 0^n,\ 0^n,\ \varphi^{\mathsf{renc}})_{\mathbb{B}}$.

Theorem 6. *The proposed basic IP-PRE scheme is payload-hiding for original ciphertexts against chosen plaintext attacks under the DLIN assumption, payload-hiding of underlying IPE scheme and strong unforgeability of one-time signature.*

Theorem 7. *The proposed basic IP-PRE scheme is payload-hiding for re-encrypted ciphertexts against chosen plaintext attacks under payload-hiding of underlying IPE scheme.*

Corollary 2 *The proposed basic IP-PRE scheme is payload-hiding for original ciphertexts against chosen plaintext attacks under the DLIN assumption and strong unforgeability of one-time signature with instantiating underlying IPE by OT12 IPE scheme.*

The proposed basic IP-PRE scheme is payload-hiding for re-encrypted ciphertexts against chosen plaintext attacks under the DLIN assumption with instantiating underlying IPE by OT12 IPE scheme.

The proof of Theorems 6 and 7 and Corollary 2 are similarly given to Theorems and Corollary for fully-anonymous IP-PRE in Section D.

D Security Proofs of Theorems 2-5

D.1 Key Technique: Information-Theoretical Insulation of a Subspace for Re-Enc Key Basis $\mathbb{D}_1^*$

The dual system encryption (DSE) approach is developed by Waters [37] for achieving an adaptively secure FE schemes, and subsequent works [15, 14, 27, 29, 16, 30] successfully apply the approach to obtain various kinds of adaptively secure schemes. The main key point in the game transformation

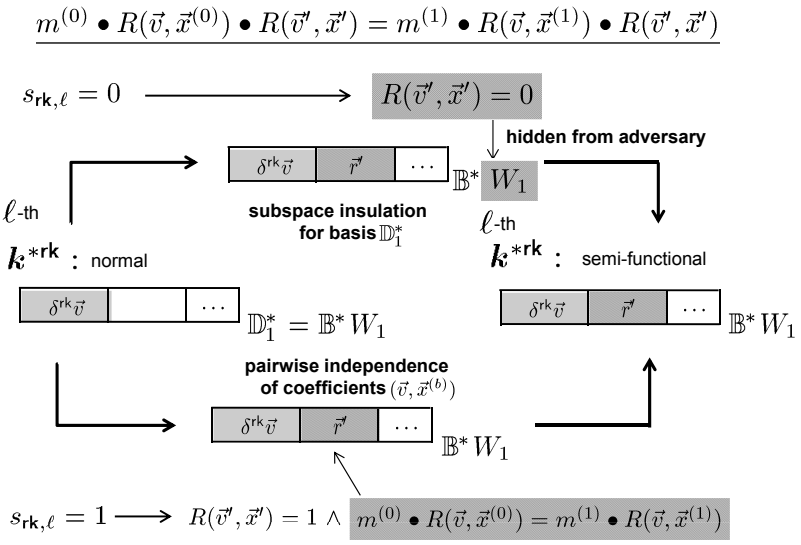

Fig. 2. Overview of Game Changes between Games 1-3-$(\ell-1)$ and 1-3-ℓ

of the approach is to interleave a computational change with a conceptual (information-theoretical) change, in turn for each key query. Usually, the computational one is given by a kind of *subspace assumption* on a dual pairing vector space (in a prime-order pairing group) or a composite-order pairing group, and the conceptual one is based on a *pairwise independence* argument for key and ciphertext parameters, e.g., attribute vector $\vec{v}$ and predicate vector $\vec{x}$ in IPE. Lewko-Waters [16] gave a nice strategy for new applications by replacing the conceptual one by some computational one.

For our application, we develop another instantiation for the above conceptual step, *subspace insulation for basis* $\mathbb{D}_1^*$. The basis $\mathbb{D}_1^* := \mathbb{B}^* W_1$ is generated in re-encryption key generation. In Figure 2, a high-level description of game changes between Games 1-3-$(\ell-1)$ and 1-3-ℓ for AH-OC is given, in particular, (a part of) a normal form reply $\boldsymbol{k}^{*\,\mathsf{rk}}$ (and $\boldsymbol{k}_{\mathsf{ran}}^{*\,\mathsf{rk}}$) for the ℓ-th re-enc key query $(\vec{v},\vec{x}')$ is changed to a semi-functional one in *two different ways* depending on $s_{\mathsf{rk},\ell} = 0$ or 1 (Precisely, the simulator first guesses the value of $s_{\mathsf{rk},\ell}$ by using $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$ and follows the guess. See Proof Outline of Lemma 5 near Figure 3 for the details.). Importantly, the obtained semi-functional forms must be the same to proceed the game transformation in turn since we cannot ramify the challenger's simulation depending on all (polynomial number of) values of $s_{\mathsf{rk},\ell}$ for $\ell = 1,\ldots,\nu_2$.

By definition of the AH-OC security game (Definition 5), the ℓ-th re-enc key query $(\vec{v},\vec{x}')$ satisfies that

> for any decryption key query $\vec{v}'$, challenge messages $(m^{(0)},m^{(1)})$ and attributes $(\vec{x}^{(0)},\vec{x}^{(1)})$, it holds that $m^{(0)} \bullet R(\vec{v},\vec{x}^{(0)}) \bullet R(\vec{v}',\vec{x}') = m^{(1)} \bullet R(\vec{v},\vec{x}^{(1)}) \bullet R(\vec{v}',\vec{x}')$.

When $s_{\mathsf{rk},\ell} = 0$, it holds that $R(\vec{v}',\vec{x}') = 0$ for any decryption key query $\vec{v}'$. When $s_{\mathsf{rk},\ell} = 1$, it holds that $m^{(0)} \bullet R(\vec{v},\vec{x}^{(0)}) = m^{(1)} \bullet R(\vec{v},\vec{x}^{(1)})$ for challenge $(m^{(0)},m^{(1)})$ and $(\vec{x}^{(0)},\vec{x}^{(1)})$. The latter condition is the same as the previous *fully-attribute-hiding* security condition for IPE schemes, hence, we can execute the proof in a similar manner to that in [29] based on a pairwise independence argument.

In the former case, since $R(\vec{v}',\vec{x}') = 0$ for any decryption key query $\vec{v}'$, the adversary cannot decrypt $\mathsf{ct}_{\vec{x}'}^{\mathsf{rk}}$, i.e., cannot obtain W_1. Therefore, the adversary has no information on the subspace basis $(\boldsymbol{d}_0^*,\ldots,\boldsymbol{d}_n^*,\boldsymbol{d}_{n+3}^*,\ldots,\boldsymbol{d}_{2n+2}^*)$. We call this *information-theoretical insulation of a subspace for basis* $\mathbb{D}_1^*$, and using this information gap for the adversary, we conceptually change a normal form

$\boldsymbol{k}^{*\,\mathsf{rk}}$ to a semi-functional one. For the details of the technique, refer to Figures 4 and 6, and their explanations ("Overview of Sub-Games") in Appendix D.3.

D.2 Preliminary Lemmas: Lemmas 3–6

Definition 16 (Problem 1). *Problem 1 is to guess β, given* $(\mathsf{param}, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,1}, \{\boldsymbol{e}_i\}_{i=2,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P1}}(1^\lambda, n)$*, where*

$$
\begin{aligned}
&\mathcal{G}_\beta^{\mathsf{P1}}(1^\lambda, n): \quad (\mathsf{param}_n, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4),\\
&\quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_0^*, .., \boldsymbol{b}_{n+2}^*, \boldsymbol{b}_{2n+3}^*, .., \boldsymbol{b}_{4n+3}^*), \quad \omega, \gamma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{z} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\ \ \vec{e}_1 := (1, 0^{n-1}) \in \mathbb{F}_q^n,\\
&\qquad\qquad \overbrace{\qquad\qquad}^{n+3} \overbrace{\qquad}^{2n} \overbrace{\quad}^{n} \overbrace{\ }^{1}\\
&\quad \boldsymbol{e}_{0,1} := (\ 0,\ \omega\vec{e}_1,\ 0^2,\quad 0^{2n},\quad 0^n,\quad \gamma\ )_{\mathbb{B}},\\
&\quad \boldsymbol{e}_{1,1} := (\ 0,\ \omega\vec{e}_1,\ 0^2,\quad \vec{z},\ 0^n,\quad 0^n,\quad \gamma\ )_{\mathbb{B}},\\
&\quad \boldsymbol{e}_i := \omega\boldsymbol{b}_i \ \text{ for } i = 2, \ldots, n,\\
&\quad \text{return } \ (\mathsf{param}_n, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,1}, \{\boldsymbol{e}_i\}_{i=2,\ldots,n}),
\end{aligned}
$$

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

Lemma 3. *For any adversary $\mathcal{B}$, there exist probabilistic machines $\mathcal{E}$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ,* $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P1}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$.

The proof of Lemma 3 is given in a similar manner to the security proof of Problem 1 in [27] to DLIN. □

Definition 17 (Problem 2). *Problem 2 is to guess β, given* $(\mathsf{param}_n, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_i\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P2}}(1^\lambda, n)$*, where*

$$
\begin{aligned}
&\mathcal{G}_\beta^{\mathsf{P2}}(1^\lambda, n): \quad (\mathsf{param}_n, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4),\\
&\quad \widehat{\mathbb{B}} := (\boldsymbol{b}_0, .., \boldsymbol{b}_{n+2}, \boldsymbol{b}_{2n+3}, .., \boldsymbol{b}_{4n+3}), \quad \delta, \omega, \tau, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\quad \text{for } i = 1, \ldots, n, \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\\
&\qquad\qquad \overbrace{\qquad\qquad}^{n+3} \overbrace{\qquad}^{2n} \overbrace{\quad}^{n} \overbrace{\ }^{1}\\
&\quad \boldsymbol{h}_{0,i}^* := (\ 0,\ \delta\vec{e}_i,\ 0^2,\quad 0^{2n},\quad \vec{\eta}_i,\quad 0\ )_{\mathbb{B}^*}\\
&\quad \boldsymbol{h}_{1,i}^* := (\ 0,\ \delta\vec{e}_i,\ 0^2,\quad \tau\vec{e}_i,\ 0^n,\quad \vec{\eta}_i,\quad 0\ )_{\mathbb{B}^*}\\
&\quad \boldsymbol{e}_i := \ \ (\ 0,\ \omega\vec{e}_i,\ 0^2,\quad \sigma\vec{e}_i,\ 0^n,\quad 0^n,\quad 0\ )_{\mathbb{B}},\\
&\quad \text{return } (\mathsf{param}_n, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}_{\beta,i}^*, \boldsymbol{e}_i\}_{i=1,..,n}),
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 2, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2}}(\lambda)$*, is similarly defined as in Definition 16.*

Lemma 4. *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ,* $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$.

The proof of Lemma 4 is given in a similar manner to the security proof of Problem 2 in [27] to DLIN. □

Definition 18 (Problem 3). *Problem 3 is to guess β, given* $(\mathsf{param}_n, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P3}}_\beta(1^\lambda, n)$, *where*

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{P3}}_\beta(1^\lambda, n): \quad (\mathsf{param}_n, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4),\\
&\widehat{\mathbb{B}} := (\boldsymbol{b}_0, .., \boldsymbol{b}_{n+2}, \boldsymbol{b}_{2n+3}, .., \boldsymbol{b}_{4n+3}), \quad \delta, \omega, \tau, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q),\ U := (Z^{-1})^{\mathrm{T}},\\
&\text{for } i = 1, 2, \quad \vec{e}_1 := (1, 0),\ \vec{e}_2 := (0, 1) \in \mathbb{F}_q^2,\ \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\\
&\qquad\qquad \overbrace{\qquad}^{n+3} \overbrace{\qquad\qquad}^{2n} \overbrace{\quad}^{n} \overbrace{\quad}^{1}\\
&\boldsymbol{h}^*_{0,i} := (\ 0^{n+1},\ \delta\vec{e}_i,\ 0^{2n},\ \vec{\eta}_i,\ 0\ )_{\mathbb{B}^*}\\
&\boldsymbol{h}^*_{1,i} := (\ 0^{n+1},\ \delta\vec{e}_i,\ (\tau\vec{e}_i, 0^{n-2})U,\ 0^n,\ \vec{\eta}_i,\ 0\ )_{\mathbb{B}^*}\\
&\boldsymbol{e}_i := \ (\ 0^{n+1},\ \omega\vec{e}_i,\ (\sigma\vec{e}_i, 0^{n-2})Z,\ 0^n,\ 0^n,\ 0\ )_{\mathbb{B}},\\
&\text{return } (\mathsf{param}_n, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,2}),
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 3, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 16.

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

The proof of Lemma 5 is given in a similar manner to the security proof of Problem 2 in [27] to DLIN. □

Definition 19 (Problem 4). *Problem 4 is to guess β, given* $(\mathsf{param}_n, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,..,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P4}}_\beta(1^\lambda, n)$, *where*

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{P4}}_\beta(1^\lambda, n): \quad (\mathsf{param}_n, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4),\\
&\widehat{\mathbb{B}} := (\boldsymbol{b}_0, .., \boldsymbol{b}_{n+2}, \boldsymbol{b}_{3n+3}, .., \boldsymbol{b}_{4n+3}), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_0, .., \boldsymbol{b}_{n+2}, \boldsymbol{b}_{2n+3}, .., \boldsymbol{b}_{4n+3}), \quad \tau, \omega', \omega'', \kappa', \kappa'' \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\text{for } i = 1, \ldots, n, \quad \vec{e}_i := (0^{i-1}, 1, 0^{n-i}) \in \mathbb{F}_q^n, \quad \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,\\
&\qquad\qquad \overbrace{\qquad}^{n+3} \overbrace{\qquad\qquad}^{2n} \overbrace{\quad}^{n} \overbrace{\quad}^{1}\\
&\boldsymbol{h}^*_{0,i} := (\quad 0^{n+3},\quad \tau\vec{e}_i,\ 0^n,\quad \vec{\eta}_i,\quad 0\ )_{\mathbb{B}^*}\\
&\boldsymbol{h}^*_{1,i} := (\quad 0^{n+3},\quad 0^n,\ \tau\vec{e}_i,\quad \vec{\eta}_i,\quad 0\ )_{\mathbb{B}^*}\\
&\boldsymbol{e}_i \quad := (\quad 0^{n+3},\quad \omega'\vec{e}_i,\ \omega''\vec{e}_i,\quad 0^n,\quad 0\ )_{\mathbb{B}},\\
&\boldsymbol{f}_i \quad := (\quad 0^{n+3},\quad \kappa'\vec{e}_i,\ \kappa''\vec{e}_i,\quad 0^n,\quad 0\ )_{\mathbb{B}},\\
&\text{return } (\mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,..,n}),
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 4, $\mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 16.

Lemma 6. *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 8/q$.*

The proof of Lemma 6 is given in a similar manner to the security proof of Problem 3 in [29] to DLIN. □

D.3 Proof of Theorem 2 (AH-OC: Attribute-Hiding for Original Ciphertexts)

The variables $s_{\mathsf{m}}, s_{\mathsf{rk},\ell}, s_{\mathsf{renc},t}$ in Definition 5 are used for defining cases in the proof of Theorem 2. For that purpose, the following claims are important, which are deduced from the restriction described in Challenge phase.

- When $s_{\mathsf{m}} = 0$, it holds that $R(v, x^{(0)}) = R(v, x^{(1)}) = 0$ for any decryption key query v.
- When $s_{\mathsf{m}} = 1$, it holds that $R(v, x^{(0)}) = R(v, x^{(1)})$ for any decryption key query v.
- When $s_{\mathsf{rk},\ell} = 0$, it holds that $R(v, x'_\ell) = 0$ for any decryption key query v and the ℓ-th re-encryption key query (v_ℓ, x'_ℓ).
- When $s_{\mathsf{m}} = 0$ and $s_{\mathsf{rk},\ell} = 1$, it holds that $R(v_\ell, x^{(0)}) = R(v_\ell, x^{(1)}) = 0$ for the ℓ-th re-encryption key query (v_ℓ, x'_ℓ).
- When $s_{\mathsf{m}} = 1$ and $s_{\mathsf{rk},\ell} = 1$, it holds that $R(v_\ell, x^{(0)}) = R(v_\ell, x^{(1)})$ for the ℓ-th re-encryption key query (v_ℓ, x'_ℓ).
- When $s_{\mathsf{renc},t} = 0$, it holds that $R(v, x'_t) = 0$ for any decryption key query v and the t-th re-encryption query $(v_t, x'_t, \mathsf{oct}_t)$.
- When $s_{\mathsf{m}} = 0$ and $s_{\mathsf{renc},t} = 1$, it holds that $R(v_t, x^{(0)}) = R(v_t, x^{(1)}) = 0$ for the t-th re-encryption query $(v_t, x'_t, \mathsf{oct}_t)$.
- When $s_{\mathsf{m}} = 1$ and $s_{\mathsf{renc},t} = 1$, it holds that $R(v_t, x^{(0)}) = R(v_t, x^{(1)})$ for the t-th re-encryption query $(v_t, x'_t, \mathsf{oct}_t)$.

Theorem 2 *The proposed IP-PRE scheme is attribute-hiding for original ciphertexts against chosen plaintext attacks under the DLIN assumption provided the underlying signature scheme is a strongly unforgeable one-time signature scheme and the underlying IPE scheme is fully attribute-hiding.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}$'s, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, the advantage $\mathsf{Adv}^{\mathsf{AH\text{-}OC}}_{\mathcal{A}}(\lambda)$ is upper-bounded by the sum of the right hand side of Eq. (4), that of Eq. (5), and that of Eq. (27). The sum is given by the total of

- *one advantage of the strong unforgeability against the underlying one-time signatures,*
- *$8(\nu_2 + \nu_3)$ advantages of the attribute-hiding security against the underlying IPE scheme, and*
- *$12(\nu_1 + \nu_2) + 11\nu_3 + 7$ advantages of DLIN*

for $\mathcal{E}$ algorithms, which are $\mathcal{E}$ machines with parameters $(\iota, h, \ell, t, j, l)$ as described in Lemmas 7, 8, and 17. Here, ν_1, ν_2, ν_3 are the maximum number of $\mathcal{A}$'s decryption key queries, that of $\mathcal{A}$'s re-encryption key queries, and that of $\mathcal{A}$'s re-encryption queries, respectively.

Proof. For each run of the security game, we define variable s_{verk} as: $s_{\mathsf{verk}} := 0$ if there exists a re-encryption query $(\vec{v}, \vec{x}', \mathsf{oct} := (C, \mathsf{verk}, S))$ such that $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$, $\mathsf{oct} \neq \mathsf{oct}^{(b)}$ and $\mathsf{verk} = \mathsf{verk}^{\clubsuit}$ where $\mathsf{oct}^{(b)} := (C^{\clubsuit}, \mathsf{verk}^{\clubsuit}, S^{\clubsuit})$ (then $(C, S) \neq (C^{\clubsuit}, S^{\clubsuit})$) is the challenge original ciphertext, and $s_{\mathsf{verk}} := 1$ otherwise.

First, we execute a preliminary game transformation from Game 0 (original game in Definition 5) to Game $0'$, which is the same as Game 0 except that flip a coin $\tau_{\mathsf{verk}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted at the final step if $s_{\mathsf{verk}} \neq \tau_{\mathsf{verk}}$. We define that $\mathcal{A}$ wins with probability $1/2$ when the game is aborted and the advantage in Game $0'$ is $\Pr[\mathcal{A} \text{ wins}] - 1/2$ as well. Since τ_{verk} is independent from s_{verk}, the probability that the game is aborted is $1/2$. So, the advantage in Game $0'$ is a half of that in Game 0, that is $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) = 1/2 \cdot \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) = 1/2 \cdot \mathsf{Adv}^{\mathsf{AH\text{-}OC}}_{\mathcal{A}}(\lambda)$. Moreover, $\Pr[\mathcal{A} \text{ wins}] = 1/2(\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{verk}} = 0] + \Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{verk}} = 1])$ in Game $0'$. Namely,

$$\begin{aligned}\mathsf{Adv}^{\mathsf{AH\text{-}OC}}_{\mathcal{A}}(\lambda) &= \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) = 2 \cdot \mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) \\ &= (\Pr[\mathcal{A} \text{ wins in Game } 0' \,|\, \tau_{\mathsf{verk}} = 0] - 1/2) + (\Pr[\mathcal{A} \text{ wins in Game } 0' \,|\, \tau_{\mathsf{verk}} = 1] - 1/2). \quad (2)\end{aligned}$$

Then, we execute a second preliminary game transformation from Game $0'$ to Game $0''$, which is the same as Game $0'$ except that flip a coin $\tau_{\mathsf{m}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted in challenge phase if $s_{\mathsf{m}} \neq \tau_{\mathsf{m}}$. As before, we define that $\mathcal{A}$ wins with probability $1/2$ when the game is aborted and the advantage in Game $0''$ is $\Pr[\mathcal{A} \text{ wins}] - 1/2$ as well. Since τ_{m} is independent from s_{m}, the probability that the game is aborted is $1/2$. So, the advantage in Game $0''$ when $\tau_{\mathsf{verk}} = 1$ is a halt of that in Game $0'$, that is $\Pr[\mathcal{A} \text{ wins in Game } 0'' \,|\, \tau_{\mathsf{verk}} = 1]) - 1/2 = 1/2(\Pr[\mathcal{A} \text{ wins in Game } 0' \,|\, \tau_{\mathsf{verk}} = 1]) - 1/2)$. Moreover, $\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{verk}} = 1] = 1/2(\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{verk}} = 1 \ \wedge \ \tau_{\mathsf{m}} = 0] + \Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{verk}} = 1 \ \wedge \ \tau_{\mathsf{m}} = 1])$ in Game $0''$. Combining Eq. (2), in Game $0''$,

$$\begin{aligned}\mathsf{Adv}^{\mathsf{AH\text{-}OC}}_{\mathcal{A}}(\lambda) = (&\Pr[\mathcal{A} \text{ wins in Game } 0' \,|\, \tau_{\mathsf{verk}} = 0] - 1/2) \\ &+ (\Pr[\mathcal{A} \text{ wins in Game } 0'' \,|\, \tau_{\mathsf{verk}} = 1 \ \wedge \ \tau_{\mathsf{m}} = 0] - 1/2) \\ &+ (\Pr[\mathcal{A} \text{ wins in Game } 0'' \,|\, \tau_{\mathsf{verk}} = 1 \ \wedge \ \tau_{\mathsf{m}} = 1] - 1/2). \end{aligned} \tag{3}$$

The advantage in the case $\tau_{\mathsf{verk}} = 0$ i.e., $\Pr[\mathcal{A} \text{ wins in Game } 0' \,|\, \tau_{\mathsf{verk}} = 0] - 1/2$ is upper-bounded by the advantage of some machine against strong unforgeability of the underlying one-time signature scheme in Lemma 7, and the advantages in the case $\tau_{\mathsf{verk}} = 1$, i.e., $\Pr[\mathcal{A} \text{ wins in Game } 0'' \,|\, \tau_{\mathsf{verk}} = 1 \ \wedge \ \tau_{\mathsf{m}} = 0] - 1/2$ and $\Pr[\mathcal{A} \text{ wins in Game } 0'' \,|\, \tau_{\mathsf{verk}} = 1 \ \wedge \ \tau_{\mathsf{m}} = 1] - 1/2$ are upper-bounded by those of DLIN in Lemmas 8 and 17, respectively.

This completes the proof of Theorem 2. □

Corollary 1-1. *The proposed IP-PRE scheme is attribute-hiding for original ciphertexts against chosen plaintext attacks under the DLIN assumption provided the underlying signature scheme is a strongly unforgeable one-time signature scheme and the underlying IPE scheme is given by the OT12 IPE scheme.*

Proof of Theorem 2 (AH-OC) in the Case $\tau_{\mathsf{verk}} = 0$

Lemma 7. *The proposed IP-PRE scheme is attribute-hiding for original ciphertexts against chosen plaintext attacks in the case $\tau_{\mathsf{verk}} = 0$ provided an underlying signature scheme is a strongly unforgeable one-time signature scheme.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ in Case 0

$$\Pr[\mathcal{A} \text{ wins in Game } 0' \,|\, \tau_{\mathsf{verk}} = 0] - 1/2 \leq \mathsf{Adv}^{\mathsf{OS,SUF}}_{\mathcal{E}}(\lambda). \tag{4}$$

Proof. In order to prove Lemma 7, we construct a probabilistic machine $\mathcal{E}$ against the strong unforgeability of the underlying one-time signature using an adversary $\mathcal{A}$ in a security game (Game $0'$) as a black box as follows:

1. $\mathcal{E}$ is given a verification key instance from the challenger of the strong unforgeability, $\mathsf{verk}^{\clubsuit}$.
2. $\mathcal{E}$ plays a role of the challenger in the security game against $\mathcal{A}$.
3. At the first step of the game, $\mathcal{E}$ generates a pair of public and secret key of the IP-PRE scheme, $(\mathsf{pk}, \mathsf{sk})$. $\mathcal{E}$ provides $\mathcal{A}$ with a public key pk.
4. When a decryption key query is issued for a vector $\vec{v}$, $\mathcal{E}$ computes a normal key $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \vec{v})$ and provides $\mathcal{A}$ with it. Similarly, when a re-encryption key query is issued for $(\vec{v}, \vec{x}')$, $\mathcal{E}$ computes a normal re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \vec{v}), \vec{x}')$ and provides $\mathcal{A}$ with it.
5. When a re-encryption query is issued for $(\vec{v}, \vec{x}', \mathsf{oct} := (C, \mathsf{verk}, S))$, if $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, $\mathcal{E}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{E}$ computes a normal form of re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \vec{v}), \vec{x}'), \mathsf{oct})$ and provides $\mathcal{A}$ with it.

6. When a challenge query is issued for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$, $\mathcal{E}$ picks a bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ and $\zeta, \omega, \omega_{\mathsf{ran}}, \rho, \rho_{\mathsf{ran}}, \varphi, \varphi_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and computes using $\mathsf{verk}^{\clubsuit}$,
$$\boldsymbol{c} := (\ \zeta,\ \omega\vec{x}^{(b)},\ \rho(\mathsf{verk}^{\clubsuit},\ 1),\ 0^{3n},\ \varphi\ )_{\mathbb{B}},\quad \boldsymbol{c}_{\mathsf{ran}} := (\ 0,\ \omega_{\mathsf{ran}}\vec{x}^{(b)},\ \rho_{\mathsf{ran}}(\mathsf{verk}^{\clubsuit},\ 1),\ 0^{3n},\ \varphi_{\mathsf{ran}}\ )_{\mathbb{B}},$$
$$c_T := m^{(b)} \cdot g_T^{\zeta},\quad \text{and}$$
$\mathcal{E}$ asks the challenger of the strong unforgeability with a signature query for message $C^{\clubsuit} := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T)$ and obtain the signature S from the challenger. $\mathcal{E}$ sets a challenge ciphertext $\mathsf{oct}^{(b)} := (C^{\clubsuit}, \mathsf{verk}^{\clubsuit}, S^{\clubsuit})$ to $\mathcal{A}$.
7. For a decryption key, re-encryption key, and re-encryption queries after the challenge, $\mathcal{E}$ responds to $\mathcal{A}$ as in the same manner as in steps 4 and 5.
8. $\mathcal{A}$ finally outputs bit b'.
If there is a re-encryption query $(\vec{v}, \vec{x}', \mathsf{oct} := (C, \mathsf{verk}, S))$ with $\mathsf{verk} = \mathsf{verk}^{\clubsuit}$, $(C,S) \neq (C^{\clubsuit}, S^{\clubsuit})$ and $\mathsf{Ver}(\mathsf{verk}, C, S)$, $\mathcal{E}$ outputs a forgery (C,S). Otherwise, $\mathcal{E}$ aborts the game.

If there is a re-encryption query $(\vec{v}, \vec{x}', \mathsf{oct} := (C, \mathsf{verk}, S))$ with $\mathsf{verk} = \mathsf{verk}^{\clubsuit}$, $(C,S) \neq (C^{\clubsuit}, S^{\clubsuit})$ and $\mathsf{Ver}(\mathsf{verk}, C, S)$, then $s_{\mathsf{verk}} = 0$. Since if $s_{\mathsf{verk}} \neq \tau_{\mathsf{verk}} (= 0)$, the game is aborted and $\mathcal{A}$ wins with probability $1/2$, i.e., $\Pr[\mathcal{A} \text{ wins in Game } 0' \mid \tau_{\mathsf{verk}} = 0 \ \wedge\ s_{\mathsf{verk}} \neq \tau_{\mathsf{verk}}] = 1/2$,

$$\begin{aligned}
&\Pr[\mathcal{A} \text{ wins in Game } 0' \mid \tau_{\mathsf{verk}} = 0] - 1/2\\
&= \Pr[\mathcal{A} \text{ wins in Game } 0' \mid \tau_{\mathsf{verk}} = 0 \ \wedge\ s_{\mathsf{verk}} = \tau_{\mathsf{verk}}] \Pr[s_{\mathsf{verk}} = \tau_{\mathsf{verk}} | \tau_{\mathsf{verk}} = 0]\\
&\quad + \Pr[\mathcal{A} \text{ wins in Game } 0' \mid \tau_{\mathsf{verk}} = 0 \ \wedge\ s_{\mathsf{verk}} \neq \tau_{\mathsf{verk}}] \Pr[s_{\mathsf{verk}} \neq \tau_{\mathsf{verk}} | \tau_{\mathsf{verk}} = 0] - 1/2\\
&= \Pr[\mathcal{A} \text{ wins in Game } 0' \mid \tau_{\mathsf{verk}} = 0 \ \wedge\ s_{\mathsf{verk}} = \tau_{\mathsf{verk}}] \Pr[s_{\mathsf{verk}} = \tau_{\mathsf{verk}} | \tau_{\mathsf{verk}} = 0]\\
&\quad + 1/2(1 - \Pr[s_{\mathsf{verk}} = \tau_{\mathsf{verk}} | \tau_{\mathsf{verk}} = 0]) - 1/2\\
&= \big(\Pr[\mathcal{A} \text{ wins in Game } 0' \mid \tau_{\mathsf{verk}} = 0 \ \wedge\ s_{\mathsf{verk}} = \tau_{\mathsf{verk}}] - 1/2\big) \Pr[s_{\mathsf{verk}} = \tau_{\mathsf{verk}} | \tau_{\mathsf{verk}} = 0]\\
&\leq \Pr[s_{\mathsf{verk}} = \tau_{\mathsf{verk}} | \tau_{\mathsf{verk}} = 0] = \mathsf{Adv}_{\mathcal{E}}^{\mathsf{OS,SUF}}(\lambda).
\end{aligned}$$

This completes the proof of Lemma 7. □

Proof of Theorem 2 (AH-OC) in the Case $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 0$

In Lemmas 8–16 and their proofs, we consider only the case $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 0$.

Lemma 8. *The proposed IP-PRE scheme is attribute-hiding for original ciphertexts against chosen plaintext attacks in the case $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 0$ under the DLIN assumption provided an underlying IPE scheme is attribute-hiding.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_{\iota\text{-}1}, \mathcal{E}_{\iota\text{-}2\text{-}j}, \mathcal{E}_{\iota\text{-}3\text{-}A\text{-}j}, \mathcal{E}_{\iota\text{-}3\text{-}B\text{-}j}, \mathcal{E}_{\iota\text{-}4\text{-}A\text{-}j}, \mathcal{E}_{\iota\text{-}4\text{-}B\text{-}j}, \mathcal{E}_{1\text{-}6}$ for $\iota = 1,2$, $j = 1,2$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\begin{aligned}
&\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 0] - 1/2\\
&\leq \sum_{\iota=1}^{2} \Big(\mathsf{Adv}_{\mathcal{E}_{\iota\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \textstyle\sum_{h=1}^{\nu_1}\sum_{j=1}^{2} \mathsf{Adv}_{\mathcal{E}_{\iota\text{-}2\text{-}h\text{-}j}}^{\mathsf{DLIN}}(\lambda) + \sum_{\ell=1}^{\nu_2}\sum_{j=1}^{2} \Big(\mathsf{Adv}_{\mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}A\text{-}j}}^{\mathsf{IPE,AH}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}B\text{-}j}}^{\mathsf{DLIN}}(\lambda) \Big)\\
&\qquad + \sum_{t=1}^{\nu_3}\sum_{j=1}^{2} \Big(\mathsf{Adv}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}A\text{-}j}}^{\mathsf{IPE,AH}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}B\text{-}j}}^{\mathsf{DLIN}}(\lambda) \Big) \Big) + \mathsf{Adv}_{\mathcal{E}_{1\text{-}6}}^{\mathsf{DLIN}}(\lambda) + \epsilon \qquad (5)
\end{aligned}$$

where $\mathcal{E}_{\iota\text{-}2\text{-}h\text{-}j}(\cdot) := \mathcal{E}_{\iota\text{-}2\text{-}j}(h,\cdot), \mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}A\text{-}j}(\cdot) := \mathcal{E}_{\iota\text{-}3\text{-}A\text{-}j}(\ell,\cdot), \mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}B\text{-}j}(\cdot) := \mathcal{E}_{\iota\text{-}3\text{-}B\text{-}j}(\ell,\cdot), \mathcal{E}_{\iota\text{-}4\text{-}t\text{-}A\text{-}j}(\cdot) := \mathcal{E}_{\iota\text{-}4\text{-}A\text{-}j}(t,\cdot), \mathcal{E}_{\iota\text{-}4\text{-}t\text{-}B\text{-}j}(\cdot) := \mathcal{E}_{\iota\text{-}4\text{-}B\text{-}j}(t,\cdot)$ for $h = 1,\ldots,\nu_1$, $\ell = 1,\ldots,\nu_2$ and $t = 1,\ldots,\nu_3$, $\epsilon = (14\nu_1 + 17\nu_2 + 17\nu_3 + 15)/q$ and ν_1, ν_2, ν_3 are the maximum numbers of $\mathcal{A}$'s decryption key queries, that of $\mathcal{A}$'s re-encryption key queries, and that of $\mathcal{A}$'s re-encryption queries, respectively.

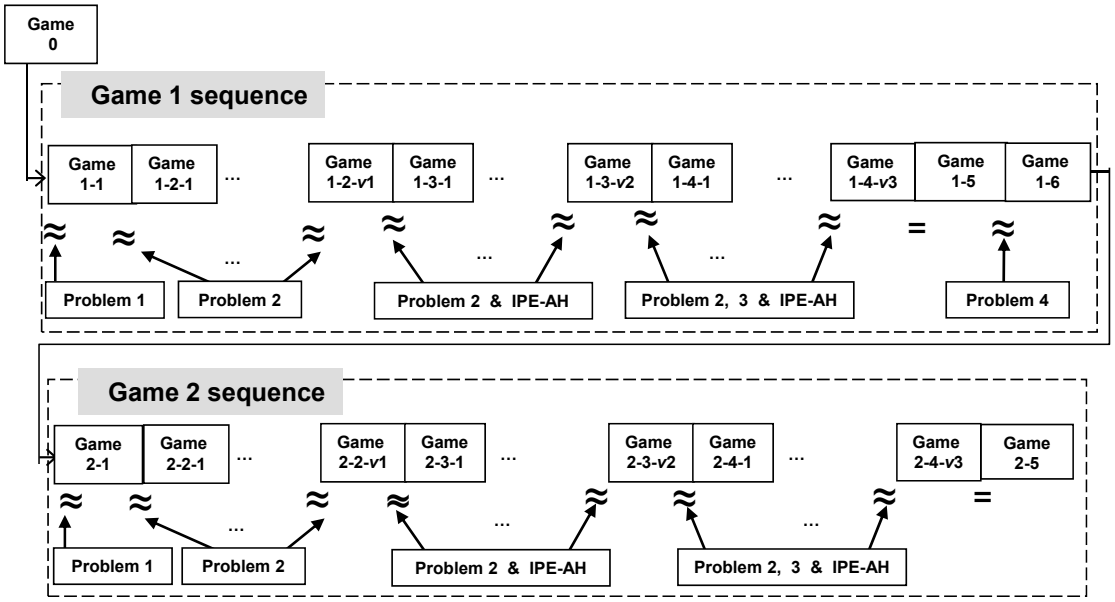

Fig. 3. Game Transformations for AH-OC Security in the Case $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 0$.

Proof Outline of Lemma 8. To prove Lemma 8, we consider $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 0$ case.
Overview of Game Transformation. We employ Game $0''$ through Game 2-5. In this proof, there are main two sequences, the Game 1 sequence and the Game 2 sequence (Figure 3), whose aims are to change components $\boldsymbol{c}$ and $\boldsymbol{c}_{\mathsf{ran}}$ of the challenge ciphertext to independent ones from challenge bit b (random form), respectively.

We employ Game $0''$ through Game 1-7 in the Game 1 sequence. In Game $0''$, all the replies to $\mathcal{A}$'s queries are in normal forms (Eqs.(6)–(10)). In Game 1-1, $\boldsymbol{c}$ of the challenge ciphertext is changed to *semi-functional* form in Eq.(11). Let ν_1, ν_2, ν_3 be the maximum numbers of $\mathcal{A}$'s decryption key queries, that of $\mathcal{A}$'s re-encryption key queries, and that of $\mathcal{A}$'s re-encryption queries, respectively. There are ν_1 game changes from Game 1-1 (Game 1-2-0) through Game 1-2-ν_1. In Game 1-2-h ($h = 1, \ldots, \nu_1$), the reply to the h-th decryption key query is changed to *semi-functional* form (Eq.(12)). There are ν_2 game changes from Game 1-2-ν_1 (Game 1-3-0) through Game 1-3-ν_2. In Game 1-3-ℓ ($\ell = 1, \ldots, \nu_2$), the reply to the ℓ-th re-encryption key query is changed to *semi-functional* form (Eq.(13)). There are ν_3 game changes from Game 1-3-ν_2 (Game 1-4-0) through Game 1-4-ν_3. In Game 1-4-t ($t = 1, \ldots, \nu_3$), the reply to the t-th re-encrypted ciphertext query is changed to *semi-functional* form (Eq.(14)). In Game 1-5, $\boldsymbol{c}$ of the challenge ciphertext is changed to random form in Eq.(15).

Then, in Game 1-6, replies to all the decryption key, re-encryption key and re-encrypted ciphertext queries are changed to a form, which is normal except for component $\boldsymbol{c}$ of the challenge, and the game is a preparation for the Game 2 sequence. In the Game 2 sequence, $\boldsymbol{c}_{\mathsf{ran}}$ is changed to random form in Eq.(16) by proceeding similar to game transformations in the Game 1 sequence. In the final Game 2-5, the advantage of the adversary is zero.

As Figure 3 shows, the advantage gap between Game 0 and Game 1-1 is bounded by the advantage of Problem 1. The advantage gaps between Games 1-2-$(h-1)$ and 1-2-h (resp. 2-2-$(h-1)$ and 2-2-h) are bounded by the advantage of Problem 2. The advantage gaps between Games 1-3-$(\ell-1)$ and 1-3-ℓ (resp. Games 2-3-$(\ell-1)$ and 2-3-ℓ) are bounded by the advantages of Problem 2 and the attribute-hiding security of the underlying IPE scheme. The advantage gaps between Games 1-4-$(t-1)$ and Game 1-4-t (resp. Games 2-4-$(t-1)$ and 2-4-t) are bounded by the advantages of Problems 2, 3

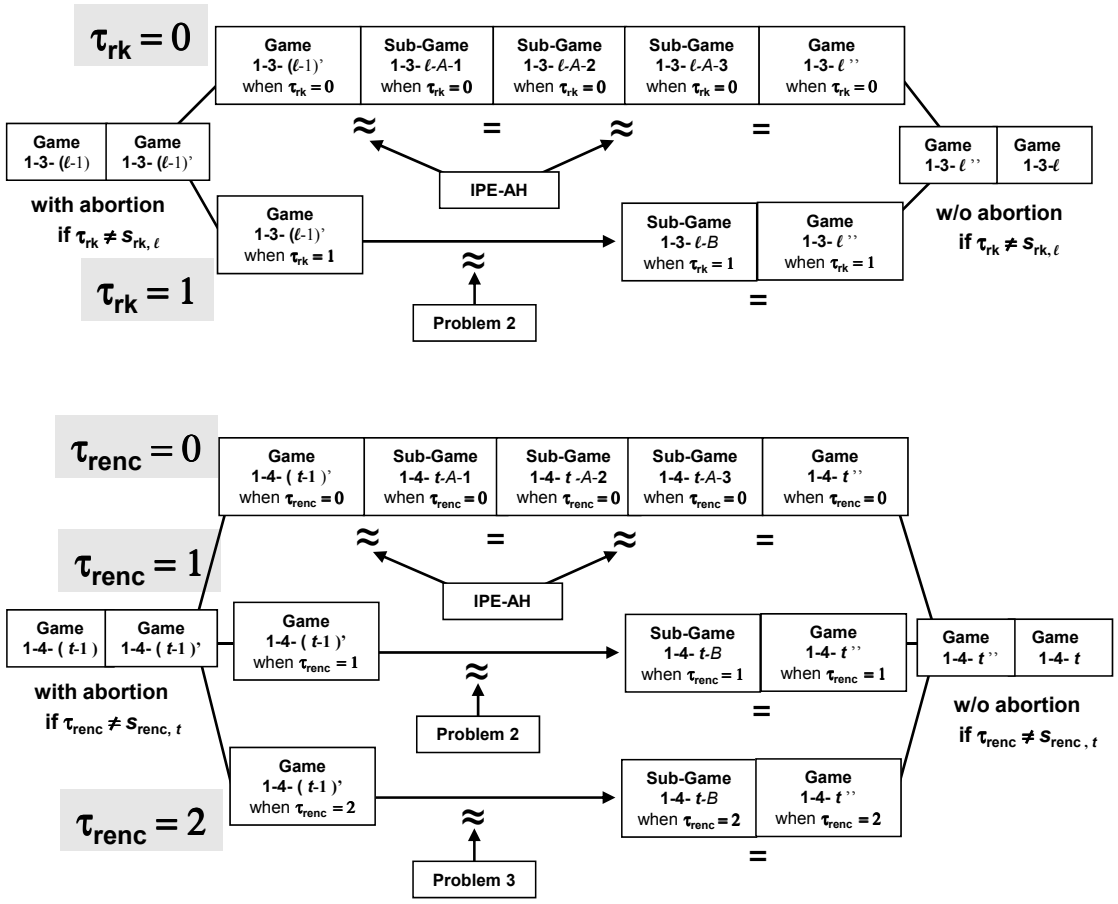

Fig. 4. Sub-Games between Games 1-3-($\ell - 1$) and 1-3-ℓ, and Games 1-4-($t - 1$) and 1-4-t

and attribute-hiding security of the underlying IPE scheme. Since the advantages of Problems 1, 2 and 3 are bounded by that of DLIN, the advantage of $\mathcal{A}$ is bounded by those of DLIN and the attribute-hiding security of the underlying IPE.

Overview of Sub-Games. We employ Sub-Games between Games 1-3-($\ell - 1$) and 1-3-ℓ, and Games 1-4-($t - 1$) and 1-4-t as described in Figure 4.

First, Game 1-3-($\ell - 1$) is changed to Game 1-3-($\ell - 1$)$'$ which is the same as Game 1-3-($\ell - 1$) except that flip a coin $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell}$ when the variable $s_{\mathsf{rk},\ell}$ is determined at the challenge step or the ℓ-th re-encryption key query step (Definition 4). Since $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$, the advantage of $\mathcal{A}$ in Game 1-3-($\ell - 1$)$'$ is a half of that in Game 1-3-($\ell - 1$).

When $\tau_{\mathsf{rk}} = 0$, we employ three intermediate sub-games, Sub-Games 1-3-ℓ-A-j ($j = 1, 2, 3$). In Game 1-3-ℓ-A-1, $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ in the reply to the ℓ-th re-encryption key query is changed to $\mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \vec{x}', R)$ where R is a random matrix in $\mathbb{F}_q^{N\times N}$. In Game 1-3-ℓ-A-2, $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ of the reply are changed to *semi-functional* forms in Eq.(13). In Game 1-3-ℓ-A-3, $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ returns back to normal $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} := \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \vec{x}', W_1)$. When $\tau_{\mathsf{rk}} = 1$, in Game 1-3-ℓ-B, $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ of the reply to the ℓ-th re-encryption key query are (directly) changed to *semi-functional* forms in Eq.(13).

Both final games, Game 1-3-ℓ-A-3 (when $\tau_{\mathsf{rk}} = 0$) and Game 1-3-ℓ-B (when $\tau_{\mathsf{rk}} = 1$) are equivalent to Game 1-3-ℓ'' which is the same as Game 1-3-ℓ except that flip a coin $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup,

and the game is aborted if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell}$ when the variable $s_{\mathsf{rk},\ell}$ is determined at the challenge step or the ℓ-th re-encryption key query step (Definition 4). Similarly to Game 1-3-$(\ell-1)'$, the advantage of $\mathcal{A}$ in Game 1-3-ℓ'' is a half of that in Game 1-3-ℓ.

As Figure 4 shows, when $\tau_{\mathsf{rk}} = 0$, the advantage gap between Games 1-3-$(\ell-1)'$ and 1-3-ℓ-A-1 (resp. 1-3-ℓ-A-2 and 1-3-ℓ-A-3) is bounded by the advantage of the attribute-hiding security of the underlying IPE scheme. Game 1-3-ℓ-A-1 (resp. 1-3-ℓ-A-3) is conceptually changed to Game 1-3-ℓ-A-2 (resp. 1-3-ℓ''). When $\tau_{\mathsf{rk}} = 1$, the advantage gap between Games 1-3-$(\ell-1)'$ and 1-3-ℓ-B is bounded by the advantage of Problem 2, and Game 1-3-ℓ-B is conceptually changed to Game 1-3-ℓ''.

For bounding the advantage gap between Games 1-4-$(t-1)$ and 1-4-t, similar Sub-Games are used (the lower diagram in Figure 4). The difference from the above is that a ternary coin $\tau_{\mathsf{renc}} \xleftarrow{\mathsf{U}} \{0,1,2\}$ is used, so, the advantage of $\mathcal{A}$ in Game 1-4-$(t-1)'$ is a third of that in Game 1-4-$(t-1)$. Here, while the gap is bounded by the advantage of Problem 2 when $\tau_{\mathsf{renc}} = 1$, the gap is bounded by that of Problem 3 when $\tau_{\mathsf{renc}} = 2$.

Proof of Lemma 8. Let ν_1 be the maximum number of $\mathcal{A}$'s decryption key queries, ν_2 be the maximum number of $\mathcal{A}$'s re-encryption key queries and ν_3 be the maximum number of $\mathcal{A}$'s re-encryption queries. To prove Lemma 8, we consider the following $2(\nu_1+\nu_2+\nu_3)+6$ games. In Game $0'$, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game $0''$: We only describe the components which are changed in the other games.

– $\boldsymbol{k}^*$ and $\boldsymbol{k}^*_{\mathsf{ran}}$ of the reply to a decryption key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ \boxed{0^n},\ \boxed{0^n},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \quad \boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{0^n},\ \boxed{0^n},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \quad (6)$$

where $\delta, \delta_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}, \vec{\eta}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$.

– $\boldsymbol{k}^{*\mathsf{rk}}$, $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ and $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ of the reply to a re-encryption key query for $(\vec{v}, \vec{x}')$ is:

$$\boldsymbol{k}^{*\mathsf{rk}} := (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ \boxed{0^n},\ \boxed{0^n},\ \vec{\eta}^{\,\mathsf{rk}},\ 0\ )_{\mathbb{D}_1^*},\ \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\ 0,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{0^n},\ \boxed{0^n},\ \vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{D}_1^*}, (7)$$

where $\delta^{\mathsf{rk}}, \delta^{\mathsf{rk}}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}^{\,\mathsf{rk}}, \vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$ and $\mathbb{D}_1^* := \mathbb{B}^* W_1$.

– $\boldsymbol{k}^{*\mathsf{renc}}$ and $\mathsf{ct}^{\mathsf{renc}}_{\vec{x}'}$ of the reply to a re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} = (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), S, \mathsf{verk}))$ is $\perp$ if $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$. Otherwise, the reply is:

$$\boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ \boxed{0^n},\ \boxed{0^n},\ \vec{\eta}^{\,\mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*}, \quad (8)$$

where $\delta^{\mathsf{renc}}, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}^{\,\mathsf{renc}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$ and $\mathbb{D}_1^* := \mathbb{B}^* W_1$.

– The reply to a challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$, $\mathsf{oct}^{(b)} := (C, \mathsf{verk}^{\clubsuit}, S)$, is given as:

$$\boldsymbol{c} := (\ \boxed{\zeta},\ \boxed{\omega\vec{x}^{(b)}},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{0^n},\ \boxed{0^n},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \quad (9)$$

$$\boldsymbol{c}_{\mathsf{ran}} := (\ 0,\ \boxed{\omega_{\mathsf{ran}}\vec{x}^{(b)}},\ \rho_{\mathsf{ran}}(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{0^n},\ 0^n,\ 0^n,\ \varphi_{\mathsf{ran}}\ )_{\mathbb{B}}, \quad (10)$$

$c_T := g_T^{\zeta}$, $C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T)$, $S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}^{\clubsuit}, C, c_T))$ where $b \xleftarrow{\mathsf{U}} \{0,1\}$, $\zeta, \omega, \omega_{\mathsf{ran}}, \rho, \rho_{\mathsf{ran}}, \varphi, \varphi_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $(\mathsf{sigk}^{\clubsuit}, \mathsf{verk}^{\clubsuit}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$.

Game 1-1: Game 1-1 is the same as Game 0″ except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is

$$\boldsymbol{c} := (\ \zeta,\ \omega\vec{x}^{(b)},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{\vec{u}},\ 0^n,\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{11}$$

where $\vec{u} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 0″.

Game 1-2-h ($h = 1, \ldots, \nu_1$): Game 1-2-0 is Game 1-1. Game 1-2-h is the same as Game 1-2-$(h-1)$ except that the reply to the h-th decryption key query for $\vec{v}$ is

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ \boxed{\vec{r}},\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \quad \boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{\vec{r}_{\mathsf{ran}}},\ 0^n,\ \vec{\eta}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*}, \tag{12}$$

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

Game 1-3-ℓ ($\ell = 1, \ldots, \nu_2$): Game 1-3-0 is Game 1-2-ν_1. Game 1-3-ℓ is the same as Game 1-3-$(\ell-1)$ except that the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x})$ is as follow:

$$\boldsymbol{k}^{*\mathsf{rk}} := (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ \boxed{\vec{r}\,'},\ 0^n,\ \vec{\eta}^{\,\mathsf{rk}},\ 0\ )_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\ 0,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{\vec{r}\,'_{\mathsf{ran}}},\ 0^n,\ \vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{D}_1^*}, \tag{13}$$

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

Game 1-4-t ($t = 1, \ldots, \nu_3$): Game 1-4-0 is Game 1-3-ν_2. Game 1-4-t is the same as Game 1-4-$(t-1)$ except that the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} = (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}, S))$ is, if $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$,

$$\boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ \boxed{\vec{r}\,''},\ 0^n,\ \vec{\eta}^{\,\mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*}, \tag{14}$$

where $\vec{r}\,'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 1-4-$(t-1)$.

Game 1-5: Game 1-5 is the same as Game 1-4-ν_3 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is:

$$\boldsymbol{c} := (\ \boxed{\zeta'},\ \boxed{\vec{u}'},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \vec{u},\ \boxed{\vec{u}''},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{15}$$

where $\zeta' \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{u}', \vec{u}'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 1-4-ν_3.

Game 1-6: Game 1-6 is the same as Game 1-5 except that the reply to every decryption key query for $\vec{v}$ is

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ \boxed{0^n,\ \vec{\pi}},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \quad \boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{0^n,\ \vec{\pi}_{\mathsf{ran}}},\ \vec{\eta}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*},$$

where $\vec{\pi}, \vec{\pi}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and the reply to every re-encryption key query for $(\vec{v}, \vec{x})$ is

$$\boldsymbol{k}^{*\mathsf{rk}} := (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ \boxed{0^n,\ \vec{\pi}\,'},\ \vec{\eta}^{\,\mathsf{rk}},\ 0\ )_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\ 0,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{0^n,\ \vec{\pi}\,'_{\mathsf{ran}}},\ \vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{D}_1^*},$$

where $\vec{\pi}\,', \vec{\pi}\,'_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and the reply to every re-encryption query for $(\vec{x}', \mathsf{oct}_{\vec{x}} = (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), S, \mathsf{verk}))$ is, if $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$,

$$\boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ \boxed{0^n,\ \vec{\pi}\,''},\ \vec{\eta}^{\,\mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*},$$

where $\vec{\pi}\,'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 1-5.

Game 2-1: Game 2-1 is the same as before Game 1-6 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is

$$\boldsymbol{c}_{\mathsf{ran}} := (\ 0,\ \omega_{\mathsf{ran}}\vec{x}^{(b)},\ \rho_{\mathsf{ran}}(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{\vec{u}_{\mathsf{ran}}},\ 0^n,\ 0^n,\ \varphi\ )_{\mathbb{B}},$$

where $\vec{u}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 1-6.

Game 2-2-h ($h = 1, \ldots, \nu_1$): Game 2-2-0 is Game 2-1. Game 2-2-h is the same as Game 2-2-$(h-1)$ except that the reply to the h-th decryption key query for $\vec{v}$, $(\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}})$, is

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ \boxed{\vec{r}},\ \vec{\pi},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \quad \boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{\vec{r}_{\mathsf{ran}}},\ \vec{\pi}_{\mathsf{ran}},\ \vec{\eta}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*},$$

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

Game 2-3-ℓ ($\ell = 1, \ldots, \nu_2$): Game 2-3-0 is Game 2-2-ν_1. Game 2-3-ℓ is the same as Game 2-3-$(\ell-1)$ except that the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x})$, $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$, is

$$\boldsymbol{k}^{*\mathsf{rk}} := (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ \boxed{\vec{r}\,'},\ \vec{\pi}\,',\ \vec{\eta}\,'^{\,\mathsf{rk}},\ 0\ )_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\ 0,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{\vec{r}\,'_{\mathsf{ran}}},\ \vec{\pi}\,'_{\mathsf{ran}},\ \vec{\eta}\,'^{\,\mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{D}_1^*},$$

where $\vec{r}', \vec{r}'_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 2-3-$(\ell-1)$.

Game 2-4-t ($t = 1, \ldots, \nu_3$): Game 2-4-0 is Game 2-3-ν_2. Game 2-4-t is the same as Game 2-4-$(t-1)$ except that the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} = (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}, S))$, $\boldsymbol{k}^{*\mathsf{renc}}$, is, if $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$,

$$\boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ \boxed{\vec{r}\,''},\ \vec{\pi}\,'',\ \vec{\eta}\,'^{\,\mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*},$$

where $\vec{r}\,'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 2-4-$(t-1)$.

Game 2-5: Game 2-5 is the same as Game 2-4-ν_3 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is:

$$\boldsymbol{c}_{\mathsf{ran}} := (\ 0,\ \boxed{\vec{u}'},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \vec{u},\ 0^n,\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{16}$$

where $\vec{u}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 2-4-ν_3.

Let $\mathsf{Adv}^{(0'')}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(\iota\text{-}1)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(\iota\text{-}2\text{-}h)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(\iota\text{-}3\text{-}\ell)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(\iota\text{-}4\text{-}t)}_{\mathcal{A}}(\lambda)$, and $\mathsf{Adv}^{(\iota\text{-}5)}_{\mathcal{A}}(\lambda)$, be the advantages of $\mathcal{A}$ in Game $0''$, ι-1, ι-2-h, ι-3-ℓ, ι-4-t and ι-5 for $\iota = 1, 2$, respectively. We will show eight lemmas (Lemma 9-16) that evaluate the gaps between pairs of neghoboring games. From these lemmas and Lemmas 3-5, we obtain

$$\begin{aligned}
\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) &\le \left|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}1)}_{\mathcal{A}}(\lambda)\right| \\
&\quad + \sum_{\iota=1}^{2} \Big(\textstyle\sum_{h=1}^{\nu_1} \left|\mathsf{Adv}^{(\iota\text{-}2\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\iota\text{-}2\text{-}h)}_{\mathcal{A}}(\lambda)\right| + \textstyle\sum_{\ell=1}^{\nu_2} \left|\mathsf{Adv}^{(\iota\text{-}3\text{-}(\ell-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\iota\text{-}3\text{-}\ell)}_{\mathcal{A}}(\lambda)\right| \\
&\qquad + \textstyle\sum_{t=1}^{\nu_3} \left|\mathsf{Adv}^{(\iota\text{-}4\text{-}(t-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\iota\text{-}4\text{-}t)}_{\mathcal{A}}(\lambda)\right| + \left|\mathsf{Adv}^{(\iota\text{-}4\text{-}\nu_3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\iota\text{-}5)}_{\mathcal{A}}(\lambda)\right| \Big) \\
&\quad + \left|\mathsf{Adv}^{(1\text{-}5)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}6)}_{\mathcal{A}}(\lambda)\right| + \mathsf{Adv}^{(2\text{-}5)}_{\mathcal{A}}(\lambda). \\
&\le \sum_{\iota=1}^{2} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}1}}(\lambda) + \textstyle\sum_{h=1}^{\nu_1}\sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}2\text{-}h\text{-}j}}(\lambda) + \sum_{\ell=1}^{\nu_2}\sum_{j=1}^{2} \left(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}A\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}B\text{-}j}}(\lambda) \right) \\
&\qquad + \textstyle\sum_{t=1}^{\nu_3}\sum_{j=1}^{2} \left(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}A\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}B\text{-}j}}(\lambda) \right) \Big) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}6}}(\lambda) + \epsilon,
\end{aligned}$$

where $\epsilon := (14\nu_1 + 17\nu_2 + 17\nu_3 + 15)/q$. This completes the proof of Lemma 8. □

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

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

1. $\mathcal{B}_{1\text{-}1}$ is given a Problem 1 instance, $(\mathsf{param}_n, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,1}, \{\boldsymbol{e}_i\}_{i=2,\ldots,n})$.
2. $\mathcal{B}_{1\text{-}1}$ plays a role of the challenger in the security game against $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{1\text{-}1}$ generates a pair of public and secret key of the underlying IPE scheme, $(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$. $\mathcal{B}_{1\text{-}1}$ sets $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n+2}, \boldsymbol{b}_{4n+3})$ and $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_{n+1}, \boldsymbol{b}^*_{n+2}, \boldsymbol{b}^*_{3n+3}, \ldots, \boldsymbol{b}^*_{4n+2})$ and provides $\mathcal{A}$ with a public key $\mathsf{pk} := (\lambda, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \mathsf{pk}^{\mathsf{IPE}})$.
4. When a decryption key query is issued for a vector $\vec{v}$, $\mathcal{B}_{1\text{-}1}$ computes a normal form of decryption key $\mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$ using $\widehat{\mathbb{B}}^*$ of the Problem 1 instance and $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}_{\mathsf{IPE}}(\mathsf{sk}^{\mathsf{IPE}}, \vec{v})$. $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with a decryption key $\mathsf{sk}_{\vec{v}}$.
5. When a re-encryption key query is issued for $(\vec{v}, \vec{x}')$, $\mathcal{B}_{1\text{-}1}$ computes a normal form of re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1)$ using $\widehat{\mathbb{B}}^*$ of the Problem 1 instance and $\mathsf{pk}^{\mathsf{IPE}}$. $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with the re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'}$.
6. When a re-encryption query is issued for $(\vec{v}, \vec{x}', \mathsf{oct} := (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}, S))$, if $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, $\mathcal{B}_{1\text{-}1}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{B}_{1\text{-}1}$ computes a normal form of re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'} := (\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2})$ using Problem 1 instance and $\mathsf{pk}^{\mathsf{IPE}}$. $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with the re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'}$.
7. When a challenge query is issued for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$, $\mathcal{B}_{1\text{-}1}$ picks a bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ and $\zeta, \rho, \rho_{\mathsf{ran}}, \omega_{\mathsf{ran}}, \varphi_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and generates $(\mathsf{sigk}^{\clubsuit}, \mathsf{verk}^{\clubsuit}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$. Next, $\mathcal{B}_{1\text{-}1}$ computes

$$\boldsymbol{c} := \zeta \boldsymbol{b}_0 + x^{(b)}_1 \boldsymbol{e}_{\beta.1} + \sum_{i=2}^{n} x^{(b)}_i \boldsymbol{e}_i + \rho\, \mathsf{verk}^{\clubsuit} \boldsymbol{b}_{n+1} + \rho \boldsymbol{b}_{n+2},$$

$$\boldsymbol{c}_{\mathsf{ran}} := \sum_{i=1}^{n} \omega_{\mathsf{ran}} x^{(b)}_i \boldsymbol{b}_i + \rho_{\mathsf{ran}} \mathsf{verk}^{\clubsuit} \boldsymbol{b}_{n+1} + \rho_{\mathsf{ran}} \boldsymbol{b}_{n+2} + \varphi_{\mathsf{ran}} \boldsymbol{b}_{4n+3},$$

$$c_T := m^{(b)} \cdot g_T^{\zeta}, \text{ and} \qquad S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}^{\clubsuit}, (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T)).$$

   $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with a challenge ciphertext $\mathsf{oct}_{\vec{x}^{(b)}} := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T, \mathsf{verk}^{\clubsuit}, S)$.
8. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{1\text{-}1}$ outputs $\beta' := 0$. Otherwise, $\mathcal{B}_{1\text{-}1}$ outputs $\beta' := 1$.

Since the challenge ciphertext $\mathsf{oct}_{\vec{x}^{(b)}}$ is of the form Eq.(9) (resp. of the form Eq.(11)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{1\text{-}1}$ is distributed as Game $0''$ (resp. Game 1) if $\beta = 0$ (resp. $\beta = 1$). Then, $\left|\mathsf{Adv}^{(0'')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}1)}_{\mathcal{A}}(\lambda)\right| = |\mathsf{Pr}[\mathcal{B}_{1\text{-}1}(1^\lambda, \varrho) \to 1 | \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_0(1^\lambda, n)] - \mathsf{Pr}[\mathcal{B}_{1\text{-}1}(1^\lambda, \varrho) \to 1 | \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_1(1^\lambda, n)]|$ $\leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_{1\text{-}1}}(\lambda)$. This completes the proof of Lemma 9. □

Lemma 10. *For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{B}_{1\text{-}2\text{-}h\text{-}1}$ and $\mathcal{B}_{1\text{-}2\text{-}h\text{-}2}$, whose running time are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}2\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}2\text{-}h)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}2}}(\lambda) + 4/q$, where $\mathcal{B}_{1\text{-}2\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{1\text{-}2\text{-}1}(h, \cdot)$ and $\mathcal{B}_{1\text{-}2\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{1\text{-}2\text{-}2}(h, \cdot)$.*

Proof. In order to prove Lemma 10, we construct probabilistic machines $\mathcal{B}_{1\text{-}2\text{-}1}$ and $\mathcal{B}_{1\text{-}2\text{-}2}$ against Problem 2 using an adversary $\mathcal{A}$ in a security game (Game 1-2-$(h-1)$ or Game 1-2-h) as a black box.

First, we consider the intermediate game Game 1-2-h-1. Game 1-2-h-1 is the same as Game 1-2-$(h-1)$ except that $\boldsymbol{k}^*$ of the reply to h-th decryption key query is of *semi-functional form* in Eq.(12). Also, $\boldsymbol{k}^*_{\mathsf{ran}}$ is the normal form Eq.(6). In order to prove that $|\mathsf{Adv}^{(\text{1-2-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\text{1-2-}h\text{-1})}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-2-}h\text{-1}}}(\lambda) + 2/q$, we construct a probabilistic machine $\mathcal{B}_{\text{1-2-1}}$ with an index h against Problem 2 using an adversary $\mathcal{A}$ in a security game (Game 1-2-$(h-1)$ or Game 1-2-h-1) as a black box as follows:

1. $\mathcal{B}_{\text{1-2-1}}$ is given an index h and a Problem 2 instance, $(\mathsf{param}_n, \mathbb{B}^*, \widehat{\mathbb{B}}, \{\boldsymbol{h}_{\beta,i}\}_{i=1,\ldots,n}, \{\boldsymbol{e}_i\}_{i=1,\ldots,n})$.
2. $\mathcal{B}_{\text{1-2-1}}$ plays a role of the challenger in the security game against $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_1$ generates a pair of public and secret key of the underlying IPE scheme, $(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$. $\mathcal{B}_1$ sets $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n+2}, \boldsymbol{b}_{4n+3})$ and $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_{n+1}, \boldsymbol{b}^*_{n+2}, \boldsymbol{b}^*_{3n+3}, \ldots, \boldsymbol{b}^*_{4n+2})$ and provides $\mathcal{A}$ with a public key $\mathsf{pk} := (\lambda, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \mathsf{pk}^{\mathsf{IPE}})$.
4. When the j-th decryption key query is issued for a vector $\vec{v}$, $\mathcal{B}_{\text{1-2-1}}$ computes $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}_{\mathsf{IPE}}(\mathsf{sk}^{\mathsf{IPE}}, \vec{v})$ and normal form $\boldsymbol{k}^*_{\mathsf{ran}}$ using $\mathbb{B}^*$ of the Problem 2 instance,
   - in the case of $j < h$, $\mathcal{B}_{\text{1-2-1}}$ computes semi-functional form $\boldsymbol{k}^*$ in Eq.(12) using $\mathbb{B}^*$ of the Problem 2 instance.
   - in the case of $j = h$, $\mathcal{B}_{\text{1-2-1}}$ chooses $\pi_i, u_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, n$,

$$\boldsymbol{k}^* := \boldsymbol{b}^*_0 + \sum_{i=1}^{n} v_i \pi_i \boldsymbol{h}^*_{\beta,i} + \sum_{i=1}^{n} u_i \boldsymbol{b}^*_{3n+2+i}$$

     using the Problem 2 instance where $\vec{v} := (v_1, \ldots, v_n)$.
   - in the case of $j > h$, $\mathcal{B}_{\text{1-2-1}}$ computes a normal form $\boldsymbol{k}^*$ in Eq.(6) using $\mathbb{B}^*$ of the Problem 2 instance.

   $\mathcal{B}_{\text{1-2-1}}$ provides $\mathcal{A}$ with a decryption key $\mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$.
5. When a re-encryption key query is issued for $(\vec{v}, \vec{x}')$, $\mathcal{B}_{\text{1-2-1}}$ computes a normal form of re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1)$ using $\mathbb{B}^*$ of the Problem 2 instance and $\mathsf{pk}^{\mathsf{IPE}}$. $\mathcal{B}_{\text{1-2-1}}$ provides $\mathcal{A}$ with a re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'}$.
6. When a re-encryption query is issued for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} := (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}, S))$, if $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, $\mathcal{B}_{\text{1-2-1}}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{B}_{\text{1-2-1}}$ computes a normal form of re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'} := (\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2})$ using Problem 2 instance and $\mathsf{pk}^{\mathsf{IPE}}$. $\mathcal{B}_{\text{1-2-1}}$ provides $\mathcal{A}$ with the re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'}$.
7. When a challenge query is issued for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$, $\mathcal{B}_{\text{1-2-1}}$ picks a bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ and $\zeta, \rho, \omega_{\mathsf{ran}}, \rho_{\mathsf{ran}}, \varphi_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and generates $(\mathsf{sigk}^{\clubsuit}, \mathsf{verk}^{\clubsuit}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$. Next, $\mathcal{B}_{\text{1-2-1}}$ computes

$$\begin{aligned}
\boldsymbol{c} &:= \zeta \boldsymbol{b}_0 + \sum_{i=1}^{n} x^{(b)}_i \boldsymbol{e}_i + \rho\ \mathsf{verk}^{\clubsuit} \boldsymbol{b}_{n+1} + \rho \boldsymbol{b}_{n+2}, \\
\boldsymbol{c}_{\mathsf{ran}} &:= \sum_{i=1}^{n} \omega_{\mathsf{ran}} x^{(b)}_i \boldsymbol{b}_i + \rho_{\mathsf{ran}}\ \mathsf{verk}^{\clubsuit} \boldsymbol{b}_{n+1} + \rho_{\mathsf{ran}} \boldsymbol{b}_{n+2} + \varphi_{\mathsf{ran}} \boldsymbol{b}_{4n+3}, \\
c_T &:= m^{(b)} \cdot g_T^{\zeta}, \quad C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \quad S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}^{\clubsuit}, C).
\end{aligned}$$

   $\mathcal{B}_{\text{1-2-1}}$ provides $\mathcal{A}$ with a challenge ciphertext $\mathsf{oct}_{x^{(b)}} := (C, \mathsf{verk}^{\clubsuit}, S)$.
8. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{\text{1-2-1}}$ outputs $\beta' := 0$. Otherwise, $\mathcal{B}_{\text{1-2-1}}$ outputs $\beta' := 1$.

Since $\boldsymbol{k}^*$ of the h-th decryption key is of the form Eq.(6) (resp. of the form Eq.(12)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{\text{1-2-1}}$ is distributed as Game 1-2-$(h-1)$ (resp. Game 1-2-h-1) if $\beta = 0$ (resp. $\beta = 1$) except that δ defined in Problem 2 is zero i.e., except for probability $1/q$ (resp.

$1/q$).
Then, $\left|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}2\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}2\text{-}h\text{-}1)}(\lambda)\right| = \left|\mathsf{Pr}\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P2}}(1^\lambda, n)\right]\right.$
$\left. - \mathsf{Pr}\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P2}}(1^\lambda, n)\right]\right| + 2/q \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}1}}(\lambda) + 2/q.$ □

Next, in order to prove that $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}2\text{-}h\text{-}2)}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}2}}(\lambda) + 2/q$, we construct a probabilistic machine $\mathcal{B}_{1\text{-}2\text{-}h\text{-}2}$ against Problem 2 using an adversary $\mathcal{A}$ in a security game (Game 1-2-h-1 or Game 1-2-h-2) as a black box. Game 1-2-h-2 is the same as Game 1-2-h-1 except that $\boldsymbol{k}^*_{\mathsf{ran}}$ of the reply to the h-th decryption key query is *semi-functional form* in Eq.(12). That is, Game 1-2-h-2 is Game 1-2-h. Hence, this proof is similar to the above proof. So, we have $\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}2\text{-}h\text{-}2)}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}2}}(\lambda) + 2/q$

By the hybrid argument, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}2\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}2\text{-}h)}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}2}}(\lambda) + 4/q$.
□

Lemma 11. *For any adversary $\mathcal{A}$, there exists probabilistic machines $\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}\iota}$ and $\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}\iota}$ ($\iota = 1, 2$), whose running time are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}3\text{-}(\ell-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}3\text{-}\ell)}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}2}}(\lambda) + 7/q$, where $\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}\iota}(\cdot) := \mathcal{B}_{1\text{-}3\text{-}A\text{-}\iota}(\ell, \cdot)$ and $\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}\iota}(\cdot) := \mathcal{B}_{1\text{-}3\text{-}B\text{-}\iota}(\ell, \cdot)$ for $\iota = 1, 2$.*

Proof. First, we execute a preliminary game transformation from Game 1-3-($\ell - 1$) to Game 1-3-($\ell - 1$)′, which is the same as Game 1-3-($\ell - 1$) except that flip a coin $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0, 1\}$ before setup, and the game is aborted when the variable $s_{\mathsf{rk},\ell}$ is determined (Definition 5) if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell}$. Since $s_{\mathsf{rk},\ell} := 0$ if $\vec{v}_\ell \cdot \vec{x}^{(0)} \neq 0 \wedge \vec{v}_\ell \cdot \vec{x}^{(1)} \neq 0$, $s_{\mathsf{rk},\ell}$ is determined at the challenge step if the ℓ-th re-encryption key query is asked in Phase 1, and at the ℓ-th re-encryption key query step if it is asked in Phase 2. We define that $\mathcal{A}$ wins with probability 1/2 when the game is aborted (and the advantage in Game 1-3-($\ell - 1$)′ is $\mathsf{Pr}[\mathcal{A}$ wins in Game 1-3-($\ell - 1$)′] − 1/2 as well). Since τ_{rk} is independent from $s_{\mathsf{rk},\ell}$, the game is aborted with probability 1/2. Hence, the advantage in Game 1-3-($\ell - 1$)′ is a half of that in Game 1-3-($\ell - 1$), i.e., $\mathsf{Adv}_{\mathcal{A}}^{1\text{-}3\text{-}(\ell-1)'}(\lambda) = 1/2 \cdot \mathsf{Adv}_{\mathcal{A}}^{1\text{-}3\text{-}(\ell-1)}(\lambda)$. Moreover, $\Pr[\mathcal{A}$ wins in Game 1-3-($\ell - 1$)′] = $\frac{1}{2}$ ($\Pr[\mathcal{A}$ wins in Game 1-3-($\ell - 1$)′ | $\tau_{\mathsf{rk}} = 0$] + $\Pr[\mathcal{A}$ wins in Game 1-3-($\ell - 1$)′ | $\tau_{\mathsf{rk}} = 1$]), since τ_{rk} is uniformly and independently generated. Therefore,

$$\begin{aligned}&\mathsf{Adv}_{\mathcal{A}}^{1\text{-}3\text{-}(\ell-1)}(\lambda) = 2 \cdot \mathsf{Adv}_{\mathcal{A}}^{1\text{-}3\text{-}(\ell-1)'}(\lambda)\\ &= \Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \,|\, \tau_{\mathsf{rk}} = 0] + \Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \,|\, \tau_{\mathsf{rk}} = 1] - 1. \quad (17)\end{aligned}$$

Similarly, we define a new game, Game 1-3-ℓ'', which is the same as Game 1-3-ℓ except that flip a coin $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0, 1\}$ before setup, and the game is aborted when the variable $s_{\mathsf{rk},\ell}$ is determined if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell}$. Note that Game 1-3-$\ell'$ aborts if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell+1}$, which is different from Game 1-3-ℓ''. Similarly to Eq. (17),

$$\begin{aligned}&\mathsf{Adv}_{\mathcal{A}}^{1\text{-}3\text{-}\ell}(\lambda) = 2 \cdot \mathsf{Adv}_{\mathcal{A}}^{1\text{-}3\text{-}\ell''}(\lambda)\\ &= \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \,|\, \tau_{\mathsf{rk}} = 0] + \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \,|\, \tau_{\mathsf{rk}} = 1] - 1. \quad (18)\end{aligned}$$

Case $\tau_{\mathsf{rk}} = 0$ As for the conditional probability with $\tau_{\mathsf{rk}} = 0$, we introduce three games as:

Sub-Game 1-3-ℓ-A-1**:** When $\tau_{\mathsf{rk}} = 0$, Sub-Game 1-3-ℓ-A-1 is the same as Game 1-3-($\ell - 1$)′ except that the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x}')$ are

$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{R}), \quad (19)$$

where $R \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q), \vec{r}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 1-3-$(\ell-1)'$.

Sub-Game 1-3-ℓ-A-2**:** When $\tau_{\mathsf{rk}} = 0$, Sub-Game 1-3-ℓ-A-2 is the same as Sub-Game 1-3-ℓ-A-1 except that $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$ of the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x}')$ are of semi-functional form as given in Eq.(13).

Sub-Game 1-3-ℓ-A-3**:** When $\tau_{\mathsf{rk}} = 0$, Sub-Game 1-3-ℓ-A-3 is the same as Sub-Game 1-3-ℓ-A-2 except that $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ of the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x}')$ is

$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{W_1}), \tag{20}$$

where $W_1 \in GL(4n+4, \mathbb{F}_q)$ is defined in Game 0'' and it satisfies that $\mathbb{D}_1^* := \mathbb{B}^* W_1$ and all the other variables are generated as in Sub-Game 1-3-ℓ-A-2. Note that Sub-Game 1-3-ℓ-A-3 is the same as Game 1-3-ℓ'' when $\tau_{\mathsf{rk}} = 0$.

From Claims 1, 2, and 3,

$$\begin{aligned}
&\big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 0]\big| \\
&\le \big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-1} \mid \tau_{\mathsf{rk}} = 0]\big| \\
&\quad + |\Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-1} \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-2} \mid \tau_{\mathsf{rk}} = 0]| \\
&\quad + |\Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-2} \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-3} \mid \tau_{\mathsf{rk}} = 0]| \\
&\le \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}2}}(\lambda) + 3/q.
\end{aligned} \tag{21}$$

Case $\tau_{\mathsf{rk}} = 1$ As for the conditional probability with $\tau_{\mathsf{rk}} = 1$, we introduce a game as:

Sub-Game 1-3-ℓ-B**:** When $\tau_{\mathsf{rk}} = 1$, Sub-Game 1-3-ℓ-B is the same as Game 1-3-$(\ell-1)'$ except that $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$ of the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x}')$ is of semi-functional form as given in Eq.(13). Note that Sub-Game 1-3-ℓ-B is the same as Game 1-3-ℓ'' when $\tau_{\mathsf{rk}} = 1$.

From Claim 4,

$$\begin{aligned}
&\big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 1]\big| \\
&= \big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}B \mid \tau_{\mathsf{rk}} = 1]\big| \\
&\le \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}2}}(\lambda) + 4/q.
\end{aligned} \tag{22}$$

Therefore, from Eqs. (17), (18), (21), and (22),

$$\begin{aligned}
&|\mathsf{Adv}^{1\text{-}3\text{-}(\ell-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{1\text{-}3\text{-}\ell}_{\mathcal{A}}(\lambda)| \\
&= |\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] + \Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - 1 \\
&\quad - \big(\Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 0] + \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 1] - 1\big)\big| \\
&= |\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 0] \\
&\quad + \Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 1]\big| \\
&\le \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}2}}(\lambda) + 7/q.
\end{aligned}$$

This completes the proof of Lemma 11. □

Claim 1 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,*
$|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-3-}\ell\text{-}A\text{-1} \mid \tau_{\mathsf{rk}} = 0]| \le \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}1}}(\lambda) + 1/q$, *where* $\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}1}(\cdot) := \mathcal{B}_{1\text{-}3\text{-}A\text{-}1}(\ell, \cdot)$.

Proof. In order to prove Claim 1, we construct a probabilistic machine $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ against the attribute-hiding security of the underlying IPE scheme using an adversary $\mathcal{A}$ in a security game (Game 1-3-$(\ell-1)'$ or Sub-Game 1-3-ℓ-A-1) as a black box as follows:

1. $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ is given an index ℓ and a public key of the IPE, $\mathsf{pk}^{\mathsf{IPE}}$, from the challenger for the IPE attribute-hiding security.
2. $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ plays a role of the challenger in the security game against $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ generates $(\mathsf{param}_n, \mathbb{B} = (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{4n+3}), \mathbb{B}^* = (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_{4n+3})) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4)$, and sets $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n+2}, \boldsymbol{b}_{4n+3})$ and $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_{n+1}, \boldsymbol{b}^*_{n+2}, \boldsymbol{b}^*_{3n+3}, \ldots, \boldsymbol{b}^*_{4n+2})$. $\mathcal{B}_1$ then provides $\mathcal{A}$ with a public key $\mathsf{pk} := (1^\lambda, \mathsf{pk}^{\mathsf{IPE}}, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$.
4. When a decryption key query is issued for a vector $\vec{v}$, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ computes a semi-functional form $(\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}})$ in Eq.(12), by using $\mathbb{B}^*$ and ask a key query $\vec{v}$ to the challenger of the underlying IPE, then obtain the decryption key $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}}$, and provides $\mathcal{A}$ with a decryption key $\mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$.
5. When the j-th re-encryption key query is issued for $(\vec{v}, \vec{x}')$, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ computes as follows:
   - When $j < \ell$, using $\mathbb{B}^*$ and $W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ computes a semi-functional form $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1)$, where $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$ are given in Eq.(13), and $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ sends $\mathsf{rk}_{\vec{v},\vec{x}'}$ to $\mathcal{A}$.
   - When $j = \ell$, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ generates $X^{(0)} := W_1, X^{(1)} := R \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$, and sends a challenge query to the challenger of the IPE scheme with $(\vec{x}^{(0)} := \vec{x}^{(1)} := \vec{x}', X^{(0)}, X^{(1)})$, receives a reply $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$. $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ then computes $\mathsf{prect}_{\vec{x}'}$ by himself. Using $\mathbb{B}^*$ and W_1, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ computes a normal form $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$, which are given in Eq.(7), and $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ sends $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1)$ to $\mathcal{A}$.
   - When $j > \ell$, using $\mathbb{B}^*$ and $W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ computes a normal form $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1)$, where $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$ are given in Eq.(7), and $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ sends $\mathsf{rk}_{\vec{v},\vec{x}'}$ to $\mathcal{A}$.
6. When a re-encryption query is issued for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} := (C, \mathsf{verk}, S))$, if $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ computes a re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'} := (\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \{\mathsf{ct}^{i,\mathsf{renc}}_{\vec{x}'}\}_{i=1,2})$ as in Definition 5. The re-encrypted ciphertext, $\mathsf{rct}_{\vec{x}'}$, is calculated by using $(\mathbb{B}, \mathbb{B}^*)$ which is given at setup since it does not include a key component of the underlying IPE scheme. $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ provides $\mathcal{A}$ with $\mathsf{rct}_{\vec{x}'}$.
7. When the challenge query is issued for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$, $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ calculates the challenge ciphertext as in Definition 5, and sends it to $\mathcal{A}$.
8. $\mathcal{A}$ finally outputs bit b. $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ then outputs b to the challenger for the IPE attribute-hiding security game.

Since $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ of the ℓ-th re-encryption key is of the form Eq.(20) (resp. of the form Eq.(19)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{1\text{-}3\text{-}A\text{-}1}$ is distributed as Game 1-3-$(\ell-1)'$ (resp. Sub-Game 1-3-ℓ-A-1) if $\beta = 0$ (resp. $\beta = 1$). Then, $|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-3-}\ell\text{-}A\text{-1} \mid \tau_{\mathsf{rk}} = 1]| \leq \mathsf{Adv}^{\mathsf{IPE},\mathsf{AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}1}}(\lambda) + 1/q$,. □

Claim 2 *For any adversary $\mathcal{A}$,*
$|\Pr[\mathcal{A} \text{ wins in Sub-Game1-3-}\ell\text{-}A\text{-1} \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-3-}\ell\text{-}A\text{-2} \mid \tau_{\mathsf{rk}} = 0]| \leq 1/q$.

Proof. To prove Claim 2, we will show distribution $(\mathsf{pk}, \{\mathsf{sk}_{\vec{v}}\}, \{\mathsf{rk}_{\vec{v},\vec{x}'}\}, \{\mathsf{rct}_{\vec{x}'}\}, \mathsf{oct}_{\vec{x}^{(b)}})$ in Game 3-ℓ and Sub-Game 3-ℓ-A-1 are equivalent. In this proof, since we change to the component $\boldsymbol{k}^{*\mathsf{rk}}_0$ of the ℓ-th re-encryption key using the base $\mathbb{D}^*_1$ in Sub-Game 3-ℓ-A-1, we focus the only components $\mathbb{D}^*_1$.

Note that there does not exist the component using $\mathbb{D}_1$ which is the dual base of $\mathbb{D}_1^*$. We define new basis $\mathbb{U}^*$ of $\mathbb{V}$ as follows; We chooses $\vec{r} := (r_1, \ldots, r_n), \vec{r}' := (r'_1, \ldots, r'_n) \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, and set

$$\boldsymbol{u}_0^* := \boldsymbol{d}_0^* - \textstyle\sum_{i=1}^n r_i \boldsymbol{d}_{n+2+i}^*, \quad \boldsymbol{u}_n^* := \boldsymbol{d}_n^* - \textstyle\sum_{i=1}^n r'_i \boldsymbol{d}_{n+2+i}^*.$$

We set $\mathbb{U}^* := (\boldsymbol{u}_0^*, \boldsymbol{d}_1^*, \ldots, \boldsymbol{d}_{n-1}^*, \boldsymbol{u}_n^*, \boldsymbol{d}_{n+1}^*, \ldots, \boldsymbol{d}_{4n+3}^*)$. The components of ℓ-th re-encryption key, $(\boldsymbol{k}_0^{*\mathsf{rk}}, \boldsymbol{k}_1^{*\mathsf{rk}})$ in Sub-Game 3-ℓ-A-1 are expressed over base $\mathbb{D}_1^*$.

$$\begin{aligned}
\boldsymbol{k}^{*\mathsf{rk}} &= (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ 0^n,\ 0^n,\ \vec{\eta}^{\ \mathsf{rk}},\ 0)_{\mathbb{D}_1^*} = (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ \vec{r},\ 0^n,\ \vec{\eta}^{\ \mathsf{rk}},\ 0)_{\mathbb{U}^*} \\
\boldsymbol{k}_{\mathsf{ran}}^{*\mathsf{rk}} &= (\ 0,\ \delta_{\mathsf{ran}}^{\mathsf{rk}}\vec{v},\ 0^2,\ 0^n,\ 0^n,\ \vec{\eta}_{\mathsf{ran}}^{\ \mathsf{rk}},\ 0)_{\mathbb{D}_1^*} = (\ 0,\ \delta_{\mathsf{ran}}^{\mathsf{rk}}\vec{v},\ 0^2,\ \delta_{\mathsf{ran}}^{\mathsf{rk}} v_n \vec{r}',\ 0^n,\ \vec{\eta}_{\mathsf{ran}}^{\ \mathsf{rk}},\ 0)_{\mathbb{U}^*},
\end{aligned}$$

where $\vec{r}, \delta_{\mathsf{ran}}^{\mathsf{rk}} v_n \vec{r}'$ are uniformly and independently distributed except that $\delta_{\mathsf{ran}}^{\mathsf{rk}} = 0$, i.e., except for probability $1/q$ since $v_n \neq 0$. Thus, Sub-Game 1-3-ℓ-A-1 can be conceptually changed to Sub-Game 1-3-ℓ-A-2 except for probability $1/q$. □

Claim 3 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{3\text{-}A\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,*
$|\Pr[\mathcal{A} \text{ wins in Sub-Game 1-3-}\ell\text{-}A\text{-2} \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-3-}\ell\text{-}A\text{-3} \mid \tau_{\mathsf{rk}} = 0]| \leq$
$\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}2}}(\lambda) + 1/q$, *where* $\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}2}(\cdot) := \mathcal{B}_{1\text{-}3\text{-}A\text{-}2}(\ell, \cdot)$.

Proof. The game change between Sub-Game 1-3-ℓ-A-2 and Sub-Game 1-3-ℓ-A-3 is the reverse of that between Game 1-3-$(\ell-1)'$ and Sub-Game 1-3-ℓ-A-1 (except the form of the ℓ-th re-encryption key $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}_{\mathsf{ran}}^{*\mathsf{rk}})$). Therefore, Claim 3 is proven in a similar manner to Claim 1. □

Claim 4 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}3\text{-}B}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,*
$|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-3-}\ell\text{-}B \mid \tau_{\mathsf{rk}} = 1]| \leq$
$\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}2}}(\lambda) + 4/q$, *where* $\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}\iota}(\cdot) := \mathcal{B}_{1\text{-}3\text{-}B}(\ell, \cdot)$ *for* $\iota = 1, 2$.

Proof. When $\tau_{\mathsf{rk}} = 1$, only when $\vec{v} \cdot \vec{x}^{(0)} \neq 0$ and $\vec{v} \cdot \vec{x}^{(1)} \neq 0$, the game is not aborted by the challenger. Then, the left hand side of the inequality in Claim 4 is related to the case $\vec{v} \cdot \vec{x}^{(0)} \neq 0$ and $\vec{v} \cdot \vec{x}^{(1)} \neq 0$. Hence, this claim is proven in a similar manner to that of Lemma 10. □

Lemma 12. *For any adversary $\mathcal{A}$, there exists probabilistic machines $\mathcal{B}_{1\text{-}4\text{-}t\text{-}A}$ and $\mathcal{B}_{1\text{-}4\text{-}t\text{-}B}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,*
$|\mathsf{Adv}^{(1\text{-}4\text{-}(t-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}4\text{-}t)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}4\text{-}t\text{-}A\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}4\text{-}t\text{-}A\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}4\text{-}t\text{-}B\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{1\text{-}4\text{-}t\text{-}B\text{-}2}}(\lambda) +$
$7/q$, *where* $\mathcal{B}_{1\text{-}4\text{-}t\text{-}A\text{-}\iota}(\cdot) := \mathcal{B}_{\mathcal{B}_{1\text{-}4\text{-}A\text{-}\iota}}(t, \cdot)$ *and* $\mathcal{B}_{1\text{-}4\text{-}t\text{-}B\text{-}\iota}(\cdot) := \mathcal{B}_{\mathcal{B}_{1\text{-}4\text{-}B\text{-}\iota}}(t, \cdot)$ *for* $\iota = 1, 2$.

Proof. First, we execute a preliminary game transformation from Game 1-4-$(t-1)$ to Game 1-4-$(t-1)'$, which is the same as Game 1-4-$(t-1)$ except that flip a coin $\tau_{\mathsf{renc}} \xleftarrow{\mathsf{U}} \{0, 1, 2\}$ before setup, and the game is aborted when the variable $s_{\mathsf{renc},t}$ is determined (Definition 5) if $\tau_{\mathsf{renc}} \neq s_{\mathsf{renc},t}$. Since $s_{\mathsf{renc},t}$ is defined by $\vec{v}_t, \vec{x}^{(0)}, \vec{x}^{(1)}, \mathsf{oct}_t, \mathsf{oct}_{\vec{x}^{(b)}}$, the value of $s_{\mathsf{renc},t}$ is determined at the t-th re-encryption query step if it is asked in Phase 2. We define that $\mathcal{A}$ wins with probability $1/2$ when the game is aborted (and the advantage in Game 1-4-$(t-1)'$ is $\mathsf{Pr}[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \,] - 1/2$ as well). Since τ_{renc} is independent from $s_{\mathsf{renc},t}$, the game is aborted with probability $2/3$. Hence, the advantage in Game 1-4-$(t-1)'$ is a third of that in Game 1-4-$(t-1)$, i.e., $\mathsf{Adv}^{1\text{-}4\text{-}(t-1)'}_{\mathcal{A}}(\lambda) = 1/3 \cdot \mathsf{Adv}^{1\text{-}4\text{-}(t-1)}_{\mathcal{A}}(\lambda)$.

Moreover, $\Pr[\mathcal{A}\text{ wins in Game 1-4-}(t-1)'] = \frac{1}{3}\sum_{\iota=0}^{2}\Pr[\mathcal{A}\text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = \iota]$ since τ_{renc} is uniformly and independently generated. Therefore,

$$\begin{aligned}\mathsf{Adv}^{\text{1-4-}(t-1)}_{\mathcal{A}}(\lambda) &= 3 \cdot \mathsf{Adv}^{\text{1-4-}(t-1)'}_{\mathcal{A}}(\lambda) \\ &= \sum_{\iota=0}^{2}\Pr[\mathcal{A}\text{ wins in Game 1-4-}(t-1)' \,|\, \tau_{\mathsf{renc}} = \iota] - 3/2. \end{aligned} \tag{23}$$

Similarly, we define a new game, Game 1-4-t'', which is the same as Game 1-4-t except that flip a coin $\tau_{\mathsf{renc}} \xleftarrow{\mathsf{U}} \{0,1,2\}$ before setup, and the game is aborted when the variable $s_{\mathsf{renc},t}$ is determined if $\tau_{\mathsf{renc}} \neq s_{\mathsf{renc},t}$. Note that Game 1-4-$t'$ aborts if $\tau_{\mathsf{renc}} \neq s_{\mathsf{renc},t+1}$, which is different from Game 1-4-t''. Similarly to Eq. (23),

$$\mathsf{Adv}^{\text{1-4-}(t-1)}_{\mathcal{A}}(\lambda) = 3 \cdot \mathsf{Adv}^{\text{1-4-}t''}_{\mathcal{A}}(\lambda) \ = \sum_{\iota=0}^{2}\Pr[\mathcal{A}\text{ wins in Game 1-4-}t'' \,|\, \tau_{\mathsf{renc}} = \iota] - 3/2. \tag{24}$$

Case $\tau_{\mathsf{renc}} = 0$ As for the conditional probability with $\tau_{\mathsf{renc}} = 0$, we introduce three games as:

Sub-Game 1-4-t-A-1**:** When $\tau_{\mathsf{renc}} = 0$, Sub-Game 1-4-t-A-1 is the same as Game 1-4-$(t-1)'$ except that the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct})$ are

$$\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{R}),$$

where $R \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$ and all the other variables are generated as in Game 1-4-$(t-1)'$.

Sub-Game 1-4-t-A-2**:** When $\tau_{\mathsf{renc}} = 0$, Sub-Game 1-4-t-A-2 is the same as Sub-Game 1-4-t-A-1 except that $\boldsymbol{k}^{*\mathsf{renc}}$ of the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct})$ are of semi-functional form as given in Eq. (14).

Sub-Game 1-4-t-A-3**:** When $\tau_{\mathsf{renc}} = 0$, Sub-Game 1-4-t-A-3 is the same as Sub-Game 1-4-t-A-2 except that $\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'}$ of the reply to the t-th re-encryption key query for $(\vec{v}, \vec{x}', \mathsf{oct})$ is

$$\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{W_1})$$

where $W_1 \in GL(4n+4, \mathbb{F}_q)$ is defined in Game $0''$ and it satisfies that $\mathbb{D}^*_1 = \mathbb{B}^* W_1$ and all the other variables are generated as in Sub-Game 1-4-t-A-2. Note that Sub-Game 1-4-t-A-3 is the same as Game 1-4-t'' when $\tau_{\mathsf{renc}} = 0$.

From Claims 5, 6, and 7,

$$\begin{aligned}&\big|\Pr[\mathcal{A}\text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A}\text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = 0]\big| \\ &\le \big|\Pr[\mathcal{A}\text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A}\text{ wins in Game 1-4-}t\text{-}A\text{-1} \mid \tau_{\mathsf{renc}} = 0]\big| \\ &\quad + |\Pr[\mathcal{A}\text{ wins in Game 1-4-}t\text{-}A\text{-1} \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A}\text{ wins in Game 1-4-}t\text{-}A\text{-2} \mid \tau_{\mathsf{renc}} = 0]| \\ &\quad + |\Pr[\mathcal{A}\text{ wins in Game 1-4-}t\text{-}A\text{-2} \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A}\text{ wins in Game 1-4-}t\text{-}A\text{-3} \mid \tau_{\mathsf{renc}} = 0]| \\ &\le \mathsf{Adv}^{\mathsf{IPE},\mathsf{AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-1}}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE},\mathsf{AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-2}}}(\lambda) + 3/q. \end{aligned} \tag{25}$$

Case $\tau_{\mathsf{renc}} = 1$ or 2 As for the conditional probability with $\tau_{\mathsf{renc}} = 1$ or 2, we introduce a game as:

Sub-Game 1-4-t-B**:** When $\tau_{\mathsf{renc}} = 1$ or $\tau_{\mathsf{renc}} = 2$, Sub-Game 1-4-t-B is the same as Game 1-4-$(t-1)'$ except that $\boldsymbol{k}^{*\mathsf{renc}}$ of the reply to the t-th re-encryption key query for $(\vec{v}, \vec{x}', \mathsf{oct})$ is of semi-functional form as given in Eq.(13). Note that Sub-Game 1-4-t-B is the same as Game 1-3-t'' when $\tau_{\mathsf{renc}} = 1$ or $\tau_{\mathsf{renc}} = 2$.

From Claim 8,

$$\begin{aligned}
&\big|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 1 \text{ or } \tau_{\mathsf{renc}} = 2] \\
&\qquad - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = 1 \text{ or } \tau_{\mathsf{renc}} = 2]\big| \\
&= \big|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 1 \text{ or } \tau_{\mathsf{renc}} = 2] \\
&\qquad - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t\text{-}B \mid \tau_{\mathsf{renc}} = 1 \text{ or } \tau_{\mathsf{renc}} = 2]| \\
&\leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-1}}}(\lambda) + \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-2}}}(\lambda) + 4/q. \qquad (26)
\end{aligned}$$

Therefore, from Eqs. (23), (24), (25), and (26),

$$\begin{aligned}
&|\mathsf{Adv}^{\text{1-4-}(t-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\text{1-4-}t}_{\mathcal{A}}(\lambda)| \\
&= \Big|\textstyle\sum_{\iota=0}^{2} \Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = \iota] - 3/2 \\
&\quad -(\textstyle\sum_{\iota=0}^{2} \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = \iota] - 3/2)\Big| \\
&= \Big|\textstyle\sum_{\iota=0}^{2} (\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = \iota] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = \iota])\Big| \\
&\leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-1}}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-2}}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-1}}}(\lambda) + \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-2}}}(\lambda) + 7/q.
\end{aligned}$$

This completes the proof of Lemma 12. □

Claim 5 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{\text{1-4-}A\text{-1}}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,* $|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-4-}t\text{-}A\text{-1} \mid \tau_{\mathsf{renc}} = 0]| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-1}}}(\lambda) + 1/q$, *where* $\mathcal{B}_{\text{1-4-}t\text{-}A\text{-1}}(\cdot) := \mathcal{B}_{\text{1-4-}A\text{-1}}(t, \cdot)$.

Claim 6 *For any adversary $\mathcal{A}$,* $|\Pr[\mathcal{A} \text{ wins in Sub-Game1-4-}t\text{-}A\text{-1} \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-4-}t\text{-}A\text{-2} \mid \tau_{\mathsf{renc}} = 0]| \leq 1/q$.

Claim 7 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{\text{4-}A\text{-2}}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,* $|\Pr[\mathcal{A} \text{ wins in Sub-Game 1-4-}t\text{-}A\text{-2} \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-4-}t\text{-}A\text{-3} \mid \tau_{\mathsf{renc}} = 0]| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-2}}}(\lambda) + 1/q$, *where* $\mathcal{B}_{\text{1-4-}t\text{-}A\text{-2}}(\cdot) := \mathcal{B}_{\text{1-4-}A\text{-2}}(t, \cdot)$.

Claim 8 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{\text{1-4-}B\text{-1}}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,* $|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 1] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-4-}t\text{-}B \mid \tau_{\mathsf{renc}} = 1]| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-1}}}(\lambda) + 2/q$, *where* $\mathcal{B}_{\text{1-4-}t\text{-}B\text{-1}}(\cdot) := \mathcal{B}_{\text{1-4-}B\text{-1}}(t, \cdot)$.

The proofs of Claims 5–8 are given in similar manners to those of Claims 1–4, respectively.

Claim 9 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{\text{1-4-}B\text{-2}}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,* $|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 2] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-4-}t\text{-}B \mid \tau_{\mathsf{renc}} = 2]| \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-2}}}(\lambda) + 2/q$, *where* $\mathcal{B}_{\text{1-4-}t\text{-}B\text{-2}}(\cdot) := \mathcal{B}_{\text{1-4-}B\text{-2}}(t, \cdot)$.

Proof. The proof strategy of Claim 9 is similar to Theorem 1 in [7]. In order to prove Claim 9, we construct a probabilistic machine $\mathcal{B}_{\text{1-4-}B\text{-2}}$ against Problem 3 using an adversary $\mathcal{A}$ in a security game (Game 1-4-$(t-1)'$ or Sub-Game 1-4-t-B) as a black box as follows:

1. $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ is given an index t and a Problem 3 instance, $(\mathsf{param}_n, \mathbb{B}^*, \widehat{\mathbb{B}}, \{\boldsymbol{h}_{\beta,i}, \boldsymbol{e}_i\}_{i=1,2})$.
2. $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ plays a role of the challenger in the security game against $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ generates a pair of public and secret key of the IPE scheme, $(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$. $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ sets $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_{n+1}, \boldsymbol{b}^*_{n+2}, \boldsymbol{b}^*_{3n+4}, \ldots, \boldsymbol{b}^*_{4n+2})$ and provides $\mathcal{A}$ with a public key $\mathsf{pk} := (\lambda, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \mathsf{pk}^{\mathsf{IPE}})$.
4. When a decryption key query is issued for a vector $\vec{v}$, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ computes semi-functional form $(\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}})$ and $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}}$. $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ provides $\mathcal{A}$ with the decryption key $\mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$.
5. When a re-encryption key query is issued for $(\vec{v}, \vec{x}')$, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ semi-functional form $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ and normal form $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$, $\mathsf{prect}_{\vec{x}'}$ and $\widehat{\mathbb{D}}^*_1$. $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ provides $\mathcal{A}$ with the re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1)$.
6. When a k-th re-encryption query is issued for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} = (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}, S))$, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ executes as follows:
   - If $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, then $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ returns $\perp$ to $\mathcal{A}$.
   - If $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$ then $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ normally computes $\boldsymbol{c}^{\mathsf{renc}}$ from $(\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}})$ and $\{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2}$ from $\{W_i \xleftarrow{\mathsf{U}} GL(N, \mathbb{F}_q)\}_{i=1,2}$, and
     - when $k < t$, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ computes semi-functional form $\boldsymbol{k}^{*\mathsf{renc}}$ from Eq.(14).
     - when $k = t$, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ chooses $\rho, u_i \xleftarrow{\mathsf{R}} \mathbb{F}_q$ for $i = 1, \ldots, n$ and computes

$$\boldsymbol{k}^{*\mathsf{renc}} := \left(\boldsymbol{b}^*_0 + \sum_{i=1}^{n} \delta v_i \boldsymbol{b}^*_i + \rho\ \mathsf{verk}\ \boldsymbol{h}^*_{\beta.1} + \rho \boldsymbol{h}^*_{\beta.2} + \sum_{i=1}^{n} u_i \boldsymbol{b}^*_{3n+2+i}\right) W_1.$$

     - when $k > t$, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ computes normal form $\boldsymbol{k}^{*\mathsf{renc}}$ from Eq.(8).

   $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ provides $\mathcal{A}$ with the re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'} := (\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{ct}^{\mathsf{renc}}_{\vec{x}'})$.
7. When a challenge query is issued for $(\vec{x}^{(0)}, \vec{x}^{(0)}, m^{(0)}, m^{(1)})$, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ picks a bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ and $\zeta, \rho \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and generates $(\mathsf{sigk}^{\clubsuit}, \mathsf{verk}^{\clubsuit}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$. Next, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ computes

$$\begin{aligned}
\boldsymbol{c} &:= \zeta \boldsymbol{b}_0 + \sum_{i=1}^{n} \omega x^{(b)}_i \boldsymbol{b}_i + \rho\ \mathsf{verk}^{\clubsuit} \boldsymbol{e}_1 + \rho \boldsymbol{e}_2 + \varphi_{\mathsf{ran}} \boldsymbol{b}_{4n+3}, \\
\boldsymbol{c}_{\mathsf{ran}} &:= \sum_{i=1}^{n} \omega_{\mathsf{ran}} x^{(b)}_i \boldsymbol{b}_i + \rho_{\mathsf{ran}} \mathsf{verk}^{\clubsuit} \boldsymbol{e}_1 + \rho_{\mathsf{ran}} \boldsymbol{e}_2 + \varphi_{\mathsf{ran}} \boldsymbol{b}_{4n+3}, \\
c_T &:= m^{(b)} \cdot g_T^{\zeta}, \quad C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \quad S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}^{\clubsuit}, C).
\end{aligned}$$

   $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ provides $\mathcal{A}$ with a challenge ciphertext $\mathsf{oct}_{\vec{x}^{(b)}} := (C, \mathsf{verk}^{\clubsuit}, S)$.
8. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ outputs $\beta' := 0$. Otherwise, $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ outputs $\beta' := 1$.

Since the t-th re-encrypted ciphertext is of the form Eq.(8) (resp. of the form Eq.(14)) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{1\text{-}4\text{-}B\text{-}2}$ is distributed as Game 1-4-$(t-1)'$ (resp. Sub-Game 1-4-t-B) if $\beta = 0$ (resp. $\beta = 1$) except that δ defined in Problem 3 is zero (i.e., except for probability $1/q$ (resp. $1/q$)). Then, $|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 2] - \Pr[\mathcal{A} \text{ wins in Sub-Game 1-4-}t\text{-}B \mid \tau_{\mathsf{renc}} = 2]| = \left|\mathsf{Pr}\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P3}}_0(1^\lambda, n)\right] - \mathsf{Pr}\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P3}}_1(1^\lambda, n)\right]\right| + 2/q \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{1\text{-}4\text{-}t\text{-}B\text{-}2}}(\lambda) + 2/q$. □

Lemma 13. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}^{(1\text{-}4\text{-}\nu_3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}5)}_{\mathcal{A}}(\lambda)| \leq 1/q$.*

Proof. To prove Lemma 13, we will show distribution $(\mathsf{pk}, \{\mathsf{sk}_{\vec{v}}\}, \{\mathsf{rk}_{\vec{v}.\vec{x}}\}, \{\mathsf{rct}_{\vec{x}'}\}, \mathsf{oct}_{\vec{x}^{(b)}})$ in Game 4-ν_3 and that in Game 5 are equivalent. In this proof, since we change to the component $\boldsymbol{c}$ of the challenger ciphertext $\mathsf{oct}_{\vec{x}^{(b)}}$ using the base $\mathbb{B}$ in the Game 4-ν_3, we focus the only components using the bases

$\mathbb{B}$ or $\mathbb{B}^*$. We define new basis $\mathbb{U}$ of $\mathbb{V}$ and $\mathbb{U}^*$ of $\mathbb{V}^*$ as follows; We generate $F := (\xi_{i,s})_{1\le i,s\le n}, \widetilde{F} := (\widetilde{\xi}_{i,s})_{1\le i,s\le n} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n\times n}, \vec{\theta} := (\theta_i)_{1\le i\le n} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and set for $i = 1, \ldots, n$

$$\boldsymbol{u}_{n+2+i} := \boldsymbol{b}_{n+2+i} - \textstyle\sum_{s=1}^n \left(\xi_{i,s}\boldsymbol{b}_s + \widetilde{\xi}_{i,s}\boldsymbol{b}_{2n+2+s}\right) - \theta_i\boldsymbol{b}_0,$$
$$\boldsymbol{u}_0^* := \boldsymbol{b}_0^* + \textstyle\sum_{s=1}^n \theta_s\boldsymbol{b}_{n+2+s}^*, \quad \boldsymbol{u}_i^* := \boldsymbol{b}_i^* + \textstyle\sum_{s=1}^n \xi_{s,i}\boldsymbol{b}_{n+2+s}^*, \quad \boldsymbol{u}_{2n+2+i}^* := \boldsymbol{b}_{2n+2+i}^* + \textstyle\sum_{s=1}^n \widetilde{\xi}_{s,i}\boldsymbol{b}_{n+2+s}^*.$$

We set $\mathbb{U} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n+2}, \boldsymbol{u}_{n+3}, \ldots, \boldsymbol{u}_{2n+2}, \boldsymbol{b}_{2n+3}, \ldots, \boldsymbol{b}_{4n+3})$ and $\mathbb{U}^* := (\boldsymbol{u}_0^*, \ldots, \boldsymbol{u}_n^*, \boldsymbol{b}_{n+1}^*, \ldots, \boldsymbol{b}_{2n+2}^*, \boldsymbol{u}_{2n+3}^*, \ldots, \boldsymbol{u}_{3n+2}^*, \boldsymbol{b}_{3n+3}^*, \ldots, \boldsymbol{b}_{4n+3}^*)$. We then easily verify that $\mathbb{U}$ and $\mathbb{U}^*$ are dual orthonormal, and are distributed the same as the original bases $\mathbb{B}$ and $\mathbb{B}^*$.

We note that if (the ℓ-th) re-encryption key query $(\vec{v}_\ell, \vec{x}'_\ell)$ has a matching decryption key query $\vec{v}$, that is, $R(\vec{v}, \vec{x}'_\ell) = 1$, then matrix W_1 and converted key $\boldsymbol{k}^{*\mathsf{rk}}W_1^{-1}$ are included in adversary's view. Similarly, if (the t-th) re-encryption query $(\vec{v}_t, \vec{x}'_t, \mathsf{oct})$ has a matching decryption key query $\vec{v}$, that is, $R(\vec{v}, \vec{x}'_t) = 1$, then matrix W_1 and converted key $\boldsymbol{k}^{*\mathsf{renc}}W_1^{-1}$ are included in adversary's view.

Therefore, in Game 1-4-ν_3, $(\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}})$ of the decryption key queries, $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$ of the re-encryption key queries with a matching decryption key query, and $\boldsymbol{k}^{*\mathsf{renc}}$ of the re-encryption queries with a matching decryption key query are expressed over bases $\mathbb{B}^*$ and $\mathbb{U}^*$ as

$$\begin{aligned}
\boldsymbol{k}^* &= (\ 1,\ \delta\vec{v},\ 0^2,\ \vec{r},\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{B}^*} = (\ 1,\ \delta\vec{v},\ 0^2,\ \vec{w},\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{U}^*},\\
\boldsymbol{k}^*_{\mathsf{ran}} &= (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ \vec{r}_{\mathsf{ran}},\ 0^n,\ \vec{\eta}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*} = (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ \vec{w}_{\mathsf{ran}},\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{U}^*},\\
\boldsymbol{k}^{*\mathsf{rk}}W_1^{-1} &= (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ \vec{r}',\ 0^n,\ \vec{\eta}^{\,\mathsf{rk}},\ 0\ )_{\mathbb{B}^*} = (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ \vec{w}',\ 0^n,\ \vec{\eta}'^{\mathsf{rk}},\ 0\ )_{\mathbb{U}^*},\\
\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}W_1^{-1} &= (\ 0,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ \vec{r}'_{\mathsf{ran}},\ 0^n,\ \vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*} = (\ 0,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ \vec{w}'_{\mathsf{ran}},\ 0^n,\ \vec{\eta}'^{\mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{U}^*},\\
\boldsymbol{k}^{*\mathsf{renc}}W_1^{-1} &= (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1,\mathsf{verk}),\ \vec{r}'',\ 0^n,\ \vec{\eta}^{\,\mathsf{renc}},\ 0\ )_{\mathbb{B}^*}\\
&= (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1,\mathsf{verk}),\ \vec{w}'',\ 0^n,\ \vec{\eta}'^{\mathsf{renc}},\ 0\ )_{\mathbb{U}^*},
\end{aligned}$$

where $\vec{w} := \vec{r} - \delta\vec{v}\cdot F^{\mathrm{T}} - \vec{\theta}$, $\vec{w}_{\mathsf{ran}} := \vec{r}_{\mathsf{ran}} - \delta_{\mathsf{ran}}\vec{v}\cdot F^{\mathrm{T}} - \vec{\theta}$, $\vec{w}' := \vec{r}' - \delta^{\mathsf{rk}}\vec{v}\cdot F^{\mathrm{T}} - \vec{\theta}$, $\vec{w}'_{\mathsf{ran}} := \vec{r}'_{\mathsf{ran}} - \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v}\cdot F^{\mathrm{T}} - \vec{\theta}$, and $\vec{w}'' := \vec{r}'' - \delta^{\mathsf{renc}}\vec{v}\cdot F^{\mathrm{T}} - \vec{\theta}$ are uniformly and independently distributed since $\vec{r}, \vec{r}_{\mathsf{ran}}, \vec{r}', \vec{r}'_{\mathsf{ran}}, \vec{r}'' \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

$\boldsymbol{c}$ and $\boldsymbol{c}_{\mathsf{ran}}$ of the challenge ciphertext $\mathsf{oct}_{\vec{x}^{(b)}} := (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}^{\clubsuit}, S)$ in Game 1-4-ν_3 are expressed over bases $\mathbb{B}$ and $\mathbb{U}$ as

$$\begin{aligned}
\boldsymbol{c} &= (\ \zeta,\ \ \omega\vec{x}^{(b)},\ \ \rho(\mathsf{verk}^{\clubsuit},1),\ \ \vec{u},\ 0^n,\ \ 0^n,\ \varphi\ )_{\mathbb{B}}\\
&= (\ \zeta+\vec{u}\cdot\vec{\theta},\ \omega\vec{x}^{(b)} + \vec{u}\cdot F,\ \rho(\mathsf{verk}^{\clubsuit},1),\ \ \vec{u},\ \vec{u}\cdot\widetilde{F},\ 0^n,\ \varphi\ )_{\mathbb{U}},\\
\boldsymbol{c}_{\mathsf{ran}} &= (\ 0,\ \ \omega_{\mathsf{ran}}\vec{x}^{(b)},\ \ \rho_{\mathsf{ran}}(\mathsf{verk}^{\clubsuit},1),\ 0^n,\ 0^n,\ \ 0^n,\ \varphi_{\mathsf{ran}}\ )_{\mathbb{B}}\\
&= (\ 0,\ \ \omega_{\mathsf{ran}}\vec{x}^{(b)},\ \ \rho_{\mathsf{ran}}(\mathsf{verk}^{\clubsuit},1),\ 0^n,\ 0^n,\ \ 0^n,\ \varphi_{\mathsf{ran}}\ )_{\mathbb{U}},
\end{aligned}$$

where $\zeta+\vec{u}\cdot\vec{\theta}$, $\omega\vec{x}^{(b)}+\vec{u}\cdot F$ and $\vec{u}\cdot\widetilde{F}$ are uniformly and independently distributed except when $\vec{u} = \vec{0}$, i.e., except for probability $\le 1/q$, since $\vec{u} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $\vec{\theta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $F, \widetilde{F} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n\times n}$. In the light of adversary's view, both $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{U}, \mathbb{U}^*)$ are consistent with public key pk. Since $\boldsymbol{k}^*$, $\boldsymbol{k}^{*\mathsf{rk}}$, $\boldsymbol{k}^{*\mathsf{renc}}$, and $\boldsymbol{c}^{\mathsf{renc}}$ can be expressed in two ways in Game 1-4-ν_3 over $(\mathbb{B}, \mathbb{B}^*)$ and in Game 1-5 over bases $(\mathbb{U}, \mathbb{U}^*)$. Thus, Game 1-4-$\nu_3$ can be conceptually changed to Game 1-5. □

Lemma 14. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}5}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}5)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}6)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{1\text{-}5}}(\lambda)$.*

Proof. In order to prove Lemma 14, we construct a probabilistic machine $\mathcal{B}_{1\text{-}5}$ against Problem 4 using an adversary $\mathcal{A}$ in a security game (Game 1-5 or Game 1-6) as a black box as follows:

1. $\mathcal{B}_{1\text{-}5}$ is given a Problem 4 instance, $(\mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,\ldots,n})$.
2. $\mathcal{B}_{1\text{-}5}$ plays a role of the challenger in the security game against $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{1\text{-}5}$ generates a pair of public and secret key of the underlying IPE scheme, $(\mathsf{pk}^{\mathsf{IPE}}, \mathsf{sk}^{\mathsf{IPE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{IPE}}(1^\lambda, n)$. $\mathcal{B}_{1\text{-}5}$ sets $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n+2}, \boldsymbol{b}_{4n+3})$ and $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_{n+1}, \boldsymbol{b}^*_{n+2}, \boldsymbol{b}^*_{3n+3}, \ldots, \boldsymbol{b}^*_{4n+2})$ and provides $\mathcal{A}$ with a public key $\mathsf{pk} := (\lambda, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \mathsf{pk}^{\mathsf{IPE}})$.
4. When a decryption key query is issued for a vector $\vec{v} := (v_1, \ldots, v_n)$, $\mathcal{B}_{1\text{-}5}$ computes $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KG}_{\mathsf{IPE}}(\mathsf{sk}^{\mathsf{IPE}}, \vec{v})$ and using $\{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\ldots,n}, \widehat{\mathbb{B}}^*$ of the Problem 4 instance,

$$\boldsymbol{k}^* := \boldsymbol{b}^*_0 + \textstyle\sum_{i=1}^n (\delta v_i \boldsymbol{b}^*_i + \pi_i \boldsymbol{h}^*_{\beta,i} + \eta_i \boldsymbol{b}^*_{3n+2+i}), \quad \boldsymbol{k}^*_{\mathsf{ran}} := \textstyle\sum_{i=1}^n (\delta_{\mathsf{ran}} v_i \boldsymbol{b}^*_i + \pi_{\mathsf{ran},i} \boldsymbol{h}^*_{\beta,i} + \eta_{\mathsf{ran},i} \boldsymbol{b}^*_{3n+2+i}),$$

where $\delta, \delta_{\mathsf{ran}}, \pi_i, \pi_{\mathsf{ran},i}, \eta_i, \eta_{\mathsf{ran},i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\mathcal{B}_{1\text{-}5}$ provides $\mathcal{A}$ with the decryption key $\mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$.
5. When a re-encryption key query is issued for $(\vec{v} := (v_1, \ldots, v_n), \vec{x}')$, $\mathcal{B}_{1\text{-}5}$ computes $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}$ using $\mathsf{pk}^{\mathsf{IPE}}$, $\widehat{\mathbb{D}}^*_1 := (\boldsymbol{d}^*_i := \boldsymbol{b}^*_i W_1)_{i=n+1,n+2,3n+3,\ldots,4n+2}$ with $W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$, and

$$\boldsymbol{k}^{*\mathsf{rk}} := \boldsymbol{b}^*_0 + \textstyle\sum_{i=1}^n (\delta^{\mathsf{rk}} v_i \boldsymbol{b}^*_i + \pi'_i \boldsymbol{h}^*_{\beta,i} + \eta^{\mathsf{rk}}_i \boldsymbol{b}^*_{3n+2+i}),$$
$$\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := \textstyle\sum_{i=1}^n (\delta^{\mathsf{rk}}_{\mathsf{ran}} v_i \boldsymbol{b}^*_i + \pi'_{\mathsf{ran},i} \boldsymbol{h}^*_{\beta,i} + \eta^{\mathsf{rk}}_{\mathsf{ran},i} \boldsymbol{b}^*_{3n+2+i}),$$

where $\delta^{\mathsf{rk}}, \delta^{\mathsf{rk}}_{\mathsf{ran}}, \pi'_i, \pi'_{\mathsf{ran},i}, \eta^{\mathsf{rk}}_i, \eta^{\mathsf{rk}}_{\mathsf{ran},i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\mathcal{B}_{1\text{-}5}$ provides $\mathcal{A}$ with the re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'}, \widehat{\mathbb{D}}^*_1)$.
6. When a re-encryption query is issued for $(\vec{v} := (v_1, \ldots, v_n), \vec{x}', \mathsf{oct} := (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), \mathsf{verk}, S))$, if $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, $\mathcal{B}_{1\text{-}5}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{B}_{1\text{-}5}$ computes a normal form of $(\boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2})$ using $C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T)$, the Problem 4 instance and $\mathsf{pk}^{\mathsf{IPE}}$, and

$$\boldsymbol{k}^{*\mathsf{renc}} := \boldsymbol{b}^*_0 + \sigma(-\boldsymbol{b}^*_{n+1} + \mathsf{verk}\, \boldsymbol{b}^*_{n+2}) + \textstyle\sum_{i=1}^n (\delta^{\mathsf{renc}} v_i \boldsymbol{b}^*_i + \pi''_i \boldsymbol{h}^*_{\beta,i} + \eta^{\mathsf{renc}}_i \boldsymbol{b}^*_{3n+2+i}),$$

where $\delta^{\mathsf{renc}}, \pi''_i, \eta^{\mathsf{renc}}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$. $\mathcal{B}_{1\text{-}5}$ provides $\mathcal{A}$ with the re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'} := (\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \{\mathsf{ct}^{\mathsf{renc}}_{i,\vec{x}'}\}_{i=1,2})$
7. When a challenge query is issued for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$, $\mathcal{B}_{1\text{-}5}$ picks a bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ and $\zeta, \rho, \omega_{\mathsf{ran}}, \rho_{\mathsf{ran}}, \varphi_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and generates $(\mathsf{sigk}^{\clubsuit}, \mathsf{verk}^{\clubsuit}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$. Next, $\mathcal{B}_{1\text{-}5}$ computes

$$\boldsymbol{c} := \zeta \boldsymbol{b}_0 + \textstyle\sum_{i=1}^n \omega x^{(b)}_i \boldsymbol{b}_i + \rho(\mathsf{verk}^{\clubsuit} \boldsymbol{b}_{n+1} + \boldsymbol{b}_{n+2}) + \sum_{i=1}^n (u_{1,i} \boldsymbol{e}_i + u_{2,i} \boldsymbol{f}_i),$$

where $\zeta, \omega, \rho, u_{1,i}, u_{2,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $\boldsymbol{c}_{\mathsf{ran}}, c_T, S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}^{\clubsuit}, C)$ are generated in a normal manner with $C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T)$. $\mathcal{B}_{1\text{-}5}$ provides $\mathcal{A}$ with the challenge ciphertext $\mathsf{oct}_{x^{(b)}} := (C, \mathsf{verk}^{\clubsuit}, S)$.
8. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{1\text{-}5}$ outputs $\beta' := 0$. Otherwise, $\mathcal{B}_{1\text{-}5}$ outputs $\beta' := 1$.

Since all the replies to decryption key, re-encryption key, re-encrypted ciphertext, and challenge queries are of the form in Game 1-5 (resp. Game 1-6) if $\beta = 0$ (resp. $\beta = 1$), $\left|\mathsf{Adv}^{(1\text{-}5)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}6)}_{\mathcal{A}}(\lambda)\right| = \left|\mathsf{Pr}\left[\mathcal{B}_{1\text{-}5}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P4}}_0(1^\lambda, n)\right] - \mathsf{Pr}\left[\mathcal{B}_{1\text{-}5}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P4}}_1(1^\lambda, n)\right]\right| \leq \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{1\text{-}5}}(\lambda)$. □

The game changes between Game 1-6 and Game 2-4-ν_3 is similar to those between Game $0''$ and Game 1-4-ν_3 except the form of the component of the challenge ciphertext $\boldsymbol{c}_{\mathsf{ran}}$ is changed to *semi-functional* form. Therefore, the advantage of between Game 1-6 and Game 2-4-ν_3 is bounded by a similar manner to those obtained in Lemmas 9–12.

Lemma 15. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}^{(2\text{-}4\text{-}\nu_3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}5)}_{\mathcal{A}}(\lambda)| \leq 1/q$.*

Proof. Lemma 15 is proven in similar manner to Lemma 13. □

Lemma 16. *For any adversary* $\mathcal{A}$, $\mathsf{Adv}^{(2\text{-}5)}_{\mathcal{A}}(\lambda) = 0$.

Proof. The value of b is independent from adversary's view in Game 2-5. So, $\mathsf{Adv}^{(2\text{-}5)}_{\mathcal{A}}(\lambda) = 0$. □

Proof of Theorem 2 (AH-OC) in the Case $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 1$
In Lemmas 17–27 and their proofs, we consider only the case $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 1$.

Lemma 17. *The proposed IP-PRE scheme is attribute-hiding for original ciphertexts against chosen plaintext attacks in the case $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 1$ under the DLIN assumption provided the underlying IPE scheme is attribute-hiding.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_{\iota\text{-}1}, \mathcal{E}_{\iota\text{-}2\text{-}j\text{-}l}, \mathcal{E}_{\iota\text{-}3\text{-}A\text{-}j}, \mathcal{E}_{\iota\text{-}3\text{-}B\text{-}j\text{-}l}, \mathcal{E}_{\iota\text{-}4\text{-}A\text{-}j}$, $\mathcal{E}_{\iota\text{-}4\text{-}B\text{-}l}, \mathcal{E}_{\iota\text{-}4\text{-}C}, \mathcal{E}_{1\text{-}6}, \mathcal{E}_{1\text{-}7}$ for $\iota = 1, 2$; $j = 1, 2$; $l = 1, 2$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ in Game $0''$,

$$\begin{aligned}\Pr[\mathcal{A}\text{ wins}|\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 1] - 1/2 \leq \sum_{\iota=1}^{2} \Big(& \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}1}}(\lambda) + \textstyle\sum_{h=1}^{\nu_1}\sum_{j=1}^{2}\sum_{l=1}^{2}\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}2\text{-}h\text{-}j\text{-}l}}(\lambda) \\ & + \textstyle\sum_{\ell=1}^{\nu_2}\sum_{j=1}^{2}\Big(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}A\text{-}j}}(\lambda) + \sum_{l=1}^{2}\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}B\text{-}j\text{-}l}}(\lambda)\Big) \\ & + \textstyle\sum_{t=1}^{\nu_3}\Big(\sum_{j=1}^{2}\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}A\text{-}j}}(\lambda) + \sum_{l=1}^{2}\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}B\text{-}l}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}C}}(\lambda)\Big)\Big) \\ & + \textstyle\sum_{t=0}^{\nu_3}\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}6\text{-}t}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}7}}(\lambda) + \epsilon, \end{aligned} \tag{27}$$

where $\mathcal{E}_{\iota\text{-}2\text{-}h\text{-}j\text{-}l}(\cdot) := \mathcal{E}_{\iota\text{-}2\text{-}j\text{-}l}(h, \cdot), \mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}A\text{-}j}(\cdot) := \mathcal{E}_{\iota\text{-}3\text{-}A\text{-}j}(\ell, \cdot), \mathcal{E}_{\iota\text{-}3\text{-}B\text{-}\ell\text{-}j\text{-}l}(\cdot) := \mathcal{E}_{\iota\text{-}3\text{-}B\text{-}j\text{-}l}(\ell, \cdot)$, $\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}A\text{-}j}(\cdot) := \mathcal{E}_{\iota\text{-}4\text{-}A\text{-}j}(t, \cdot), \mathcal{E}_{\iota\text{-}4\text{-}t\text{-}B\text{-}l}(\cdot) := \mathcal{E}_{\iota\text{-}4\text{-}B\text{-}l}(t, \cdot), \mathcal{E}_{\iota\text{-}4\text{-}t\text{-}C}(\cdot) := \mathcal{E}_{\iota\text{-}4\text{-}C}(t, \cdot), \mathcal{E}_{1\text{-}6\text{-}t}(\cdot) := \mathcal{E}_{1\text{-}6}(t, \cdot)$, $\epsilon := (66\nu_1 + 70\nu_2 + 91\nu_3 + 20)/q$ and ν_1, ν_2, ν_3 are the maximum number of $\mathcal{A}$'s decryption key queries, that of $\mathcal{A}$'s re-encryption key queries, and that of $\mathcal{A}$'s re-encryption queries, respectively.

Proof Outline of Lemma 17. To prove Lemma 17, we consider $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 1$ case.
Overview of Game Transformation. We employ Game $0''$ through Game 2-5. In this proof, there are main two sequences, the Game 1 sequence and the Game 2 sequence (Figure 5), whose aims are to change components $\boldsymbol{c}$ and $\boldsymbol{c}_{\mathsf{ran}}$ of the challenge ciphertext to independent ones from challenge bit b (random form), respectively.

We employ Game $0''$ through Game 1-7 in the Game 1 sequence. In Game $0''$, all the replies to $\mathcal{A}$'s queries are in normal forms (Eqs.(28)–(32)). In Game 1-1, $\boldsymbol{c}$ of the challenge ciphertext is changed to *temporal 1* form given in [29] (Eq.(33)). Let ν_1, ν_2, ν_3 be the maximum numbers of $\mathcal{A}$'s decryption key queries, that of $\mathcal{A}$'s re-encryption key queries, and that of $\mathcal{A}$'s re-encryption queries, respectively. There are ν_1 game changes from Game 1-1 (Game 1-2-0) through Game 1-2-ν_1. In Game 1-2-h ($h = 1, \ldots, \nu_1$), the reply to the h-th decryption key query is changed to *temporal 2* form given in [29] (Eq.(34)). There are ν_2 game changes from Game 1-2-ν_1 (Game 1-3-0) through Game 1-3-ν_2. In Game 1-3-ℓ ($\ell = 1, \ldots, \nu_2$), the reply to the ℓ-th re-encryption key query is changed to *temporal 2* form given in [29] (Eq.(35)). There are ν_3 game changes from Game 1-3-ν_2 (Game 1-4-0) through Game 1-4-ν_3. In Game 1-4-t ($t = 1, \ldots, \nu_3$), the reply to the t-th re-encrypted ciphertext query is changed to *temporal 2* form in [29] (Eq.(36)) or *semi-functional* form (Eq.(37)). In Game 1-5, $\boldsymbol{c}$ of the challenge ciphertext is changed to unbiased form in [29] (Eq.(38)).

Then, through Game 1-6-t ($t = 0, \ldots, \nu_3$), replies to all the decryption key, re-encryption key and re-encrypted ciphertext queries are changed to a normal form. In Game 1-7, the challenge ciphertext

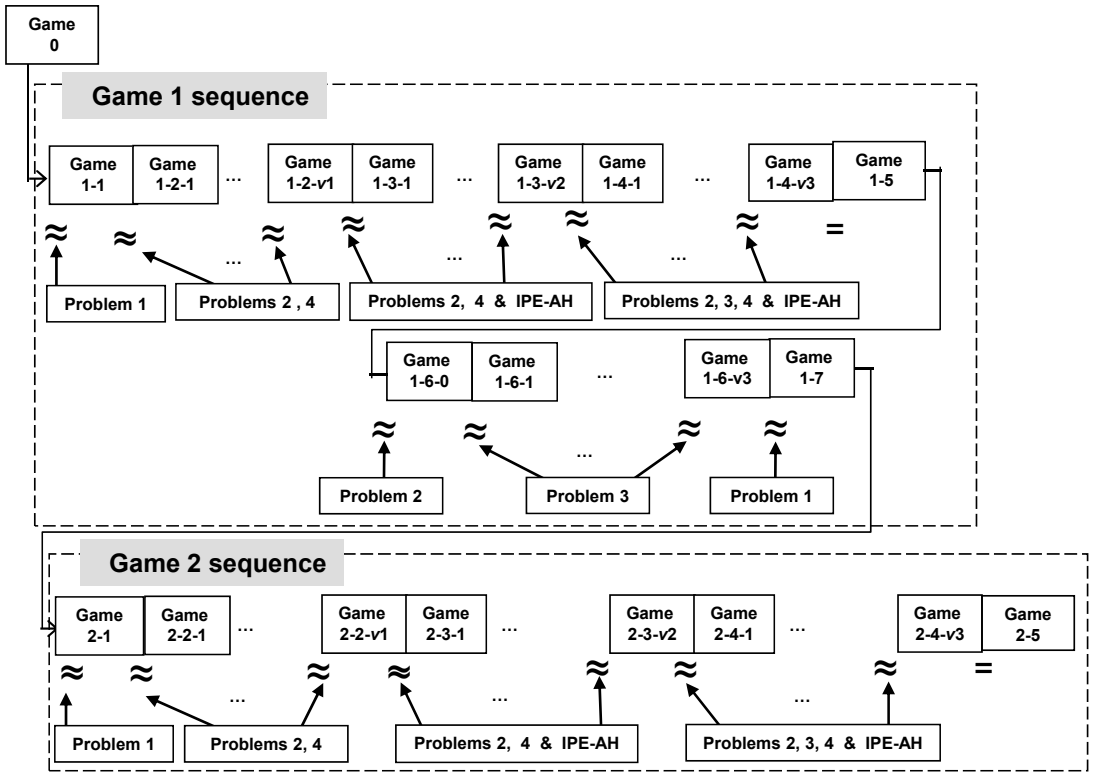

Fig. 5. Game Transformations for AH-OC Security in the case $\tau_{\mathsf{verk}} = 1 \wedge \tau_{\mathsf{m}} = 1$.

is changed to a normal and unbiased ciphertext (Eq. (39)), and the game is a preparation for the Game 2 sequence. In the Game 2 sequence, $\boldsymbol{c}_{\mathsf{ran}}$ is changed to random form in Eq.(40) by proceeding similar to game transformations in the Game 1 sequence. In the final Game 2-5, the advantage of the adversary is zero.

As Figure 5 shows, the advantage gap between Game $0''$ and Game 1-1 is bounded by the advantage of Problem 1. The advantage gaps between Games 1-2-$(h-1)$ and 1-2-h (resp. 2-2-$(h-1)$ and 2-2-h) are bounded by the advantage of Problems 2 and 4. The advantage gaps between Games 1-3-$(\ell-1)$ and 1-3-ℓ (resp. Games 2-3-$(\ell-1)$ and 2-3-ℓ) are bounded by the advantages of Problems 2, 4 and the attribute-hiding security of the underlying IPE scheme. The advantage gaps between Games 1-4-$(t-1)$ and Game 1-4-t (resp. Games 2-4-$(t-1)$ and 2-4-t) are bounded by the advantages of Problems 2, 3, 4 and attribute-hiding security of the underlying IPE scheme. Since the advantages of Problems 1, 2, 3 and 4 are bounded by that of DLIN, the advantage of $\mathcal{A}$ is bounded by those of DLIN and the attribute-hiding security of the underlying IPE.

Overview of Sub-Games. We employ Sub-Games between Games 1-3-$(\ell-1)$ and 1-3-ℓ, and Games 1-4-$(t-1)$ and 1-4-t as described in Figure 6.

First, Game 1-3-$(\ell-1)$ is changed to Game 1-3-$(\ell-1)'$ which is the same as Game 1-3-$(\ell-1)$ except that flip a coin $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell}$ when the variable $s_{\mathsf{rk},\ell}$ is determined at the challenge step or the ℓ-th re-encryption key query step (Definition 4). Since $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$, the advantage of $\mathcal{A}$ in Game 1-3-$(\ell-1)'$ is a half of that in Game 1-3-$(\ell-1)$.

When $\tau_{\mathsf{rk}} = 0$, we employ three intermediate sub-games, Sub-Games 1-3-ℓ-A-j ($j = 1, 2, 3$). In Game 1-3-ℓ-A-1, $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ in the reply to the ℓ-th re-encryption key query is changed to $\mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \vec{x}', R)$

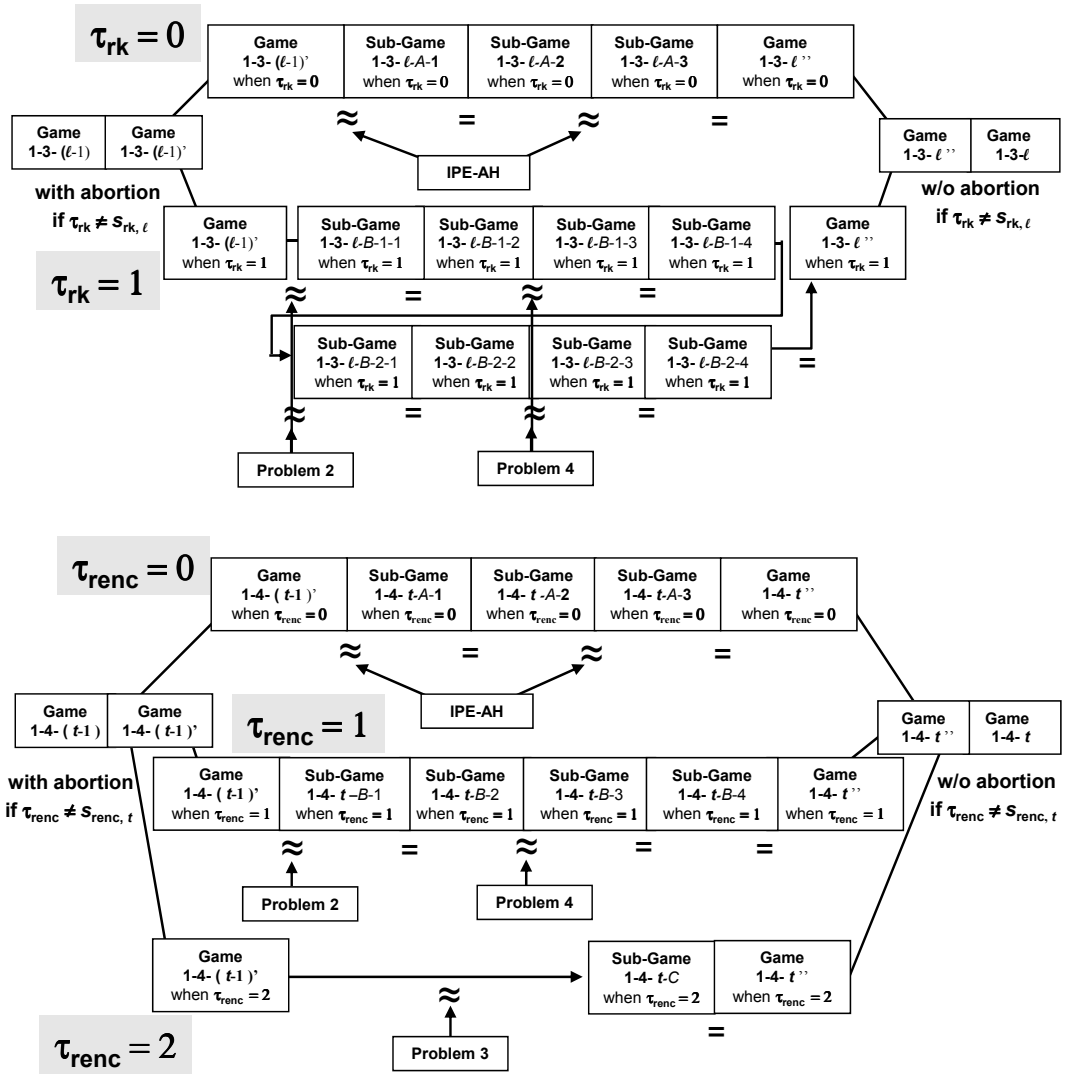

Fig. 6. Sub-Games between Games 1-3-$(\ell-1)$ and 1-3-ℓ, and Games 1-4-$(t-1)$ and 1-4-t

where R is a random matrix in $\mathbb{F}_q^{N\times N}$. In Game 1-3-ℓ-A-2, $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ of the reply are changed to *temporal 2* forms in Eq.(35). In Game 1-3-ℓ-A-3, $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ returns back to normal $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} := \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathtt{IPE}}, \vec{x}', W_1)$. When $\tau_{\mathsf{rk}} = 1$, we employ eight intermediate sub-games, Sub-Games 1-3-ℓ-B-j-l ($j = 1, 2$; $l = 1, \ldots, 4$). Through the eight games, in Game 1-3-ℓ-B-2-4, $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ of the reply to the ℓ-th re-encryption key query are changed to *temporal 2* forms in Eq.(35).

Both final games, Game 1-3-ℓ-A-3 (when $\tau_{\mathsf{rk}} = 0$) and Game 1-3-ℓ-B-2-4 (when $\tau_{\mathsf{rk}} = 1$) are equivalent to Game 1-3-ℓ'' which is the same as Game 1-3-ℓ except that flip a coin $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell}$ when the variable $s_{\mathsf{rk},\ell}$ is determined at the challenge step or the ℓ-th re-encryption key query step (Definition 4). Similarly to Game 1-3-$(\ell-1)'$, the advantage of $\mathcal{A}$ in Game 1-3-ℓ'' is a half of that in Game 1-3-ℓ.

As Figure 6 shows, when $\tau_{\mathsf{rk}} = 0$, the advantage gap between Games 1-3-$(\ell-1)'$ and 1-3-ℓ-A-1 (resp. 1-3-ℓ-A-2 and 1-3-ℓ-A-3) is bounded by the advantage of the attribute-hiding security of the underlying IPE scheme. When $\tau_{\mathsf{rk}} = 1$, the advantage gap between Games 1-3-$(\ell-1)'$ and 1-3-ℓ-B-1-1

(resp. 1-3-ℓ-B-1-4 and 1-3-ℓ-B-2-1) is bounded by the advantage of Problem 2, that between Games 1-3-ℓ-1-2 and 1-3-ℓ-B-1-3 (resp. 1-3-ℓ-B-2-2 and 1-3-ℓ-B-2-3) is bounded by the advantage of Problem 4. All the other games are conceptually changed from the previous one.

For bounding the advantage gap between Games 1-4-$(t-1)$ and 1-4-t, similar Sub-Games are used (the lower diagram in Figure 6). The difference from the above is that a ternary coin $\tau_{\mathsf{renc}} \xleftarrow{\mathsf{U}} \{0,1,2\}$ is used, so, the advantage of $\mathcal{A}$ in Game 1-4-$(t-1)'$ is a third of that in Game 1-4-$(t-1)$. And, when $\tau_{\mathsf{renc}} = 1$, there are just four intermediate sub-games. Here, while the gap is bounded by the advantage of Problems 2 and 4 when $\tau_{\mathsf{renc}} = 1$, the gap is bounded by that of Problem 3 when $\tau_{\mathsf{renc}} = 2$.

Proof of Lemma 17. Let ν_1 be the maximum number of $\mathcal{A}$'s decryption key queries, ν_2 be the maximum number of $\mathcal{A}$'s re-encryption key queries and ν_3 be the maximum number of $\mathcal{A}$'s re-encryption queries. To prove Lemma 17, we consider the following $2(\nu_1+\nu_2)+3\nu_3+6$ games. In Game $0''$, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game $0''$: We only describe the components which are changed in the other games.

The reply to a decryption key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ 0^n,\ \boxed{0^n},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \quad \boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ 0^n,\ \boxed{0^n},\ \vec{\eta}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*}, \tag{28}$$

and $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}}$, where $\delta, \delta_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}, \vec{\eta}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$.

$\boldsymbol{k}^{*\mathsf{rk}}$, $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ and $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ of the reply to a re-encryption key query for $(\vec{v}, \vec{x}')$ is:

$$\boldsymbol{k}^{*\mathsf{rk}} := (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ 0^n,\ \boxed{0^n},\ \vec{\eta}^{\ \mathsf{rk}},\ 0)_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\ 0,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ 0^n,\ \boxed{0^n},\ \vec{\eta}^{\ \mathsf{rk}}_{\mathsf{ran}},\ 0)_{\mathbb{D}_1^*}, \tag{29}$$

where $\delta^{\mathsf{rk}}, \delta^{\mathsf{rk}}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}^{\ \mathsf{rk}}, \vec{\eta}^{\ \mathsf{rk}}_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$, $\mathbb{D}_1^* := \mathbb{B}^* W_1$.

$\boldsymbol{k}^{*\mathsf{renc}}$ of the reply to a re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} = (C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), S, \mathsf{verk}))$ is $\perp$ if $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$. Otherwise, the reply is:

$$\boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \boxed{0^n},\ \vec{\eta}^{\ \mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*}, \tag{30}$$

where, $\delta^{\mathsf{renc}}, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\eta}^{\ \mathsf{renc}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $W_1 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$, $\mathbb{D}_1^* := \mathbb{B}^* W_1$.

The reply to a challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is:

$$\boldsymbol{c} := (\ \zeta,\ \boxed{\omega\vec{x}^{(b)}},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{0^n},\ \boxed{0^n},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{31}$$

$$\boldsymbol{c}_{\mathsf{ran}} := (\ 0,\ \boxed{\omega_{\mathsf{ran}}\vec{x}^{(b)}},\ \rho_{\mathsf{ran}}(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{0^n},\ \boxed{0^n},\ 0^n,\ \varphi_{\mathsf{ran}}\ )_{\mathbb{B}}, \tag{32}$$

$c_T := m^{(b)} \cdot g_T^{\zeta}$, $C := (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T)$, $S \xleftarrow{\mathsf{R}} \mathsf{Sign}(\mathsf{sigk}^{\clubsuit}, C)$, where $b \xleftarrow{\mathsf{U}} \{0,1\}$, $\zeta, \omega, \omega_{\mathsf{ran}}, \rho, \rho_{\mathsf{ran}}, \varphi, \varphi_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $(\mathsf{sigk}^{\clubsuit}, \mathsf{verk}^{\clubsuit}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$.

Game 1-1: Game 1-1 is the same as Game $0''$ except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is

$$\boldsymbol{c} := (\ \zeta,\ \omega\vec{x}^{(b)},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{\omega'\vec{x}^{(b)}},\ \boxed{\omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)}},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{33}$$

where $\omega', \omega''_0, \omega''_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game $0''$.

Game 1-2-h ($h = 1, \ldots, \nu_1$): Game 1-2-0 is Game 1-1. Game 1-2-h is the same as Game 1-2-$(h-1)$ except that the reply to the h-th decryption key query for $\vec{v}$ is

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ 0^n,\ \boxed{\delta'\vec{v}},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \quad \boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ 0^n,\ \boxed{\delta'\vec{v}},\ \vec{\eta}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*}, \quad (34)$$

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

Game 1-3-ℓ ($\ell = 1, \ldots, \nu_2$): Game 1-3-0 is Game 1-2-ν_1. Game 1-3-ℓ is the same as Game 1-3-$(\ell-1)$ except that the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x}')$ is as follow:

$$\boldsymbol{k}^{*\mathsf{rk}} := (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ 0^n,\ \boxed{\delta'^{\mathsf{rk}}\vec{v}},\ \vec{\eta}^{\ \mathsf{rk}},\ 0\ )_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\ 1,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ 0^n,\ \boxed{\delta'^{\mathsf{rk}}_{\mathsf{ran}}\vec{v}},\ \vec{\eta}^{\ \mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{D}_1^*}, \quad (35)$$

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

Game 1-4-t ($t = 1, \ldots, \nu_3$): Game 1-4-0 is Game 1-3-ν_2. Game 1-4-t is the same as Game 4-$(t-1)$ except that the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct} = (C, \mathsf{verk}, S))$ is, if $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$,

$$\text{if } \mathsf{oct} = \mathsf{oct}_{\vec{x}^{(b)}},\ \boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \boxed{\delta'^{\mathsf{renc}}\vec{v}},\ \vec{\eta}^{\ \mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*}, \quad (36)$$

$$\text{if } \mathsf{oct} \neq \mathsf{oct}_{\vec{x}^{(b)}},\ \boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \boxed{\vec{r}''},\ \vec{\eta}^{\ \mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*}, \quad (37)$$

where $\delta'^{\mathsf{renc}} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{r}'' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 1-4-$(t-1)$.

Game 1-5: Game 1-5 is the same as Game 1-4-ν_3 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is:

$$\boldsymbol{c} := (\ \zeta,\ \boxed{\omega_0\vec{x}^{(0)} + \omega_1\vec{x}^{(1)}},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \quad (38)$$

where $\omega_0, \omega_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 1-4-ν_3.

Game 1-6-0: Game 1-6-0 is the same as Game 1-5 except that the reply to every decryption key query for $\vec{v}$ is

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ 0^n,\ \boxed{0^n},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \quad \boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ 0^n,\ \boxed{0^n},\ \vec{\eta}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*},$$

and the reply to every re-encryption key query for $(\vec{v}, \vec{x})$ is as

$$\boldsymbol{k}^{*\mathsf{rk}} := (\ 1,\ \delta^{\mathsf{rk}}\vec{v},\ 0^2,\ 0^n,\ \boxed{0^n},\ \vec{\eta}^{\ \mathsf{rk}},\ 0\ )_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\ 1,\ \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v},\ 0^2,\ 0^n,\ \boxed{0^n},\ \vec{\eta}^{\ \mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{D}_1^*},$$

and the reply to every re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct} = (C, S, \mathsf{verk}))$ is, if $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$,

$$\text{if } \mathsf{oct} = \mathsf{oct}_{\vec{x}^{(b)}},\ \boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \boxed{0^n},\ \vec{\eta}^{\ \mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*},$$

where all the other variables are generated as in Game 1-5.

Game 1-6-t ($t = 1, \ldots, \nu_3$): Game 1-6-t is the same as Game 1-6-$(t-1)$ except that the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct} = (C, S, \mathsf{verk}))$ is, if $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$,

$$\text{if } \mathsf{oct} \neq \mathsf{oct}_{\vec{x}^{(b)}},\ \boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1, \mathsf{verk}),\ 0^n,\ \boxed{0^n},\ \vec{\eta}^{\ \mathsf{renc}},\ 0\ )_{\mathbb{D}_1^*},$$

where all the variables are generated as in Game 1-6-$(t-1)$.

Game 1-7: Game 1-7 is the same as Game 1-6-ν_3 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is:

$$\boldsymbol{c} := (\ \zeta,\ \omega_0\vec{x}^{(0)} + \omega_1\vec{x}^{(1)},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{0^n,\ 0^n},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \quad (39)$$

where $\omega_0, \omega_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 1-6-ν_3.

Game 2-1: Game 2-1 is the same as Game 1-7 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is

$$\boldsymbol{c}_{\mathsf{ran}} := (\ 0,\ \omega\vec{x}^{(b)},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{\omega'\vec{x}^{(b)}},\ \boxed{\omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)}},\ 0^n,\ \varphi\ )_{\mathbb{B}},$$

where $\omega', \omega''_0, \omega''_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 1-7.

Game 2-2-h ($h = 1, \ldots, \nu_1$): Game 2-1 is Game 2-2-0. Game 2-2-h is the same as Game 2-2-$(h-1)$ except that the reply to the h-th decryption key query for $\vec{v}$, $(\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}})$, is of the form in Eq. (34), where $\delta' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-2-$(h-1)$.

Game 2-3-ℓ ($\ell = 1, \ldots, \nu_2$): Game 2-3-0 is Game 2-2-ν_1. Game 2-3-ℓ is the same as Game 2-3-$(\ell-1)$ except that the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x})$, $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$, is of the form in Eq. (35), where $\delta'^{\mathsf{rk}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-3-$(\ell-1)$.

Game 2-4-t ($t = 1, \ldots, \nu_3$): Game 2-4-0 is Game 2-3-ν_2. Game 2-4-t is the same as Game 2-4-$(t-1)$ except that the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct} = (C, \mathsf{verk}, S))$, $\boldsymbol{k}^{*\mathsf{renc}}$, is given, if $\mathsf{Ver}(\mathsf{verk}, C, S) = 1$, of the form in Eq. (36) if $\mathsf{oct} = \mathsf{oct}_{\vec{x}^{(b)}}$, or of the form in Eq. (37) if $\mathsf{oct} \neq \mathsf{oct}_{\vec{x}^{(b)}}$, where $\delta'^{\mathsf{renc}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-4-$(t-1)$.

Game 2-5: Game 2-5 is the same as Game 2-4-ν_3 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ is:

$$\boldsymbol{c}_{\mathsf{ran}} := (\ 0,\ \boxed{\omega_0\vec{x}^{(0)} + \omega_1\vec{x}^{(1)}},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ \varphi\ )_{\mathbb{B}}, \tag{40}$$

where $\omega_0, \omega_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-4-ν_3.

Let $\mathsf{Adv}^{(0'')}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(\iota\text{-}1)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(\iota\text{-}2\text{-}h)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(\iota\text{-}3\text{-}\ell)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(\iota\text{-}4\text{-}t)}_{\mathcal{A}}(\lambda)$, and $\mathsf{Adv}^{(\iota\text{-}5)}_{\mathcal{A}}(\lambda)$, be the advantages of $\mathcal{A}$ in Game $0''$, ι-1, ι-2-h, ι-3-ℓ, ι-4-t and ι-5 for $\iota = 1, 2$, respectively. We will show seven lemmas (Lemmas 18-27) that evaluate the gaps between pairs of neghoboring games. From these lemmas and Lemma 3-6, we obtain

$$\begin{aligned}
\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) &\leq \left|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}1)}_{\mathcal{A}}(\lambda)\right| \\
&\quad + \sum_{\iota=1}^{2} \Big(\textstyle\sum_{h=1}^{\nu_1} \left|\mathsf{Adv}^{(\iota\text{-}2\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\iota\text{-}2\text{-}h)}_{\mathcal{A}}(\lambda)\right| + \textstyle\sum_{\ell=1}^{\nu_2} \left|\mathsf{Adv}^{(\iota\text{-}3\text{-}(\ell-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\iota\text{-}3\text{-}\ell)}_{\mathcal{A}}(\lambda)\right| \\
&\qquad + \textstyle\sum_{t=1}^{\nu_3} \left|\mathsf{Adv}^{(\iota\text{-}4\text{-}(t-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\iota\text{-}4\text{-}t)}_{\mathcal{A}}(\lambda)\right| + \left|\mathsf{Adv}^{(\iota\text{-}4\text{-}\nu_3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\iota\text{-}5)}_{\mathcal{A}}(\lambda)\right| \Big) \\
&\quad + \left|\mathsf{Adv}^{(1\text{-}5)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}6\text{-}0)}_{\mathcal{A}}(\lambda)\right| + \textstyle\sum_{t=1}^{\nu_3} \left|\mathsf{Adv}^{(1\text{-}6\text{-}(t-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}6\text{-}t)}_{\mathcal{A}}(\lambda)\right| \\
&\quad + \left|\mathsf{Adv}^{(1\text{-}6\text{-}\nu_3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}7)}_{\mathcal{A}}(\lambda)\right| + \mathsf{Adv}^{(2\text{-}5)}_{\mathcal{A}}(\lambda). \\
&\leq \sum_{\iota=1}^{2} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}1}}(\lambda) + \textstyle\sum_{h=1}^{\nu_1}\sum_{j=1}^{2}\sum_{l=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}2\text{-}h\text{-}j\text{-}l}}(\lambda) \\
&\quad + \textstyle\sum_{\ell=1}^{\nu_2}\sum_{j=1}^{2} \Big(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}A\text{-}j}}(\lambda) + \sum_{l=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}3\text{-}\ell\text{-}B\text{-}j\text{-}l}}(\lambda) \Big) \\
&\quad + \textstyle\sum_{t=1}^{\nu_3} \Big(\sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}A\text{-}j}}(\lambda) + \sum_{l=1}^{2} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}B\text{-}l}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{\iota\text{-}4\text{-}t\text{-}C}}(\lambda) \Big) \Big) \\
&\quad + \textstyle\sum_{t=0}^{\nu_3} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}6\text{-}t}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}7}}(\lambda) + \epsilon,
\end{aligned}$$

where $\epsilon := (66\nu_1 + 70\nu_2 + 91\nu_3 + 20)/q$. This completes the proof of Lemma 17. □

Lemma 18. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_{1\text{-}1}}(\lambda) + 2/q$.*

Proof. Lemma 18 is proven in similar manner to Lemmas 6 and 7 in [29]. □

Lemma 19. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}2\text{-}j\text{-}2}$ and $\mathcal{B}_{1\text{-}2\text{-}j\text{-}4}$ for $j = 1, 2$ whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1\text{-}2\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}2\text{-}h)}_{\mathcal{A}}(\lambda)| \leq \sum_{j=1}^{2} \left(\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}j\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{1\text{-}2\text{-}h\text{-}j\text{-}4}}(\lambda)\right) + 20/q$, where $\mathcal{B}_{1\text{-}2\text{-}h\text{-}j\text{-}2}(\cdot) := \mathcal{B}_{1\text{-}2\text{-}j\text{-}2}(h, \cdot)$ and $\mathcal{B}_{1\text{-}2\text{-}h\text{-}j\text{-}4}(\cdot) := \mathcal{B}_{1\text{-}2\text{-}j\text{-}4}(h, \cdot)$ for $j = 1, 2$.*

Proof. Lemma 19 is proven in similar manner to Lemmas 7-10 in [29]. We define intermediate games, Sub-Game 1-2-h-1-ι and Sub-Game 1-2-h-2-ι ($\iota := 1 \ldots, 4$) as follows. The purpose of the game changes between Sub-Game 1-2-h-1-1 and Sub-Game 1-2-h-1-4 (resp. between Sub-Game 1-2-h-2-1 and Sub-Game 1-2-h-2-4) is that the normal form $\boldsymbol{k}^*$ (resp. $\boldsymbol{k}^*_{\mathsf{ran}}$) is changed to temporal 2 form.

Sub-Game 1-2-h-1-1 ($h = 1, \ldots, \nu_1$)**:** Sub-Game 1-2-h-1-1 is the same as Sub-Game 1-2-($h-1$)-2-4 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ where $m^{(0)} = m^{(1)}$ is:

$$\boldsymbol{c} := (\ \zeta,\ \omega\vec{x}^{(b)},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{\omega'\vec{x}^{(b)}},\ \boxed{\omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)}},\ 0^n,\ \varphi\ )_{\mathbb{B}},$$

where $\omega', \omega''_0, \omega''_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Sub-Game 1-2-($h-1$)-2-4.

Sub-Game 1-2-h-1-2 ($h = 1, \ldots, \nu_1$)**:** Sub-Game 1-2-h-1-2 is the same as Sub-Game 1-2-h-1-1 except that the reply to the decryption key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ \boxed{\delta'\vec{v}},\ 0^n,\ \vec{\eta}^{\,\mathsf{rk}},\ 0\ )_{\mathbb{B}^*}, \tag{41}$$

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

Sub-Game 1-2-h-1-3 ($h = 1, \ldots, \nu_1$)**:** Sub-Game 1-2-h-1-3 is the same as Sub-Game 1-2-h-1-2 except that the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ where $m^{(0)} = m^{(1)}$ is:

$$\boldsymbol{c} := (\ \zeta,\ \omega\vec{x}^{(b)},\ \rho(\mathsf{verk}^{\clubsuit}, 1),\ \boxed{\omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)}},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{42}$$

where $\omega'_0, \omega'_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Sub-Game 1-2-h-1-2.

Sub-Game 1-2-h-1-4 ($h = 1, \ldots, \nu_1$)**:** Sub-Game 1-2-h-1-4 is the same as Sub-Game 1-2-h-1-3 except that the reply to the decryption key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \delta\vec{v},\ 0^2,\ \boxed{0^n,\ \delta''\vec{v}},\ \vec{\eta}^{\,\mathsf{rk}},\ 0\ )_{\mathbb{B}^*}, \tag{43}$$

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

Sub-Game 1-2-h-2-1 ($h = 1, \ldots, \nu_1$)**:** Sub-Game 1-2-h-2-1 is the same as Sub-Game 1-2-h-1-4. That is, Sub-Game 1-2-h-2-1 is the same as Sub-Game 1-2-h-1-4 except that $\boldsymbol{c}$ of the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ where $m^{(0)} = m^{(1)}$ is temporal 1 form Eq. (33).

Sub-Game 1-2-h-2-2 ($h = 1, \ldots, \nu_1$)**:** Sub-Game 1-2-h-2-2 is the same as Sub-Game 1-2-h-2-1 except that the reply to the decryption key query for $\vec{v}$ is:

$$\boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{\delta'_{\mathsf{ran}}\vec{v}},\ 0^n,\ \vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*}, \tag{44}$$

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

Sub-Game 1-2-h-2-3 $(h = 1, \ldots, \nu_1)$**:** Sub-Game 1-2-h-2-3 is the same as Sub-Game 1-2-h-2-2. That is, Sub-Game 1-2-h-2-3 is the same as Sub-Game 1-2-h-2-2 except that $\boldsymbol{c}$ of the reply to the challenge query for $(\vec{x}^{(0)}, \vec{x}^{(1)}, m^{(0)}, m^{(1)})$ where $m^{(0)} = m^{(1)}$ is temporal 2 form Eq. (42).

Sub-Game 1-2-h-2-4 $(h = 1, \ldots, \nu_1)$**:** Sub-Game 1-2-h-2-4 is the same as Sub-Game 1-2-h-2-3 except that the reply to the decryption key query for $\vec{v}$ is:

$$\boldsymbol{k}^*_{\mathsf{ran}} := (\ 0,\ \delta_{\mathsf{ran}}\vec{v},\ 0^2,\ \boxed{0^n,\ \delta''_{\mathsf{ran}}\vec{v}},\ \vec{\eta}^{\,\mathsf{rk}}_{\mathsf{ran}},\ 0\ )_{\mathbb{B}^*}, \tag{45}$$

where $\delta''_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Sub-Game 1-2-h-2-3.

The advantage gaps between Sub-Game 1-2-h-1-1 and Sub-Game 1-2-h-1-4 (resp. Sub-Game 1-2-h-2-1 and Sub-Game 1-2-h-2-4) are bounded by the advantages of Problem 2 and Problem 4, respectively. The proof of this lemma is completed in a similar manner to Lemmas 7-10 in [29]. □

Lemma 20. *For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{B}_{1\text{-}3\text{-}A\text{-}j}$ and $\mathcal{B}_{1\text{-}3\text{-}B\text{-}j\text{-}l}$ for $j = 1, 2;\ l = 1, 2$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,*
$|\mathsf{Adv}^{(1\text{-}3\text{-}(\ell-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1\text{-}3\text{-}\ell)}_{\mathcal{A}}(\lambda)| \leq \sum_{j=1}^{2} \left(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}j\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}j\text{-}2}}(\lambda)\right) + 22/q$, *where* $\mathcal{B}_{1\text{-}3\text{-}\ell\text{-}A\text{-}j}(\cdot) := \mathcal{B}_{1\text{-}3\text{-}A\text{-}j}(\ell, \cdot),\ \mathcal{B}_{1\text{-}3\text{-}\ell\text{-}B\text{-}j\text{-}l}(\cdot) := \mathcal{B}_{1\text{-}3\text{-}B\text{-}j\text{-}l}(\ell, \cdot)$.

Proof. The proof strategy is similar to Lemma 11.

First, we execute a preliminary game transformation from Game 1-3-$(\ell-1)$ to Game 1-3-$(\ell-1)'$, which is the same as Game 1-3-$(\ell-1)$ except that flip a coin $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted when the variable $s_{\mathsf{rk},\ell}$ is determined (Definition 5) if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell}$. Since $s_{\mathsf{rk},\ell} := 0$ if $\vec{v}\cdot\vec{x}^{(0)} \neq 0 \ \wedge\ \vec{v}\cdot\vec{x}^{(1)} \neq 0$, or $\vec{v}\cdot\vec{x}^{(0)} = 0 \ \wedge\ \vec{v}\cdot\vec{x}^{(1)} = 0$, $s_{\mathsf{rk},\ell}$ is determined at the challenge step if the ℓ-th re-encryption key query is asked in Phase 1, and at the ℓ-th re-encryption key query step if it is asked in Phase 2. We define that $\mathcal{A}$ wins with probability 1/2 when the game is aborted (and the advantage in Game 1-3-$(\ell-1)'$ is $\mathsf{Pr}[\mathcal{A}$ wins in Game 1-3-$(\ell-1)'\,] - 1/2$ as well). Since τ_{rk} is independent from $s_{\mathsf{rk},\ell}$, the game is aborted with probability 1/2. Hence, the advantage in Game 1-3-$(\ell-1)'$ is a half of that in Game 1-3-$(\ell-1)$, i.e., $\mathsf{Adv}^{1\text{-}3\text{-}(\ell-1)'}_{\mathcal{A}}(\lambda) = 1/2 \cdot \mathsf{Adv}^{1\text{-}3\text{-}(\ell-1)}_{\mathcal{A}}(\lambda)$. Moreover, $\Pr[\mathcal{A}$ wins in Game 1-3-$(\ell-1)']$ $= \frac{1}{2}\left(\Pr[\mathcal{A}\text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] + \Pr[\mathcal{A}\text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1]\right)$ since τ_{rk} is uniformly and independently generated. As in the proof of Lemma 20, Eq. (17) holds.

Similarly, we define a new game, Game 1-3-ℓ'', which is the same as Game 1-3-ℓ except that flip a coin $\tau_{\mathsf{rk}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted when the variable $s_{\mathsf{rk},\ell}$ is determined if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell}$. Note that Game 1-3-$\ell'$ aborts if $\tau_{\mathsf{rk}} \neq s_{\mathsf{rk},\ell+1}$, which is different from Game 1-3-ℓ''. As in the proof of Lemma 20, Eq. (18) holds.

Case $\tau_{\mathsf{rk}} = 0$ As for the conditional probability with $\tau_{\mathsf{rk}} = 0$, we introduce three games as:

Sub-Game 1-3-ℓ-A-1**:** When $\tau_{\mathsf{rk}} = 0$, Sub-Game 1-3-ℓ-A-1 is the same as Game 1-3-$(\ell-1)'$ except that the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x}')$ are

$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}',\ \boxed{R}),$$

where $R \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q), \vec{r}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and all the other variables are generated as in Game 1-3-$(\ell-1)'$.

Sub-Game 1-3-ℓ-A-2**:** When $\tau_{\mathsf{rk}} = 0$, Sub-Game 1-3-ℓ-A-2 is the same as Sub-Game 1-3-ℓ-A-1 except that $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$ of the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x}')$ is of the form as given in Eq. (35).

Sub-Game 1-3-ℓ-A-3**:** When $\tau_{\mathsf{rk}} = 0$, Sub-Game 1-3-ℓ-A-3 is the same as Sub-Game 1-3-ℓ-A-2 except that $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ of the reply to the ℓ-th re-encryption key query for $(\vec{v}, \vec{x}')$ is

$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{W_1}),$$

where $W_1 \in GL(4n+4, \mathbb{F}_q)$ is defined in Game 0″ and it satisfies that $\mathbb{D}^*_1 = \mathbb{B}^* W_1$ and all the other variables are generated as in Sub-Game 1-3-ℓ-A-2. Note that Sub-Game 1-3-ℓ-A-3 is the same as Game 1-3-ℓ'' when $\tau_{\mathsf{rk}} = 0$.

As in the proof of Lemma 11,

$$\begin{aligned}
&\big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 0]\big| \\
&\le \big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-}1 \mid \tau_{\mathsf{rk}} = 0]\big| \\
&\quad + \big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-}1 \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-}2 \mid \tau_{\mathsf{rk}} = 0]\big| \\
&\quad + \big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-}2 \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell\text{-}A\text{-}3 \mid \tau_{\mathsf{rk}} = 0]\big| \\
&\le \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-3-}\ell\text{-}A\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-3-}\ell\text{-}A\text{-}2}}(\lambda) + 2/q. \qquad (46)
\end{aligned}$$

Case $\tau_{\mathsf{rk}} = 1$ As for the conditional probability with $\tau_{\mathsf{rk}} = 1$, we introduce eight games as in the proof of Lemma 19:

Eight Sub-Games, i.e., Sub-Game 1-3-ℓ-B-1-1, …, Sub-Game 1-3-ℓ-B-2-4 are defined as in similar manners to Sub-Game 1-2-h-1-1, …, Sub-Game 1-2-h-2-4: In Sub-Game 1-3-ℓ-B's, the reply to the ℓ-th re-encryption key query, $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}})$, are transformed to the form Eqs. (41),(43), and Eqs. (44),(45), respectively, instead of $(\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}})$ used in Sub-Game 1-2-h's.

As in the proof of Lemma 19, we have

$$\begin{aligned}
&\big|\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 1]\big| \\
&\le \sum_{\iota=1}^{2} \Big(\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-3-}\ell\text{-}B\text{-}1\text{-}\iota}}(\lambda) + \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{\text{1-3-}\ell\text{-}B\text{-}2\text{-}\iota}}(\lambda)\Big) + 20/q. \qquad (47)
\end{aligned}$$

Therefore, from Eqs. (17), (18), (46), and (47),

$$\begin{aligned}
&|\mathsf{Adv}^{\text{1-3-}(\ell-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\text{1-3-}\ell}_{\mathcal{A}}(\lambda)| \\
&= |\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] + \Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - 1 \\
&\quad - \big(\Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 0] + \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 1] - 1\big)\big| \\
&= |\Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 0] \\
&\quad + \Pr[\mathcal{A} \text{ wins in Game 1-3-}(\ell-1)' \mid \tau_{\mathsf{rk}} = 1] - \Pr[\mathcal{A} \text{ wins in Game 1-3-}\ell'' \mid \tau_{\mathsf{rk}} = 1]\big| \\
&\le \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-3-}\ell\text{-}A\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-3-}\ell\text{-}A\text{-}2}}(\lambda) + \sum_{\iota=1}^{2} \Big(\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-3-}\ell\text{-}B\text{-}1\text{-}\iota}}(\lambda) + \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{\text{1-3-}\ell\text{-}B\text{-}2\text{-}\iota}}(\lambda)\Big) + 22/q.
\end{aligned}$$

This completes the proof of Lemma 20. □

Lemma 21. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{\text{1-4-}A\text{-}j}$, $\mathcal{B}_{\text{1-4-}B\text{-}j}$ for $j = 1, 2$, and $\mathcal{B}_{\text{1-4-}C}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(\text{1-4-}(t-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\text{1-4-}t)}_{\mathcal{A}}(\lambda)| \le \sum_{j=1}^{2} \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-}j}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{\text{1-4-}t\text{-}C}}(\lambda) + 24/q$,*
where $\mathcal{B}_{\text{1-4-}t\text{-}A\text{-}j}(\cdot) := \mathcal{B}_{\text{1-4-}A\text{-}j}(t, \cdot)$, $\mathcal{B}_{\text{1-4-}t\text{-}B\text{-}j}(\cdot) := \mathcal{B}_{\text{1-4-}B\text{-}j}(t, \cdot)$, $\mathcal{B}_{\text{1-4-}t\text{-}C}(\cdot) := \mathcal{B}_{\text{1-4-}C}(t, \cdot)$.

Proof. The proof strategy is similar to Lemma 12.

First, we execute a preliminary game transformation from Game 1-4-$(t-1)$ to Game 1-4-$(t-1)'$, which is the same as Game 1-4-$(t-1)$ except that flip a coin $\tau_{\mathsf{renc}} \xleftarrow{\mathsf{U}} \{0,1,2\}$ before setup, and the game is aborted when the variable $s_{\mathsf{renc},t}$ is determined (Definition 5) if $\tau_{\mathsf{renc}} \neq s_{\mathsf{renc},t}$. Since $s_{\mathsf{renc},t}$ is defined by $\vec{v}_t, \vec{x}^{(0)}, \vec{x}^{(1)}, \mathsf{oct}_t, \mathsf{oct}_{\vec{x}^{(b)}}$, the value of $s_{\mathsf{renc},t}$ is determined at the t-th re-encryption query step if it is asked in Phase 2. We define that $\mathcal{A}$ wins with probability $1/2$ when the game is aborted (and the advantage in Game 1-4-$(t-1)'$ is $\mathsf{Pr}[\mathcal{A}$ wins in Game 1-4-$(t-1)'\,] - 1/2$ as well). Since τ_{renc} is independent from $s_{\mathsf{renc},t}$, the game is aborted with probability $2/3$. Hence, the advantage in Game 1-4-$(t-1)'$ is a third of that in Game 1-4-$(t-1)$, i.e., $\mathsf{Adv}_{\mathcal{A}}^{\text{1-4-}(t-1)'}(\lambda) = 1/3 \cdot \mathsf{Adv}_{\mathcal{A}}^{\text{1-4-}(t-1)}(\lambda)$. Moreover, $\Pr[\mathcal{A}$ wins in Game 1-4-$(t-1)'] = \frac{1}{3}\sum_{\iota=0}^{2} \Pr[\mathcal{A}$ wins in Game 1-4-$(t-1)' \mid \tau_{\mathsf{renc}} = \iota]$ since τ_{renc} is uniformly and independently generated. Therefore,

$$\begin{aligned}\mathsf{Adv}_{\mathcal{A}}^{\text{1-4-}(t-1)}(\lambda) &= 3 \cdot \mathsf{Adv}_{\mathcal{A}}^{\text{1-4-}(t-1)'}(\lambda) \\ &= \sum_{\iota=0}^{2} \Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \,|\, \tau_{\mathsf{renc}} = \iota] - 3/2. \end{aligned} \tag{48}$$

Similarly, we define a new game, Game 1-4-t'', which is the same as Game 1-4-t except that flip a coin $\tau_{\mathsf{renc}} \xleftarrow{\mathsf{U}} \{0,1,2\}$ before setup, and the game is aborted when the variable $s_{\mathsf{renc},t}$ is determined if $\tau_{\mathsf{renc}} \neq s_{\mathsf{renc},t}$. Note that Game 1-4-$t'$ aborts if $\tau_{\mathsf{renc}} \neq s_{\mathsf{renc},t+1}$, which is different from Game 1-4-t''. Similarly to Eq. (48),

$$\mathsf{Adv}_{\mathcal{A}}^{\text{1-4-}(t-1)}(\lambda) = 3 \cdot \mathsf{Adv}_{\mathcal{A}}^{\text{1-4-}t''}(\lambda) \;= \sum_{\iota=0}^{2} \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \,|\, \tau_{\mathsf{renc}} = \iota] - 3/2. \tag{49}$$

Case $\tau_{\mathsf{renc}} = 0$ As for the conditional probability with $\tau_{\mathsf{renc}} = 0$, we introduce three games as:

Sub-Game 1-4-t-A-1**:** When $\tau_{\mathsf{renc}} = 0$, Sub-Game 1-4-t-A-1 is the same as Game 1-4-$(t-1)'$ except that the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct})$ are

$$\mathsf{ct}_{1,\vec{x}'}^{\mathsf{renc}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{R}),$$

where $R \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$ and all the other variables are generated as in Game 1-4-$(t-1)'$.

Sub-Game 1-4-t-A-2**:** When $\tau_{\mathsf{renc}} = 0$, Sub-Game 1-4-t-A-2 is the same as Sub-Game 1-4-t-A-1 except that $\boldsymbol{k}^{*\mathsf{renc}}$ of the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct})$ are of the form as given in Eq. (36).

Sub-Game 1-4-t-A-3**:** When $\tau_{\mathsf{renc}} = 0$, Sub-Game 1-4-t-A-3 is the same as Sub-Game 1-4-t-A-2 except that $\mathsf{ct}_{\vec{x}'}^{\mathsf{rk}}$ of the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct})$ is

$$\mathsf{ct}_{1,\vec{x}'}^{\mathsf{renc}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{W_1}),$$

where $W_1 \in GL(4n+4, \mathbb{F}_q)$ is defined in Game $0''$ and it satisfies that $\mathbb{D}_1^* = \mathbb{B}^* W_1$ and all the other variables are generated as in Sub-Game 1-4-t-A-2. Note that Sub-Game 1-4-t-A-3 is the same as Game 1-4-t'' when $\tau_{\mathsf{renc}} = 0$.

As in the proof of Lemma 12 (Claims 5, 6, and 7),

$$\begin{aligned}&\big|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = 0]\big| \\ &\le \big|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t\text{-}A\text{-}1 \mid \tau_{\mathsf{renc}} = 0]\big| \\ &\quad + |\Pr[\mathcal{A} \text{ wins in Game 1-4-}t\text{-}A\text{-}1 \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t\text{-}A\text{-}2 \mid \tau_{\mathsf{renc}} = 0]| \\ &\quad + |\Pr[\mathcal{A} \text{ wins in Game 1-4-}t\text{-}A\text{-}2 \mid \tau_{\mathsf{renc}} = 0] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t\text{-}A\text{-}3 \mid \tau_{\mathsf{renc}} = 0]| \\ &\le \mathsf{Adv}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-}1}}^{\mathsf{IPE},\mathsf{AH}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-}2}}^{\mathsf{IPE},\mathsf{AH}}(\lambda) + 2/q. \end{aligned} \tag{50}$$

Case $\tau_{\mathsf{renc}} = 1$ As for the conditional probability with $\tau_{\mathsf{renc}} = 1$, we introduce four new games.

Four Sub-Games, i.e., Sub-Game 1-4-t-B-1, ..., Sub-Game 1-4-t-B-4 are defined as in similar manners to Sub-Game 1-2-h-1-1, ..., Sub-Game 1-2-h-1-4: In Sub-Game 1-4-t-B's, the reply to the t-th re-encryption query, $\boldsymbol{k}^{*\mathsf{renc}}$, are transformed to the form Eqs. (41),(34), respectively, instead of $\boldsymbol{k}^*$ used in Sub-Game 1-2-h's.

As in the proof of Lemma 19, we have

$$\begin{aligned}&\left|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 1] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = 1]\right| \\ &\leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-}2}}(\lambda) + 20/q. \end{aligned} \tag{51}$$

Case $\tau_{\mathsf{renc}} = 2$ As for the conditional probability with $\tau_{\mathsf{renc}} = 2$, we introduce a game as:

Sub-Game 1-4-t-C**:** When $\tau_{\mathsf{renc}} = 2$, Sub-Game 1-4-t-C is the same as Game 1-4-$(t-1)'$ except that $\boldsymbol{k}^{*\mathsf{renc}}$ of the reply to the t-th re-encryption query for $(\vec{v}, \vec{x}', \mathsf{oct})$ is of the form as given in Eq.(37). Note that Sub-Game 1-4-t-C is the same as Game 1-4-t'' when $\tau_{\mathsf{renc}} = 2$.

From Claim 9,

$$\begin{aligned}&\left|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 2] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = 2]\right| \\ &= \left|\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = 2] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t\text{-}B \mid \tau_{\mathsf{renc}} = 2]\right| \\ &\leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{\text{1-4-}t\text{-}C}}(\lambda) + 2/q. \end{aligned} \tag{52}$$

Therefore, from Eqs. (48), (49), (50), (51), and (52),

$$\begin{aligned}&|\mathsf{Adv}^{\text{1-4-}(t-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\text{1-4-}t}_{\mathcal{A}}(\lambda)| \\ &= \Big|\textstyle\sum_{\iota=0}^{2} \Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = \iota] - 3/2 \\ &\quad -(\textstyle\sum_{\iota=0}^{2} \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = \iota] - 3/2)\Big| \\ &= \Big|\textstyle\sum_{\iota=0}^{2} (\Pr[\mathcal{A} \text{ wins in Game 1-4-}(t-1)' \mid \tau_{\mathsf{renc}} = \iota] - \Pr[\mathcal{A} \text{ wins in Game 1-4-}t'' \mid \tau_{\mathsf{renc}} = \iota])\Big| \\ &\leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{\text{1-4-}t\text{-}A\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P4}}_{\mathcal{B}_{\text{1-4-}t\text{-}B\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{\text{1-4-}t\text{-}C}}(\lambda) + 24/q. \end{aligned}$$

This completes the proof of Lemma 21. □

Lemma 22. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}^{(\text{1-4-}\nu_3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\text{1-5})}_{\mathcal{A}}(\lambda)| \leq 1/q$,.*

Proof. Lemma 22 is proven in a similar manner to Lemma 11 in [29]. □

Lemma 23. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{\text{1-5}}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(\text{1-5})}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\text{1-6-0})}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{\text{1-6-0}}}(\lambda)$.*

Proof. Lemma 23 is proven in a similar manner to Lemma 14 using Problem 2 instead of Problem 4. □

Lemma 24. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{\text{1-6}}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(\text{1-6-}(t-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(\text{1-6-}t)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{\text{1-6-}t}}(\lambda) + 2/q$, where $\mathcal{B}_{\text{1-6-}t}(\cdot) := \mathcal{B}_{\text{1-6}}(t, \cdot)$.*

Proof. Lemma 24 is proven in a similar manner to Claim 9. □

Lemma 25. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}7}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(1\text{-}6)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1\text{-}7)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{1\text{-}7}}^{\mathsf{P1}}(\lambda) + 2/q$.*

Proof. Lemma 25 is proven in a similar manner to Lemma 18. □

The game changes between Game 1-7 and Game 2-4-ν_3 is similar to those between Game $0''$ and Game 1-4-ν_3 except the form of the component of the challenge ciphertext $\boldsymbol{c}_{\mathsf{ran}}$ is changed to *unbiased* form. Therefore, the advantage of between Game 1-7 and Game 2-4-ν_3 is bounded by a similar manner to those obtained in Lemmas 18–21.

Lemma 26. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}4\text{-}\nu_3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}5)}(\lambda)| \leq 1/q,$.*

Proof. Lemma 26 is proven in similar manner to Lemma 11 in [29].

Lemma 27. *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}5)}(\lambda) = 0$.*

Proof. The value of b is independent from adversary's view in Game 2-5. So, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}5)}(\lambda) = 0$. □

D.4 Proof of Theorem 3 (PAH-RC: Predicate- and Attribute-Hiding for Re-Encrypted Ciphertexts)

The variable $s_{\mathsf{m},\mathsf{x},\mathsf{v}}$ in Definition 6 is used for defining cases in the proof of Theorem 3. For that purpose, the following claims are important, which are deduced from the restriction described in Challenge phase.

- When $s_{\mathsf{m},\mathsf{x},\mathsf{v}} = 0$, it holds that $R(v', x'^{(0)}) = R(v', x'^{(1)}) = 0$ for any decryption key query v'.
- When $s_{\mathsf{m},\mathsf{x},\mathsf{v}} = 1$, it holds that $R(v', x'^{(0)}) = R(v', x'^{(1)})$ for any decryption key query v'.

Theorem 3. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encrypted ciphertexts against chosen plaintext attacks provided the underlying IPE scheme is fully attribute-hiding.* For any adversary $\mathcal{A}$ there exist probabilistic machines $\mathcal{E}_{1\text{-}1}$, $\mathcal{E}_{1\text{-}2}$, $\mathcal{E}_{2\text{-}1}$ 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,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PAH\text{-}RC}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}_{1\text{-}1}}^{\mathsf{IPE,AH}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{1\text{-}2}}^{\mathsf{IPE,AH}}(\lambda) + \frac{1}{2}(\mathsf{Adv}_{\mathcal{E}_{2\text{-}1}}^{\mathsf{IPE,AH}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{2\text{-}2}}^{\mathsf{IPE,AH}}(\lambda)).$$

Proof. First, we execute a game transformation from the original security game (Game 0) to Game $0'$ which is the same as Game 0 except flip a coin $\tau_{\mathsf{m},\mathsf{x},\mathsf{v}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup and game is aborted if $\tau_{\mathsf{m},\mathsf{x},\mathsf{v}} \neq s_{\mathsf{m},\mathsf{x},\mathsf{v}}$. We define that $\mathcal{A}$ wins with probability $1/2$ when the game is aborted.

Hence the advantage in Game $0'$ is a half of that in Game 0' i.e., $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) = 1/2 \cdot \mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$ where $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{PAH\text{-}RC}}(\lambda)$. Moreover, $\Pr[\mathcal{A} \text{ wins}] := 1/2 \cdot (\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 0] + \Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 1])$ in Game $0'$.

$$\begin{aligned}
\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PAH\text{-}RC}}(\lambda) &= \mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) = 2 \cdot \mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) \\
&= \Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 0] + \Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 1] - 1 \\
&= (\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 0] - 1/2) + (\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 1] - 1/2).
\end{aligned}$$

As for the conditional probabilities with $\tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 0$ and $\tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 1$, i.e., $\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 0]$ and $\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m},\mathsf{x},\mathsf{v}} = 1]$, Lemmas 28 and 32 hold. Therefore, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PAH\text{-}RC}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}_{1\text{-}1}}^{\mathsf{IPE,AH}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{1\text{-}2}}^{\mathsf{IPE,AH}}(\lambda) + \frac{1}{2}(\mathsf{Adv}_{\mathcal{E}_{2\text{-}1}}^{\mathsf{IPE,AH}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{2\text{-}2}}^{\mathsf{IPE,AH}}(\lambda))$. This completes the proof of Theorem 3. □

Corollary 1-2. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encrypted ciphertexts against chosen plaintext attacks under the DLIN assumption provided the underlying IPE scheme is given by the OT12 IPE scheme.*

Proof of Theorem 3 (PAH-RC) in the Case $\tau_{\mathsf{m,x,v}} = 0$

Lemma 28. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encrypted ciphertexts against chosen plaintext attack in the case $\tau_{\mathsf{m,x,v}} = 0$ under the attribute-hiding security of the underlying IPE scheme.*

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

$$\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m,x,v}} = 0] - 1/2 \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}2}}(\lambda).$$

Proof Outline of Lemma 28. The purpose of this game transformation is that $\{\mathsf{ct}^{\mathsf{renc}}_{\iota,\vec{x}^{(b)}}\}_{\iota=1,2}$ are changed to ciphertexts with a *random* attribute and a *random* plaintext. We employ Game 0′, Game 1 and Game 2. In Game 1, $\{\mathsf{ct}^{\mathsf{renc}}_{\iota,\vec{x}^{(b)}}\}_{\iota=1,2}$ are changed to $\{\mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{r}_\iota, R_\iota)\}_{\iota=1,2}$, respectively, where $\vec{r}_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and $R_\iota \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$ for $\iota = 1, 2$. In the Case $\tau_{\mathsf{m,x,v}} = 0$, the adversary does not make decryption query $\vec{v}$ such that $\vec{v} \cdot \vec{x}^{(b)} = 0$. So, $\{\mathsf{ct}^{\mathsf{renc}}_{\iota,\vec{x}^{(b)}}\}_{\iota=1,2}$ is changed to $\{\mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{r}_\iota, R_\iota)\}_{\iota=1,2}$ by using the attribute-hiding security of the underlying IPE scheme.

To prove the advantage gap between Game 0′ and Game 1 is bounded by the advantage of the attribute-hiding security of the underlying IPE scheme, we construct a simulator of the challenger of Game 0′ or Game 1 by using an instance with $\mathsf{pk}^{\mathsf{IPE}}$ of the underlying IPE scheme.

Proof of Lemma 28. To prove Lemma 28, we consider the following 2 games. In Game 0′, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0′: Same as a Game 0 except that flip a coin $\tau_{\mathsf{m,x,v}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted if $\tau_{\mathsf{m,x,v}} \neq s_{\mathsf{m,x,v}}$. In order to prove Lemma 28, we consider the case with $\tau_{\mathsf{m,x,v}} = 0$. We only describe the components which are changed in the other games. $\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, \{\mathsf{ct}^{\mathsf{renc}}_{\iota,\vec{x}'^{(b)}}\}_{\iota=1,2}$ of the reply to a challenge query for $(m^{(0)}, m^{(1)}, \vec{x}^{(0)}, \vec{x}^{(1)}, \vec{v}^{(0)}, \vec{v}^{(1)}, \vec{x}'^{(0)}, \vec{x}'^{(1)})$ are:

$$\begin{aligned}
&\boldsymbol{k}^{*\mathsf{renc}} := (\ 1,\ \boxed{\delta^{\mathsf{renc}} \vec{v}^{(b)}},\ \sigma(-1, \mathsf{verk}^{\clubsuit}),\ 0^n,\ 0^n,\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{D}_1^*},\\
&\boldsymbol{c}^{\mathsf{renc}} := (\boxed{\zeta^{\mathsf{renc}}},\ \boxed{\omega^{\mathsf{renc}} \vec{x}^{(b)}},\ \rho^{\mathsf{renc}}(\mathsf{verk}^{\clubsuit}, 1),\ 0^n,\ 0^n,\ \varphi^{\mathsf{renc}})_{\mathbb{D}_2},\ \ c_T^{\mathsf{renc}} := m^{(b)} \cdot g_T^{\zeta^{\mathsf{renc}}},\\
&\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(b)}}, \boxed{W_1}),\quad \mathsf{ct}^{\mathsf{renc}}_{2,\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(b)}}, \boxed{W_2}),
\end{aligned} \tag{53}$$

where $W_1, W_2 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q),\ \mathbb{D}_1^* := \mathbb{B}^* W_1,\ \mathbb{D}_2 := \mathbb{B} W_2$.

Game 1: Game 1 is the same as Game 0′ except that the reply to the challenge query for $(m^{(0)}, m^{(1)}, \vec{x}^{(0)}, \vec{x}^{(1)}, \vec{v}^{(0)}, \vec{v}^{(1)}, \vec{x}'^{(0)}, \vec{x}'^{(1)})$ is

$$\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{r}_1}, \boxed{R_1}),\quad \mathsf{ct}^{\mathsf{renc}}_{2,\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{r}_2}, \boxed{R_2}), \tag{54}$$

where $\vec{r}_1, \vec{r}_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and $R_1, R_2 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$ (R_1, R_2 are independent from W_1, W_2) and all the other variables are generated as in Game 0′.

Game 2: Game 2 is the same as Game 1 except that the reply to the challenge query for $(m^{(0)}, m^{(1)}, \vec{x}^{(0)}, \vec{x}^{(1)}, \vec{v}^{(0)}, \vec{v}^{(1)}, \vec{x}'^{(0)}, \vec{x}'^{(1)})$ is

$$\begin{aligned}
&\boldsymbol{k}^{*\mathsf{renc}} = (\ 1,\ \boxed{\vec{u}},\ \sigma(-1, \mathsf{verk}^{\clubsuit}),\ 0^n,\ 0^n,\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{D}_1^*},\\
&\boldsymbol{c}^{\mathsf{renc}} := (\ \boxed{\zeta'},\ \ \boxed{\vec{u}'},\ \rho^{\mathsf{renc}}(\mathsf{verk}^{\clubsuit}, 1),\ 0^n,\ 0^n,\ \varphi^{\mathsf{renc}}\ )_{\mathbb{D}_2},\ \ c_T^{\mathsf{renc}} := m^{(b)} \cdot g_T^{\zeta^{\mathsf{renc}}},
\end{aligned}$$

where $\vec{u}, \vec{u}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, $\zeta' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ (ζ' is independent from ζ^{renc}) and all the other variables are generated as in Game 1.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda)$ be the advantages of $\mathcal{A}$ in Games 0′, 1, and 2, respectively. We will show three lemmas (Lemma 29- 31) that evaluate the gaps between pairs of neghoboring games. We obtain $\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) \leq \left|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| + \left|\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda)\right| + \mathsf{Adv}_{\mathcal{A}}^{(2)}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}_{1\text{-}1}}^{\mathsf{IPE,AH}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{1\text{-}2}}^{\mathsf{IPE,AH}}(\lambda)$. This completes the proof of Lemma 28. □

Lemma 29. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}1}$ and $\mathcal{B}_{1\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{1\text{-}1}}^{\mathsf{IPE,AH}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_{1\text{-}2}}^{\mathsf{IPE,AH}}(\lambda)$.*

Proof. In order to prove to Lemma 29, we construct probabilistic machines $\mathcal{B}_{1\text{-}1}$ and $\mathcal{B}_{1\text{-}2}$ against the fully attribute-hiding security using an adversary $\mathcal{A}$ in a security game (Game 0′ or Game 1) as a black box. First, we consider the intermediate game Game 1′. Game 1' is the same as Game 0′ except that $\mathsf{ct}_{\vec{x}'}^{\mathsf{renc}}$ of the reply to the challenge re-encrypted ciphertext is of the form in Eq.(54). In order to prove that $|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1')}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{1\text{-}1}}^{\mathsf{IPE,AH}}(\lambda)$, we construct a probabilistic machine $\mathcal{B}_{1\text{-}1}$ against the fully attribute-hiding security using an adversary $\mathcal{A}$ in a security game (Game 0′ or Game 1′) as a black box as follows:

1. $\mathcal{B}_{1\text{-}1}$ is given a public key $\mathsf{pk}^{\mathsf{IPE}}$ of the IPE, from the challenger for the attribute-hiding security of the underlying IPE.
2. $\mathcal{B}_{1\text{-}1}$ plays a role of the challenger in the security game against $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{1\text{-}1}$ generates a public and secret key as follows: $(\mathsf{param}_n, \mathbb{B} = (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{4n+3}), \mathbb{B}^* = (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_{4n+3}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4)$, $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n+2}, \boldsymbol{b}_{4n+3})$, $\widehat{\mathbb{B}}^* := (\boldsymbol{b}_{n+1}^*, \boldsymbol{b}_{n+2}^* \boldsymbol{b}_{3n+3}^*, \ldots, \boldsymbol{b}_{4n+2}^*)$. Finally, $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with $\mathsf{pk} := (1^\lambda, \mathsf{pk}^{\mathsf{IPE}}, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$.
4. When a decryption key query is issued for a vector $\vec{v}$, $\mathcal{B}_{1\text{-}1}$ computes a normal form decryption key $\boldsymbol{k}^*, \boldsymbol{k}_{\mathsf{ran}}^*$ using $\mathbb{B}^*$ and ask a key query $\vec{v}$ to the challenger of the underlying IPE, then obtain the decryption key $\mathsf{sk}_{\vec{v}}^{\mathsf{IPE}}$, and provides $\mathcal{A}$ with a decryption key $\mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}_{\mathsf{ran}}^*, \mathsf{sk}_{\vec{v}}^{\mathsf{IPE}})$.
5. When a re-encryption key query is issued for $(\vec{v}, \vec{x}')$, $\mathcal{B}_{1\text{-}1}$ computes a normal form re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}_{\mathsf{ran}}^{*\mathsf{rk}}, \widehat{\mathbb{D}}_1^*, \mathsf{ct}_{\vec{x}'}^{\mathsf{rk}}, \mathsf{prect}_{\vec{x}'})$ using $\mathbb{B}^*$ and $\mathsf{pk}^{\mathsf{IPE}}$. Finally, $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with a re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'}$.
6. When a re-encryption query is issued for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} = (\vec{x}, \boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T, \mathsf{verk}, S))$, if $\mathsf{Ver}(\mathsf{verk}, (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), S) \neq 1$, $\mathcal{B}_{1\text{-}1}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{B}_{1\text{-}1}$ computes a normal form re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'} := (\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c_T^{\mathsf{renc}}, \{\mathsf{ct}_{\iota,\vec{x}'}^{\mathsf{renc}}\}_{\iota=1,2})$ using $\mathbb{B}$, $\mathbb{B}^*$ and $\mathsf{pk}^{\mathsf{IPE}}$. $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with a re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'}$.
7. When the challenge query is issued for $(m^{(0)}, m^{(1)}, \vec{x}^{(0)}, \vec{x}^{(1)}, \vec{v}^{(0)}, \vec{v}^{(1)}, \vec{x}'^{(0)}, \vec{x}'^{(1)})$, $\mathcal{B}_{1\text{-}1}$ picks a bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ and generates $(\mathsf{sigk}^{\clubsuit}, \mathsf{verk}^{\clubsuit}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$. $\mathcal{B}_{1\text{-}1}$ computes a normal form $\boldsymbol{k}^{*\mathsf{renc}}$, $\boldsymbol{c}^{\mathsf{renc}}$, c_T^{renc} and $\mathsf{ct}_{\vec{x}^{(b)}}^{\mathsf{rk}}$ using $\mathbb{B}$, $\mathbb{B}^*$ and $\mathsf{pk}^{\mathsf{IPE}}$. Next, $\mathcal{B}_{1\text{-}1}$ submits $(X^{(b)} := W_2, X^{(1-b)} := R, \vec{x}^{(b)} := \vec{x}'^{(b)}, \vec{x}^{(1-b)} := \vec{r})$ to the attribute-hiding challenger of the underlying IPE scheme where $\vec{r} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$ and $R \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$ and receives $\mathsf{ct}_{\vec{x}^{(\beta)}}$ for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. Finally, $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with a challenge re-encrypted ciphertext $\mathsf{rct}_{\vec{x}^{(b)}} := (\boldsymbol{c}^{\mathsf{renc}}, c_T^{\mathsf{renc}}, \boldsymbol{k}^{*\mathsf{renc}}, \mathsf{ct}_{1,\vec{x}'^{(b)}}^{\mathsf{renc}}, \mathsf{ct}_{2.\vec{x}'^{(b)}}^{\mathsf{renc}} := \mathsf{ct}_{\vec{x}'^{\beta}})$.
8. $\mathcal{A}$ finally outputs bit b'. $\mathcal{B}_{1\text{-}1}$ outputs $\beta = 0$ if $b' = b$, otherwise outputs $\beta = 1$.

Since $\mathsf{ct}_{2,\vec{x}'}^{\mathsf{renc}}$ of the challenge re-encrypted ciphertext is of the form Eq.(53) (resp. of the form Eq.(54) if $\beta = 0$ (resp. $\beta = 1$), the view of $\mathcal{A}$ given by $\mathcal{B}_{1\text{-}1}$ is distributed as Game 1′ (resp. Game 0′) if $\beta = 0$ (resp. $\beta = 1$). Then, $\left|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1')}(\lambda)\right| \leq |\Pr[b = b'] - 1/2| \leq \mathsf{Adv}_{\mathcal{B}_{1\text{-}1}}^{\mathsf{IPE,AH}}(\lambda)$.

Next, in order to prove that $|\mathsf{Adv}^{(1')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda)$, we construct a probabilistic machine $\mathcal{B}_{1\text{-}2}$ against the fully attribute-hiding security using an adversary $\mathcal{A}$ in a security game (Game 1' or Game 1) as a black box. Game 1 is the same as Game 1' except that $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ of the reply to the challenge re-encrypted ciphertext $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} = \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{r}\,', W_1)$ where $\vec{r}\,' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$. Hence, this proof is similar to the above proof. So, we have $|\mathsf{Adv}^{(1')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda)$.

By using hybrid argument, we have $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda)$. □

Lemma 30. *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda)$*

Proof. The basis of $\boldsymbol{c}^{\mathsf{renc}}$, that is $\mathbb{D}_2 := \mathbb{B}W_2$ is random basis for the adversary $\mathcal{A}$ since the information of W_2 appears only in $\boldsymbol{c}^{\mathsf{renc}}$ in Game 1. So, from the adversary's view, $(\zeta^{\mathsf{renc}}, \omega^{\mathsf{renc}}\vec{x}, \rho^*(\mathsf{verk}^{\clubsuit}, 1), 0^n, 0^n, \varphi^{\mathsf{renc}})_{\mathbb{D}_2}$ and $\boldsymbol{c}^{\mathsf{renc}} := (\zeta'^{\mathsf{renc}}, \omega^{\mathsf{renc}}\vec{x}, \rho^*(\mathsf{verk}^{\clubsuit}, 1), 0^n, 0^n, \varphi^{\mathsf{renc}})_{\mathbb{D}_2}$ where $\zeta'^{\mathsf{renc}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ are information theoretically indistinguishable. This completes the proof of Lemma 30 □

Lemma 31. *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda) = 0$.*

Proof. The value of b is independent from adversary's view in Game 2. So, $\mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda) = 0$. □

Proof of Theorem 3 (PAH-RC) in the Case $\tau_{\mathsf{m,x,v}} = 1$

Lemma 32. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encrypted ciphertexts against chosen plaintext attack in the case $\tau_{\mathsf{m,x,v}} = 1$ under the fully-attribute-hiding security of the underlying IPE scheme.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_{2\text{-}1}$ 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 the case $\tau_{\mathsf{m,x,v}} = 1$,

$$\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{m,x,v}} = 1] - 1/2 \leq \frac{1}{2}(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{2\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{2\text{-}2}}(\lambda)).$$

Proof Outline Lemma 32. The purpose of this game transformation is that $\{\mathsf{ct}^{\mathsf{renc}}_{\iota,\vec{x}'^{(b)}}\}_{\iota=1,2}$ are changed to ciphertexts with the opposite attribute $\vec{x}'^{(1-b)}$. We employ Game 0′ and Game 1. In Game 1, $\{\mathsf{ct}^{\mathsf{renc}}_{\iota,\vec{x}'^{(b)}}\}_{\iota=1,2}$ are changed to $\mathsf{ct}^{\mathsf{renc}}_{\iota,\vec{x}'^{(b)}} \xleftarrow{\mathsf{U}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}'^{(1-b)}, W_\iota)$, respectively, by using the fully-attribute-hiding security of the IPE scheme. For the proof, we construct a simulator of the challenger of Game 0′ or Game 1 by using an instance with $\mathsf{pk}^{\mathsf{IPE}}$ of the underlying IPE scheme.

Proof of Lemma 32. To prove Lemma 32, we consider the following 2 games. In Game 0′, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0′: Same as a Game 0 expect that flip a coin $\tau_{\mathsf{m,x,v}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted if $\tau_{\mathsf{m,x,v}} \neq s_{\mathsf{m,x,v}}$. In order to prove Lemma 32, we consider the case with $\tau_{\mathsf{m,x,v}} = 1$. We only describe the components which are changed in the other games. The reply to a challenge query for $(m, \vec{x}, \vec{v}, \vec{x}'^{(0)}, \vec{x}'^{(1)})$ with $(m, \vec{x}, \vec{v}) := (m^{(0)}, \vec{x}^{(0)}, \vec{v}^{(0)}) = (m^{(1)}, \vec{x}^{(1)}, \vec{v}^{(1)})$ is:

$$\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(b)}}, W_1), \quad \mathsf{ct}^{\mathsf{renc}}_{2,\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(b)}}, W_2),$$

where $W_1, W_2 \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$.

Game 1: Game 1 is the same as Game $0'$ except that the reply to the challenge query for $(m, \vec{x}, \vec{v}, \vec{x}'^{(0)}, \vec{x}'^{(1)})$ with $(m, \vec{x}, \vec{v}) := (m^{(0)}, \vec{x}^{(0)}, \vec{v}^{(0)}) = (m^{(1)}, \vec{x}^{(1)}, \vec{v}^{(1)})$ is

$$\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(1-b)}}, W_1), \quad \mathsf{ct}^{\mathsf{renc}}_{2,\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(1-b)}}, W_2),$$

and all the other variables are generated as in Game $0'$.

Let $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda)$ and $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)$ be the advantages of $\mathcal{A}$ in Game $0'$ and Game 1, respectively. We will show two lemmas (Lemma 33- 34) that evaluate the gaps between pairs of neghoboring games. We obtain $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) \leq \left|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)\right| + \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}2}}(\lambda) + \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)$. From Lemma 34, $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) \leq \frac{1}{2}(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}2}}(\lambda))$ This completes the proof of Lemma 32. □

Lemma 33. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}1}$ and $\mathcal{B}_{2\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}2}}(\lambda)$.*

Proof. Lemma 33 is proven in similar manner to Lemma 29.

Lemma 34. *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) = -\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda)$.*

Proof. The challenge re-encrypted ciphertext for the opposite bit $1-b$ to the challenge bit b and the others components are normal forms in Game 1 Hence, success probability $\Pr[\mathsf{Succ}^{(1)}_{\mathcal{A}}]$ in Game 1 is $1 - \Pr[\mathsf{Succ}^{(0')}_{\mathcal{A}}]$, where $\mathsf{Succ}^{(0')}_{\mathcal{A}}$ is success probability in Game $0'$. Therefore, we have $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) = -\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda)$. □

D.5 Proof of Theorem 4 (PAH-RK: Predicate- and Attribute-Hiding for Re-Encryption Keys)

The variable s_{v} in Definition 7 is used for defining cases in the proof of Theorem 4. For that purpose, the following claims are important, which are deduced from the restriction described in Challenge phase.

- When $s_{\mathsf{v}} = 0$, it holds that $R(v', x'^{(0)}) = R(v', x'^{(1)}) = 0$ for any decryption key query v'.
- When $s_{\mathsf{v}} = 1$, it holds that $R(v', x'^{(0)}) = R(v', x'^{(1)})$ for any decryption key query v'.

Theorem 4. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encryption keys against chosen plaintext attacks provided the underlying IPE scheme is fully attribute-hiding.*

For any adversary $\mathcal{A}$ there exist probabilistic machines $\mathcal{E}_{1\text{-}1}$, $\mathcal{E}_{1\text{-}2}$, $\mathcal{E}_{2\text{-}1}$ 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,

$$\mathsf{Adv}^{\mathsf{PAH\text{-}RK}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}2}}(\lambda) + \frac{1}{2}(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{2\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{2\text{-}2}}(\lambda)).$$

Proof. The main proof strategy of Theorem 4 is similar to the proof of the fully attribute-hiding security for IPE scheme in [29].

First, we execute a game transformation from the original security game (Game 0) to Game $0'$ which is the same as Game 0 except flip a coin $\tau_{\mathsf{v}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup and game is aborted if $\tau_{\mathsf{v}} \neq s_{\mathsf{v}}$. We define that $\mathcal{A}$ wins with probability $1/2$ when the game is aborted.

Hence the advantage in Game 0′ is a half of that in Game 0 i.e., $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) = 1/2 \cdot \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$ where $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{\mathsf{PAH\text{-}RK}}_{\mathcal{A}}(\lambda)$. Moreover, $\Pr[\mathcal{A} \text{ wins}] = 1/2 \cdot (\Pr[\mathcal{A} \text{ wins}|\tau_{\mathsf{v}} = 0] + \Pr[\mathcal{A} \text{ wins}|\tau_{\mathsf{v}} = 1])$ in Game 0′.

$$\begin{aligned}\mathsf{Adv}^{\mathsf{PAH\text{-}RK}}_{\mathcal{A}}(\lambda) &= \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) = 2 \cdot \mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) \\ &= \Pr[\mathcal{A} \text{ wins}|\tau_{\mathsf{v}} = 0] + \Pr[\mathcal{A} \text{ wins}|\tau_{\mathsf{v}} = 1] - 1 \\ &= (\Pr[\mathcal{A} \text{ wins}|\tau_{\mathsf{v}} = 0] - 1/2) + (\Pr[\mathcal{A} \text{ wins}|\tau_{\mathsf{v}} = 1] - 1/2).\end{aligned}$$

As for the conditional probabilities with $\tau_{\mathsf{v}} = 0$ and $\tau_{\mathsf{v}} = 1$, i.e., $\Pr[\mathcal{A}\text{wins}|\tau_{\mathsf{v}} = 0]$ and $\Pr[\mathcal{A}\text{wins}|\tau_{\mathsf{v}} = 1]$, Lemmas 35 and 39 hold. Therefore, $\mathsf{Adv}^{\mathsf{PAH\text{-}RK}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}2}}(\lambda)$. This completes the proof of Theorem 4. □

Corollary 1-3. *The proposed IP-PRE scheme is predicate- and attribute- hiding for re-encryption key against chosen plaintext attacks under the DLIN assumption provided the underlying IPE scheme is given by the OT12 IPE scheme.*

Proof of Theorem 4 (PAH-RK) in the Case $\tau_{\mathsf{v}} = 0$

Lemma 35. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encryption keys against chosen plaintext attack in the case $\tau_{\mathsf{v}} = 0$ under attribute-hiding security of an underlying IPE scheme.*

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

$$\Pr[\mathcal{A} \text{ wins}|\tau_{\mathsf{v}} = 0] - 1/2 \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}2}}(\lambda).$$

Proof Outline of Lemma 35. The challenge re-encryption key is $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \widehat{\mathbb{D}}^*_1, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}}, \mathsf{prect}_{\vec{x}'^{(b)}})$. In the case $\tau_{\mathsf{v}} = 0$, the adversary does not issues decryption key query on $\vec{v}'$ such that $\vec{v}' \cdot \vec{x}'^{(0)} = 1$ or $\vec{v}' \cdot \vec{x}'^{(1)} = 1$. So, a matrix W_1 which is the plaintext of $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}}$ and $\vec{x}'^{(b)}$ which is an attribute of $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}}$ and $\mathsf{prect}_{\vec{x}'^{(b)}}$ are hidden from the adversary by using the payload and attribute-hiding property of the underlying IPE scheme. So, the basis vectors $(\boldsymbol{d}^*_0, \ldots, \boldsymbol{d}^*_n)$ are unknown to the adversary. Therefore, the predicate $\vec{v}^{(b)}$ is hidden to the adversary. In the case $\tau_{\mathsf{v}} = 0$, we employ Game 0′ through Game 2. In Game 1, $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}} := \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}^{(b)}, W_1)$ and $\mathsf{prect}_{\vec{x}'^{(b)}} := \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}^{(b)})$ are changed to $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}} := \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{r}, R)$ and $\mathsf{prect}_{\vec{x}'^{(b)}} := \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{r}')$, respectively, where $\vec{r}, \vec{r}' \xleftarrow{\mathsf{U}} \mathbb{F}^n_q$ and $R \xleftarrow{\mathsf{U}} GL(4n + 4, \mathbb{F}_q)$ by using the payload and attribute-hiding property of the underlying IPE. Next, we show Game 1 can be conceptually changed to Game 2 by using the fact that a part of basis, $(\boldsymbol{d}^*_0, \ldots, \boldsymbol{d}^*_n, \boldsymbol{d}^*_{n+3}, \ldots, \boldsymbol{d}^*_{2n+2})$ are unknown to the adversary.

Proof of Lemma 35. To prove Lemma 35, we consider the following 3 games when $\tau_{\mathsf{v}} = 0$. 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′: We only describe the components which are changed in the other games. Same as a Game 0 expect that flip a coin $\tau_{\mathsf{v}} \xleftarrow{\mathsf{U}} \{0, 1\}$ before setup, and the game is aborted if $\tau_{\mathsf{v}} \neq s_{\mathsf{v}}$. In order to prove Lemma 35, we consider the case with $\tau_{\mathsf{v}} = 0$. The reply to a challenge re-encryption

$\mathsf{rk}_{\vec{v}^{(b)},\vec{x}'^{(b)}}$ for $(\vec{v}^{(0)},\vec{v}^{(1)},\vec{x}'^{(0)},\vec{x}'^{(1)})$ is

$$\boldsymbol{k}^{*\mathsf{rk}} := (\boxed{1,\delta^{\mathsf{rk}}\vec{v}^{(b)}},0^2,0^n,\vec{\eta}^{\mathsf{rk}},0)_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\boxed{0,\delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v}^{(b)}},0^2,0^n,\vec{\eta}^{\mathsf{rk}}_{\mathsf{ran}},0)_{\mathbb{D}_1^*},$$
$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}},\boxed{\vec{x}'^{(b)}},\boxed{W_1}), \quad \mathsf{prect}_{\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}},\boxed{\vec{x}'^{(b)}}),$$

where $b \xleftarrow{\mathsf{U}} \{0,1\}$, $W_1 \xleftarrow{\mathsf{R}} GL(4n+4,\mathbb{F}_q)$ and $\mathbb{D}_1^* := \mathbb{B}^* W_1$.

Game 1: Game 1 is the same as Game 0′ except that $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}}$ and $\mathsf{prect}_{\vec{x}'^{(b)}}$ of the challenge re-encryption key $\mathsf{rk}_{\vec{v}^{(b)},\vec{x}'^{(b)}}$

$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}},\boxed{\vec{r}},\boxed{R}), \quad \mathsf{prect}_{\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}},\boxed{\vec{r}\,'}), \tag{55}$$

where $R \xleftarrow{\mathsf{R}} GL(4n+4,\mathbb{F}_q)$ and $\vec{r},\vec{r}\,' \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$, and all the other variables are generated as in Game 0′.

Game 2: Game 2 is the same as Game 1 except that $\boldsymbol{k}^{*\mathsf{rk}}$ and $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$ of the challenge re-encryption key $\mathsf{rk}_{\vec{v}^{(b)},\vec{x}'^{(b)}}$

$$\boldsymbol{k}^{*\mathsf{rk}} := (\boxed{\vec{u}},0^2,0^{2n},\vec{\eta}^{\mathsf{rk}},0)_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (\boxed{\vec{u}'},0^2,0^{2n},\vec{\eta}^{\mathsf{rk}}_{\mathsf{ran}},0)_{\mathbb{D}_1^*}, \tag{56}$$

where $\vec{u},\vec{u}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n+1}$ and all the other variables are generated as in Game 1.

Let $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda)$,$\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)$, and $\mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda)$ be the advantage of $\mathcal{A}$ in Game 0′, Game 1, and Game 2 when $\tau_{\mathsf{v}} = 0$, respectively. We will show two lemmas (Lemma 36 - Lemma 38) that evaluate the gaps between pairs of neghoboring games. From these lemmas, we obtain $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) \leq |\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| + |\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda)| + \mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda)$. □

Lemma 36. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{1\text{-}1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda)$.*

Proof. In order to prove to Lemma 36, we construct a probabilistic machine $\mathcal{B}_{1\text{-}1}$ and $\mathcal{B}_{1\text{-}2}$ against the fully attribute-hiding using an adversary $\mathcal{A}$ in a security game (Game 0′ or Game 1) as a black box.

First, we consider the intermediate game Game 1′. Game 1′ is the same as Game 0′ except that $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ of the reply to the challenge re-encryption key is of the form in Eq.(55). In order to prove that $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1')}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}1}}(\lambda)$, we construct a probabilistic machine $\mathcal{B}_{1\text{-}1}$ against the fully attribute-hiding using an adversary $\mathcal{A}$ in a security game (Game 0′ or Game 1′) as a black box as follows:

1. $\mathcal{B}_{1\text{-}1}$ is given a public key $\mathsf{pk}^{\mathsf{IPE}}$ of the IPE, from the challenger for the attribute-hiding security of the underlying IPE.
2. $\mathcal{B}_{1\text{-}1}$ plays a role of the challenger in the security game against $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{1\text{-}1}$ generates a public and secret key as follows: $(\mathsf{param}_n, \mathbb{B} = (\boldsymbol{b}_0,\ldots,\boldsymbol{b}_{3n+3}), \mathbb{B}^* = (\boldsymbol{b}^*_0,\ldots,\boldsymbol{b}^*_{4n+3})) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+4)$, $\widehat{\mathbb{B}} := (\boldsymbol{b}_0,\ldots,\boldsymbol{b}_{n+2},\boldsymbol{b}_{3n+3})$, $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_{n+1},\boldsymbol{b}^*_{n+2},\boldsymbol{b}^*_{3n+2},\ldots,\boldsymbol{b}^*_{4n+2})$. Finally, $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with $\mathsf{pk} := (1^\lambda, \mathsf{pk}^{\mathsf{IPE}}, \mathsf{param}_n, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$.
4. When a decryption key query is issued for a vector $\vec{v}$, $\mathcal{B}_{1\text{-}1}$ computes a normal form decryption key $\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}$ using $\mathbb{B}^*$ and ask a key query $\vec{v}$ to the challenger of the underlying IPE, then obtain the decryption key $\mathsf{sk}^{\mathsf{IPE}}_{\vec{v}}$, and provides $\mathcal{A}$ with a decryption key $\mathsf{sk}_{\vec{v}} := (\boldsymbol{k}^*, \boldsymbol{k}^*_{\mathsf{ran}}, \mathsf{sk}^{\mathsf{IPE}}_{\vec{v}})$.

5. When a re-encryption key query is issued for $(\vec{v}, \vec{x}')$, $\mathcal{B}_{1\text{-}1}$ computes a normal form of re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \widehat{\mathbb{D}}^*_1, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{prect}_{\vec{x}'})$. Finally, $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with a re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'}$.
6. When a re-encryption query is issued for $(\vec{v}, \vec{x}', \mathsf{oct}_{\vec{x}} = (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T, \mathsf{verk}, S))$, if $\mathsf{Ver}(\mathsf{verk}, (\boldsymbol{c}, \boldsymbol{c}_{\mathsf{ran}}, c_T), S) \neq 1$, $\mathcal{B}_{1\text{-}1}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{B}_{1\text{-}1}$ computes a normal form of re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'} := (\boldsymbol{k}^{*\mathsf{renc}}, \boldsymbol{c}^{\mathsf{renc}}, c^{\mathsf{renc}}_T, \{\mathsf{ct}^{\mathsf{renc}}_{\iota,\vec{x}'}\}_{\iota=1,2})$. $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with a re-encrypted ciphertext $\mathsf{rct}_{\vec{x}'}$.
7. When the challenge query is issued for $(\vec{v}^{(0)}, \vec{v}^{(1)}, \vec{x}'^{(0)}, \vec{x}'^{(1)})$, $\mathcal{B}_{1\text{-}1}$ chooses $b \xleftarrow{\mathsf{U}} \{0,1\}$, $W_1, R \xleftarrow{\mathsf{U}} GL(4n+4, \mathbb{F}_q)$ and a random vector $\vec{r} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$. $\mathcal{B}_{1\text{-}1}$ submits $(X^{(b)} := W_1, X^{(1-b)} := R, \vec{x}^{(b)} := \vec{x}'^{(b)}, \vec{x}^{(1-b)} := \vec{r})$ to the attribute-hiding challenger and receives $\mathsf{ct}_{\vec{x}^{(\beta)}}$ for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. $\mathcal{B}_{1\text{-}1}$ computes a normal form $\boldsymbol{k}^{*\mathsf{rk}}$, $\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}$, $\widehat{\mathbb{D}}^*_1$ and $\mathsf{prect}_{\vec{x}^{(b)}}$. Finally, $\mathcal{B}_{1\text{-}1}$ provides $\mathcal{A}$ with $\mathsf{rk}_{\vec{v}^{(b)},\vec{x}^{(b)}} := (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \widehat{\mathbb{D}}^*_1, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}^{(b)}} := \mathsf{ct}_{\vec{x}^{(\beta)}}, \mathsf{prect}_{\vec{x}^{(b)}})$.
8. Finally, $\mathcal{A}$ outputs b'. $\mathcal{B}_{1\text{-}1}$ outputs $\beta = b$ if $b = b'$, otherwise, $\mathcal{B}_{1\text{-}1}$ outputs $\beta = 1 - b$.

Since the challenge re-encryption key is of the form $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}^{(\beta)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}'^{(b)}, W_1)$ (resp. of the form $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}^{(\beta)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{r}, R)$ if $\beta = b$ (resp. $\beta = 1-b$), the view of $\mathcal{A}$ given by $\mathcal{B}_{1\text{-}1}$ is distributed as Game 1 (resp. Game $0'$). Then, $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1')}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}1}}(\lambda)$.

Next, in order to prove that $|\mathsf{Adv}^{(1')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda)$, we construct a probabilistic machine $\mathcal{B}_{1\text{-}2}$ against the fully attribute-hiding security using an adversary $\mathcal{A}$ in a security game (Game 1' or Game 1) as a black box. Game 2 is the same as Game 1' except that $\mathsf{prect}_{\vec{x}'}$ of the reply to the challenge re-encryption key $\mathsf{prect}_{\vec{x}'} = \mathsf{Enc}^{\times}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{r})$ where $\vec{r} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$. Hence, this proof is similar to the above proof. So, we have $|\mathsf{Adv}^{(1')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda)$.

By using hybrid argument, we have $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}2}}(\lambda)$. □

Lemma 37. *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda)$.*

Proof. First, we note that since $\mathbb{D}^*_1$ and the public key $\widehat{\mathbb{B}}$ are independent from adversary $\mathcal{A}$ not in possession of a matrix W_1, we only consider vector element over basis $\mathbb{D}^*_1$, now.

We define new dual orthonormal basis $(\mathbb{U}, \mathbb{U}^*)$ of DPVS $\mathbb{V}$ below. First we generate $U \xleftarrow{\mathsf{R}} GL(n+1, \mathbb{F}_q)$, and set $\begin{pmatrix} \boldsymbol{u}^*_0 \\ \vdots \\ \boldsymbol{u}^*_n \end{pmatrix} := U \cdot \begin{pmatrix} \boldsymbol{d}^*_0 \\ \vdots \\ \boldsymbol{d}^*_n \end{pmatrix}$, and $\mathbb{U}^* := (\boldsymbol{u}^*_0, \ldots, \boldsymbol{u}^*_n, \boldsymbol{d}^*_{n+1}, \ldots, \boldsymbol{d}^*_{4n+3})$. Since non-zero vectors $(1, \delta^{\mathsf{rk}}\vec{v}^{(b)})$ and $(0, \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v}^{(b)})$ in $\mathbb{F}_q^{n+1}$ are linearly independent and $U \xleftarrow{\mathsf{U}} GL(n+1, \mathbb{F}_q)$,

$$\begin{aligned}
\boldsymbol{k}^{*\mathsf{rk}} &:= (1, \delta^{\mathsf{rk}}\vec{v}^{(b)}, 0^2, 0^{2n}, \vec{\eta}^{\mathsf{rk}}, 0)_{\mathbb{D}^*_1} = (\vec{u}, 0^2, 0^{2n}, \vec{\eta}^{\mathsf{rk}}, 0)_{\mathbb{U}^*} \\
\boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} &:= (0, \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v}^{(b)}, 0^2, 0^{2n}, \vec{\eta}^{\mathsf{rk}}_{\mathsf{ran}}, 0)_{\mathbb{D}^*_1} = (\vec{u}', 0^2, 0^{2n}, \vec{\eta}^{\mathsf{rk}}_{\mathsf{ran}}, 0)_{\mathbb{U}^*},
\end{aligned}$$

where $\vec{u} := (1, \delta^{\mathsf{rk}}\vec{v}^{(b)}) \cdot U$ and $\vec{u}' := (0, \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v}^{(b)}) \cdot U$ in $\mathbb{F}_q^{n+1}$ are uniformly and independently distributed. Therefore, the view of $\mathcal{A}$ in Game 1 can be conceptually changed to that in Game 2. □

Lemma 38. $\mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda) = 0$.

Proof. The value of b is independent from $\mathcal{A}$'s view in Game 2. Hence, $\mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda) = 0$. □

Proof of Theorem 4 (PAH-RK) in the Case $\tau_{\mathsf{v}} = 1$

Lemma 39. *The proposed IP-PRE scheme is predicate- and attribute-hiding for re-encryption keys against chosen plaintext attack in the case $\tau_{\mathsf{v}} = 1$ under fully-attribute-hiding of the underlying IPE scheme.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_{2\text{-}1}$ 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 $0'$.

$$\Pr[\mathcal{A} \text{ wins} | \tau_{\mathsf{v}} = 1] - 1/2 \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{2\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{2\text{-}2}}(\lambda).$$

Proof Outline of Lemma 39. In the case $\tau_{\mathsf{v}} = 1$, $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}}$ and $\mathsf{prect}_{\vec{x}'^{(b)}}$ are changed to ciphertexts with the opposite attribute $\vec{x}'^{(1-b)}$ by using the *fully* attribute-hiding property of the underlying IPE scheme. Also, the challenge predicates are equal, $\vec{v}^{(0)} = \vec{v}^{(1)}$, by the restriction of the game in this case. Hence, in the final game, a bit b is hidden to the adversary. In the case $\tau_{\mathsf{v}} = 1$, we employ Game $0'$ and Game 1. In Game 1, $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}} := \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}^{(b)}, W_1)$ and $\mathsf{prect}_{\vec{x}'^{(b)}} := \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}^{(b)})$ are changed to $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}} := \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}^{(1-b)}, W_1)$ and $\mathsf{prect}_{\vec{x}'^{(b)}} := \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}^{(1-b)})$, respectively.

Proof of Lemma 39. To prove Lemma 39, we consider the following 2 games when $\tau_{\mathsf{v}} = 1$. 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 a Game 0 expect that flip a coin $\tau_{\mathsf{v}} \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted if $\tau_{\mathsf{v}} \neq s_{\mathsf{v}}$. In order to prove Lemma 39, we consider the case with $\tau_{\mathsf{v}} = 1$. We only describe the components which are changed in the other games. $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}}$ and $\mathsf{prect}_{\vec{x}'^{(b)}}$ of the reply to a challenge re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'^{(b)}}$ for $(\vec{v}, \vec{x}'^{(0)}, \vec{x}'^{(1)})$ where $\vec{v} := \vec{v}^{(0)} = \vec{v}^{(1)}$ are given as,

$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(b)}}, W_1), \quad \mathsf{prect}_{\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(b)}}),$$

where $b \xleftarrow{\mathsf{U}} \{0,1\}, W_1 \xleftarrow{\mathsf{R}} GL(4n+4, \mathbb{F}_q)$.

Game 1: Game 1 is the same as Game $0'$ except that $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}}$ and $\mathsf{prect}_{\vec{x}'^{(b)}}$ of the challenge re-encryption key $\mathsf{rk}_{\vec{v},\vec{x}'^{(b)}}$ are

$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(1-b)}}, W_1), \quad \mathsf{prect}_{\vec{x}'^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}^{\mathsf{x}}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \boxed{\vec{x}'^{(1-b)}}),$$

where $b \xleftarrow{\mathsf{U}} \{0,1\}$ and all the other variables are generated as in Game $0'$.

Let $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda)$ and $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0'$ and Game 1 when $\tau_{\mathsf{v}} = 1$, respectively. We will show Lemma 39 that evaluate the gaps between Game $0'$ and Game 1. From Lemmas 40 and 41, we obtain $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) \leq |\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| + \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) \leq \frac{1}{2}(\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}2}}(\lambda))$. □

Lemma 40. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}1}$ and $\mathcal{B}_{2\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{2\text{-}2}}(\lambda)$.*

Proof. Lemma 40 is proven in similar manner to Lemma 36.

Lemma 41. $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) = -\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda)$.

Proof. The challenge re-encryption key for the opposite bit $1-b$ to the challenge bit b and the others components are normal forms in Game 1. Hence, success probability $\Pr[\mathsf{Succ}^{(1)}_{\mathcal{A}}]$ in Game 1 is $1 - \Pr[\mathsf{Succ}^{(0')}_{\mathcal{A}}]$, where $\mathsf{Succ}^{(0')}_{\mathcal{A}}$ is success probability in Game $0'$. Therefore, we have $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) = -\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda)$. □

D.6 Proof of Theorem 5

Theorem 5 *The proposed IP-PRE scheme is unlinkable.*

Proof. The item 1 of Remark 1 (Section 4.2) shows the *unconditional* unlinkability of re-encryption keys, and, Lemma 42 shows the *computational* unlinkability of re-encrypted ciphertexts. This completes the proof of Theorem 5. □

Lemma 42. *The proposed IP-PRE scheme is (computationally) unlinkable for re-encrypted ciphertexts.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_{1\text{-}1}, \mathcal{E}_{1\text{-}2}$ and $\mathcal{E}_2$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, for the security game defined in Definition 8,

$$\Pr[\mathcal{A} \text{ wins}] - 1/2 \leq \sum_{i=1}^{2} \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}i}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_2}(\lambda) + \epsilon,$$

where $\epsilon := 6/q$

Proof. We show the (computational) unlinkability of re-encrypted ciphertexts. Note that, as shown in item 2 of Remark 1 (Section 4.2), randomness $(\zeta^{\mathsf{renc}}, \omega^{\mathsf{renc}}, \rho^{\mathsf{renc}}, \varphi^{\mathsf{renc}}, W_2)$ used in components $(\boldsymbol{c}^{\mathsf{renc}}, c_T^{\mathsf{renc}})$ in $\mathsf{rct}_{\vec{x}'} (\xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{\vec{v},\vec{x}'}, \mathsf{oct}_{\vec{x}}))$ are uniformly and independently distributed from input $\mathsf{oct}_{\vec{x}}$. From this fact and the (unconditional) unlinkability of re-encryption keys, we need to show that, for any probabilistic poly-time adversary $\mathcal{A}$ in the game, the challenge

$$\left(\ \mathsf{rk}_{\vec{v},\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \vec{x}'), \quad \mathsf{rct}^{(0)}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{\vec{v},\vec{x}'}, \mathsf{oct}_{\vec{x}}) \ \right) \text{ if } b = 0,$$

and

$$\left(\ \mathsf{rk}_{\vec{v},\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \vec{x}'), \quad \mathsf{rct}^{(1)}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}^{(1)}_{\vec{v},\vec{x}'}, \mathsf{oct}_{\vec{x}}) \ \right) \text{ if } b = 1,$$
$$\text{where } \ \mathsf{rk}^{(1)}_{\vec{v},\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \vec{x}')$$

are indistinguishable by $\mathcal{A}$. We define Game 0 as a security game, where a challenger flips a coin $b \xleftarrow{\mathsf{U}} \{0,1\}$, and gives the upper (resp. lower) instance to $\mathcal{A}$ when $b = 0$ (resp. $b = 1$) in the challenge phase, and the rest of the game is the same as in Definition 8. (In particular, any decryption key query $\vec{v}'$ satisfy $R(\vec{v}', \vec{x}') = 0$ for the challenge $\vec{x}'$.) We will show that any probabilistic poly-time $\mathcal{A}$ has no advantage over it. Let components $(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \widehat{\mathbb{D}}^*_1, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'})$ be in $\mathsf{rk}_{\vec{v},\vec{x}'}$ and $(\boldsymbol{k}^{*\mathsf{renc}(b)}, \mathsf{ct}^{\mathsf{renc}(b)}_{1,\vec{x}'})$ in $\mathsf{rct}^{(b)}_{\vec{x}'}$ for $b \in \{0,1\}$. As is mentioned above, we should show that

$$(\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \widehat{\mathbb{D}}^*_1, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}; \boldsymbol{k}^{*\mathsf{renc}(0)}, \mathsf{ct}^{\mathsf{renc}(0)}_{1,\vec{x}'}) \text{ and } (\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}}, \widehat{\mathbb{D}}^*_1, \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}; \boldsymbol{k}^{*\mathsf{renc}(1)}, \mathsf{ct}^{\mathsf{renc}(1)}_{1,\vec{x}'})$$

are indistinguishable by $\mathcal{A}$, in particular. Here, note that $\mathsf{ct}^{\mathsf{renc}(b)}_{1,\vec{x}'}$ are generated by the re-randomization of IPE ciphertexts, then, it is distributed as $\mathsf{ct}^{\mathsf{renc}(b)}_{1,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', W_1^{(b)})$. We will show the security by game changes: We consider the following 4 games. In Game 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0: We only describe the components which are related for the subsequent game changes.

$$\boldsymbol{k}^{*\mathsf{rk}} := (1, \delta^{\mathsf{rk}}\vec{v}, 0^2, 0^{2n}, \vec{\eta}^{\mathsf{rk}}, 0)_{\mathbb{D}_1^*}, \quad \boldsymbol{k}^{*\mathsf{rk}}_{\mathsf{ran}} := (0, \delta^{\mathsf{rk}}_{\mathsf{ran}}\vec{v}, 0^2, 0^{2n}, \vec{\eta}^{\mathsf{rk}}_{\mathsf{ran}}, 0)_{\mathbb{D}_1^*},$$
$$\widehat{\mathbb{D}}_1^* := (\boldsymbol{d}_i^* := \boldsymbol{b}_i^* W_1)_{i=n+1,n+2,3n+3,\ldots,4n+2}, \quad \mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{W_1}),$$
$$\boldsymbol{k}^{*\mathsf{renc}(b)} := \boxed{(\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1,\mathsf{verk}),\ 0^{2n},\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{D}_1^{*(b)}}},$$
$$\mathsf{ct}^{\mathsf{renc}(b)}_{1,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{W_1^{(b)}}),$$

where $b \xleftarrow{\mathsf{U}} \{0,1\},\ W_1 := W_1^{(0)}, W_1^{(1)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{N\times N},\ \mathbb{D}_1^* := \mathbb{D}_1^{*(0)} := \mathbb{B}^* \cdot W_1,\ \mathbb{D}_1^{*(1)} := \mathbb{B}^* \cdot W_1^{(1)}$.

Game 1: Game 1 is the same as Game 0 except that $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}$ and $\mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'}$ of the challenge are

$$\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{R_1}), \quad \mathsf{ct}^{\mathsf{renc}(b)}_{1,\vec{x}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{IPE}}(\mathsf{pk}^{\mathsf{IPE}}, \vec{x}', \boxed{R_2}),$$

where $R_1, R_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{N\times N}$ and all the other variables are generated as in Game 0.

Game 2: Game 2 is the same as Game 1 except that $\boldsymbol{k}^{*\mathsf{renc}(b)}$ of the challenge is

$$\boldsymbol{k}^{*\mathsf{renc}(b)} := (\ 1,\ \delta^{\mathsf{renc}}\vec{v},\ \sigma(-1,\mathsf{verk}),\ \boxed{\vec{r}^{\mathsf{renc}}},\ \vec{\eta}^{\ \mathsf{renc}},\ 0)_{\mathbb{D}_1^{*(b)}},$$

where $\vec{r}^{\mathsf{renc}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n}$.

Game 3: Game 3 is the same as Game 2 except that $\boldsymbol{k}^{*\mathsf{renc}(b)}$ of the challenge is

$$\boldsymbol{k}^{*\mathsf{renc}(b)} \xleftarrow{\mathsf{U}} \mathbb{V},$$

and all the other variables are generated as in Game 2.

Let $\mathsf{Adv}^{(j)}_{\mathcal{A}}(\lambda)$ be the advantage of $\mathcal{A}$ in Game j ($j = 0, \ldots, 3$), respectively. From Lemmas 43–46, we obtain $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) \le \sum_{i=1}^{3} |\mathsf{Adv}^{(i\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(i)}_{\mathcal{A}}(\lambda)| + \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) \le \sum_{i=1}^{2} \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}i}}(\lambda) + \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_2}(\lambda) + 1/q \le \sum_{i=1}^{2} \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{E}_{1\text{-}i}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_2}(\lambda) + 6/q$. □

Lemma 43. *For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{B}_{1\text{-}1}$ and $\mathcal{B}_{1\text{-}2}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \le \sum_{i=1}^{2} \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{B}_{1\text{-}i}}(\lambda)$.*

Proof. Lemma 43 is proven in similar manner to Lemmas 29 and 36.

Lemma 44. *For any adversary $\mathcal{A}$, there exist a probabilistic machine $\mathcal{B}_2$ whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_2}(\lambda)$.*

Proof. Since $\mathsf{ct}^{\mathsf{rk}}_{\vec{x}'}, \mathsf{ct}^{\mathsf{renc}}_{1,\vec{x}'}$ are ciphertexts of random matrices and in Game 1, subbasis $(\boldsymbol{d}_i^{*(b)})_{i=n+3,\ldots,3n+2}$ of $\mathbb{D}^{*(b)}$ are hidden from the adversary's view. Hence, a simulator with a Problem 1 instance can be constructed for Lemma 44 as in Lemma 9. □

Lemma 45. $|\mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)| \le 1/q$.

Proof. A coefficient of $\boldsymbol{k}^{*\mathsf{renc}(b)}$ over a hidden subbasis $(\boldsymbol{d}_i^{*(b)})_{i=n+3,\ldots,3n+2}$ of $\mathbb{D}^{*(b)}$ is given by $\bar{r}^{\mathsf{renc}}$, which is non-zero except for the probability $1/q$. Moreover, coefficients of $\boldsymbol{k}^{*\mathsf{rk}}, \boldsymbol{k}_{\mathsf{ran}}^{*\mathsf{rk}}$ over a hidden subbasis $(\boldsymbol{d}_i^*)_{i=n+3,\ldots,3n+2}$ are 0. Therefore, $\boldsymbol{k}^{*\mathsf{renc}}$ is uniformly distributed in the whole space $\mathbb{V}$ and independent from other variables since the hidden subbasis vectors $(\boldsymbol{d}_i^*)_{i=n+3,\ldots,3n+2}$ are uniformly and independently generated. □

Lemma 46. $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$.

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

E Ciphertext Policy Functional Proxy-Re-Encryption (CP-F-PRE)

We will construct a CP-F-PRE scheme with the access structure given by Okamoto-Takashima [27]. The scheme has the *attribute-hiding* security for a re-encryption key, $\mathsf{rk}_{\Gamma,\mathbb{S}}$, as well as usual payload hiding for original and re-encrypted ciphertexts. In a typical application, Γ indicates attributes of a user who generates $\mathsf{rk}_{\Gamma,\mathbb{S}}$ for a proxy, where hiding attributes Γ is an important requirement for *anonymous re-encryption outsourcing.*

E.1 Span Programs and Non-Monotone Access Structures

Definition 20 (Span Programs [3]). *Let $\{p_1, \ldots, p_n\}$ be a set of variables. A span program over $\mathbb{F}_q$ is a labelled matrix $\hat{M} := (M, \rho)$ where M is a $(\ell \times r)$ matrix over $\mathbb{F}_q$ and ρ is a labelling of the rows of M by literals from $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ (every row is labelled 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 labelled by some p_i such that $\delta_i = 1$ or rows labelled 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 by using the inner-product of attribute vectors, that is employed in the proposed functional encryption schemes.

Definition 21 (Inner-Products of Attribute Vectors and Access Structures). *$\mathcal{U}_t$ $(t = 1, \ldots, d$ and $\mathcal{U}_t \subset \{0,1\}^*)$ is a sub-universe, a set of attributes, each of which is expressed by a pair of sub-universe id and n_t-dimensional vector, i.e., $(t, \vec{v})$, where $t \in \{1, \ldots, d\}$ and $\vec{v} \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$.*

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

Let Γ be a set of attributes, i.e., $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}, 1 \le t \le d\}$, where $1 \le t \le d$ 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 $[\rho(i) = (t, \vec{v}_i)] \wedge [(t, \vec{x}_t) \in \Gamma] \wedge [\vec{v}_i \cdot \vec{x}_t = 0]$ or $[\rho(i) = \neg(t, \vec{v}_i)] \wedge [(t, \vec{x}_t) \in \Gamma] \wedge [\vec{v}_i \cdot \vec{x}_t \neq 0]$. 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 22. *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.*

We define a CP-F-PRE scheme For access structures, Γ and $\mathbb{S}$, given in Definition 21, and its security below. (Definition 23 is just a specialization of Definition 3 with Γ and $\mathbb{S}$.)

Definition 23. *A functional proxy-re-encryption scheme consists of the following seven algorithms.*

Setup**:** *takes as input a security parameter 1^λ and a format $\vec{n} := (d; n_1, \ldots, n_d)$. It outputs public key pk and (master) secret key sk.*

KG**:** *takes as input the public key pk, the (master) secret key sk, and attributes Γ. It outputs a corresponding decryption key sk_Γ.*

Enc**:** *takes as input the public key pk, an access structure $\mathbb{S}$, and a plaintext m in some associated plaintext space. It outputs an original ciphertext $\mathsf{oct}_\mathbb{S}$.*

RKG**:** *takes as input the public key pk, a decryption key sk_Γ, and an access structure $\mathbb{S}'$. It outputs a re-encryption key $\mathsf{rk}_{\Gamma,\mathbb{S}'}$.*

REnc**:** *takes as input the public key pk, a re-encryption key $\mathsf{rk}_{\Gamma,\mathbb{S}'}$, and an original ciphertext $\mathsf{oct}_\mathbb{S}$. It outputs a re-encrypted ciphertext $\mathsf{rct}_{\mathbb{S}'}$.*

$\mathsf{Dec}_{\mathsf{oct}}$**:** *takes as input the public key pk, a decryption key sk_Γ, and an original ciphertext $\mathsf{oct}_\mathbb{S}$. It outputs either a plaintext m or the distinguished symbol $\perp$.*

$\mathsf{Dec}_{\mathsf{rct}}$**:** *takes as input the public key pk, a decryption key $\mathsf{sk}_{\Gamma'}$, and a re-encrypted ciphertext $\mathsf{rct}_{\mathbb{S}'}$. It outputs either a plaintext m or the distinguished symbol $\perp$.*

The correctness for a CP-F-PRE scheme is defined in a similar manner as general F-PRE in Section 3.

Next, we define three security properties of CP-F-PRE.

Definition 24 (Payload-Hiding for Original Ciphertexts). *The model for defining the adaptively payload-hiding security for original ciphertexts of CP-F-PRE under chosen plaintext attack is given by the following game:*

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

Phase 1. *The adversary $\mathcal{A}$ is allowed to adaptively issue a polynomial number of queries as follows.*

Decryption key query. *For a decryption key query Γ, the challenger gives $\mathsf{sk}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$ to $\mathcal{A}$.*

Re-encryption key query. *For a re-encryption key query* $(\Gamma, \mathbb{S}')$*, the challenger computes* $\mathsf{rk}_{\Gamma,\mathbb{S}'} \xleftarrow{R} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathbb{S}')$ *where* $\mathsf{sk}_\Gamma \xleftarrow{R} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$*. It gives* $\mathsf{rk}_{\Gamma,\mathbb{S}'}$ *to* $\mathcal{A}$*.*

Re-encryption query. *For a re-encryption query* $(\Gamma, \mathbb{S}', \mathsf{oct}_\mathbb{S})$*, the challenger computes* $\mathsf{rk}_{\Gamma,\mathbb{S}'} \xleftarrow{R} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathbb{S}')$ *where* $\mathsf{sk}_\Gamma \xleftarrow{R} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$ *and* $\mathsf{rct}_{\mathbb{S}'} \xleftarrow{R} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{\Gamma,\mathbb{S}'}, \mathsf{oct}_\mathbb{S})$*. It gives* $\mathsf{rct}_{\mathbb{S}'}$ *to* $\mathcal{A}$*.*

Challenge. *For a challenge query* $(m^{(0)}, m^{(1)}, \mathbb{S})$ *subjected to the following restrictions:*

- *Any decryption key query* Γ *satisfies* $R(\Gamma, \mathbb{S}) = 0$*, and any re-encryption key query* $(\Gamma, \mathbb{S}')$ *satisfies*
  - $R(\Gamma, \mathbb{S}) = 0$ *or*
  - $R(\Gamma', \mathbb{S}') = 0$ *for any decryption key query* Γ' *(and no restriction on* Γ*)*

The challenger flips a random bit $b \in \{0, 1\}$ *and gives* $\mathsf{oct}_\mathbb{S}^{(b)} \xleftarrow{R} \mathsf{Enc}(\mathsf{pk}, \mathbb{S}, m^{(b)})$ *to* $\mathcal{A}$*.*

Phase 2. *The adversary* $\mathcal{A}$ *may continue to issue decryption key queries, re-encryption key queries and re-encryption queries, subjected to the restriction in challenge phase and the following additional restriction for re-encryption queries.*

Re-encryption query. *For a re-encryption query* $(\Gamma, \mathbb{S}', \mathsf{oct}_\mathbb{S})$*, subject to the following restrictions:*

- $R(\Gamma', \mathbb{S}') = 0$ *for any decryption key query for* Γ' *if* $\mathsf{oct}_\mathbb{S} = \mathsf{oct}_\mathbb{S}^{(b)}$

The challenger computes $\mathsf{rk}_{\Gamma,\mathbb{S}'} \xleftarrow{R} \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma), \mathbb{S}')$ *and* $\mathsf{rct}_{\mathbb{S}'} \xleftarrow{R} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{\Gamma,\mathbb{S}'}, \mathsf{oct}_\mathbb{S})$*. It gives* $\mathsf{rct}_{\mathbb{S}'}$ *to* $\mathcal{A}$*.*

Guess. $\mathcal{A}$ *outputs its guess* $b' \in \{0, 1\}$ *for* b *and wins the game if* $b = b'$*.*

We define the advantage of $\mathcal{A}$ *as* $\mathsf{Adv}_\mathcal{A}^{\mathsf{CPFPRE,PH\text{-}OC}}(\lambda) := \Pr[b = b'] - \frac{1}{2}$*. A CP-F-PRE scheme is payload-hiding for original ciphertexts if all polynomial time adversaries have at most negligible advantage in the above game.*

Definition 25 (Payload-Hiding for Re-Encrypted Ciphertexts). *The model for defining the adaptively payload-hiding security for re-encrypted ciphertexts of CP-F-PRE under chosen plaintext attack is given by the following game:*

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

Phase 1. *The adversary* $\mathcal{A}$ *is allowed to adaptively issue a polynomial number of queries as follows.*

Decryption key query. *For a decryption key query* Γ*, the challenger gives* $\mathsf{sk}_\Gamma \xleftarrow{R} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$ *to* $\mathcal{A}$*.*

Re-encryption key query. *For a re-encryption key query* $(\Gamma, \mathbb{S}')$*, the challenger computes* $\mathsf{rk}_{\Gamma,\mathbb{S}'} \xleftarrow{R} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathbb{S}')$ *where* $\mathsf{sk}_\Gamma \xleftarrow{R} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$*. It gives* $\mathsf{rk}_{\Gamma,\mathbb{S}'}$ *to* $\mathcal{A}$*.*

Re-encryption query. *For a re-encryption query* $(\Gamma, \mathbb{S}', \mathsf{oct}_\mathbb{S})$*, the challenger computes* $\mathsf{rk}_{\Gamma,\mathbb{S}'} \xleftarrow{R} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathbb{S}')$ *where* $\mathsf{sk}_\Gamma \xleftarrow{R} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$ *and* $\mathsf{rct}_{\mathbb{S}'} \xleftarrow{R} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{\Gamma,\mathbb{S}'}, \mathsf{oct}_\mathbb{S})$*. It gives* $\mathsf{rct}_{\mathbb{S}'}$ *to* $\mathcal{A}$*.*

Challenge. *For a challenge query* $(m^{(0)}, m^{(1)}, \mathbb{S}, \Gamma, \mathbb{S}')$ *subjected to the following restrictions:*

- $R(\Gamma', \mathbb{S}') = 0$ *for all the decryption key queries* Γ'*.*

The challenger flips a random bit $b \in \{0, 1\}$ *and gives* $\mathsf{rct}_{\mathbb{S}'} \xleftarrow{R} \mathsf{REnc}(\mathsf{RKG}(\mathsf{pk}, \Gamma, \mathbb{S}'), \mathsf{Enc}(\mathbb{S}, m^{(b)}))$*. Then it gives* $\mathsf{rct}_{\mathbb{S}'}$ *to* $\mathcal{A}$*.*

Phase 2. *The adversary* $\mathcal{A}$ *may continue to issue decryption key queries, re-encryption key queries and re-encryption queries, subjected to the restriction in challenge phase.*

Guess. $\mathcal{A}$ *outputs its guess* $b' \in \{0, 1\}$ *for* b *and wins the game if* $b = b'$*.*

We define the advantage of $\mathcal{A}$ as $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CPFPRE,PH\text{-}RC}}(\lambda) := \Pr[b = b'] - \frac{1}{2}$. *A CP-F-PRE scheme is payload-hiding for re-encrypted ciphertexts if all polynomial time adversaries have at most negligible advantage in the above game.*

Definition 26 (Attribute-Hiding for Re-Encryption Keys). *The model for defining the adaptively attribute-hiding security for re-encryption keys of CP-F-PRE under chosen plaintext attack is given by the following game:*

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

Phase 1. *The adversary $\mathcal{A}$ is allowed to adaptively issue a polynomial number of queries as follows.*

- **Decryption key query.** *For a decryption key query Γ, the challenger gives* $\mathsf{sk}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$ *to $\mathcal{A}$.*
- **Re-encryption key query.** *For a re-encryption key query $(\Gamma, \mathbb{S}')$, the challenger computes* $\mathsf{rk}_{\Gamma,\mathbb{S}'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathbb{S}')$ *where* $\mathsf{sk}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$. *It gives* $\mathsf{rk}_{\Gamma,\mathbb{S}'}$ *to $\mathcal{A}$.*
- **Re-encryption query.** *For a re-encryption query $(\Gamma, \mathbb{S}', \mathsf{oct}_\mathbb{S})$, the challenger computes* $\mathsf{rk}_{\Gamma,\mathbb{S}'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathbb{S}')$ *where* $\mathsf{sk}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma)$ *and* $\mathsf{rct}_{\mathbb{S}'} \xleftarrow{\mathsf{R}} \mathsf{REnc}(\mathsf{pk}, \mathsf{rk}_{\Gamma,\mathbb{S}'}, \mathsf{oct}_\mathbb{S})$. *It gives* $\mathsf{rct}_{\mathbb{S}'}$ *to $\mathcal{A}$.*

Challenge. *For a challenge query $(\Gamma^{(0)}, \Gamma^{(1)}, \mathbb{S}')$, subject to the following restrictions:*

- $R(\Gamma', \mathbb{S}') = 0$ *for all decryption key queries Γ'.*

The challenger flips a random bit $b \xleftarrow{\mathsf{U}} \{0,1\}$ *and computes* $\mathsf{rk}_{\Gamma^{(b)},\mathbb{S}'} \xleftarrow{\mathsf{R}} \mathsf{RKG}(\mathsf{pk}, \mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma^{(b)}), \mathbb{S}')$. *Then it gives* $\mathsf{rk}_{\Gamma^{(b)},\mathbb{S}'}$ *to $\mathcal{A}$.*

Phase 2. *The adversary $\mathcal{A}$ may continue to issue decryption key queries, re-encryption key queries and re-encryption queries, subjected to the restriction in challenge phase.*

Guess. *$\mathcal{A}$ outputs its guess $b' \in \{0,1\}$ for b and wins the game if $b = b'$.*

We define the advantage of $\mathcal{A}$ as $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{CPFPRE,AH\text{-}RK}}(\lambda) := \Pr[b = b'] - \frac{1}{2}$. *A CP-F-PRE scheme is attribute-hiding for re-encryption keys if all polynomial time adversaries have at most negligible advantage in the above game.*

The unlinkability of a CP-F-PRE scheme is defined in a similar manner to that in Definition 8.

E.2 Underlying Ciphertext-Policy Functional Encryption (CP-FE)

We use a payload-hiding CP-FE scheme with message space $\mathbb{F}_q^{N_0 \times N_0} \times \cdots \times \mathbb{F}_q^{N_d \times N_d} \times \mathcal{X}$ as an underlying CP-FE scheme, where $N_0 := 9, \{N_t := 3n_t + 1\}_{t=1,\ldots,d}$ for a format $\vec{n} := (d; n_1, \ldots, n_d)$, and $\mathcal{X}$ is a set of all attributes Γ with security parameter λ.

Definition 27 (Ciphertext-Policy Functional Encryption : CP-FE). *A ciphertext-policy functional encryption scheme consists of four algorithms.*

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

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

Enc *This is a randomized algorithm that takes as input access structure $\mathbb{S} := (M, \rho)$, a message X in a message space $\mathbb{F}_q^{N_0 \times N_0} \times \cdots \times \mathbb{F}_q^{N_d \times N_d} \times \mathcal{X}$, and the public parameters* pk. *It outputs the ciphertext.*

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

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

Definition 28. *The model for defining the adaptively payload-hiding security of CP-FE under chosen plaintext attack is given by the following game:*

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

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

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

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

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

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

We obtain a payload-hiding CP-FE scheme with the above message space based on a payload hiding CP-FE in [27], with a similar encoding of messages as in Definition 15. We call it the OT10 CP-FE.

E.3 Construction

We assume that $x_{t,1} = 1$ for $\vec{x}_t := (x_{t,1}, \ldots, x_{t,n})$ in attributes Γ and $v_{j,n} \neq 0$ for $\vec{v}_j := (v_{j,1}, \ldots, v_{j,n})$ in an access structure $\mathbb{S}$.

Our CP-F-PRE is constructed with using our IP-PRE schemes as a building block. While payload-hiding are obtained as in IP-PRE, to achieve the attribute-hiding security, we add dummy components $(\boldsymbol{k}_t^{*\mathsf{rk}}, \boldsymbol{k}_{t,\mathsf{ran}}^{*\mathsf{rk}})$ for $(t, \cdot) \notin \Gamma$ in re-encryption-key $\mathsf{rk}_{\Gamma,\mathbb{S}}$, where Γ is attributes.

$\mathsf{Setup}(1^\lambda, \vec{n} = (d; n_1, \ldots, n_d)) : (\mathsf{pk}^{\mathsf{CP\text{-}FE}}, \mathsf{sk}^{\mathsf{CP\text{-}FE}}) \xleftarrow{\mathsf{R}} \mathsf{Setup}_{\mathsf{CP\text{-}FE}}(1^\lambda, \vec{n})$

$N_0 := 9, \quad N_t := 3n_t + 1$ for $t = 1, \ldots, d, \quad \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, g_T := e(G, G)^\psi,$

for $t = 0, \ldots, d,$

$\mathsf{param}'_t := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t),$

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

$\mathsf{param}_{\vec{n}} := (\{\mathsf{param}_t\}_{t=0,\ldots,d}, g_T),$

$\boldsymbol{b}_{t.i} := \sum_{j=1}^{N_t} \chi_{t,i,j}\boldsymbol{a}_{t,j}, \mathbb{B}_t := (\boldsymbol{b}_{t.1}, \ldots, \boldsymbol{b}_{t.N_t})$,
$\boldsymbol{b}^*_{t.i} := \sum_{j=1}^{N_t} \vartheta_{t,i,j}\boldsymbol{a}_{t,j}, \mathbb{B}^*_t := (\boldsymbol{b}^*_{t.1}, \ldots, \boldsymbol{b}^*_{t.N_t})$,
$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \ldots, \boldsymbol{b}_{0,4}, \boldsymbol{b}_{0,9})$, $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,N_t})$ for $t = 1, \ldots, d$,
$\widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,2}, \boldsymbol{b}^*_{0,3}, \boldsymbol{b}^*_{0,4}, \boldsymbol{b}^*_{0,7}, \boldsymbol{b}^*_{0,8})$, $\widehat{\mathbb{B}}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,2n_t+1}, \ldots, \boldsymbol{b}^*_{t,3n_t})$ for $t = 1, \ldots, d$,
return $\mathsf{pk} = (1^\lambda, \mathsf{pk}^{\mathsf{CP\text{-}FE}}, \mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t\}_{t=0,\ldots,d})$, $\mathsf{sk} = (\mathsf{sk}^{\mathsf{CP\text{-}FE}}, \boldsymbol{b}^*_{0,1})$.

$\mathsf{KG}(\mathsf{pk}, \mathsf{sk}, \Gamma = (\{(t, \vec{x}_t) | \vec{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}, 1 \le t \le d\})$:
$\mathsf{sk}^{\mathsf{CP\text{-}FE}}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}^{\mathsf{CP\text{-}FE}}(\mathsf{pk}^{\mathsf{CP\text{-}FE}}, \mathsf{sk}^{\mathsf{CP\text{-}FE}}, \Gamma)$, $\quad \delta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, $\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $(t, \vec{x}_t) \in \Gamma$

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

return $\mathsf{sk}_\Gamma := (\Gamma, \mathsf{sk}^{\mathsf{CP\text{-}FE}}_\Gamma, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\vec{x}_t)\in\Gamma})$.

$\mathsf{Enc}(\mathsf{pk}, m, \mathbb{S} = (M, \rho))$: $\quad (\mathsf{sigk}, \mathsf{verk}) \xleftarrow{\mathsf{R}} \mathsf{SigKG}(1^\lambda)$,
$\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_l)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $\pi, \eta_0, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$\boldsymbol{c}_0 := (\ \zeta,\ -s_0,\ \pi(\mathsf{verk}, 1),\ 0^2,\ 0^2,\ \eta_0\ )_{\mathbb{B}_0}$, $\quad c_T := m \cdot g_T^\zeta$,

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

$$\theta_i, \eta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{c}_i := (\ \overbrace{\quad s_i\vec{e}_{t,1} + \theta_i\vec{v}_i,}^{n_t}\ \overbrace{\quad 0^{n_t},}^{n_t}\ \overbrace{\quad 0^{n_t},}^{n_t}\ \overbrace{\quad \eta_i\quad}^{1}\ )_{\mathbb{B}_t},$$

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

$$\eta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{c}_i := (\ \overbrace{\quad s_i\vec{v}_i,}^{n_t}\ \overbrace{\quad 0^{n_t},}^{n_t}\ \overbrace{\quad 0^{n_t},}^{n_t}\ \overbrace{\quad \eta_i\quad}^{1}\ )_{\mathbb{B}_t},$$

$S \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{sigk}, C := (\mathbb{S}, \{\boldsymbol{c}_i\}_{i=0,\ldots,l}, c_T))$,
return $\mathsf{oct}_\mathbb{S} := (\mathbb{S}, \{\boldsymbol{c}_i\}_{i=0,\ldots,l}, c_T, \mathsf{verk}, S)$.

$\mathsf{RKG}\ (\mathsf{pk}, \mathsf{sk}_\Gamma := (\Gamma, \mathsf{sk}^{\mathsf{CP\text{-}FE}}_\Gamma, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\vec{x}_t)\in\Gamma}),\ \mathbb{S}')$:
$\delta', \delta'_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\varphi}', \vec{\varphi}'_{\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, $\vec{\varphi}'_t, \vec{\varphi}'_{t,\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$,
$W_{1,0} \xleftarrow{\mathsf{U}} GL(9, \mathbb{F}_q)$, $\quad W_{1.t} \xleftarrow{\mathsf{U}} GL(3n_t + 1, \mathbb{F}_q)$ for $t = 1, \ldots, d$,
$\widehat{\mathbb{D}}^*_0 := (\boldsymbol{d}^*_{0,i} := \boldsymbol{b}^*_{0,i}W_{1,0})_{i=3,4,7,8}$, $\quad \widehat{\mathbb{D}}^*_t := (\boldsymbol{d}^*_{t,i} := \boldsymbol{b}^*_{0,i}W_{1,t})_{i=2n_t+1,\ldots,3n_t}$ for $t = 1, \ldots, d$,
$\boldsymbol{k}^{*\mathsf{rk}}_0 := (\boldsymbol{k}^*_0 + (\ 0,\ \delta',\ 0^4,\ \vec{\varphi}',\ 0)_{\mathbb{B}^*})W_{1,0}$, $\quad \boldsymbol{k}^{*\mathsf{rk}}_{0,\mathsf{ran}} := (\ 0,\ \delta'_{\mathsf{ran}},\ 0^4,\ \vec{\varphi}'_{\mathsf{ran}},\ 0)_{\mathbb{B}^*}W_{1,0}$,
$\boldsymbol{k}^{*\mathsf{rk}}_t := (\boldsymbol{k}^*_t + (\ \delta'\vec{x}_t,\ 0^{n_t},\ \vec{\varphi}'_t,\ 0)_{\mathbb{B}^*_t})W_{1,t}$, $\quad \boldsymbol{k}^{*\mathsf{rk}}_{t,\mathsf{ran}} := (\ \delta'_{\mathsf{ran}}\vec{x}_t,\ 0^{n_t},\ \vec{\varphi}'_{t,\mathsf{ran}},\ 0)_{\mathbb{B}^*_t}W_{1,t}$ for $(t, \vec{x}_t) \in \Gamma$,
$\boldsymbol{k}^{*\mathsf{rk}}_t,\ \boldsymbol{k}^{*\mathsf{rk}}_{t,\mathsf{ran}} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{d}^*_{t,1}, \ldots, \boldsymbol{d}^*_{t,n_t}, \boldsymbol{d}^*_{t,2n_t+1}, \ldots, \boldsymbol{d}^*_{t,3n_t}\rangle$ for $(t, \cdot) \notin \Gamma$,
$\mathsf{ct}^{\mathsf{rk}}_{\mathbb{S}'} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{CP\text{-}FE}}(\mathsf{pk}^{\mathsf{CP\text{-}FE}}, \mathbb{S}',\ (\{W_{1,t}\}_{t=0,\ldots,d}, \Gamma))$,
return $\mathsf{rk}_{\Gamma,\mathbb{S}'} := (\mathbb{S}', \{\boldsymbol{k}^{*\mathsf{rk}}_t, \boldsymbol{k}^{*\mathsf{rk}}_{t,\mathsf{ran}}, \widehat{\mathbb{D}}^*_t\}_{t=0,\ldots,d}, \mathsf{ct}^{\mathsf{rk}}_{\mathbb{S}'})$.

$\mathsf{REnc}\ (\mathsf{pk}, \mathsf{rk}_{\Gamma,\mathbb{S}'} := (\mathbb{S}', \{\boldsymbol{k}_t^{*\mathsf{rk}}, \boldsymbol{k}_{t,\mathsf{ran}}^{*\mathsf{rk}}, \widehat{\mathbb{D}}_t^*\}_{t=0,\ldots,d}, \mathsf{ct}_{\mathbb{S}'}^{\mathsf{rk}}),\ \mathsf{oct}_{\mathbb{S}} := (C := (\mathbb{S}, \{\boldsymbol{c}_i\}_{i=0,\ldots,l}, c_T), \mathsf{verk}, S)):$
If $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, return $\perp$,
$r, \sigma, \pi', \eta', \zeta' \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\varphi}_0' \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$, $\vec{\varphi}_t' \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $t = 1, \ldots, d$,
$\vec{f}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\vec{s}'^{\mathrm{T}} := (s_1', \ldots, s_l')^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}}$, $s_0' := \vec{1} \cdot \vec{f}'^{\mathrm{T}}$, $W_2 \xleftarrow{\mathsf{R}} GL(9, \mathbb{F}_q)$
$\boldsymbol{k}_0^{*\mathsf{renc}} := \boldsymbol{k}_0^{*\mathsf{rk}} + r\boldsymbol{k}_{0.\mathsf{ran}}^{*\mathsf{rk}} + (\ 0^2,\ \sigma(-1, \mathsf{verk}),\ 0^2,\ \vec{\varphi}_0',\ 0\ )_{\mathbb{D}_0^*}$
$\boldsymbol{k}_t^{*\mathsf{renc}} := \boldsymbol{k}_t^{*\mathsf{rk}} + r\boldsymbol{k}_{t.\mathsf{ran}}^{*\mathsf{rk}} + (\ 0^{2n_t}, \vec{\varphi}_t',\ 0\ )_{\mathbb{D}_t^*}$ for $t = 1, \ldots, d$,

$\boldsymbol{c}_0^{\mathsf{renc}} := (\boldsymbol{c}_0 + (\ \zeta',\ -s_0',\ \pi'(\mathsf{verk}, 1),\ 0^2,\ 0^2,\ \eta')_{\mathbb{B}_0})W_2$,
$\mathsf{ct}_{1,\mathbb{S}'}^{\mathsf{renc}} \xleftarrow{\mathsf{R}} \mathsf{RR}_{\mathsf{CP\text{-}FE}}(\mathsf{pk}^{\mathsf{CP\text{-}FE}}, \mathsf{ct}_{\mathbb{S}'}^{\mathsf{rk}})$, $\mathsf{ct}_{2,\mathbb{S}'}^{\mathsf{renc}} \xleftarrow{\mathsf{R}} \mathsf{Enc}_{\mathsf{CP\text{-}FE}}(\mathsf{pk}^{\mathsf{CP\text{-}FE}}, \mathbb{S}', W_2)$, $c_T^{\mathsf{renc}} := c_T \cdot g_T^{\zeta'}$,
for $i = 1, \ldots, l$,
if $\rho(i) = (t, \vec{v}_i := (v_{i.1}, \ldots, v_{i.n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\})(v_{i,n_t} \neq 0)$, $\theta_i', \eta_i' \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{c}_i^{\mathsf{renc}} := \boldsymbol{c}_i + (\ \overbrace{\quad s_i'\vec{e}_{t.1} + \theta_i'\vec{v}_i,\quad}^{n_t}\ \overbrace{\quad 0^{n_t},\quad}^{n_t}\ \overbrace{\quad 0^{n_t},\quad}^{n_t}\ \overbrace{\quad \eta_i'\quad}^{1}\ )_{\mathbb{B}_t},$$

if $\rho(i) = \neg(t, \vec{v}_i)$, $\eta_i' \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{c}_i^{\mathsf{renc}} := \boldsymbol{c}_i + (\ \overbrace{\quad s_i'\vec{v}_i,\quad}^{n_t}\ \overbrace{\quad 0^{n_t},\quad}^{n_t}\ \overbrace{\quad 0^{n_t},\quad}^{n_t}\ \overbrace{\quad \eta_i'\quad}^{1}\ )_{\mathbb{B}_t},$$

return $\mathsf{rct}_{\mathbb{S}'} := (\mathbb{S}', \mathbb{S}, \{\boldsymbol{k}_t^{*\mathsf{renc}}\}_{t=0,\ldots,d}, \{\boldsymbol{c}_i^{\mathsf{renc}}\}_{i=0,\ldots,\ell}, c_T^{\mathsf{renc}}, \{\mathsf{ct}_{\iota,\mathbb{S}'}^{\mathsf{renc}}\}_{\iota=1,2})$.

$\mathsf{Dec}_{\mathsf{oct}}\ (\mathsf{pk}, \mathsf{sk}_\Gamma = (\Gamma, \mathsf{sk}_\Gamma^{\mathsf{CP\text{-}FE}}, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t)\in\Gamma}),\ \mathsf{oct}_{\mathbb{S}} = (C := (\mathbb{S}, \{\boldsymbol{c}_i\}_{i=0,\ldots,l}, c_T), \mathsf{verk}, S)):$
If $\mathsf{Ver}(\mathsf{verk}, C, S) \neq 1$, return $\perp$,
If $\mathbb{S} = (M, \rho)$ accepts $\Gamma := \{(t, \vec{x}_t)\}$, 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
$I \subseteq \{i \in \{1, .., l\} \mid [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0] \vee [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\}$,

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

return $m' := c_T/K$.

$\mathsf{Dec}_{\mathsf{rct}}\ (\mathsf{pk}, \mathsf{sk}_{\Gamma'} := (\mathsf{sk}_{\Gamma'}^{\mathsf{CP\text{-}FE}}, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t')\in\Gamma'}),$
$\mathsf{rct}_{\mathbb{S}'} := (\mathbb{S}', \mathbb{S}, \{\boldsymbol{k}_t^{*\mathsf{renc}}\}_{t=0,\ldots,d}, \{\boldsymbol{c}_i^{\mathsf{renc}}\}_{i=0,\ldots,\ell}, c_T^{\mathsf{renc}}, \{\mathsf{ct}_{\iota,\mathbb{S}'}^{\mathsf{renc}}\}_{\iota=1,2})):$
$(\{\widetilde{W}_{1,t}\}_{t=0,\ldots,d}, \Gamma) \xleftarrow{\mathsf{R}} \mathsf{Dec}_{\mathsf{CP\text{-}FE}}(\mathsf{pk}^{\mathsf{CP\text{-}FE}}, \mathsf{sk}_{\Gamma'}^{\mathsf{CP\text{-}FE}}, \mathsf{ct}_{1,\mathbb{S}'}^{\mathsf{renc}})$, $\widetilde{W}_2 \xleftarrow{\mathsf{R}} \mathsf{Dec}_{\mathsf{CP\text{-}FE}}(\mathsf{pk}^{\mathsf{CP\text{-}FE}}, \mathsf{sk}_{\Gamma'}^{\mathsf{CP\text{-}FE}}, \mathsf{ct}_{2,\mathbb{S}'}^{\mathsf{renc}})$,
If $\mathbb{S} = (M, \rho)$ accepts $\Gamma := \{(t, \vec{x}_t)\}$, 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
$I \subseteq \{i \in \{1, .., l\} \mid [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0] \vee [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\}$,

$\widetilde{\boldsymbol{k}}_0^* := \boldsymbol{k}_0^{*\mathsf{renc}}\widetilde{W}_{1,0}^{-1}$, $\widetilde{\boldsymbol{k}}_t^* := \boldsymbol{k}_t^{*\mathsf{renc}}\widetilde{W}_{1,t}^{-1}$ for $(t, \vec{x}) \in \Gamma$, $\widetilde{\boldsymbol{c}}_0 := \boldsymbol{c}_0^{\mathsf{renc}}\widetilde{W}_2^{-1}$,

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

return $m' := c_T/\widetilde{K}$,

E.4 Security

Theorem 8. *The proposed CP-F-PRE scheme is payload-hiding for original ciphertexts against chosen plaintext attacks under the DLIN assumption, payload-hiding of underlying CP-FE scheme and strong unforgeability of one-time signature.*

Theorem 9. *The proposed CP-F-PRE scheme is payload-hiding for re-encrypted ciphertexts against chosen plaintext attacks under payload-hiding of underlying CP-FE scheme.*

Theorem 10. *The proposed CP-F-PRE scheme is attribute-hiding for re-encryption key against chosen plaintext attacks under payload-hiding of underlying CP-FE scheme.*

Corollary 3 *The proposed CP-F-PRE scheme is payload-hiding for original ciphertexts against chosen plaintext attacks under the DLIN assumption and strong unforgeability of one-time signature with instantiating underlying CP-FE by the OT10 CP-FE scheme.*

The proposed CP-F-PRE scheme is payload-hiding for re-encrypted ciphertexts against chosen plaintext attacks under the DLIN assumption with instantiating underlying CP-FE by the OT10 CP-FE scheme.

The proposed CP-F-PRE scheme is attribute-hiding for re-encryption keys against chosen attribute attacks under the DLIN assumption with instantiating underlying CP-FE by the OT10 CP-FE scheme.

Theorem 11. *The proposed CP-F-PRE scheme is unlinkable.*

The proofs of Theorems 8–10 (and Corollary 3) and Theorem 11 are given in the full version of this paper. They are given in a similar manner to the security proofs for IP-PRE given in Appendix D.