Compact Bounded-Collusion Identity-based Encryption via Group Testing

Shingo Sato* Junji Shikata*

Abstract

Bounded-collusion identity-based encryption (BC-IBE) is a variant of identity-based encryption, where an adversary obtains user secrete keys corresponding to at most d identities. From results of existing work, it is proven that BC-IBE can be constructed from public key encryption (PKE) with several properties. In particular, we focus on post-quantum PKE schemes submitted to the NIST PQC competition, as the underlying PKE of BC-IBE schemes. This is because post-quantum cryptography is one of active research areas, due to recent advancement of developing quantum computers. Hence, it is reasonable to consider converting such PKE schemes into encryption schemes with additional functionalities. By using existing generic constructions of BC-IBE, those post-quantum PKE schemes are transformed into BC-IBE with non-compact public parameter.

In this paper, we propose generic constructions of BC-IBE whose public parameter-size is more compact, and it is possible to apply many post-quantum PKE schemes secure against chosen plaintext attacks, into our generic constructions. To this end, we construct BC-IBE schemes from a group testing perspective, while existing ones are constructed by employing error-correcting codes or cover-free families. As a result, we can obtain BC-IBE schemes with more compact public parameter, which are constructed from the NIST PQC PKE schemes.

1 Introduction

1.1 Background

Identity-based encryption (IBE) is one of fundamental and important cryptosystems. A trusted key generation center generates a public parameter and a master secret key. Anyone can encrypt a message to any user by using the public parameter and the user's identity. To decrypt a ciphertext, a user must obtain the secrete key for the user's identity from the key generation center. There are many researches related to IBE such as pairing-based IBE (e.g., [3, 2, 23, 24]) and lattice-based IBE (e.g., [12, 4, 1, 25, 26]).

As a variant of IBE, *bounded-collusion IBE* (BC-IBE) has been studied. BC-IBE just ensures security in the (security) model where an adversary obtains secret keys associated with at most d identities. This security model can capture a realistic assumption. Even though BC-IBE is a weak variant of IBE, this cryptography is one of the most important research areas. This is because BC-IBE schemes can be constructed from public key encryption (PKE) schemes with several properties due to the results of [7, 13, 21, 6], while we cannot convert PKE into IBE, in general. Namely, by elaborating a PKE construction, we can obtain the resulting BC-IBE with similar advantages of the underlying PKE. In particular, we focus on transforming post-quantum PKE into BC-IBE. Post-quantum cryptography (PQC) is one of the most important research areas, due to recent

*Yokohama National University, Yokohama, Japan. sato-shingo-zk@ynu.ac.jp, shikata-junji-rb@ynu.ac.jp.

Table 1: Adaptively secure BC-IBE schemes constructed from PKE

Scheme	Requirements for PKE	CT-Size	PP-Size	StdM?
[7]	IND-CPA security	$O(d \log n)\|\mathsf{ct}\|$	$O(d^2 \log n)\|\mathsf{pk}\|$	✓
[13]	IND-CPA security Linear Hash Proof property Key Homomorphism	$\|\mathsf{ct}\|$	$O(d \log n)\|\mathsf{pk}\|$	✓
[21]	IND-CPA security Key Homomorphism Weak Multi-Key Malleability	$\|\mathsf{ct}\|$	$O(d^2 \log n)\|\mathsf{pk}\|$	✓
	IND-CPA security Multi-Key Malleability			
[6]	IND-CPA security Key Homomorphism Weak Multi-Key Malleability Power of Message-and-key	$\|\mathsf{ct}\|$	$O(d)\|\mathsf{pk}\|$	ROM
This work (Sec. 3.1)	IND-CPA security	$O(\log(n/d))\|\mathsf{ct}\|$	$O(d \log(n/d))\|\mathsf{pk}\|$	ROM
This work (Sec. 3.2)	IND-CPA security Key Homomorphism Weak Multi-Key Malleability	$\|\mathsf{ct}\|$		
This work (Sec. 3.3)	IND-CPA security Multi-Key Malleability			

"CT-Size" and "PP-Size" mean ciphertext-size and public parameter-size, respectively. d is the collusion parameter (i.e., the number of queries issued to the key extraction oracle). n is the size of an identity space. $|\mathsf{ct}|$ and $|\mathsf{pk}|$ are the bit-lengths of ciphertexts and public keys of the underlying PKE, respectively. "StdM" means the standard model which is the model without idealized oracles such as random oracles. "ROM" means the random oracle model.

advancement of developing quantum computers. So, many researchers have paid much attention to developing post-quantum cryptosystems such as PKE and key encapsulation mechanisms (KEMs). In fact, there are many research on PKE/KEM constructions submitted to the NIST (National Institute of Standards and Technology) PQC standardization process.

Related Work. There are the following existing BC-IBE schemes constructed from PKE with several properties: Dodis et al. proposed the first BC-IBE scheme constructed from any PKE scheme with *indistinguishability against chosen plaintext attacks* (denoted by IND-CPA security) [7]. Goldwasser, Lewko, and Wilson presented a generic construction starting from PKE with linear hash proof property and key homomorphism [13]. Tessaro and Wilson provided an adaptively secure BC-IBE scheme constructed from a PKE scheme with key homomorphism and weak multi-key malleability, and a scheme constructed from key multi-key malleability [21]. Choi et al. proposed a BC-IBE scheme constructed from a PKE scheme with key homomorphism, weak multi-key malleability, and power of message-and-key [6].

1.2 Contribution

Our goal is to convert many post-quantum PKE into adaptively secure BC-IBE with compact public parameter. Table 1 shows generic constructions of adaptively secure BC-IBE. From this table, we can see that there is no existing BC-IBE scheme with compact public parameter, which is

constructed from a PKE scheme submitted to the NIST PQC competition. Although the BC-IBE scheme of [7] can be constructed from any IND-CPA secure PKE (with $|\mathsf{pk}|$-size public key and $|\mathsf{ct}|$-size ciphertext), its public parameter-size and ciphertext-size are $O(d^2 \log n)|\mathsf{pk}|$ and $O(d \log n)|\mathsf{ct}|$, respectively, where d is the collusion parameter, and n is the size of the identity space. Although the public parameter-size of the scheme of [13] is $O(d \log n)$, there is no post-quantum PKE scheme which can be applied to this generic construction, because the linear hash proof property introduced in [13] is required for the underlying PKE. Regarding the generic constructions of [21], only the GPV cryptosystem [12] and a variant of NTRU [20] can be applied to these constructions, and the public parameter-size of the resulting BC-IBE schemes grows with $O(d^2 \log n)$. Although the public parameter-size of the construction of [6] is $O(d)|\mathsf{pk}|$, only the GPV cryptosystem can be applied to this BC-IBE construction. From these results, when a BC-IBE scheme is constructed from a NIST PQC PKE scheme, its public parameter-size is $O(d^2 \log n)|\mathsf{pk}|$ and is not compact. Hence, we aim at converting such post-quantum PKE schemes into BC-IBE schemes with more compact public parameter.

In order to achieve our goal, we utilize list disjunct matrices used in group testing methodology [9, 10], while existing schemes employ error-correcting codes or cover-free families. Then, we can construct BC-IBE schemes with $O(d \log (n/d))|\mathsf{pk}|$-size public parameter, by using properties of a list-disjunct matrix and a random oracle. Details on our contribution are as follows:

- First, we propose a generic construction (in Section 3.1) starting from any IND-CPA secure PKE. Namely, it is possible to apply any post-quantum PKE schemes to this construction. This scheme is similar to the BC-IBE scheme of [7]. However, we utilize a particular construction of a (d, d)-list-disjunct matrix in order to construct a BC-IBE with more compact public parameter and ciphertext, while the existing one employs d-disjunct matrices (see Definition 12) whose notion is identical to those of error-correcting codes and cover-free families. Concretely, the public parameter-size and ciphertext-size of ours are $O(d \log (n/d))|\mathsf{pk}|$ and $O(\log (n/d))|\mathsf{ct}|$, respectively. On the other hand, the public parameter-size and ciphertext-size of the scheme of [7] are $O(d^2 \log n)|\mathsf{pk}|$ and $O(d \log (n))|\mathsf{ct}|$, respectively. Notice that the security of our scheme is ensured in the random oracle model, while the [7] scheme is secure in the standard model.

- Second, we present two generic constructions (in Sections 3.2 and 3.3) starting from IND-CPA secure PKE with several properties. One requires the underlying PKE to satisfy *key homomorphism* and *weak multi-key malleability*. The other requires the PKE to satisfy *multi-key malleability*. These properties were introduced in [21]. The ciphertext-size of these BC-IBE schemes is better than that of our first scheme, because this size is the same as that of the underlying PKE, due to the required properties. In addition, the public parameter-size of these schemes also grows with $O(d \log (n/d))$ due to (d, ℓ)-list-disjunct matrices.

In addition, if the underlying PKE satisfies *disjoint simulatability* instead of IND-CPA security, it is possible to convert such PKE into the objective BC-IBE scheme (see Appendix A). Namely, it is possible to apply deterministic post-quantum PKE schemes into BC-IBE with compact public parameter. We should notice that the size of the identity space in our schemes all is exponential in a security parameter, so that we can give security proofs for these schemes. However, we do not have to store a list-disjunct matrix whose size is exponential, by using an explicit construction of a list-disjunct matrix (e.g., [16, 5]).

From the results above, it is possible to apply any IND-CPA secure post-quantum PKE to the first generic construction in Section 3.1, and thus we can convert post-quantum PKE into BC-IBE with public parameter whose size is $O(d \log n)|\mathsf{pk}|$.

2 Preliminaries

In this paper, we use the following notation: For a positive integer n, let $[n] := \{1, \ldots, n\}$. For values $x_1, \ldots, x_n$ and a subset $S \subseteq [n]$, let $\{x_i\}_{i \in S}$ (resp. $(x_i)_{i \in S}$) be the set (resp. sequence) of values whose indexes are in S. For a positive integer n, let 0^n be the n-bit zero-string. For a function $f : \mathbb{N} \to \mathbb{R}$, f is negligible in λ (denoted by $f(\lambda) \leq \mathsf{negl}(\lambda)$) if $f(\lambda) = o(\lambda^{-c})$ for any constant $c > 0$ and sufficiently large $\lambda \in \mathbb{N}$. A probability is an overwhelming probability if it is $1 - \mathsf{negl}(\lambda)$. "Probabilistic polynomial time" is abbreviated as PPT. For a positive integer λ, let $\mathsf{poly}(\lambda)$ be a universal polynomial of λ.

Matrices and vectors. For consistency, we use capital bold letters for matrices, non-capital letters for scalars, and bold letters for (column) vectors. For a (binary) matrix $\boldsymbol{M} \in \{0,1\}^{u \times n}$, we use the standard notation $\boldsymbol{M} = (m_{i,j})$. For a n-dimensional vector $\boldsymbol{v}$, v_i is the i-th entry, namely $\boldsymbol{v} = (v_1, \ldots, v_n)^\top$. For a binary matrix $\boldsymbol{x} \in \{0,1\}^n$, let $\mathrm{supp}(\boldsymbol{x}) := \{i \in [n] \mid x_i = 1\}$. For a binary matrix $\boldsymbol{M} = (m_{i,j}) \in \{0,1\}^{u \times n}$ and a binary vector $\boldsymbol{x} \in \{0,1\}^n$, the binary vector $\boldsymbol{y} = \boldsymbol{M} \odot \boldsymbol{x} \in \{0,1\}^u$ is defined as

$$\forall i \in [u], y_i = \bigvee_{j \in [n] \text{ s.t. } m_{i,j}=1} x_j,$$

where $\bigvee$ is the bitwise-OR. For a binary matrix $\boldsymbol{M} = (m_{i,j}) \in \{0,1\}^{u \times n}$ and $c \in [n]$, let $\phi_{\boldsymbol{M}}(c) := \{i \in [u] \mid m_{i,c} = 1\}$.

Furthermore, we describe definitions of several (cryptographic) primitives, in the sections below.

2.1 Public Key Encryption (PKE)

Regarding PKE, we describe its syntax and security definitions required for constructing our BC-IBE schemes.

Definition 1 (PKE)**.** *A PKE scheme consists of three polynomial-time algorithms* $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$*: For a security parameter* λ*, let* $\mathcal{M} = \mathcal{M}(\lambda)$ *be the message space.*

Key Generation. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$*: The randomized algorithm* KGen *takes as input a security parameter* 1^λ *and outputs a public key* pk *and a secret key* sk*.*

Encryption. $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m})$*: The randomized or deterministic algorithm* Enc *takes as input a public key* pk *and a message* m*, and it outputs a ciphertext* ct*.*

Decryption. $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$*: The deterministic algorithm* Dec *takes as input a secret key* sk *and a ciphertext* ct*, and it outputs a message* $\mathsf{m} \in \mathcal{M}$*.*

We require a PKE scheme to be *correct*, as follows:

Definition 2 (Correctness)**.** *A PKE scheme* $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *is* $\mathsf{correct}$ *if for every* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$ *and every* $\mathsf{m} \in \mathcal{M}$*, it holds that* $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \mathsf{m}$ *with overwhelming probability, where* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m})$*.*

Security of PKE. As security notions of PKE, we describe the definitions of *indistinguishability against chosen plaintext attacks* (denoted by $\mathsf{IND\text{-}CPA}$ security) and *disjoint simulatability*.

Definition 3 ($\mathsf{IND\text{-}CPA}$ security)**.** *A PKE scheme* $\mathsf{PKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *is* $\mathsf{IND\text{-}CPA}$ *secure, if for any PPT adversary* $\mathcal{A}$ *against* PKE*, its advantage* $\mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A} \text{ wins}] - 1/2|$ *is negligible in* λ*, where* $[\mathcal{A} \text{ wins}]$ *is the event that* $\mathcal{A}$ *wins in the following game:*

Setup. *The challenger generates* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$ *and gives* pk *to the adversary* $\mathcal{A}$.

Challenge. *When* $\mathcal{A}$ *submits* $(\mathsf{m}_0^*, \mathsf{m}_1^*) \in \mathcal{M}^2$ *such that* $|\mathsf{m}_0^*| = |\mathsf{m}_1^*|$, *the challenger chooses* $b \xleftarrow{\$} \{0,1\}$ *and returns* $\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}_b^*)$.

Output. $\mathcal{A}$ *outputs the guessing bit* $b' \in \{0,1\}$. $\mathcal{A}$ *wins if* $b = b'$.

Following [19, 14], we describe this definition, as follows:

Definition 4 (Disjoint Simulatability)**.** *A PKE scheme* $\mathsf{PKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *is* ϵ_{ds}-disjoint simulatable*, if there exists a PPT algorithm* $\overline{\mathsf{Enc}}$ *satisfying the following:*

- *For any PPT adversary* $\mathcal{A}$ *against* PKE*, its advantage* $\mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE},\mathcal{A}}(\lambda)$ *is negligible in* λ*, where* $\mathsf{Adv}^{\text{ds}}_{\mathsf{PKE},\mathcal{A}}(\lambda)$ *is defined as*

$$\mathsf{Adv}^{\text{ds}}_{\mathsf{PKE},\mathcal{A}}(\lambda) := \left| \Pr\left[1 \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{ct}) \;\middle|\; \begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda); \\ \mathsf{m} \xleftarrow{\$} \mathcal{M}; \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \end{array} \right] \right. \\ \left. - \Pr[1 \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{ct}) \mid (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda); \mathsf{ct} \leftarrow \overline{\mathsf{Enc}}(\mathsf{pk})] \right|.$$

- *For every* $\mathsf{pk} \in \mathsf{supp}(\mathsf{KGen})$, $\Pr[\mathsf{ct} \in \mathsf{Enc}(\mathsf{pk}, \mathcal{M}; \mathcal{R}) \mid \mathsf{ct} \leftarrow \overline{\mathsf{Enc}}(\mathsf{pk})] \leq \epsilon_{ds}$*, where* $\mathsf{supp}(\mathsf{KGen}) = \{\mathsf{pk} \mid (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)\}$*, and* $\mathcal{R}$ *is the randomness space of* Enc.

Special Properties of PKE. We describe the definitions of several properties required for constructing our BC-IBE schemes: *key-homomorphism* and *(weak) multi-key malleability.*

Definition 5 (Secret to Public Key Homomorphism [21])**.** *Let* $\mathsf{PKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a PKE scheme with the secret key space* $\mathcal{K}_{\mathsf{sk}} = \mathcal{K}_{\mathsf{sk}}(\lambda)$ *and the public key space* $\mathcal{K}_{\mathsf{pk}} = \mathcal{K}_{\mathsf{pk}}(\lambda)$ *for a security parameter* λ. *The PKE scheme* PKE *satisfies* key-homomorphism *if there exists a map* $\mu : \mathcal{K}_{sk} \to \mathcal{K}_{pk}$ *such that*

- μ *is a homomorphism (i.e., for all* $\mathsf{sk}, \mathsf{sk}' \in \mathcal{K}_{sk}$, $\mu(\mathsf{sk} + \mathsf{sk}') = \mu(\mathsf{sk}) \cdot \mu(\mathsf{sk}')$*);*
- *Every* $(\mathsf{pk}, \mathsf{sk})$ *generated by* KGen *satisfies* $\mathsf{pk} = \mu(\mathsf{sk})$.

Definition 6 (Weak Multi-Key Malleability [21])**.** *A PKE scheme* $\mathsf{PKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *is* weakly u-key malleable *if there exists a polynomial-time algorithm* $\mathsf{Simulate}$ *such that for every* $\mathsf{m} \in \mathcal{M}$*, every* $I \subseteq [u]$*, and every* $i^* \in I$*, the probability distributions* D_0 *and* D_1 *are computationally indistinguishable, where for* $\{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KGen}(1^\lambda)\}_{i \in [u]}$, D_b *consists of* $((\mathsf{pk}_i)_{i \in [u]}, (\mathsf{sk}_i)_{i \in I \setminus \{i^*\}}, \mathsf{ct}_b)$ *such that*

- $\mathsf{ct}_0 \leftarrow \mathsf{Enc}(\prod_{i \in I} \mathsf{pk}_i, \mathsf{m})$*;*
- $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}_{i^*}, \mathsf{m})$, $\mathsf{ct}_1 \leftarrow \mathsf{Simulate}(i^*, I, \mathsf{ct}, (\mathsf{pk}_i)_{i \in [u]}, (\mathsf{sk}_i)_{i \in I \setminus \{i^*\}})$.

Definition 7 (Multi-Key Malleability [21])**.** *A PKE scheme* $\mathsf{PKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *is* u-key malleable*, if there exists the two polynomial-time algorithms* Modify *and* $\mathsf{Combine}$ *such that the following conditions hold:*

1. *For every* $\mathsf{m} \in \mathcal{M}$*, every* $I \subseteq [u]$ *and every* $i^* \in I$*, the probability*

$$\Pr\left[\mathsf{Dec}(\mathsf{Combine}(I, (\mathsf{sk}_i)_{i \in [u]}), \mathsf{ct}^*) \neq \mathsf{m} \;\middle|\; \begin{array}{l} \forall i \in [u], (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KGen}(1^\lambda); \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}_{i^*}, \mathsf{m}); \\ \mathsf{ct}^* \leftarrow \mathsf{Modify}(i^*, I, (\mathsf{pk}_i)_{i \in [u]}, \mathsf{ct}) \end{array} \right]$$

is negligible in λ[1].

2. *For every* $I \subseteq [u]$, $\mathsf{Combine}(I, (\mathsf{sk}_i)_{i\in[u]})$ *does not depend on* sk_i *for* $i \notin I$.

3. *For every* $I \subseteq [u]$ *and every* $(\mathsf{pk}_i, \mathsf{sk}_i)_{i\in[u]}$, *for all* $i^*, j^* \in I$ *such that* $i^* \neq j^*$, *the values* $\mathsf{Modify}(i^*, I, (\mathsf{pk}_i)_{i\in[u]}, \mathsf{ct})$ *and* $\mathsf{Modify}(j^*, I, (\mathsf{pk}_i)_{i\in[u]}, \mathsf{ct})$ *are identically distributed.*

2.2 Bounded-Collusion Identity-based Encryption (BC-IBE)

Following [21], we describe the syntax and a security definition of BC-IBE.

Definition 8 (BC-IBE)**.** *A BC-IBE scheme consists of four polynomial-time algorithms* (Setup, Extract, Enc, Dec)*: For a security parameter* λ, *let* $\mathcal{ID} = \mathcal{ID}(\lambda)$ *be the identity space and let* $\mathcal{M} = \mathcal{M}(\lambda)$ *be the message space.*

Setup. $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$*: The randomized algorithm* Setup *takes as input a security parameter* 1^λ *and outputs a public parameter* pp *and a master secret key* msk.

Key Extraction. $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{msk}, \mathsf{id})$*: The randomized or deterministic algorithm* Extract *takes as input a master secret key* msk *and an identity* $\mathsf{id} \in \mathcal{ID}$, *and it outputs a secret key* $\mathsf{sk}_{\mathsf{id}}$.

Encryption. $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{id}, \mathsf{m})$*: The randomized or deterministic algorithm* Enc *takes as input a public parameter* pp, *an identity* $\mathsf{id} \in \mathcal{ID}$, *and a message* $\mathsf{m} \in \mathcal{M}$, *and it outputs a ciphertext* ct.

Decryption. $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$*: The deterministic algorithm* Dec *takes as input a secret key* $\mathsf{sk}_{\mathsf{id}}$ *and a ciphertext* ct, *and it outputs a message* m.

A BC-IBE scheme is required to be *correct*, as follows:

Definition 9 (Correctness)**.** *A BC-IBE scheme* (Setup, Extract, Enc, Dec) *is* correct *if for every* $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$, *every* $\mathsf{id} \in \mathcal{ID}$, *every* $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{msk}, \mathsf{id})$, *and every* $\mathsf{m} \in \mathcal{M}$, *it holds that* $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) = \mathsf{m}$ *with overwhelming probability, where* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{id}, \mathsf{m})$.

As a security notion of BC-IBE, we describe the definition of *adaptive security against chosen plaintext attacks* (denoted by d-adaptive CPA security), as follows:

Definition 10 (d-adaptive CPA security)**.** *A BC-IBE scheme* BC-IBE = (Setup, Extract, Enc, Dec) *is* d-adaptive CPA *secure, if for any PPT adversary* $\mathcal{A}$ *against* BC-IBE, *its advantage* $\mathsf{Adv}^{\mathrm{adaptive}}_{\mathsf{BC\text{-}IBE},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}\ \textit{wins}] - 1/2|$ *is negligible in* λ, *where* $[\mathcal{A}\ \textit{wins}]$ *is the event that* $\mathcal{A}$ *wins in the following security game:*

Setup. *The challenger generates* $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ *and gives* pp *to* $\mathcal{A}$.

Phase 1. $\mathcal{A}$ *is allowed to issue the key extraction oracle* $\mathsf{O}_{\mathsf{EXT}}$ *which, on input a key extraction query* $\mathsf{id} \in \mathcal{ID}$, *returns* $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KGen}(\mathsf{msk}, \mathsf{id})$.

Challenge. $\mathcal{A}$ *submits* $(\mathsf{id}^*, \mathsf{m}_0^*, \mathsf{m}_1^*) \in \mathcal{ID} \times \mathcal{M}^2$ *such that* id^* *has never been issued to* $\mathsf{O}_{\mathsf{EXT}}$ *and* $|\mathsf{m}_0^*| = |\mathsf{m}_1^*|$. *The challenger chooses* $b \xleftarrow{\$} \{0,1\}$ *and returns* $\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{id}^*, \mathsf{m}_b^*)$.

[1]The chosen ciphertext ct can be regarded as a ciphertext generated by Enc or $\overline{\mathsf{Enc}}$, since ct is a valid ciphertext drawn from $\mathcal{C}$.

Phase 2. $\mathcal{A}$ *can issue queries to* $\mathsf{O}_{\mathsf{EXT}}$. *Notice that* $\mathcal{A}$ *is forbidden to issue* id^* *to this oracle.*

Output. $\mathcal{A}$ *outputs* $b' \in \{0,1\}$. $\mathcal{A}$ *wins if* $b = b'$.

Here, $\mathcal{A}$ *is allowed to issue at most* d *queries to the* $\mathsf{O}_{\mathsf{EXT}}$ *oracle.*

2.3 All-or-Nothing Transform (AONT)

We describe the definition of AONTs because our BC-IBE scheme uses this cryptographic primitive. An AONT splits a message X into v secret shares $x_1, \ldots, x_v$ and a public share z, and can recover X from the shares $(x_1, \ldots, x_v, z)$.

Following [7], we describe the definition of AONTs, as follows:

Definition 11 (AONT)**.** *An efficient randomized transformation* Trans *is* $(\mu, \bar{\mu}, v)$-AONT *if all the following conditions hold:*

1. *Given* $X \in \{0,1\}^{\mu}$, Trans *outputs* $v+1$ *blocks* $(x_1, \ldots, x_v, z)$, *where for* $i \in [v]$, $x_i \in \{0,1\}^{\bar{\mu}}$ *is a secret share, and* $z \in \mathcal{Z}$ *is a public share.*

2. *There exists an efficient inverse function* $\mathsf{Inverse}$ *which, on input* $(x_1, \ldots, x_v, z) \in (\{0,1\}^{\bar{\mu}})^v \times \mathcal{Z}$, *outputs* $X \in \{0,1\}^{\mu}$.

3. *For any PPT algorithm* $\mathcal{A}$ *against* Trans, *its advantage*

$$\mathsf{Adv}^{\mathrm{ind}}_{\mathsf{Trans},\mathcal{A}}(\lambda) := \left| \Pr[b = b' \mid b \xleftarrow{\$} \{0,1\}; b' \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{LR}}}(1^{\lambda})] - \frac{1}{2} \right|$$

is negligible in λ, *where* O_{LR} *is the* $\mathsf{left\text{-}or\text{-}right}$ *oracle which, on input* $(j, X_0, X_1) \in [v] \times (\{0,1\}^{\mu})^2$, *returns* $(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_v, z)$.

2.4 Group Testing

Dorfman introduced the notion of group testing [9] in order to efficiently detect blood samples contaminated by syphilis during the World War II. Group testing (e.g., [10]) is a method to detect positive items called *defectives* among many whole items with a small number of tests than individually testing each item in the trivial way.

The group testing techniques are classified into two types: non-adaptive setting (e.g., [22, 18, 11]) and adaptive setting (e.g., [9, 17, 15]). Suppose that there are totally n items of which there are (at most) d defectives. In non-adaptive group testing, we need to know d beforehand and to select all the subsets of n items to be tested without knowing the results of other tests. On the other hand, in adaptive group testing, we do tests several times such that we can select a subset of items to be tested after observing the result of the previous test. In this paper, we focus on non-adaptive group testing. This is because non-adaptive group testing can run all tests simultaneously, and all test-designs are determined in advance. On the other hand, adaptive group testing cannot execute all tests at the same time, since each test-design depends on the result of the previous test. To sum up, non-adaptive group testing is much better than adaptive one, in terms of time-complexity.

Non-adaptive group testing is typically designed by using a d-disjunct matrix, a cover-free family, or an error-correcting code (e.g., see [10]). And, a non-adaptive group testing protocol with u tests for n items is represented by a $u \times n$ binary matrix, and the (i,j)-th element of the matrix is equal to 1 if and only if the i-th test is executed to the j-th item. Among such matrices for representing non-adaptive group testing, a disjunct matrix (or cover-free family) is well studied in combinatorics and bioinformatics, and it is defined as follows:

Definition 12 (Disjunct Matrices). *A binary matrix* $\boldsymbol{M} = (m_{i,j}) \in \{0,1\}^{u \times n}$ *is* d*-disjunct if for every distinct* $s_1, \ldots, s_d \in [n]$ *and every* $j \in [n] \backslash \{s_1, \ldots, s_d\}$*, there exists a row* $q \in [u]$ *such that* $m_{q,j} = 1$ *and* $\forall j' \in \{s_1, \ldots, s_d\}$, $m_{q,j'} = 0$.

Furthermore, the notion of list-disjunct matrices was introduced in [16]. This matrix is often used for designing a two-stage adaptive group testing protocol.

Definition 13 (List-disjunct Matrices). *A binary matrix* $\boldsymbol{M} = (m_{i,j}) \in \{0,1\}^{u \times n}$ *is* (d, ℓ)*-list-disjunct if for every two disjoint sets* $S, T \subseteq [n]$ *with* $|S| = d$ *and* $|T| = \ell + 1$*, there exists an element* $j \in T$ *and a row* $q \in [u]$ *such that* $m_{q,j} = 1 \wedge \forall j' \in S, m_{q,j'} = 0$.

Note that the notion of $(d, 0)$-list-disjunct matrices corresponds to that of d-disjunct matrices. In addition, the following definition is also considered for list-disjunct matrices:

Definition 14 (Associated List for List-disjunct Matrices [5]). *Assume that* $\boldsymbol{M} \in \{0,1\}^{u \times n}$ *is a* (d, ℓ)*-disjunct matrix and* $\boldsymbol{x} \in \{0,1\}^n$ *is a binary vector such that* $|\mathsf{supp}(\boldsymbol{x})| \leq k$*. Then, for* $\boldsymbol{y} = \boldsymbol{M} \odot \boldsymbol{x}$*,* $L(\boldsymbol{y})$ *is defined as the list of elements* $i \in [n]$ *(called the associated list of* $\boldsymbol{x}$*) satisfying* $m_{q,i} = 1$ *for every* $q \in [u]$ *such that* $y_q = 1$.

Note that for $\boldsymbol{y} = \boldsymbol{M} \odot \boldsymbol{x}$, the associated list $L(\boldsymbol{y})$ corresponds to the indexes $i \in [n]$ which appear to be defective, and $|L(\boldsymbol{y})| \leq d + \ell$.

The following proposition was proved as one of the results of [5]:

Proposition 1 ([5]). *There exists a Monte-Carlo construction of a* (d, d)*-list-disjunct matrix* $\boldsymbol{M} \in \{0,1\}^{u \times n}$ *with* $u = O(d \log(n/d))$ *and* $|\phi_{\boldsymbol{M}}(j)| = \log(n/d)$ *for all* $j \in [n]$.

3 Our Proposed BC-IBE

3.1 The Basic BC-IBE from IND-CPA secure PKE

We propose a BC-IBE scheme with $O(d \log(n/d))|\mathsf{pk}|$-size public parameter from any IND-CPA secure PKE with $|\mathsf{pk}|$-size public key. Although this one is similar to the scheme of [7], we employ a (d, ℓ)-list-disjunct matrix $\boldsymbol{M} \in \{0,1\}^{u \times n}$ with $|\phi_{\boldsymbol{M}}(j)| = \log(n/d)$ for all $j \in [n]$. There exists a concrete construction of such list-disjunct matrices, from results of [16, 5]. Due to the property of $|\phi_{\boldsymbol{M}}(j)| = \log(n/d)$, the ciphertext-size of this BC-IBE scheme is $O(\log(n/d))|\mathsf{ct}|$, where $|\mathsf{ct}|$ is the ciphertext-size of the underlying PKE. In addition, by requiring the underlying PKE to satisfy additional properties, it is possible to construct BC-IBE schemes with $|\mathsf{ct}|$-size ciphertext (see Sections 3.2 and 3.3). That is, these schemes are based on the BC-IBE in this section, and we present this basic BC-IBE scheme.

The base BC-IBE scheme $\mathsf{BC\text{-}IBE}_{\mathsf{basic}} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ is constructed as follows: For a security parameter λ, let $n = n(\lambda)$, $u = u(\lambda)$, $\mu = \mu(\lambda)$, $\bar{\mu} = \bar{\mu}(\lambda)$, $v = v(\lambda)$ be positive integers. Let $\mathcal{ID} = \mathcal{ID}(\lambda)$ be the identity space such that $|\mathcal{ID}| = n$ and $\mathcal{M} = \{0,1\}^{\mu}$ be the message space.

As system parameters of $\mathsf{BC\text{-}IBE}_{\mathsf{basic}}$, let d be the collusion parameter of d-adaptive CPA security, and let $H : \mathcal{ID} \to [n]$ be a random oracle. We employ a PKE scheme $\mathsf{PKE} = (\mathsf{PKE.KGen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ with the message space $\mathcal{M}_{\mathsf{PKE}} = \{0,1\}^{\bar{\mu}}$ and a $(\mu, \bar{\mu}, v)$-AONT Trans with an efficient inverse function Inverse. Let $\boldsymbol{M} \in \{0,1\}^{u \times n}$ be a (d, ℓ)-list-disjunct matrix constructed in Proposition 1. Notice that we can set $\ell = d$ and $v = \log(n/d)$ in order to construct BC-IBE with $O(d \log(n/d))|\mathsf{pk}|$-size public parameter and $O(\log(n/d))|\mathsf{ct}|$-size ciphertext, due to Proposition 1.

- $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^{\lambda})$:

1. Generate $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KGen}(1^\lambda)$ for $i \in [u]$.
2. Output $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u)$ and $\mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_u)$.

- $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{msk}, \mathsf{id})$:
  1. Parse $\mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_u)$.
  2. Output $\mathsf{sk}_{\mathsf{id}} = (\mathsf{sk}_i)_{i \in \phi_{\boldsymbol{M}}(H(\mathsf{id}))}$.
- $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{id}, \mathsf{m})$:
  1. Parse $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u)$.
  2. Compute $(x_1, \ldots, x_v, z) \leftarrow \mathsf{Trans}(\mathsf{m})$.
  3. Compute $c_i \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\sigma_i}, x_i)$ for $i \in [v]$, where $\phi_{\boldsymbol{M}}(H(\mathsf{id})) = \{\sigma_1, \ldots, \sigma_v\}$, and $\sigma_1, \ldots, \sigma_v \in [u]$ are all distinct.
  4. Output $\mathsf{ct} = (c_1, \ldots, c_v, z)$.
- $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$:
  1. Parse $\mathsf{sk}_{\mathsf{id}} = (\mathsf{sk}_i)_{i \in \phi_{\boldsymbol{M}}(H(\mathsf{id}))}$ and $\mathsf{ct} = (c_1, \ldots, c_v, z)$.
  2. Compute $x_i \leftarrow \mathsf{PKE.Dec}(\mathsf{sk}_{\sigma_i}, c_i)$ for every $i \in [v]$, where $\phi_{\boldsymbol{M}}(H(\mathsf{id})) = \{\sigma_1, \ldots, \sigma_v\}$ for all distinct $\sigma_1, \ldots, \sigma_v$.
  3. Output $\mathsf{m}' \leftarrow \mathsf{Inverse}(x_1, \ldots, x_v, z)$.

It is clear that the BC-IBE scheme $\mathsf{BC\text{-}IBE}_{\mathsf{basic}}$ is correct if the underlying PKE and AONT Trans are correct. The following theorem shows the security of $\mathsf{BC\text{-}IBE}_{\mathsf{basic}}$:

Theorem 1. *If a PKE scheme* PKE *is* IND-CPA *secure, an efficient randomized transformation* Trans *with an inverse function* Inverse *is a* $(\mu, \bar{\mu}, v)$-AONT*, and a binary matrix* $\boldsymbol{M}$ *is* (d, ℓ)*-list-disjunct, then the resulting BC-IBE scheme* $\mathsf{BC\text{-}IBE}_{\mathsf{basic}}$ *is* d-adaptive CPA *secure in the random oracle model.*

Proof. Let $\mathcal{A}$ be a PPT adversary against the d-adaptive CPA security of $\mathsf{BC\text{-}IBE}_{\mathsf{basic}}$, q_H be the maximum number of queries issued to the random oracle H, and T_H be the table of query-response pairs to the H oracle. We define $\mathsf{ct}^* = (c_1^*, \ldots, c_v^*, \hat{c}^*, z^*)$ as the challenge ciphertext.

In order to prove Theorem 1, we consider the security games $\mathsf{Game}_0, \mathsf{Game}_1$. For $i \in \{0, 1\}$, W_i is defined as the event that $\mathcal{A}$ outputs $b' \in \{0, 1\}$ such that $b = b'$ in Game_i.

$\underline{\mathsf{Game}_0}$. This is the ordinary d-adaptive CPA security game. Then, we have $\mathsf{Adv}^{\mathrm{adaptive}}_{\mathsf{BC\text{-}IBE}_{\mathsf{basic}}, \mathcal{A}}(\lambda) = |\Pr[W_0] - 1/2|$.

$\underline{\mathsf{Game}_1}$. This game is the same as Game_0 except that the procedure of the H oracle is modified as follows: We assume that at the beginning of the security game, an index $h_{\mathsf{id}^*} \in [n]$ is chosen uniformly at random. Given a query $\mathsf{id} \in \mathcal{ID}$, the H oracle checks whether $\mathsf{T}_H[\mathsf{id}] = \emptyset$. If $\mathsf{T}_H[\mathsf{id}] = h_{\mathsf{id}} \in [n]$, it returns h_{id}. Otherwise, it chooses $h_{\mathsf{id}} \xleftarrow{\$} [n]$. Then the challenger aborts if $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$. If $h_{\mathsf{id}} \notin L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$, H returns h_{id} and sets $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$. Here, let Abort be the event that $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$ holds when choosing $h_{\mathsf{id}} \xleftarrow{\$} [n]$.

We estimate the upper bound of the probability that Abort occurs, because Game_0 and Game_1 are identical unless this event occurs. Due to the (d, ℓ)-list-disjunct property of $\boldsymbol{M}$, $\ell + 1$ is the maximum number of $|L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))|$. The probability that for the i-th query id to H, $h_{\mathsf{id}} \xleftarrow{\$} [n]$ is

included in the associated list $L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$ is at most $(\ell+1)/(n-(i-1))$. In addition, the total number of queries to H is at most q_H+d, since $\mathsf{O}_{\mathsf{EXT}}$ calls H at most d times. Hence, we have

$$\Pr[\mathsf{Abort}] \leq \sum_{i\in[q_H+d]} \frac{\ell+1}{n-(i-1)} \leq \sum_{i\in[q_H+d]} \frac{\ell+1}{n-(q_H+d)} \leq \frac{(q_H+d)(\ell+1)}{n-(q_H+d)}.$$

Hence, we have $|\Pr[W_0]-\Pr[W_1]| \leq (q_H+d)(\ell+1)/(n-(q_H+d))$.

Furthermore, in order to show that the winning probability in Game_1 is negligible, we assume that some random index $i^* \in \phi_{\boldsymbol{M}}(H(\mathsf{id}^*))$ is fixed, and the challenger computes $(x_1^*,\ldots,x_v^*,z^*) \leftarrow \mathsf{Trans}(\mathsf{m}_b^*)$, $c_{j^*}^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{i^*}, 0^{|\mathsf{m}_0^*|})$, and $c_i^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\sigma_i^*}, x_i^*)$ for $i \in [u]\backslash\{j^*\}$ (where $j^* \in [v]$ is the index such that $i^* = \sigma_{j^*}^*$ and $\phi_{\boldsymbol{M}}(H(\mathsf{id}^*)) = \{\sigma_1^*,\ldots,\sigma_v^*\}$), when generating the challenge ciphertext $\mathsf{ct}^* = (c_1^*,\ldots,c_v^*,z^*)$. We define $\widehat{\mathsf{Game}_1}$ as Game_1 under this assumption, and let $\widehat{W_1}$ be the event that $\mathcal{A}$ outputs b' such that $b=b'$ in $\widehat{\mathsf{Game}_1}$.

We show the indistinguishability between Game_1 and $\widehat{\mathsf{Game}_1}$ follows the $\mathsf{IND\text{-}CPA}$ security of PKE. By using $\mathcal{A}$, we construct a PPT algorithm $\mathcal{D}_1$ against the $\mathsf{IND\text{-}CPA}$ security of PKE, as follows: $\mathcal{D}_1$ is given a public key pk^* of PKE. At the beginning of the security game, $\mathcal{D}_1$ chooses $h_{\mathsf{id}^*} \xleftarrow{\$} [n]$, $i^* \xleftarrow{\$} \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*})$, and sets $\mathsf{pk}_{i^*} = \mathsf{pk}^*$. Then it generates $(\mathsf{pk}_i,\mathsf{sk}_i) \leftarrow \mathsf{PKE.KGen}(1^\lambda)$ for $i \in [u]\backslash\{i^*\}$, initializes the table $\mathsf{T}_H \leftarrow \emptyset$, and gives $\mathsf{pp} = (\mathsf{pk}_1,\ldots,\mathsf{pk}_u)$ to $\mathcal{A}$. The H and $\mathsf{O}_{\mathsf{EXT}}$ oracles are simulated in the following way:

- H: Given $\mathsf{id} \in \mathcal{ID}$, return h_{id} if $\mathsf{T}_H(\mathsf{id}) = h_{\mathsf{id}} \in [n]$. If $\mathsf{T}_H[\mathsf{id}] = \emptyset$, do the following:
  1. Choose $h_{\mathsf{id}} \xleftarrow{\$} [n]$.
  2. If $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$, abort and output a random bit.
  3. If $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})$, abort and output a random bit.
  4. Return h_{id} and set $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$.
- $\mathsf{O}_{\mathsf{EXT}}$: Given an extraction query $\mathsf{id} \in \mathcal{ID}$, obtain $h_{\mathsf{id}} \in [n]$ by calling the H oracle and return $\mathsf{sk}_{\mathsf{id}} = (\mathsf{sk}_i)_{i\in\phi_{\boldsymbol{M}}(h_{\mathsf{id}})}$.

When $\mathcal{A}$ submits $(\mathsf{id}^*,\mathsf{m}_0^*,\mathsf{m}_1^*)$, $\mathcal{D}_1$ does the following:

1. Choose $b \xleftarrow{\$} \{0,1\}$.
2. Let $\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}) = \{\sigma_1^*,\ldots,\sigma_v^*\}$ for all distinct $\sigma_1^*,\ldots,\sigma_v^* \in [u]$.
3. Compute $(x_1^*,\ldots,x_v^*,z^*) \leftarrow \mathsf{Trans}(\mathsf{m}_b^*)$.
4. Compute $c_i^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\sigma_i^*}, x_i^*)$ for $i \in [v]\backslash\{j^*\}$, where $\sigma_{j^*}^* = i^*$.
5. For $i \in [v]$ such that $\sigma_i^* = i^*$, obtain the challenge ciphertext ct_i^* by submitting $(\mathsf{m}_b^*, 0^{|\mathsf{m}_0^*|})$ to the $\mathsf{IND\text{-}CPA}$ security game.
6. Return $\mathsf{ct}^* = (c_1^*,\ldots,c_v^*,z^*)$ and set $\mathsf{T}_H[\mathsf{id}^*] \leftarrow h_{\mathsf{id}^*}$.

Finally, when $\mathcal{A}$ outputs the guessing bit $b' \in \{0,1\}$, $\mathcal{D}_1$ outputs 1 if $b=b'$, and otherwise 0.

The H and $\mathsf{O}_{\mathsf{EXT}}$ oracles are simulated correctly. Regarding the challenge ciphertext ct^*, Game_1 is simulated if $c_i^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{i^*}, \mathsf{m}_b^*)$, and $\widehat{\mathsf{Game}_1}$ is simulated otherwise. Furthermore, the simulation of the environment of $\mathcal{A}$ succeeds unless the H oracle chooses a random hash value

$h_{\mathsf{id}} \in [n]$ such that $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})$. This event occurs with at least probability $1/u$. Hence, we have $\left|\Pr[W_1] - \Pr[\widehat{W_1}]\right| \leq u \cdot \mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{D}_1}(\lambda)$.

Finally, we show that the winning probability in $\widehat{\mathsf{Game}_1}$ follows the security of $(\mu, \bar{\mu}, v)$-AONT. By using $\mathcal{A}$, we construct a PPT algorithm $\mathcal{D}_2$ breaking the security of $(\mu, \bar{\mu}, v)$-AONT, as follows: $\mathcal{D}_2$ chooses $h_{\mathsf{id}^*} \xleftarrow{\$} [n]$, $i^* \xleftarrow{\$} \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*})$. At the beginning of the security game, $\mathcal{D}_2$ generates $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KGen}(1^\lambda)$ for $i \in [u]$, sets $\mathsf{T}_H \leftarrow \emptyset$, and gives $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u)$ to $\mathcal{A}$. The H and $\mathsf{O}_{\mathsf{EXT}}$ oracles are simulated in the same way as $\mathcal{D}_1$. When $\mathcal{A}$ submits $(\mathsf{id}^*, \mathsf{m}_0^*, \mathsf{m}_1^*)$, $\mathcal{D}_2$ does the following:

1. Let $\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}) = \{\sigma_1^*, \ldots, \sigma_v^*\}$ for all distinct $\sigma_1^*, \ldots, \sigma_v^* \in [u]$, and let $j^* \in [v]$ be an index such that $i^* = \sigma_{j^*}^*$.
2. Obtain $(x_1^*, \ldots, x_{j^*-1}, x_{j^*+1}, \ldots, x_v^*, z^*)$ by issuing $(j^*, \mathsf{m}_0^*, \mathsf{m}_1^*)$ to the given O_{LR} oracle.
3. Compute $c_{j^*} \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{i^*}, 0^{|\mathsf{m}_0^*|})$, and for $i \in [v] \backslash \{j^*\}$, compute $c_i^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\sigma_i^*}, x_i^*)$.
4. Return $\mathsf{ct}^* = (c_1^*, \ldots, c_v^*, z^*)$ and set $\mathsf{T}_H[\mathsf{id}^*] \leftarrow h_{\mathsf{id}^*}$.

Finally, when $\mathcal{A}$ outputs $b' \in \{0, 1\}$, $\mathcal{D}_2$ also outputs b'.

The simulation of the $\mathsf{O}_{\mathsf{EXT}}$ and H oracles are simulated correctly, in the same way as $\mathcal{D}_1$. The challenge ciphertext is correctly generated in $\widehat{\mathsf{Game}_1}$, since the j^*-th ciphertext is an encryption of $0^{|\mathsf{m}_0^*|}$, instead of $c_{j^*}^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{i^*}, x_{j^*})$. Furthermore, $\mathcal{D}_2$ succeeds in simulating the view of $\mathcal{A}$ unless the H oracle chooses h_{id} such that $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})$. Hence, we have $\left|\Pr[\widehat{W_1}] - 1/2\right| \leq u \cdot \mathsf{Adv}^{\text{ind}}_{\mathsf{AONT},\mathcal{D}_2}(\lambda)$.

From the above discussion, we obtain

$$\mathsf{Adv}^{\text{adaptive}}_{\mathsf{BC\text{-}IBE}_{\mathsf{basic}},\mathcal{A}}(\lambda) \leq u \cdot \mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{D}_1}(\lambda) + u \cdot \mathsf{Adv}^{\text{ind}}_{\mathsf{AONT},\mathcal{D}_2}(\lambda) + \frac{(q_H + d)(\ell + 1)}{n - (q_H + d)},$$

and thus the objective inequality holds. □

3.2 BC-IBE from Weak Multi-Key Malleable PKE with Key Homomorphism

In this section, we present a generic construction of BC-IBE whose ciphertext-size is the same as that of the underlying PKE. As described beforehand, this scheme is based on the $\mathsf{BC\text{-}IBE}_{\mathsf{basic}}$ scheme presented in Section 3.1. However, unlike this scheme, the underlying ($\mathsf{IND\text{-}CPA}$ secure) PKE is required to satisfy (secret to public) key homomorphism and weak multi-key malleability. Concretely, key homomorphism is necessary to generate a single PKE ciphertext rather than multiple ciphertexts, and weak multi-key malleability is required to achieve d-adaptive CPA security.

The proposed BC-IBE scheme $\mathsf{BC\text{-}IBE}_{\mathsf{kh}} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ is constructed as follows: For a security parameter λ, let $n = n(\lambda)$, $u = u(\lambda)$ be positive integers. Let $\mathcal{ID} = \mathcal{ID}(\lambda)$ be the identity space such that $|\mathcal{ID}| = n$, and let $\mathcal{M}_{\mathsf{BC\text{-}IBE}} = \mathcal{M}_{\mathsf{BC\text{-}IBE}}(\lambda)$ be the message space. Let $\mathsf{PKE} = (\mathsf{PKE.KGen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ be a PKE scheme with the same message space as $\mathcal{M}_{\mathsf{BC\text{-}IBE}}$. Let $H : \mathcal{ID} \to [n]$ be a random oracle and $\boldsymbol{M} \in \{0, 1\}^{u \times n}$ be a (d, ℓ)-list-disjunct matrix.

- $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$:
  1. Generate $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KGen}(1^\lambda)$ for $i \in [u]$.
  2. Output $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u)$ and $\mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_u)$.

- $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{msk}, \mathsf{id})$:
  1. Parse $\mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_u)$
  2. Output $\mathsf{sk}_{\mathsf{id}} \leftarrow \sum_{k \in \phi_{\boldsymbol{M}}(H(\mathsf{id}))} \mathsf{sk}_k$.
- $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{id}, \mathsf{m})$:
  1. Parse $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u)$.
  2. Compute $\mathsf{pk}_{\mathsf{id}} \leftarrow \prod_{k \in \phi_{\boldsymbol{M}}(H(\mathsf{id}))} \mathsf{pk}_k$.
  3. Output $\mathsf{ct} \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\mathsf{id}}, \mathsf{m})$.
- $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$: Output $\mathsf{m}' \leftarrow \mathsf{PKE.Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$.

It is clear that $\mathsf{BC\text{-}IBE}_{\mathsf{kh}}$ is correct if PKE is correct and satisfies key homomorphism. The following theorem shows the security of this BC-IBE scheme:

Theorem 2. *If a PKE scheme* PKE *is* IND-CPA *secure and* weakly u-key malleable*, and a binary matrix* $\boldsymbol{M}$ *is* (d, ℓ)*-list-disjunct, then the resulting BC-IBE scheme* $\mathsf{BC\text{-}IBE}_{\mathsf{kh}}$ *is* d-adaptive CPA *secure in the random oracle model.*

Proof. Let $\mathcal{A}$ be a PPT adversary breaking the d-adaptive CPA security of $\mathsf{BC\text{-}IBE}_{\mathsf{kh}}$. We define q_H as the maximum number of queries issued to the random oracle H, and T_H as the table of query-response pairs to H.

We define $\widehat{\mathsf{Game}}$ as the security game which is the same as the ordinary d-adaptive CPA security game except that the procedure of the H oracle is modified as follows: We assume that, at the beginning of the security game, an index $h_{\mathsf{id}^*} \in [n]$ is chosen uniformly at random. Given a query $\mathsf{id} \in \mathcal{ID}$, the H oracle checks whether $\mathsf{T}_H[\mathsf{id}] = \emptyset$. If $\mathsf{T}_H[\mathsf{id}] = h_{\mathsf{id}} \in [n]$, it returns h_{id}. Otherwise, it chooses $h_{\mathsf{id}} \xleftarrow{\$} [n]$. Then the challenger aborts if $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$. If $h_{\mathsf{id}} \notin L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$, H returns h_{id} and sets $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$.

In addition, W and $\widehat{W}$ are defined as the events that $\mathcal{A}$ outputs $b' \in \{0, 1\}$ such that $b = b'$ in the d-adaptive CPA game and $\widehat{\mathsf{Game}}$, respectively. Let Abort be the event that $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$ holds in $\widehat{\mathsf{Game}}$ when H chooses $h_{\mathsf{id}} \xleftarrow{\$} [n]$.

We estimate the upper bound of the aborting probability, because $\widehat{\mathsf{Game}}$ is identical to the d-adaptive CPA security game unless Abort occurs. In the same way as the proof of Theorem 1, this bound is obtained as follows:

$$\Pr[\mathsf{Abort}] \leq \sum_{i \in [q_H + d]} \frac{\ell + 1}{n - (i - 1)} \leq \sum_{i \in [q_H + d]} \frac{\ell + 1}{n - (q_H + d)} \leq \frac{(q_H + d)(\ell + 1)}{n - (q_H + d)}.$$

Hence, we have $\left|\Pr[W] - \Pr[\widehat{W}]\right| \leq (q_H + d)(\ell + 1)/(n - (q_H + d))$.

We show that the indistinguishability in $\widehat{\mathsf{Game}}$ follows the IND-CPA security of PKE. In order to do this, by using $\mathcal{A}$, we construct a PPT algorithm $\mathcal{D}$ against PKE, as follows: On input the public key pk^* of PKE, $\mathcal{D}$ chooses two indexes $h_{\mathsf{id}^*} \xleftarrow{\$} [n]$, $i^* \xleftarrow{\$} \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*})$, and sets $\mathsf{pk}_{i^*} \leftarrow \mathsf{pk}^*$. At the beginning of the security game of BC-IBE, $\mathcal{D}$ generates $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KGen}(1^\lambda)$ for $i \in [u] \backslash \{i^*\}$, sets the table $\mathsf{T}_H \leftarrow \emptyset$, and gives $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u)$ to $\mathcal{A}$. The $\mathsf{O}_{\mathsf{EXT}}$ and H oracles are simulated as follows:

- H: Given $\mathsf{id} \in \mathcal{ID}$, return h_{id} if $\mathsf{T}_H(\mathsf{id}) = h_{\mathsf{id}} \in [n]$. If $\mathsf{T}_H[\mathsf{id}] = \emptyset$, do the following:

1. Choose $h_{\mathsf{id}} \xleftarrow{\$} [n]$.
2. If $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$, abort and output a random bit.
3. If $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})$, abort and output a random bit.
4. Return h_{id} and set $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$.

- $\mathsf{O}_{\mathsf{EXT}}$: Given an extraction query $\mathsf{id} \in \mathcal{ID}$, obtain $h_{\mathsf{id}} \in [n]$ by accessing H, and return $\mathsf{sk}_{\mathsf{id}} \leftarrow \sum_{k \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})} \mathsf{sk}_k$.

When $\mathcal{A}$ submits $(\mathsf{id}^*, \mathsf{m}_0^*, \mathsf{m}_1^*)$, $\mathcal{D}$ obtains c_{i^*} by issuing $(\mathsf{m}_0^*, \mathsf{m}_1^*)$ to the IND-CPA security game, and returns $\mathsf{ct}^* \leftarrow \mathsf{Simulate}(i^*, \phi_{\boldsymbol{M}}(H(\mathsf{id})), c_{i^*}, \mathsf{pp}, (\mathsf{sk}_i)_{i \in [u] \setminus \{i^*\}})$. Finally, when $\mathcal{A}$ outputs $b' \in \{0,1\}$, $\mathcal{D}$ also outputs b'.

The two oracles H and $\mathsf{O}_{\mathsf{EXT}}$ are correctly simulated in $\widehat{\mathsf{Game}}$. Furthermore, the challenge ciphertext is also simulated because $\mathsf{ct}^* \leftarrow \mathsf{Simulate}(i^*, \phi_{\boldsymbol{M}}(H(\mathsf{id})), c_{i^*}, \mathsf{pp}, (\mathsf{sk}_i)_{i \in [u] \setminus \{i^*\}})$ is indistinguishable from the real challenge ciphertext, due to the weak multi-key malleability of PKE. Hence, $\mathcal{D}$ correctly simulates the environment of $\mathcal{A}$ in $\widehat{\mathsf{Game}}$. It is shown that $\mathcal{D}$ breaks the IND-CPA security unless $h_{\mathsf{id}} \in [n]$ such that $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})$ is chosen by the H oracle. Therefore, we have $\left|\Pr[\widehat{W}] - 1/2\right| \leq u \cdot \mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{D}}(\lambda)$.

From the discussion above, we obtain

$$\mathsf{Adv}^{\text{adaptive}}_{\mathsf{BC\text{-}IBE_{kh}},\mathcal{A}}(\lambda) \leq u \cdot \mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{D}}(\lambda) + \frac{(q_H + d)(\ell + 1)}{n - (q_H + d)},$$

and the proof is completed. □

3.3 BC-IBE from Multi-Key Malleable PKE

We describe a generic construction from PKE with multi-key malleability (Definition 7). Although the public parameter-size and ciphertext-size of this scheme are the same as those of the BC-IBE scheme $\mathsf{BC\text{-}IBE_{kh}}$ in Section 3.2, the classes of the underlying PKE are different. Thus, it is meaningful to present this scheme. Notice that multi-key malleability is necessary to reduce the ciphertext-size and satisfy d-adaptive CPA security.

The proposed BC-IBE scheme $\mathsf{BC\text{-}IBE_{mkm}} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ is constructed as follows: For a security parameter λ, let $n = n(\lambda)$, $u = u(\lambda)$ be positive integers, let $\mathcal{ID} = \mathcal{ID}(\lambda)$ be the identity space such that $|\mathcal{ID}| = n$, and let $\mathcal{M}_{\mathsf{BC\text{-}IBE}} = \mathcal{M}_{\mathsf{BC\text{-}IBE}}(\lambda)$ be the message space. We use a PKE scheme $\mathsf{PKE} = (\mathsf{PKE.KGen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$. Let $H : \mathcal{ID} \to [n]$ be a random oracle and $\boldsymbol{M} \in \{0,1\}^{u \times n}$ be a (d, ℓ)-list-disjunct matrix.

- $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$:
  1. Generate $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KGen}(1^\lambda)$ for $i \in [u]$.
  2. Output $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u)$ and $\mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_u)$.
- $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{msk}, \mathsf{id})$:
  1. Parse $\mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_u)$.
  2. Output $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Combine}(\phi_{\boldsymbol{M}}(H(\mathsf{id})), (\mathsf{sk}_i)_{i \in [u]})$.
- $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{id}, \mathsf{m})$:
  1. Compute $i \leftarrow \min(\phi_{\boldsymbol{M}}(H(\mathsf{id})))$.

2. Compute $c' \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_i, \mathsf{m})$.
3. Output $\mathsf{ct} \leftarrow \mathsf{Modify}(i, \phi_{\boldsymbol{M}}(H(\mathsf{id})), \mathsf{pp}, c')$.

- $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$: Output $\mathsf{m}' \leftarrow \mathsf{PKE.Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$.

It is clear that the $\mathsf{BC\text{-}IBE}_{\mathsf{mkm}}$ is correct if PKE is correct and u-key malleable. The following theorem shows the security of this BC-IBE scheme:

Theorem 3. *If a PKE scheme* PKE *is* IND-CPA *secure and* u-key malleable*, and a binary matrix* $\boldsymbol{M}$ *is* (d, ℓ)*-list-disjunct, then the resulting BC-IBE scheme* $\mathsf{BC\text{-}IBE}_{\mathsf{mkm}}$ *is* d-adaptive CPA *secure in the random oracle model.*

Proof. Let $\mathcal{A}$ be a PPT adversary against the d-adaptive CPA security of $\mathsf{BC\text{-}IBE}_{\mathsf{kh}}$. We define q_H as the maximum number of queries issued to the random oracle H, and T_H as the table-list of query-response pairs to H.

We define $\widehat{\mathsf{Game}}$ as the security game which is the same as the ordinary d-adaptive CPA security game except that the procedure of the H oracle is modified as follows: At the beginning of the security game, an index $h_{\mathsf{id}^*} \in [n]$ for the challenge identity id^* is chosen uniformly at random. Given a query $\mathsf{id} \in \mathcal{ID}$, the H oracle checks whether $\mathsf{T}[\mathsf{id}] = \emptyset$. If $\mathsf{T}[\mathsf{id}] = h_{\mathsf{id}} \in [n]$, it returns h_{id}. Otherwise, it chooses $h_{\mathsf{id}} \xleftarrow{\$} [n]$. Then the challenger aborts if $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$. If $h_{\mathsf{id}} \notin L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$, H returns h_{id} and sets $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$. Here, let Abort be the event that $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$ occurs when choosing $h_{\mathsf{id}} \xleftarrow{\$} [n]$.

In addition, W and $\widehat{W}$ are defined as the events that $\mathcal{A}$ outputs b' such that $b = b'$ in the d-adaptive CPA game and $\widehat{\mathsf{Game}}$, respectively. Let Abort be the event that h_{id} is included in $L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$ in $\widehat{\mathsf{Game}}$ if H chooses h_{id} uniformly at random.

In the same way as the proof of Theorem 2, we have the following upper bound of $\Pr[\mathsf{Abort}]$:

$$\Pr[\mathsf{Abort}] \leq \sum_{i \in [q_H + d]} \frac{\ell + 1}{n - (i-1)} \leq \sum_{i \in [q_H + d]} \frac{\ell + 1}{n - (q_H + d)} \leq \frac{(q_H + d)(\ell + 1)}{n - (q_H + d)}.$$

In addition, $\widehat{\mathsf{Game}}$ is identical to the ordinary adaptive CPA security game, unless Abort occurs. Hence, we have $|\Pr[W] - \Pr[\widehat{W}]| \leq (q_H + d)(\ell + 1)/(n - (q_H + d))$.

We show that the winning probability in $\widehat{\mathsf{Game}}$ is negligible assuming the IND-CPA security of PKE. By using $\mathcal{A}$, a PPT algorithm $\mathcal{D}$ against PKE, as follows: $\mathcal{D}$ is given the public key pk^* of PKE. In the **Setup** phase of the d-adaptive CPA security game, $\mathcal{D}$ chooses $h_{\mathsf{id}^*} \xleftarrow{\$} [n]$, $i^* \xleftarrow{\$} \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*})$ and sets $\mathsf{pk}_{i^*} = \mathsf{pk}^*$. For every $i \in [u] \backslash \{i^*\}$, it generates $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KGen}(1^\lambda)$, sets $\mathsf{T}_H \leftarrow \emptyset$, and gives $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u)$ to $\mathcal{A}$. The $\mathsf{O}_{\mathsf{EXT}}$ and H oracles are simulated as follows:

- H: Given $\mathsf{id} \in \mathcal{ID}$, return h_{id} if $\mathsf{T}_H(\mathsf{id}) = h_{\mathsf{id}} \in [n]$. If $\mathsf{T}_H[\mathsf{id}] = \emptyset$, do the following:
  1. Choose $h_{\mathsf{id}} \xleftarrow{\$} [n]$.
  2. If $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$, abort and output a random bit.
  3. If $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})$, abort and output a random bit.
  4. Return h_{id} and set $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$.
- $\mathsf{O}_{\mathsf{EXT}}$: Given an extraction query $\mathsf{id} \in \mathcal{ID}$, obtain $h_{\mathsf{id}} \in [n]$ by accessing H, and return $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Combine}(\phi_{\boldsymbol{M}}(H(\mathsf{id})), (\mathsf{sk}_i)_{i \in [u]})$.

When $\mathcal{A}$ submits $(\mathsf{id}^*, \mathsf{m}_0^*, \mathsf{m}_1^*)$, $\mathcal{D}$ obtains c_{i^*} by issuing $(\mathsf{m}_0^*, \mathsf{m}_1^*)$ to the IND-CPA security game, and then returns $\mathsf{ct}^* \leftarrow \mathsf{Modify}(i^*, \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}), \mathsf{pp}, c_{i^*})$. Finally, $\mathcal{D}$ outputs $b' \in \{0,1\}$ if $\mathcal{A}$ outputs b'.

In the same way as the proofs of Theorems 1 and 2, it is shown that the simulation of the H and $\mathsf{O}_{\mathsf{EXT}}$ are correct. Furthermore, the challenge ciphertext generated by $\mathcal{D}$ is indistinguishable from the real challenge ciphertext, due to the u-key malleability of PKE. In addition, it is clear that the winning condition of $\mathcal{D}$ is identical to that of $\mathcal{A}$. Hence, we have $|\Pr[\widehat{W}] - 1/2| \leq u \cdot \mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{D}}(\lambda)$.

From the above, we obtain

$$\mathsf{Adv}^{\text{adaptive}}_{\mathsf{BC\text{-}IBE},\mathcal{A}}(\lambda) \leq u \cdot \mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{D}}(\lambda) + \frac{(q_H + d)(\ell + 1)}{n - (q_H + d)},$$

and complete the proof. □

Acknowledgements. This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan. This work was in part supported by JSPS KAKENHI Grant Number JP22K19773.

References

[1] Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: EUROCRYPT. LNCS, vol. 6110, pp. 553–572. Springer (2010)

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

[3] Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: CRYPTO. LNCS, vol. 2139, pp. 213–229. Springer (2001)

[4] Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: EUROCRYPT. LNCS, vol. 6110, pp. 523–552. Springer (2010)

[5] Cheraghchi, M., Nakos, V.: Combinatorial group testing and sparse recovery schemes with near-optimal decoding time. In: FOCS. pp. 1203–1213. IEEE (2020)

[6] Choi, K.Y., Kim, E., Yoon, H.J., Moon, D., Cho, J.: Generic construction of bounded-collusion IBE via table-based id-to-key map. In: CANS. LNCS, vol. 11829, pp. 457–469. Springer (2019)

[7] Dodis, Y., Katz, J., Xu, S., Yung, M.: Key-insulated public key cryptosystems. In: EUROCRYPT. LNCS, vol. 2332, pp. 65–82. Springer (2002)

[8] Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.D.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J. Comput. **38**(1), 97–139 (2008)

[9] Dorfman, R.: The detection of defective members of large populations. The Annals of Mathematical Statistics **Vol. 14, No. 4**, 436–440 (1943)

[10] Du, D.Z., Hwang, F.K.: Combinatorial Group Testing and Its Applications (2nd Edition), Series on Applied Mathematics, vol. 12. World Scientific (2000)

[11] Eppstein, D., Goodrich, M.T., Hirschberg, D.S.: Improved combinatorial group testing algorithms for real-world problem sizes. SIAM J. Comput. **36**(5), 1360–1375 (2007)

[12] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC. pp. 197–206. ACM (2008)

[13] Goldwasser, S., Lewko, A.B., Wilson, D.A.: Bounded-collusion IBE from key homomorphism. In: TCC. LNCS, vol. 7194, pp. 564–581. Springer (2012)

[14] Hövelmanns, K., Kiltz, E., Schäge, S., Unruh, D.: Generic authenticated key exchange in the quantum random oracle model. In: Public Key Cryptography (2). LNCS, vol. 12111, pp. 389–422. Springer (2020)

[15] Hwang, F.K.: A method for detecting all defective members in a population by group testing. Journal of the American Statistical Association **Vol. 67, No. 339**, 605–608 (1972)

[16] Indyk, P., Ngo, H.Q., Rudra, A.: Efficiently decodable non-adaptive group testing. In: SODA. pp. 1126–1142. SIAM (2010)

[17] Li, C.H.: A sequential method for screening experimental variables. Journal of the American Statistical Association **Vol. 57, No. 298**, 455–477 (1962)

[18] Porat, E., Rothschild, A.: Explicit non-adaptive combinatorial group testing schemes. In: ICALP (1). LNCS, vol. 5125, pp. 748–759. Springer (2008)

[19] Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: EUROCRYPT (3). LNCS, vol. 10822, pp. 520–551. Springer (2018)

[20] Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: EUROCRYPT. LNCS, vol. 6632, pp. 27–47. Springer (2011)

[21] Tessaro, S., Wilson, D.A.: Bounded-collusion identity-based encryption from semantically-secure public-key encryption: Generic constructions with short ciphertexts. In: Public Key Cryptography. LNCS, vol. 8383, pp. 257–274. Springer (2014)

[22] Thierry-Mieg, N.: A new pooling strategy for high-throughput screening: the shifted transversal design. BMC Bioinformatics **7**, 28 (2006)

[23] Waters, B.: Efficient identity-based encryption without random oracles. In: EUROCRYPT. LNCS, vol. 3494, pp. 114–127. Springer (2005)

[24] Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: CRYPTO. LNCS, vol. 5677, pp. 619–636. Springer (2009)

[25] Yamada, S.: Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In: EUROCRYPT (2). LNCS, vol. 9666, pp. 32–62. Springer (2016)

[26] Zhang, J., Chen, Y., Zhang, Z.: Programmable hash functions from lattices: Short signatures and ibes with small key sizes. In: CRYPTO (3). LNCS, vol. 9816, pp. 303–332. Springer (2016)

A BC-IBE from Disjoint Simulatable PKE

We present a BC-IBE scheme constructed from disjoint simulatable PKE, in order to extend the class of the underlying PKE. To do this, we employ an additional primitive: a universal hash function. Notice that, by additionally assuming multi-key malleability or the two properties key homomorphism and weak multi-key malleability, it is possible to show the d-adaptive CPA security of the resulting BC-IBE, in the same way as the security proof for the scheme in this section.

Since we employ a universal hash function to construct the BC-IBE scheme, we describe this definition.

Definition 15. *A function family $\mathcal{H}_\lambda = \{h : \{0,1\}^\mu \to \{0,1\}^\nu\}$ is a universal hash family (where $\mu = \mu(\lambda)$ and $\nu = \nu(\lambda)$) if the following holds:*

- *For every λ, $\nu < \mu$.*
- *For any PPT algorithm $\mathcal{A}$, the probability*

$$\Pr\left[x \neq x' \wedge h(x) = h(x') \mid h \xleftarrow{\$} \mathcal{H}_\lambda; (x, x') \leftarrow \mathcal{A}(h)\right].$$

  is negligible in λ.

Our proposed BC-IBE scheme $\mathsf{BC\text{-}IBE}_{\mathsf{ds}} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ is constructed as follows: For a security parameter λ, let $n = n(\lambda)$, $u = u(\lambda), \mu = \mu(\lambda), \bar{\mu} = \bar{\mu}(\lambda), \nu = \nu(\lambda)$ be positive integers, let $\mathcal{ID} = \mathcal{ID}(\lambda)$ be the identity space such that $|\mathcal{ID}| = n$, and let $\mathcal{M} = \{0,1\}^\nu$ be the message space. We use a PKE scheme $\mathsf{PKE} = (\mathsf{PKE.KGen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ with the message space $\{0,1\}^{\bar{\mu}}$ and a $(\mu, \bar{\mu}, v)$-AONT Trans with an efficient inverse function $\mathsf{Inverse}$. $H : \mathcal{ID} \to [n]$ is a random oracle, $\boldsymbol{M} \in \{0,1\}^{u \times n}$ is a (d, ℓ)-list-disjunct matrix, and $\mathcal{H}_\lambda = \{h : \{0,1\}^\mu \to \{0,1\}^\nu\}$ is a family of universal hash functions.

- $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$:
  1. Generate $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KGen}(1^\lambda)$ for $i \in [u]$.
  2. Choose $h \xleftarrow{\$} \mathcal{H}_\lambda$.
  3. Output $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u, h)$ and $\mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_u)$.
- $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{msk}, \mathsf{id})$:
  1. Parse $\mathsf{msk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_u)$.
  2. Output $\mathsf{sk}_{\mathsf{id}} = (\mathsf{sk}_i)_{i \in \phi_{\boldsymbol{M}}(H(\mathsf{id}))}$.
- $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{id}, \mathsf{m})$:
  1. Parse $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u, h)$.
  2. Choose $x \xleftarrow{\$} \{0,1\}^\mu$.
  3. Compute $\hat{c} \leftarrow h(x) \oplus \mathsf{m}$.
  4. Compute $(x_1, \ldots, x_v, z) \leftarrow \mathsf{Trans}(x)$.
  5. Compute $c_i \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\sigma_i}, x_i)$ for $i \in [v]$, where $\phi_{\boldsymbol{M}}(H(\mathsf{id})) = \{\sigma_1, \ldots, \sigma_v\}$ for all distinct $\sigma_1, \ldots, \sigma_v$.
  6. Output $\mathsf{ct} = (c_1, \ldots, c_v, \hat{c}, z)$.

- $\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$:
  1. Parse $\mathsf{sk}_{\mathsf{id}} = (\mathsf{sk}_i)_{i \in \phi_{\boldsymbol{M}}(H(\mathsf{id}))}$ and $\mathsf{ct} = (c_1, \ldots, c_v, \hat{c}, z)$.
  2. Compute $x_i \leftarrow \mathsf{PKE.Dec}(\mathsf{sk}_{\sigma_i}, c_i)$ for every $i \in [v]$.
  3. Compute $x' \leftarrow \mathsf{Inverse}(x_1, \ldots, x_v, z)$
  4. Output $\mathsf{m}' \leftarrow h(x') \oplus \hat{c}$.

It is clear that the correctness of $\mathsf{BC\text{-}IBE}_{\mathsf{ds}}$ follows the correctness of PKE. We prove the security of this BC-IBE scheme, as follows:

Theorem 4. *If a PKE scheme* PKE *is* ϵ_{ds}-disjoint simulatable*, an efficient randomized transformation* Trans *with an inverse function* Inverse *is a* $(\mu, \bar{\mu}, v)$-AONT*, and a binary matrix* $\boldsymbol{M}$ *is* (d, ℓ)*-list-disjunct, then the resulting BC-IBE scheme* $\mathsf{BC\text{-}IBE}_{\mathsf{ds}}$ *is* d-adaptive CPA *secure in the random oracle model.*

Proof. Let $\mathcal{A}$ be a PPT adversary against the d-adaptive CPA security of $\mathsf{BC\text{-}IBE}_{\mathsf{ds}}$. We define q_H as the maximum number of queries issued to the random oracle H, and T_H as the table of query-response pairs to H. We define $\mathsf{ct}^* = (c_1, \ldots, c_v^*, \hat{c}^*, z^*)$ as the challenge ciphertext.

In order to prove Theorem 4, we consider several security games. For an integer $i \geq 0$, let W_i be the event that $\mathcal{A}$ wins in a security game Game_i.

$\underline{\mathsf{Game}_0}$: This is the same game as the standard adaptive security game. Thus, we have $\mathsf{Adv}^{\mathrm{adaptive}}_{\mathsf{BC\text{-}IBE},\mathcal{A}}(\lambda) = |\Pr[W_0] - 1/2|$.

$\underline{\mathsf{Game}_1}$. This game is the same as Game_0 except that the procedure of the H oracle is modified as follows: Suppose that at the beginning of the security game, an index $h_{\mathsf{id}^*} \in [n]$ for the challenge identity id^* is chosen uniformly at random. Given a query $\mathsf{id} \in \mathcal{ID}$, the H oracle checks whether $\mathsf{T}[\mathsf{id}] = \emptyset$. If $\mathsf{T}[\mathsf{id}] = h_{\mathsf{id}} \in [n]$, it returns h_{id}. Otherwise, it chooses $h_{\mathsf{id}} \xleftarrow{\$} [n]$. Then the challenger aborts if $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$. Otherwise H returns h_{id} and sets $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$.

Let Abort be the event that $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$ holds when H chooses $h_{\mathsf{id}} \xleftarrow{\$} [n]$. We estimate the upper bound of the probability $\Pr[\mathsf{Abort}]$, because Game_0 and Game_1 are identical unless Abort occurs. In the same way as the proof of Theorem 1, this upper bound is obtained as follows:

$$\Pr[\mathsf{Abort}] \leq \sum_{i \in [q_H + d]} \frac{\ell + 1}{n - (i-1)} \leq \sum_{i \in [q_H + d]} \frac{\ell + 1}{n - (q_H + d)} \leq \frac{(q_H + d)(\ell + 1)}{n - (q_H + d)}.$$

Hence, we have $|\Pr[W_0] - \Pr[W_1]| \leq (q_H + d)(\ell + 1)/(n - (q_H + d))$.

In order to show that the winning probability in Game_1 is negligible, we consider additional security games $\widehat{\mathsf{Game}_1}, \widehat{\mathsf{Game}_2}, \widehat{\mathsf{Game}_3}$. Let $\widehat{W_i}$ be the event that $\mathcal{A}$ wins $\widehat{\mathsf{Game}_i}$ for $i \in \{1, 2, 3\}$.

$\underline{\widehat{\mathsf{Game}_1}}$. This game is the same as Game_1 except that some random index $i^* \in \phi_{\boldsymbol{M}}(H(\mathsf{id}^*))$ is fixed, and the challenger computes $(x_1^*, \ldots, x_v^*, z^*) \leftarrow \mathsf{Trans}(\mathsf{m}_b^*)$, $c_{j^*}^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{i^*}, 0^{|\mathsf{m}_0^*|})$, and $c_i^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\sigma_i^*}, x_i^*)$ for $i \in [u] \backslash \{j^*\}$ (where $j^* \in [v]$ is the index such that $i^* = \sigma_{j^*}^*$ and $\phi_{\boldsymbol{M}}(H(\mathsf{id}^*)) = \{\sigma_1^*, \ldots, \sigma_v^*\}$), when generating the challenge ciphertext $\mathsf{ct}^* = (c_1^*, \ldots, c_v^*, z^*)$.

We show that the indistinguishability between Game_1 and $\widehat{\mathsf{Game}_1}$ follows the disjoint simulatability of PKE. By using $\mathcal{A}$, we construct a PPT algorithm $\mathcal{D}_1$ breaking the disjoint simulatability of PKE, as follows: $\mathcal{D}_1$ is given a public key pk^* of PKE. At the beginning of the security game, $\mathcal{D}_1$ chooses $h_{\mathsf{id}^*} \xleftarrow{\$} [n]$, $i^* \xleftarrow{\$} \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*})$, and sets $\mathsf{pk}_{i^*} = \mathsf{pk}^*$. Then it generates $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KGen}(1^\lambda)$ for $i \in [u] \backslash \{i^*\}$ and chooses $h \xleftarrow{\$} \mathcal{H}_\lambda$. It gives $\mathsf{pp} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_u, h)$ to $\mathcal{A}$ and initializes the table $\mathsf{T}_H \leftarrow \emptyset$. The H and $\mathsf{O}_{\mathsf{EXT}}$ oracles are simulated in the following way:

- H: Given $\mathsf{id} \in \mathcal{ID}$, return h_{id} if $\mathsf{T}_H(\mathsf{id}) = h_{\mathsf{id}} \in [n]$. If $\mathsf{T}_H[\mathsf{id}] = \emptyset$, do the following:
  1. Choose $h_{\mathsf{id}} \xleftarrow{\$} [n]$.
  2. If $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$, abort and output a random bit.
  3. If $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})$, abort and output a random bit.
  4. Return h_{id} and set $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$.
- $\mathsf{O}_{\mathsf{EXT}}$: Given an extraction query $\mathsf{id} \in \mathcal{ID}$, obtain $h_{\mathsf{id}} \in [n]$ by calling the H oracle and return $\mathsf{sk}_{\mathsf{id}} = (\mathsf{sk}_i)_{i \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})}$.

When $\mathcal{A}$ submits $(\mathsf{id}^*, \mathsf{m}_0^*, \mathsf{m}_1^*)$, $\mathcal{D}_1$ does the following:

1. Choose $b \xleftarrow{\$} \{0,1\}$.
2. Choose $x^* \xleftarrow{\$} \{0,1\}^\mu$.
3. Compute $\hat{c}^* \leftarrow h(x^*) \oplus \mathsf{m}_b^*$.
4. Compute $(x_1^*, \ldots, x_v^*, z^*) \leftarrow \mathsf{Trans}(x^*)$.
5. Compute $c_i^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\sigma_i^*}, x_i^*)$ for $i \in [v] \backslash \{j^*\}$ where $\sigma_{j^*}^* = i^*$.
6. Obtain the j^*-th PKE ciphertext $c_{j^*}^*$ by requesting the challenge ciphertext in the disjoint simulatability game.
7. Return $\mathsf{ct}^* = (c_1^*, \ldots, c_v^*, \hat{c}^*, z^*)$ and set $\mathsf{T}_H[\mathsf{id}^*] \leftarrow h_{\mathsf{id}^*}$.

Finally, when $\mathcal{A}$ outputs the guessing bit $b' \in \{0,1\}$, $\mathcal{D}_1$ outputs 1 if $b = b'$, and otherwise 0.

The simulation of the H oracle is correct, since for a query id, $H(\mathsf{id}) \notin L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$ holds in $\widehat{\mathsf{Game}_1}$, and H chooses a random $h_{\mathsf{id}} = H(\mathsf{id})$ satisfying this condition. Regarding the challenge ciphertext ct^*, Game_1 is simulated if $c_i^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{i^*}, \mathsf{m}_b^*)$, and Game_2 is simulated otherwise. In addition, it is clear that $\mathcal{D}_1$ wins the IND-CPA security game unless the H oracle chooses $h_{\mathsf{id}} \in [n]$ such that $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}})$. Hence, we have $\left|\Pr[W_1] - \Pr[\widehat{W_1}]\right| \leq u \cdot \mathsf{Adv}^{\mathrm{ds}}_{\mathsf{PKE},\mathcal{D}_1}(\lambda)$.

$\widehat{\mathsf{Game}_2}$. This game is the same as $\widehat{\mathsf{Game}_1}$ except that the challenger computes $(x_1^*, \ldots, x_v^*, z^*) \leftarrow \mathsf{AONT}(0^{|x^*|})$ instead of $(x_1^*, \ldots, x_v^*, z^*) \leftarrow \mathsf{AONT}(x^*)$, when generating the challenge ciphertext $\mathsf{ct}^* = (c_1^*, \ldots, c_v^*, \hat{c}^*, z^*)$.

We show that the indistinguishability between Game_2 and Game_3 follows the security of AONT. To do this, we construct a PPT algorithm $\mathcal{D}_2$ against $(\mu, \bar{\mu}, v)$-AONT, as follows: $\mathcal{D}_2$ is given the O_{LR} oracle and chooses $h_{\mathsf{id}^*} \xleftarrow{\$} [n]$ and $i^* \xleftarrow{\$} \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*})$. At the beginning of the d-adaptive CPA security game, it generates $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KGen}(1^\lambda)$ for $i \in [u]$ and chooses $h \xleftarrow{\$} \mathcal{H}_\lambda$. When $\mathcal{A}$ accesses the H and $\mathsf{O}_{\mathsf{EXT}}$ oracles, $\mathcal{D}_2$ simulates these oracles, as follows:

- H: Given $\mathsf{id} \in \mathcal{ID}$, return h_{id} if $\mathsf{T}_H(\mathsf{id}) = h_{\mathsf{id}} \in [n]$. If $\mathsf{T}_H[\mathsf{id}] = \emptyset$, do the following:
  1. Choose $h_{\mathsf{id}} \xleftarrow{\$} [n]$.
  2. If $h_{\mathsf{id}} \in L(\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}))$, abort and output a random bit.
  3. If $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*})$, abort and output a random bit.
  4. Return h_{id} and set $\mathsf{T}_H[\mathsf{id}] \leftarrow h_{\mathsf{id}}$.

- $\mathsf{O}_{\mathsf{EXT}}$: Given an extraction query $\mathsf{id} \in \mathcal{ID}$, obtain $h_{\mathsf{id}} \in [n]$ by accessing H, and return $\mathsf{sk}_{\mathsf{id}} \leftarrow (\mathsf{sk}_i)_{i \in \phi_H(h_{\mathsf{id}})}$.

When $\mathcal{A}$ submits $(\mathsf{id}^*, \mathsf{m}_0^*, \mathsf{m}_1^*)$, $\mathcal{D}_2$ does the following:

1. Let $\phi_{\boldsymbol{M}}(h_{\mathsf{id}^*}) = \{\sigma_1^*, \ldots, \sigma_v^*\}$ for all distinct $\sigma_1^*, \ldots, \sigma_v^* \in [u]$, and let $j^* \in [u]$ be an index such that $i^* = \sigma_{j^*}^*$.
2. Choose $x^* \xleftarrow{\$} \{0,1\}^\mu$.
3. Compute $\hat{c}^* \leftarrow h(x^*) \oplus \mathsf{m}$.
4. Obtain $(x_1^*, \ldots, x_{j^*-1}^*, x_{j^*+1}^*, \ldots, x_v^*, z^*)$ by issuing $(j^*, x^*, 0^{|x^*|})$ to the given O_{LR} oracle.
5. Compute $c_{j^*} \leftarrow \mathsf{PKE.}\overline{\mathsf{Enc}}(\mathsf{pk}_{i^*})$, and for $i \in [v] \backslash \{j^*\}$, compute $c_i^* \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_{\sigma_i^*}, x_i^*)$.
6. Return $\mathsf{ct}^* = (c_1^*, \ldots, c_v^*, \hat{c}^*, z^*)$.

Finally, when $\mathcal{A}$ outputs $b' \in \{0,1\}$, $\mathcal{D}_2$ outputs 1 if $b = b'$ and 0 otherwise.

The simulation of the H and $\mathsf{O}_{\mathsf{EXT}}$ oracles is correct since $\mathcal{D}_2$ generates all secret keys of the underlying PKE. Regarding the challenge ciphertext, $\widehat{\mathsf{Game}_1}$ is simulated if x^* is transformed, and $\widehat{\mathsf{Game}_2}$ is simulated if $\mathsf{Trans}(0^{|x^*|})$ is given. Furthermore, $\mathcal{D}_2$ breaks the security of AONT unless $h_{\mathsf{id}} \in [n]$ such that $i^* \in \phi_{\boldsymbol{M}}(h_{\mathsf{id}^*})$ is chosen by the H oracle. Hence, we have $\left|\Pr[\widehat{W}_1] - \Pr[\widehat{W}_2]\right| \leq u \cdot \mathsf{Adv}^{\mathrm{ind}}_{\mathsf{AONT},\mathcal{D}_2}(\lambda)$.

$\underline{\widehat{\mathsf{Game}_3}}$. This game is the same as $\widehat{\mathsf{Game}_2}$ except that the challenger chooses $r^* \xleftarrow{\$} \{0,1\}^\nu$ and computes $\hat{c}^* \xleftarrow{\$} r^* \oplus \mathsf{m}_b^*$ instead of $\hat{c}^* \leftarrow h(x^*) \oplus \mathsf{m}_b^*$, when generating the challenge ciphertext $\mathsf{ct}^* = (c_1^*, \ldots, c_v^*, \hat{c}^*, z^*)$.

Since no information of m_b^* is contained in $(c_1^*, \ldots, c_v^*, z^*)$, we have $\left|\Pr[\widehat{W}_2] - \Pr[\widehat{W}_3]\right| \leq \mathsf{negl}(\lambda)$, due to [8, Lemma 2.1].

Let Bad be the event that $\hat{c}^* \in \mathsf{PKE.Enc}(\mathsf{pk}, \{0,1\}^{\bar{\mu}})$, where $\mathsf{PKE.Enc}(\mathsf{pk}, \{0,1\}^{\bar{\mu}})$ is the set of all ciphertexts which are generated by encrypting messages in $\{0,1\}^{\bar{\mu}}$. Then, we have $\Pr[\mathsf{Bad}] \leq \epsilon_{ds}$. In addition, we have $\Pr[\widehat{W}_3 \mid \neg\mathsf{Bad}] = 1/2$ since $\mathcal{A}$ is not given any information of m_b^*. Hence, we have

$$\begin{aligned}
\left|\Pr[\widehat{W}_3] - \frac{1}{2}\right| &= \left|\Pr[\widehat{W}_3 \wedge \mathsf{Bad}] + \Pr[\widehat{W}_3 \wedge \neg\mathsf{Bad}] - \frac{1}{2}(\Pr[\mathsf{Bad}] + \Pr[\neg\mathsf{Bad}])\right| \\
&= \left|\Pr[\mathsf{Bad}] \cdot \left(\Pr[\widehat{W}_3 \mid \mathsf{Bad}] - \frac{1}{2}\right) + \Pr[\neg\mathsf{Bad}] \cdot \left(\Pr[\widehat{W}_3 \mid \neg\mathsf{Bad}] - \frac{1}{2}\right)\right| \\
&\leq \Pr[\mathsf{Bad}] + \left|\Pr[\widehat{W}_3 \mid \neg\mathsf{Bad}] - \frac{1}{2}\right| \\
&\leq \epsilon_{ds}
\end{aligned}$$

From the discussion above, we obtain

$$\mathsf{Adv}^{\mathrm{adaptive}}_{\mathsf{BC\text{-}IBE},\mathcal{A}}(\lambda) \leq u \cdot \mathsf{Adv}^{\mathrm{ds}}_{\mathsf{PKE},\mathcal{D}}(\lambda) + u \cdot \epsilon_{ds} + \frac{(q_H + d)(\ell + 1)}{n - (q_H + d)} + \mathsf{negl}(\lambda),$$

and complete the proof. □