Attribute-based Keyed (Fully) Homomorphic Encryption

Keita Emura* Shingo Sato† Atsushi Takayasu‡

February 14, 2024

Abstract

Keyed homomorphic public key encryption (KHPKE) is a variant of homomorphic public key encryption, where only users who have a homomorphic evaluation key can perform a homomorphic evaluation. Then, KHPKE satisfies the CCA2 security against users who do not have a homomorphic evaluation key, while it satisfies the CCA1 security against users who have the key. Thus far, several KHPKE schemes have been proposed under the standard Diffie-Hellman-type assumptions and *keyed fully homomorphic encryption* (KFHE) schemes have also been proposed from lattices. As a natural extension, there is an identity-based variant of KHPKE; however, the security is based on a q-type assumption and there are no attribute-based variants. Moreover, there are no identity-based variants of KFHE schemes due to the complex design of the known KFHE schemes. In this paper, we obtain two results for constructing the attribute-based variants. First, we propose an attribute-based KFHE (ABKFHE) scheme from lattices. We start by designing the first KFHE scheme secure solely under the LWE assumption in the standard model. Since the design is conceptually much simpler than known KFHE schemes, we just replace their building blocks with attribute-based ones and obtain the proposed ABKFHE schemes. Next, we propose an efficient attribute-based KHPKE (ABKHE) scheme from a pair encoding scheme (PES). Due to the benefit of PES, we obtain various ABKHE schemes that contain the first identity-based KHPKE scheme secure under the standard k-linear assumption and the first pairing-based ABKHE schemes supporting more expressive predicates.

*Kanazawa University, Japan
†Yokohama National University, Japan
‡The University of Tokyo and National Institute of Advanced Industrial Science and Technology, Japan

Contents

1 Introduction

1.1 Background

Given two ciphertexts $\mathsf{ct}^{(1)}$ and $\mathsf{ct}^{(2)}$ of (multiplicative) homomorphic encryption (HE), where they are encryptions of $\mu^{(1)}$ and $\mu^{(2)}$, respectively, arbitrary users can compute an evaluated ciphertext ct that is an encryption of $\mu^{(1)} \cdot \mu^{(2)}$. Given an arbitrary circuit C and ciphertexts $\mathsf{ct}^{(1)}, \ldots, \mathsf{ct}^{(L)}$ of fully homomorphic encryption (FHE), where they are encryptions of $\mu^{(1)}, \ldots, \mu^{(L)}$, respectively, arbitrary users can compute an evaluated ciphertext ct_{C} that is an encryption of $\mathsf{C}(\mu^{(1)}, \ldots, \mu^{(L)})$. After Gentry [Gen09] proposed the first FHE scheme, several improved FHE schemes have been proposed such as [Bra12, BGV12, BV11a, BV11b, BV14, GSW13, vGHV10]. The publicly computable homomorphism provides several applications such as delegated computation and multi-party computation. In contrast, the nature prevents (F)HE schemes from achieving the CCA2 security. Thus, several CCA1-secure (F)HE schemes have been proposed such as the Cramer-Shoup-lite [CS98] and several FHE schemes [CRRV17, DGM15, LMSV12, ZPS12]. However, Loftus et al. showed that CCA1-secure FHE schemes may be vulnerable if there are ciphertext validity checking oracles [LMSV12] as Bleichenbacher's attack on RSA [Ble98].

To reconcile homomorphic operations and the chosen ciphertext security, Emura et al. introduced a notion of *keyed homomorphic public key encryption* (KHPKE) [EHO+13]. As opposed to (F)HE, only users who have a homomorphic evaluation key hk can compute evaluated ciphertexts of KHPKE. The standard security requirement of KHPKE called the KH-CCA security ensures that a KHPKE scheme satisfies the CCA2/CCA1 security against an adversary without/with hk, respectively. Thus, the KH-CCA security is strictly stronger than the CCA1 security. Moreover, KH-CCA-secure KHPKE schemes are secure even in the presence of ciphertext validity checking oracles [Emu21]. Libert et al. [LPJY14] proposed the first KH-CCA-secure multiplicative KHPKE scheme, then Jutla and Roy [JR15] and Emura et al. [EHN+18] proposed improved schemes. Among them, Emura et al.'s scheme is the most efficient since it does not require pairing unlike [JR15, LPJY14] and satisfies the KH-CCA security under the DDH assumption.

Lai et al. extended the notion of KHPKE and proposed the first keyed FHE (KFHE) scheme [LDM+16] under the LWE assumption and iO [BGI+01]; however, it does not satisfy the KH-CCA security but only the weaker security which is not CCA1 but only the CPA security against an adversary with hk. Then, Sato et al. proposed the first KH-CCA-secure KFHE scheme under the LWE assumption [SET22]. In particular, Sato et al. followed the complex design methodology of Jutla and Roy's KHPKE scheme [JR15] based on a strong dual-system simulation-sound NIZK system for Diffie-Hellman languages. To construct a strong dual-system simulation-sound NIZK system for FHE ciphertexts, Sato et al. have to rely on either zk-SNARKs for arithmetic circuits based on knowledge assumptions [BBC+18, BCC+17, BCCT13, GGPR13, MBKM19, ZSZ+22] or zk-SNARKs for NP in the (quantum) random oracle model [CMS19]. Thus, there are no known KFHE schemes whose KH-CCA security is based solely on the LWE assumption in the standard model. Maeda and Nuida [MN22] proposed a keyed two-level homomorphic encryption scheme which supports the additive homomorphism with a single multiplication under the SXDH assumption.

As another direction of the topic, Emura et al. constructed a pairing-based identity-based keyed homomorphic encryption (IBKHE) scheme [EHN+18]. Although the scheme satisfies the adaptive KH-CCA security, it is based on a q-type assumption. Thus far, there are no known pairing-based IBKHE schemes under the standard assumptions although there are various pairing-based homomorphic identity-based encryption (IBE) schemes under such assumptions [BB04, CLL+14, CW14, Lew12, Wat09, Wat05]. Similarly, there are no known attribute-based keyed homomorphic encryption (ABKHE) schemes supporting more expressive predicates although the pair encoding framework [Att14, Wee14] enables us to construct various pairing-based expressive attribute-based encryption (ABE) schemes [AC16, AC17, Amb21, ABS17, Att16, CGW15, CG17, Tak21]. The ABE schemes are adaptively secure under the q-ratio assumption and the standard k-linear assumption for expressive and simple predicates, respectively. Moreover, there are no known identity-based keyed fully homomorphic encryption (IBKFHE) schemes and attribute-based keyed fully homomorphic encryption (ABKFHE) schemes, while there are various known lattice-based identity-based and attribute-based FHE schemes such as [BCTW16, CM15, GSW13, HK17, ML19, PD20]. These situations stem from the fact that known design methodologies of KHPKE and KFHE are too complex to extend to identity/attribute-based settings. In other words, proving the KH-CCA security seems to require a specific technique which is not common in the context of public key encryption. For example, Emura et al. [EHN$^+$18] introduced additional security notions for universal$_2$ hash proof system [CS02] and proved the KH-CCA security, where the additional security notions have not been used in other papers. As we explained above, Jutla and Roy [JR15] and Sato et al. [SET22] used strong dual-system simulation-sound NIZK systems that have been used only in these papers.

1.2 Our Contribution

In this paper, we first propose a generic construction of ABKFHE whose building blocks can be instantiated under the standard LWE assumption. For this purpose, we start by designing the first KH-CCA-secure KFHE scheme solely based on the LWE assumption in the standard model by modifying Canetti et al.'s CCA1-secure FHE scheme [CRRV17]. Specifically, Canetti et al. constructed a CCA1-secure FHE scheme from multi-key FHE (MFHE) [AJJM20, CM15, LTV12, MW16, PS16] and IBE, where MFHE schemes [AJJM20, MW16, PS16] are secure in the standard model and there are various IBE schemes secure in the standard model such as [ABB10, Yam17]. In addition to MFHE and IBE, we use only simple primitives and construct KFHE. Indeed, we additionally use one-time signatures (OTS) and message authentication codes (MAC). The design methodology is very simple since we just combine the Canetti-Halevi-Katz transformation [CHK04] and the encrypt-then-MAC paradigm [BN08] which are the standard techniques to prove the CCA2 security. As a result, the simplicity enables us to extend the proposed KFHE scheme and obtain a KH-CCA-secure ABKFHE scheme supporting cross-attribute evaluations by replacing IBE and MAC with delegatable ABE (DABE).

Unfortunately, the proposed ABKFHE scheme is not very efficient since the size of an evaluated ciphertext depends on the number of input ciphertexts although the feature is not the disadvantage of the proposed ABKFHE scheme. Indeed, the known CCA1-secure FHE scheme secure solely under the LWE assumption in the standard model [CRRV17] and attribute-based FHE schemes supporting cross-attribute evaluation [BCTW16, ML19, PD20] have similar features. Nevertheless, we overcome the issue by restricting the functionality and propose an efficient ABKHE scheme which supports multiplicative homomorphism without cross-attribute evaluations. Specifically, we construct the proposed ABKHE scheme from a pair encoding scheme (PES) [Att14, Wee14]. Due to the benefit of the pair encoding framework, we obtain adaptively KH-CCA-secure ABKHE schemes for various expressive predicates under the q-ratio assumption and those for simple predicates under the standard k-linear assumption using known PES such as [AC16, AC17, Att14, Att16, Att19, AY15, CGW15, Tak21, Wee14]. The result includes the first pairing-based IBKHE scheme under the standard k-linear assumption. Our design methodology is similar to Emura et al.'s KHPKE scheme [EHN$^+$18]. Although Emura et al.'s proof based on the hash proof system is complicated, we can simply prove the KH-CCA security when we focus on the KHPKE scheme instantiated under the matrix DDH assumption [EHK$^+$17]. Then, as Emura et al.

Table 1: Comparison among proposed ABK(F)HE schemes and known keyed homomorphic schemes

Scheme	Homomorphism	Access Control	Complexity Assumption
LPJY14 [LPJY14]	Multiplicative	None	DLIN
JR15 [JR15]	Multiplicative	None	SXDH
LDM+16 [LDM+16]	Fully	None	LWE + iO
EHN+18 [EHN+18]	Multiplicative	None	DDH
	Additive	None	DCR
	Multiplicative	Identity-based	q-ABDHE
SET22 [SET22]	Fully	None	LWE + Knowledge LWE + (Q)ROM
MN22 [MN22]	Two-Level	None	SXDH
This Work	Fully	Attribute-based	LWE
	Multiplicative	Identity-based	k-Lin
	Multiplicative	Attribute-based	k-Lin or q-ratio

extended the Cramer-Shoup cryptosystem [CS98] to their KHPKE scheme, we extend PES-based ABE schemes over dual system groups [AC16, AC17, CGW15] to our proposed ABKHE schemes.

Table 1 summarizes the comparison among proposed ABK(F)HE schemes and known keyed homomorphic schemes.

Notation. For non-negative integers a and b such that $a < b$, let $[a] \coloneqq \{1, 2, \ldots, a\}$ and $[a, b] \coloneqq \{a, a+1, \ldots, b\}$. For a finite set S, let $s \leftarrow_R S$ denote a uniform sampling from S and $|S|$ denote the size of S. For two strings a and b, $a \| b$ denotes their concatenation. "Probabilistic polynomial time" is abbreviated as "PPT". For two security games Game_i and Game_j, $\mathsf{Game}_i \approx_c \mathsf{Game}_j$ indicates that Game_i and Game_j are computationally indistinguishable.

1.3 Organization

In Section 2, we extend the definition of IBKHE [EHN+18] and define ABK(F)HE. In Section 3, we propose a generic construction of ABKFHE whose building blocks can be instantiated under the LWE assumption. In Section 4, we propose an efficient pairing-based ABKHE from pair encoding schemes.

2 Attribute-based Keyed (Fully) Homomorphic Encryption

In Section 2.1, we review a definition of keyed fully homomorphic encryption (KFHE). In Section 2.2, we define an attribute-based keyed (fully) homomorphic encryption (ABK(F)HE).

2.1 Keyed Fully Homomorphic Encryption

We review a definition of keyed fully homomorphic encryption (KFHE) by following [EHN+18, SET22].

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

- $\mathsf{KFHE.KGen}(1^\lambda) \to (\mathsf{KFHE.pk}, \mathsf{KFHE.dk}, \mathsf{KFHE.hk})$*: On input the security parameter* 1^λ*, it outputs a public key* $\mathsf{KFHE.pk}$ *a decryption key* $\mathsf{KFHE.dk}$*, and a homomorphic evaluation key* $\mathsf{KFHE.hk}$*.*

- $\mathsf{KFHE.Enc}(\mathsf{KFHE.pk}, \mu) \to \mathsf{KFHE.ct}$*: On input a* $\mathsf{KFHE.pk}$ *and a message* $\mu \in \mathcal{M}$*, it outputs a pre-evaluated ciphertext* $\mathsf{KFHE.ct}$*.*

- $\mathsf{KFHE.Eval}(\mathsf{KFHE.pk}, \mathsf{KFHE.hk}, (\mathsf{KFHE.ct}^{(\ell)})_{\ell \in [L]}, \mathsf{C}) \to \mathsf{KFHE.ct}_\mathsf{C}/\perp$*: On input a* $\mathsf{KFHE.pk}$*,* $\mathsf{KFHE.hk}$*, a tuple of* L *ciphertexts* $(\mathsf{KFHE.ct}^{(\ell)})_{\ell \in [L]}$*, and a circuit* $\mathsf{C} : \mathcal{M}^L \to \mathcal{M}$*, it outputs an evaluated ciphertext* $\mathsf{KFHE.ct}_\mathsf{C}$ *or a rejection symbol* $\perp$*.*

- $\mathsf{KFHE.Dec}(\mathsf{KFHE.pk}, \mathsf{KFHE.dk}, \mathsf{KFHE.ct}/\mathsf{KFHE.ct}_\mathsf{C}) \to \mu/\perp$*: On input a* $\mathsf{KFHE.pk}$*,* $\mathsf{KFHE.dk}$ *and* $\mathsf{KFHE.ct}/\mathsf{KFHE.ct}_\mathsf{C}$*, it outputs a decryption result* $\mu \in \mathcal{M}$ *or a rejection symbol* $\perp$*.*

It is required that an Π_KFHE satisfies both correctness and compactness.

Definition 2 (Correctness)**.** $\Pi_\mathsf{KFHE} = (\mathsf{KFHE.KGen}, \mathsf{KFHE.Enc}, \mathsf{KFHE.Eval}, \mathsf{KFHE.Dec})$ *satisfies* correctness *if the following conditions hold with overwhelming probability:*

- *For every* $(\mathsf{KFHE.pk}, \mathsf{KFHE.dk}, \mathsf{KFHE.hk}) \leftarrow \mathsf{KFHE.KGen}(1^\lambda)$ *and* $\mu \in \mathcal{M}$*, it holds that* $\mathsf{KFHE.Dec}(\mathsf{KFHE.pk}, \mathsf{KFHE.dk}, \mathsf{KFHE.Enc}(\mathsf{KFHE.pk}, \mu)) = \mu$*.*

- *For every* $(\mathsf{KFHE.pk}, \mathsf{KFHE.dk}, \mathsf{KFHE.hk}) \leftarrow \mathsf{KFHE.KGen}(1^\lambda)$*, circuit* $\mathsf{C} : \mathcal{M}^L \to \mathcal{M}$*, and* $(\mu^{(1)}, \ldots, \mu^{(L)}) \in \mathcal{M}^L$*, it holds that* $\mathsf{KFHE.Dec}(\mathsf{KFHE.pk}, \mathsf{KFHE.dk}, \mathsf{KFHE.ct}_\mathsf{C}) = \mathsf{C}(\mu^{(1)}, \ldots, \mu^{(L)})$*, where* $\mathsf{KFHE.ct}_\mathsf{C} \leftarrow \mathsf{KFHE.Eval}(\mathsf{KFHE.pk}, \mathsf{KFHE.hk}, (\mathsf{KFHE.ct}^{(\ell)})_{\ell \in [L]}, \mathsf{C})$ *and* $\mathsf{KFHE.ct}^{(\ell)} \leftarrow \mathsf{KFHE.Enc}(\mathsf{KFHE.pk}, \mu^{(\ell)})$ *for every* $\ell \in [L]$*.*

Definition 3 (Compactness)**.** $\Pi_\mathsf{KFHE} = (\mathsf{KFHE.KGen}, \mathsf{KFHE.Enc}, \mathsf{KFHE.Eval}, \mathsf{KFHE.Dec})$ *satisfies* compactness *if there exists a polynomial* poly *such that* $|\mathsf{KFHE.ct}_\mathsf{C}|$*, where* $\mathsf{KFHE.ct}_\mathsf{C} \leftarrow \mathsf{KFHE.Eval}(\mathsf{KFHE.pk}, \mathsf{KFHE.hk}, (\mathsf{KFHE.ct}^{(\ell)})_{\ell \in [L]}, \mathsf{C})$*, is independent of the size and depth of* C *and at most* $L \cdot \mathsf{poly}(\lambda)$ *for every security parameter* λ*.*

We define the KH-CCA security for KFHE. Specifically, to introduce as strong requirement as possible, we consider the case that a pre-evaluated ciphertext $\mathsf{KFHE.ct}$ and an evaluated ciphertext $\mathsf{KFHE.ct}_\mathsf{C}$ follow distinct distributions which are easily detectable. Our proposed KFHE scheme satisfies the condition.

Definition 4 (KH-CCA security)**.** *The* KH-CCA *security of* $\Pi_\mathsf{KFHE} = (\mathsf{KFHE.KGen}, \mathsf{KFHE.Enc}, \mathsf{KFHE.Eval}, \mathsf{KFHE.Dec})$ *is defined by the security game between a challenger* $\mathcal{C}$ *and an adversary* $\mathcal{A}$ *as follows.*

- **Init.** $\mathcal{C}$ *runs* $(\mathsf{KFHE.pk}, \mathsf{KFHE.dk}, \mathsf{KFHE.hk}) \leftarrow \mathsf{KFHE.KGen}(1^\lambda)$ *and sends* $\mathsf{KFHE.pk}$ *to* $\mathcal{A}$*.*

- **Phase 1.** $\mathcal{A}$ *is allowed to make the following three types of queries to* $\mathcal{C}$*.*

  - **Homomorphic Evaluation Key Reveal Query.** *Upon* $\mathcal{A}$*'s query,* $\mathcal{C}$ *sends* $\mathsf{KFHE.hk}$ *to* $\mathcal{A}$*.*
  - **Evaluation Query.** *Upon* $\mathcal{A}$*'s query on* $((\mathsf{KFHE.ct}^{(\ell)})_{\ell \in [L]}, \mathsf{C})$*,* $\mathcal{C}$ *sends the result of* $\mathsf{KFHE.Eval}(\mathsf{KFHE.pk}, \mathsf{KFHE.hk}, (\mathsf{KFHE.ct}^{(\ell)})_{\ell \in [L]}, \mathsf{C})$ *to* $\mathcal{A}$*.*
  - **Decryption Query.** *Upon* $\mathcal{A}$*'s query on* $\mathsf{KFHE.ct}/\mathsf{KFHE.ct}_\mathsf{C}$*,* $\mathcal{C}$ *sends the result of* $\mathsf{KFHE.Dec}(\mathsf{KFHE.pk}, \mathsf{KFHE.dk}, \mathsf{KFHE.ct}/\mathsf{KFHE.ct}_\mathsf{C})$ *to* $\mathcal{A}$*.*

- **Challenge Query.** *$\mathcal{A}$ is allowed to make the query only once. Upon $\mathcal{A}$'s query on $(\mu_0^\star, \mu_1^\star)$ such that $|\mu_0^\star| = |\mu_1^\star|$, $\mathcal{C}$ samples* $\mathsf{coin} \leftarrow_R \{0,1\}$, *runs* $\mathsf{KFHE.ct}^\star \leftarrow \mathsf{KFHE.Enc}(\mathsf{KFHE.pk}, \mu^\star_{\mathsf{coin}})$, *creates a list of ciphertexts* $\mathcal{L} = \{\mathsf{KFHE.ct}^\star\}$, *and sends* $\mathsf{KFHE.ct}^\star$ *to* $\mathcal{A}$.

- **Phase 2.** *$\mathcal{A}$ is allowed to make the same three types of queries to $\mathcal{C}$ as in Phase 1 with the following exceptions.*

  – **Evaluation Query.** *If* $\{\mathsf{KFHE.ct}^{(\ell)}\}_{\ell\in[L]} \cap \mathcal{L} \neq \emptyset$ *holds and the evaluation result is not* $\perp$ *but* $\mathsf{KFHE.ct}_\mathsf{C}$, *$\mathcal{C}$ updates a list* $\mathcal{L} \leftarrow \mathcal{L} \cup \{\mathsf{KFHE.ct}_\mathsf{C}\}$.

  – **Decryption Query.** *Upon $\mathcal{A}$'s query on* $\mathsf{KFHE.ct}$, *$\mathcal{C}$ outputs $\perp$ if* $\mathsf{KFHE.ct} = \mathsf{KFHE.ct}^\star$ *holds.*

    Upon $\mathcal{A}$'s query on $\mathsf{KFHE.ct}_\mathsf{C}$, *$\mathcal{C}$ outputs $\perp$ if* $\mathsf{KFHE.ct}_\mathsf{C} \in \mathcal{L}$ *holds. $\mathcal{C}$ also outputs $\perp$ if $\mathcal{A}$ has already made a homomorphic evaluation key reveal query.*

- **Guess.** *$\mathcal{A}$ outputs* $\widehat{\mathsf{coin}} \in \{0,1\}$ *as a guess of* coin *and terminates the game.*

If the advantage of $\mathcal{A}$ for breaking the KH-CCA *security of* Π_{KFHE} *defined by* $\mathsf{Adv}^{\mathsf{KH\text{-}CCA}}_{\Pi_{\mathsf{KFHE}},\mathcal{A}}(\lambda) := \left|\Pr\left[\widehat{\mathsf{coin}} = \mathsf{coin}\right] - \frac{1}{2}\right|$ *is negligible in λ,* Π_{KFHE} *is said to satisfy the* KH-CCA *security.*

Remark 1. *If a pre-evaluated ciphertext* $\mathsf{KFHE.ct}$ *and an evaluated ciphertext* $\mathsf{KFHE.ct}_\mathsf{C}$ *follow the same distribution, we change the restriction of decryption queries in Phase 2:*

- **Decryption Query.** *Upon $\mathcal{A}$'s query on* $\mathsf{KFHE.ct}$, *$\mathcal{C}$ outputs $\perp$ if* $\mathsf{KFHE.ct} \in \mathcal{L}$ *holds. Otherwise, $\mathcal{C}$ proceeds the same way as in Phase 1.*

Specifically, in Definition 4, the adversary is allowed to make a decryption query on a pre-evaluated ciphertext $\mathsf{KFHE.ct} \neq \mathsf{KFHE.ct}^\star$. *When a pre-evaluated ciphertext* $\mathsf{KFHE.ct}$ *and an evaluated ciphertext* $\mathsf{KFHE.ct}_\mathsf{C}$ *follow the same distribution, we have to prohibit such queries since the queried* $\mathsf{KFHE.ct}$ *may be an evaluation result of* $\mathsf{KFHE.ct}^\star$ *by* $\mathsf{KFHE.hk}$.

2.2 Attribute-based Keyed (Fully) Homomorphic Encryption

We define attribute-based keyed fully homomorphic encryption (ABKFHE).

Definition 5. *An attribute-based keyed fully homomorphic encryption (*ABKFHE*) scheme for a predicate* $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ *consists of five polynomial-time algorithms* $\Pi_{\mathsf{ABKFHE}} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$: *For a security parameter λ, let* $\mathcal{M} = \mathcal{M}(\lambda)$ *denote a message space.*

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$: *On input the security parameter 1^λ, it outputs a master public/secret key pair* $(\mathsf{mpk}, \mathsf{msk})$.

- $\mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y) \to (\mathsf{dk}_y, \mathsf{hk}_y)$: *On input a* mpk, msk, *and a key attribute* $y \in \mathcal{Y}$, *it outputs a decryption key* dk_y *and a homomorphic evaluation key* hk_y *for y.*

- $\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x$: *On input a* mpk, *a ciphertext attribute* $x \in \mathcal{X}$, *and a message* $\mu \in \mathcal{M}$, *it outputs a pre-evaluated ciphertext* ct_x *for x.*

- $\mathsf{Eval}(\mathsf{mpk}, \mathsf{hk}_y, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell\in[L]}, \mathsf{C}) \to \mathsf{ct}_{\mathbf{x},\mathsf{C}}/\perp$: *On input a* mpk, hk_y *for y, a circuit* $\mathsf{C} : \mathcal{M}^L \to \mathcal{M}$, *and a tuple of L ciphertexts* $(\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell\in[L]}$, *it outputs an evaluated ciphertext* $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$ *for* $\mathbf{x} = (x^{(1)}, \ldots, x^{(\ell)})$ *or a rejection symbol $\perp$.*

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_y, \mathsf{ct}_x/\mathsf{ct}_{\mathbf{x},\mathsf{C}}) \to \mu/\perp$: *On input a* mpk, dk_y *and* $\mathsf{ct}_x/\mathsf{ct}_{\mathbf{x},\mathsf{C}}$, *it outputs a decryption result* $\mu \in \mathcal{M}$ *or a rejection symbol* $\perp$.

It is required that an Π_{ABKFHE} satisfies both correctness and compactness.

Definition 6 (Correctness). *For a vector of ciphertext attributes* $\mathbf{x} = (x_1, \ldots, x_L) \in \mathcal{X}^L$ *and a key attribute* $y \in \mathcal{Y}$, *we use the notation* $f(\mathbf{x}, y) = 1$ *if it holds that* $f(x_\ell, y) = 1$ *for all* $\ell \in [L]$. $\Pi_{\mathsf{ABKFHE}} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ *satisfies* correctness *if the following conditions hold with overwhelming probability:*

- *For every* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, $(x, y) \in \mathcal{X} \times \mathcal{Y}$ *such that* $f(x, y) = 1$, $(\mathsf{dk}_y, \mathsf{hk}_y) \leftarrow \mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y)$, *and* $\mu \in \mathcal{M}$, *it holds that* $\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_y, \mathsf{Enc}(\mathsf{mpk}, x, \mu)) = \mu$.

- *For every* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, $(\mathbf{x} = (x^{(1)}, \ldots, x^{(L)}), y, y') \in \mathcal{X}^L \times \mathcal{Y}^2$ *such that* $f(\mathbf{x}, y) = f(\mathbf{x}, y') = 1$, $(\mathsf{dk}_y, \mathsf{hk}_y) \leftarrow \mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y)$, $(\mathsf{dk}_{y'}, \mathsf{hk}_{y'}) \leftarrow \mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y')$, *circuit* $\mathsf{C} : \mathcal{M}^L \to \mathcal{M}$, *and* $(\mu^{(1)}, \ldots, \mu^{(L)}) \in \mathcal{M}^L$, *it holds that* $\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_y, \mathsf{ct}_{\mathbf{x},\mathsf{C}}) = \mathsf{C}(\mu^{(1)}, \ldots, \mu^{(L)})$ *with overwhelming probability, where* $\mathsf{ct}_{\mathbf{x},\mathsf{C}} \leftarrow \mathsf{Eval}(\mathsf{mpk}, \mathsf{hk}_{y'}, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell \in [L]}, \mathsf{C})$ *and* $\mathsf{ct}^{(\ell)}_{x^{(\ell)}} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^{(\ell)}, \mu^{(\ell)})$ *for every* $\ell \in [L]$.

Definition 7 (Compactness). $\Pi_{\mathsf{ABKFHE}} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ *satisfies* compactness *if there exists a polynomial* poly *such that* $|\mathsf{ct}_{\mathbf{x},\mathsf{C}}|$, *where* $\mathsf{ct}_{\mathbf{x},\mathsf{C}} \leftarrow \mathsf{Eval}(\mathsf{mpk}, \mathsf{hk}_y, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell \in [L]}, \mathsf{C})$, *is independent of the size and depth of* C *and at most* $L \cdot \mathsf{poly}(\lambda)$ *for every security parameter* λ.

Remark 2. *An attribute-based keyed homomorphic encryption (*ABKHE*) scheme* $\Pi_{\mathsf{ABKHE}} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ *is defined in the same way except the* Eval *algorithm in two points. At first, since we will construct a fully compact* ABKHE *scheme* Π_{ABKHE} *in the sense that a pre-evaluated ciphertext* ct_x *and an evaluated ciphertext* $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$ *follow the same distribution,* $\mathsf{ct}^{(1)}_{x^{(1)}}, \ldots, \mathsf{ct}^{(L)}_{x^{(L)}}$ *which are inputs of* Eval *satisfy* $x = x^{(1)} = \cdots = x^{(L)}$. *Next, since we will construct an* ABKHE *scheme* Π_{ABKHE} *with multiplicative homomorphism,* Eval *does not take a circuit* C *as input. The correctness ensures that a decryption result of* $\mathsf{ct}_x \leftarrow \mathsf{Eval}(\mathsf{mpk}, \mathsf{hk}_y, (\mathsf{ct}^{(\ell)}_x)_{\ell \in [L]})$ *is a product of decryption results of* $\mathsf{ct}^{(\ell)}_x$.

We define the KH-CCA security for ABKFHE by following Definition 4.

Definition 8 (KH-CCA security). *The adaptive* KH-CCA *security of* $\Pi_{\mathsf{ABKFHE}} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ *is defined by the security game between a challenger* $\mathcal{C}$ *and an adversary* $\mathcal{A}$ *as follows.*

- **Init.** $\mathcal{C}$ *runs* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ *and sends* mpk *to* $\mathcal{A}$.

- **Phase 1.** $\mathcal{A}$ *is allowed to make the following four types of queries to* $\mathcal{C}$.

  – **Decryption Key Reveal Query.** *Upon* $\mathcal{A}$*'s query on* $y \in \mathcal{Y}$, $\mathcal{C}$ *runs* $(\mathsf{dk}_y, \mathsf{hk}_y) \leftarrow \mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y)$ *and sends* dk_y *to* $\mathcal{A}$.

  – **Homomorphic Evaluation Key Reveal Query.** *Upon* $\mathcal{A}$*'s query on* $y \in \mathcal{Y}$, $\mathcal{C}$ *runs* $(\mathsf{dk}_y, \mathsf{hk}_y) \leftarrow \mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y)$ *and sends* hk_y *to* $\mathcal{A}$.

  – **Evaluation Query.** *Upon* $\mathcal{A}$*'s query on* $(y, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell \in [L]}, \mathsf{C})$, $\mathcal{C}$ *runs* $(\mathsf{dk}_y, \mathsf{hk}_y) \leftarrow \mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y)$ *and sends the result of* $\mathsf{Eval}(\mathsf{mpk}, \mathsf{hk}_y, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell \in [L]}, \mathsf{C})$ *to* $\mathcal{A}$.

  – **Decryption Query.** *Upon* $\mathcal{A}$*'s query on* $(y, \mathsf{ct}_x/\mathsf{ct}_{\mathbf{x},\mathsf{C}})$, $\mathcal{C}$ *runs* $(\mathsf{dk}_y, \mathsf{hk}_y) \leftarrow \mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y)$ *and sends the result of* $\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_y, \mathsf{ct}_x/\mathsf{ct}_{\mathbf{x},\mathsf{C}})$ *to* $\mathcal{A}$.

- **Challenge Query.** *$\mathcal{A}$ is allowed to make the query only once. Upon $\mathcal{A}$'s query on $(x^\star, \mu_0^\star, \mu_1^\star)$ such that $|\mu_0^\star| = |\mu_1^\star|$, $\mathcal{C}$ outputs $\perp$ if $\mathcal{A}$ has already made a decryption key reveal query on y such that $f(x^\star, y) = 1$. Otherwise, $\mathcal{C}$ samples* $\mathsf{coin} \leftarrow_R \{0,1\}$, *runs* $\mathsf{ct}_{x^\star}^\star \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^\star, \mu_{\mathsf{coin}}^\star)$, *creates a list of ciphertexts* $\mathcal{L} = \{\mathsf{ct}_{x^\star}^\star\}$, *and sends* $\mathsf{ct}_{x^\star}^\star$ *to* $\mathcal{A}$.

- **Phase 2.** *$\mathcal{A}$ is allowed to make the same four types of queries to $\mathcal{C}$ as in Phase 1 with the following exceptions.*

  – **Decryption Key Reveal Query.** *Upon $\mathcal{A}$'s query on $y \in \mathcal{Y}$, $\mathcal{C}$ outputs $\perp$ if $f(x^\star, y) = 1$ holds.*

  – **Evaluation Query.** *If $\{\mathsf{ct}_{x^{(\ell)}}^{(\ell)}\}_{\ell \in [L]} \cap \mathcal{L} \neq \emptyset$ holds and the evaluation result is not $\perp$ but* $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$, *$\mathcal{C}$ updates a list* $\mathcal{L} \leftarrow \mathcal{L} \cup \{\mathsf{ct}_{\mathbf{x},\mathsf{C}}\}$.

  – **Decryption Query.** *Upon $\mathcal{A}$'s query on (y, ct_x), $\mathcal{C}$ outputs $\perp$ if $\mathsf{ct}_x = \mathsf{ct}_{x^\star}^\star$ holds.*
  Upon $\mathcal{A}$'s query on $(y, \mathsf{ct}_{\mathbf{x},\mathsf{C}})$, $\mathcal{C}$ outputs $\perp$ if $\mathsf{ct}_{\mathbf{x},\mathsf{C}} \in \mathcal{L}$ holds. $\mathcal{C}$ also outputs $\perp$ if $f(x^\star, y) = 1$ holds and $\mathcal{A}$ has already made a homomorphic evaluation key reveal query on y' such that $f(x^\star, y') = 1$.

- **Guess.** *$\mathcal{A}$ outputs* $\widehat{\mathsf{coin}} \in \{0,1\}$ *as a guess of* coin *and terminates the game.*

If the advantage of $\mathcal{A}$ for breaking the $\mathsf{KH\text{-}CCA}$ *security of* Π_{ABKFHE} *defined by* $\mathsf{Adv}_{\Pi_{\mathsf{ABKFHE}},\mathcal{A}}^{\mathsf{KH\text{-}CCA}}(\lambda) := \left|\Pr\left[\widehat{\mathsf{coin}} = \mathsf{coin}\right] - \frac{1}{2}\right|$ *is negligible in λ,* Π_{ABKFHE} *is said to satisfy the adaptive* $\mathsf{KH\text{-}CCA}$ *security. The* selective $\mathsf{KH\text{-}CCA}$ *security is the same except that $\mathcal{A}$ declares $x^\star$ at the beginning of the security game.*

Remark 3. *Since a pre-evaluated ciphertext and an evaluated ciphertext of* ABKHE *follow the same distribution as we claimed in Remark 2, we change the restriction of decryption queries in Phase 2 as we claimed in Remark 1:*

- **Decryption Query.** *Upon $\mathcal{A}$'s query on (y, ct_x), $\mathcal{C}$ outputs $\perp$ if $\mathsf{ct}_x \in \mathcal{L}$ holds. $\mathcal{C}$ also outputs $\perp$ if $f(x^\star, y) = 1$ holds and $\mathcal{A}$ has already made a homomorphic evaluation key reveal query on y' such that $f(x^\star, y') = 1$. Otherwise, $\mathcal{C}$ proceeds the same way as in Phase 1.*

3 Generic Construction of ABKFHE

In this section, we propose a generic construction of ABKFHE scheme Π_{ABKFHE}. In Section 3.2, we provide a construction of Π_{ABKFHE}. In Section 3.3, we prove the selective KH-CCA security. In advance, we summarize cryptographic primitives which we will use to construct Π_{ABKFHE}.

Delegatable ABE (DABE). Let $\Pi_{\mathsf{DABE}} = (\mathsf{DABE.Setup}, \mathsf{DABE.KGen}, \mathsf{DABE.Enc}, \mathsf{DABE.Dec})$ denote a DABE scheme for a predicate $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ with a three-level hierarchical structure, where ciphertext attributes live in $\mathcal{X} \times \{0,1\} \times \mathcal{ID}$, while key attributes live in either $\mathcal{Y} \times \{0,1\}$ or $\mathcal{Y} \times \{0,1\} \times \mathcal{ID}$. A ciphertext $\mathsf{DABE.ct}_{(x,b,\mathsf{id})}$ for (x, b, id) can be decrypted by a secret key $\mathsf{DABE.sk}_{(y,b',\mathsf{id}')}$ for (y, b', id') iff $f(x,y) = 1 \wedge b = b' \wedge \mathsf{id} = \mathsf{id}'$, while $\mathsf{DABE.sk}_{(y,b',\mathsf{id}')}$ can be computed from $\mathsf{DABE.sk}_{(y,b')}$ for (y, b').

- $\mathsf{DABE.Setup}(1^\lambda) \to (\mathsf{DABE.mpk}, \mathsf{DABE.msk})$: On input the security parameter 1^λ, it outputs a master public/secret key pair $(\mathsf{DABE.mpk}, \mathsf{DABE.msk})$. Although we do not explicitly describe, the following algorithms take $\mathsf{DABE.mpk}$ as input.

- $\mathsf{DABE.Enc}(X, \mu) \to \mathsf{DABE.ct}_X$: On input a ciphertext attribute X and a message μ, it outputs a ciphertext $\mathsf{DABE.ct}_X$ for X.

- $\mathsf{DABE.KGen}(\mathsf{DABE.sk}_Y, Y') \to \mathsf{DABE.sk}_{Y'}$: On input a secret key $\mathsf{DABE.sk}_Y$ for a key attribute Y and another key attribute Y', it outputs a secret key $\mathsf{DABE.sk}_{Y'}$ for Y'.

- $\mathsf{DABE.Dec}(\mathsf{DABE.sk}_Y, \mathsf{DABE.ct}_X) \to \mu/\perp$: On input $\mathsf{DABE.sk}_Y$ and $\mathsf{DABE.ct}_X$, it outputs a decryption result μ or a failure symbol $\perp$.

We define two security notions called *selective* IND-CPA *security* and *third-level adaptive* OW-CPA *security*. The selective IND-CPA security follows the traditional definition of IND-CPA security, where the adversary declares the target ciphertext attribute $(x^\star, b^\star, \mathsf{id}^\star)$ at the beginning of the security game. The third-level adaptive OW-CPA security follows the traditional definition of the OW-CPA security, where the adversary declares the first and second level of the target ciphertext attribute $(x^\star, b^\star)$ at the beginning of the security game and declares the third level $\mathsf{id}^\star$ in the challenge phase.

We can easily construct DABE schemes satisfying the selective IND-CPA security and the third-level adaptive OW-CPA security under the LWE assumption. Specifically, we encode the first, second, and third levels using selectively secure Boneh et al.'s ABE scheme for circuits [BGG+14], selectively secure Agrawal et al.'s IBE scheme [ABB10], and adaptively secure IBE scheme such as Yamada's scheme [Yam17].

Multi-Key FHE (MFHE). An MFHE scheme consists of five polynomial-time algorithms $\Pi_{\mathsf{MFHE}} = (\mathsf{MFHE.Setup}, \mathsf{MFHE.KGen}, \mathsf{MFHE.Enc}, \mathsf{MFHE.Dec}, \mathsf{MFHE.Eval})$ defined as follows.

- $\mathsf{MFHE.Setup}(1^\lambda) \to \mathsf{MFHE.pp}$: On input the security parameter 1^λ, it outputs a public parameter $\mathsf{MFHE.pp}$. Although we do not explicitly describe, the following algorithms take $\mathsf{MFHE.pp}$ as input.

- $\mathsf{MFHE.KGen} \to (\mathsf{MFHE.pk}, \mathsf{MFHE.sk})$: It outputs a public/secret key pair $(\mathsf{MFHE.pk}, \mathsf{MFHE.sk})$.

- $\mathsf{MFHE.Enc}(\mathsf{MFHE.pk}, \mu) \to \mathsf{MFHE.ct}$: On input $\mathsf{MFHE.pk}$ and a message μ, it outputs a pre-evaluated ciphertext $\mathsf{MFHE.ct}$.

- $\mathsf{MFHE.Dec}(\mathsf{MFHE.sk}, \mathsf{MFHE.ct}) \to \mu/\perp$: On input a secret key $\mathsf{MFHE.sk}$ and a pre-evaluated ciphertext $\mathsf{MFHE.ct}$, it outputs a decryption result μ or a failure symbol $\perp$.

- $\mathsf{MFHE.Eval}((\mathsf{MFHE.pk}^{(\ell)}, \mathsf{MFHE.ct}^{(\ell)})_{\ell \in [L]}, \mathsf{C}) \to \mathsf{MFHE.ct}_\mathsf{C}$: On input L public key/ciphertext pairs $(\mathsf{MFHE.pk}^{(\ell)}, \mathsf{MFHE.ct}^{(\ell)})_{\ell \in [L]}$ and a circuit C, it outputs an evaluated ciphertext $\mathsf{MFHE.ct}_\mathsf{C}$.

- $\mathsf{MFHE.Dec}((\mathsf{MFHE.sk}^{(\ell)})_{\ell \in [L]}, \mathsf{MFHE.ct}_\mathsf{C}) \to \mu/\perp$: On input L secret keys $(\mathsf{MFHE.sk}^{(\ell)})_{\ell \in [L]}$ and an evaluated ciphertext $\mathsf{MFHE.ct}_\mathsf{C}$, it outputs a decryption result μ or a failure symbol $\perp$.

We will use the traditional IND-CPA security of MFHE, where the PPT adversary cannot detect whether the challenge ciphertext $\mathsf{MFHE.ct}^\star$ is an encryption of a random message or that of $\mu^\star$ which the adversary declared.

One-time Signature (OTS). A OTS scheme consists of three polynomial-time algorithms $\Pi_{\mathsf{OTS}} = (\mathsf{OTS.KGen}, \mathsf{OTS.Sign}, \mathsf{OTS.Ver})$ defined as follows.

- $\mathsf{OTS.KGen}(1^\lambda) \to (\mathsf{sigk}, \mathsf{vk})$: On input the security parameter 1^λ, it outputs a signing/verification key pair $(\mathsf{sigk}, \mathsf{vk})$.

- $\mathsf{Sign}(\mathsf{sigk}, \mu) \to \sigma$: On input sigk and a message μ, it outputs a signature σ.

- $\mathsf{OTS.Ver}(\mathsf{vk}, \sigma, \mu) \to 0/1$: On input vk, σ, and μ, it outputs 0 which indicates "reject" or 1 which indicates "accept".

The correctness of OTS ensures that the output of $\mathsf{OTS.Ver}$ is 1 with overwhelming probability if σ was correctly created by the Sign algorithm. The strong unforgeability of OTS ensures that given vk output by $\mathsf{OTS.KGen}$, any PPT adversary cannot create a new message/signature pair (μ, σ) which is verified as "accept" by vk if it can make a signature generation query only once.

3.1 Technical Overview: Case of IBKFHE

We explain an overview of Π_{IBKFHE} based on MFHE scheme Π_{MFHE}, hierarchical IBE (HIBE) scheme Π_{HIBE}, a collision-resistant hash function H, and a one-time signature (OTS) scheme Π_{OTS}.

CCA1*-secure* FHE *Scheme.* We start the overview from Canetti et al.'s CCA1-secure FHE scheme Π_{FHE} [CRRV17] based on Brakerski et al.'s generic construction of IBFHE [BCTW16] from MFHE and IBE. The CCA1-secure FHE scheme Π_{FHE} has $\mathsf{FHE.pk} = (\mathsf{MFHE.pp}, \mathsf{IBE.mpk})$ and $\mathsf{FHE.sk} = \mathsf{IBE.msk}$. To encrypt a message μ, an encryptor runs the key generation algorithm of MFHE; $(\mathsf{MFHE.pk}, \mathsf{MFHE.sk}) \leftarrow \mathsf{MFHE.KGen}(\mathsf{MFHE.pp})$, samples a random identity $\mathsf{rid} \leftarrow_R \mathcal{ID}$, and computes a pre-evaluated ciphertext;

$$\mathsf{FHE.ct} = (\mathsf{rid}, \mathsf{MFHE.pk}, \mathsf{IBE.ct}_{\mathsf{rid}}, \mathsf{MFHE.ct}),$$

where $\mathsf{IBE.ct}_{\mathsf{rid}}$ and $\mathsf{MFHE.ct}$ are encryptions of $\mathsf{MFHE.sk}$ and μ, respectively. To decrypt a pre-evaluated FHE ciphertext $\mathsf{FHE.ct}$, a decryptor computes an IBE secret key $\mathsf{IBE.sk}_{\mathsf{rid}}$ by using $\mathsf{FHE.sk} = \mathsf{IBE.msk}$, recovers an MFHE secret key $\mathsf{MFHE.sk}$ by decrypting $\mathsf{IBE.ct}_{\mathsf{rid}}$ using $\mathsf{IBE.sk}_{\mathsf{rid}}$, and recovers a message μ by decrypting $\mathsf{MFHE.ct}$ using $\mathsf{MFHE.sk}$. To evaluate L pre-evaluated ciphertexts $(\mathsf{FHE.ct}^{(\ell)} = (\mathsf{rid}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{IBE.ct}^{(\ell)}_{\mathsf{rid}^{(\ell)}}, \mathsf{MFHE.ct}^{(\ell)}))_{\ell\in[L]}$ for a circuit C, where $\mathsf{IBE.ct}^{(\ell)}_{\mathsf{rid}^{(\ell)}}$ and $\mathsf{MFHE.ct}^{(\ell)}$ are encryptions of $\mathsf{MFHE.sk}^{(\ell)}$ and $\mu^{(\ell)}$, respectively, an evaluator computes $\mathsf{MFHE.ct}_{\mathsf{C}}$ which is an MFHE evaluated ciphertext of $(\mathsf{MFHE.ct}^{(\ell)})_{\ell\in[L]}$ for C and outputs

$$\mathsf{FHE.ct}_{\mathsf{C}} = \left((\mathsf{rid}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{IBE.ct}^{(\ell)}_{\mathsf{rid}^{(\ell)}})_{\ell\in[L]}, \mathsf{MFHE.}\ \mathsf{C}\right).$$

To decrypt an evaluated FHE ciphertext $\mathsf{FHE.ct}_{\mathsf{C}}$, a decryptor computes IBE secret keys $\mathsf{IBE.sk}^{(\ell)}_{\mathsf{rid}^{(\ell)}}$ by using $\mathsf{FHE.sk} = \mathsf{IBE.msk}$ and recovers MFHE secret keys $\mathsf{MFHE.sk}^{(\ell)}$ by decrypting $\mathsf{IBE.ct}^{(\ell)}_{\mathsf{rid}^{(\ell)}}$ using $\mathsf{IBE.sk}^{(\ell)}_{\mathsf{rid}^{(\ell)}}$ for $\ell \in [L]$, and recovers a message $\mathsf{C}((\mu^{(\ell)})_{\ell\in[L]})$ by decrypting $\mathsf{MFHE.ct}_{\mathsf{C}}$ using $(\mathsf{MFHE.sk}^{(\ell)})_{\ell\in[L]}$.

Let $\mathsf{FHE.ct}^\star = (\mathsf{rid}^\star, \mathsf{MFHE.pk}^\star, \mathsf{IBE.ct}^\star_{\mathsf{rid}^\star}, \mathsf{MFHE.ct}^\star)$ be the challenge ciphertext. The CCA1 security of the FHE scheme Π_{FHE} follows from the CPA security of Π_{MFHE} and Π_{IBE}. In particular, we first use the CPA security of IBE to ensure that $\mathsf{IBE.ct}^\star_{\mathsf{rid}^\star}$ is indistinguishable from an encryption of a random string, then the CPA security of MFHE ensures that $\mathsf{MFHE.ct}^\star$ is indistinguishable from an encryption of a random string. We briefly explain the first reduction. In Phase 1, $\mathcal{A}$ does not know $\mathsf{rid}^\star$ sampled by $\mathcal{C}$ uniformly from an exponentially large space $\mathcal{ID}$. Thus, all ciphertexts $\mathsf{FHE.ct} = (\mathsf{rid}, \mathsf{MFHE.pk}, \mathsf{IBE.ct}_{\mathsf{rid}}, \mathsf{MFHE.ct})$ on which the CCA1 adversary $\mathcal{A}$ makes decryption queries satisfy $\mathsf{rid} \neq \mathsf{rid}^\star$. Therefore, the reduction algorithm of IBE can answer all decryption queries. In contrast, the FHE scheme Π_{FHE} does not satisfy the $\mathsf{CCA2}$ security since the $\mathsf{CCA2}$ adversary $\mathcal{A}$ can make a decryption query on $\mathsf{FHE.ct} = (\mathsf{MFHE.pk}, \mathsf{IBE.ct}_{\mathsf{rid}}, \mathsf{MFHE.ct})$ such that $\mathsf{rid} = \mathsf{rid}^\star$ in Phase 2.

KH-CCA-*secure* KFHE. By modifying Π_{FHE}, we construct the first KFHE scheme Π_{KFHE} whose KH-CCA security is based solely on the LWE assumption. At first, we apply the CHK transform [CHK04] to pre-evaluated ciphertexts so that Π_{KFHE} satisfies the $\mathsf{CCA2}$ security against an adversary without hk. Then, we have

$$\mathsf{KFHE.ct} = (\mathsf{rid}, \mathsf{vk}, \mathsf{MFHE.pk}, \mathsf{IBE.ct}_{\mathsf{rid}\|\mathsf{vk}}, \mathsf{MFHE.ct}, \sigma),$$

where a random identity rid is replaced by a concatenation of rid and a verification key vk of Π_{OTS}, and σ is a signature for a message $(\mathsf{rid}, \mathsf{vk}, \mathsf{MFHE.pk}, \mathsf{IBE.ct}_{\mathsf{rid}\|\mathsf{vk}}, \mathsf{MFHE.ct})$. To evaluate L pre-evaluated ciphertexts $(\mathsf{KFHE.ct}^{(\ell)} = (\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{IBE.ct}^{(\ell)}_{\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)}}, \mathsf{MFHE.ct}^{(\ell)}, \sigma^{(\ell)}))_{\ell\in[L]}$, we discard signatures[1] $\left(\sigma^{(\ell)}\right)_{\ell\in[L]}$, apply the evaluation algorithm of Π_{FHE}, and obtain $\mathsf{KFHE.ct}_{\mathsf{C}} = \left((\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{IBE.ct}^{(\ell)}_{\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)}})_{\ell\in[L]}, \mathsf{MFHE.ct}_{\mathsf{C}}\right)$ which is the same as $\mathsf{FHE.ct}_{\mathsf{C}}$ except the existence of $\mathsf{vk}^{(\ell)}$. As the case of $\mathsf{FHE.ct}_{\mathsf{C}}$, $\mathsf{rid}^{(\ell)}$ enables the reduction algorithm of IBE to answer all decryption queries.[2]

Since we do not introduce a homomorphic evaluation key hk, the current scheme is insecure. What we have achieved so far is that the CHK transform ensures that the pre-evaluated ciphertexts $\mathsf{KFHE.ct}$ satisfy the $\mathsf{CCA2}$ security as long as it cannot be evaluated, while the $\mathsf{CCA1}$ security of Π_{FHE} ensures that the evaluated ciphertexts satisfy the $\mathsf{CCA1}$ security. Thus, we design an evaluation algorithm and a homomorphic evaluation key hk so that pre-evaluated ciphertexts cannot be evaluated without hk and evaluated ciphertexts satisfy the $\mathsf{CCA2}$ security against an adversary without hk. In other words, we only have to focus on an adversary without hk. To this end, although KFHE itself is a public key primitive, the treatment of hk is similar to a symmetric key primitive. Therefore, we use a simple encrypt-then-MAC paradigm [BN08] for constructing a $\mathsf{CCA2}$-secure symmetric key encryption scheme to design Π_{KFHE}. We set hk as a secret key of MAC and an evaluated ciphertext becomes

$$\mathsf{KFHE.ct}_{\mathsf{C}} = \left((\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{IBE.ct}^{(\ell)}_{\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)}})_{\ell\in[L]}, \mathsf{MFHE.ct}_{\mathsf{C}}, \sigma\right),$$

where σ is a MAC of a message $((\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{IBE.ct}^{(\ell)}_{\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)}})_{\ell\in[L]}, \mathsf{MFHE.ct}_{\mathsf{C}})$. The decryption key dk consists of $\mathsf{IBE.msk}$ and the secret key of MAC. A decryptor first checks the validity of σ and recovers a message $\mathsf{C}((\mu^{(\ell)})_{\ell\in[L]})$ in the same way as $\mathsf{FHE.ct}_{\mathsf{C}}$. Since the security of MAC ensures that an adversary without hk cannot evaluate ciphertexts by itself, Π_{KFHE} satisfies the $\mathsf{CCA2}$ security against the adversary. Thus, Π_{KFHE} achieves the KH-CCA security.

KH-CCA-*secure* IBKFHE. Due to the simplicity of the above KFHE scheme, we can immediately obtain a KH-CCA-secure IBKFHE scheme Π_{IBKFHE}. To capture identity-based setting, we replace IBE of Π_{KFHE} by HIBE. Similarly, we also replace MAC with an identity-based signature scheme, where HIBE is sufficient for the purpose due to the Naor transform. We use one three-level HIBE

[1] Since there are no $\mathsf{MFHE.ct}^{(1)}, \ldots, \mathsf{MFHE.ct}^{(L)}$ in an evaluated ciphertext, the signatures $\left(\sigma^{(\ell)}\right)_{\ell\in[L]}$ are useless in the sense that we cannot verify them.

[2] If we can assume that the adversary cannot guess $\mathsf{vk}^\star$ which is a component of the challenge ciphertext, the scheme does not require a random identity rid; however, OTS schemes Π_{OTS} do not satisfy the condition in general.

scheme Π_{HIBE} to perform the two tasks simultaneously and construct Π_{IBKFHE}. For an identity id, we set a decryption key $\mathsf{IBKFHE.dk}_{\mathsf{id}} = \mathsf{HIBE.sk}_{(\mathsf{id},0)}$, a homomorphic evaluation key $\mathsf{IBKFHE.hk}_{\mathsf{id}} = \mathsf{HIBE.sk}_{(\mathsf{id},1)}$, a pre-evaluated ciphertext

$$\mathsf{IBKFHE.ct}_{\mathsf{id}} = (\mathsf{rid}, \mathsf{vk}, \mathsf{MFHE.pk}, \mathsf{HIBE.ct}_{(\mathsf{id},0,\mathsf{rid}\|\mathsf{vk})}, \mathsf{MFHE.ct}, \sigma),$$

where $\mathsf{HIBE.ct}_{(\mathsf{id},0,\mathsf{rid}\|\mathsf{vk})}$ and $\mathsf{MFHE.ct}$ are encryptions of $\mathsf{MFHE.sk}$ and μ, respectively, and an evaluated ciphertext

$$\mathsf{IBKFHE.ct}_{\mathsf{id},\mathsf{C}} = \begin{pmatrix} (\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{HIBE.ct}^{(\ell)}_{(\mathsf{id},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})})_{\ell\in[L]} \\ \mathsf{MFHE.ct}_{\mathsf{C}}, \mathsf{HIBE.sk}_{(\mathsf{id},1,h)} \end{pmatrix},$$

where h is a hash value of $((\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{HIBE.ct}^{(\ell)}_{(\mathsf{id},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})})_{\ell\in[L]}, \mathsf{MFHE.ct})$ and $\mathsf{HIBE.sk}_{(\mathsf{id},1,h)}$ plays a role of id's signature for the message h. The $\mathsf{KH\text{-}CCA}$ security of Π_{IBKFHE} follows from the similar discussion as the case of Π_{KFHE}.

3.2 Construction

We construct an ABKFHE scheme Π_{ABKFHE}. Let $\mathcal{ID}$ denote an identity space for the third-level of Π_{DABE} and let $\mathcal{RID}$ denote an exponentially large space from which an encryptor samples random identities rid, where it holds that $\mathsf{rid}\|\mathsf{vk} \in \mathcal{ID}$ for $\mathsf{rid} \leftarrow_R \mathcal{RID}$ and $(\mathsf{vk}, \mathsf{sigk}) \leftarrow \mathsf{OTS.KGen}(1^\lambda)$.

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$: Run $\mathsf{MFHE.pp} \leftarrow \mathsf{MFHE.Setup}(1^\lambda)$ and $(\mathsf{DABE.mpk}, \mathsf{DABE.msk}) \leftarrow \mathsf{DABE.Setup}(1^\lambda)$. Choose a one-time signature scheme Π_{OTS} and a collision-resistant hash function $H : \{0,1\}^* \to \mathcal{ID}$. Output $\mathsf{mpk} = (\mathsf{MFHE.pp}, \mathsf{DABE.mpk}, \Pi_{\mathsf{OTS}}, H)$ and $\mathsf{msk} = \mathsf{DABE.msk}$.

- $\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x$: Parse $\mathsf{mpk} = (\mathsf{MFHE.pp}, \mathsf{DABE.mpk}, \Pi_{\mathsf{OTS}}, H)$. Sample a random identity $\mathsf{rid} \leftarrow_R \mathcal{RID}$ and run

  - $(\mathsf{MFHE.pk}, \mathsf{MFHE.sk}) \leftarrow \mathsf{MFHE.KGen}(1^\lambda)$,
  - $\mathsf{MFHE.ct} \leftarrow \mathsf{MFHE.Enc}(\mathsf{MFHE.pk}, \mu)$,
  - $(\mathsf{vk}, \mathsf{sigk}) \leftarrow \mathsf{OTS.KGen}(1^\lambda)$,
  - $\mathsf{DABE.ct}_{(x,0,\mathsf{rid}\|\mathsf{vk})} \leftarrow \mathsf{DABE.Enc}((x, 0, \mathsf{rid}\|\mathsf{vk}), \mathsf{MFHE.sk})$,
  - $\sigma \leftarrow \mathsf{Sign}\left(\mathsf{sigk}, (\mathsf{rid}, \mathsf{vk}, \mathsf{MFHE.pk}, \mathsf{DABE.ct}_{(x,0,\mathsf{rid}\|\mathsf{vk})}, \mathsf{MFHE.ct})\right)$.

  Output

  $$\mathsf{ct}_x = (\mathsf{rid}, \mathsf{vk}, \mathsf{MFHE.pk}, \mathsf{DABE.ct}_{(x,0,\mathsf{rid}\|\mathsf{vk})}, \mathsf{MFHE.ct}, \sigma).$$

  We say that a pre-evaluated ciphertext ct_x is valid if σ is a valid signature for $(\mathsf{rid}, \mathsf{vk}, \mathsf{MFHE.pk}, \mathsf{DABE.ct}_{(x,0,\mathsf{rid}\|\mathsf{vk})}, \mathsf{MFHE.ct})$.

- $\mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y) \to (\mathsf{dk}_y, \mathsf{hk}_y)$: Pares $\mathsf{mpk} = (\mathsf{MFHE.pp}, \mathsf{DABE.mpk}, \Pi_{\mathsf{OTS}}, H)$ and $\mathsf{msk} = \mathsf{DABE.msk}$. Run

  - $\mathsf{DABE.sk}_{(y,0)} \leftarrow \mathsf{DABE.KGen}(\mathsf{DABE.msk}, (y, 0))$,
  - $\mathsf{DABE.sk}_{(y,1)} \leftarrow \mathsf{DABE.KGen}(\mathsf{DABE.msk}, (y, 1))$.

Output $\mathsf{dk}_y = \mathsf{DABE.sk}_{(y,0)}$ and $\mathsf{hk}_y = \mathsf{DABE.sk}_{(y,1)}$.

- $\mathsf{Eval}(\mathsf{mpk}, \mathsf{hk}_y, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell\in[L]}, \mathsf{C}) \to \mathsf{ct}_{\mathbf{x},\mathsf{C}}/\bot$: Output $\bot$ if $f(x,y) = 0$ holds or there are invalid ciphertexts $\mathsf{ct}^{(\ell)}_{x^{(\ell)}}$ for some $\ell \in [L]$. Otherwise, parse $\mathsf{mpk} = (\mathsf{MFHE.pp}, \mathsf{DABE.mpk}, \Pi_{\mathsf{OTS}}, H)$, $\mathsf{hk}_y = \mathsf{DABE.sk}_{(y,1)}$, and $\mathsf{ct}^{(\ell)}_{x^{(\ell)}} = (\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{DABE.ct}^{(\ell)}_{(x^{(\ell)},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})}, \mathsf{MFHE.ct}^{(\ell)}, \sigma^{(\ell)})$ for $\ell \in [L]$. Run
  - $\mathsf{MFHE.ct}_{\mathsf{C}} \leftarrow \mathsf{MFHE.Eval}((\mathsf{MFHE.pk}^{(\ell)}, \mathsf{MFHE.ct}^{(\ell)})_{\ell\in[L]}, \mathsf{C})$,
  - $\mathsf{DABE.sk}_{(y,1,h)} \leftarrow \mathsf{DABE.KGen}(\mathsf{DABE.sk}_{(y,1)}, (y,1,h))$,

  where $h = H((\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{DABE.ct}^{(\ell)}_{(x^{(\ell)},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})})_{\ell\in[L]}, \mathsf{MFHE.ct}_{\mathsf{C}})$. Output

$$\mathsf{ct}_{\mathbf{x},\mathsf{C}} = \begin{pmatrix} (\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{DABE.ct}^{(\ell)}_{(x^{(\ell)},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})})_{\ell\in[L]} \\ \mathsf{MFHE.ct}_{\mathsf{C}}, \mathsf{DABE.sk}_{(y,1,h)} \end{pmatrix}.$$

  We say that an evaluated ciphertext $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$ is valid if $f(\mathbf{x}, y) = 1$ holds and $\mathsf{DABE.sk}_{(y,1,h)}$ is a valid DABE secret key for $(y,1,h)$.

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_y, \mathsf{ct}_x/\mathsf{ct}_{\mathbf{x},\mathsf{C}}) \to \mu/\bot$: Parse $\mathsf{mpk} = (\mathsf{MFHE.pp}, \mathsf{DABE.mpk}, \Pi_{\mathsf{OTS}}, H)$ and $\mathsf{dk}_y = \mathsf{DABE.sk}_{(y,0)}$. Proceed as follows.
  - *Case of Pre-evaluated Ciphertexts.* Output $\bot$ if $f(x,y) = 0$ holds or ct_x is invalid. Otherwise, parse $\mathsf{ct}_x = (\mathsf{rid}, \mathsf{vk}, \mathsf{MFHE.pk}, \mathsf{DABE.ct}_{(x,0,\mathsf{rid}\|\mathsf{vk})}, \mathsf{MFHE.ct}, \sigma)$. Run
    * $\mathsf{DABE.sk}_{(y,0,\mathsf{rid}\|\mathsf{vk})} \leftarrow \mathsf{DABE.KGen}(\mathsf{DABE.sk}_{(y,0)}, (y,0,\mathsf{rid}\|\mathsf{vk}))$,
    * $\mathsf{MFHE.sk} \leftarrow \mathsf{DABE.Dec}(\mathsf{DABE.sk}_{(y,0,\mathsf{rid}\|\mathsf{vk})}, \mathsf{DABE.ct}_{(x,0,\mathsf{rid}\|\mathsf{vk})})$,

    and output $\mu \leftarrow \mathsf{MFHE.Dec}(\mathsf{MFHE.sk}, \mathsf{MFHE.ct})$.
  - *Case of Evaluated Ciphertexts.* Output $\bot$ if $f(\mathbf{x}, y) = 0$ holds or $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$ is invalid. Otherwise, parse $\mathsf{ct}_{\mathbf{x},\mathsf{C}} = ((\mathsf{rid}^{(\ell)}, \mathsf{vk}^{(\ell)}, \mathsf{MFHE.pk}^{(\ell)}, \mathsf{DABE.ct}^{(\ell)}_{(x^{(\ell)},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})})_{\ell\in[L]}, \mathsf{MFHE.ct}_{\mathsf{C}}, \mathsf{DABE.sk}_{(y',1,h)})$. For $\ell \in [L]$, run
    * $\mathsf{DABE.sk}_{(y,0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})} \leftarrow \mathsf{DABE.KGen}(\mathsf{DABE.sk}_{(y,0)}, (y,0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)}))$,
    * $\mathsf{MFHE.sk}^{(\ell)} \leftarrow \mathsf{DABE.Dec}(\mathsf{DABE.sk}_{(y,0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})}, \mathsf{DABE.ct}^{(\ell)}_{(x^{(\ell)},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})})$,

    and output $\mu \leftarrow \mathsf{MFHE.Dec}((\mathsf{MFHE.sk}^{(\ell)})_{\ell\in[L]}, \mathsf{MFHE.ct}_{\mathsf{C}})$.

Correctness. Although we skip the proof, Π_{ABKFHE} satisfies the correctness.

Theorem 1. *The proposed* ABKFHE *scheme* Π_{ABKFHE} *satisfies correctness if the underlying* MFHE *scheme* Π_{MFHE}*,* DABE *scheme* Π_{DABE}*, and one-time signature scheme* Π_{OTS} *satisfy correctness.*

3.3 Security

Theorem 2. *The proposed* ABKFHE *scheme* Π_{ABKFHE} *satisfies the selective* KH-CCA *security if the underlying* MFHE *scheme* Π_{MFHE} *satisfies the* IND-CPA *security,* DABE *scheme* Π_{DABE} *satisfies the selective* IND-CPA *security and the third level adaptive* OW-CPA *security,* OTS *scheme* Π_{OTS} *satisfies the strong unforgeability, and* H *satisfies the collision resistance.*

Proof. We prove the theorem by using a sequence of games $\mathsf{Game}_0, \cdots, \mathsf{Game}_5$.

- Game_0. This is the $\mathsf{KH\text{-}CCA}$ security game between the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$. Hereafter, let

  $$\mathsf{ct}^\star_{x^\star} = (\mathsf{rid}^\star, \mathsf{vk}^\star, \mathsf{MFHE.pk}^\star, \mathsf{DABE.ct}^\star_{(x^\star,0,\mathsf{rid}^\star\|\mathsf{vk}^\star)}, \mathsf{MFHE.ct}^\star, \sigma^\star)$$

  denote the challenge ciphertext, where $\mathsf{DABE.ct}^\star_{(x^\star,0,\mathsf{rid}^\star\|\mathsf{vk}^\star)}$ and $\mathsf{MFHE.ct}^\star$ are encryptions of $\mathsf{MFHE.sk}^\star$ and $\mu^\star_{\mathsf{coin}}$, respectively. Due to the definition of the $\mathsf{KH\text{-}CCA}$ security game, $\mathcal{C}$ stores the challenge ciphertext $\mathsf{ct}^\star_{x^\star}$ and its evaluation results in the list $\mathcal{L}$.

- Game_1. This is the same as Game_0 except that a collision does not occur for a hash function H among all ciphertexts that appeared in the security game.

  The collision resistance of H ensures that $\mathsf{Game}_0 \approx_c \mathsf{Game}_1$ holds.

- Game_2. This is the same as Game_1 except that upon $\mathcal{A}$'s evaluation queries and decryption queries on pre-evaluated ciphertexts $\mathsf{ct}_x = (\mathsf{vk}, \cdots)$ such that $\mathsf{vk} = \mathsf{vk}^\star$, $\mathcal{C}$ always outputs $\perp$ unless they are evaluation queries and $\mathsf{ct}_x = \mathsf{ct}^\star_{x^\star}$ holds.

  If it is a decryption query and $\mathsf{ct}_x = \mathsf{ct}^\star_{x^\star}$ holds, the definition of the $\mathsf{KH\text{-}CCA}$ security game ensures that $\mathcal{C}$ outputs $\perp$. The strong unforgeability of Π_{OTS} ensures that the adversary cannot create a signature σ that is verified accept by $\mathsf{vk}^\star$ unless $\mathsf{ct}_x = \mathsf{ct}^\star_{x^\star}$ holds. Thus, $\mathsf{Game}_1 \approx_c \mathsf{Game}_2$ holds.

- Game_3. This is the same as Game_2 except that upon $\mathcal{A}$'s decryption queries on $(y, \mathsf{ct}_{\mathbf{x},\mathsf{C}})$ for evaluated ciphertexts $\mathsf{ct}_{\mathbf{x},\mathsf{C}} = ((\cdots, \mathsf{DABE.ct}^{(\ell)}_{(x^{(\ell)},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})})_{\ell\in[L]}, \cdots, \mathsf{DABE.sk}_{(y',1,h')})$, $\mathcal{C}$ always outputs $\perp$ if there is $\ell \in [L]$ such that $(x^{(\ell)}, 0, \mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)}) = (x^\star, 0, \mathsf{rid}^\star\|\mathsf{vk}^\star)$.

  The change in Game_2 ensures that $\mathcal{A}$ does not make evaluation queries on pre-evaluated ciphertexts $\mathsf{ct}_x = (\mathsf{vk}, \cdots)$ such that $\mathsf{ct}_x \neq \mathsf{ct}^\star_{x^\star} \wedge \mathsf{vk} = \mathsf{vk}^\star$. Thus, if there is $\ell \in [L]$ such that $(x^{(\ell)}, 0, \mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)}) = (x^\star, 0, \mathsf{rid}^\star\|\mathsf{vk}^\star)$ upon $\mathcal{A}$'s decryption queries on $(y, \mathsf{ct}_{\mathbf{x},\mathsf{C}})$, it holds that $\mathsf{ct}_{\mathbf{x},\mathsf{C}} \in \mathcal{L}$ or the evaluated ciphertext $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$ is not $\mathcal{C}$'s answer of an evaluation query. Due to the definition of the $\mathsf{KH\text{-}CCA}$ security game, $\mathcal{C}$ outputs $\perp$ if $\mathsf{ct}_{\mathbf{x},\mathsf{C}} \in \mathcal{L}$ holds. Thus, we focus on the other case. Moreover, if $f(\mathbf{x}, y') = 0$ holds, $\mathcal{C}$ outputs $\perp$ since the evaluated ciphertext $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$ is invalid. Then, if $\mathbf{x}$ contains $x^\star$ and $\mathcal{C}$ does not output $\perp$, $f(x^\star, y') = 1$ is required to hold. Due to the definition of the $\mathsf{KH\text{-}CCA}$ security game, $\mathcal{A}$ can make the decryption queries only until $\mathcal{A}$ receives $\mathsf{hk}_{y'}$ such that $f(x^\star, y') = 1$. Summarizing the discussion so far, we prove $\mathsf{Game}_2 \approx_c \mathsf{Game}_3$ by showing the following stronger claim.

  > In Game_2, upon all $\mathcal{A}$'s decryption queries on $(y, \mathsf{ct}_{\mathbf{x},\mathsf{C}})$ for evaluated ciphertexts $\mathsf{ct}_{\mathbf{x},\mathsf{C}} = (\cdots, \mathsf{DABE.sk}_{(y',1,h')})$ such that $f(x^\star, y') = 1$, $\mathsf{DABE.sk}_{(y',1,h')}$ are not valid DABE secret keys for $(y', 1, h')$ unless $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$ were output by $\mathcal{C}$ as the answers of evaluation queries or $\mathcal{A}$ has received $\mathsf{hk}_{y'}$ such that $f(x^\star, y') = 1$.

  The claim ensures that upon all $\mathcal{A}$'s decryption queries on $(y, \mathsf{ct}_{\mathbf{x},\mathsf{C}})$ for evaluated ciphertexts $\mathsf{ct}_{\mathbf{x},\mathsf{C}} = ((\cdots, \mathsf{DABE.ct}^{(\ell)}_{(x^{(\ell)},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})})_{\ell\in[L]}, \cdots, \mathsf{DABE.sk}_{(y',1,h')})$, where there is $\ell \in [L]$ such that $\mathsf{DABE.ct}^{(\ell)}_{(x^{(\ell)},0,\mathsf{rid}^{(\ell)}\|\mathsf{vk}^{(\ell)})} = \mathsf{DABE.ct}_{(x^\star,0,\mathsf{rid}^\star\|\mathsf{vk}^\star)}$, the ciphertext is valid only when $\mathsf{ct}_{\mathbf{x},\mathsf{C}} \in \mathcal{L}$ holds or $\mathcal{A}$ is not allowed to make the decryption queries. As a result, $\mathcal{C}$ always outputs $\perp$ to answer the queries.

The third-level adaptive $\mathsf{OW\text{-}CPA}$ security of Π_{DABE} ensures the claim. Just after the reduction algorithm receives $x^\star$ from $\mathcal{A}$ at the beginning of the $\mathsf{KH\text{-}CCA}$ security game, it declares $(x^\star, 1)$ as the first and second levels of the target attribute. When $\mathcal{A}$ has not received $\mathsf{hk}_{y'}$ such that $f(x^\star, y') = 1$ and makes a decryption query on $(y, \mathsf{ct}_{\mathbf{x},\mathsf{C}})$ for evaluated ciphertexts $\mathsf{ct}_{\mathbf{x},\mathsf{C}} = (\cdots, \mathsf{DABE.sk}_{(y',1,h^\star)})$ such that $f(x^\star, y') = 1$, $\mathsf{DABE.sk}_{(y',1,h^\star)}$ is a valid DABE secret for $(y', 1, h^\star)$, and $\mathsf{ct}_{\mathbf{x},\mathsf{C}}$ was not output by the reduction algorithm as the answers of evaluation queries, the reduction algorithm declares $h^\star$ as the third level of the target attribute in the DABE security game. The reduction algorithm wins the DABE security game since it knows $\mathsf{DABE.sk}_{(y',1,h^\star)}$.

We check that the reduction algorithm can answer all $\mathcal{A}$'s queries. Since the reduction algorithm is allowed to receive $\mathsf{DABE.sk}_{(y,0)}$ for all y, it can answer all $\mathcal{A}$'s decryption key reveal queries and decryption queries. Since the change in Game_1 ensures that a collision does not occur for H, the reduction algorithm is allowed to receive $\mathsf{DABE.sk}_{(y',1,h')}$ for all y' to answer $\mathcal{A}$'s evaluation queries. Since it is sufficient to prove the above claim when $\mathcal{A}$ has not received $\mathsf{hk}_{y'}$ such that $f(x^\star, y') = 1$, all $\mathcal{A}$'s homomorphic evaluation key reveal queries on y' satisfies $f(x^\star, y') = 0$; thus, the reduction algorithm can answer all the queries. Thus, it holds that $\mathsf{Game}_2 \approx_c \mathsf{Game}_3$.

- Game_4. This is the same as Game_3 except that $\mathsf{DABE.ct}^\star_{(x^\star,0,\mathsf{rid}^\star\|\mathsf{vk}^\star)}$ is an encryption of a random string sampled independently from $\mathsf{MFHE.sk}^\star$.

  The selective $\mathsf{IND\text{-}CPA}$ security of the DABE scheme ensures that $\mathsf{Game}_3 \approx_c \mathsf{Game}_4$ holds. In short, the reduction algorithm samples $\mathsf{rid}^\star \leftarrow_R \mathcal{RID}$ and creates $\mathsf{vk}^\star$ at the beginning of the security game. After $\mathcal{A}$ declares the challenge attribute $x^\star$ in the $\mathsf{KH\text{-}CCA}$ security game, the reduction algorithm declares $(x^\star, 0, \mathsf{rid}^\star\|\mathsf{vk}^\star)$ as the challenge attribute of DABE security game. In the challenge phase, the reduction algorithm runs $(\mathsf{MFHE.pk}^\star, \mathsf{MFHE.sk}^\star) \leftarrow \mathsf{MFHE.KGen}(1^\lambda)$, samples a random string $\mu^\star$ whose length is the same as $\mathsf{MFHE.sk}^\star$ but the distribution is independent of $\mathsf{MFHE.sk}^\star$. Then, the reduction algorithm declares $(\mathsf{MFHE.sk}^\star, \mu^\star)$ as the challenge messages in the DABE security game and receives $\mathsf{DABE.ct}^\star_{(x^\star,0,\mathsf{rid}^\star\|\mathsf{vk}^\star)}$ from the DABE challenger. The reduction algorithm can create the other elements of the challenge ciphertext by itself.

  We check that the reduction algorithm does not use $\mathsf{DABE.sk}_{(y,0)}$ and $\mathsf{DABE.sk}_{(y,0,\mathsf{rid}^\star\|\mathsf{vk}^\star)}$ such that $f(x^\star, y) = 1$ to answer all $\mathcal{A}$'s queries. The reduction algorithm can answer all $\mathcal{A}$'s homomorphic evaluation key reveal queries and evaluation queries since it is allowed to receive $\mathsf{DABE.sk}_{(y',1)}$ for all y'. The definition of the $\mathsf{KH\text{-}CCA}$ security game ensures that $\mathcal{A}$ cannot receive $\mathsf{DABE.sk}_{(y,0)}$ such that $f(x^\star, y) = 1$ via the decryption key reveal queries. The definition of the $\mathsf{KH\text{-}CCA}$ security game ensures the reduction algorithm can answer $\perp$ upon $\mathcal{A}$'s decryption queries on $(y, \mathsf{ct}_x/\mathsf{ct}_{\mathbf{x},\mathsf{C}})$ such that $\mathsf{ct}_x/\mathsf{ct}_{\mathbf{x},\mathsf{C}} \in \mathcal{L}$. Thanks to the changes in Game_2 and Game_3, the reduction algorithm does not use $\mathsf{DABE.sk}_{(y,0,\mathsf{rid}^\star\|\mathsf{vk}^\star)}$ to answer all $\mathcal{A}$'s decryption queries. Thus, it holds that $\mathsf{Game}_3 \approx_c \mathsf{Game}_4$.

- Game_5. This is the same as Game_4 except that $\mathsf{MFHE.ct}^\star$ is independent of coin.

  Due to the change in Game_4, it is clear that the CPA security of MFHE ensures that $\mathsf{Game}_4 \approx_c \mathsf{Game}_5$ holds.

Thus, we complete the proof. □

4 Pairing-based Construction of ABKHE

In this section, we propose a pairing-based ABKHE scheme Π_{ABKHE} from a pair encoding scheme (PES). In Section 4.1, we review the definition of PES. In Section 4.3, we provide a construction of Π_{ABKHE}. In Section 4.4, we prove the security.

4.1 Pair Encoding Scheme

At first, we review the bilinear groups.

Bilinear Groups. We use $\mathcal{G}$ to denote a bilinear group generator which takes the security parameter 1^λ as input, and outputs $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$, where p is a $\Theta(\lambda)$-bit prime number, $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are cyclic groups of order p, g_1 and g_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficient non-degenerate bilinear map. Let 1_T denote the identity element of $\mathbb{G}_T$. For simplicity, let $\mathcal{G}(1^\lambda) := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$ denote the output of $\mathcal{G}(1^\lambda)$. For $a \in \mathbb{Z}_p$, we use the notation $[a]_1 := g_1^a \in \mathbb{G}_1$, $[a]_2 := g_2^a \in \mathbb{G}_2$, and $[a]_T := e(g_1, g_2)^a \in \mathbb{G}_T$. For a vector $\mathbf{a} := (a_1, \ldots, a_d) \in \mathbb{Z}_p^d$, we use the notation $[\mathbf{a}]_1 := ([a_1]_1, \ldots, [a_d]_1) \in \mathbb{G}_1^d$. Similarly, let $[\mathbf{a}]_2, [\mathbf{a}]_T$ and a matrix $[\mathbf{A}]_1, [\mathbf{A}]_2, [\mathbf{A}]_T$. For matrices $\mathbf{A}$ and $\mathbf{B}$ of compatible dimensions, $e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{A}^\top \mathbf{B}]_T$ is efficiently calculated with an efficient bilinear map e. Let $\mathcal{D}_k$ be an efficiently sampleable matrix distribution [EHK+17] that outputs $(\mathbf{A}, \mathbf{a}^\perp) \in \mathbb{Z}_p^{(k+1)\times k} \times \mathbb{Z}_p^{k+1}$ such that $\mathbf{A}^\top \cdot \mathbf{a}^\perp = \mathbf{0}$ and $\mathbf{a}^\perp \neq \mathbf{0}$.

Hereafter, we review a pair encoding scheme (PES) by following [AC16, AC17, Att14, Tak21]. A PES for a predicate $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ consists of the following four polynomial time algorithms (Param, EncK, EncC, Pair) defined as follows.

- $\mathsf{Param}(\mathsf{par}) \to n$: On input par, Param outputs $n \in \mathbb{N}$ that specifies the number of common variables denoted by $\mathbf{b} := (b_1, \ldots, b_n)$.

- $\mathsf{EncC}(x, N) \to (w_1, w_2, \mathbf{c})$: On input $x \in \mathcal{X}$ and $N \in \mathbb{N}$, EncC outputs a vector of w_3 ciphertext-encoding polynomials $\mathbf{c} = (c_1, \ldots, c_{w_3})$ in non-lone ciphertext-encoding variables s_0 and $\mathbf{s} = (s_1, s_1, \ldots, s_{w_1})$ and lone ciphertext-encoding variables $\hat{\mathbf{s}} = (\hat{s}_1, \ldots, \hat{s}_{w_2})$. The t-th polynomial is given by

$$c_t := \sum_{i \in [w_2]} \eta_{t,i} \hat{s}_i + \sum_{i \in [0, w_1], j \in [n]} \eta_{t,i,j} s_i b_j$$

  for $t \in [w_3]$, where $\eta_{t,i}, \eta_{t,i,j} \in \mathbb{Z}_N$.

- $\mathsf{EncK}(y, N) \to (m_1, m_2, \mathbf{k})$: On input $y \in \mathcal{Y}$ and $N \in \mathbb{N}$, EncK outputs a vector of m_3 key-encoding polynomials $\mathbf{k} = (k_1, \ldots, k_{m_3})$ in non-lone key-encoding variables $\mathbf{r} = (r_1, \ldots, r_{m_1})$ and lone key-encoding variables α and $\hat{\mathbf{r}} = (\hat{r}_1, \ldots, \hat{r}_{m_2})$. The t'-th polynomial is given by

$$k_{t'} := \phi_{t'} \alpha + \sum_{i' \in [m_2]} \phi_{t',i'} \hat{r}_{i'} + \sum_{i' \in [m_1], j \in [n]} \phi_{t',i',j} r_{i'} b_j$$

  for $t' \in [m_3]$, where $\phi_{t'}, \phi_{t',i'}, \phi_{t',i',j} \in \mathbb{Z}_N$.

- $\mathsf{Pair}(x, y, N) \to (\mathbf{E}, \overline{\mathbf{E}})$: On input $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $N \in \mathbb{N}$, Pair outputs two matrices $\mathbf{E}$ and $\overline{\mathbf{E}}$ of size $(w_1 + 1) \times m_3$ and $w_3 \times m_1$, respectively.

Correctness. A PES for a predicate f is correct if for all (N, par), $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ such that $f(x, y) = 1$, it holds that

$$\mathbf{s}^\top \mathbf{E}\mathbf{k} - \mathbf{c}^\top \overline{\mathbf{E}}\mathbf{r} = \sum_{i \in [0,w_1], t' \in [m_3]} s_i E_{i,t'} k_{t'} - \sum_{t \in [w_3], i' \in [m_1]} c_t \overline{E}_{t,i'} r_{i'} = \alpha s_0.$$

Remark 4. *For example, a* PES *for* IBE *has two common variables* (b_1, b_2)*, one ciphertext-encoding polynomial* $s(b_1 + \mathsf{id} \cdot b_2)$ *and one key-encoding polynomial* $s(b_1 + \mathsf{id} \cdot b_2)$*.*

Although there are various security definitions for PES, we do not review them in detail. The simplest one is *perfect security* [Att14, CGW15, Wee14]. Briefly speaking, a pair of ciphertext/key-encoding polynomials $(\mathbf{c}, \mathbf{k})$ for perfectly secure PES such that $f(x, y) = 0$ follows the same distribution regardless of the value of α. If PES for f satisfies the perfect security, there is an adaptively secure ABE scheme for the same f over dual system groups [CGW15, CW14] under the standard k-linear assumption [AC16, CGW15]. Although the perfect security captures only simple predicates, there are various PES for expressive predicates satisfying *symbolic security* [AC17]. If PES for f satisfies the symbolic security, there is an adaptively secure ABE scheme for the same f over dual system groups [AC17]; however, it requires the q-ratio assumption.

4.2 Technical Overview: Case of IBKHE

We first review a variant of a CPA-secure ElGamal encryption scheme. Then, we review an adaptively CPA-secure IBE scheme over dual system groups Π_{IBE} [CGW15, CW14] and Emura et al.'s KH-CCA-secure KHPKE scheme Π_{KHPKE} [EHN+18], then explain an overview of our proposed adaptively KH-CCA-secure IBKHE scheme Π_{IBKHE}.

CPA-*secure* PKE. Let $(\mathbf{A}, \mathbf{a}^\perp) \in \mathbb{Z}_p^{(k+1)\times k} \times \mathbb{Z}_p^{k+1}$ denote an instance of the matrix distribution such that $\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{0}$. A variant of the ElGamal PKE scheme Π_{PKE} is described as follows:

$$\mathsf{PKE.pk} = ([\mathbf{A}], [\mathbf{A}^\top \mathbf{u}]), \qquad \mathsf{PKE.sk} = \mathbf{u},$$
$$\mathsf{PKE.ct} = \left(\mathsf{PKE.ct}_0 = [\mathbf{A}\mathbf{s}], \quad \mathsf{PKE.ct}_\mu = \mu \cdot [\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}]\right),$$

where $\mathbf{u} \leftarrow_R \mathbb{Z}_p^{k+1}$ and $\mathbf{s} \leftarrow_R \mathbb{Z}_p^k$. We can correctly decrypt $\mathsf{PKE.ct} = (\mathsf{PKE.ct}_0, \mathsf{PKE.ct}_\mu)$ and recover a plaintext μ by using $\mathsf{PKE.sk}$ since we can compute $[\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}]$ from $\mathsf{PKE.ct}_0$ and $\mathsf{PKE.sk}$.

To prove the CPA security, we change the challenge ciphertext to be

$$\mathsf{PKE.ct}^\star = \left(\mathsf{PKE.ct}_0^\star = [\mathbf{c}], \quad \mathsf{PKE.ct}_\mu^\star = \mu^\star \cdot [\mathbf{c}^\top \mathbf{u}]\right),$$

where $\mathbf{c} \leftarrow_R \mathbb{Z}_p^{k+1}$. $\mathcal{A}$ cannot detect the change under the matrix DDH assumption. Then, even an unbounded adversary $\mathcal{A}$ cannot learn $\mu^\star$ from $\mathsf{PKE.ct}^\star$. Specifically, although the unbounded $\mathcal{A}$ can learn $\widehat{\mathbf{u}}$ such that $\mathbf{u} = \widehat{\mathbf{u}} + \alpha \mathbf{a}^\perp$ from $[\mathbf{A}]$ and $[\mathbf{A}^\top \mathbf{u}]$, α is distributed uniformly at random over $\mathbb{Z}_p$ from $\mathcal{A}$'s view. Observe that

$$\mathsf{PKE.ct}_\mu^\star = \mu^\star \cdot [\mathbf{c}^\top \mathbf{u}] = \mu^\star \cdot [\mathbf{c}^\top (\widehat{\mathbf{u}} + \alpha \mathbf{a}^\perp)] = \mu^\star \cdot [\mathbf{c}^\top \widehat{\mathbf{u}}] \cdot [\mathbf{c}^\top \mathbf{a}^\perp]^\alpha. \tag{1}$$

Since $\mathbf{c}$ is distributed uniformly at random over $\mathbb{Z}_p^{k+1}$, it does not live in the span of $\mathbf{A}$, i,e., $\mathbf{c}^\top \mathbf{a}^\perp \neq \mathbf{0}$, with overwhelming probability. Thus, $[\mathbf{c}^\top \mathbf{a}^\perp]$ is a generator of $\mathbb{G}$. Therefore, $[\mathbf{c}^\top \mathbf{a}^\perp]^\alpha$ is distributed uniformly at random over $\mathbb{G}$ from $\mathcal{A}$'s view and masks $\mu^\star$.

CPA-secure IBE Scheme Π_{IBE}. We review an IBE scheme Π_{IBE} over the dual system group [CGW15, CW14] equipped with an asymmetric bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ as follows:

$$
\begin{aligned}
\mathsf{IBE.mpk} &= \left(\mathsf{IBE.pp} = \left(\begin{array}{c}[\mathbf{A}]_1, [\mathbf{W}_1^\top \mathbf{A}]_1, [\mathbf{W}_2^\top \mathbf{A}]_1 \\ [\mathbf{B}]_2, [\mathbf{W}_1 \mathbf{B}]_2, [\mathbf{W}_2 \mathbf{B}]_2\end{array}\right), [\mathbf{A}^\top \mathbf{u}]_T\right), \qquad \mathsf{IBE.msk} = \mathbf{u}, \\
\mathsf{IBE.sk}_{\mathsf{id}} &= ([\mathbf{Br}]_2, [\mathbf{u}]_2 \cdot [(\mathbf{W}_1 + \mathsf{id} \cdot \mathbf{W}_2)\mathbf{Br}]_2), \\
\mathsf{IBE.ct}_{\mathsf{id}} &= \left(\mathsf{IBE.ct}_0 = [\mathbf{As}]_1, \mathsf{IBE.ct}_1 = [(\mathbf{W}_1^\top + \mathsf{id} \cdot \mathbf{W}_2^\top)\mathbf{As}]_1, \mathsf{IBE.ct}_\mu = \mu \cdot [\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}]_T\right),
\end{aligned}
$$

where $\mathbf{B} \in \mathbb{Z}_p^{(k+1)\times k}$ is a matrix sampled from the matrix distribution and $\mathbf{W}_1, \mathbf{W}_2 \leftarrow_R \mathbb{Z}_p^{(k+1)\times(k+1)}$. $\mathsf{IBE.mpk}$ and $\mathsf{IBE.ct}_{\mathsf{id}}$ are similar to $\mathsf{PKE.pk}$ and $\mathsf{PKE.ct}$, respectively, except that the matrices $\mathbf{W}_1, \mathbf{W}_2$ are used to encode id. As the case of Π_{PKE}, Π_{IBE} is correct since we can recover $[\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}]_T$ from $(\mathsf{IBE.ct}_0, \mathsf{IBE.ct}_1)$ and $\mathsf{IBE.sk}_{\mathsf{id}}$ by computing

$$
\frac{e(\mathsf{IBE.ct}_0, [\mathbf{u}]_2 \cdot [(\mathbf{W}_1 + \mathsf{id} \cdot \mathbf{W}_2)\mathbf{Br}]_2)}{e(\mathsf{IBE.ct}_1, [\mathbf{Br}]_2)} = [\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}]_T.
$$

To prove the adaptively CPA security of Π_{IBE}, we follow the proof of Π_{PKE} and change the challenge ciphertext to be

$$
\mathsf{IBE.ct}^\star_{\mathsf{id}^\star} = \left(\mathsf{IBE.ct}_0 = [\mathbf{c}]_1, \mathsf{IBE.ct}_1 = [(\mathbf{W}_1^\top + \mathsf{id}^\star \cdot \mathbf{W}_2^\top)\mathbf{c}]_1, \mathsf{IBE.ct}_\mu = \mu^\star \cdot [\mathbf{c}^\top \mathbf{u}]_T\right), \tag{2}
$$

where $\mathbf{c} \leftarrow_R \mathbb{Z}_p^{k+1}$. $\mathcal{A}$ cannot detect the change under the matrix DDH assumption over $\mathbb{G}_1$. However, unlike the case of Π_{PKE}, the unbounded $\mathcal{A}$ can still learn $\mu^\star$ since it can receive $\mathsf{IBE.sk}_{\mathsf{id}}$ for $\mathsf{id} \neq \mathsf{id}^\star$. In particular, the unbounded $\mathcal{A}$ can learn $\mathsf{IBE.msk} = \mathbf{u}$ from $\mathsf{IBE.mpk}$ and $\mathsf{IBE.sk}_{\mathsf{id}}$.

The dual system encryption methodology [Wat09] enables us to circumvent the issue by using the following *semi-functional* secret key

$$
\mathsf{IBE.sk}_{\mathsf{id}} = \left([\mathbf{Br}]_2, [\mathbf{u} + \tilde{\alpha}\mathbf{a}^\perp]_2 \cdot [(\mathbf{W}_1 + \mathsf{id} \cdot \mathbf{W}_2)\mathbf{Br}]_2\right),
$$

where $\tilde{\alpha} \leftarrow_R \mathbb{Z}_p$. Briefly speaking, the semi-functional $\mathsf{IBE.sk}_{\mathsf{id}}$ is the same as the normal one except that $\mathsf{IBE.msk} = \mathbf{u}$ is replaced with $\mathbf{u} + \tilde{\alpha}\mathbf{a}^\perp$. After we change the challenge ciphertext to be (2), we change $\mathsf{IBE.sk}_{\mathsf{id}}$ queried by $\mathcal{A}$ to be semi-functional one by one. When all $\mathsf{IBE.sk}_{\mathsf{id}}$ which $\mathcal{A}$ receives become semi-functional, it cannot learn $\mathsf{IBE.msk} = \mathbf{u}$ but can learn only $\mathbf{u} + \tilde{\alpha}\mathbf{a}^\perp$. As the proof of Π_{PKE}, $\mathcal{A}$ can learn $\hat{\mathbf{u}}$ such that $\mathbf{u} = \hat{\mathbf{u}} + \alpha\mathbf{a}^\perp$ from $[\mathbf{A}]_1$ and $[\mathbf{A}^\top \mathbf{u}]_T$. Since $\mathbf{u} + \tilde{\alpha}\mathbf{a}^\perp$ which $\mathcal{A}$ learns from semi-functional $\mathsf{IBE.sk}_{\mathsf{id}}$ does not help to reveal α, α is distributed uniformly at random over $\mathbb{Z}_p$ from $\mathcal{A}$'s view. Thus, $[\mathbf{c}^\top \mathbf{a}^\perp]^\alpha$ is distributed uniformly at random over $\mathbb{G}$ from $\mathcal{A}$'s view and masks $\mu^\star$ as the proof of Π_{PKE}.

As we discussed, we can prove the CPA security of Π_{IBE} if we can change all $\mathsf{IBE.sk}_{\mathsf{id}}$ queried by $\mathcal{A}$ to be semi-functional. To complete the change, there is an inherent property of the dual system technique. In particular, $\mathcal{A}$ itself cannot create $\mathsf{IBE.ct}_{\mathsf{id}}$ which follows the same distribution as (2). More specifically, $\mathcal{A}$ cannot create $\mathsf{IBE.ct}_{\mathsf{id}} = \left(\mathsf{IBE.ct}_0 = [\mathbf{c}]_1, \mathsf{IBE.ct}_1 = [(\mathbf{W}_1^\top + \mathsf{id} \cdot \mathbf{W}_2^\top)\mathbf{c}]_1, \mathsf{IBE.ct}_\mu = \mu \cdot [\mathbf{c}^\top \mathbf{u}]_T\right)$ if the discrete logarithm of $\mathsf{IBE.ct}_0$, i.e., $\mathbf{c} \in \mathbb{Z}_p^{k+1}$, does not live in the span of $\mathbf{A}$, i.e., $\mathbf{c}^\top \mathbf{a}^\perp \neq \mathbf{0}$. If $\mathcal{A}$ can create such $\mathsf{IBE.ct}_{\mathsf{id}}$, it can detect whether given $\mathsf{IBE.sk}_{\mathsf{id}}$ is normal or semi-functional by decrypting the above $\mathsf{IBE.ct}_{\mathsf{id}}$. Here, we use the fact that a decryption result of $\mathsf{IBE.ct}_{\mathsf{id}}$ by a semi-functional $\mathsf{IBE.sk}_{\mathsf{id}}$ is not μ but $\mu \cdot [\mathbf{c}^\top \mathbf{a}^\perp]^{\tilde{\alpha}}$ by following the similar calculation as (1).

KH-CCA-*secure* KHPKE. We review Emura et al.'s KHPKE scheme Π_{KHPKE} [EHN+18] by instantiating the hash proof system under the matrix DDH assumption [EHK+17] as follows:

$$\begin{aligned}
&\mathsf{KHPKE.pk} = ([\mathbf{A}], ([\mathbf{A}^\top \mathbf{u}_\iota]_{\iota \in [0,3]}), H), \\
&\mathsf{KHPKE.dk} = (\mathbf{u}_\iota)_{\iota \in [0,3]}, \qquad \mathsf{KHPKE.hk} = (\mathbf{u}_\iota)_{\iota \in [2]}, \\
&\mathsf{KHPKE.ct} = \begin{pmatrix} \mathsf{KHPKE.ct}_0 = [\mathbf{A}\mathbf{s}], \quad \mathsf{KHPKE.ct}_\mu = \mu \cdot [\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}_0] \\ \mathsf{KHPKE}.\pi = [\mathbf{s}^\top \mathbf{A}^\top (\mathbf{u}_1 + h \cdot \mathbf{u}_2)], \quad \mathsf{KHPKE}.\pi' = [\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}_3] \end{pmatrix},
\end{aligned}$$

where $\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3 \leftarrow_R \mathbb{Z}_p^{k+1}$, H is a collision-resistant hash function, and $h = H(\mathsf{KHPKE.ct}_0, \mathsf{KHPKE.ct}_\mu, \mathsf{KHPKE}.\pi')$. Briefly speaking, $\mathsf{KHPKE.pk}$ is the same as $\mathsf{PKE.pk}$ with four secret keys $(\mathbf{u}_\iota)_{\iota \in [0,3]}$. Moreover, Π_{KHPKE} is a combination of the $\mathsf{CCA1}$-secure Cramer-Shoup-lite and the $\mathsf{CCA2}$-secure Cramer-Shoup cryptosystem [CS98]; Π_{KHPKE} becomes the same as the former and the latter by removing the elements depending on $(\mathbf{u}_1, \mathbf{u}_2)$ and $\mathbf{u}_3$, respectively. As the case of Π_{PKE}, Π_{KHPKE} is correct since the structure of Π_{PKE} enables us to recover $[\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}_\iota]$ from $\mathsf{KHPKE.ct}_0$ and $\mathbf{u}_\iota$. Given a ciphertext $\mathsf{KHPKE.ct} = (\mathsf{KHPKE.ct}_0, \mathsf{KHPKE.ct}_\mu, \mathsf{KHPKE}.\pi, \mathsf{KHPKE}.\pi')$, a decryptor first checks the validities of $\mathsf{KHPKE}.\pi$ and $\mathsf{KHPKE}.\pi'$ by using $([\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}_\iota])_{\iota \in [2]}$ and $[\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}_3]$, respectively. If they are valid, the decryptor recovers μ from $\mathsf{KHPKE.ct}_\mu$ and $[\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}_0]$. To evaluate $\mathsf{KHPKE.ct}^{(1)} = (\mathsf{KHPKE.ct}_0^{(1)} = [\mathbf{A}\mathbf{s}^{(1)}], \mathsf{KHPKE.ct}_\mu^{(1)}, \mathsf{KHPKE}.\pi^{(1)}, \mathsf{KHPKE}.\pi'^{(1)})$ and $\mathsf{KHPKE.ct}^{(2)} = (\mathsf{KHPKE.ct}_0^{(2)} = [\mathbf{A}\mathbf{s}^{(2)}], \mathsf{KHPKE.ct}_\mu^{(2)}, \mathsf{KHPKE}.\pi^{(2)}, \mathsf{KHPKE}.\pi'(2))$, an evaluator first checks the validities of $\mathsf{KHPKE}.\pi^{(1)}$ and $\mathsf{KHPKE}.\pi^{(2)}$ by using $([(\mathbf{s}^{(1)})^\top \mathbf{A}^\top \mathbf{u}_\iota])_{\iota \in [2]}$ and $([(\mathbf{s}^{(2)})^\top \mathbf{A}^\top \mathbf{u}_\iota])_{\iota \in [2]}$, respectively. If they are valid, the evaluator computes $\mathsf{KHPKE.ct}_0 = [\mathbf{A}\mathbf{s}], \mathsf{KHPKE.ct}_\mu, \mathsf{KHPKE}.\pi'$ by multiplying $\mathsf{KHPKE.ct}_0^{(1)}, \mathsf{KHPKE.ct}_\mu^{(1)}, \mathsf{KHPKE}.\pi'^{(1)}$ with $\mathsf{KHPKE.ct}_0^{(2)}, \mathsf{KHPKE.ct}_\mu^{(2)}, \mathsf{KHPKE}.\pi'^{(2)}$, respectively, and computes $\mathsf{KHPKE}.\pi$ from $h = H(\mathsf{KHPKE.ct}_0, \mathsf{KHPKE.ct}_\mu, \mathsf{KHPKE}.\pi')$ and $([\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}_\iota])_{\iota \in [2]}$.

Let $\mathsf{KHPKE.ct}^\star$ denote the challenge ciphertext and $\mathsf{KHPKE.ct}^{(1)} = \mathsf{KHPKE.ct}^\star, \mathsf{KHPKE.ct}^{(2)}, \ldots, \mathsf{KHPKE.ct}^{(D)}$ denote ciphertexts in the list $\mathcal{L}$. To prove the KH-CCA security, we change distributions of the ciphertexts in $\mathcal{L}$ one by one so that they are independent of $\mu^\star$. Here, we explain how to change the distribution of $\mathsf{KHPKE.ct}^\star$. For this purpose, we follow the proof of Π_{PKE} and change the challenge ciphertext to be

$$\mathsf{KHPKE.ct}^\star = ([\mathbf{c}], \mu^\star \cdot [\mathbf{c}^\top \mathbf{u}_0], [\mathbf{c}^\top (\mathbf{u}_1 + h^\star \cdot \mathbf{u}_2)], [\mathbf{c}^\top \mathbf{u}_3]), \tag{3}$$

where $\mathbf{c} \leftarrow_R \mathbb{Z}_p^{k+1}$. $\mathcal{A}$ cannot detect the change under the matrix DDH assumption. We note that we do not use the above $\mathsf{KHPKE.ct}^\star$ but a normal encryption of $\mu^\star$ to compute $\mathsf{KHPKE.ct}^{(2)}, \ldots, \mathsf{KHPKE.ct}^{(D)}$ in the list $\mathcal{L}$. Then, the distribution of $\mathsf{KHPKE.ct}^\star$ does not depend on $\mu^\star$ since even an unbounded $\mathcal{A}$ cannot learn $\mu^\star$ from $\mathsf{KHPKE.ct}^\star$. As the proof of Π_{PKE}, $\mathcal{A}$ can learn $\widehat{\mathbf{u}}_\iota$ such that $\mathbf{u}_\iota = \widehat{\mathbf{u}}_\iota + \alpha_\iota \mathbf{a}^\perp$ from $[\mathbf{A}]$ and $[\mathbf{A}^\top \mathbf{u}_\iota]$ for $\iota \in [0,3]$, respectively; however, α_0 is distributed uniformly at random over $\mathbb{Z}_p$ from $\mathcal{A}$'s view. Thus, $[\mathbf{c}^\top \mathbf{a}^\perp]^{\alpha_0}$ is distributed uniformly at random over $\mathbb{G}$ from $\mathcal{A}$'s view and masks $\mu^\star$ as the proof of Π_{PKE}.

To ensure that the unbounded $\mathcal{A}$ cannot learn α_0, we have to care $\mathcal{A}$'s decryption queries and evaluation queries which are not allowed in the case of Π_{PKE}. We call $\mathcal{A}$'s decryption query on $\mathsf{KHPKE.ct} = (\mathsf{KHPKE.ct}_0 = [\mathbf{c}], \mathsf{KHPKE.ct}_\mu, \mathsf{KHPKE}.\pi, \mathsf{KHPKE}.\pi')$ a *critical decryption query* if $\mathsf{KHPKE}.\pi$ and $\mathsf{KHPKE}.\pi'$ are valid, $\mathsf{KHPKE.ct}$ follows the same distribution as (3), and $\mathbf{c}$ does not live in the span of $\mathbf{A}$, i.e., $\mathbf{c}^\top \mathbf{a}^\perp \neq \mathbf{0}$. If $\mathcal{A}$ can make a critical decryption query, the answer is $\mu \cdot [\mathbf{c}^\top \mathbf{a}^\perp]^{\alpha_0}$ by following the similar calculation as (1) and $\mathcal{A}$ can learn α_0. In contrast, answers of decryption queries do not reveal the information of α_0 if $\mathbf{c}$ lives in the span of $\mathbf{A}$. The structures of the $\mathsf{CCA1}$-secure Cramer-Shoup-lite and the $\mathsf{CCA2}$-secure Cramer-Shoup cryptosystem [CS98] ensure that $\mathcal{A}$ cannot make critical decryption queries since it cannot create valid $\mathsf{KHPKE}.\pi$ or

$\mathsf{KHPKE}.\pi'$. If the unbounded $\mathcal{A}$ can create valid $\mathsf{KHPKE}.\pi$ and $\mathsf{KHPKE}.\pi'$, and make critical decryption queries, it has to know $(\alpha_\iota)_{\iota\in[2]}$ and α_3, respectively. We note that $\mathcal{A}$ can receive $\mathsf{KHPKE.hk} = (\mathbf{u}_\iota)_{\iota\in[2]}$ in the $\mathsf{KH\text{-}CCA}$ security game and is allowed to make decryption queries until it receives both $\mathsf{KHPKE.hk}$ and $\mathsf{KHPKE.ct}^\star$. Thus, all we have to ensure is that $\mathcal{A}$ does not know $(\alpha_\iota)_{\iota\in[2]}$ or α_3 until it receives both $\mathsf{KHPKE.hk}$ and $\mathsf{KHPKE.ct}^\star$. At first, $\mathcal{A}$ cannot learn α_3 until it receives $\mathsf{KHPKE.ct}^\star$ thanks to the structure of the $\mathsf{CCA1}$-secure Cramer-Shoup-lite [CS98]. When $\mathcal{A}$ makes a decryption query or an evaluation query on $\mathsf{KHPKE.ct} = (\mathsf{KHPKE.ct}_0, \ldots)$ such that the discrete logarithm of $\mathsf{KHPKE.ct}_0$ does not live in the span of $\mathbf{A}$ and the answer is $\perp$, $\mathcal{A}$ can reduce a candidate of α_3; however, it can reduce only polynomially many numbers of candidates throughout the security game. Thus, $\mathcal{A}$ cannot guess α_3 with non-negligible probability. Next, $\mathcal{A}$ cannot learn $(\alpha_\iota)_{\iota\in[2]}$ until it receives $\mathsf{KHPKE.hk}$ thanks to the structure of the $\mathsf{CCA2}$-secure Cramer-Shoup cryptosytem [CS98]. Observe that $\mathsf{KHPKE.ct}^\star$ reveals the value of $\alpha_1 + h^\star\alpha_2$ to the unbounded $\mathcal{A}$. Thus, $\mathcal{A}$ can learn $(\alpha_\iota)_{\iota\in[2]}$ if it learns the value of $\alpha_1 + h\alpha_2$ for some $h \neq h^\star$. When $\mathcal{A}$ makes a decryption query on $\mathsf{KHPKE.ct} = (\mathsf{KHPKE.ct}_0, \ldots)$ such that the discrete logarithm of $\mathsf{KHPKE.ct}_0$ does not live in the span of $\mathbf{A}$ and the answer is $\perp$, $\mathcal{A}$ can reduce a candidate of $\alpha_1 + h\alpha_2$; however, it can reduce only polynomially many numbers of candidates throughout the security game. Thus, $\mathcal{A}$ cannot guess $(\alpha_\iota)_{\iota\in[2]}$ with non-negligible probability.

$\mathsf{KH\text{-}CCA}$-secure IBKHE Scheme Π_{IBKHE}. Hereafter, we explain an overview of our proposed IBKHE Scheme Π_{IBKHE}. Let $\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota]$ denote id's secret key of Π_{IBE} for a master secret key $\mathbf{u}_\iota$. We combine Π_{IBE} and Π_{KHPKE}, and construct Π_{IBKHE} as follows:

$$\begin{aligned}
\mathsf{mpk} &= \left(\mathsf{IBE.pp}, ([\mathbf{A}^\top \mathbf{u}_\iota]_T)_{\iota\in[0,2]}, H\right), \qquad \mathsf{msk} = (\mathbf{u}_\iota)_{\iota\in[0,2]},\\
\mathsf{dk}_{\mathsf{id}} &= (\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[0,2]}, \qquad \mathsf{hk}_{\mathsf{id}} = (\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[2]},\\
\mathsf{ct}_{\mathsf{id}} &= \left(\mathsf{IBE.ct}_{\mathsf{id}} = (\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{ct}_\mu), \pi = [\mathbf{s}^\top \mathbf{A}^\top (\mathbf{u}_1 + h \cdot \mathbf{u}_2)]_T\right),
\end{aligned}$$

where $h = H(\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{ct}_\mu)$. Briefly speaking, mpk is the same as $\mathsf{IBE.mpk}$ with three master secret keys $(\mathbf{u}_\iota)_{\iota\in[0,2]}$, while $\mathsf{KHPKE.pk}$ is the same as $\mathsf{PKE.pk}$ with four secret keys $(\mathbf{u}_\iota)_{\iota\in[0,2]}$. As the case of Π_{KHPKE}, Π_{IBKHE} is correct since the structure of Π_{IBE} enables us to recover $[\mathbf{s}^\top \mathbf{A}^\top \mathbf{u}_\iota]_T$ from $(\mathsf{ct}_0, \mathsf{ct}_1)$ and $\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota]$.

To prove the adaptively $\mathsf{KH\text{-}CCA}$ security, we change distributions of the ciphertexts in $\mathcal{L}$ one by one so that they are independent of $\mu^\star$ as the case of Π_{KHPKE}. Here, we explain how to change the distribution of the challenge ciphertext $\mathsf{ct}^\star_{\mathsf{id}^\star}$. As the proofs of Π_{IBE} and Π_{KHPKE}, we change the challenge ciphertext to be

$$\mathsf{ct}^\star_{\mathsf{id}^\star} = ([\mathbf{c}]_1, [(\mathbf{W}_1^\top + \mathsf{id}^\star \cdot \mathbf{W}_2^\top)\mathbf{c}]_1, \mu^\star \cdot [\mathbf{c}^\top \mathbf{u}_0]_T, [\mathbf{c}^\top (\mathbf{u}_1 + h^\star \cdot \mathbf{u}_2)]_T), \tag{4}$$

where $\mathbf{c} \leftarrow_R \mathbb{Z}_p^{k+1}$. The unbounded $\mathcal{A}$ can learn $\widehat{\mathbf{u}}_\iota$ such that $\mathbf{u}_\iota = \widehat{\mathbf{u}}_\iota + \alpha_\iota \mathbf{a}^\perp$ from $[\mathbf{A}]_1$ and $[\mathbf{A}^\top \mathbf{u}_\iota]_T$ for $\iota \in [0,2]$, respectively. If $\mathcal{A}$ cannot learn α_0, we can prove the security. Although $\mathcal{A}$ can receive $\mathsf{dk}_{\mathsf{id}} = (\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[0,2]}$ and still learn α_0 from $\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_0]$, the dual system technique enables us to circumvent the issue by changing all normal $\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_0]$ which $\mathcal{A}$ receives to be semi-functional $\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_0 + \tilde{\alpha}_0 \mathbf{a}^\perp]$ as the case of Π_{IBE}. As the case of Π_{KHPKE}, the unbounded $\mathcal{A}$ may be able to learn α_0 via decryption queries.

We call $\mathcal{A}$'s decryption query on $\mathsf{ct}_{\mathsf{id}} = (\mathsf{ct}_0 = [\mathbf{c}]_1, \mathsf{ct}_1, \mathsf{ct}_\mu, \pi)$ a *critical decryption query* if π is valid, ct follows the same distribution as (4), and $\mathbf{c}$ does not live in the span of $\mathbf{A}$, i.e., $\mathbf{c}^\top \mathbf{a}^\perp \neq \mathbf{0}$. As the case of Π_{KHPKE}, all we have to ensure is that $\mathcal{A}$ cannot make critical decryption queries until it receives both $\mathsf{hk}_{\mathsf{id}^\star}$ and $\mathsf{ct}^\star_{\mathsf{id}^\star}$. Observe that the unbounded $\mathcal{A}$ can make critical decryption queries since it can receive $(\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[2]}$ unlike the case of Π_{KHPKE}. On the surface, the dual system technique seems to be sufficient to circumvent the issue by changing all normal $(\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[2]}$ which $\mathcal{A}$ receives to be semi-functional $(\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[2]}$; however, we cannot take the approach directly since $\mathcal{A}$ can receive $\mathsf{hk}_{\mathsf{id}^\star} = (\mathsf{IBE.sk}_{\mathsf{id}^\star}[\mathbf{u}_\iota])_{\iota\in[2]}$ which we cannot change to be semi-functional. Moreover, even when $\mathsf{id} \neq \mathsf{id}^\star$ holds, we cannot also change $\mathsf{hk}_{\mathsf{id}} = (\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[2]}$ which $\mathcal{A}$ receives in Phase 1 to be semi-functional since we cannot detect whether $\mathsf{id} \neq \mathsf{id}^\star$ holds.

To circumvent the issue, we divide $\mathcal{A}$'s attack strategies into two types. We call a strategy Type-1 if $\mathcal{A}$ receives $\mathsf{hk}_{\mathsf{id}^\star}$ in Phase 1 and Type-2 otherwise. To prove the security against the Type-2 $\mathcal{A}$, we change all normal $(\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[2]}$ which $\mathcal{A}$ receives to be semi-functional $(\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota + \tilde{\alpha}_\iota \mathbf{a}^\perp])_{\iota\in[2]}$ until $\mathcal{A}$'s query to receive $\mathsf{hk}_{\mathsf{id}^\star}$. Since the definition of the Type-2 strategy ensures that $\mathcal{A}$ queries to receive $\mathsf{hk}_{\mathsf{id}^\star}$ only in Phase 2, we can detect whether $\mathsf{id} \neq \mathsf{id}^\star$ holds and complete the change. Since $\mathcal{A}$ cannot learn $(\alpha_\iota)_{\iota\in[2]}$ until it receives both $\mathsf{hk}_{\mathsf{id}^\star}$ and $\mathsf{ct}^\star_{\mathsf{id}^\star}$, it cannot create valid π and make critical decryption queries. To prove the security against the Type-1 $\mathcal{A}$, we cannot change $(\mathsf{IBE.sk}_{\mathsf{id}}[\mathbf{u}_\iota])_{\iota\in[2]}$ which $\mathcal{A}$ receives to be semi-functional since we cannot detect whether $\mathsf{id} \neq \mathsf{id}^\star$ holds upon $\mathcal{A}$'s queries to receive $\mathsf{hk}_{\mathsf{id}}$. Although we ensured that $\mathcal{A}$ cannot create $\mathsf{KHPKE}.\pi'$ and make critical decryption queries in the case of Π_{KHPKE}, there does not seem to be the corresponding element in $\mathsf{ct}_{\mathsf{id}}$ on the surface. However, the inherent property of the dual system technique ensures that $\mathcal{A}$ cannot make critical decryption queries. In particular, since $\mathcal{A}$ against Π_{IBE} cannot create $\mathsf{IBE.ct}_{\mathsf{id}}$ to make critical decryption queries, the Type-1 $\mathcal{A}$ cannot also create $\mathsf{ct}_{\mathsf{id}} = (\mathsf{IBE.ct}_{\mathsf{id}}, \pi)$ and make critical decryption queries. Thus, we can prove the adaptively KH-CCA security of Π_{IBKHE} against both types of $\mathcal{A}$ as the case of Π_{KHPKE}.

4.3 Construction

We construct an ABKHE scheme Π_{ABKHE} from $\mathsf{PES} = (\mathsf{Param}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ for a predicate $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$. Let Π_{ABE} denote an ABE scheme from PES over dual system groups [AC16, AC17, CGW15]. Briefly speaking, Π_{ABKHE} is based on Π_{ABE} with three master secret keys $(\mathbf{u}_\iota)_{\iota\in[0,2]}$ by combining with Emura et al.'s KHPKE scheme Π_{KHPKE} [EHN+18]. A ciphertext of Π_{ABKHE} is described as $\mathsf{ct}_x = (\mathsf{ABE.ct}_x, \pi)$, where $\mathsf{ABE.ct}_x$ is a ciphertext of Π_{ABE} and we will use π to realize the CCA2 security. Let $\mathsf{sk}_{y,\iota}$ denote a secret key of Π_{ABE} for a master secret key $\mathbf{u}_\iota$. Then, a decryption key and a homomorphic evaluation key are described as $\mathsf{dk}_y = (\mathsf{sk}_{y,\iota})_{\iota\in[0,2]}$ and $\mathsf{dk}_y = (\mathsf{sk}_{y,\iota})_{\iota\in[2]}$, respectively.

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$: Run $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \leftarrow \mathcal{G}(1^\lambda)$ and $n \leftarrow \mathsf{Param}(\mathsf{par})$, and choose a collision-resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p$. Sample $(\mathbf{A}, \mathbf{a}^\perp), (\mathbf{B}, \mathbf{b}^\perp) \leftarrow \mathcal{D}_k$, uniformly random matrices $\mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow_R \mathbb{Z}_p^{(k+1)\times(k+1)}$, and random vectors $(\mathbf{u}_\iota)_{\iota\in[0,2]} \leftarrow_R \mathbb{Z}_p^{k+1}$, then output
$$\mathsf{mpk} \coloneqq \Big(\mathcal{G}(1^\lambda), [\mathbf{A}]_1, [\mathbf{B}]_2, ([\mathbf{W}_j^\top \mathbf{A}]_1, [\mathbf{W}_j \mathbf{B}]_2)_{j\in[n]}, ([\mathbf{A}^\top \mathbf{u}_\iota]_T)_{\iota\in[0,2]}, H\Big)$$
and $\mathsf{msk} \coloneqq ([\mathbf{u}_\iota]_2)_{\iota\in[0,2]}$.

- $\mathsf{Enc}(\mathsf{mpk}, x, \mu) \to \mathsf{ct}_x$: Run $\mathsf{EncC}(x, p)$ to obtain w_3 key-encoding polynomials $(c_1, \ldots, c_{w_3})$, sample $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{w_1+w_2} \leftarrow_R \mathbb{Z}_p^k$, and output $\mathsf{ct}_x \coloneqq ((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, (\mathsf{ct}_{1,t})_{t\in[w_3]}, \mathsf{ct}_T, \pi)$;
$$\mathsf{ct}_{0,i} \coloneqq [\mathbf{A}\mathbf{s}_i]_1, \qquad \mathsf{ct}_{1,t} \coloneqq \prod_{i\in[w_2]} [\mathbf{A}\mathbf{s}_{w_1+i}]_1^{\eta_{t,i}} \cdot \prod_{i\in[0,w_1], j\in[n]} [\mathbf{W}_j^\top \mathbf{A}\mathbf{s}_i]_1^{\eta_{t,i,j}},$$
$$\mathsf{ct}_T \coloneqq \mu \cdot [\mathbf{s}_0^\top \mathbf{A}^\top \mathbf{u}_0]_T, \quad \pi \coloneqq [\mathbf{s}_0^\top \mathbf{A}^\top (\mathbf{u}_1 + h \cdot \mathbf{u}_2)]_T,$$
where $h = H((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, \mathsf{ct}_T)$.

- $\mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y) \rightarrow (\mathsf{dk}_y, \mathsf{hk}_y)$: Run $\mathsf{EncK}(y, p)$ to obtain m_3 key-encoding polynomials $(k_1, \ldots, k_{m_3})$, sample $\mathbf{r}_{\iota,1}, \ldots, \mathbf{r}_{\iota,m_1+m_2} \leftarrow_R \mathbb{Z}_p^k$, and compute $\mathsf{sk}_{y,\iota} \coloneqq ((\mathsf{sk}_{\iota,0,i'})_{i' \in [m_1]}, (\mathsf{sk}_{\iota,1,t'})_{t' \in [m_3]})$ for $\iota \in [0, 3]$;

$$\begin{aligned}\mathsf{sk}_{\iota,0,i'} &\coloneqq [\mathbf{B}\mathbf{r}_{\iota,i'}]_2,\\ \mathsf{sk}_{\iota,1,t'} &\coloneqq [\mathbf{u}_\iota]_2^{\phi_{t'}} \cdot \prod_{i' \in [m_2]} [\mathbf{B}\mathbf{r}_{\iota,m_1+i'}]_2^{\phi_{t',i'}} \cdot \prod_{i' \in [m_2], j \in [n]} [\mathbf{W}_j \mathbf{B}\mathbf{r}_{\iota,i'}]_2^{\phi_{t',i',j}}.\end{aligned} \tag{5}$$

  Output $\mathsf{dk}_y \coloneqq (\mathsf{sk}_{y,\iota})_{\iota \in [0,2]}$ and $\mathsf{hk}_y \coloneqq (\mathsf{sk}_{y,\iota})_{\iota \in [2]}$.

- $\mathsf{Eval}(\mathsf{mpk}, \mathsf{hk}_y, (\mathsf{ct}_x^{(\ell)})_{\ell \in [L]}) \rightarrow \mathsf{ct}_x/\bot$: Output $\bot$ if $f(x, y) = 0$ holds. Otherwise, parse $\mathsf{hk}_y = ((\mathsf{sk}_{\iota,0,i'})_{i' \in [m_1]}, (\mathsf{sk}_{\iota,1,t'})_{t' \in [m_3]})_{\iota \in [2]}$ and $\mathsf{ct}_x^{(\ell)} = ((\mathsf{ct}_{0,i}^{(\ell)})_{i \in [0,w_1]}, (\mathsf{ct}_{1,t}^{(\ell)})_{t \in [w_3]}, \mathsf{ct}_T^{(\ell)}, \pi^{(\ell)})$, run $(\mathbf{E}, \overline{\mathbf{E}}) \leftarrow \mathsf{Pair}(x, y, p)$, and check whether the following conditions (a) and (b) simultaneously hold for all $\ell \in [L]$:

  (a) Compute $\mathsf{sk}_y \coloneqq ((\mathsf{sk}_{0,i'})_{i' \in [m_1]}, (\mathsf{sk}_{1,t})_{t' \in [m_3]})$ in the same way as (5) except that $\mathbf{u}_\iota$ is replaced with a zero vector. It holds that

  $$\prod_{i \in [0,w_1], t' \in [m_3]} e(\mathsf{ct}_{0,i}^{(\ell)}, \mathsf{sk}_{1,t'})^{E_{i,t'}} = \prod_{t \in [w_3], i' \in [m_1]} e(\mathsf{ct}_{1,t}^{(\ell)}, \mathsf{sk}_{0,i'})^{\overline{E}_{t,i'}}.$$

  (b) It holds that

  $$\frac{\prod_{i \in [0,w_1], t' \in [m_3]} e(\mathsf{ct}_{0,i}^{(\ell)}, \mathsf{sk}_{1,1,t'} \cdot \mathsf{sk}_{2,1,t'}^{h^{(\ell)}})^{E_{i,t'}}}{\prod_{t \in [w_3], i' \in [m_1]} e(\mathsf{ct}_{1,t}^{(\ell)}, \mathsf{sk}_{1,0,i'} \cdot \mathsf{sk}_{2,0,i'}^{h^{(\ell)}})^{\overline{E}_{t,i'}}} = \pi,$$

  where $h^{(\ell)} = H((\mathsf{ct}_{0,i}^{(\ell)})_{i \in [0,w_1]}, \mathsf{ct}_T^{(\ell)})$.

  If one of the conditions does not hold for some $\ell \in [L]$, output $\bot$. Otherwise, run $\mathsf{ct}_x^{(0)} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, 1_T)$ and output $\mathsf{ct}_x \coloneqq ((\mathsf{ct}_{0,i})_{i \in [0,w_1]}, (\mathsf{ct}_{1,t})_{t \in [w_3]}, \mathsf{ct}_T, \pi)$;

  $$\begin{aligned}\mathsf{ct}_{0,i} &\coloneqq \prod_{\ell \in [0,L]} \mathsf{ct}_{0,i}^{(\ell)}, \qquad \mathsf{ct}_{1,t} \coloneqq \prod_{\ell \in [0,L]} \mathsf{ct}_{1,t}^{(\ell)}, \qquad \mathsf{ct}_T \coloneqq \prod_{\ell \in [0,L]} \mathsf{ct}_T^{(\ell)},\\ \pi &\coloneqq \frac{\prod_{i \in [0,w_1], t' \in [m_3]} e(\mathsf{ct}_{0,i}, \mathsf{sk}_{1,1,t} \cdot \mathsf{sk}_{2,1,t'}^{h})^{E_{i,t'}}}{\prod_{t \in [w_3], i' \in [m_1]} e(\mathsf{ct}_{1,t}, \mathsf{sk}_{1,0,i'} \cdot \mathsf{sk}_{2,0,i'}^{h})^{\overline{E}_{t,i'}}},\end{aligned}$$

  where $h = H((\mathsf{ct}_{0,i})_{i \in [0,w_1]}, \mathsf{ct}_T)$.

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_y, \mathsf{ct}_x) \rightarrow \mu/\bot$: Output $\bot$ if $f(x, y) = 0$ holds. Otherwise, parse $\mathsf{dk}_y = ((\mathsf{sk}_{\iota,0,i'})_{i' \in [m_1]}, (\mathsf{sk}_{\iota,1,t'})_{t' \in [m_3]})_{\iota \in [0,2]}$ and $\mathsf{ct}_x = ((\mathsf{ct}_{0,i})_{i \in [0,w_1]}, (\mathsf{ct}_{1,t})_{t \in [w_3]}, \mathsf{ct}_T, \pi)$, run $(\mathbf{E}, \overline{\mathbf{E}}) \leftarrow \mathsf{Pair}(x, y, p)$, and check whether the conditions (a) and (b) defined in Eval simultaneously hold. If one of the conditions does not hold, output $\bot$. Otherwise, output

  $$\mathsf{ct}_T \cdot \frac{\prod_{t \in [w_3], i' \in [m_1]} e(\mathsf{ct}_{1,t}, \mathsf{sk}_{0,0,i'})^{\overline{E}_{t,i'}}}{\prod_{i \in [0,w_1], t' \in [m_3]} e(\mathsf{ct}_{0,i}, \mathsf{sk}_{0,1,t'})^{E_{i,t'}}}.$$

Correctness. Our proposed Π_{ABKHE} satisfies the correctness as follows.

Theorem 3. *The proposed* ABKHE *scheme* Π_{ABKHE} *satisfies correctness if the* $\mathsf{PES} = (\mathsf{Param}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ *for* f *satisfies the correctness.*

Proof. At first, we show that a pre-evaluated ciphertext $\mathsf{ct}_x = ((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, (\mathsf{ct}_{1,t})_{t\in[w_3]}, \mathsf{ct}_T, \pi)$ output by $\mathsf{Enc}(\mathsf{mpk}, x, \mu)$ can be correctly decrypted by $\mathsf{dk}_y = ((\mathsf{sk}_{\iota,0,i'})_{i'\in[m_1]}, (\mathsf{sk}_{\iota,1,t'})_{t'\in[m_3]})_{\iota\in[0,2]}$ output by $\mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y)$ such that $f(x, y) = 1$. In general, if we substitute

$$\begin{array}{llll} s_i : \mathbf{A}\mathbf{s}_i, & \hat{s}_i : \mathbf{A}\mathbf{s}_{w_1+i}, & s_i b_j : \mathbf{W}_j^\top \mathbf{A}\mathbf{s}_i, & \\ \alpha : \mathbf{u}_\iota, & r_{i'} : \mathbf{B}\mathbf{r}_{\iota,i'}, & \hat{r}_{i'} : \mathbf{B}\mathbf{r}_{\iota,m_1+i'}, & r_{i'} b_j : \mathbf{W}_j \mathbf{B}\mathbf{r}_{\iota,i'}, \end{array}$$

the discrete logarithms of $\mathsf{ct}_{1,t}$ and $\mathsf{sk}_{\iota,1,t'}$ are t-th ciphertext-encoding polynomial c_t and t'-th key-encoding polynomial $k_{t'}$, respectively. Thus, the correctness of PES implies

$$\frac{\prod_{i\in[0,w_1],t'\in[m_3]} e(\mathsf{ct}_{0,i}, \mathsf{sk}_{\iota,1,t'})^{E_{i,t'}}}{\prod_{t\in[w_3],i'\in[m_1]} e(\mathsf{ct}_{1,t}, \mathsf{sk}_{\iota,0,i'})^{\overline{E}_{t,i'}}} = [\mathbf{s}_0^\top \mathbf{A}^\top \mathbf{u}_\iota]_T. \tag{6}$$

The equation (6) ensures that the conditions (a) and (b) hold and Dec outputs the correct decryption result.

The correctness also holds for an evaluated ciphertext. In particular, if pre-evaluated ciphertexts $\mathsf{ct}_x^{(1)}, \ldots, \mathsf{ct}_x^{(L)}$ which are inputs of Eval are encryptions of $\mu^{(1)}, \ldots, \mu^{(L)}$, respectively, then an evaluated ciphertext $\mathsf{ct}_x = ((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, (\mathsf{ct}_{1,t})_{t\in[w_3]}, \mathsf{ct}_T, \pi)$ output by Eval is an encryption of $\prod_{\ell\in[L]} \mu^{(\ell)}$ and follows the same distribution as a pre-evaluated ciphertext ct_x output by Enc. In particular, when we use $\mathbf{s}_0^{(\ell)}, \mathbf{s}_1^{(\ell)}, \ldots, \mathbf{s}_{w_1+w_2}^{(\ell)}$ to denote uniformly random vectors for creating $\mathsf{ct}_x^{(\ell)}$ for $\ell \in [0, L]$, respectively, then $\sum_{\ell\in[0,L]} \mathbf{s}_0^{(\ell)}, \sum_{\ell\in[0,L]} \mathbf{s}_1^{(\ell)}, \ldots, \sum_{\ell\in[0,L]} \mathbf{s}_{w_1+w_2}^{(\ell)}$ are uniformly random vectors for creating ct_x. Indeed, the vectors are uniformly random due to $\mathbf{s}_0^{(0)}, \mathbf{s}_1^{(0)}, \ldots, \mathbf{s}_{w_1+w_2}^{(0)}$ which are sampled during Eval. We can easily check the claim for $(\mathsf{ct}_{0,i})_{i\in[0,w_1]}$, $(\mathsf{ct}_{1,t})_{t\in[w_3]}$, and ct_T. The claim also holds for π since the computation is the same as the validity check of the condition (b). Thus, we complete the proof. □

4.4 Security

Theorem 4. *If the* $\mathsf{PES} = (\mathsf{Param}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ *for* f *satisfies the perfect security and the symbolic security,* Π_{ABKHE} *satisfies the adaptive* $\mathsf{KH\text{-}CCA}$ *security under the* k*-linear assumption and the* q*-ratio assumption, respectively.*

To prove the theorem, we prepare auxiliary *semi-functional* distributions for a ciphertext and an ABE secret key by following [AC16, AC17, CGW15].

- *Semi-functional Ciphertext.* A semi-functional ciphertext ct_x for x encrypting μ is defined as $\mathsf{ct}_x = ((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, (\mathsf{ct}_{1,t})_{t\in[w_3]}, \mathsf{ct}_T, \pi)$;

$$\mathsf{ct}_{0,i} \coloneqq [\mathbf{c}_i]_1, \qquad \mathsf{ct}_{1,t} \coloneqq \prod_{i\in[w_2]} [\mathbf{c}_{w_1+i}]_1^{\eta_{t,i}} \cdot \prod_{i\in[0,w_1],j\in[n]} [\mathbf{W}_j^\top \mathbf{c}_i]_1^{\eta_{t,i,j}},$$
$$\mathsf{ct}_T \coloneqq \mu \cdot [\mathbf{c}_0^\top \mathbf{u}_0]_T, \qquad \pi \coloneqq [\mathbf{c}_0^\top (\mathbf{u}_1 + h \cdot \mathbf{u}_2)]_T,$$

where $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{w_1+w_2} \leftarrow_R \mathbb{Z}_p^{k+1}$ and $h = H((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, \mathsf{ct}_T)$.

- *Semi-functional Secret Key.* An ι-th semi-functional secret key $\mathsf{sk}_{y,\iota}$ for y is defined as $\mathsf{sk}_{y,\iota} = ((\mathsf{sk}_{\iota,0,i'})_{i'\in[m_1]}, (\mathsf{sk}_{\iota,1,t'})_{t'\in[m_3]})$;

$$\begin{aligned}\mathsf{sk}_{\iota,0,i'} &= [\mathbf{B}\mathbf{r}_{\iota,i'}]_2,\\ \mathsf{sk}_{\iota,1,t'} &= [\mathbf{u}_\iota + \tilde{\alpha}_\iota \mathbf{a}^\perp]_2^{\phi_{t'}} \cdot \prod_{i'\in[m_2]} [\mathbf{B}\mathbf{r}_{\iota,m_1+i'}]_2^{\phi_{t',i'}} \cdot \prod_{i'\in[m_2],j\in[n]} [\mathbf{W}_j\mathbf{B}\mathbf{r}_{\iota,i'}]_2^{\phi_{t',i',j}},\end{aligned}$$

where $\mathbf{r}_{\iota,1}, \ldots, \mathbf{r}_{\iota,m_1+m_2} \leftarrow_R \mathbb{Z}_p^k$ and $\tilde{\alpha}_\iota \leftarrow_R \mathbb{Z}_p$. We note that $\tilde{\alpha}_\iota$ is shared by all semi-functional $\mathsf{sk}_{y,\iota}$ for distinct y's.

For a semi-functional $\mathsf{ct}_x = ((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, (\mathsf{ct}_{1,t})_{t\in[w_3]}, \mathsf{ct}_T, \pi)$ and a semi-functional $\mathsf{sk}_{y,\iota} = ((\mathsf{sk}_{\iota,0,i'})_{i'\in[m_1]}, (\mathsf{sk}_{\iota,1,t'})_{t'\in[m_3]})$, the equation (6) becomes

$$\frac{\prod_{i\in[0,w_1],t'\in[m_3]} e(\mathsf{ct}_{0,i}, \mathsf{sk}_{\iota,1,t'})^{E_{i,t'}}}{\prod_{t\in[w_3],i'\in[m_1]} e(\mathsf{ct}_{1,t}, \mathsf{sk}_{\iota,0,i'})^{\overline{E}_{t,i'}}} = [\mathbf{c}_0^\top(\mathbf{u}_\iota + \tilde{\alpha}_\iota\mathbf{a}^\perp)]_T = [\mathbf{c}_0^\top\mathbf{u}_\iota]_T \cdot [\mathbf{c}_0^\top\mathbf{a}^\perp]_T^{\tilde{\alpha}_\iota}.$$

Thus, the decryption and the check of the condition (b) fail since $\mathbf{c}_0^\top\mathbf{a}^\perp \neq 0$ holds with overwhelming probability. In other words, if $\mathbf{c}_0$ lives in the span of $\mathbf{A}$ and $\mathbf{c}_0^\top\mathbf{a}^\perp = 0$ holds, the decryption and the check of the condition (b) succeed by using the semi-functional $\mathsf{sk}_{y,\iota}$.

Proof. We introduce a *critical decryption query* which is $\mathcal{A}$'s decryption query on $(y, \mathsf{ct}_x = ((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, \cdots))$ such that ct_x is valid, $\mathsf{ct}_x \notin \mathcal{L}$ holds, and the discrete logarithm of $\mathsf{ct}_{0,0}$ does not live in the span of $\mathbf{A}$. Similarly, we say that $\mathcal{A}$'s evaluation query on $(y, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell\in[L]})$ a *critical evaluation query* if there is an index ℓ such that ℓ-th ciphertext is as above. We introduce a *critical homomorphic evaluation key reveal query* which is $\mathcal{A}$'s homomorphic evaluation key reveal query on y such that $f(x^\star, y) = 1$. We introduce a *dependent evaluation query* which is $\mathcal{A}$'s evaluation query whose answer is stored in the list $\mathcal{L}$ by $\mathcal{C}$. Otherwise, we call $\mathcal{A}$'s evaluation query an *independent evaluation query*.

To prove Theorem 4, we divide $\mathcal{A}$'s attack strategies into two types, where the Type-1 $\mathcal{A}$ makes at least one critical homomorphic evaluation key reveal query in Phase 1, while the Type-2 $\mathcal{A}$ does not make such queries in Phase 1. By definition, Type-1 and Type-2 are mutually exclusive and cover all possible strategies of $\mathcal{A}$. At first, we prove the adaptive KH-CCA security against the Type-2 $\mathcal{A}$ by using the following sequence of games.

- Game_0: This is the adaptive KH-CCA security game. Hereafter, let $\mathsf{ct}^\star_{x^\star} = ((\mathsf{ct}^\star_{0,i})_{i\in[0,w_1]}, (\mathsf{ct}^\star_{1,t})_{t\in[w_3]}, \mathsf{ct}^\star_T, \pi^\star)$ denote a challenge ciphertext for a challenge ciphertext attribute $x^\star$ and a message $\mu^\star_{\mathsf{coin}}$.

- Game_1: This is the same as Game_0 except that a collision does not occur for a hash function H among all ciphertexts that appeared in the security game.

  The collision resistance of H ensures that $\mathsf{Game}_0 \approx_c \mathsf{Game}_1$ holds.

- Game_2. This is the same as Game_1 except $\mathcal{C}$'s behavior upon $\mathcal{A}$'s challenge query and dependent evaluation queries so that the distribution of evaluated ciphertexts in $\mathcal{L}$ are independent of pre-evaluated ciphertexts. Specifically, upon $\mathcal{A}$'s challenge query on $(x^\star, \mu^\star_0, \mu^\star_1)$, $\mathcal{C}$ sends $\mathsf{ct}^\star_{x^\star} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^\star, \mu^\star_{\mathsf{coin}})$ to $\mathcal{A}$ as in Game_1. Moreover, $\mathcal{C}$ stores a pair $(\mu^\star_{\mathsf{coin}}, \mathsf{ct}^\star_{x^\star})$ in the list $\mathcal{L}$ to indicate that $\mathsf{ct}^\star_{x^\star}$ is an encryption of $\mu^\star_{\mathsf{coin}}$. Upon $\mathcal{A}$'s dependent evaluation query on $(y, (\mathsf{ct}^{(\ell)}_{x^\star})_{\ell\in[L]})$, for all indices ℓ such that $\mathsf{ct}^{(\ell)}_{x^\star} \in \mathcal{L}$, $\mathcal{C}$ retrieves pairs $(\mu^{(\ell)}, \mathsf{ct}^{(\ell)}_{x^\star})$ from $\mathcal{L}$

and runs $\mu^{(\ell)} \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{KGen}(\mathsf{mpk}, \mathsf{msk}, y), \mathsf{ct}_{x^\star}^{(\ell)})$ for all the other indices. Then, $\mathcal{C}$ sends $\mathsf{ct}_{x^\star} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^\star, \prod_{\ell\in[L]} \mu^{(\ell)})$ to $\mathcal{A}$ as the answer of the evaluation query and stores a pair $(\prod_{\ell\in[L]} \mu^{(\ell)}, \mathsf{ct}_{x^\star})$ in $\mathcal{L}$ to indicate that $\mathsf{ct}_{x^\star}$ is an encryption of $\prod_{\ell\in[L]} \mu^{(\ell)}$. From $\mathcal{A}$'s view, Game_1 and Game_2 follow the same distribution.

Let D denote the number of ciphertexts in $\mathcal{L}$ at the end of the game, where the challenge ciphertext $\mathsf{ct}_{x^\star}^\star$ is the first ciphertext and $\mathcal{A}$ makes $D-1$ dependent evaluation queries. From now on, we change a distribution of d-th ciphertext $\mathsf{ct}_x = (\cdots, \mathsf{ct}_T, \cdots)$ in $\mathcal{L}$ for $d \in [D]$ one by one so that ct_T is independent of the other elements of $\mathsf{ct}_{x^\star}$ and distributed uniformly at random over $\mathbb{G}_T$. For this purpose, we use the following sequence of games $\mathsf{Game}_{3,d}, \ldots, \mathsf{Game}_{9,d}$ for $d \in [D]$, where $\mathsf{Game}_{9,0} = \mathsf{Game}_2$ and the proof terminates in $\mathsf{Game}_{6,D}$. In all the games, only d-th ciphertext in $\mathcal{L}$ may be semi-functional, while all the other ciphertexts follow the normal distribution. Hereafter, let $\widetilde{\mathsf{ct}}_{x^\star}$ denote the d-th ciphertext in the list $\mathcal{L}$.

- $\mathsf{Game}_{3,d}$: This is the same as $\mathsf{Game}_{9,d-1}$ except that $\mathcal{C}$ answers d-th ciphertext $\widetilde{\mathsf{ct}}_{x^\star}$ in $\mathcal{L}$ as the semi-functional ciphertext to answer $\mathcal{A}$'s query.

  We can prove $\mathsf{Game}_{9,d-1} \approx_c \mathsf{Game}_{3,d}$ under the matrix DDH assumption over $\mathbb{G}_1$ by following the proofs of Π_{ABE} [AC16, AC17, CGW15].

- $\mathsf{Game}_{4,d}$: This is the same as $\mathsf{Game}_{3,d}$ except that $\mathcal{C}$ answers semi-functional $\mathsf{sk}_{y,0}$ to answer $\mathcal{A}$'s decryption key reveal queries on y.

  Since $f(x^\star, y) = 0$ holds due to the definition of the KH-CCA security game, we can prove $\mathsf{Game}_{3,d} \approx_c \mathsf{Game}_{4,d}$ under the matrix DDH assumption over $\mathbb{G}_2$ and the q-ratio assumption by following the proofs of Π_{ABE} [AC16, AC17, CGW15].

- $\mathsf{Game}_{5,d}$: This is the same as $\mathsf{Game}_{4,d}$ except that $\mathcal{C}$ uses semi-functional $\mathsf{sk}_{y,1}, \mathsf{sk}_{y,2}$ to answer $\mathcal{A}$'s decryption key reveal queries and homomorphic evaluation key reveal queries on y until the first critical homomorphic evaluation key reveal query. Thus, once $\mathcal{A}$ makes the critical homomorphic evaluation key reveal query, $\mathcal{C}$ uses normal $\mathsf{sk}_{y,1}, \mathsf{sk}_{y,2}$ to answer $\mathcal{A}$'s subsequent decryption key reveal queries and homomorphic evaluation key reveal queries.

  Since $f(x^\star, y) = 0$ holds due to the definitions of the KH-CCA security game and $\mathsf{Game}_{5,d}$, we can prove $\mathsf{Game}_{4,d} \approx_c \mathsf{Game}_{5,d}$ under the matrix DDH assumption over $\mathbb{G}_2$ and the q-ratio assumption by following the proofs of Π_{ABE} [AC16, AC17, CGW15].

- $\mathsf{Game}_{6,d}$: This is the same as $\mathsf{Game}_{5,d}$ except that $\mathcal{C}$ answers d-th ciphertext $\widetilde{\mathsf{ct}}_{x^\star} = ((\widetilde{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, (\widetilde{\mathsf{ct}}_{1,t})_{t\in[w_3]}, \widetilde{\mathsf{ct}}_T, \widetilde{\pi})$ in $\mathcal{L}$ by setting $\widetilde{\mathsf{ct}}_T \leftarrow_R \mathbb{G}_T$ whose distribution is independent of $((\widetilde{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, (\widetilde{\mathsf{ct}}_{1,t})_{t\in[w_3]}, \widetilde{\pi})$. In other words, the d-th ciphertext in $\mathcal{L}$ is independent of $\mu^\star_{\mathsf{coin}}$. Thus, in $\mathsf{Game}_{6,D}$, $\mathcal{A}$'s advantage is exactly 0 since all $\mathcal{C}$'s answers are independent of $\mu^\star_{\mathsf{coin}}$.

  After we describe the game sequence, we will show that $\mathsf{Game}_{5,d}$ and $\mathsf{Game}_{6,d}$ follow the same distribution from $\mathcal{A}$'s view with overwhelming probability.

- $\mathsf{Game}_{7,d}$: This is the same as $\mathsf{Game}_{6,d}$ except that $\mathcal{C}$ uses normal $\mathsf{sk}_{y,1}, \mathsf{sk}_{y,2}$ to answer $\mathcal{A}$'s decryption key reveal queries and homomorphic evaluation key reveal queries on y.

  By following the proof of $\mathsf{Game}_{4,d} \approx_c \mathsf{Game}_{5,d}$, $\mathsf{Game}_{6,d} \approx_c \mathsf{Game}_{7,d}$ holds under the matrix DDH assumption over $\mathbb{G}_2$ and the q-ratio assumption.

- $\mathsf{Game}_{8,d}$: This is the same as $\mathsf{Game}_{7,d}$ except that $\mathcal{C}$ uses normal $\mathsf{sk}_{y,0}$ to answer $\mathcal{A}$'s decryption key reveal queries on y.

  By following the proof of $\mathsf{Game}_{3,d} \approx_c \mathsf{Game}_{4,d}$, $\mathsf{Game}_{7,d} \approx_c \mathsf{Game}_{8,d}$ holds under the matrix DDH assumption over $\mathbb{G}_2$ and the q-ratio assumption.

- $\mathsf{Game}_{9,d}$: This is the same as $\mathsf{Game}_{8,d}$ except that $\mathcal{C}$ answers d-th ciphertext $\widetilde{\mathsf{ct}}_{x^\star} = ((\widetilde{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, (\widetilde{\mathsf{ct}}_{1,t})_{t\in[w_3]}, \widetilde{\mathsf{ct}}_T, \widetilde{\pi})$ in $\mathcal{L}$ so that $((\widetilde{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, (\widetilde{\mathsf{ct}}_{1,t})_{t\in[w_3]}, \widetilde{\pi})$ follows the normal distribution.

  By following the proof of $\mathsf{Game}_{9,d-1} \approx_c \mathsf{Game}_{3,d}$, $\mathsf{Game}_{8,d} \approx_c \mathsf{Game}_{9,d}$ holds under the matrix DDH assumption over $\mathbb{G}_1$.

We complete the proof against the Type-2 $\mathcal{A}$ by showing that $\mathsf{Game}_{5,d}$ and $\mathsf{Game}_{6,d}$ follow the same distribution from the $\mathcal{A}$'s view. For this purpose, we simulate $\mathcal{C}$ of $\mathsf{Game}_{5,d}$ by using $\mathbf{u}_0$ only for creating the d-th ciphertext $\widetilde{\mathsf{ct}}_{x^\star}$ in $\mathcal{L}$ and using $\mathbf{u}_1, \mathbf{u}_2$ only after the first critical homomorphic evaluation key reveal query. We sample $(\mathbf{A}, \mathbf{a}^\perp), (\mathbf{B}, \mathbf{b}^\perp) \leftarrow \mathcal{D}_k$ and uniformly random matrices $\mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow_R \mathbb{Z}_p^{(k+1)\times(k+1)}$. For $\iota \in [0,2]$, we sample random vectors $\widehat{\mathbf{u}}_\iota \leftarrow_R \mathbb{Z}_p^{k+1}$ and $\alpha_\iota \leftarrow_R \mathbb{Z}_p$, and set

$$\mathbf{u}_\iota = \widehat{\mathbf{u}}_\iota + \alpha_\iota \mathbf{a}^\perp.$$

Then, we compute mpk in the same way as the real scheme except that

$$[\mathbf{A}^\top \widehat{\mathbf{u}}_\iota]_T = [\mathbf{A}^\top(\mathbf{u}_\iota - \alpha_\iota \mathbf{a}^\perp)]_T = [\mathbf{A}^\top \mathbf{u}_\iota]_T \cdot [\mathbf{A}^\top \cdot \mathbf{a}^\perp]_T^{-\alpha_\iota} = [\mathbf{A}^\top \mathbf{u}_\iota]_T$$

which distributes in the same way as the real scheme although we do not use $\mathbf{u}_\iota$ for $\iota \in [0,2]$. We answer $\mathcal{A}$'s decryption key reveal queries on y and decryption queries on (y, ct_x) by using semi-functional ABE secret keys $\mathsf{sk}_{y,\iota}$ which are computed from $\widehat{\mathbf{u}}_\iota$ for $\iota \in [0,2]$ even when $f(x^\star, y) = 1$ holds. Similarly, before the first critical homomorphic evaluation key reveal query, we answers $\mathcal{A}$'s homomorphic evaluation key reveal queries on y and independent evaluation queries on $(y, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell\in[L]})$ by using semi-functional ABE secret keys $\mathsf{sk}_{y,\iota}$ which are computed from $\widehat{\mathbf{u}}_\iota$ for $\iota \in [2]$ even when $f(x^\star, y) = 1$ holds. In contrast, from the first critical homomorphic evaluation key reveal query, we answer $\mathcal{A}$'s homomorphic evaluation key reveal queries on y and independent evaluation queries on $(y, (\mathsf{ct}^{(\ell)}_{x^{(\ell)}})_{\ell\in[L]})$ by using normal ABE secret keys $\mathsf{sk}_{y,\iota}$ which are computed from $\mathbf{u}_\iota$ for $\iota \in [2]$ as in $\mathsf{Game}_{5,d}$. The answers of the decryption key reveal queries and the homomorphic evaluation key reveal queries before the first critical homomorphic evaluation key reveal query are properly distributed since ABE secret keys $\mathsf{sk}_{y,\iota}$ are semi-functional. The answers of the homomorphic evaluation key reveal queries from the first critical homomorphic evaluation key reveal query are properly distributed since ABE secret keys $\mathsf{sk}_{y,\iota}$ are normal. If all $\mathcal{A}$'s decryption queries and independent evaluation queries before the first critical homomorphic evaluation key reveal query are not critical, their answers are properly distributed although we do not use $\mathbf{u}_\iota$ but $\widehat{\mathbf{u}}_\iota$ for $\iota \in [0,2]$. We will show that the claim holds with overwhelming probability.

We complete the description of the simulation by showing how to answer $\mathcal{A}$'s challenge query and dependent evaluation queries. We explain the case of $d > 1$, where the proof for $d = 1$ is essentially the same. Upon $\mathcal{A}$'s challenge query on $(x^\star, \mu_0^\star, \mu_1^\star)$, we sample $\mathsf{coin} \leftarrow_R \{0,1\}$, create a normal ciphertext $\mathsf{ct}^\star_{x^\star} = (\cdots, \mathsf{ct}^\star_T, \cdots)$ except $\mathsf{ct}^\star_T \leftarrow_R \mathbb{G}_T$, send $\mathsf{ct}^\star_{x^\star}$ to $\mathcal{A}$, and store $(\mu^\star_{\mathsf{coin}}, \mathsf{ct}^\star_{x^\star})$. To create an encryption of μ before the d-th ciphertext in $\mathcal{L}$, we compute normal ciphertexts $\mathsf{ct}_{x^\star} = (\cdots, \mathsf{ct}_T, \cdots)$ except $\mathsf{ct}_T \leftarrow_R \mathbb{G}_T$. To create an encryption of μ as the d-th ciphertext in $\mathcal{L}$, we sample $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{w_1+w_2} \leftarrow_R \mathbb{Z}_p^{k+1}$ and compute a semi-functional ciphertext $\widetilde{\mathsf{ct}}_{x^\star} = ((\widetilde{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, (\widetilde{\mathsf{ct}}_{1,t})_{t\in[w_3]}, \widetilde{\mathsf{ct}}_T, \widetilde{\pi})$;

$$\widetilde{\mathsf{ct}}_{0,i} = [\mathbf{c}_i]_1, \qquad \widetilde{\mathsf{ct}}_{1,t} = \prod_{i\in[w_2]} [\mathbf{c}_{w_1+i}]_1^{\eta_{t,i}} \cdot \prod_{i\in[0,w_1], j\in[n]} [\mathbf{W}_j^\top \mathbf{c}_i]_1^{\eta_{t,i,j}},$$
$$\widetilde{\mathsf{ct}}_T = \mu \cdot [\mathbf{c}_0^\top \mathbf{u}_0]_T, \qquad \widetilde{\pi} = [\mathbf{c}_0^\top(\mathbf{u}_1 + \tilde{h}\cdot \mathbf{u}_2)]_T,$$

where $\tilde{h} = H((\widetilde{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, \widetilde{\mathsf{ct}}_T)$ as in $\mathsf{Game}_{5,d}$. To create an encryption of μ after the d-th ciphertext in $\mathcal{L}$, we compute normal ciphertexts $\mathsf{ct}_{x^\star}$. Observe that the d-th ciphertext in $\mathcal{L}$ is the only element which we use $\mathbf{u}_0$ to create and

$$\widetilde{\mathsf{ct}}_T = \mu\cdot[\mathbf{c}_0^\top \mathbf{u}_0]_T = \mu\cdot[\mathbf{c}_0^\top(\widehat{\mathbf{u}}_0 + \alpha_0 \mathbf{a}^\perp)]_T = \mu\cdot[\mathbf{c}_0^\top \widehat{\mathbf{u}}_0]_T \cdot [\mathbf{c}_0^\top \mathbf{a}^\perp]_T^{\alpha_0}$$

holds. When $\mathbf{c}_0$ does not live in the span of $\mathbf{A}$ that happens with overwhelming probability $1-1/p$, $[\mathbf{c}_0^\top \mathbf{a}^\perp]_T$ is a generator of $\mathbb{G}_T$. Since ct_T is the only element whose distribution depends on $\alpha_0 \leftarrow_R \mathbb{Z}_p$ from $\mathcal{A}$'s view, $[\mathbf{c}_0^\top \mathbf{a}^\perp]_T^{\alpha_0}$ is distributed uniformly at random over $\mathbb{G}_T$. As a result, the d-th ciphertext in $\mathcal{L}$ follows the same distribution as in $\mathsf{Game}_{6,d}$.

We complete the proof against the Type-2 $\mathcal{A}$ by showing that all $\mathcal{A}$'s decryption queries and independent evaluation queries before the first critical homomorphic evaluation key reveal query are not critical with overwhelming probability. First of all, the dual system proofs of ABE schemes [AC16, AC17, CGW15] inherently imply that $\mathcal{A}$ by itself cannot create a ciphertext $\mathsf{ct}_x = ((\mathsf{ct}_{0,i})_{i\in[0,w_1]}, \cdots)$ such that the discrete logarithm of $\mathsf{ct}_{0,0}$ does not live in the span of $\mathbf{A}$ and the condition (a) holds. Specifically, $\mathcal{A}$ cannot create such ciphertexts for all x in Phase 1 and those for all $x \neq x^\star$ in Phase 2. Otherwise, the proofs [AC16, AC17, CGW15] fail since $\mathcal{A}$ can distinguish normal and semi-functional ABE secret keys. Moreover, the only ciphertext as above which we created is the semi-functional d-th ciphertext $\widetilde{\mathsf{ct}}_{x^\star}$ in $\mathcal{L}$. Therefore, the only way for $\mathcal{A}$ to make the critical queries is evaluating the d-th ciphertext $\widetilde{\mathsf{ct}}_{x^\star}$ in $\mathcal{L}$. The definition of the $\mathsf{KH\text{-}CCA}$ security game ensures that $\mathcal{A}$ cannot make decryption queries on $(y, \mathsf{ct}_{x^\star})$ such that $f(x^\star, y) = 1$ after the first critical homomorphic evaluation key reveal query. In other words, $\mathcal{A}$ has to evaluate the d-th ciphertext $\widetilde{\mathsf{ct}}_{x^\star}$ in $\mathcal{L}$ and create a ciphertext $\overline{\mathsf{ct}}_{x^\star} = ((\overline{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, (\overline{\mathsf{ct}}_{1,t})_{t\in[w_3]}, \overline{\mathsf{ct}}_T, \overline{\pi})$ without receiving hk_y such that $f(x^\star, y) = 1$. By following the discussion of the Cramer-Shoup cryptosystem [CS98], we can conclude that $\mathcal{A}$ cannot complete the task since $\mathcal{A}$ cannot create a valid $\overline{\pi}$ satisfying the condition (b) even when $\mathcal{A}$ is computationally unbounded. Here, the modification of Game_1 ensures that $H((\overline{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, \overline{\mathsf{ct}}_T) \neq H((\widetilde{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, \widetilde{\mathsf{ct}}_T) = \tilde{h}$ holds. Observe that the d-th ciphertext $\widetilde{\mathsf{ct}}_{x^\star} = ((\widetilde{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, (\widetilde{\mathsf{ct}}_{1,t})_{t\in[w_3]}, \widetilde{\mathsf{ct}}_T, \widetilde{\pi})$ in $\mathcal{L}$ is the only element which we use $\mathbf{u}_1, \mathbf{u}_2$ to create and it holds that

$$\begin{aligned}\widetilde{\pi} &= [\mathbf{c}_0^\top(\mathbf{u}_1 + \tilde{h}\cdot\mathbf{u}_2)]_T = [\mathbf{c}_0^\top(\widehat{\mathbf{u}}_1 + \alpha_1\mathbf{a}^\perp + \tilde{h}\cdot(\widehat{\mathbf{u}}_2 + \alpha_2\mathbf{a}^\perp))]_T \\ &= [\mathbf{c}_0^\top(\widehat{\mathbf{u}}_1 + \tilde{h}\cdot\widehat{\mathbf{u}}_2)]_T \cdot [\mathbf{c}_0^\top\mathbf{a}^\perp]_T^{\alpha_1 + \tilde{h}\cdot\alpha_2}.\end{aligned}$$

Thus, the unbounded $\mathcal{A}$ learns that

$$\alpha_1 + \tilde{h}\cdot\alpha_2 = \log_{[\mathbf{c}_0^\top \mathbf{a}^\perp]_T}(\pi/[\mathbf{c}_0^\top(\widehat{\mathbf{u}}_1 + \tilde{h}\cdot\widehat{\mathbf{u}}_2)]_T)$$

holds. Then, there are p possible candidates of a pair (α_1, α_2). For unbounded $\mathcal{A}$, making critical queries is equivalent to learn (α_1, α_2). However, the only way for $\mathcal{A}$ to learn (α_1, α_2) is making decryption queries and evaluation queries by modifying the d-th ciphertext in $\mathcal{L}$ since the queries do not reveal information of (α_1, α_2) when they are not critical. If $\mathcal{A}$ makes queries with a ciphertext $\overline{\mathsf{ct}}_{x^\star} = ((\overline{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, (\overline{\mathsf{ct}}_{1,t})_{t\in[w_3]}, \overline{\mathsf{ct}}_T, \overline{\pi})$ and the answers are $\perp$, $\mathcal{A}$ can learn that

$$\alpha_1 + \bar{h} \cdot \alpha_2 \neq \log_{e(\overline{\mathsf{ct}}_{0,0},[\mathbf{a}^\perp]_2)}(\overline{\pi}/e(\overline{\mathsf{ct}}_{0,0}, [\widehat{\mathbf{u}}_1 + \bar{h} \cdot \widehat{\mathbf{u}}_2)]_2))$$

holds, where $\bar{h} = H((\overline{\mathsf{ct}}_{0,i})_{i\in[0,w_1]}, \overline{\mathsf{ct}}_T)$. However, $\mathcal{A}$ can eliminate only one candidate of (α_1, α_2) by one query although there are exponentially many candidates of (α_1, α_2). Therefore, we have proved the claim.

The proof against the Type-1 $\mathcal{A}$ is essentially the same. Specifically, we use the same game sequence except that we skip $\mathsf{Game}_{5,d}$ and $\mathsf{Game}_{7,d}$ so that we do not change $\mathsf{sk}_{y,1}, \mathsf{sk}_{y,2}$ to be semi-functional throughout the game. The definition of the KH-CCA security game and the Type-1 strategy ensures that $\mathcal{A}$ is allowed to make decryption queries on (y, ct_x) such that $f(x^\star, y) = 1$ only in Phase 1. By following the discussion against the Type-2 $\mathcal{A}$, the dual system proofs of ABE schemes [AC16, AC17, CGW15] inherently imply that $\mathcal{A}$ cannot make critical decryption queries on (y, ct_x) for all x in Phase 1 and those for all $x \neq x^\star$ in Phase 2. Therefore, we can simulate the challenger of $\mathsf{Game}_{4,d}$ by using $\mathbf{u}_0$ only for creating the d-th ciphertext in $\mathcal{L}$; thus, $\mathsf{Game}_{4,d}$ and $\mathsf{Game}_{6,d}$ follow the same distribution from $\mathcal{A}$'s view with overwhelming probability.

Summarizing the discussion so far, we complete the proof. □

Acknowledgement. We would like to thank anonymous reviewers of PKC 2024.

References

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer, Heidelberg, May / June 2010. https://doi.org/10.1007/978-3-642-13190-5_28

[ABS17] Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt. Generic transformations of predicate encodings: Constructions and applications. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 36–66. Springer, Heidelberg, August 2017. https://doi.org/10.1007/978-3-319-63688-7_2

[AC16] Shashank Agrawal and Melissa Chase. A study of pair encodings: Predicate encryption in prime order groups. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A: 13th Theory of Cryptography Conference, Part II*, volume 9563 of *Lecture Notes in Computer Science*, pages 259–288. Springer, Heidelberg, January 2016. https://doi.org/10.1007/978-3-662-49099-0_10

[AC17] Shashank Agrawal and Melissa Chase. Simplifying design and analysis of complex predicate encryption schemes. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 627–656. Springer, Heidelberg, April / May 2017. https://doi.org/10.1007/978-3-319-56620-7_22

[AJJM20] Prabhanjan Ananth, Abhishek Jain, Zhengzhong Jin, and Giulio Malavolta. Multi-key fully-homomorphic encryption in the plain model. In Rafael Pass and Krzysztof

Pietrzak, editors, *TCC 2020: 18th Theory of Cryptography Conference, Part I*, volume 12550 of *Lecture Notes in Computer Science*, pages 28–57. Springer, Heidelberg, November 2020. https://doi.org/10.1007/978-3-030-64375-1_2

[Amb21] Miguel Ambrona. Generic negation of pair encodings. In Juan Garay, editor, *PKC 2021: 24th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 12711 of *Lecture Notes in Computer Science*, pages 120–146. Springer, Heidelberg, May 2021. https://doi.org/10.1007/978-3-030-75248-4_5

[Att14] Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 557–577. Springer, Heidelberg, May 2014. https://doi.org/10.1007/978-3-642-55220-5_31

[Att16] Nuttapong Attrapadung. Dual system encryption framework in prime-order groups via computational pair encodings. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 591–623. Springer, Heidelberg, December 2016. https://doi.org/10.1007/978-3-662-53890-6_20

[Att19] Nuttapong Attrapadung. Unbounded dynamic predicate compositions in attribute-based encryption. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 34–67. Springer, Heidelberg, May 2019. https://doi.org/10.1007/978-3-030-17653-2_2

[AY15] Nuttapong Attrapadung and Shota Yamada. Duality in ABE: Converting attribute based encryption for dual predicate and dual policy via computational encodings. In Kaisa Nyberg, editor, *Topics in Cryptology – CT-RSA 2015*, volume 9048 of *Lecture Notes in Computer Science*, pages 87–105. Springer, Heidelberg, April 2015. https://doi.org/10.1007/978-3-319-16715-2_5

[BB04] Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer, Heidelberg, August 2004. https://doi.org/10.1007/978-3-540-28628-8_27

[BBC+18] Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafaël del Pino, Jens Groth, and Vadim Lyubashevsky. Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 669–699. Springer, Heidelberg, August 2018. https://doi.org/10.1007/978-3-319-96881-0_23

[BCC+17] Nir Bitansky, Ran Canetti, Alessandro Chiesa, Shafi Goldwasser, Huijia Lin, Aviad Rubinstein, and Eran Tromer. The hunting of the SNARK. *Journal of Cryptology*, 30(4):989–1066, October 2017. https://doi.org/10.1007/s00145-016-9241-9

[BCCT13] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. Recursive composition and bootstrapping for SNARKS and proof-carrying data. In Dan Boneh, Tim

Roughgarden, and Joan Feigenbaum, editors, *45th Annual ACM Symposium on Theory of Computing*, pages 111–120. ACM Press, June 2013. https://doi.org/10.1145/2488608.2488623

[BCTW16] Zvika Brakerski, David Cash, Rotem Tsabary, and Hoeteck Wee. Targeted homomorphic attribute-based encryption. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B: 14th Theory of Cryptography Conference, Part II*, volume 9986 of *Lecture Notes in Computer Science*, pages 330–360. Springer, Heidelberg, October / November 2016. https://doi.org/10.1007/978-3-662-53644-5_13

[BGG+14] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 533–556. Springer, Heidelberg, May 2014. https://doi.org/10.1007/978-3-642-55220-5_30

[BGI+01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 1–18. Springer, Heidelberg, August 2001. https://doi.org/10.1007/3-540-44647-8_1

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS 2012: 3rd Innovations in Theoretical Computer Science*, pages 309–325. Association for Computing Machinery, January 2012. https://doi.org/10.1145/2090236.2090262

[Ble98] Daniel Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO'98*, volume 1462 of *Lecture Notes in Computer Science*, pages 1–12. Springer, Heidelberg, August 1998. https://doi.org/10.1007/BFb0055716

[BN08] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *Journal of Cryptology*, 21(4):469–491, October 2008. https://doi.org/10.1007/s00145-008-9026-x

[Bra12] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 868–886. Springer, Heidelberg, August 2012. https://doi.org/10.1007/978-3-642-32009-5_50

[BV11a] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In Rafail Ostrovsky, editor, *52nd Annual Symposium on Foundations of Computer Science*, pages 97–106. IEEE Computer Society Press, October 2011. https://doi.org/10.1109/FOCS.2011.12

[BV11b] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer*

Science, pages 505–524. Springer, Heidelberg, August 2011. https://doi.org/10.1007/978-3-642-22792-9_29

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Lattice-based FHE as secure as PKE. In Moni Naor, editor, *ITCS 2014: 5th Conference on Innovations in Theoretical Computer Science*, pages 1–12. Association for Computing Machinery, January 2014. https://doi.org/10.1145/2554797.2554799

[CG17] Jie Chen and Junqing Gong. ABE with tag made easy - concise framework and new instantiations in prime-order groups. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 35–65. Springer, Heidelberg, December 2017. https://doi.org/10.1007/978-3-319-70697-9_2

[CGW15] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 595–624. Springer, Heidelberg, April 2015. https://doi.org/10.1007/978-3-662-46803-6_20

[CHK04] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 207–222. Springer, Heidelberg, May 2004. https://doi.org/10.1007/978-3-540-24676-3_13

[CLL+14] Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Hoeteck Wee. Shorter identity-based encryption via asymmetric pairings. *Des. Codes Cryptogr.*, 73(3):911–947, 2014. https://doi.org/10.1007/S10623-013-9834-3

[CM15] Michael Clear and Ciaran McGoldrick. Multi-identity and multi-key leveled FHE from learning with errors. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 630–656. Springer, Heidelberg, August 2015. https://doi.org/10.1007/978-3-662-48000-7_31

[CMS19] Alessandro Chiesa, Peter Manohar, and Nicholas Spooner. Succinct arguments in the quantum random oracle model. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019: 17th Theory of Cryptography Conference, Part II*, volume 11892 of *Lecture Notes in Computer Science*, pages 1–29. Springer, Heidelberg, December 2019. https://doi.org/10.1007/978-3-030-36033-7_1

[CRRV17] Ran Canetti, Srinivasan Raghuraman, Silas Richelson, and Vinod Vaikuntanathan. Chosen-ciphertext secure fully homomorphic encryption. In Serge Fehr, editor, *PKC 2017: 20th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 10175 of *Lecture Notes in Computer Science*, pages 213–240. Springer, Heidelberg, March 2017. https://doi.org/10.1007/978-3-662-54388-7_8

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *Advances in*

Cryptology – CRYPTO'98, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer, Heidelberg, August 1998. https://doi.org/10.1007/BFb0055717

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64. Springer, Heidelberg, April / May 2002. https://doi.org/10.1007/3-540-46035-7_4

[CW14] Jie Chen and Hoeteck Wee. Dual system groups and its applications — compact HIBE and more. Cryptology ePrint Archive, Report 2014/265, 2014. https://eprint.iacr.org/2014/265.

[DGM15] Ricardo Dahab, Steven Galbraith, and Eduardo Morais. Adaptive key recovery attacks on NTRU-based somewhat homomorphic encryption schemes. In Anja Lehmann and Stefan Wolf, editors, *ICITS 15: 8th International Conference on Information Theoretic Security*, volume 9063 of *Lecture Notes in Computer Science*, pages 283–296. Springer, Heidelberg, May 2015. https://doi.org/10.1007/978-3-319-17470-9_17

[EHK+17] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Luis Villar. An algebraic framework for Diffie-Hellman assumptions. *Journal of Cryptology*, 30(1):242–288, January 2017. https://doi.org/10.1007/s00145-015-9220-6

[EHN+18] Keita Emura, Goichiro Hanaoka, Koji Nuida, Go Ohtake, Takahiro Matsuda, and Shota Yamada. Chosen ciphertext secure keyed-homomorphic public-key cryptosystems. *Des. Codes Cryptogr.*, 86(8):1623–1683, 2018. https://doi.org/10.1007/S10623-017-0417-6

[EHO+13] Keita Emura, Goichiro Hanaoka, Go Ohtake, Takahiro Matsuda, and Shota Yamada. Chosen ciphertext secure keyed-homomorphic public-key encryption. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013: 16th International Conference on Theory and Practice of Public Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 32–50. Springer, Heidelberg, February / March 2013. https://doi.org/10.1007/978-3-642-36362-7_3

[Emu21] Keita Emura. On the security of keyed-homomorphic PKE: preventing key recovery attacks and ciphertext validity attacks. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 104-A(1):310–314, 2021. https://doi.org/10.1587/TRANSFUN.2020EAL2039

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st Annual ACM Symposium on Theory of Computing*, pages 169–178. ACM Press, May / June 2009. https://doi.org/10.1145/1536414.1536440

[GGPR13] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct NIZKs without PCPs. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 626–645. Springer, Heidelberg, May 2013. https://doi.org/10.1007/978-3-642-38348-9_37

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer, Heidelberg, August 2013. https://doi.org/10.1007/978-3-642-40041-4_5

[HK17] Ryo Hiromasa and Yutaka Kawai. Dynamic multi target homomorphic attribute-based encryption. In Máire O'Neill, editor, *16th IMA International Conference on Cryptography and Coding*, volume 10655 of *Lecture Notes in Computer Science*, pages 25–43. Springer, Heidelberg, December 2017.

[JR15] Charanjit S. Jutla and Arnab Roy. Dual-system simulation-soundness with applications to UC-PAKE and more. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 630–655. Springer, Heidelberg, November / December 2015. https://doi.org/10.1007/978-3-662-48797-6_26

[LDM+16] Junzuo Lai, Robert H. Deng, Changshe Ma, Kouichi Sakurai, and Jian Weng. CCA-secure keyed-fully homomorphic encryption. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *PKC 2016: 19th International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 9614 of *Lecture Notes in Computer Science*, pages 70–98. Springer, Heidelberg, March 2016. https://doi.org/10.1007/978-3-662-49384-7_4

[Lew12] Allison B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 318–335. Springer, Heidelberg, April 2012. https://doi.org/10.1007/978-3-642-29011-4_20

[LMSV12] Jake Loftus, Alexander May, Nigel P. Smart, and Frederik Vercauteren. On CCA-secure somewhat homomorphic encryption. In Ali Miri and Serge Vaudenay, editors, *SAC 2011: 18th Annual International Workshop on Selected Areas in Cryptography*, volume 7118 of *Lecture Notes in Computer Science*, pages 55–72. Springer, Heidelberg, August 2012. https://doi.org/10.1007/978-3-642-28496-0_4

[LPJY14] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 514–532. Springer, Heidelberg, May 2014. https://doi.org/10.1007/978-3-642-55220-5_29

[LTV12] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In Howard J. Karloff and Toniann Pitassi, editors, *44th Annual ACM Symposium on Theory of Computing*, pages 1219–1234. ACM Press, May 2012. https://doi.org/10.1145/2213977.2214086

[MBKM19] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. Sonic: Zero-knowledge SNARKs from linear-size universal and updatable structured reference strings. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *ACM CCS 2019: 26th Conference on Computer and Communications Security*, pages 2111–2128. ACM Press, November 2019. https://doi.org/10.1145/3319535.3339817

[ML19] Xuecheng Ma and Dongdai Lin. Multi-identity IBFHE and multi-attribute ABFHE in the standard model. In Kwangsu Lee, editor, *ICISC 18: 21st International Conference on Information Security and Cryptology*, volume 11396 of *Lecture Notes in Computer Science*, pages 69–84. Springer, Heidelberg, November 2019. https://doi.org/10.1007/978-3-030-12146-4_5

[MN22] Yusaku Maeda and Koji Nuida. Chosen ciphertext secure keyed two-level homomorphic encryption. In Khoa Nguyen, Guomin Yang, Fuchun Guo, and Willy Susilo, editors, *ACISP 22: 27th Australasian Conference on Information Security and Privacy*, volume 13494 of *Lecture Notes in Computer Science*, pages 209–228. Springer, Heidelberg, November 2022. https://doi.org/10.1007/978-3-031-22301-3_11

[MW16] Pratyay Mukherjee and Daniel Wichs. Two round multiparty computation via multi-key FHE. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 735–763. Springer, Heidelberg, May 2016. https://doi.org/10.1007/978-3-662-49896-5_26

[PD20] Tapas Pal and Ratna Dutta. Chosen-ciphertext secure multi-identity and multi-attribute pure FHE. In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *CANS 20: 19th International Conference on Cryptology and Network Security*, volume 12579 of *Lecture Notes in Computer Science*, pages 387–408. Springer, Heidelberg, December 2020. https://doi.org/10.1007/978-3-030-65411-5_19

[PS16] Chris Peikert and Sina Shiehian. Multi-key FHE from LWE, revisited. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B: 14th Theory of Cryptography Conference, Part II*, volume 9986 of *Lecture Notes in Computer Science*, pages 217–238. Springer, Heidelberg, October / November 2016. https://doi.org/10.1007/978-3-662-53644-5_9

[SET22] Shingo Sato, Keita Emura, and Atsushi Takayasu. Keyed-fully homomorphic encryption without indistinguishability obfuscation. In Giuseppe Ateniese and Daniele Venturi, editors, *ACNS 22: 20th International Conference on Applied Cryptography and Network Security*, volume 13269 of *Lecture Notes in Computer Science*, pages 3–23. Springer, Heidelberg, June 2022. https://doi.org/10.1007/978-3-031-09234-3_1

[Tak21] Atsushi Takayasu. Tag-based ABE in prime-order groups via pair encoding. *Des. Codes Cryptogr.*, 89(8):1927–1963, 2021. https://doi.org/10.1007/S10623-021-00894-4

[vGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 24–43. Springer, Heidelberg, May / June 2010. https://doi.org/10.1007/978-3-642-13190-5_2

[Wat05] Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, Heidelberg, May 2005. https://doi.org/10.1007/11426639_7

[Wat09] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636. Springer, Heidelberg, August 2009. https://doi.org/10.1007/978-3-642-03356-8_36

[Wee14] Hoeteck Wee. Dual system encryption via predicate encodings. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 616–637. Springer, Heidelberg, February 2014. https://doi.org/10.1007/978-3-642-54242-8_26

[Yam17] Shota Yamada. Asymptotically compact adaptively secure lattice IBEs and verifiable random functions via generalized partitioning techniques. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 161–193. Springer, Heidelberg, August 2017. https://doi.org/10.1007/978-3-319-63697-9_6

[ZPS12] Zhenfei Zhang, Thomas Plantard, and Willy Susilo. On the CCA-1 security of somewhat homomorphic encryption over the integers. In Mark Dermot Ryan, Ben Smyth, and Guilin Wang, editors, *Information Security Practice and Experience - 8th International Conference, ISPEC 2012, Hangzhou, China, April 9-12, 2012. Proceedings*, volume 7232 of *Lecture Notes in Computer Science*, pages 353–368. Springer, 2012. https://doi.org/10.1007/978-3-642-29101-2_24

[ZSZ+22] Yuncong Zhang, Alan Szepieniec, Ren Zhang, Shi-Feng Sun, Geng Wang, and Dawu Gu. VOProof: Efficient zkSNARKs from vector oracle compilers. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *ACM CCS 2022: 29th Conference on Computer and Communications Security*, pages 3195–3208. ACM Press, November 2022. https://doi.org/10.1145/3548606.3559387