Multi-Input Quadratic Functional Encryption from Pairings

Junichi Tomida

NTT Corporation, Japan
junichi.tomida.vw@hco.ntt.co.jp

Abstract. Multi-input functional encryption (MIFE) is a generalization of functional encryption and allows decryptor to learn only function values $f(x_1, \ldots, x_n)$ from ciphertexts of $x_1, \ldots, x_n$. We present the first MIFE schemes for quadratic functions (MQFE) from pairings. We first observe that public-key MQFE can be obtained from inner product functional encryption in a relatively simple manner whereas obtaining secret-key MQFE from standard assumptions is completely nontrivial. The main contribution of this paper is to construct the first secret-key MQFE scheme that achieves indistinguishability-based selective security against unbounded collusion under the standard bilateral matrix Diffie-Hellman assumption. All previous MIFE schemes either support only inner products (linear functions) or rely on non-standard cryptographic assumptions such as indistinguishability obfuscation or multi-linear maps. Thus, our schemes are the first MIFE for functionality beyond linear functions from polynomial hardness of standard assumptions.

Keywords: functional encryption, multi-input, quadratic functions, pairings

Table of Contents

1 Introduction

Multi-Input Functional Encryption. Functional encryption (FE) [13,31] is a novel cryptographic paradigm that has an essentially different feature from traditional encryption schemes. Concretely, FE allows us to obtain computation results from encrypted data without revealing any other information about the underlying data. This is in contrast to the traditional encryption schemes, where only owners of legitimate keys can learn entire underlying data from ciphertexts whereas others can learn nothing. An FE scheme that supports a function class $\mathcal{F}$ allows an owner of a master secret to issue a secret key SK for a function $f \in \mathcal{F}$. Decryption of a ciphertext CT for a message x with SK yields $f(x)$ and nothing else. Functional encryption is quite useful for securely delegating computation since it allows a sever to learn only function values from encrypted data.

Multi-input functional encryption (MIFE) [24] is a natural generalization of FE, which can handle functions that take multiple inputs. That is, an owner of SK for f can learn only $f(x_1, \ldots, x_\mu)$ from $\mathsf{CT}_1, \ldots, \mathsf{CT}_n$ of messages $x_1, \ldots, x_n$. MIFE schemes can be basically classified into two categories with respect to their function classes.

General functionalities: The first consists of MIFE schemes for general circuits or Turing machines, e.g., [7,9,14,15,24,25]. Although they are powerful enough to handle all functions computable in polynomial time, they are built on non-standard cryptographic assumptions such as indistinguishability obfuscation (iO) [22] or multi-linear maps [21] and thus prohibitively inefficient. Very recently, iO was constructed from sub-exponential hardness of four well-founded assumptions [26]. Note that, however, we refer to *polynomial hardness* of a well-founded problem as a standard assumption in this paper.

Specific functionalities: The second covers MIFE schemes for specific functions such as inner products and order revealing, e.g., [1,2,4,6,12,16,19,29,32]. They are aimed at obtaining more practical features, namely, efficiency and concrete security, with sacrificing the generality. Therefore, most of them have efficient constructions, and their security is based on standard assumptions, except the order-revealing encryption by Boneh *et al.* [12], which relies on multi-linear maps.

Recent works proposed extensions of MIFE that do not require a trusted third party for secret-key generation [7,17].

Functional Encryption for Specific Functionalities. This paper is categorized to the latter since we are interested in the specific functionality, namely, quadratic functions. We recall related works on FE for the latter category in a bit more detail. Abdalla *et al.* first presented FE schemes for inner products (linear functions) based on DDH and LWE [3], which is called inner product functional encryption (IPFE). An IPFE scheme from DCR is proposed later by Agrawal *et al.* [8]. Then, Abdalla *et al.* presented a multi-input IPFE (MIPFE) scheme based on pairings [6]. Abdalla *et al.* also constructed MIPFE schemes based on DDH or k-Lin without pairings, LWE, and DCR by introducing a generic conversion from IPFE to MIPFE [4]. As another line of works, several FE schemes for quadratic functions have been constructed from pairings [10,23,30]. Note that FE for quadratic functions are trivially constructible from IPFE by encrypting all quadratic terms in advance, although the ciphertext size inherently becomes $O(n^2)$ where n is the number of elements to be encrypted. Thus, FE for quadratic functions normally refers to that with the ciphertext size being $O(n)$.

Since the first introduction of MIPFE scheme [6], no MIFE schemes for functionality beyond linear functions based on standard cryptographic assumptions have been proposed until now. Although (MI)FE for linear functions is expected to be applied for statistical analysis as it can provide weighted means, linear functions are insufficient for evaluating important values for statistics such as variance and standard deviation. This motivates the fundamental question:

Can we construct an (efficient) MIFE scheme for more than linear functions from standard cryptographic assumptions?

Alternatively, considering the fact that MIFE for inner products is constructible without pairings, the following question naturally comes to mind:

Can we construct an MIFE scheme for quadratic functions from pairings?

1.1 Our Results

We answer these questions affirmatively, that is, we construct the first MIFE schemes for quadratic functions, or multi-input quadratic functional encryption (MQFE) schemes, from pairings [20]. Our first observation is that public-key MQFE can be generically obtained from public-key IPFE, which can be constructed even without pairings, in a relatively simple manner as the case of public-key MIPFE [6].

The main result of this paper is to construct a secret-key MQFE scheme from the bilateral matrix Diffie-Hellmen assumption, in which users need a master secret key for encryption. Recall that public-key MIFE does not imply secret-key MIFE. Roughly speaking, a user who has CT_1 for x_1 and SK for f of a public-key scheme is allowed to learn $f(x_1, x_2, \ldots, x_n)$ for all $(x_2, \ldots, x_n)$ since this is inherent leakage, while it is not the case in secret-key MIFE. Hence, just including a public key of a public-key MIFE scheme in a master secret key does not necessarily result in a secret-key MIFE scheme due to the leakage. Our secret-key scheme has indistinguishability-based selective security against unbounded collusion. Roughly speaking, the security implies that an adversary that has any numbers of ciphertexts and secret keys can learn only decryption values for all decryptable combinations and nothing else. Our scheme has no limits on the numbers of encryption slots and elements per slot while they are fixed at the setup. The ciphertext size of our scheme is $O(m^2 n)$, and the secret-key size is $O(m^2 n^2)$, where m is the number of elements per slot and n is the number of encryption slots.[1] Furthermore, our scheme is far more efficient than MIFE schemes for general functions since ours basically uses only efficient IPFE as a building block in a direct manner.

Our secret-key MQFE scheme is built on two newly introduced primitives that we call predicated IPFE and multi-input mixed-group IPFE. Both of them need to have the function-hiding property to construct our MQFE scheme, and we construct them from a (multi-input) function-hiding IPFE scheme based on pairings [4, 11, 19] in a generic way. In a function-hiding scheme, secret keys hide underlying functions as well as ciphertexts hide plaintexts.

Multi-Input Quadratic Functional Encryption. Informally, a function class $\mathcal{F}_{m,n}$ for n-input MQFE is defined as follows. Each function $f \in \mathcal{F}_{m,n}$ is represented by a vector $\mathbf{c} \in \mathbb{Z}^{(mn)^2}$. For inputs $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{Z}^m$, f is defined as

$$f(\mathbf{x}_1, \ldots, \mathbf{x}_n) := \langle \mathbf{c}, \mathbf{x} \otimes \mathbf{x} \rangle$$

where $\mathbf{x} = (\mathbf{x}_1 || \cdots || \mathbf{x}_n)$ and $\otimes$ denotes the Kronecker product. In an MQFE scheme for $\mathcal{F}_{m,n}$, a user can encrypt $\mathbf{x}_i \in \mathbb{Z}^m$ to CT_i for slot $i \in [n]$, a key issuer can generate a secret key SK for $\mathbf{c} \in \mathbb{Z}^{(mn)^2}$, and decryption of $\mathsf{CT}_1, \ldots, \mathsf{CT}_n$ with SK reveals only $\langle \mathbf{c}, \mathbf{x} \otimes \mathbf{x} \rangle$.

An important fact on MQFE is that the relation between linear and quadratic functions in the multi-input case is essentially different from that in the single-input case. As mentioned above, FE for quadratic functions aims short ciphertexts because it is trivially implied by IPFE if there are no ciphertext-size requirements. On the other hand, an MQFE scheme cannot be trivially constructed from MIPFE scheme even if there are no ciphertext-size requirements. This is because the method of encrypting all quadratic terms in advance cannot deal with the quadratic terms derived from two different users. In other words, MQFE enables us to perform some sort of computation that is uncomputable with MIPFE such as computing variance over multiple data sources encrypted by different users. We remark that although the ciphertext size of our scheme is not optimal, i.e., $O(m)$, our result is by no means trivial as discussed.

As the case of MIFE for general functions or inner products, we can also consider the security model where an adversary can choose users to be corrupted, which is called multi-client setting [1,2,16,24,29].

[1] Precisely, sizes of ciphertexts and secret keys refer to the number of group elements.

Our secret-key scheme is not easily applicable to the multi-client setting. The intuitive reason is that the function-hiding IPFE, which is the main building block of our scheme, works only when encryption keys are hidden (uncorrupted). Constructing a multi-client functional encryption for quadratic functions is an interesting open problem, and we leave it for a future direction.

1.2 Technical Overview

Public-Key MQFE. For simplicity, we consider the two-input case in this paragraph. We also assume that quadratic functions are represented by matrices $\mathbf{C} \in \mathbb{Z}^{2m \times 2m}$, where $f(\mathbf{x}_1, \mathbf{x}_2) = (\mathbf{x}_1^\top || \mathbf{x}_2^\top)\mathbf{C}\begin{pmatrix}\mathbf{x}_1 \\ \mathbf{x}_2\end{pmatrix}$. In a public-key scheme, an adversary that has CT_1 for $\mathbf{x}_1$, CT_2 for $\mathbf{x}_2$, and SK for $\mathbf{C} = \begin{pmatrix}\mathbf{C}_{1,1}\mathbf{C}_{1,2} \\ \mathbf{C}_{2,1}\mathbf{C}_{2,2}\end{pmatrix}$ can learn $(\widetilde{\mathbf{x}}_1^\top || \mathbf{x}_2^\top)\mathbf{C}\begin{pmatrix}\widetilde{\mathbf{x}}_1 \\ \mathbf{x}_2\end{pmatrix}$ and $(\mathbf{x}_1^\top || \widetilde{\mathbf{x}}_2^\top)\mathbf{C}\begin{pmatrix}\mathbf{x}_1 \\ \widetilde{\mathbf{x}}_2\end{pmatrix}$ for all $\widetilde{\mathbf{x}}_1, \widetilde{\mathbf{x}}_2$ since it can encrypt $\widetilde{\mathbf{x}}_1, \widetilde{\mathbf{x}}_2$. By setting $\widetilde{\mathbf{x}}_2 = \mathbf{0}$ and $\widetilde{\mathbf{x}}_1 = \mathbf{0}$, the adversary can learn $\mathbf{x}_1^\top \mathbf{C}_{1,1}\mathbf{x}_1$ and $\mathbf{x}_2^\top \mathbf{C}_{2,2}\mathbf{x}_2$, respectively. By setting $\widetilde{\mathbf{x}}_2 = \mathbf{e}_i$ and $\widetilde{\mathbf{x}}_1 = \mathbf{e}_i$ for all $i \in [m]$ where $\mathbf{e}_1, \ldots, \mathbf{e}_m$ are linearly independent vectors, the adversary can learn $\mathbf{x}_1^\top(\mathbf{C}_{1,2} + \mathbf{C}_{2,1}^\top)$ and $(\mathbf{C}_{1,2} + \mathbf{C}_{2,1}^\top)\mathbf{x}_2$, respectively. This is because the adversary can compute $\widetilde{\mathbf{x}}_1^\top \mathbf{C}_{1,1}\widetilde{\mathbf{x}}_1$ and $\widetilde{\mathbf{x}}_2^\top \mathbf{C}_{2,2}\widetilde{\mathbf{x}}_2$ by itself. Furthermore, $\mathsf{Dec}(\mathsf{CT}_1, \mathsf{CT}_2, \mathsf{SK}) = (\mathbf{x}_1^\top || \mathbf{x}_2^\top)\mathbf{C}\begin{pmatrix}\mathbf{x}_1 \\ \mathbf{x}_2\end{pmatrix}$ is computable from the inherent leakage as follows:

$$\mathbf{x}_1^\top \mathbf{C}_{1,1}\mathbf{x}_1 + \mathbf{x}_2^\top \mathbf{C}_{2,2}\mathbf{x}_2 + \mathbf{x}_1^\top(\mathbf{C}_{1,2} + \mathbf{C}_{2,1}^\top)(\mathbf{C}_{1,2} + \mathbf{C}_{2,1}^\top)^+(\mathbf{C}_{1,2} + \mathbf{C}_{2,1}^\top)\mathbf{x}_2^\top$$

where $(\mathbf{C}_{1,2} + \mathbf{C}_{2,1}^\top)^+ \in \mathbb{Q}^{m \times m}$ denotes the Moore-Penrose inverse of $\mathbf{C}_{1,2} + \mathbf{C}_{2,1}^\top$. It is not hard to see that the inherent leakage can be computed by IPFE since they are linear functions over a single input. Thus, public-key 2-input MQFE can be constructed from public-key IPFE. This construction can be easily extended to the general multi-input case, which is presented in Appx. A.

Secret-Key MQFE. Our secret-key MQFE scheme is inspired by the secret-key FE scheme for quadratic functions (or quadratic functional encryption (QFE) scheme) from pairings by Lin [30]. First of all, we briefly recall the public-key IPFE scheme from DDH by Abdalla *et al.* [3] (ABDP). Let m be a vector length in the scheme. For a matrix $\mathbf{M} = (m_{i,j})_{i,j}$ and a generator g_ℓ of a cyclic group of order p, we denote $(g_\ell^{m_{i,j}})_{i,j}$ by $[\mathbf{M}]_\ell$. The ABDP scheme works as follows:

$\mathsf{Setup}(1^\lambda)$**:** $\mathbf{w} \leftarrow \mathbb{Z}_p^m,\ \mathsf{PK} := [\mathbf{w}],\ \mathsf{MSK} := \mathbf{w}$.
$\mathsf{Enc}(\mathsf{PK}, \mathbf{x} \in \mathbb{Z}^m)$**:** $s \leftarrow \mathbb{Z}_p,\ \mathsf{CT} := ([s], [\mathbf{x} + s\mathbf{w}])$.
$\mathsf{KeyGen}(\mathsf{MSK}, \mathbf{c} \in \mathbb{Z}^m)$**:** $\mathsf{SK} := -\mathbf{c}^\top \mathbf{w}$.
$\mathsf{Dec}(\mathsf{CT}, \mathsf{SK})$**:** $-\mathbf{c}^\top \mathbf{w}[s] + \mathbf{c}^\top[\mathbf{x} + s\mathbf{w}] = [\langle \mathbf{c}, \mathbf{x}\rangle]$.

Lin's idea for constructing QFE is to use function-hiding IPFE, which is inherently secret-key FE [11], to compress the size of ABDP ciphertexts for quadratic terms. Recall that the function-hiding property requires that secret keys hide its function (or vector in IPFE). Let $\mathsf{iFE} = (\mathsf{iSetup}, \mathsf{iEnc}, \mathsf{iKeyGen}, \mathsf{iDec})$ be a function-hiding IPFE scheme based on pairings. Note that all known function-hiding IPFE schemes based on pairings output a decryption value as an exponent of the target-group generator [11, 18, 28, 30, 33]. Informally, her secret-key QFE scheme works as follows:

$\mathsf{Setup}(1^\lambda)$**:** $\mathbf{w} = (w_1, \ldots, w_m), \widetilde{\mathbf{w}} = (\widetilde{w}_1, \ldots, \widetilde{w}_m) \leftarrow \mathbb{Z}_p^m,\ \mathsf{iMSK}' \leftarrow \mathsf{iSetup}(1^\lambda)$
    $\mathsf{MSK} := (\mathsf{iMSK}', \mathbf{w}, \widetilde{\mathbf{w}})$.
$\mathsf{Enc}(\mathsf{MSK}, \mathbf{x} \in \mathbb{Z}^m)$**:** $s \leftarrow \mathbb{Z}_p,\ \mathsf{iCT}' \leftarrow \mathsf{iEnc}(\mathsf{MSK}', s),\ \mathsf{iMSK} \leftarrow \mathsf{iSetup}(1^\lambda)$
    $\mathsf{iCT}_i \leftarrow \mathsf{iEnc}(\mathsf{iMSK}, (x_i, w_i)), \mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}, (x_i, s\widetilde{w}_i))$.
    $\mathsf{CT} := (\mathsf{iCT}', \{\mathsf{iCT}_i, \mathsf{iSK}_i\}_{i \in [m]})$.
$\mathsf{KeyGen}(\mathsf{MSK}, \mathbf{c} = \{c_{i,j}\}_{i,j \in [m]} \in \mathbb{Z}^{m^2})$**:**
    $\mathsf{SK} := \mathsf{iSK}' \leftarrow \mathsf{iKeyGen}(\mathsf{MSK}', -\mathbf{c}^\top(\mathbf{w} \otimes \widetilde{\mathbf{w}}))$.

$\mathsf{Dec}(\mathsf{CT}, \mathsf{SK})$**:** $\mathsf{iDec}(\mathsf{iCT}', \mathsf{iSK}') + \sum_{i,j \in [m]} c_{i,j} \mathsf{iDec}(\mathsf{iCT}_i, \mathsf{iSK}_j) = [\langle \mathbf{c}, \mathbf{x} \otimes \mathbf{x} \rangle]_T$.

In decryption, her scheme first generates an ABDP ciphertext and an ABDP secret key for quadratic terms in the target group G_T of bilinear groups from ciphertexts and secret keys of iFE. Then, it decrypts the ABDP ciphertext in the same way as the ABDP scheme. That is, we have $\mathsf{iDec}(\mathsf{iCT}_i, \mathsf{iSK}_j) = [x_i x_j + s w_i \widetilde{w}_j]_T$, which can be seen as the (i,j)-th element of the ABDP ciphertext $[\mathbf{x} \otimes \mathbf{x} + s\mathbf{w} \otimes \widetilde{\mathbf{w}}]_T$, and $\mathsf{iDec}(\mathsf{iCT}', \mathsf{iSK}') = [-s\mathbf{c}^\top(\mathbf{w} \otimes \widetilde{\mathbf{w}})]_T$, where $-\mathbf{c}^\top(\mathbf{w} \otimes \widetilde{\mathbf{w}})$ is an ABDP secret key for $\mathbf{c}$. The function-hiding property of iFE guarantees that iSK hides x_i. Since $\mathbf{w} \otimes \widetilde{\mathbf{w}}$ only appears on the exponent of group elements, we can argue that it is computationally indistinguishable from random in $\mathbb{Z}_p^{m^2}$ in the security proof.

MIPFE instead of IPFE. Our first attempt is to modify Lin's scheme so that it generates ciphertexts of secret-key MIPFE scheme from DDH by Abdalla *et al.* [4] (ACFGU) in G_T instead of the ABDP ciphertext (recall that the ACFGU scheme does not use pairings). That is, the decryption algorithm similarly generates ACFGU ciphertexts for all quadratic terms over all inputs and then decrypt it similarly to the ACFGU scheme. The reason for using MIPFE instead of IPFE is to deal with multiple independent randomnesses derived from different users, which inherently come in when generating the IPFE ciphertext elements for quadratic terms. We also remark that the reason for decomposing the ACFGU ciphertext into ciphertexts and secret keys of function-hiding IPFE is to allow decryptors to generate ACFGU ciphertext elements for quadratic terms derived from two different users. This is in contrast to Lin's QFE scheme, which uses function-hiding IPFE to compress the ciphertext size.

The n-input ACFGU scheme is described as follows:

$\mathsf{Setup}(1^\lambda)$**:** $\mathsf{MSK} := \mathbf{w}_1, \ldots, \mathbf{w}_n, \mathbf{u}_1, \ldots, \mathbf{u}_n \leftarrow \mathbb{Z}_p^m$.
$\mathsf{Enc}(\mathsf{MSK}, i, \mathbf{x}_i \in \mathbb{Z}^m)$**:** $s_i \leftarrow \mathbb{Z}_p$, $\mathsf{CT}_i := ([s_i], [\mathbf{x}_i + s_i \mathbf{w}_i + \mathbf{u}_i])$.
$\mathsf{KeyGen}(\mathsf{MSK}, (\mathbf{c}_1, \ldots, \mathbf{c}_n) \in \mathbb{Z}^{mn})$**:** $\mathsf{SK} := (-\sum_{i \in [n]} \langle \mathbf{c}_i, \mathbf{u}_i \rangle, \{-\mathbf{c}_i^\top \mathbf{w}_i\}_{i \in [n]})$.
$\mathsf{Dec}(\mathsf{CT}_1, \ldots, \mathsf{CT}_n, \mathsf{SK})$**:**
$\sum_{i \in [n]} (-\mathbf{c}_i^\top \mathbf{w}_i [s_i] + \mathbf{c}_i^\top [\mathbf{x}_i + s_i \mathbf{w}_i + \mathbf{u}_i]) - [\sum_{i \in [n]} \langle \mathbf{c}_i, \mathbf{u}_i \rangle] = [\sum_{i \in [n]} \langle \mathbf{c}_i, \mathbf{x}_i \rangle]$.

Then, the candidate MQFE construction $\mathsf{qFE} = (\mathsf{qSetup}, \mathsf{qEnc}, \mathsf{qKeyGen}, \mathsf{qDec})$ will be defined as follows (for simplicity, we assume $m = 1$ in what follows):

$\mathsf{qSetup}(1^\lambda)$**:** $\mathsf{iMSK}, \mathsf{iMSK}' \leftarrow \mathsf{iSetup}(1^\lambda)$, $w_i, \widetilde{w}_i, u_i, \widetilde{u}_i \leftarrow \mathbb{Z}_p$
$\mathsf{qMSK} := (\mathsf{iMSK}, \mathsf{iMSK}', \{w_i, \widetilde{w}_i, u_i, \widetilde{u}_i\}_{i \in [n]})$.
$\mathsf{qEnc}(\mathsf{qMSK}, i, x_i \in \mathbb{Z})$**:** $s_i, \widetilde{s}_i \leftarrow \mathbb{Z}_p$
$\mathsf{iCT}'_i \leftarrow \mathsf{iEnc}(\mathsf{iMSK}', s_i)$, $\mathsf{iSK}'_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}', \widetilde{s}_i)$
$\mathsf{iCT}_i \leftarrow \mathsf{iEnc}(\mathsf{iMSK}, (x_i, s_i w_i, u_i))$, $\mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}, (x_i, \widetilde{s}_i \widetilde{w}_i, \widetilde{u}_i))$
$\mathsf{qCT}_i := (\mathsf{iCT}'_i, \mathsf{iSK}'_i, \mathsf{iCT}_i, \mathsf{iSK}_i)$.
$\mathsf{qKeyGen}(\mathsf{MSK}, \mathbf{c} = \{c_{i,j}\}_{i,j \in [n]})$**:** $\mathsf{qSK} := ([-\sum_{i,j \in [n]} c_{i,j} u_i \widetilde{u}_j]_T, \{-c_{i,j} w_i \widetilde{w}_j\}_{i,j \in [n]})$.
$\mathsf{qDec}(\mathsf{qCT}_1, \ldots, \mathsf{qCT}_n, \mathsf{qSK})$**:**
$-\sum_{i,j \in [n]} c_{i,j} w_i \widetilde{w}_j \mathsf{iDec}(\mathsf{iCT}'_i, \mathsf{iSK}'_j) + \sum_{i,j \in [n]} c_{i,j} \mathsf{iDec}(\mathsf{iCT}_i, \mathsf{iSK}_j)$
$-[\sum_{i,j \in [n]} c_{i,j} u_i \widetilde{u}_j]_T = [\langle \mathbf{c}, \mathbf{x} \otimes \mathbf{x} \rangle]_T$

Observe that $\{\mathsf{iCT}_i, \mathsf{iSK}_i\}_{i \in [n]}$ yield $\{[x_i x_j + s_i \widetilde{s}_j w_i \widetilde{w}_j + u_i \widetilde{u}_j]_T\}_{i,j \in [n]}$ in decryption, which can be seen as ciphertexts of the n^2-input ACFGU scheme.

However, this scheme is not secure, that is, it leaks unnecessary information to decryptors more than expected. The problem is that the candidate scheme allows two types of mixed-up attacks where an adversary can simultaneously use two different ciphertexts with the same index for decryption:

1. For $\mathsf{iCT}_i^1, \mathsf{iSK}_i^2$ in $\mathsf{qCT}_i^1, \mathsf{qCT}_i^2$, respectively, $\mathsf{iDec}(\mathsf{iCT}_i^1, \mathsf{iSK}_i^2)$ is a valid ACFGU ciphertext and usable for the ACFGU decryption with qSK.
2. Let $i_1 \neq i_2$. For $\{\mathsf{iCT}_{i_1}^1, \mathsf{iSK}_{i_1}^1\}, \{\mathsf{iCT}_{i_2}^1, \mathsf{iSK}_{i_2}^1\}, \mathsf{iCT}_{i_2}^2$ in $\mathsf{qCT}_{i_1}^1, \mathsf{qCT}_{i_2}^1, \mathsf{qCT}_{i_2}^2$, respectively, $\mathsf{iDec}(\mathsf{iCT}_{i_1}^1, \mathsf{iSK}_{i_1}^1)$, $\mathsf{iDec}(\mathsf{iCT}_{i_2}^2, \mathsf{iSK}_{i_1}^1)$ and $\mathsf{iDec}(\mathsf{iCT}_{i_2}^1, \mathsf{iSK}_{i_2}^1)$ are valid ACFGU ciphertexts and usable for the ACFGU decryption with qSK together.

Preventing Attack 1. Recall that Lin's QFE scheme does not allow Attack 1 since the encryption algorithm generate new iMSK for each ciphertext. On the other hand, our candidate uses the same iMSK for all ciphertexts so that decryptors can generate ACFGU ciphertext elements for quadratic terms from two different users. To prevent this attack, we need a function-hiding IPFE scheme where iCT is decryptable with iSK if and only if they come from either different slots or the same qCT_i. For that purpose, we introduce predicated IPFE (PIPFE), which can be seen as a combination of inner product encryption [27] and IPFE. Informally, a ciphertext pCT and a secret key pSK of a PIPFE scheme are associated with two vectors $\{\mathbf{x}_1, \mathbf{x}_2\}$ and $\{\mathbf{y}_1, \mathbf{y}_2\}$, respectively. Decryption of pCT with pSK reveals $\langle \mathbf{x}_2, \mathbf{y}_2 \rangle$ iff $\langle \mathbf{x}_1, \mathbf{y}_1 \rangle = 0$. Although PIPFE can be captured as a class of IPFE with fine-grained access control [5], they did not consider the function-hiding property. Thus, our PIPFE scheme is the first instantiation of function-hiding IPFE with fine-grained access control, which is of independent interest.[2]

PIPFE yields the expected decryption mechanism by setting $\mathbf{x}_1 = (0^{2(i-1)}, 1, L, 0^{2(n-i)})$, $\mathbf{y}_1 = (0^{2(i-1)}, L, -1, 0^{2(n-i)})$ where $L \leftarrow \mathbb{Z}_p$ in each encryption. Let (i_1, L_1) (resp. (i_2, L_2)) be a pair of a slot index and random element of $\mathbf{x}_1$ (resp. $\mathbf{y}_1$). It is easy to see that $\langle \mathbf{x}_1, \mathbf{y}_1 \rangle = 0$ iff $i_1 \neq i_2$ or $L_1 = L_2$. Since L is chosen from an exponentially large space, $L_1 \neq L_2$ with overwhelming probability if they are chosen independently. We construct a function-hiding PIPFE scheme pFE from a function-hiding IPFE scheme iFE in a generic way. The construction is very simple, that is, pCT is iCT for $(a\mathbf{x}_1 || \mathbf{x}_2)$ and pSK is iSK for $(b\mathbf{y}_1 || \mathbf{y}_2)$ where $a, b \leftarrow \mathbb{Z}_p$. We define $\mathsf{pDec}(\mathsf{pCT}, \mathsf{pSK}) = \mathsf{iDec}(\mathsf{iCT}, \mathsf{iSK}) = [ab\langle \mathbf{x}_1, \mathbf{y}_1 \rangle + \langle \mathbf{x}_2, \mathbf{y}_2 \rangle]_T$, where $\langle \mathbf{x}_2, \mathbf{y}_2 \rangle$ is computable iff $\langle \mathbf{x}_1, \mathbf{y}_1 \rangle = 0$.

Preventing Attack 2. A cumbersome point of Attack 2 is the fact that $\mathsf{iDec}(\mathsf{iCT}^1_{i_1}, \mathsf{iSK}^1_{i_1})$ and $\mathsf{iDec}(\mathsf{iCT}^1_{i_2}, \mathsf{iSK}^1_{i_2})$ are necessary for decryption with $\mathsf{qCT}^1_{i_1}, \mathsf{qCT}^1_{i_2}$, and $\mathsf{iDec}(\mathsf{iCT}^2_{i_2}, \mathsf{iSK}^1_{i_1})$ is necessary for decryption with $\mathsf{qCT}^1_{i_1}, \mathsf{qCT}^2_{i_2}$. However, they leak inappropriate information if both of them are used in decryption simultaneously. Thus, we cannot solve the problem by prohibiting some sort of iFE decryption like the case of Attack 1.

Our solution is to bind ACFGU ciphertexts generated from the iFE decryption with common random elements. That is, iCT_i in qCT_i is changed to encryption of $(x_i, s_i w_i, u_i, t_i v_i)$, and iSK_i is changed to a secret key of $(x_i, \widetilde{s}_i \widetilde{w}_i, r_i \widetilde{u}_i, \widetilde{v}_i)$ where $v_i, \widetilde{v}_i$ are new elements in qMSK and r_i, t_i are the common random elements for binding ACFGU ciphertexts, which is chosen by qEnc. Then, decryption with $\{\mathsf{iCT}_i, \mathsf{iSK}_i\}_{i \in [n]}$ yields $\{[x_i x_j + s_i \widetilde{s}_j w_i \widetilde{w}_j + r_j u_i \widetilde{u}_j + t_i v_i \widetilde{v}_j]_T\}_{i,j \in [n]}$. According to the change of $\mathsf{iCT}, \mathsf{iSK}$, the first element of an ACFGU secret key should be modified as $\mathsf{qSK}_1 = [-\sum_{i,j \in [n]} c_{i,j}(r_j u_i \widetilde{u}_j + t_i v_i \widetilde{v}_j)]_T$. By this construction, we cannot simultaneously use $\mathsf{iDec}(\mathsf{iCT}^1_{i_1}, \mathsf{iSK}^1_{i_1})$, $\mathsf{iDec}(\mathsf{iCT}^1_{i_2}, \mathsf{iSK}^1_{i_2})$ and $\mathsf{iDec}(\mathsf{iCT}^2_{i_2}, \mathsf{iSK}^1_{i_1})$ for ACFGU decryption. Intuitively, qSK_1 must involve $t^1_{i_2}$ and $t^2_{i_2}$ (randomnesses used in $\mathsf{iCT}^1_{i_2}$ and $\mathsf{iCT}^2_{i_2}$, respectively) to decrypt the ACFGU ciphertexts generated from $\mathsf{iDec}(\mathsf{iCT}^1_{i_1}, \mathsf{iSK}^1_{i_1})$, $\mathsf{iDec}(\mathsf{iCT}^1_{i_2}, \mathsf{iSK}^1_{i_2})$ and $\mathsf{iDec}(\mathsf{iCT}^2_{i_2}, \mathsf{iSK}^1_{i_1})$ together, but in fact qSK_1 can involve only one of $t^1_{i_2}$ and $t^2_{i_2}$.

How to Generate the Modified Secret Key. The last challenge is how to generate the modified secret key. It is obvious that $\mathsf{qKeyGen}$ cannot generate the modified key since it contains random elements r_i, t_i used in ciphertexts. We solve the problem by employing an additional function-hiding MIPFE scheme, denoted by miFE, into the candidate scheme. That is, qEnc additionally generates an MIPFE ciphertext miCT_i for (r_i, t_i), and $\mathsf{qKeyGen}$ generates an MIPFE secret key miSK for $\{(\sum_{j \in [n]} c_{j,i} u_j \widetilde{u}_i, \sum_{j \in [n]} c_{i,j} v_i \widetilde{v}_j)\}_{i \in [n]}$. Then, a decryptor can generate the secret-key element $-\sum_{i,j \in [n]} c_{i,j}(r_j u_i \widetilde{u}_j + t_i v_i \widetilde{v}_j)$ from $\mathsf{miCT}_1, \ldots, \mathsf{miCT}_n, \mathsf{miSK}$ without knowing unnecessary information. This technique similar to Gay's technique in [23], which uses (partially) function-hiding IPFE to generate a "decryption key" consisting of both elements inherently derived from a ciphertext and a secret key. Note that our actual scheme needs multi-input mixed-group IPFE instead of MIPFE so that the security proof go through, although they are similar primitives.

This is a rough sketch of our MQFE scheme. We need a further modification to make the scheme satisfy the formal security definition, since we cannot argue that $\{w_i \widetilde{w}_j\}_{i,j \in [n]}$ is distributed pseudo-

[2] To be precise, secret keys of our PIPFE scheme hide $\mathbf{y}_2$ but do not $\mathbf{y}_1$, and we call this property partially function-hiding.

randomly. This is because qSK contains them as not the exponent of group elements but $\mathbb{Z}_p$ elements in the candidate. The modification is simple; we use $\{w_{i,j}\}_{i,j\in[n]}$ instead of $\{w_i\widetilde{w}_j\}_{i,j\in[n]}$. We also need hidden spaces of IPFEs that are used only for the security proof as in [30]. These modifications make the ciphertext size be $O(m^2n)$. We give an overview of the security proof for very simple case in Sec. 5 besides the full proof in Sec. 6.

2 Preliminaries

2.1 Notations

For a natural number $m, n \in \mathbb{N}$, $[m]$ denotes a set $\{1, \ldots, m\}$, and $[m, n]$ denotes a set $\{m, \ldots, n\}$. For matrices $\mathbf{M}_1, \ldots, \mathbf{M}_n$ with the same number of rows, $(\mathbf{M}_1||\cdots||\mathbf{M}_n)$ denotes their matrix concatenation. For vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$, $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ denotes the vector concatenation as row vectors *regardless of* whether each $\mathbf{v}_i$ is a row or column vector. For instance, for $\mathbf{v}_1 \in \mathbb{Z}_p^{m\times 1}, \mathbf{v}_2 \in \mathbb{Z}_p^{1\times n}$, $(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{v}_1^\top||\mathbf{v}_2)$. We use $\otimes$ for the Kronecker product. We denotes an n-dimensional unit vector $(0^{i-1}, 1, 0^{n-1})$ by $\mathbf{e}_{i/n}$. For families of distributions $X := \{X_\lambda\}_{\lambda\in\mathbb{N}}$ and $Y := \{Y_\lambda\}_{\lambda\in\mathbb{N}}$, we denote $X \approx_c Y$ as computational indistinguishability.

2.2 Basic Tools and Assumptions

Definition 2.1 (Bilinear Groups). A description of bilinear groups $\mathbb{G}:=(p, G_1, G_2, G_T, g_1, g_2, e)$ consist of a prime p, cyclic groups G_1, G_2, G_T of order p, generators g_1 and g_2 of G_1 and G_2 respectively, and a bilinear map $e : G_1 \times G_2 \to G_T$, which has two properties.

- (Bilinearity): $\forall h_1 \in G_1, h_2 \in G_2, a, b \in \mathbb{Z}_p, e(h_1^a, h_2^b) = e(h_1, h_2)^{ab}$.
- (Non-degeneracy): For generators g_1 and g_2, $g_T := e(g_1, g_2)$ is a generator of G_T.

A bilinear group generator $\mathcal{G}_{\mathsf{BG}}(1^\lambda)$ takes a security parameter 1^λ and outputs a description of bilinear groups $\mathbb{G}$ with a $\Omega(\lambda)$-bit prime p.

Definition 2.2 ($\mathcal{D}_{j,k}$-MDDH Assumption [20]). For $j > k$, let $\mathcal{D}_{j,k}$ be a matrix distribution over matrices in $\mathbb{Z}_p^{j\times k}$, which outputs a full-rank matrix with overwhelming probability. Let $\mathbb{G}$ be bilinear groups. We can assume that, wlog, the first k rows of a matrix chosen from $\mathcal{D}_{j,k}$ form an invertible matrix. We consider the following distribution: $\mathbf{A} \leftarrow \mathcal{D}_{j,k},\ \mathbf{z} \leftarrow \mathbb{Z}_p^k,\ \mathbf{k}_0 := \mathbf{A}\mathbf{z},\ \mathbf{k}_1 \leftarrow \mathbb{Z}_p^j,\ P_{i,\beta} := (\mathbb{G}, [\mathbf{A}]_i, [\mathbf{k}_\beta]_i)$. We say that the $\mathcal{D}_{j,k}$-MDDH assumption holds with respect to $\mathbb{G}$ if, for any PPT adversary $\mathcal{A}$,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathcal{D}_{j,k}\text{-}\mathsf{MDDH}}(\lambda) := \max_{i\in\{1,2\}} |\Pr[1 \leftarrow \mathcal{A}(P_{i,0})] - \Pr[1 \leftarrow \mathcal{A}(P_{i,1})]| \leq \mathsf{negl}(\lambda).$$

In what follows, we denote $\mathcal{D}_{k+1,k}$ by $\mathcal{D}_k$. Note that the well-known k-Lin assumption can be captured as the $\mathcal{D}_k$-MDDH assumption.

Bilateral Variant. Let $\mathbb{G}, \mathbf{A}, \mathbf{k}_\beta$ be the same as above and $P_\beta := (\mathbb{G}, [\mathbf{A}]_1, [\mathbf{A}]_2, [\mathbf{k}_\beta]_1, [\mathbf{k}_\beta]_2)$. We say the bilateral $\mathcal{D}_{j,k}$-MDDH assumption holds with respect to $\mathcal{G}_{\mathsf{BG}}$ if P_0 and P_1 are computationally indistinguishable as above. The bilateral $\mathcal{D}_{j,k}$-MDDH assumption generically holds in bilinear groups if $k \geq 2$. Note that the following two properties are applicable to the bilateral case similarly.

Uniform Distribution. Let $\mathcal{U}_{j,k}$ be a uniform distribution over $\mathbb{Z}_p^{j\times k}$. Then, the following holds with tight reductions: $\mathcal{D}_k$-MDDH $\Rightarrow$ $\mathcal{U}_k$-MDDH $\Rightarrow$ $\mathcal{U}_{j,k}$-MDDH.

Random Self-Reducibility. We can obtain arbitrarily many instances of the $\mathcal{D}_{j,k}$-MDDH problem from a single instance. For any $n \in \mathbb{N}$, we define the following distribution: $\mathbf{A} \leftarrow \mathcal{D}_{j,k},\ \mathbf{Z} \leftarrow \mathbb{Z}_p^{k\times n},\ \mathbf{K}_0 := \mathbf{A}\mathbf{Z},\ \mathbf{K}_1 \leftarrow \mathbb{Z}_p^{j\times n},\ P_{i,\beta} := (\mathbb{G}, [\mathbf{A}]_i, [\mathbf{K}_\beta]_i)$. The n-fold $\mathcal{D}_{j,k}$-MDDH assumption is similarly defined to the $\mathcal{D}_{j,k}$-MDDH assumption. Then, the n-fold $\mathcal{D}_{j,k}$-MDDH assumption is implied by the $\mathcal{D}_{j,k}$-MDDH assumption with security loss of $\min\{n, j-k\}$.

2.3 Multi-Input Functional Encryption

There are several definitions for MIFE such as the public-key setting, secret-key setting, and multi-client setting [24]. We focus on the case where encryption keys are hidden from an adversary, which is called secret-key MIFE. In what follows, we omit the term "secret-key" since we only consider the secret-key variant. The definition of public-key MIFE is presented in Def. A.1.

Definition 2.3 (Multi-Input Functional Encryption). Let $\mathcal{F}$ be a function family such that, for all $f \in \mathcal{F}$, $f : \mathcal{X}_1 \times \cdots \times \mathcal{X}_n \to \mathcal{Z}$. An MIFE scheme for $\mathcal{F}$, MIFE, consists of four algorithms.

$\mathsf{Setup}(1^\lambda)$**:** It takes a security parameter 1^λ and outputs a public parameter PP and a master secret key MSK. The other three algorithms implicitly takes PP as input.

$\mathsf{Enc}(\mathsf{MSK}, i, x_i)$**:** It takes MSK, an index $i \in [n]$, and $x_i \in \mathcal{X}_i$ and outputs a ciphertext CT_i.

$\mathsf{KeyGen}(\mathsf{MSK}, f)$**:** It takes MSK, and $f \in \mathcal{F}$, and outputs a secret key SK.

$\mathsf{Dec}(\mathsf{CT}_1, \ldots, \mathsf{CT}_n, \mathsf{SK})$**:** It takes $\mathsf{CT}_1, \ldots, \mathsf{CT}_n$ and SK, and outputs a decryption value $d \in \mathcal{Z}$ or a symbol $\perp$.

When $n = 1$, we call it just a functional encryption (FE) scheme and omit the second argument of Enc.

Correctness. MIFE is *correct* if it satisfies the following condition. For all $\lambda \in \mathbb{N}$, $(x_1, \ldots, x_n) \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$, $f \in \mathcal{F}$, we have

$$\Pr\left[d = f(x_1, \ldots, x_n) \;\middle|\; \begin{array}{l} \mathsf{PP}, \mathsf{MSK} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{CT}_i \leftarrow \mathsf{Enc}(\mathsf{MSK}, i, x_i) \\ \mathsf{SK} \leftarrow \mathsf{KeyGen}(\mathsf{MSK}, f) \\ d := \mathsf{Dec}(\mathsf{CT}_1, \ldots, , \mathsf{CT}_n, \mathsf{SK}) \end{array} \right] = 1.$$

Security. We define two indistinguishability-based security definitions for MIFE, namely, message-hiding and function-hiding. For a stateful PPT adversary $\mathcal{A}$ and $\lambda \in \mathbb{N}$, let

$$\mathsf{P}^{\mathsf{MIFE},\beta}_{\mathcal{A},\mathsf{mh}}(\lambda) := \Pr\left[\beta' = 1 \;\middle|\; \begin{array}{l} \{i, x_i^{j,0}, x_i^{j,1}\}_{i \in [n], j \in [q_{\mathsf{CT},i}]} \leftarrow \mathcal{A}(1^\lambda) \\ \mathsf{PP}, \mathsf{MSK} \leftarrow \mathsf{Setup}(1^\lambda), \\ \mathsf{CT}_i^j \leftarrow \mathsf{Enc}(\mathsf{MSK}, i, x_i^{j,\beta}) \\ \beta' \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{MSK},\cdot)}(\mathsf{PP}, \{\mathsf{CT}_i^j\}_{i \in [n], j \in [q_{\mathsf{CT},i}]}) \end{array} \right].$$

Let q_{SK} be a number of queries to KeyGen. We say $\mathcal{A}$ is *admissible* if, in case of $q_{\mathsf{CT},1}, \ldots, q_{\mathsf{CT},n}, q_{\mathsf{SK}} \geq 1$, $\mathcal{A}$'s queries satisfy $f^\ell(x_1^{j_1,0}, \ldots, x_n^{j_n,0}) = f^\ell(x_1^{j_1,1}, \ldots, x_n^{j_n,1})$ for all $(j_1, \ldots, j_n) \in [q_{\mathsf{CT},1}] \times \cdots \times [q_{\mathsf{CT},n}]$ and $\ell \in [q_{\mathsf{SK}}]$. MIFE is *message-hiding* if, for all admissible PPT adversaries $\mathcal{A}$, the following advantage of $\mathcal{A}$ is negligible in λ: $\mathsf{Adv}^{\mathsf{MIFE}}_{\mathcal{A},\mathsf{mh}}(\lambda) := |\mathsf{P}^{\mathsf{MIFE},0}_{\mathcal{A},\mathsf{mh}}(\lambda) - \mathsf{P}^{\mathsf{MIFE},1}_{\mathcal{A},\mathsf{mh}}(\lambda)|$.

Next, we define a function-hiding property. Let $\mathsf{P}^{\mathsf{MIFE},\beta}_{\mathcal{A},\mathsf{fh}}(\lambda)$ be defined the same as $\mathsf{P}^{\mathsf{MIFE},\beta}_{\mathcal{A},\mathsf{mh}}(\lambda)$ except that $\mathcal{A}$'s oracle is $\mathcal{O}_{\mathsf{SK}}(\beta, \cdot)$ instead of $\mathsf{KeyGen}(\mathsf{MSK}, \cdot)$, where $\mathcal{O}_{\mathsf{SK}}(\beta, \cdot)$ takes (f^0, f^1) and outputs $\mathsf{KeyGen}(\mathsf{MSK}, f^\beta)$. This time, $\mathcal{A}$ is *admissible* if, in case of $q_{\mathsf{CT},1}, \ldots, q_{\mathsf{CT},n}, q_{\mathsf{SK}} \geq 1$, $\mathcal{A}$'s queries satisfy $f^{\ell,0}(x_1^{j_1,0}, \ldots, x_n^{j_n,0}) = f^{\ell,1}(x_1^{j_1,1}, \ldots, x_n^{j_n,1})$ for all $(j_1, \ldots, j_n) \in [q_{\mathsf{CT},1}] \times \cdots \times [q_{\mathsf{CT},n}]$ and $\ell \in [q_{\mathsf{SK}}]$. Then, MIFE is *function-hiding* if, for all admissible PPT adversaries $\mathcal{A}$, the following advantage of $\mathcal{A}$ is negligible in λ: $\mathsf{Adv}^{\mathsf{MIFE}}_{\mathcal{A},\mathsf{fh}}(\lambda) := |\mathsf{P}^{\mathsf{MIFE},0}_{\mathcal{A},\mathsf{fh}}(\lambda) - \mathsf{P}^{\mathsf{MIFE},1}_{\mathcal{A},\mathsf{fh}}(\lambda)|$.

Remark 2.1. These security definitions are the so-called selective security, where an adversary declares the challenge messages before it gets PP. We do not use the term "selective" in security definitions since we only consider the selective security throughout the paper.

Remark 2.2. In this paper, we assume that $q_{\mathsf{CT},i} \geq 1$ for all $i \in [n]$. Note that this condition can be easily removed by simply utilizing symmetric key encryption (SKE) [6, 19]. Roughly speaking, by encrypting all ciphertexts and secret keys with an SKE scheme and attaching the secret shares of the secret key of the SKE scheme to ciphertexts of the MIFE scheme, we can reduce the indistinguishability in the case where $q_{\mathsf{CT}} = 0$ for some $i \in [n]$ to the security of the SKE scheme. Furthermore, without loss of generality, we can assume that $q_{\mathsf{CT},1} = \cdots = q_{\mathsf{CT},n} (= q_{\mathsf{CT}})$.

We next define quadratic functions. Our scheme computes the functions on the exponent of a group element where the discrete log (DL) problem is hard. Thus, we need to bound norms of vectors used in the scheme so that the decryption algorithm can compute DL of function values. Note that this restriction is common in all previous FE schemes for inner products or quadratic functions based on cyclic groups. We formally define the functionality as follows.

Definition 2.4 (Bounded-Norm Multi-Input Quadratic functions over $\mathbb{Z}$). A function family $\mathcal{F}^{\mathsf{MQF}}_{m,n,X,C}$ for bounded-norm multi-input quadratic functions consist of functions $f : (\mathcal{X}^m)^n \to \mathbb{Z}$ where $\mathcal{X} = \{i \mid i \in \mathbb{Z}, |i| \leq X\}$. Each $f \in \mathcal{F}^{\mathsf{MQF}}_{m,n,X,C}$ is specified by $\mathbf{c} = \{c_{\mu,\nu}\}_{\mu,\nu \in [mn]} \in \mathbb{Z}^{(mn)^2}$ s.t. $||\mathbf{c}||_\infty \leq C$ and $c_{\mu,\nu} = 0$ if $\mu > \nu$. Let x_μ be the μ-th element of $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n) \in (\mathcal{X}^m)^n$. Then, f specified by $\mathbf{c}$ is defined as

$$f(\mathbf{x}_1, \ldots, \mathbf{x}_n) := \sum_{\mu,\nu \in [mn]} c_{\mu,\nu} x_\mu x_\nu.$$

3 Predicated Inner Product Functional Encryption

In this section, we define a new primitive called predicated inner product functional encryption and show how to construct it. We use it as a building block of our MQFE scheme.

3.1 Definitions

Definition 3.1 (Inner Products over Bilinear Groups). Let $\mathbb{G} = (p, G_1, G_2, G_T, g_1, g_2, e)$ be bilinear groups. A function family $\mathcal{F}^{\mathsf{IP}}_{m,\mathbb{G}}$ for inner products over bilinear groups consists of functions $f : G_1^m \to G_T$. Each $f \in \mathcal{F}^{\mathsf{IP}}_{m,\mathbb{G}}$ is specified by $[\mathbf{y}]_2$ where $\mathbf{y} \in \mathbb{Z}_p^m$ and defined as $f([\mathbf{x}]_1) := [\langle \mathbf{x}, \mathbf{y} \rangle]_T$.

Definition 3.2 (Predicated Inner Products over Bilinear Groups). A function family $\mathcal{F}^{\mathsf{PIP}}_{d,m,\mathbb{G}}$ for predicated inner products over bilinear groups consists of functions $f : \mathbb{Z}_p^d \times G_1^m \to G_T \cup \{\perp\}$. Each $f \in \mathcal{F}^{\mathsf{PIP}}_{d,m,\mathbb{G}}$ is specified by $\mathbf{y}_1 \in \mathbb{Z}_p^d$ and $[\mathbf{y}_2]_2$ where $\mathbf{y}_2 \in \mathbb{Z}_p^m$ and defined as

$$f(\mathbf{x}_1, [\mathbf{x}_2]_1) := \begin{cases} [\langle \mathbf{x}_2, \mathbf{y}_2 \rangle]_T & \text{if } \langle \mathbf{x}_1, \mathbf{y}_1 \rangle = 0 \\ \perp & \text{if } \langle \mathbf{x}_1, \mathbf{y}_1 \rangle \neq 0 \end{cases}.$$

We refer to FE for $\mathcal{F}^{\mathsf{IP}}_{m,\mathbb{G}}$ and $\mathcal{F}^{\mathsf{PIP}}_{d,m,\mathbb{G}}$ as IPFE and predicated IPFE, respectively.

Then, we define partially function-hiding security of FE for $\mathcal{F}^{\mathsf{PIP}}_{d,m,\mathbb{G}}$. Intuitively, partially function-hiding security guarantees that secret keys hide $\mathbf{y}_2$ (but do not $\mathbf{y}_1$).

Partially Function-Hiding Security. Let $\mathsf{pFE} = (\mathsf{pSetup}, \mathsf{pEnc}, \mathsf{pKeyGen}, \mathsf{pDec})$ be a FE scheme for $\mathcal{F}^{\mathsf{PIP}}_{d,m,\mathbb{G}}$. For a stateful PPT adversary $\mathcal{A}$ and $\lambda \in \mathbb{N}$, let

$$\mathsf{P}^{\mathsf{pFE},\beta}_{\mathcal{A},\mathsf{pfh}}(\lambda) := \Pr\left[\beta' = 1 \;\middle|\; \begin{array}{l} \{\mathbf{x}_1^j, [\mathbf{x}_2^{j,0}]_1, [\mathbf{x}_2^{j,1}]_1\}_{j \in [q_{\mathsf{CT}}]} \leftarrow \mathcal{A}(1^\lambda) \\ \mathsf{pPP}, \mathsf{pMSK} \leftarrow \mathsf{pSetup}(1^\lambda), \\ \mathsf{pCT}^j \leftarrow \mathsf{pEnc}(\mathsf{pMSK}, (\mathbf{x}_1^j, [\mathbf{x}_2^{j,\beta}]_1)) \\ \beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{SK}}(\beta,\cdot)}(\mathsf{pPP}, \{\mathsf{pCT}^j\}_{j \in [q_{\mathsf{CT}}]}) \end{array}\right]$$

where $\mathcal{O}_{\mathsf{SK}}$ takes $(\mathbf{y}_1, [\mathbf{y}_2^0]_2, [\mathbf{y}_2^1]_2)$ and outputs $\mathsf{pKeyGen}(\mathsf{MSK}, (\mathbf{y}_1, [\mathbf{y}_2^\beta]_2))$. Let q_{SK} be a number of queries to $\mathcal{O}_{\mathsf{SK}}$. We say $\mathcal{A}$ is *admissible* if $\mathcal{A}$'s queries satisfy $\langle \mathbf{x}_2^{j,0}, \mathbf{y}_2^{\ell,0} \rangle = \langle \mathbf{x}_2^{j,1}, \mathbf{y}_2^{\ell,1} \rangle$ *when* $\langle \mathbf{x}_1^j, \mathbf{y}_1^\ell \rangle = 0$ for all $j \in [q_{\mathsf{CT}}]$ and $\ell \in [q_{\mathsf{SK}}]$. pFE is *partially function-hiding* if, for all admissible PPT adversaries $\mathcal{A}$, the following advantage of $\mathcal{A}$ is negligible in λ: $\mathsf{Adv}^{\mathsf{pFE}}_{\mathcal{A},\mathsf{pfh}}(\lambda) := |\mathsf{P}^{\mathsf{pFE},0}_{\mathcal{A},\mathsf{pfh}}(\lambda) - \mathsf{P}^{\mathsf{pFE},1}_{\mathcal{A},\mathsf{pfh}}(\lambda)|$.

3.2 Predicated IPFE from IPFE

We construct a partially function-hiding FE scheme for $\mathcal{F}^{\mathsf{PIP}}_{d,m,\mathbb{G}}$ from a function-hiding FE scheme for $\mathcal{F}^{\mathsf{IP}}_{kd+2m+1,\mathbb{G}}$ in a generic way. Note that k is a parameter for the MDDH assumption. A function-hiding FE scheme for $\mathcal{F}^{\mathsf{IP}}_{m,\mathbb{G}}$ based on MDDH is easily obtained from a function-hiding inner product FE scheme described in [32, Appx. A], which is obtained by applying Lin's technique to the IPFE scheme by Abdalla *et al.* [6,30]. This is since the scheme works even if input vectors for Enc and KeyGen consist of group elements, and Dec first obtains decryption values on the exponent of a target-group generator and then computes its discrete log.

Construction. Let $\mathsf{iFE} = (\mathsf{iSetup}, \mathsf{iEnc}, \mathsf{iKeyGen}, \mathsf{iDec})$ be a function-hiding FE scheme for $\mathcal{F}^{\mathsf{IP}}_{kd+2m+1,\mathbb{G}}$. Then, our partially function-hiding FE scheme $\mathsf{pFE} = (\mathsf{pSetup}, \mathsf{pEnc}, \mathsf{pKeyGen}, \mathsf{pDec})$ for $\mathcal{F}^{\mathsf{PIP}}_{d,m,\mathbb{G}}$ is constructed as follows.

$\mathsf{pSetup}(1^\lambda)$**:** It outputs $(\mathsf{pPP}, \mathsf{pMSK}) := (\mathsf{iPP}, \mathsf{iMSK}) \leftarrow \mathsf{iSetup}(1^\lambda)$.
$\mathsf{pEnc}(\mathsf{MSK}, (\mathbf{x}_1, [\mathbf{x}_2]_1))$**:** It outputs pCT as follows:

$$\mathbf{z} \leftarrow \mathbb{Z}_p^k,\ \mathbf{x} := (\mathbf{z} \otimes \mathbf{x}_1, \mathbf{x}_2, 0^m, 0) \in \mathbb{Z}_p^{kd+2m+1}$$
$$\mathsf{iCT} \leftarrow \mathsf{iEnc}(\mathsf{iMSK}, [\mathbf{x}]_1),\ \mathsf{pCT} := (\mathbf{x}_1, \mathsf{iCT}).$$

$\mathsf{pKeyGen}(\mathsf{pMSK}, (\mathbf{y}_1, [\mathbf{y}_2]_2))$**:** It outputs SK as follows:

$$\mathbf{a} \leftarrow \mathbb{Z}_p^k,\ \mathbf{y} := (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2, 0^m, 0) \in \mathbb{Z}_p^{kd+2m+1}$$
$$\mathsf{iSK} \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}, [\mathbf{y}]_2),\ \mathsf{pSK} := (\mathbf{y}_1, \mathsf{iSK}).$$

$\mathsf{pDec}(\mathsf{pCT}, \mathsf{pSK})$**:** If $\langle \mathbf{x}_1, \mathbf{y}_1 \rangle \neq 0$, it outputs $\perp$. Otherwise, outputs $\mathsf{iDec}(\mathsf{iCT}, \mathsf{iSK})$.

Correctness. Since $\langle \mathbf{z} \otimes \mathbf{x}_1, \mathbf{a} \otimes \mathbf{y}_1 \rangle = \langle \mathbf{z}, \mathbf{a} \rangle \cdot \langle \mathbf{x}_1, \mathbf{y}_1 \rangle$, $\mathsf{iDec}(\mathsf{iCT}, \mathsf{iSK})$ outputs $[\langle \mathbf{x}, \mathbf{y} \rangle]_T = [\langle \mathbf{x}_2, \mathbf{y}_2 \rangle]_T$ if $\langle \mathbf{x}_1, \mathbf{y}_1 \rangle = 0$. This follows from the correctness of iFE.

3.3 Security of Our Predicated Inner Product FE Scheme

For security, we have the following theorem.

Theorem 3.1. *If* iFE *is function-hiding, and the MDDH assumption holds in* $\mathbb{G}$*, then* pFE *is partially function-hiding. More precisely, for all PPT adversaries* $\mathcal{A}$*, there exist PPT adversaries* $\mathcal{B}_1, \mathcal{B}_2$ *such that*

$$\mathsf{Adv}^{\mathsf{pFE}}_{\mathcal{A},\mathsf{pfh}}(\lambda) \leq q_{\mathsf{CT}}(3\mathsf{Adv}^{\mathsf{iFE}}_{\mathcal{B}_1,\mathsf{fh}}(\lambda) + 2\mathsf{Adv}^{\mathcal{D}_k\text{-}\mathsf{MDDH}}_{\mathcal{B}_2}(\lambda)).$$

Proof. We prove Theorem 3.1 via a series of hybrid games $\mathsf{H}_{\iota,1}, \dots, \mathsf{H}_{\iota,5}$ for $\iota \in [q_{\mathsf{CT}}]$. We show that $\mathsf{G}_0 \approx_c \mathsf{H}_{1,1} \approx_c \cdots \approx_c \mathsf{H}_{1,5} \approx_c \mathsf{H}_{2,1} \approx_c \cdots \approx_c \mathsf{H}_{q_{\mathsf{CT}},4} \approx_c \mathsf{G}_1$, where G_β for $\beta \in \{0,1\}$ is the original security game (described in Fig 1). Each hybrid is defined as follows.

$\mathsf{H}_{\iota,1}$**:** This game is the same as G_0 except that

- for $j \in [q_{\mathsf{CT}}]$, $\mathbf{x}^j$ to be encrypted is set as

$$\mathbf{x}^j := \begin{cases} (\mathbf{z}^j \otimes \mathbf{x}_1^j, \boxed{0^m, \mathbf{x}_2^{j,1}}, 0) & \text{if } j < \iota \\ (\boxed{0^{kd}}, \mathbf{x}_2^{j,0}, 0^m, \boxed{1}) & \text{if } j = \iota \\ (\mathbf{z}^j \otimes \mathbf{x}_1^j, \mathbf{x}_2^{j,0}, 0^m, 0) & \text{if } j > \iota \end{cases} \tag{3.1}$$

- $\mathcal{O}_{\mathsf{SK}}$ sets $\mathbf{y} := (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2^0, \boxed{\mathbf{y}_2^1, \langle \mathbf{z}^\iota, \mathbf{a} \rangle \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1 \rangle})$ for all queries.

```
$\underline{\mathsf{G}_\beta}$
$\{\mathbf{x}_1^j, [\mathbf{x}_2^{j,0}]_1, [\mathbf{x}_2^{j,1}]_1\}_{j \in [q_{\mathsf{CT}}]} \leftarrow \mathcal{A}(1^\lambda)$
$(\mathsf{pPP}, \mathsf{pMSK}) := (\mathsf{iPP}, \mathsf{iMSK}) \leftarrow \mathsf{iSetup}(1^\lambda)$
$\mathbf{z}^j \leftarrow \mathbb{Z}_p^k,\ \mathbf{x}^j := (\mathbf{z}^j \otimes \mathbf{x}_1^j, \mathbf{x}_2^{j,\beta}, 0^m, 0) \in \mathbb{Z}_p^{kd+2m+1}$
$\mathsf{iCT}^j \leftarrow \mathsf{iEnc}(\mathsf{iMSK}, [\mathbf{x}^j]_1),\ \mathsf{pCT}^j := (\mathbf{x}_1^j, \mathsf{iCT}^j)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{SK}}(\beta,\cdot)}(\mathsf{pPP}, \{\mathsf{pCT}^j\}_{j \in [q_{\mathsf{CT}}]})$
$\underline{\mathcal{O}_{\mathsf{SK}}(\beta,\cdot)}$
Input: $(\mathbf{y}_1, [\mathbf{y}_2^0]_2, [\mathbf{y}_2^1]_2)$
$\mathbf{a} \leftarrow \mathbb{Z}_p^k,\ \mathbf{y} := (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2^\beta, 0^m, 0) \in \mathbb{Z}_p^{kd+2m+1}$
$\mathsf{iSK} \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}, [\mathbf{y}]_2),\ \mathsf{pSK} := (\mathbf{y}_1, \mathsf{iSK})$
Output: $\mathsf{pSK}$
```

Fig 1. Partially function-hiding security game for pFE.

$\mathsf{H}_{\iota,2}$**:** This game is the same as $\mathsf{H}_{\iota,1}$ except that $\mathcal{O}_{\mathsf{SK}}$ samples $t \leftarrow \mathbb{Z}_p$ and sets $\mathbf{y} := (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2^0, \mathbf{y}_2^1, \boxed{t} \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1 \rangle)$ for each query.

$\mathsf{H}_{\iota,3}$**:** This game is the same as $\mathsf{H}_{\iota,2}$ except that $\mathbf{x}_\iota := (0^{kd}, \boxed{0^m, \mathbf{x}_2^{\iota,1}}, 1)$.

$\mathsf{H}_{\iota,4}$**:** This game is the same as $\mathsf{H}_{\iota,3}$ except that $\mathcal{O}_{\mathsf{SK}}$ sets $\mathbf{y} := (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2^0, \mathbf{y}_2^1, \boxed{\langle \mathbf{z}^\iota, \mathbf{a} \rangle} \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1 \rangle)$ for all queries.

$\mathsf{H}_{\iota,5}$ ($\iota \in [q_{\mathsf{CT}} - 1]$)**:** This game is the same as $\mathsf{H}_{\iota,4}$ except that

- $\mathbf{x}^\iota := (\boxed{\mathbf{z}^\iota \otimes \mathbf{x}_1^\iota}, 0^m, \mathbf{x}_2^{\iota,1}, \boxed{0})$;
- $\mathcal{O}_{\mathsf{SK}}$ sets $\mathbf{y} := (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2^0, \mathbf{y}_2^1, \boxed{0})$ for all queries.

Thanks to Lemmata 3.1 to 3.5, Theorem 3.1 holds. □

Next, we prove the indistinguishability of each pair of hybrid games. Let $\mathsf{P}(\mathcal{A}, \mathsf{G})$ be the probability that $\mathcal{A}$ outputs 1 in a security game G with the security parameter being λ, i.e., $\mathsf{P}(\mathcal{A}, \mathsf{G}_\beta) = \mathsf{P}_{\mathcal{A},\mathsf{pfh}}^{\mathsf{pFE},\beta}(\lambda)$.

Lemma 3.1. *Let* $\mathsf{H}_{0,5} = \mathsf{G}_0$*. For all PPT adversaries* $\mathcal{A}$ *and* $\iota \in [q_{\mathsf{CT}}]$*, there exists a PPT adversary* $\mathcal{B}$ *such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota-1,5}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,1})| \leq \mathsf{Adv}_{\mathcal{B},\mathsf{fh}}^{\mathsf{iFE}}(\lambda)$.

Proof. Recall that the differences between $\mathsf{H}_{\iota-1,5}$ and $\mathsf{H}_{\iota,1}$ are

- $\mathbf{x}^\iota := (\mathbf{z}^\iota \otimes \mathbf{x}_1^\iota, \mathbf{x}_2^{\iota,0}, 0^m, 0) \longrightarrow \mathbf{x}^\iota := (0^{kd}, \mathbf{x}_2^{\iota,0}, 0^m, 1)$;
- $\mathbf{y} := \begin{cases} (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2^0, 0^m, 0) & \text{if } \iota = 1 \\ (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2^0, \mathbf{y}_2^1, 0) & \text{if } \iota > 1 \end{cases} \longrightarrow \mathbf{y} := (\mathbf{a} \otimes \mathbf{y}_1, \mathbf{y}_2^0, \mathbf{y}_2^1, \langle \mathbf{z}^\iota, \mathbf{a} \rangle \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1 \rangle)$.

For $j \in [q_{\mathsf{CT}}]$ and $\ell \in [q_{\mathsf{SK}}]$, let $\mathbf{x}^{j,0}$ and $\mathbf{y}^{\ell,0}$ be $\mathbf{x}^j$ and $\mathbf{y}^\ell$ defined in $\mathsf{H}_{\iota-1,5}$, respectively. Similarly, let $\mathbf{x}^{j,1}$ and $\mathbf{y}^{\ell,1}$ be $\mathbf{x}^j$ and $\mathbf{y}^\ell$ defined in $\mathsf{H}_{\iota,1}$, respectively. Then, it is not hard to see that we have $\langle \mathbf{x}^{j,0}, \mathbf{y}^{\ell,0} \rangle = \langle \mathbf{x}^{j,1}, \mathbf{y}^{\ell,1} \rangle$ for all $j \in [q_{\mathsf{CT}}]$ and $\ell \in [q_{\mathsf{SK}}]$. Thus, we can reduce the indistinguishability between $\mathsf{H}_{\iota-1,5}$ and $\mathsf{H}_{\iota,1}$ to the function-hiding property of iFE. Note that since $\mathbf{x}^j$ is independent of $\mathbf{y}_1^\ell, \mathbf{y}_2^{\ell,0}, \mathbf{y}_2^{\ell,1}$, the adaptiveness of secret-key queries does not become a matter in the reduction. This concludes the proof. □

Lemma 3.2. *For all PPT adversaries* $\mathcal{A}$ *and* $\iota \in [q_{\mathsf{CT}}]$*, there exists a PPT adversary* $\mathcal{B}$ *such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,1}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,2})| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathcal{U}_{q_{\mathsf{SK}},k}\text{-MDDH}}(\lambda)$.

Proof. We describe the reduction $\mathcal{B}$.

1. $\mathcal{B}$ obtains a $\mathcal{U}_{q_{\mathsf{SK}},k}$-MDDH instance $(\mathbb{G}, [\mathbf{A}]_2, [\mathbf{k}_\beta]_2)$, where $\mathbf{A} \in \mathbb{Z}_p^{q_{\mathsf{SK}} \times k}$, $\mathbf{k}_0 = \mathbf{A}\mathbf{z}$, $\mathbf{k}_1 \leftarrow \mathbb{Z}_p^{q_{\mathsf{SK}}}$.
2. When $\mathcal{A}$ outputs $\{\mathbf{x}_1^j, [\mathbf{x}_2^{j,0}]_1, [\mathbf{x}_2^{j,1}]_1\}_{j \in [q_{\mathsf{CT}}]}$, $\mathcal{B}$ sets $(\mathsf{pPP}, \mathsf{pMSK}) := (\mathsf{iPP}, \mathsf{iMSK}) \leftarrow \mathsf{iSetup}$ and gives $\mathsf{pPP}, \{\mathsf{pCT}^j := (\mathbf{x}_1^j, \mathsf{iEnc}(\mathsf{iMSK}, [\mathbf{x}^j]_1))\}_{j \in [q_{\mathsf{CT}}]}$ to $\mathcal{A}$, where $\mathbf{x}^j$ is set as Eq. (3.1).

3. For the ℓ-th query to $\mathcal{O}_{\mathsf{SK}}$ on $(\mathbf{y}_1^\ell, [\mathbf{y}_2^{\ell,0}]_2, [\mathbf{y}_2^{\ell,1}]_2)$, $\mathcal{B}$ replies pSK by setting $\mathbf{y}^\ell := (\mathbf{a}^\ell \otimes \mathbf{y}_1^\ell, \mathbf{y}_2^{\ell,0}, \mathbf{y}_2^{\ell,1}, k_{\beta,\ell} \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1^\ell \rangle)$, where $\mathbf{a}^\ell$ is the ℓ-th row of $\mathbf{A}$ and $k_{\beta,\ell}$ is the ℓ-th entry of $\mathbf{k}_\beta$.
4. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

It is not hard to see that $\mathcal{A}$'s view corresponds to $\mathsf{H}_{\iota,1}$ if $\beta = 0$ and $\mathsf{H}_{\iota,2}$ otherwise. Note that $\mathcal{U}_{q_{\mathsf{SK}},k}$-MDDH is tightly reduced to $\mathcal{D}_k$-MDDH. □

Lemma 3.3. *For all PPT adversaries $\mathcal{A}$ and $\iota \in [q_{\mathsf{CT}}]$, there exists a PPT adversary $\mathcal{B}$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,2}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,3})| \leq \mathsf{Adv}_{\mathcal{B},\mathsf{fh}}^{\mathsf{iFE}}(\lambda)$.

Proof. Let $\mathbf{x}^{j,0}$ be $\mathbf{x}^j$ defined in $\mathsf{H}_{\iota,2}$, i.e., as in Eq. (3.1), and $\mathbf{x}^{j,1}$ be $\mathbf{x}^j$ defined in $\mathsf{H}_{\iota,3}$, i.e., the same as in Eq. (3.1) except that $\mathbf{x}^\iota := (0^{kd}, 0^m, \mathbf{x}_2^{\iota,1}, 1)$. Let us define that

$$\mathbf{y}^{\ell,0} := (\mathbf{a}^\ell \otimes \mathbf{y}_1^\ell, \mathbf{y}_2^{\ell,0}, \mathbf{y}_2^{\ell,1}, t_\ell \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1^\ell \rangle)$$
$$\mathbf{y}^{\ell,1} := (\mathbf{a}^\ell \otimes \mathbf{y}_1^\ell, \mathbf{y}_2^{\ell,0}, \mathbf{y}_2^{\ell,1}, t_\ell \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1^\ell \rangle + (\langle \mathbf{x}_2^{\iota,0}, \mathbf{y}_2^{\ell,0} \rangle - \langle \mathbf{x}_2^{\iota,1}, \mathbf{y}_2^{\ell,1} \rangle)).$$

Then, it is not hard to see that we have $\langle \mathbf{x}^{j,0}, \mathbf{y}^{\ell,0} \rangle = \langle \mathbf{x}^{j,1}, \mathbf{y}^{\ell,1} \rangle$ for all $j \in [q_{\mathsf{CT}}]$ and $\ell \in [q_{\mathsf{SK}}]$. Thus, we can reduce the indistinguishability between the 0-side and 1-side to the function-hiding property of iFE. Here, we have the two cases:

$\langle \mathbf{x}_1^\iota, \mathbf{y}_1^\ell \rangle = 0$: The game condition imposes $\langle \mathbf{x}_2^{\iota,0}, \mathbf{y}_2^{\ell,0} \rangle - \langle \mathbf{x}_2^{\iota,1}, \mathbf{y}_2^{\ell,1} \rangle = 0$ on $\mathcal{A}$.

$\langle \mathbf{x}_1^\iota, \mathbf{y}_1^\ell \rangle \neq 0$: Since t_ℓ is distributed randomly in $\mathbb{Z}_p$, the terms $t_\ell \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1^\ell \rangle$ and $t_\ell \cdot \langle \mathbf{x}_1^\iota, \mathbf{y}_1^\ell \rangle + (\langle \mathbf{x}_2^{\iota,0}, \mathbf{y}_2^{\ell,0} \rangle - \langle \mathbf{x}_2^{\iota,1}, \mathbf{y}_2^{\ell,1} \rangle)$ are also distributed randomly.

Hence, $\mathbf{y}^{\ell,0}$ and $\mathbf{y}^{\ell,1}$ are identically distributed in both cases, which means that the 0-side corresponds to $\mathsf{H}_{\iota,2}$ and the 1-side corresponds to $\mathsf{H}_{\iota,3}$. □

Lemma 3.4. *For all PPT adversaries $\mathcal{A}$ and $\iota \in [q_{\mathsf{CT}}]$, there exists a PPT adversary $\mathcal{B}$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,3}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,4})| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathcal{U}_{q_{\mathsf{SK}},k}\text{-}\mathsf{MDDH}}(\lambda)$.

We omit the proof since Lemma 3.4 can be proven similarly to Lemma 3.2.

Lemma 3.5. *Let $\mathsf{H}_{q_{\mathsf{CT}},5} = \mathsf{G}_1$. For all PPT adversaries $\mathcal{A}$ and $\iota \in [q_{\mathsf{CT}}]$, there exists a PPT adversary $\mathcal{B}$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,4}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota,5})| \leq \mathsf{Adv}_{\mathcal{B},\mathsf{fh}}^{\mathsf{iFE}}(\lambda)$.

We omit the proof since Lemma 3.5 can be proven similarly to Lemma 3.1.

4 Multi-Input Mixed-Group Inner Product Functional Encryption

In this section, we define a new primitive called multi-input mixed-group inner product functional encryption and show how to construct it. We use it as a building block of our MQFE scheme.

4.1 Definitions

Definition 4.1 (Multi-Input Inner Products over Bilinear Groups). Let $\mathbb{G} = (p, G_1, G_2, G_T, g_1, g_2, e)$ be bilinear groups. A function family $\mathcal{F}_{m,n,\mathbb{G}}^{\mathsf{MIP}}$ for multi-input inner products over bilinear groups consists of functions $f : (G_1^m)^n \to G_T$. Each $f \in \mathcal{F}_{m,n,\mathbb{G}}^{\mathsf{MIP}}$ is specified by $[\mathbf{y}_1]_2, \ldots, [\mathbf{y}_n]_2$ where $\mathbf{y}_i \in \mathbb{Z}_p^m$ and defined as $f([\mathbf{x}]_1, \ldots, [\mathbf{x}]_n) := [\sum_{i \in [n]} \langle \mathbf{x}_i, \mathbf{y}_i \rangle]_T$.

Definition 4.2 (Multi-Input Mixed-Group Inner Products over Bilinear Groups). Let $\mathbb{G} = (p, G_1, G_2, G_T, g_1, g_2, e)$ be bilinear groups. A function family $\mathcal{F}_{m_1,m_2,n,\mathbb{G}}^{\mathsf{MGIP}}$ for multi-input mixed-group inner products over bilinear groups consists of functions $f : (G_1^{m_1} \times G_2^{m_2})^n \to G_T$. Each $f \in \mathcal{F}_{m_1,m_2,n,\mathbb{G}}^{\mathsf{MGIP}}$ is specified by $([\mathbf{y}_{1,1}]_2, [\mathbf{y}_{1,2}]_1, \ldots, [\mathbf{y}_{n,1}]_2, [\mathbf{y}_{n,2}]_1)$ where $\mathbf{y}_{i,1} \in \mathbb{Z}_p^{m_1}$ and $\mathbf{y}_{i,2} \in \mathbb{Z}_p^{m_2}$ and defined as $f(([\mathbf{x}_{1,1}]_1, [\mathbf{x}_{1,2}]_2), \ldots, ([\mathbf{x}_{n,1}]_1, [\mathbf{x}_{n,2}]_2)) := [\langle \mathbf{x}, \mathbf{y} \rangle]_T$ where $\mathbf{x} := (\mathbf{x}_{1,1}, \mathbf{x}_{1,2}, \ldots, \mathbf{x}_{n,1}, \mathbf{x}_{n,2})$ and $\mathbf{y} := (\mathbf{y}_{1,1}, \mathbf{y}_{1,2}, \ldots, \mathbf{y}_{n,1}, \mathbf{y}_{n,2})$.

We refer to MIFE for $\mathcal{F}_{m,n,\mathbb{G}}^{\mathsf{MIP}}$ and $\mathcal{F}_{m_1,m_2,n,\mathbb{G}}^{\mathsf{MGIP}}$ as MIPFE and multi-input mixed-group IPFE, respectively.

4.2 Multi-Input Mixed-Group IPFE from MIPFE

Let $\mathcal{F}^{\mathsf{IP}'}_{m,\mathbb{G}}$ be a function class defined the same as $\mathcal{F}^{\mathsf{IP}}_{m,\mathbb{G}}$ in Def. 3.1 except that G_1 and G_2 are switched, that is, each $f : G_2^m \to G_T$ is specified by $[\mathbf{y}]_1$. We construct a function-hiding MIFE scheme for $\mathcal{F}^{\mathsf{MGIP}}_{m_1,m_2,n,\mathbb{G}}$ from a function-hiding MIFE scheme for $\mathcal{F}^{\mathsf{MIP}}_{m_1+m_2+k+1,n,\mathbb{G}}$ and function-hiding FE scheme for $\mathcal{F}^{\mathsf{IP}'}_{m_2+k+1,\mathbb{G}}$ in a generic way. Note that k is a parameter for the MDDH assumption. A function-hiding MIFE scheme for $\mathcal{F}^{\mathsf{MIP}}_{m,n,\mathbb{G}}$ based on MDDH is easily obtained from a function-hiding multi-input IPFE schemes in [4,19,32]. This is since these schemes in the literetures work even if input vectors for Enc and KeyGen consist of group elements, and Dec first obtains decryption values on the exponent of a target-group generator and then computes its discrete log.

Construction. Let $\mathsf{miFE} = (\mathsf{miSetup}, \mathsf{miEnc}, \mathsf{miKeyGen}, \mathsf{miDec})$ be a function-hiding MIFE scheme for $\mathcal{F}^{\mathsf{MIP}}_{m_1+m_2+k+1,n,\mathbb{G}}$ and $\mathsf{iFE} = (\mathsf{iSetup}, \mathsf{iEnc}, \mathsf{iKeyGen}, \mathsf{iDec})$ be a function-hiding FE scheme for $\mathcal{F}^{\mathsf{IP}'}_{m_2+k+1,\mathbb{G}}$. Then, our function-hiding MIFE scheme $\mathsf{gFE} = (\mathsf{gSetup}, \mathsf{gEnc}, \mathsf{gKeyGen}, \mathsf{gDec})$ for $\mathcal{F}^{\mathsf{MGIP}}_{m_1,m_2,n,\mathbb{G}}$ is constructed as follows.

$\mathsf{gSetup}(1^\lambda)$**:** It outputs $\mathsf{gPP}, \mathsf{gMSK}$ as follows:

$$\begin{aligned}&\mathsf{miPP}, \mathsf{miMSK} \leftarrow \mathsf{miSetup}(1^\lambda),\ (\mathsf{iPP}_1, \mathsf{iMSK}_1), \dots, (\mathsf{iPP}_n, \mathsf{iMSK}_n) \leftarrow \mathsf{iSetup}(1^\lambda)\\ &\mathsf{gPP} := (\mathsf{miPP}, \mathsf{iPP}_1, \dots, \mathsf{iPP}_n),\ \mathsf{gMSK} := (\mathsf{miMSK}, \mathsf{iMSK}_1, \dots, \mathsf{iMSK}_n).\end{aligned}$$

$\mathsf{gEnc}(\mathsf{MSK}, i, ([\mathbf{x}_{i,1}]_1, [\mathbf{x}_{i,2}]_2))$**:** It outputs CT_i as follows:

$$\begin{aligned}&\mathbf{z} \leftarrow \mathbb{Z}_p^k,\ \widetilde{\mathbf{x}}_{i,1} := (\mathbf{x}_{i,1}, 0^{m_2}, \mathbf{z}, 0) \in \mathbb{Z}_p^{m_1+m_2+k+1},\ \widetilde{\mathbf{x}}_{i,2} := (\mathbf{x}_{i,2}, -\mathbf{z}, 0) \in \mathbb{Z}_p^{m_2+k+1}\\ &\mathsf{miCT}_i \leftarrow \mathsf{miEnc}(\mathsf{miMSK}, i, [\widetilde{\mathbf{x}}_{i,1}]_1),\ \mathsf{iCT}_i \leftarrow \mathsf{iEnc}(\mathsf{iMSK}_i, [\widetilde{\mathbf{x}}_{i,2}]_2)\\ &\mathsf{gCT}_i := (\mathsf{miCT}_i, \mathsf{iCT}_i).\end{aligned}$$

$\mathsf{gKeyGen}(\mathsf{MSK}, \{[\mathbf{y}_{i,1}]_2, [\mathbf{y}_{i,2}]_1\}_{i\in[n]})$**:** It outputs SK as follows:

$$\begin{aligned}&\mathbf{a} \leftarrow \mathbb{Z}_p^k,\ \widetilde{\mathbf{y}}_{i,1} := (\mathbf{y}_{i,1}, 0^{m_2}, \mathbf{a}, 0) \in \mathbb{Z}_p^{m_1+m_2+k+1},\ \widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}_{i,2}, \mathbf{a}, 0) \in \mathbb{Z}_p^{m_2+k+1}\\ &\widetilde{\mathbf{y}} := (\widetilde{\mathbf{y}}_{1,1}, \dots, \widetilde{\mathbf{y}}_{n,1}),\ \mathsf{miSK} \leftarrow \mathsf{miKeyGen}(\mathsf{miMSK}, [\widetilde{\mathbf{y}}]_2)\\ &\mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}_i, [\widetilde{\mathbf{y}}_{i,2}]_1),\ \mathsf{gSK} := (\mathsf{miSK}, \{\mathsf{iSK}_i\}_{i\in[n]}).\end{aligned}$$

$\mathsf{gDec}(\mathsf{gCT}_1, \dots, \mathsf{gCT}_n, \mathsf{gSK})$**:** It outputs

$$\mathsf{miDec}(\mathsf{miCT}_1, \dots, \mathsf{miCT}_n, \mathsf{miSK}) \prod_{i\in[n]} \mathsf{iDec}(\mathsf{iCT}_i, \mathsf{iSK}_i).$$

Correctness. Due to the correctness of miFE and iFE, gDec outputs

$$\left[\sum_{i\in[n]} (\langle \widetilde{\mathbf{x}}_{i,1}, \widetilde{\mathbf{y}}_{i,1}\rangle + \langle \widetilde{\mathbf{x}}_{i,2}, \widetilde{\mathbf{y}}_{i,2}\rangle)\right]_T = \left[\sum_{i\in[n]} (\langle \mathbf{x}_{i,1}, \mathbf{y}_{i,1}\rangle + \langle \mathbf{x}_{i,2}, \mathbf{y}_{i,2}\rangle)\right]_T.$$

4.3 Security of Our Multi-Input Mixed-Group IPFE scheme

For security, we have the following theorem.

Theorem 4.1. *If* miFE *and* iFE *are function-hiding, and the bilateral MDDH assumption holds in* $\mathbb{G}$*, then* gFE *is function-hiding. More precisely, for all PPT adversaries* $\mathcal{A}$*, there exist PPT adversaries* $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ *such that*

$$\mathsf{Adv}^{\mathsf{gFE}}_{\mathcal{A},\mathsf{fh}}(\lambda) \le (4q_{\mathsf{CT}} + 1)\mathsf{Adv}^{\mathsf{miFE}}_{\mathcal{B}_1,\mathsf{fh}}(\lambda) + n(4q_{\mathsf{CT}} + 1)\mathsf{Adv}^{\mathsf{iFE}}_{\mathcal{B}_2,\mathsf{fh}}(\lambda) + 4nq_{\mathsf{CT}}\mathsf{Adv}^{\mathsf{bi}\text{-}\mathcal{D}_k\text{-}\mathsf{MDDH}}_{\mathcal{B}_3}(\lambda).$$

```
$\underline{\mathsf{G}_\beta}$
$\{i, ([\mathbf{x}^{j,0}_{i,1}]_1, [\mathbf{x}^{j,0}_{i,2}]_2), ([\mathbf{x}^{j,1}_{i,1}]_1, [\mathbf{x}^{j,1}_{i,2}]_2)\}_{i\in[n], j\in[q_{\mathsf{CT}}]} \leftarrow \mathcal{A}(1^\lambda)$
$\mathsf{miPP}, \mathsf{miMSK} \leftarrow \mathsf{miSetup}(1^\lambda),\ (\mathsf{iPP}_1, \mathsf{iMSK}_1), \ldots, (\mathsf{iPP}_n, \mathsf{iMSK}_n) \leftarrow \mathsf{iSetup}(1^\lambda)$
$\mathsf{gPP} := (\mathsf{miPP}, \mathsf{iPP}_1, \ldots, \mathsf{iPP}_n),\ \mathsf{gMSK} := (\mathsf{miMSK}, \mathsf{iMSK}_1, \ldots, \mathsf{iMSK}_n)$
$\mathbf{z}^j_i \leftarrow \mathbb{Z}^k_p,\ \widetilde{\mathbf{x}}^j_{i,1} := (\mathbf{x}^{j,\beta}_{i,1}, 0^{m_2}, \mathbf{z}^j_i, 0),\ \widetilde{\mathbf{x}}^j_{i,2} := (\mathbf{x}^{j,\beta}_{i,2}, -\mathbf{z}^j_i, 0)$
$\mathsf{miCT}^j_i \leftarrow \mathsf{miEnc}(\mathsf{miMSK}, i, [\widetilde{\mathbf{x}}^j_{i,1}]_1),\ \mathsf{iCT}^j_i \leftarrow \mathsf{iEnc}(\mathsf{iMSK}_i, [\widetilde{\mathbf{x}}^j_{i,2}]_2),\ \mathsf{gCT}^j_i := (\mathsf{miCT}^j_i, \mathsf{iCT}^j_i)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{SK}}(\beta,\cdot)}(\mathsf{gPP}, \{\mathsf{gCT}^j_i\}_{i\in[n], j\in[q_{\mathsf{CT}}]})$
---
$\underline{\mathcal{O}_{\mathsf{SK}}(\beta,\cdot)}$
Input: $\{([\mathbf{y}^0_{i,1}]_2, [\mathbf{y}^0_{i,2}]_1), ([\mathbf{y}^1_{i,1}]_2, [\mathbf{y}^1_{i,2}]_1)\}_{i\in[n]}$
$\mathbf{a} \leftarrow \mathbb{Z}^k_p,\ \widetilde{\mathbf{y}}_{i,1} := (\mathbf{y}^\beta_{i,1}, 0^{m_2}, \mathbf{a}, 0),\ \widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}^\beta_{i,2}, \mathbf{a}, 0)$
$\widetilde{\mathbf{y}} := (\widetilde{\mathbf{y}}_{1,1}, \ldots, \widetilde{\mathbf{y}}_{n,1}),\ \mathsf{miSK} \leftarrow \mathsf{miKeyGen}(\mathsf{miMSK}, [\widetilde{\mathbf{y}}]_2),\ \mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}_i, [\widetilde{\mathbf{y}}_{i,2}]_1)$
$\mathsf{gSK} := (\mathsf{miSK}, \{\mathsf{iSK}_i\}_{i\in[n]})$.
Output: $\mathsf{gSK}$
```

Fig 2. Function-hiding security game for gFE.

Proof. We prove Theorem 4.1 via a series of hybrid games $\mathsf{H}_{1,\iota,1}, \ldots, \mathsf{H}_{1,\iota,5}, \mathsf{H}_2$ for $\iota \in [q_{\mathsf{CT}}]$. We show that $\mathsf{G}_0 \approx_c \mathsf{H}_{1,1,1} \approx_c \cdots \approx_c \mathsf{H}_{1,1,5} \approx_c \mathsf{H}_{1,2,1} \approx_c \cdots \approx_c \mathsf{H}_{1,q_{\mathsf{CT}},5} \approx_c \mathsf{H}_2 \approx_c \mathsf{G}_1$, where G_β for $\beta \in \{0,1\}$ is the original security game (described in Fig 2). Each hybrid is defined as follows.

$\mathsf{H}_{1,\iota,1}$**:** This game is the same as G_0 except that

- for $(i,j) \in [n] \times [q_{\mathsf{CT}}]$, $\widetilde{\mathbf{x}}^j_{i,1}, \widetilde{\mathbf{x}}^j_{i,2}$ to be encrypted are set as

$$\widetilde{\mathbf{x}}^j_{i,1} := \begin{cases} (\mathbf{x}^{j,0}_{i,1}, \boxed{\mathbf{x}^{j,0}_{i,2}}, \mathbf{z}^j_i, 0) \\ (\mathbf{x}^{j,0}_{i,1}, 0^{m_2}, \boxed{0^k, 1}) \\ (\mathbf{x}^{j,0}_{i,1}, 0^{m_2}, \mathbf{z}^j_i, 0) \end{cases} \quad \widetilde{\mathbf{x}}^j_{i,2} := \begin{cases} (\boxed{0^{m_2}}, -\mathbf{z}^j_i, 0) & \text{if } j < \iota \\ (\boxed{0^{m_2}, 0^k, 1}) & \text{if } j = \iota \\ (\mathbf{x}^{j,0}_{i,2}, -\mathbf{z}^j_i, 0) & \text{if } j > \iota \end{cases} \tag{4.1}$$

- $\mathcal{O}_{\mathsf{SK}}$ sets $\widetilde{\mathbf{y}}_{i,1} := (\mathbf{y}^0_{i,1}, \boxed{\mathbf{y}^0_{i,2}}, \mathbf{a}, \boxed{\langle \mathbf{z}^\iota_i, \mathbf{a}\rangle})$, $\widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}^0_{i,2}, \mathbf{a}, \boxed{-\langle \mathbf{z}^\iota_i, \mathbf{a}\rangle + \langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^0_{i,2}\rangle})$ for all queries.

$\mathsf{H}_{1,\iota,2}$**:** This game is the same as $\mathsf{H}_{1,\iota,1}$ except that $\mathcal{O}_{\mathsf{SK}}$ samples $t_i \leftarrow \mathbb{Z}_p$ and sets $\widetilde{\mathbf{y}}_{i,1} := (\mathbf{y}^0_{i,1}, \mathbf{y}^0_{i,2}, \mathbf{a}, \boxed{t_i})$, $\widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}^0_{i,2}, \mathbf{a}, \boxed{-t_i} + \langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^0_{i,2}\rangle)$ for each query.

$\mathsf{H}_{1,\iota,3}$**:** This game is the same as $\mathsf{H}_{1,\iota,2}$ except that $\mathcal{O}_{\mathsf{SK}}$ sets $\widetilde{\mathbf{y}}_{i,1} := (\mathbf{y}^0_{i,1}, \mathbf{y}^0_{i,2}, \mathbf{a}, t_i \boxed{+\langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^0_{i,2}\rangle})$, $\widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}^0_{i,2}, \mathbf{a}, -t_i + \cancel{\langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^0_{i,2}\rangle})$ for each query.

$\mathsf{H}_{1,\iota,4}$**:** This game is the same as $\mathsf{H}_{1,\iota,3}$ except that $\mathcal{O}_{\mathsf{SK}}$ sets $\widetilde{\mathbf{y}}_{i,1} := (\mathbf{y}^0_{i,1}, \mathbf{y}^0_{i,2}, \mathbf{a}, \boxed{\langle \mathbf{z}^\iota_i, \mathbf{a}\rangle} + \langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^0_{i,2}\rangle)$, $\widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}^0_{i,2}, \mathbf{a}, \boxed{-\langle \mathbf{z}^\iota_i, \mathbf{a}\rangle})$ for all queries.

$\mathsf{H}_{1,\iota,5}$**:** This game is the same as $\mathsf{H}_{1,\iota,4}$ except that

- $\widetilde{\mathbf{x}}^\iota_{i,1} := (\mathbf{x}^{\iota,0}_{i,1}, \boxed{\mathbf{x}^{\iota,0}_{i,2}, \mathbf{z}^\iota_i, 0})$, $\widetilde{\mathbf{x}}^\iota_{i,2} := (0^{m_2}, \boxed{-\mathbf{z}^\iota_i, 0})$ for all $i \in [n]$;
- $\mathcal{O}_{\mathsf{SK}}$ sets $\widetilde{\mathbf{y}}_{i,1} := (\mathbf{y}^0_{i,1}, \mathbf{y}^0_{i,2}, \mathbf{a}, \boxed{0})$, $\widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}^0_{i,2}, \mathbf{a}, \boxed{0})$ for all queries.

H_2**:** This game is the same as $\mathsf{H}_{1,q_{\mathsf{CT}},5}$ except that

- $\widetilde{\mathbf{x}}^j_{i,1} := (\boxed{\mathbf{x}^{j,1}_{i,1}, \mathbf{x}^{j,1}_{i,2}}, \mathbf{z}^j_i, 0)$, $\widetilde{\mathbf{x}}^j_{i,2} := (0^{m_2}, -\mathbf{z}^j_i, 0)$ for all $(i,j) \in [n] \times [q_{\mathsf{CT}}]$;
- $\mathcal{O}_{\mathsf{SK}}$ sets $\widetilde{\mathbf{y}}_{i,1} := (\boxed{\mathbf{y}^1_{i,1}, \mathbf{y}^1_{i,2}}, \mathbf{a}, 0)$, $\widetilde{\mathbf{y}}_{i,2} := (\boxed{\mathbf{y}^1_{i,2}}, \mathbf{a}, 0)$ for all queries.

Thanks to Lemmata 4.1 to 4.7, Theorem 4.1 holds. □

Next, we prove the indistinguishability of each pair of hybrid games. Let $P(\mathcal{A}, \mathsf{G})$ be the probability that $\mathcal{A}$ outputs 1 in G with the security parameter being λ, i.e., $\mathsf{P}(\mathcal{A}, \mathsf{G}_\beta) = \mathsf{P}^{\mathsf{gFE},\beta}_{\mathcal{A},\mathsf{fh}}(\lambda)$.

Lemma 4.1. *Let* $\mathsf{H}_{1,0,5} = \mathsf{G}_0$*. For all PPT adversaries* $\mathcal{A}$ *and* $\iota \in [q_{\mathsf{CT}}]$*, there exist PPT adversary* $\mathcal{B}_1, \mathcal{B}_2$ *such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota-1,5}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,1})| \leq \mathsf{Adv}^{\mathsf{miFE}}_{\mathcal{B}_1,\mathsf{fh}}(\lambda) + n\mathsf{Adv}^{\mathsf{iFE}}_{\mathcal{B}_2,\mathsf{fh}}(\lambda)$*.*

Proof. Recall that the differences between $\mathsf{H}_{1,\iota-1,5}$ and $\mathsf{H}_{1,\iota,1}$ are

- $\widetilde{\mathbf{x}}^{\iota}_{i,1} := (\mathbf{x}^{\iota,0}_{i,1}, 0^{m_2}, \mathbf{z}^{\iota}_i, 0) \longrightarrow \widetilde{\mathbf{x}}^{\iota}_{i,1} := (\mathbf{x}^{\iota,0}_{i,1}, 0^{m_2}, 0^k, 1)$;
- $\widetilde{\mathbf{x}}^{\iota}_{i,2} := (\mathbf{x}^{\iota,0}_{i,2}, -\mathbf{z}^{\iota}_i, 0) \longrightarrow \widetilde{\mathbf{x}}^{\iota}_{i,2} := (0^{m_2}, 0^k, 1)$;
- $\widetilde{\mathbf{y}}_{i,1} := \begin{cases} (\mathbf{y}^0_{i,1}, 0^{m_2}, \mathbf{a}, 0) & \text{if } \iota = 1 \\ (\mathbf{y}^0_{i,1}, \mathbf{y}^0_{i,2}, \mathbf{a}, 0) & \text{if } \iota > 1 \end{cases} \longrightarrow \widetilde{\mathbf{y}}_{i,1} := (\mathbf{y}^0_{i,1}, \mathbf{y}^0_{i,2}, \mathbf{a}, \langle \mathbf{z}^{\iota}_i, \mathbf{a} \rangle)$;
- $\widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}^0_{i,2}, \mathbf{a}, 0) \longrightarrow \widetilde{\mathbf{y}}_{i,2} := (\mathbf{y}^0_{i,2}, \mathbf{a}, -\langle \mathbf{z}^{\iota}_i, \mathbf{a} \rangle + \langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^0_{i,2} \rangle)$.

For all $i \in [n], j \in [q_{\mathsf{CT}}], \ell \in [q_{\mathsf{SK}}]$, let $\widetilde{\mathbf{x}}^{j,0}_{i,1}$ and $\widetilde{\mathbf{y}}^{\ell,0}_{i,1}$ be $\widetilde{\mathbf{x}}^{j}_{i,1}$ and $\widetilde{\mathbf{y}}^{\ell}_{i,1}$ defined in $\mathsf{H}_{1,\iota-1,5}$, respectively. Let $\widetilde{\mathbf{x}}^{j,1}_{i,1}$ and $\widetilde{\mathbf{y}}^{\ell,1}_{i,1}$ be $\widetilde{\mathbf{x}}^{j}_{i,1}$ and $\widetilde{\mathbf{y}}^{\ell}_{i,1}$ defined in $\mathsf{H}_{1,\iota,1}$, respectively. Then, it is not hard to see that we have $\langle \widetilde{\mathbf{x}}^{j,0}_{i,1}, \widetilde{\mathbf{y}}^{\ell,0}_{i,1} \rangle = \langle \widetilde{\mathbf{x}}^{j,1}_{i,1}, \widetilde{\mathbf{y}}^{\ell,1}_{i,1} \rangle$. Hence, for all $(j_1, \ldots, j_n) \in [q_{\mathsf{CT}}]^n, \ell \in [q_{\mathsf{SK}}]$, we have $\sum_{i \in [n]} \langle \widetilde{\mathbf{x}}^{j,0}_{i,1}, \widetilde{\mathbf{y}}^{\ell,0}_{i,1} \rangle = \sum_{i \in [n]} \langle \widetilde{\mathbf{x}}^{j,1}_{i,1}, \widetilde{\mathbf{y}}^{\ell,1}_{i,1} \rangle$ and can reduce the indistinguishability between $\widetilde{\mathbf{x}}^{j}_{i,1}$ and $\widetilde{\mathbf{y}}^{\ell}_{i,1}$ in $\mathsf{H}_{1,\iota-1,5}$ and those in $\mathsf{H}_{1,\iota,1}$ to the function-hiding property of miFE.

Similarly, for all $i \in [n], j \in [q_{\mathsf{CT}}], \ell \in [q_{\mathsf{SK}}]$, let $\widetilde{\mathbf{x}}^{j,0}_{i,2}$ and $\widetilde{\mathbf{y}}^{\ell,0}_{i,2}$ be $\widetilde{\mathbf{x}}^{j}_{i,2}$ and $\widetilde{\mathbf{y}}^{\ell}_{i,2}$ defined in $\mathsf{H}_{1,\iota-1,5}$, respectively. Let $\widetilde{\mathbf{x}}^{j,1}_{i,2}$ and $\widetilde{\mathbf{y}}^{\ell,1}_{i,2}$ be $\widetilde{\mathbf{x}}^{j}_{i,2}$ and $\widetilde{\mathbf{y}}^{\ell}_{i,2}$ defined in $\mathsf{H}_{1,\iota,1}$, respectively. Then, we have $\langle \widetilde{\mathbf{x}}^{j,0}_{i,2}, \widetilde{\mathbf{y}}^{\ell,0}_{i,2} \rangle = \langle \widetilde{\mathbf{x}}^{j,1}_{i,2}, \widetilde{\mathbf{y}}^{\ell,1}_{i,2} \rangle$. Thus, we can reduce the indistinguishability between $\widetilde{\mathbf{x}}^{j}_{i,2}$ and $\widetilde{\mathbf{y}}^{\ell}_{i,2}$ in $\mathsf{H}_{1,\iota-1,5}$ and those in $\mathsf{H}_{1,\iota,1}$ to the function-hiding property of iFE. Note that the function-hiding property of iFE in the multi-instance setting is easily reduced to that in the single-instance setting via hybrid argument. This concludes the proof. □

Lemma 4.2. *For all PPT adversaries* $\mathcal{A}$ *and* $\iota \in [q_{\mathsf{CT}}]$*, there exists a PPT adversary* $\mathcal{B}$ *against* n*-fold bilateral* $\mathcal{U}_{q_{\mathsf{SK}},k}$*-MDDH such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,1}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,2})| \leq \mathsf{Adv}^{n\text{-}\mathsf{bi}\text{-}\mathcal{U}_{q_{\mathsf{SK}},k}\text{-}\mathsf{MDDH}}_{\mathcal{B}}(\lambda)$*.*

Proof. We describe the reduction $\mathcal{B}$.

1. $\mathcal{B}$ obtains an n-fold bilateral $\mathcal{U}_{q_{\mathsf{SK}},k}$-MDDH instance $(\mathbb{G}, [\mathbf{A}]_1, [\mathbf{K}_\beta]_1, [\mathbf{A}]_2, [\mathbf{K}_\beta]_2)$, where $\mathbf{A} \in \mathbb{Z}_p^{q_{\mathsf{SK}} \times k}$, $\mathbf{Z} \leftarrow \mathbb{Z}_p^{k \times n}$, $\mathbf{K}_0 = \mathbf{AZ}$, $\mathbf{K}_1 \leftarrow \mathbb{Z}_p^{q_{\mathsf{SK}} \times n}$.
2. When $\mathcal{A}$ outputs $\{i, ([\mathbf{x}^{j,0}_{i,1}]_1, [\mathbf{x}^{j,0}_{i,2}]_2), ([\mathbf{x}^{j,1}_{i,1}]_1, [\mathbf{x}^{j,1}_{i,2}]_2)\}_{i \in [n], j \in [q_{\mathsf{CT}}]}$, $\mathcal{B}$ computes $\mathsf{gPP}, \mathsf{gMSK}$ as in Fig 2 and gives $\mathsf{gPP}, \{\mathsf{miCT}^j_i, \mathsf{iCT}^j_i\}_{i \in [n], j \in [q_{\mathsf{CT}}]}$ to $\mathcal{A}$, where $\mathsf{miCT}^j_i \leftarrow \mathsf{miEnc}(\mathsf{miMSK}, i, [\widetilde{\mathbf{x}}^j_{i,1}]_1)$, $\mathsf{iCT}^j_i \leftarrow \mathsf{iEnc}(\mathsf{iMSK}_i, [\widetilde{\mathbf{x}}^j_{i,2}]_2)$ with $\widetilde{\mathbf{x}}^j_{i,1}, \widetilde{\mathbf{x}}^j_{i,2}$ being set as in Eq. (4.1).
3. For the ℓ-th query to $\mathcal{O}_{\mathsf{SK}}$ on $\{([\mathbf{y}^{\ell,0}_{i,1}]_2, [\mathbf{y}^{\ell,0}_{i,2}]_1), ([\mathbf{y}^{\ell,1}_{i,1}]_2, [\mathbf{y}^{\ell,1}_{i,2}]_1)\}_{i \in [n]}$, $\mathcal{B}$ replies $\mathsf{gSK} := (\mathsf{miSK}, \{\mathsf{iSK}_i\}_{i \in [n]})$ as follows:
$$\begin{aligned} &\widetilde{\mathbf{y}}^{\ell}_{i,1} := (\mathbf{y}^{\ell,0}_{i,1}, \mathbf{y}^{\ell,0}_{i,2}, \mathbf{a}^{\ell}, k_{\beta,\ell,i}),\ \widetilde{\mathbf{y}}^{\ell}_{i,2} := (\mathbf{y}^{0}_{i,2}, \mathbf{a}^{\ell}, -k_{\beta,\ell,i} + \langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^{\ell,0}_{i,2} \rangle) \\ &\widetilde{\mathbf{y}}^{\ell} := (\widetilde{\mathbf{y}}^{\ell}_{1,1}, \ldots, \widetilde{\mathbf{y}}^{\ell}_{n,1}),\ \mathsf{miSK} \leftarrow \mathsf{miKeyGen}(\mathsf{miMSK}, [\widetilde{\mathbf{y}}^{\ell}]_2) \\ &\mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}_i, [\widetilde{\mathbf{y}}^{\ell}_{i,2}]_1) \end{aligned}$$
where $\mathbf{a}^{\ell}$ is the ℓ-th row of $\mathbf{A}$ and $k_{\beta,\ell,i}$ is the (ℓ, i)-th entry of $\mathbf{K}_\beta$.
4. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

It is not hard to see that $\mathcal{A}$'s view corresponds to $\mathsf{H}_{1,\iota,1}$ if $\beta = 0$ and $\mathsf{H}_{1,\iota,2}$ otherwise. Note that n-fold bilateral $\mathcal{U}_{q_{\mathsf{SK}},k}$-MDDH reduced to bilateral $\mathcal{D}_k$-MDDH with the security loss of n. □

Lemma 4.3. *For all PPT adversaries* $\mathcal{A}$ *and* $\iota \in [q_{\mathsf{CT}}]$*, we have* $\mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,2}) = \mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,3})$*.*

Proof. We implicitly define $t_{i,\ell} := t'_{i,\ell} + \langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^{\ell,0}_{i,2} \rangle$ where $t'_{i,\ell} \leftarrow \mathbb{Z}_p$ for all $i \in [n], \ell \in [q_{\mathsf{SK}}]$. This does not change the distribution of $t_{i,\ell}$. Then, it is easy to see that $\mathcal{O}_{\mathsf{SK}}$ sets $\widetilde{\mathbf{y}}^{\ell}_{i,1} := (\mathbf{y}^{\ell,0}_{i,1}, \mathbf{y}^{\ell,0}_{i,2}, \mathbf{a}, t'_{i,\ell} + \langle \mathbf{x}^{\iota,0}_{i,2}, \mathbf{y}^{\ell,0}_{i,2} \rangle)$, $\widetilde{\mathbf{y}}^{\ell}_{i,2} := (\mathbf{y}^{\ell,0}_{i,2}, \mathbf{a}^{\ell}, -t'_{i,\ell})$ in $\mathsf{H}_{1,\iota,2}$, which are identically distributed to $\widetilde{\mathbf{y}}^{\ell}_{i,1}, \widetilde{\mathbf{y}}^{\ell}_{i,2}$ in $\mathsf{H}_{1,\iota,3}$. Thus, $\mathcal{A}$'s views in both hybrids are identical. □

Lemma 4.4. *For all PPT adversaries $\mathcal{A}$ and $\iota \in [q_{\mathsf{CT}}]$, there exists a PPT adversary $\mathcal{B}$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,3}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,4})| \leq n\mathsf{Adv}_{\mathcal{B}}^{\mathsf{bi}\text{-}\mathcal{U}_{q_{\mathsf{SK}},k}\text{-}\mathsf{MDDH}}(\lambda)$.

We omit the proof since Lemma 4.4 can be proven similarly to Lemma 4.2.

Lemma 4.5. *For all PPT adversaries $\mathcal{A}$ and $\iota \in [q_{\mathsf{CT}}]$, there exist PPT adversary $\mathcal{B}_1, \mathcal{B}_2$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,4}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_{1,\iota,5})| \leq \mathsf{Adv}_{\mathcal{B}_1,\mathsf{fh}}^{\mathsf{miFE}}(\lambda) + n\mathsf{Adv}_{\mathcal{B}_2,\mathsf{fh}}^{\mathsf{iFE}}(\lambda)$.

We omit the proof since Lemma 4.5 can be proven similarly to Lemma 4.1.

Lemma 4.6. *For all PPT adversaries $\mathcal{A}$, there exist PPT adversary $\mathcal{B}_1, \mathcal{B}_2$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{1,q_{\mathsf{SK}},5}) - \mathsf{P}(\mathcal{A}, \mathsf{H}_2)| \leq \mathsf{Adv}_{\mathcal{B}_1,\mathsf{fh}}^{\mathsf{miFE}}(\lambda) + n\mathsf{Adv}_{\mathcal{B}_2,\mathsf{fh}}^{\mathsf{iFE}}(\lambda)$.

Proof. For all $i \in [n], j \in [q_{\mathsf{CT}}], \ell \in [q_{\mathsf{SK}}]$, let $\widetilde{\mathbf{x}}_{i,1}^{j,0}$ and $\widetilde{\mathbf{y}}_{i,1}^{\ell,0}$ be $\widetilde{\mathbf{x}}_{i,1}^{j}$ and $\widetilde{\mathbf{y}}_{i,1}^{\ell}$ defined in $\mathsf{H}_{1,q_{\mathsf{SK}},5}$, respectively. Let $\widetilde{\mathbf{x}}_{i,1}^{j,1}$ and $\widetilde{\mathbf{y}}_{i,1}^{\ell,1}$ be $\widetilde{\mathbf{x}}_{i,1}^{j}$ and $\widetilde{\mathbf{y}}_{i,1}^{\ell}$ defined in H_2, respectively. Due to the admissibility of $\mathcal{A}$ against gFE, its queries satisfy that $\sum_{i\in[n]}(\langle \mathbf{x}_{i,1}^{j,0}, \mathbf{y}_{i,1}^{\ell,0}\rangle + \langle \mathbf{x}_{i,2}^{j,0}, \mathbf{y}_{i,2}^{\ell,0}\rangle) = \sum_{i\in[n]}(\langle \mathbf{x}_{i,1}^{j,1}, \mathbf{y}_{i,1}^{\ell,1}\rangle + \langle \mathbf{x}_{i,2}^{j,1}, \mathbf{y}_{i,2}^{\ell,1}\rangle)$ for all $(j_1, \ldots, j_n) \in [q_{\mathsf{CT}}]^n, \ell \in [q_{\mathsf{SK}}]$. Thus, we have $\sum_{i\in[n]}\langle \widetilde{\mathbf{x}}_{i,1}^{j,0}, \widetilde{\mathbf{y}}_{i,1}^{\ell,0}\rangle = \sum_{i\in[n]}\langle \widetilde{\mathbf{x}}_{i,1}^{j,1}, \widetilde{\mathbf{y}}_{i,1}^{\ell,1}\rangle$ and can reduce the indistinguishability between $\widetilde{\mathbf{x}}_{i,1}^{j}$ and $\widetilde{\mathbf{y}}_{i,1}^{\ell}$ in $\mathsf{H}_{1,q_{\mathsf{SK}},5}$ and those in H_2 to the function-hiding property of miFE.

Similarly, for all $i \in [n], j \in [q_{\mathsf{CT}}], \ell \in [q_{\mathsf{SK}}]$, let $\widetilde{\mathbf{x}}_{i,2}^{j,0}$ and $\widetilde{\mathbf{y}}_{i,2}^{\ell,0}$ be $\widetilde{\mathbf{x}}_{i,2}^{j}$ and $\widetilde{\mathbf{y}}_{i,2}^{\ell}$ defined in $\mathsf{H}_{1,q_{\mathsf{SK}},5}$, respectively. Let $\widetilde{\mathbf{x}}_{i,2}^{j,1}$ and $\widetilde{\mathbf{y}}_{i,2}^{\ell,1}$ be $\widetilde{\mathbf{x}}_{i,2}^{j}$ and $\widetilde{\mathbf{y}}_{i,2}^{\ell}$ defined in H_2, respectively. Then, we have $\langle \widetilde{\mathbf{x}}_{i,2}^{j,0}, \widetilde{\mathbf{y}}_{i,2}^{\ell,0}\rangle = \langle \widetilde{\mathbf{x}}_{i,2}^{j,1}, \widetilde{\mathbf{y}}_{i,2}^{\ell,1}\rangle$. Thus, we can reduce the indistinguishability between $\widetilde{\mathbf{x}}_{i,2}^{j}$ and $\widetilde{\mathbf{y}}_{i,2}^{\ell}$ in $\mathsf{H}_{1,q_{\mathsf{SK}},5}$ and those in H_2 to the function-hiding property of iFE. This concludes the proof. □

Lemma 4.7. *For all $\mathcal{A}$, there exist $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_2) - \mathsf{P}(\mathcal{A}, \mathsf{G}_1)| \leq 2q_{\mathsf{CT}}(\mathsf{Adv}_{\mathcal{B}_1,\mathsf{fh}}^{\mathsf{miFE}}(\lambda) + n\mathsf{Adv}_{\mathcal{B}_2,\mathsf{fh}}^{\mathsf{iFE}}(\lambda) + n\mathsf{Adv}_{\mathcal{B}_3}^{\mathsf{bi}\text{-}\mathcal{U}_{q_{\mathsf{SK}},k}\text{-}\mathsf{MDDH}}(\lambda))$.

We omit the proof since Lemma 4.7 is proven similarly to Lemmata 4.1 to 4.5.

5 Warm-up: Toy MQFE Scheme

Since our MQFE scheme, presented in Sec. 6, is highly complicated, and its security analysis is quite hard to follow, we first present a toy scheme, which will help to understand the idea of our full MQFE scheme. The toy scheme is a MIFE scheme for $\mathcal{F}_{1,2,X,C}^{\mathsf{MQF}}$ from the SXDH assumption, that is, it has two slots and one element per slot. The SXDH assumption is captured as the $\mathcal{D}_k$ assumption where $\mathcal{D}_k$ consists of all matrices with the form of $(a, 1)^\top \in \mathbb{Z}_p^2$. Note that the toy scheme is obtained by not only just setting the full scheme as $m = 1, n = 2$, but also given simplification that is applicable only when $m = 1$ and the number of ciphertext queries is 2 per slot. Concretely, we omit the elements that corresponds to $\widetilde{\mathbf{U}}_i$ and $\widetilde{\mathbf{v}}_i$ in the full scheme and some free spaces for security proof.

Let $\mathsf{pFE} = (\mathsf{pSetup}, \mathsf{pEnc}, \mathsf{pKeyGen}, \mathsf{pDec})$ be an FE scheme for $\mathcal{F}_{4,8,\mathbb{G}}^{\mathsf{PIP}}$ (Def. 3.2), $\mathsf{iFE} = (\mathsf{iSetup}, \mathsf{iEnc}, \mathsf{iKeyGen}, \mathsf{iDec})$ be an FE scheme for $\mathcal{F}_{2,\mathbb{G}}^{\mathsf{IP}}$ (Def.3.1), and $\mathsf{gFE} = (\mathsf{gSetup}, \mathsf{gEnc}, \mathsf{gKeyGen}, \mathsf{gDec})$ be an FE scheme for $\mathcal{F}_{4,1,2,\mathbb{G}}^{\mathsf{MGIP}}$ (Def. 4.2). The toy scheme $\mathsf{qFE} = (\mathsf{qSetup}, \mathsf{qEnc}, \mathsf{qKeyGen}, \mathsf{qDec})$ is constructed from pFE, iFE, and gFE. Precisely, since gFE cannot be instantiated from SXDH, the toy scheme needs an additional assumption such as XDLIN (bilateral 2-Lin). $\mathbb{G}$ is fixed by qSetup.

5.1 Construction

$\mathsf{qSetup}(1^\lambda)$**:** It outputs $\mathsf{qPP}, \mathsf{qMSK}$ as follows:

$$\begin{aligned}
&\mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda),\ w_{1,1}, w_{1,2}, w_{2,1}, w_{2,2}, u_1, u_2, v_1, v_2 \leftarrow \mathbb{Z}_p \\
&\mathsf{pPP}, \mathsf{pMSK} \leftarrow \mathsf{pSetup}(1^\lambda),\ \mathsf{iPP}, \mathsf{iMSK} \leftarrow \mathsf{iSetup}(1^\lambda),\ \mathsf{gPP}, \mathsf{gMSK} \leftarrow \mathsf{gSetup}(1^\lambda) \\
&\mathsf{qPP} := (\mathbb{G}, \mathsf{pPP}, \mathsf{iPP}, \mathsf{gPP}) \\
&\mathsf{qMSK} := (\{w_{i,j}\}_{i,j\in[2]}, \{u_i, v_i\}_{i\in[2]}, \mathsf{pMSK}, \mathsf{iMSK}, \mathsf{gMSK}).
\end{aligned}$$

$\mathsf{qEnc}(\mathsf{qMSK}, i, x_i)$**:** First, it samples vectors as follows:

$$\begin{aligned}
&s, \widetilde{s}, r, t, L \leftarrow \mathbb{Z}_p \\
&\mathbf{l} := \mathbf{e}_{i/2} \otimes (1, L) \in \mathbb{Z}_p^4,\ \widetilde{\mathbf{l}} := \mathbf{e}_{i/2} \otimes (L, -1) \in \mathbb{Z}_p^4 \\
&\mathbf{b} := (x_i, 0,\ sw_{1,i}, sw_{2,i},\ u_i,\ t,\ 0, 0) \in \mathbb{Z}_p^8 \\
&\widetilde{\mathbf{b}} := (x_i, 0,\ \ \ \ \widetilde{s}\mathbf{e}_{i/2},\ \ \ \ r,\ v_i, 0, 0) \in \mathbb{Z}_p^8 \\
&\mathbf{d} := (s, 0) \in \mathbb{Z}_p^2,\ \widetilde{\mathbf{d}} := (\widetilde{s}, 0) \in \mathbb{Z}_p^2 \\
&\mathbf{f} := (r, t, 0, 0) \in \mathbb{Z}_p^4,\ h := 0
\end{aligned}$$

Then, it outputs qCT_i as follows:

$$\begin{aligned}
&\mathsf{pCT}_i \leftarrow \mathsf{pEnc}(\mathsf{pMSK}, (\mathbf{l}, [\mathbf{b}]_1)),\ \mathsf{pSK}_i \leftarrow \mathsf{pKeyGen}(\mathsf{pMSK}, (\widetilde{\mathbf{l}}, [\widetilde{\mathbf{b}}]_2)) \\
&\mathsf{iCT}_i \leftarrow \mathsf{iEnc}(\mathsf{iMSK}, [\mathbf{d}]_1),\ \mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}, [\widetilde{\mathbf{d}}]_2) \\
&\mathsf{gCT}_i \leftarrow \mathsf{gEnc}(\mathsf{gMSK}, i, ([\mathbf{f}]_1, [h]_2)) \\
&\mathsf{qCT}_i := (\mathsf{pCT}_i, \mathsf{pSK}_i, \mathsf{iCT}_i, \mathsf{iSK}_i, \mathsf{gCT}_i)
\end{aligned}$$

$\mathsf{qKeyGen}(\mathsf{qMSK}, \mathbf{c} = \{c_{\mu,\nu}\}_{\mu,\nu \in [2]})$**:** It outputs qSK as follows:

$$\begin{aligned}
&\widetilde{\mathbf{f}}_i := \left(\sum_{\mu \in [2]} c_{i,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,i} v_\mu, 0, 0 \right) \in \mathbb{Z}_p^4 \\
&\widetilde{h}_i := 0 \\
&\mathsf{gSK} \leftarrow \mathsf{gKeyGen}(\mathsf{gMSK}, \{[\widetilde{\mathbf{f}}_i]_2, [\widetilde{h}_i]_1\}_{i \in [2]}) \\
&\sigma_{i,\theta} := c_{i,\theta} w_{i,\theta} \\
&\mathsf{qSK} := (\mathbf{c}, \mathsf{gSK}, \{\sigma_{i,\theta}\}_{i,\theta \in [2]}).
\end{aligned}$$

$\mathsf{qDec}(\mathsf{qCT}_1, \mathsf{qCT}_2, \mathsf{qSK})$**:** It computes

$$\begin{aligned}
&[z_1]_T := \prod_{\mu,\nu \in [2]} \mathsf{pDec}(\mathsf{pCT}_\nu, \mathsf{pSK}_\mu)^{c_{\mu,\nu}} \\
&[z_2]_T := \prod_{i,\theta \in [2]} \mathsf{iDec}(\mathsf{iCT}_\theta, \mathsf{iSK}_i)^{\sigma_{i,\theta}} \\
&[z_3]_T := \mathsf{gDec}(\mathsf{gCT}_1, \mathsf{gCT}_2, \mathsf{gSK}) \\
&[z]_T := [z_1 - z_2 - z_3]_T.
\end{aligned}$$

Then, it searches for z within the range of $z \leq |4CX^2|$.

Correctness. Let $s_i, \widetilde{s}_i, r_i, t_i, \mathbf{l}_i, \widetilde{\mathbf{l}}_i, \mathbf{b}_i, \widetilde{\mathbf{b}}_i$ for $i \in [2]$ be random elements used to generate qCT_i. Observe that $\langle \mathbf{l}_i, \widetilde{\mathbf{l}}_I \rangle = 0$ for all $i, I \in [2]$, and thus $\mathsf{pDec}(\mathsf{pCT}_i, \mathsf{pSK}_I) = \langle \mathbf{b}_i, \widetilde{\mathbf{b}}_I \rangle$. Due to the correctness of $\mathsf{pFE}, \mathsf{iFE}, \mathsf{gEF}$, we have

$$\begin{aligned}
z_1 &= \sum_{\mu,\nu \in [2]} c_{\mu,\nu} (x_\mu x_\nu + s_\nu \widetilde{s}_\mu w_{\mu,\nu} + r_\mu u_\nu + t_\nu v_\mu) \\
z_2 &= \sum_{\mu,\nu \in [2]} c_{\mu,\nu} s_\nu \widetilde{s}_\mu w_{\mu,\nu} \\
z_3 &= \sum_{\mu,\nu \in [2]} c_{\mu,\nu} (r_\mu u_\nu + t_\nu v_\mu).
\end{aligned}$$

Hence, we have $z = \sum_{\mu,\nu \in [2]} c_{\mu,\nu} x_\mu x_\nu$.

```
$\underline{\mathsf{G}_\beta}$
$\{i, \mathbf{x}_i^{j,0}, \mathbf{x}_i^{j,1}\}_{i\in[2],j\in[2]} \leftarrow \mathcal{A}(1^\lambda)$
$\mathsf{qPP}, \mathsf{qMSK} \leftarrow \mathsf{qSetup}(1^\lambda)\ \ \mathsf{qCT}_i^j \leftarrow \mathsf{qEnc}(\mathsf{qMSK}, i, \mathbf{x}_i^{j,\beta})$
$\mathbf{c} \leftarrow \mathcal{A}(\mathsf{qPP}, \{\mathsf{qCT}_i^j\}_{i\in[2],j\in[2]})$
$\mathsf{qSK} \leftarrow \mathsf{qKeyGen}(\mathsf{qMSK}, \mathbf{c})$
$\beta' \leftarrow \mathcal{A}(\mathsf{qSK})$
```

Fig 3. Toy security game for qFE.

5.2 Multi-input IPFE Scheme for Security Analysis

Before going to the security analysis of our MQFE scheme, we introduce a message-hiding MIPFE scheme (the MIFE scheme for $\mathcal{F}^{\mathsf{MIP}}_{m,n,\mathbb{G}}$, denoted by $\mathsf{miFE} = (\mathsf{miSetup}, \mathsf{miEnc}, \mathsf{miKeyGen}, \mathsf{miDec})$) that we use for the security proof. The scheme is obtained by applying the conversion by Abdalla *et al.* [4, Sec. 4.1], which converts a single-input IPFE scheme into a multi-input one, to the single-input IPFE scheme by Abdalla *et al.* [3, Sec. 5]. The resulting scheme satisfies the message-hiding security under the DDH assumption. Note that although Abdalla *et al.* considered the conversion in the adaptive setting, it is not hard to see that the conversion works in the selective setting. The original scheme in [3] uses a pairing-free group for the construction, but it is easy to see that their scheme can be similarly built on pairing groups where the SXDH assumption holds. We use the scheme built on the pairing groups in the security proof of our toy MQFE scheme. The scheme is described as follows.

$\mathsf{miSetup}(1^\lambda)$: It outputs $\mathsf{miPP}, \mathsf{miMSK}$ as follows:

$$\mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda),\ \mathbf{w}_1, \ldots, \mathbf{w}_n \leftarrow \mathbb{Z}_p^m,\ \mathbf{u}_1, \ldots, \mathbf{u}_n \leftarrow \mathbb{Z}_p^m$$
$$\mathsf{miPP} := (\mathbb{G}, [\mathbf{w}_1]_1, \ldots, [\mathbf{w}_n]_1),\ \mathsf{miMSK} := (\mathbf{w}_1, \ldots, \mathbf{w}_n, \mathbf{u}_1, \ldots, \mathbf{u}_n).$$

$\mathsf{miEnc}(\mathsf{miMSK}, i, \mathbf{x}_i)$: It outputs miCT_i as follows:

$$s \leftarrow \mathbb{Z}_p,\ \mathsf{miCT}_i := [\mathbf{c}_i]_1 = ([s]_1, [s\mathbf{w}_i + \mathbf{u}_i + \mathbf{x}_i]_1).$$

$\mathsf{miKeyGen}(\mathsf{miMSK}, \mathbf{y}_1, \ldots, \mathbf{y}_n)$: It outputs miSK as follows:

$$\mathsf{miSK}_0 := -\sum_{i\in[n]} \langle \mathbf{y}_i, \mathbf{u}_i \rangle,\ \mathsf{miSK}_i := (-\mathbf{y}_i^\top \mathbf{w}_i, \mathbf{y}_i),\ \mathsf{miSK} := (\mathsf{miSK}_0, \{\mathsf{miSK}_i\}_{i\in[n]}).$$

$\mathsf{miDec}(\mathsf{miCT}_1, \ldots, \mathsf{miCT}_n, \mathsf{miSK})$: It computes d where $[d]_1 = [\sum_{i\in[n]} \langle \mathbf{c}_i, \mathsf{miSK}_i \rangle + \mathsf{miSK}_0]_1$.

5.3 Security Analysis for Simple Case

In this section, we consider the security analysis for the simple case where an adversary makes two ciphertext queries per slot and one secret key query. The reason for considering two ciphertext queries is that the ways of changing the first and second ciphertexts in hybrid games are different. In the general case, the second and subsequent ciphertexts are changed similarly in the hybrid sequence. Thus, the two-ciphertexts case suffices for understanding the basic strategy for security analysis. In a high-level view, the security proof of our MQFE scheme is similar to that of the MIPFE schemes by Abdalla *et al.* [4] in which the first ciphertexts of each slot are changed from the 0-side to the 1-side by the information-theoretical property of the one-time pad and the rest of ciphertexts is changed by the security of an IPFE scheme (in our case, the IPFE scheme corresponds to the MIPFE scheme in Sec. 5.2). Since the formal security proof for our MQFE scheme is given in Sec. 6, we present a security proof for the simple case in an informal way.

We want to prove $\mathsf{G}_0 \approx_c \mathsf{G}_1$ where G_β is the message-hiding security game (described in Fig 3). In G_β, the vectors in the ciphertexts and the secret key that the adversary obtains are defined as Fig 4. We introduce a series of hybrid games, $\mathsf{H}_1, \ldots, \mathsf{H}_{15}$, and prove $\mathsf{G}_0 \approx_c \mathsf{H}_1 \approx_c \cdots \approx_c \mathsf{H}_{15} \approx_c \mathsf{G}_1$. In each

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b}_1^1 := (x_1^{1,\beta},\ 0,\ s_1^1 w_{1,1},\ s_1^1 w_{2,1},\ u_1,\ t_1^1,\ 0,\ 0)$ $\widetilde{\mathbf{b}}_1^1 := (x_1^{1,\beta},\ 0,\ \widetilde{s}_1^1,\ 0,\ r_1^1,\ v_1,\ 0,\ 0)$ $\mathbf{d}_1^1 := (s_1^1, 0),\ \widetilde{\mathbf{d}}_1^1 := (\widetilde{s}_1^1, 0)$ $\mathbf{f}_1^1 := (r_1^1, t_1^1, 0, 0),\ h_1^1 := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b}_2^1 := (x_2^{1,\beta},\ 0,\ s_2^1 w_{1,2},\ s_2^1 w_{2,2},\ u_2,\ t_2^1,\ 0,\ 0)$ $\widetilde{\mathbf{b}}_2^1 := (x_2^{1,\beta},\ 0,\ 0,\ \widetilde{s}_2^1,\ r_2^1,\ v_2,\ 0,\ 0)$ $\mathbf{d}_2^1 := (s_2^1, 0),\ \widetilde{\mathbf{d}}_2^1 := (\widetilde{s}_2^1, 0)$ $\mathbf{f}_2^1 := (r_2^1, t_2^1, 0, 0),\ h_2^1 := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b}_1^2 := (x_1^{2,\beta},\ 0,\ s_1^2 w_{1,1},\ s_1^2 w_{2,1},\ u_1,\ t_1^2,\ 0,\ 0)$ $\widetilde{\mathbf{b}}_1^2 := (x_1^{2,\beta},\ 0,\ \widetilde{s}_1^2,\ 0,\ r_1^2,\ v_1,\ 0,\ 0)$ $\mathbf{d}_1^2 := (s_1^2, 0),\ \widetilde{\mathbf{d}}_1^2 := (\widetilde{s}_1^2, 0)$ $\mathbf{f}_1^2 := (r_1^2, t_1^2, 0, 0),\ h_1^2 := 0$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b}_2^2 := (x_2^{2,\beta},\ 0,\ s_2^2 w_{1,2},\ s_2^2 w_{2,2},\ u_2,\ t_2^2,\ 0,\ 0)$ $\widetilde{\mathbf{b}}_2^2 := (x_2^{2,\beta},\ 0,\ 0,\ \widetilde{s}_2^2,\ r_2^2,\ v_2,\ 0,\ 0)$ $\mathbf{d}_2^2 := (s_2^2, 0),\ \widetilde{\mathbf{d}}_2^2 := (\widetilde{s}_2^2, 0)$ $\mathbf{f}_2^2 := (r_2^2, t_2^2, 0, 0),\ h_2^2 := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,1}v_\mu, 0, 0)$ $\widetilde{h}_1 := 0$	 $\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,2}v_\mu, 0, 0)$ $\widetilde{h}_2 := 0$

Fig 4. Vectors in G_β.

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b} := (\ x_1^{1,0},\ \boxed{x_1^{1,1}},\ s_1^1 w_{1,1},\ s_1^1 w_{2,1},\ u_1,\ t_1^1,\ 0,\ \boxed{t_1^1 v_1 + x_1^{1,0} x_1^{1,0}}\ )$ $\widetilde{\mathbf{b}} := (\ \boxed{0},\ 0,\ \widetilde{s}_1^1,\ 0,\ r_1^1,\ \boxed{0},\ 0,\ \boxed{1}\ )$ $\mathbf{d} := (s_1^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, \boxed{t_1^1 v_1}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b} := (\ x_2^{1,0},\ \boxed{x_2^{1,1}},\ s_2^1 w_{1,2},\ s_2^1 w_{2,2},\ u_2,\ t_2^1,\ \boxed{t_2^1 v_1},\ \boxed{t_2^1 v_1 + x_1^{1,0} x_2^{1,0}}\ )$ $\widetilde{\mathbf{b}} := (\ x_2^{1,0},\ 0,\ 0,\ \widetilde{s}_2^1,\ r_2^1,\ v_2,\ 0,\ 0\ )$ $\mathbf{d} := (s_2^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, \boxed{t_2^1 v_1}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b} := (\ x_1^{2,0},\ \boxed{x_1^{2,1}},\ s_1^2 w_{1,1},\ s_1^2 w_{2,1},\ u_1,\ t_1^2,\ \boxed{t_1^2 v_1},\ 0\ )$ $\widetilde{\mathbf{b}} := (\ x_1^{2,0},\ 0,\ \widetilde{s}_1^2,\ 0,\ r_1^2,\ \boxed{0},\ \boxed{1},\ 0\ )$ $\mathbf{d} := (s_1^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, \boxed{t_1^2 v_1}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b} := (\ x_2^{2,0},\ \boxed{x_2^{2,1}},\ s_2^2 w_{1,2},\ s_2^2 w_{2,2},\ u_2,\ t_2^2,\ \boxed{t_2^2 v_1},\ \boxed{t_2^2 v_1 + x_1^{1,0} x_2^{2,0}}\ )$ $\widetilde{\mathbf{b}} := (\ x_2^{2,0},\ 0,\ 0,\ \widetilde{s}_2^2,\ r_2^2,\ v_2,\ 0,\ 0\ )$ $\mathbf{d} := (s_2^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, \boxed{t_2^2 v_1}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \boxed{c_{2,1}v_2}, \boxed{c_{1,1}}, \boxed{c_{2,1}})$ $\widetilde{h}_1 := 0$	 $\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \boxed{c_{2,2}v_2}, \boxed{c_{1,2}}, \boxed{c_{2,2}})$ $\widetilde{h}_2 := 0$

Fig 5. Vectors in H_1.

$\underline{\mathsf{qCT}_1^1}$ $\boxed{\ddot{v}_1^1 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\ x_1^{1,0},\ x_1^{1,1},\ s_1^1 w_{1,1},\ s_1^1 w_{2,1},\ u_1,\ t_1^1,\ 0,\ \boxed{\ddot{v}_1^1} + x_1^{1,0} x_1^{1,0}\ )$ $\widetilde{\mathbf{b}} := (\ 0,\ 0,\ \widetilde{s}_1^1,\ 0,\ r_1^1,\ 0,\ 0,\ 1\ )$ $\mathbf{d} := (s_1^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, \boxed{\ddot{v}_1^1}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\boxed{\ddot{v}_2^1 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\ x_2^{1,0},\ x_2^{1,1},\ s_2^1 w_{1,2},\ s_2^1 w_{2,2},\ u_2,\ t_2^1,\ \boxed{\ddot{v}_2^1},\ \boxed{\ddot{v}_2^1} + x_1^{1,0} x_2^{1,0}\ )$ $\widetilde{\mathbf{b}} := (\ x_2^{1,0},\ 0,\ 0,\ \widetilde{s}_2^1,\ r_2^1,\ v_2,\ 0,\ 0\ )$ $\mathbf{d} := (s_2^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, \boxed{\ddot{v}_2^1}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\boxed{\ddot{v}_1^2 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\ x_1^{2,0},\ x_1^{2,1},\ s_1^2 w_{1,1},\ s_1^2 w_{2,1},\ u_1,\ t_1^2,\ \boxed{\ddot{v}_1^2},\ 0\ )$ $\widetilde{\mathbf{b}} := (\ x_1^{2,0},\ 0,\ \widetilde{s}_1^2,\ 0,\ r_1^2,\ 0,\ 1,\ 0\ )$ $\mathbf{d} := (s_1^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, \boxed{\ddot{v}_1^2}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\boxed{\ddot{v}_2^2 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\ x_2^{2,0},\ x_2^{2,1},\ s_2^2 w_{1,2},\ s_2^2 w_{2,2},\ u_2,\ t_2^2,\ \boxed{\ddot{v}_2^2},\ \boxed{\ddot{v}_2^2} + x_1^{1,0} x_2^{2,0}\ )$ $\widetilde{\mathbf{b}} := (\ x_2^{2,0},\ 0,\ 0,\ \widetilde{s}_2^2,\ r_2^2,\ v_2,\ 0,\ 0\ )$ $\mathbf{d} := (s_2^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, \boxed{\ddot{v}_2^2}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, c_{2,1}v_2, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := 0$	 $\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, c_{2,2}v_2, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 6. Vectors in H_2.

hybrid game, the vectors for generating the ciphertexts and the secret keys are changed from G_0, which

$\underline{\mathsf{qCT}_1^1}$ $\ddot{v}_1^1 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, 0,\ \ddot{v}_1^1 + \boxed{x_1^{1,1}x_1^{1,1}}\,)$ $\widetilde{\mathbf{b}} := (\,—, 0,\ 1\,)$ $\mathbf{d} := (s_1^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, \ddot{v}_1^1 + \boxed{x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\ddot{v}_2^1 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{v}_2^1 + \boxed{x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}}, \ddot{v}_2^1 + \boxed{x_1^{1,1}x_2^{1,1}}\,)$ $\widetilde{\mathbf{b}} := (\,—,\ 0,\ 0\,)$ $\mathbf{d} := (s_2^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, \ddot{v}_2^1 + \boxed{x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\ddot{v}_1^2 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{v}_1^2 + \boxed{x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}}, 0\,)$ $\widetilde{\mathbf{b}} := (\,—,\ 1,\ 0\,)$ $\mathbf{d} := (s_1^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, \ddot{v}_1^2 + \boxed{x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\ddot{v}_2^2 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{v}_2^2 + \boxed{x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}}, \ddot{v}_2^2 + \boxed{x_1^{1,1}x_2^{2,1}}\,)$ $\widetilde{\mathbf{b}} := (\,—,\ 0,\ 0\,)$ $\mathbf{d} := (s_2^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, \ddot{v}_2^2 + \boxed{x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu \in [2]} c_{1,\mu}u_\mu, c_{2,1}v_2, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := 0$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu \in [2]} c_{2,\mu}u_\mu, c_{2,2}v_2, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 7. Vectors in H_3.

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b} := (\,—, 0, \boxed{t_1^1 v_1} + x_1^{1,1}x_1^{1,1}\,)$ $\widetilde{\mathbf{b}} := (\,—, 0,\ 1\,)$ $\mathbf{d} := (s_1^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, \boxed{t_1^1 v_1} + x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b} := (\,—, \boxed{t_2^1 v_1} + x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, \boxed{t_2^1 v_1} + x_1^{1,1}x_2^{1,1}\,)$ $\widetilde{\mathbf{b}} := (\,—,\ 0,\ 0\,)$ $\mathbf{d} := (s_2^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, \boxed{t_2^1 v_1} + x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b} := (\,—, \boxed{t_1^2 v_1} + x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0\,)$ $\widetilde{\mathbf{b}} := (\,—,\ 1,\ 0\,)$ $\mathbf{d} := (s_1^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, \boxed{t_1^2 v_1} + x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b} := (\,—, \boxed{t_2^2 v_1} + x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}, \boxed{t_2^2 v_1} + x_1^{1,1}x_2^{2,1}\,)$ $\widetilde{\mathbf{b}} := (\,—,\ 0,\ 0\,)$ $\mathbf{d} := (s_2^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, \boxed{t_2^2 v_1} + x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu \in [2]} c_{1,\mu}u_\mu, c_{2,1}v_2, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := 0$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu \in [2]} c_{2,\mu}u_\mu, c_{2,2}v_2, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 8. Vectors in H_4.

is shown in Fig 5 to 19. We frame the parts that are changed from the previous game by a box and sometimes denote the parts that are not changed by —.

$\underline{\mathsf{G}_0 \approx_c \mathsf{H}_1.}$ We can justify this indistinguishability by the (partially) function-hiding property of pFE and gFE. For all $i, j, I, J \in [2]$, we can see that $\langle \mathbf{b}_i^j, \widetilde{\mathbf{b}}_I^J \rangle$ in G_0 and that in H_1 are equal unless $i = I$ and $j \neq J$. Recall that $\langle \mathbf{l}_i^j, \widetilde{\mathbf{l}}_I^J \rangle \neq 0$ with overwhelming probability if $i = I$ and $j \neq J$, since L is chosen from the exponentially large space, $\mathbb{Z}_p$. Hence, the indistinguishability of $\{\mathbf{b}, \widetilde{\mathbf{b}}\}$ between G_0 and H_1 is implied by the partially function-hiding property of pFE.

Similarly, for all $i, j \in [2]$, $\langle \mathbf{f}_i^j, \widetilde{\mathbf{f}}_i \rangle$ in G_0 and that in H_1 are equal, which implies, for all $j_1, j_2 \in [2]$, $\sum_{i \in [2]} (\langle \mathbf{f}_i^{j_i}, \widetilde{\mathbf{f}}_i \rangle + h_i^{j_i} \widetilde{h}_i)$ in G_0 and that in H_1 are equal. Thus, the indistinguishability of $\{\mathbf{f}, \widetilde{\mathbf{f}}\}$ between G_0 and H_1 is implied by the function-hiding property of gFE.

$\underline{\mathsf{H}_1 \approx_c \mathsf{H}_2.}$ We can justify this indistinguishability by the SXDH assumption, which implies $(\mathbb{G}, [\mathbf{t}]_1, [v_1 \mathbf{t}]_1) \approx_c (\mathbb{G}, [\mathbf{t}]_1, [\ddot{\mathbf{v}}]_1)$ where $\mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda), \mathbf{t} = \{t_i^j\}_{i,j \in [2]}, \ddot{\mathbf{v}} = \{\ddot{v}_i^j\}_{i,j \in [2]} \leftarrow \mathbb{Z}_p^4, v_1 \leftarrow \mathbb{Z}_p$.

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b} := (\, x_1^{1,0},\ x_1^{1,1},\ s_1^1 w_{1,1},\ s_1^1 w_{2,1},\ u_1,\ t_1^1,\ 0,\ \boxed{0}\,)$ $\widetilde{\mathbf{b}} := (\, 0,\ \boxed{x_1^{1,1}},\ \widetilde{s}_1^1,\ 0,\ r_1^1,\ \boxed{v_1},\ 0,\ \boxed{0}\,)$ $\mathbf{d} := (s_1^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, \cancel{t_1^1 v_1} + x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b} := (\, \text{—}, \cancel{t_2^1 v_1} + x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0},\ \boxed{0}\,)$ $\widetilde{\mathbf{b}} := (\, \text{—},\ 0,\ 0\,)$ $\mathbf{d} := (s_2^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, \cancel{t_2^1 v_1} + x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b} := (\, x_1^{2,0},\ x_1^{2,1},\ s_1^2 w_{1,1},\ s_1^2 w_{2,1},\ u_1,\ t_1^2,\ \cancel{t_1^2 v_1} + x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0},\ 0\,)$ $\widetilde{\mathbf{b}} := (\, x_1^{2,0},\ 0,\ \widetilde{s}_1^2,\ 0,\ r_1^2,\ \boxed{v_1},\ 1,\ 0\,)$ $\mathbf{d} := (s_1^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, \cancel{t_1^2 v_1} + x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b} := (\, \text{—}, \cancel{t_2^2 v_1} + x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0},\ \boxed{0}\,)$ $\widetilde{\mathbf{b}} := (\, \text{—},\ 0,\ 0\,)$ $\mathbf{d} := (s_2^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, \cancel{t_2^2 v_1} + x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \boxed{\sum_{\mu\in[2]} c_{\mu,1}v_\mu}, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := 0$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \boxed{\sum_{\mu\in[2]} c_{\mu,2}v_\mu}, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 9. Vectors in H_5.

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b} := (\, x_1^{1,0},\ x_1^{1,1},\ s_1^1 w_{1,1},\ s_1^1 w_{2,1},\ u_1,\ t_1^1,\ 0,\ 0\,)$ $\widetilde{\mathbf{b}} := (\, 0,\ x_1^{1,1},\ \widetilde{s}_1^1,\ 0,\ r_1^1,\ v_1,\ 0,\ 0\,)$ $\mathbf{d} := (s_1^1, \boxed{s_1^1\widetilde{s}_1^2}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b} := (\, \text{—}, \boxed{s_2^1\widetilde{s}_1^2 w_{1,2} + r_1^2 u_2 + x_1^{2,0}x_2^{1,0}} + x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0},\ 0\,)$ $\widetilde{\mathbf{b}} := (\, \text{—},\ 0,\ 0\,)$ $\mathbf{d} := (s_2^1, \boxed{s_2^1\widetilde{s}_1^2}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b} := (\, \text{—}, \boxed{s_1^2\widetilde{s}_1^2 w_{1,1} + r_1^2 u_1 + x_1^{2,0}x_1^{2,0}} + x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0},\ 0\,)$ $\widetilde{\mathbf{b}} := (\, \boxed{0}, 0, \boxed{0}, 0, \boxed{0}, v_1,\ 1,\ 0\,)$ $\mathbf{d} := (s_1^2, \boxed{s_1^2\widetilde{s}_1^2}),\ \widetilde{\mathbf{d}} := (\boxed{0}, \boxed{1})$ $\mathbf{f} := (\boxed{0}, t_1^2, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := \boxed{1}$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b} := (\, \text{—}, \boxed{s_2^2\widetilde{s}_1^2 w_{1,2} + r_1^2 u_2 + x_1^{2,0}x_2^{2,0}} + x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0},\ 0\,)$ $\widetilde{\mathbf{b}} := (\, \text{—},\ 0,\ 0\,)$ $\mathbf{d} := (s_2^2, \boxed{s_2^2\widetilde{s}_1^2}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,1}v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := \boxed{r_1^2 \sum_{\mu\in[2]} c_{1,\mu}u_\mu}$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,2}v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 10. Vectors in H_6.

$\underline{\text{Additional sampling for } \mathsf{qMSK}}$ $\boxed{\ddot{u}_1, \ddot{u}_2 \leftarrow \mathbb{Z}_p}$	
$\underline{\mathsf{qCT}_1^1}$ $\boxed{\ddot{s}_1^1 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\, x_1^{1,0},\ x_1^{1,1},\ s_1^1 w_{1,1},\ s_1^1 w_{2,1},\ u_1,\ t_1^1,\ 0,\ 0\,)$ $\widetilde{\mathbf{b}} := (\, 0,\ x_1^{1,1},\ \widetilde{s}_1^1,\ 0,\ r_1^1,\ v_1,\ 0,\ 0\,)$ $\mathbf{d} := (s_1^1, \boxed{\ddot{s}_1^1}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\boxed{\ddot{s}_2^1 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\, \text{—}, \boxed{\ddot{s}_2^1} w_{1,2} + \boxed{\ddot{u}_2} + x_1^{2,0}x_2^{1,0} + x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0},\ 0\,)$ $\widetilde{\mathbf{b}} := (\, \text{—},\ 0,\ 0\,)$ $\mathbf{d} := (s_2^1, \boxed{\ddot{s}_2^1}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\boxed{\ddot{s}_1^2 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\, \text{—}, \boxed{\ddot{s}_1^2} w_{1,1} + \boxed{\ddot{u}_1} + x_1^{2,0}x_1^{2,0} + x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0},\ 0\,)$ $\widetilde{\mathbf{b}} := (\, \text{—},\ 1,\ 0\,)$ $\mathbf{d} := (s_1^2, \boxed{\ddot{s}_1^2}),\ \widetilde{\mathbf{d}} := (0, 1)$ $\mathbf{f} := (0, t_1^2, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := 1$	$\underline{\mathsf{qCT}_2^2}$ $\boxed{\ddot{s}_2^2 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\, \text{—}, \boxed{\ddot{s}_2^2} w_{1,2} + \boxed{\ddot{u}_2} + x_1^{2,0}x_2^{2,0} + x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0},\ 0\,)$ $\widetilde{\mathbf{b}} := (\, \text{—},\ 0,\ 0\,)$ $\mathbf{d} := (s_2^2, \boxed{\ddot{s}_2^2}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,1}v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := \boxed{\sum_{\mu\in[2]} c_{1,\mu}\ddot{u}_\mu}$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,2}v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 11. Vectors in H_7.

$\underline{\mathsf{H}_2 = \mathsf{H}_3.}$ These hybrid games are information-theoretically equivalent. This can be confirmed by setting

$$\ddot{v}_i^j := \begin{cases} \ddot{v}_i'^j + x_1^{1,1}x_i^{1,1} - x_1^{1,0}x_i^{1,0} & (i=1) \\ \ddot{v}_i'^j + x_1^{1,1}x_i^{j,1} - x_1^{1,0}x_i^{j,0} & (i=2) \end{cases} \quad \text{where } \ddot{v}_i'^j \leftarrow \mathbb{Z}_p.$$

Additional sampling for qMSK $\ddot{u}_1, \ddot{u}_2 \leftarrow \mathbb{Z}_p$	
qCT_1^1 $\ddot{s}_1^1 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\ x_1^{1,0},\ x_1^{1,1},\ s_1^1 w_{1,1},\ s_1^1 w_{2,1},\ u_1,\ t_1^1,\ 0,\ 0\ )$ $\widetilde{\mathbf{b}} := (\ \ 0,\ \ x_1^{1,1},\ \ \widetilde{s}_1^1,\ \ \ \ 0,\ \ r_1^1,\ v_1, 0, 0\ )$ $\mathbf{d} := (s_1^1, \ddot{s}_1^1),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1} x_1^{1,1} - x_1^{1,0} x_1^{1,0}, 0),\ h := 0$	qCT_2^1 $\ddot{s}_2^1 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\ —, \ddot{s}_2^1 w_{1,2} + \ddot{u}_2 + \boxed{x_1^{2,1} x_2^{1,1}}, 0\ )$ $\widetilde{\mathbf{b}} := (\ —,\ \ \ \ 0,\ \ \ \ 0\ )$ $\mathbf{d} := (s_2^1, \ddot{s}_2^1),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1} x_2^{1,1} - x_1^{1,0} x_2^{1,0}, 0),\ h := 0$
qCT_1^2 $\ddot{s}_1^2 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\ —, \ddot{s}_1^2 w_{1,1} + \ddot{u}_1 + \boxed{x_1^{2,1} x_1^{2,1}}, 0\ )$ $\widetilde{\mathbf{b}} := (\ —,\ \ \ \ 1,\ \ \ \ 0\ )$ $\mathbf{d} := (s_1^2, \ddot{s}_1^2),\ \widetilde{\mathbf{d}} := (0, 1)$ $\mathbf{f} := (0, t_1^2, x_1^{1,1} x_1^{1,1} - x_1^{1,0} x_1^{1,0}, 0),\ h := 1$	qCT_2^2 $\ddot{s}_2^2 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\ —, \ddot{s}_2^2 w_{1,2} + \ddot{u}_2 + \boxed{x_1^{2,1} x_2^{2,1}}, 0\ )$ $\widetilde{\mathbf{b}} := (\ —,\ \ \ \ 0,\ \ \ \ 0\ )$ $\mathbf{d} := (s_2^2, \ddot{s}_2^2),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, x_1^{1,1} x_2^{2,1} - x_1^{1,0} x_2^{2,0}, 0),\ h := 0$
qSK $\widetilde{\mathbf{f}}_1 := (\sum_{\mu \in [2]} c_{1,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,1} v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := \sum_{\mu \in [2]} c_{1,\mu} \ddot{u}_\mu$	 $\widetilde{\mathbf{f}}_2 := (\sum_{\mu \in [2]} c_{2,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,2} v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 12. Vectors in H_8.

$\mathsf{H}_3 \approx_c \mathsf{H}_4$. We can justify this indistinguishability by the SXDH assumption, and the indistinguishability can be shown similarly to that between H_1 and H_2.

$\mathsf{H}_4 \approx_c \mathsf{H}_5$. We can justify this indistinguishability by the (partially) function-hiding property of pFE and gFE, similarly to the case of $\mathsf{G}_0 \approx_c \mathsf{H}_1$.

$\mathsf{G}_5 \approx_c \mathsf{H}_6$. We can justify this indistinguishability by the (partially) function-hiding property of pFE, iFE, and gFE, similarly to the case of $\mathsf{G}_0 \approx_c \mathsf{H}_1$. Note that here we also need to consider iFE since $\{\mathbf{d}, \widetilde{\mathbf{d}}\}$ is also changed, but it is easy to see that, for all $i, j, I, J \in [2]$, $\langle \mathbf{d}_i^j, \widehat{\mathbf{d}}_I^J \rangle$ in H_5 and that in H_6 are equal.

$\mathsf{H}_6 \approx_c \mathsf{H}_7$. We can justify this indistinguishability by the SXDH assumption, which implies $(\mathbb{G}, [\mathbf{s}]_1, [\widetilde{s}_1^2 \mathbf{s}]_1) \approx_c (\mathbb{G}, [\mathbf{s}]_1, [\ddot{\mathbf{s}}]_1)$ and $(\mathbb{G}, [\mathbf{u}]_1, [r_1^2 \mathbf{u}]_1) \approx_c (\mathbb{G}, [\mathbf{u}]_1, [\ddot{\mathbf{u}}]_1)$ where $\mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda), \mathbf{s} = \{s_i^j\}_{i,j \in [2]}, \ddot{\mathbf{s}} = \{\ddot{s}_i^j\}_{i,j \in [2]} \leftarrow \mathbb{Z}_p^4, \widetilde{s}_1^2 \leftarrow \mathbb{Z}_p, \mathbf{u} = \{u_i\}_{i \in [2]}, \ddot{\mathbf{u}} = \{\ddot{u}_i\}_{i \in [2]} \leftarrow \mathbb{Z}_p^2, r_1^2 \leftarrow \mathbb{Z}_p$.

$\mathsf{H}_7 \approx_c \mathsf{H}_8$. We can justify this indistinguishability by the message-hiding property of miFE. First, we prove that, for all $j \in [2]$, we have

$$\begin{aligned} & c_{1,1}(x_1^{2,0} x_1^{2,0} - x_1^{1,0} x_1^{1,0}) + c_{1,2}(x_1^{2,0} x_2^{j,0} - x_1^{1,0} x_2^{j,0}) \\ =& c_{1,1}(x_1^{2,1} x_1^{2,1} - x_1^{1,1} x_1^{1,1}) + c_{1,2}(x_1^{2,1} x_2^{j,1} - x_1^{1,1} x_2^{j,1}). \end{aligned} \tag{5.1}$$

Due to the game condition defined in Def. 2.3, the queries by the adversary satisfy

$$\sum_{i,\theta \in [2]} c_{i,\theta} x_i^{f(i),0} x_\theta^{f(\theta),0} = \sum_{i,\theta \in [2]} c_{i,\theta} x_i^{f(i),1} x_\theta^{f(\theta),1} \tag{5.2}$$

$$\sum_{i,\theta \in [2]} c_{i,\theta} x_i^{g(i),0} x_\theta^{g(\theta),0} = \sum_{i,\theta \in [2]} c_{i,\theta} x_i^{g(i),1} x_\theta^{g(\theta),1} \tag{5.3}$$

where

$$f(i) = \begin{cases} 2 & (i = 1) \\ j & (i = 2) \end{cases}, \quad g(i) = \begin{cases} 1 & (i = 1) \\ j & (i = 2) \end{cases}.$$

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b} := (\ x_1^{1,0},\ x_1^{1,1},\ s_1^1 w_{1,1},\ s_1^1 w_{2,1},\ u_1,\ t_1^1,\ 0,\ 0\ )$ $\widetilde{\mathbf{b}} := (\ \ 0,\ \ x_1^{1,1},\ \ \widetilde{s}_1^1,\ \ \ 0,\ \ r_1^1,\ v_1,\ 0,\ 0\ )$ $\mathbf{d} := (s_1^1, \boxed{s_1^1 \widetilde{s}_1^2}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1} x_1^{1,1} - x_1^{1,0} x_1^{1,0}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b} := (\ —, \boxed{s_2^1 \widetilde{s}_1^2 w_{1,2}} + \boxed{r_1^2 u_2} + x_1^{2,1} x_2^{1,1},\ 0\ )$ $\widetilde{\mathbf{b}} := (\ —,\ \ \ 0,\ \ \ 0\ )$ $\mathbf{d} := (s_2^1, \boxed{s_2^1 \widetilde{s}_1^2}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1} x_2^{1,1} - x_1^{1,0} x_2^{1,0}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b} := (\ x_1^{2,0},\ x_1^{2,1},\ s_1^2 w_{1,1},\ s_1^2 w_{2,1},\ u_1,\ t_1^2, \boxed{s_1^2 \widetilde{s}_1^2 w_{1,1}} + \boxed{r_1^2 u_1} + x_1^{2,1} x_1^{2,1},\ 0\ )$ $\widetilde{\mathbf{b}} := (\ \ 0,\ \ 0,\ \ \widetilde{s}_1^2,\ \ \ 0,\ \ r_1^2,\ v_1,\ \ \ 1,\ \ \ 0\ )$ $\mathbf{d} := (s_1^2, \boxed{s_1^2 \widetilde{s}_1^2}),\ \widetilde{\mathbf{d}} := (0, 1)$ $\mathbf{f} := (0, t_1^2, x_1^{1,1} x_1^{1,1} - x_1^{1,0} x_1^{1,0}, 0),\ h := 1$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b} := (\ —, \boxed{s_2^2 \widetilde{s}_1^2 w_{1,2}} + \boxed{r_1^2 u_2} + x_1^{2,1} x_2^{2,1},\ 0\ )$ $\widetilde{\mathbf{b}} := (\ —,\ \ \ 0,\ \ \ 0\ )$ $\mathbf{d} := (s_2^2, \boxed{s_2^2 \widetilde{s}_1^2}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, x_1^{1,1} x_2^{2,1} - x_1^{1,0} x_2^{2,0}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu \in [2]} c_{1,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,1} v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := \boxed{r_1^2 \sum_{\mu \in [2]} c_{1,\mu} u_\mu}$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu \in [2]} c_{2,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,2} v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 13. Vectors in H_9.

Note that Eq. (5.2) represents the restriction $f(x_1^{2,0}, x_2^{j,0}) = f(x_1^{2,1}, x_2^{j,1})$, and Eq. (5.3) represents the restriction $f(x_1^{1,0}, x_2^{j,0}) = f(x_1^{1,1}, x_2^{j,1})$. Eq. (5.2) $-$ Eq. (5.3) implies Eq. (5.1) by reflecting the fact that $c_{2,1} = 0$, which is defined in Def. 2.4.

Thanks to the message-hiding property of 2-slot miFE and Eq. (5.1), we have

$$\{\mathsf{miPP}, \mathsf{miCT}_1^{1,0}, \mathsf{miCT}_2^{1,0}, \mathsf{miCT}_2^{2,0}, \mathsf{miSK}\} \approx_c \{\mathsf{miPP}, \mathsf{miCT}_1^{1,1}, \mathsf{miCT}_2^{1,1}, \mathsf{miCT}_2^{2,1}, \mathsf{miSK}\}$$

where

$$\begin{aligned}
\mathsf{miPP} &= (\mathbb{G}, [w_{1,1}]_1, [w_{1,2}]_1) \\
\mathsf{miCT}_1^{1,\beta} &= ([\ddot{s}_1^2]_1, [\ddot{s}_1^2 w_{1,1} + \ddot{u}_1 + x_1^{2,\beta} x_1^{2,\beta} - x_1^{1,\beta} x_1^{1,\beta}]_1) \\
\mathsf{miCT}_2^{j,\beta} &= ([\ddot{s}_2^j]_1, [\ddot{s}_2^j w_{1,2} + \ddot{u}_2 + \underbrace{x_1^{2,\beta} x_2^{j,\beta} - x_1^{1,\beta} x_2^{j,\beta}}_{\text{message vectors}}]_1) \\
\mathsf{miSK} &= (\sum_{\mu \in [2]} c_{1,\mu} \ddot{u}_\mu, -c_{1,1} w_{1,1}, -c_{1,2} w_{1,2}, \underbrace{c_{1,1}, c_{1,2}}_{\text{key vector}}).
\end{aligned}$$

Roughly speaking, $[\mathbf{b}]_1$ in $\mathsf{qCT}_1^2, \mathsf{qCT}_2^1, \mathsf{qCT}_2^2$ is simulatable from $\mathsf{miCT}_1^{1,\beta}, \mathsf{miCT}_2^{1,\beta}, \mathsf{miCT}_2^{2,\beta}$, respectively, and $[\widetilde{h}_1]_1$ in qSK is simulatable from miSK, and the case of $\beta = 0$ corresponds to H_7 and $\beta = 1$ corresponds to H_8.

$\underline{\mathsf{H}_8 \approx_c \mathsf{H}_9.}$ We can justify this indistinguishability by the SXDH assumption similarly to the case of $\mathsf{H}_6 \approx_c \mathsf{H}_7$.

$\underline{\mathsf{H}_9 \approx_c \mathsf{H}_{10}.}$ We can justify this indistinguishability by the (partially) function-hiding property of pFE, iFE, and gFE, similarly to the case of $\mathsf{G}_5 \approx_c \mathsf{H}_6$. At this point, all ciphertexts for slot 1 are changed from encryption of 0-side to that of 1-side.

$\underline{\mathsf{H}_{10} \approx_c \mathsf{H}_{11}.}$ As stated above, G_0 to H_{10} are hybrid games for processing the ciphertexts for slot 1. Next, we apply a similar procedure to slot 2. H_{11} in the process for slot 2 corresponds to H_7 in the process for slot 1. That is, $\mathsf{G}_{10} \approx_c \mathsf{H}_{11}$ can be proven similarly to $\mathsf{G}_0 \approx_c \mathsf{H}_7$.

$\underline{\mathsf{H}_{11} \approx_c \mathsf{H}_{12}.}$ This indistinguishability can be prove similarly to the case of $\mathsf{H}_7 \approx_c \mathsf{H}_8$, but we need an additional tweak in this case. First, we prove that, for all $j \in [2]$, we have

$$\begin{aligned}
&c_{2,1}(x_2^{2,0} x_1^{j,0} - x_2^{1,0} x_1^{j,0}) + c_{2,2}(x_2^{2,0} x_2^{2,0} - x_2^{1,0} x_2^{1,0}) + c_{1,2}(x_1^{1,0} x_2^{2,0} - x_1^{1,0} x_2^{1,0}) \\
=&c_{2,1}(x_2^{2,1} x_1^{j,1} - x_2^{1,1} x_1^{j,1}) + c_{2,2}(x_2^{2,1} x_2^{2,1} - x_2^{1,1} x_2^{1,1}) + c_{1,2}(x_1^{1,1} x_2^{2,1} - x_1^{1,1} x_2^{1,1}).
\end{aligned} \tag{5.4}$$

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b} := (\, x_1^{1,0},\, x_1^{1,1},\, s_1^1 w_{1,1},\, s_1^1 w_{2,1},\, u_1,\, t_1^1,\, 0,\, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad x_1^{1,1},\quad \widetilde{s}_1^1,\qquad 0,\quad r_1^1,\, v_1,\, 0,\, 0)$ $\mathbf{d} := (s_1^1, \boxed{0}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b} := (\, x_2^{1,0},\, x_2^{1,1},\, s_2^1 w_{1,2},\, s_2^1 w_{2,2},\, u_2,\, t_2^1,\, \boxed{0},\, 0)$ $\widetilde{\mathbf{b}} := (\, x_2^{1,0},\quad 0,\qquad 0,\qquad \widetilde{s}_2^1,\quad r_2^1,\, v_2,\quad 0,\quad 0)$ $\mathbf{d} := (s_2^1, \boxed{0}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, 0),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b} := (\, x_1^{2,0},\ \ x_1^{2,1},\ \ s_1^2 w_{1,1},\, s_1^2 w_{2,1},\ \ u_1,\ \ t_1^2,\, \boxed{0},\, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad \boxed{x_1^{2,1}},\quad \boxed{\widetilde{s}_1^2},\qquad 0,\qquad \boxed{r_1^2},\, v_1,\, \boxed{0},\, 0)$ $\mathbf{d} := (s_1^2, \boxed{0}),\ \widetilde{\mathbf{d}} := (\boxed{\widetilde{s}_1^2}, \boxed{0})$ $\mathbf{f} := (r_1^2, t_1^2, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, 0),\ h := \boxed{0}$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b} := (\, x_2^{2,0},\, x_2^{2,1},\, s_2^2 w_{1,2},\, s_2^2 w_{2,2},\, u_2,\, t_2^2,\, \boxed{0},\, 0)$ $\widetilde{\mathbf{b}} := (\, x_2^{2,0},\quad 0,\qquad 0,\qquad \widetilde{s}_2^2,\quad r_2^2,\, v_2,\quad 0,\quad 0)$ $\mathbf{d} := (s_2^2, \boxed{0}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}, 0),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,1}v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := \boxed{0}$	 $\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,2}v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := 0$

Fig 14. Vectors in H_{10}.

Additional sampling for qMSK $\boxed{\ddot{u}_1, \ddot{u}_2 \leftarrow \mathbb{Z}_p}$	
$\underline{\mathsf{qCT}_1^1}$ $\boxed{\ddot{s}_1^1 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\,—, \boxed{\ddot{s}_1^1 w_{2,1} + \ddot{u}_1 + x_2^{2,0}x_1^{1,0} + x_2^{1,1}x_1^{1,1} - x_2^{1,0}x_1^{1,0}}, 0)$ $\widetilde{\mathbf{b}} := (\,—,\qquad 0,\qquad 0)$ $\mathbf{d} := (s_1^1, \boxed{\ddot{s}_1^1}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, \boxed{x_2^{1,1}x_1^{1,1} - x_2^{1,0}x_1^{1,0}}),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\boxed{\ddot{s}_2^1 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\qquad —\qquad , 0, 0)$ $\widetilde{\mathbf{b}} := (\,\boxed{0}, \boxed{x_2^{1,1}}, 0, \widetilde{s}_2^1, r_2^1, v_2, 0, 0)$ $\mathbf{d} := (s_2^1, \boxed{\ddot{s}_2^1}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, \boxed{x_2^{1,1}x_2^{1,1} - x_2^{1,0}x_2^{1,0}}),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\boxed{\ddot{s}_1^2 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\,—, \boxed{\ddot{s}_1^2 w_{2,1} + \ddot{u}_1 + x_2^{2,0}x_1^{2,0} + x_2^{1,1}x_1^{2,1} - x_2^{1,0}x_1^{2,0}}, 0)$ $\widetilde{\mathbf{b}} := (\,—,\qquad 0,\qquad 0)$ $\mathbf{d} := (s_1^2, \boxed{\ddot{s}_1^2}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, \boxed{x_2^{1,1}x_1^{2,1} - x_2^{1,0}x_1^{2,0}}),\ h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\boxed{\ddot{s}_2^2 \leftarrow \mathbb{Z}_p}$ $\mathbf{b} := (\qquad —\qquad , \boxed{\ddot{s}_2^2 w_{2,2} + \ddot{u}_2 + x_2^{2,0}x_2^{2,0} + x_2^{1,1}x_2^{1,1} - x_2^{1,0}x_2^{1,0}}, 0)$ $\widetilde{\mathbf{b}} := (\,\boxed{0}, 0, 0, \boxed{0}, \boxed{0}, v_2,\qquad \boxed{1},\qquad 0)$ $\mathbf{d} := (s_2^2, \boxed{\ddot{s}_2^2}),\ \widetilde{\mathbf{d}} := (\boxed{0}, \boxed{1})$ $\mathbf{f} := (\boxed{0}, t_2^2, x_1^{1,1}x_2^{2,1} - x_1^{1,0}x_2^{2,0}, \boxed{x_2^{1,1}x_2^{1,1} - x_2^{1,0}x_2^{1,0}}),\ h := \boxed{1}$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,1}v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := 0$	 $\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,2}v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := \boxed{\sum_{\mu\in[2]} c_{1,\mu}\ddot{u}_\mu}$

Fig 15. Vectors in H_{11}.

Due to the game condition defined in Def. 2.3, the queries by the adversary satisfy

$$\sum_{i,\theta\in[2]} c_{i,\theta} x_i^{f(i),0} x_\theta^{f(\theta),0} = \sum_{i,\theta\in[2]} c_{i,\theta} x_i^{f(i),1} x_\theta^{f(\theta),1} \tag{5.5}$$

$$\sum_{i,\theta\in[2]} c_{i,\theta} x_i^{g(i),0} x_\theta^{g(\theta),0} = \sum_{i,\theta\in[2]} c_{i,\theta} x_i^{g(i),1} x_\theta^{g(\theta),1} \tag{5.6}$$

where

$$f(i) = \begin{cases} 1 & (i = 1) \\ 2 & (i = 2) \end{cases},\quad g(i) = \begin{cases} 1 & (i = 1) \\ 1 & (i = 2) \end{cases}.$$

Note that Eq. (5.5) represents the restriction $f(x_1^{1,0}, x_2^{2,0}) = f(x_1^{1,1}, x_2^{2,1})$, and Eq. (5.6) represents the restriction $f(x_1^{1,0}, x_2^{1,0}) = f(x_1^{1,1}, x_2^{1,1})$. Eq. (5.5) − Eq. (5.6) implies Eq. (5.4) by reflecting the fact that $c_{2,1} = 0$, which is defined in Def. 2.4.

$\underline{\text{Additional sampling for } \mathsf{qMSK}}$ $\ddot{u}_1, \ddot{u}_2 \leftarrow \mathbb{Z}_p$	
$\underline{\mathsf{qCT}_1^1}$ $\ddot{s}_1^1 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{s}_1^1 w_{2,1} + \ddot{u}_1 + \boxed{x_2^{2,1} x_1^{1,1}}, 0)$ $\widetilde{\mathbf{b}} := (\,—, \quad 0, \quad 0)$ $\mathbf{d} := (s_1^1, \ddot{s}_1^1),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1} x_1^{1,1} - x_1^{1,0} x_1^{1,0}, x_2^{1,1} x_1^{1,1} - x_2^{1,0} x_1^{1,0})$ $h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\ddot{s}_2^1 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, 0, 0)$ $\widetilde{\mathbf{b}} := (\,—, 0, 0)$ $\mathbf{d} := (s_2^1, \ddot{s}_2^1),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1} x_2^{1,1} - x_1^{1,0} x_2^{1,0}, x_2^{1,1} x_2^{1,1} - x_2^{1,0} x_2^{1,0}),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\ddot{s}_1^2 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{s}_1^2 w_{2,1} + \ddot{u}_1 + \boxed{x_2^{2,1} x_1^{2,1}}, 0)$ $\widetilde{\mathbf{b}} := (\,—, \quad 0, \quad 0)$ $\mathbf{d} := (s_1^2, \ddot{s}_1^2),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, x_1^{1,1} x_1^{1,1} - x_1^{1,0} x_1^{1,0}, x_2^{1,1} x_1^{2,1} - x_2^{1,0} x_1^{2,0})$ $h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\ddot{s}_2^2 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{s}_2^2 w_{2,2} + \ddot{u}_2 + \boxed{x_2^{2,1} x_2^{2,1}}, 0)$ $\widetilde{\mathbf{b}} := (\,—, \quad 1, \quad 0)$ $\mathbf{d} := (s_2^2, \ddot{s}_2^2),\ \widetilde{\mathbf{d}} := (0, 1)$ $\mathbf{f} := (0, t_2^2, x_1^{1,1} x_2^{2,1} - x_1^{1,0} x_2^{2,0}, x_2^{1,1} x_2^{1,1} - x_2^{1,0} x_2^{1,0}),\ h := 1$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu \in [2]} c_{1,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,1} v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := 0$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu \in [2]} c_{2,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,2} v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := \sum_{\mu \in [2]} c_{1,\mu} \ddot{u}_\mu \boxed{+ c_{1,2}(x_1^{1,1} x_2^{1,1} - x_1^{1,0} x_2^{1,0} - (x_1^{1,1} x_2^{2,1} - x_1^{1,0} x_2^{2,0}))}$

Fig 16. Vectors in H_{12}.

$\underline{\text{Additional sampling for } \mathsf{qMSK}}$ $\ddot{u}_1, \ddot{u}_2 \leftarrow \mathbb{Z}_p$	
$\underline{\mathsf{qCT}_1^1}$ $\ddot{s}_1^1 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{s}_1^1 w_{2,1} + \ddot{u}_1 + x_2^{2,1} x_1^{1,1}, 0)$ $\widetilde{\mathbf{b}} := (\,—, \quad 0, \quad 0)$ $\mathbf{d} := (s_1^1, \ddot{s}_1^1),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1} x_1^{1,1} - x_1^{1,0} x_1^{1,0}, x_2^{1,1} x_1^{1,1} - x_2^{1,0} x_1^{1,0})$ $h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\ddot{s}_2^1 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, 0, 0)$ $\widetilde{\mathbf{b}} := (\,—, 0, 0)$ $\mathbf{d} := (s_2^1, \ddot{s}_2^1),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1} x_2^{1,1} - x_1^{1,0} x_2^{1,0}, x_2^{1,1} x_2^{1,1} - x_2^{1,0} x_2^{1,0}),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\ddot{s}_1^2 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{s}_1^2 w_{2,1} + \ddot{u}_1 + x_2^{2,1} x_1^{2,1}, 0)$ $\widetilde{\mathbf{b}} := (\,—, \quad 0, \quad 0)$ $\mathbf{d} := (s_1^2, \ddot{s}_1^2),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, x_1^{1,1} x_1^{1,1} - x_1^{1,0} x_1^{1,0}, \boxed{x_2^{1,1} x_1^{1,1} - x_2^{1,0} x_1^{1,0}})$ $h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\ddot{s}_2^2 \leftarrow \mathbb{Z}_p$ $\mathbf{b} := (\,—, \ddot{s}_2^2 w_{2,2} + \ddot{u}_2 + x_2^{2,1} x_2^{2,1}, 0)$ $\widetilde{\mathbf{b}} := (\,—, \quad 1, \quad 0)$ $\mathbf{d} := (s_2^2, \ddot{s}_2^2),\ \widetilde{\mathbf{d}} := (0, 1)$ $\mathbf{f} := (0, t_2^2, \boxed{x_1^{1,1} x_2^{1,1} - x_1^{1,0} x_2^{1,0}}, x_2^{1,1} x_2^{1,1} - x_2^{1,0} x_2^{1,0}),\ h := 1$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu \in [2]} c_{1,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,1} v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := 0$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu \in [2]} c_{2,\mu} u_\mu, \sum_{\mu \in [2]} c_{\mu,2} v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := \sum_{\mu \in [2]} c_{1,\mu} \ddot{u}_\mu + c_{1,2}(\cancel{x_1^{1,1} x_2^{1,1} - x_1^{1,0} x_2^{1,0}} - (\cancel{x_1^{1,1} x_2^{2,1} - x_1^{1,0} x_2^{2,0}}))$

Fig 17. Vectors in H_{13}.

Thanks to the message-hiding property of 3-slot miFE and Eq. (5.4), we have

$$\begin{aligned} &\{\mathsf{miPP}, \mathsf{miCT}_1^{1,0}, \mathsf{miCT}_1^{2,0}, \mathsf{miCT}_2^{1,0}, \mathsf{miCT}_3^{1,0}, \mathsf{miSK}\} \\ \approx_c &\{\mathsf{miPP}, \mathsf{miCT}_1^{1,1}, \mathsf{miCT}_1^{2,1}, \mathsf{miCT}_2^{1,1}, \mathsf{miCT}_3^{1,1}, \mathsf{miSK}\} \end{aligned}$$

where

$$\begin{aligned} \mathsf{miPP} &= (\mathbb{G}, [w_{2,1}]_1, [w_{2,2}]_1, [w_{2,3}]_1) \\ \mathsf{miCT}_1^{j,\beta} &= ([\ddot{s}_1^j]_1, [\ddot{s}_1^j w_{2,1} + \ddot{u}_1 + x_2^{2,\beta} x_1^{j,\beta} - x_2^{1,\beta} x_1^{j,\beta}]_1) \\ \mathsf{miCT}_2^{1,\beta} &= ([\ddot{s}_2^2]_1, [\ddot{s}_2^2 w_{2,2} + \ddot{u}_2 + x_2^{2,\beta} x_2^{2,\beta} - x_2^{1,\beta} x_2^{1,\beta}]_1) \end{aligned}$$

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b} := (\, x_1^{1,0},\, x_1^{1,1},\, s_1^1 w_{1,1},\, s_1^1 w_{2,1},\, u_1,\, t_1^1,\, \boxed{0}, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad x_1^{1,1},\quad \widetilde{s}_1^1,\qquad 0,\quad r_1^1,\, v_1,\;\, 0,\;\, 0)$ $\mathbf{d} := (s_1^1, \boxed{0}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, x_2^{1,1}x_1^{1,1} - x_2^{1,0}x_1^{1,0}),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b} := (\, x_2^{1,0},\, x_2^{1,1},\, s_2^1 w_{1,2},\, s_2^1 w_{2,2},\, u_2,\, t_2^1,\, 0,\, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad x_2^{1,1},\quad 0,\qquad \widetilde{s}_2^1,\quad r_2^1,\, v_2,\, 0,\, 0)$ $\mathbf{d} := (s_2^1, \boxed{0}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, x_2^{1,1}x_2^{1,1} - x_2^{1,0}x_2^{1,0}),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b} := (\, x_1^{2,0},\, x_1^{2,1},\, s_1^2 w_{1,1},\, s_1^2 w_{2,1},\, u_1,\, t_1^2,\, \boxed{0}, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad x_1^{2,1},\quad 0,\qquad \widetilde{s}_1^2,\quad r_1^2,\, v_1,\;\, 0,\;\, 0)$ $\mathbf{d} := (s_1^2, \boxed{0}),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, x_1^{1,1}x_1^{1,1} - x_1^{1,0}x_1^{1,0}, x_2^{1,1}x_1^{1,1} - x_2^{1,0}x_1^{1,0}),\ h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b} := (\, x_2^{2,0},\;\, x_2^{2,1},\;\, s_2^2 w_{1,2},\, s_2^2 w_{2,2},\;\, u_2,\;\, t_2^2,\, \boxed{0}, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad \boxed{x_2^{2,1}},\quad \boxed{\widetilde{s}_2^2},\qquad 0,\quad \boxed{r_2^2}, v_2, \boxed{0}, 0)$ $\mathbf{d} := (s_2^2, \boxed{0}),\ \widetilde{\mathbf{d}} := (\boxed{\widetilde{s}_2^2}, \boxed{0})$ $\mathbf{f} := (\boxed{r_2^2}, t_2^2, x_1^{1,1}x_2^{1,1} - x_1^{1,0}x_2^{1,0}, x_2^{1,1}x_2^{1,1} - x_2^{1,0}x_2^{1,0}),\ h := \boxed{0}$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,1}v_\mu, c_{1,1}, c_{2,1})$ $\widetilde{h}_1 := 0$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,2}v_\mu, c_{1,2}, c_{2,2})$ $\widetilde{h}_2 := \boxed{0}$

Fig 18. Vectors in H_{14}.

$\underline{\mathsf{qCT}_1^1}$ $\mathbf{b} := (\, x_1^{1,0},\, x_1^{1,1},\, s_1^1 w_{1,1},\, s_1^1 w_{2,1},\, u_1,\, t_1^1,\, 0,\, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad x_1^{1,1},\quad \widetilde{s}_1^1,\qquad 0,\quad r_1^1,\, v_1,\, 0,\, 0)$ $\mathbf{d} := (s_1^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^1, 0)$ $\mathbf{f} := (r_1^1, t_1^1, \boxed{0}, \boxed{0}),\ h := 0$	$\underline{\mathsf{qCT}_2^1}$ $\mathbf{b} := (\, x_2^{1,0},\, x_2^{1,1},\, s_2^1 w_{1,2},\, s_2^1 w_{2,2},\, u_2,\, t_2^1,\, 0,\, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad x_2^{1,1},\quad 0,\qquad \widetilde{s}_2^1,\quad r_2^1,\, v_2,\, 0,\, 0)$ $\mathbf{d} := (s_2^1, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^1, 0)$ $\mathbf{f} := (r_2^1, t_2^1, \boxed{0}, \boxed{0}),\ h := 0$
$\underline{\mathsf{qCT}_1^2}$ $\mathbf{b} := (\, x_1^{2,0},\, x_1^{2,1},\, s_1^2 w_{1,1},\, s_1^2 w_{2,1},\, u_1,\, t_1^2,\, 0,\, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad x_1^{2,1},\quad 0,\qquad \widetilde{s}_1^2,\quad r_1^2,\, v_1,\, 0,\, 0)$ $\mathbf{d} := (s_1^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_1^2, 0)$ $\mathbf{f} := (r_1^2, t_1^2, \boxed{0}, \boxed{0}),\ h := 0$	$\underline{\mathsf{qCT}_2^2}$ $\mathbf{b} := (\, x_2^{2,0},\, x_2^{2,1},\, s_2^2 w_{1,2},\, s_2^2 w_{2,2},\, u_2,\, t_2^2,\, 0,\, 0)$ $\widetilde{\mathbf{b}} := (\quad 0,\quad x_2^{2,1},\quad \widetilde{s}_2^2,\qquad 0,\quad r_2^2,\, v_2,\, 0,\, 0)$ $\mathbf{d} := (s_2^2, 0),\ \widetilde{\mathbf{d}} := (\widetilde{s}_2^2, 0)$ $\mathbf{f} := (r_2^2, t_2^2, \boxed{0}, \boxed{0}),\ h := 0$
$\underline{\mathsf{qSK}}$ $\widetilde{\mathbf{f}}_1 := (\sum_{\mu\in[2]} c_{1,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,1}v_\mu, \boxed{0}, \boxed{0})$ $\widetilde{h}_1 := 0$	$\widetilde{\mathbf{f}}_2 := (\sum_{\mu\in[2]} c_{2,\mu}u_\mu, \sum_{\mu\in[2]} c_{\mu,2}v_\mu, \boxed{0}, \boxed{0})$ $\widetilde{h}_2 := 0$

Fig 19. Vectors in H_{15}.

$$\mathsf{miCT}_3^{1,\beta} = ([\ddot{s}_3^1]_1, [\ddot{s}_3^1 w_{2,3} + \ddot{u}_3 + \underbrace{x_1^{1,\beta}x_2^{2,\beta} - x_1^{1,\beta}x_2^{1,\beta}}_{\text{message vectors}}]_1)$$

$$\mathsf{miSK} = (\sum_{\mu\in[2]} c_{2,\mu}\ddot{u}_\mu + c_{1,2}\ddot{u}_3, -c_{2,1}w_{2,1}, -c_{2,2}w_{2,2}, -c_{1,2}w_{2,3}, \underbrace{c_{2,1}, c_{2,2}, c_{1,2}}_{\text{key vector}}).$$

Roughly speaking, $[\mathbf{b}]_1$ in $\mathsf{qCT}_1^1, \mathsf{qCT}_1^2, \mathsf{qCT}_2^2$ is simulatable from $\mathsf{miCT}_1^{1,\beta}, \mathsf{miCT}_1^{2,\beta}, \mathsf{miCT}_2^{1,\beta}$, respectively, and $[\widetilde{h}_2]_1$ in qSK is simulatable from miSK and $\mathsf{miCT}_3^{1,\beta}$. More precisely,

$$\widetilde{h}_2 = \mathsf{K}_1 - \mathsf{C}_1\mathsf{K}_4 - c_{1,2}(\mathsf{C}_2 + x_1^{1,0}x_2^{2,0} - x_1^{1,0}x_2^{1,0})$$

where $\mathsf{miCT}_3^{1,\beta} = ([\mathsf{C}_1]_1, [\mathsf{C}_2]_1)$ and $\mathsf{miSK} = (\mathsf{K}_1, \ldots, \mathsf{K}_7)$. The case of $\beta = 0$ corresponds to H_{11} and $\beta = 1$ corresponds to H_{12}.

$\underline{\mathsf{H}_{12} \approx_c \mathsf{H}_{13}.}$ We can justify this indistinguishability by the function-hiding property of gFE. For all $i, j \in [2]$, $\langle \mathbf{f}_i^j, \widehat{\mathbf{f}}_i \rangle + h_i^j \widetilde{h}_i$ in H_{12} and that in H_{13} are equal, which implies, for all $j_1, j_2 \in [2]$, $\sum_{i\in[2]}(\langle \mathbf{f}_i^{j_i}, \widehat{\mathbf{f}}_i \rangle + h_i^{j_i} \widetilde{h}_i)$ in H_{12} and that in H_{13} are equal. Thus, the indistinguishability of $\{\mathbf{f}, \widetilde{\mathbf{f}}, h, \widetilde{h}\}$ between H_{12} and H_{13} is implied by the function-hiding property of gFE.

$\underline{\mathsf{H}_{13} \approx_c \mathsf{H}_{14}.}$ This indistinguishability can be proven similarly to $\mathsf{H}_8 \approx_c \mathsf{H}_{10}$.

$\underline{\mathsf{H}_{14} \approx_c \mathsf{H}_{15}}$. Due to the game condition defined in Def. 2.3, the queries by the adversary satisfy

$$\sum_{i,\theta \in [2]} c_{i,\theta}(x_i^{1,1} x_\theta^{1,1} - x_i^{1,0} x_\theta^{1,0}) = 0,$$

which implies, for all $j_1, j_2 \in [2]$, $\sum_{i \in [2]} (\langle \mathbf{f}_i^{j_i}, \widehat{\mathbf{f}}_i \rangle + h_i^{j_i} \widetilde{h}_i)$ in H_{14} and that in H_{15} are equal. Thus, the indistinguishability of $\{\mathbf{f}, \widetilde{\mathbf{f}}\}$ between H_{14} and H_{15} is implied by the function-hiding property of gFE.

$\underline{\mathsf{H}_{15} \approx_c \mathsf{G}_1}$. It is easy to see that this indistinguishability is implied by the partially function-hiding property of pFE, since, for all $i, j, I, J \in [2]$, $\langle \mathbf{b}_i^j, \widehat{\mathbf{b}}_I^J \rangle$ in H_{15} and that in G_1 are equal.

6 Our Full MQFE Scheme

6.1 Construction

We present our MQFE scheme, that is, a MIFE scheme for $\mathcal{F}^{\mathsf{MQF}}_{m,n,X,C}$. It is convenient for us to define the following functions that relate indices in $[n] \times [m]$ with those in $[mn]$:

- location function, $\mathsf{lo} : [n] \times [m] \to [mn]$, defined as $\mathsf{lo}(x, y) = (x - 1)m + y$;
- location set function, $\mathsf{ls} : [n] \to 2^{[mn]}$, defined as $\mathsf{ls}(x) = \{\mathsf{lo}(x, 1), \ldots, \mathsf{lo}(x, m)\}$;
- slot function, $\mathsf{sl} : [mn] \to [n]$, defined as $\mathsf{sl}(x) = \lceil x/m \rceil$;
- entry function, $\mathsf{en} : [mn] \to [m]$, defined as $\mathsf{en}(x) = x - m(\mathsf{sl}(x) - 1)$.

Note that we have $\mathsf{lo}(\mathsf{sl}(x), \mathsf{en}(x)) = x$ for all $x \in [mn]$. Let $\mathcal{D}_k$ be a matrix distribution. Let $\mathsf{pFE} = (\mathsf{pSetup}, \mathsf{pEnc}, \mathsf{pKeyGen}, \mathsf{pDec})$ be an FE scheme for $\mathcal{F}^{\mathsf{PIP}}_{2n, 2+(mn+2)k+(2+k)m, \mathbb{G}}$ (Def. 3.2), $\mathsf{iFE} = (\mathsf{iSetup}, \mathsf{iEnc}, \mathsf{iKeyGen}, \mathsf{iDec})$ be an FE scheme for $\mathcal{F}^{\mathsf{IP}}_{k+1,\mathbb{G}}$ (Def. 3.1), and $\mathsf{gFE} = (\mathsf{gSetup}, \mathsf{gEnc}, \mathsf{gKeyGen}, \mathsf{gDec})$ be an FE scheme for $\mathcal{F}^{\mathsf{MGIP}}_{2k+m^2n,1,n,\mathbb{G}}$ (Def. 4.2). We construct our MQFE scheme $\mathsf{qFE} = (\mathsf{qSetup}, \mathsf{qEnc}, \mathsf{qKeyGen}, \mathsf{qDec})$ from pFE, iFE, and gFE. Note that $\mathbb{G}$ is fixed by qSetup.

$\mathsf{qSetup}(1^\lambda)$**:** It outputs $\mathsf{qPP}, \mathsf{qMSK}$ as follows:

$$\mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda)$$
$$\mathbf{A}_1, \ldots, \mathbf{A}_n \leftarrow \mathcal{D}_k,\ \{\mathbf{w}_{i,j}\}_{i,j \in [mn]} \leftarrow \mathbb{Z}_p^{k+1},\ \widetilde{\mathbf{U}}_1, \ldots, \widetilde{\mathbf{U}}_{mn} \leftarrow \mathbb{Z}_p^{k \times k}$$
$$\mathbf{u}_1, \ldots, \mathbf{u}_{mn} \leftarrow \mathbb{Z}_p^k,\ \mathbf{V}_1, \ldots, \mathbf{V}_{mn} \leftarrow \mathbb{Z}_p^{k \times k},\ \widetilde{\mathbf{v}}_1, \ldots, \widetilde{\mathbf{v}}_{mn} \leftarrow \mathbb{Z}_p^k$$
$$\mathsf{pPP}, \mathsf{pMSK} \leftarrow \mathsf{pSetup}(1^\lambda),\ \mathsf{iPP}, \mathsf{iMSK} \leftarrow \mathsf{iSetup}(1^\lambda),\ \mathsf{gPP}, \mathsf{gMSK} \leftarrow \mathsf{gSetup}(1^\lambda)$$
$$\mathsf{qPP} := (\mathbb{G}, \mathsf{pPP}, \mathsf{iPP}, \mathsf{gPP})$$
$$\mathsf{qMSK} := (\mathbf{A}_1, \ldots, \mathbf{A}_n, \{\mathbf{w}_{i,j}\}_{i,j \in [mn]}, \{\widetilde{\mathbf{U}}_i, \mathbf{u}_i, \mathbf{V}_i, \widetilde{\mathbf{v}}_i\}_{i \in [mn]}, \mathsf{pMSK}, \mathsf{iMSK}, \mathsf{gMSK}).$$

$\mathsf{qEnc}(\mathsf{qMSK}, i, \mathbf{x}_i)$**:** Let $\mathbf{w}_{\mathsf{lo}(i,\kappa)}^\top := (\mathbf{w}_{1,\mathsf{lo}(i,\kappa)}, \ldots, \mathbf{w}_{mn,\mathsf{lo}(i,\kappa)})$. First, it samples vectors as follows:

$$\mathbf{S} \leftarrow \mathbb{Z}_p^{k \times k},\ \widetilde{\mathbf{s}}, \mathbf{r}, \mathbf{t} \leftarrow \mathbb{Z}_p^k,\ L \leftarrow \mathbb{Z}_p$$
$$\mathbf{l} := \mathbf{e}_{i/n} \otimes (1, L) \in \mathbb{Z}_p^{2n},\ \widetilde{\mathbf{l}} := \mathbf{e}_{i/n} \otimes (L, -1) \in \mathbb{Z}_p^{2n}$$
$$\mathbf{b}_{\kappa,1} := (x_{i,\kappa}, 0) \in \mathbb{Z}_p^2,\ \mathbf{b}_{\kappa,2} := (\mathbf{w}_{\mathsf{lo}(i,\kappa)}^\top (\mathbf{I}_{mn} \otimes \mathbf{A}_i \mathbf{S}), \mathbf{u}_{\mathsf{lo}(i,\kappa)}) \in \mathbb{Z}_p^{(mn+1)k}$$
$$\mathbf{b}_{\kappa,3} := \mathbf{t}^\top \mathbf{V}_{\mathsf{lo}(i,\kappa)} \in \mathbb{Z}_p^k,\ \mathbf{b}_{\kappa,4} = \mathbf{b}_{\kappa,5} := \mathbf{0} \in \mathbb{Z}_p^m,\ \widetilde{\mathbf{b}}_{\kappa,6} := \mathbf{0} \in \mathbb{Z}_p^{km}$$
$$\mathbf{b}_\kappa := (\mathbf{b}_{\kappa,1}, \ldots, \mathbf{b}_{\kappa,6})$$
$$\widetilde{\mathbf{b}}_{\kappa,1} := (x_{i,\kappa}, 0) \in \mathbb{Z}_p^2,\ \widetilde{\mathbf{b}}_{\kappa,2} := (\mathbf{e}_{\mathsf{lo}(i,\kappa)/mn} \otimes \widetilde{\mathbf{s}}, \mathbf{r}^\top \widetilde{\mathbf{U}}_{\mathsf{lo}(i,\kappa)}) \in \mathbb{Z}_p^{(mn+1)k}$$
$$\widetilde{\mathbf{b}}_{\kappa,3} := \widetilde{\mathbf{v}}_{\mathsf{lo}(i,\kappa)}^\top \in \mathbb{Z}_p^k,\ \widetilde{\mathbf{b}}_{\kappa,4} = \widetilde{\mathbf{b}}_{\kappa,5} := \mathbf{0} \in \mathbb{Z}_p^m,\ \widetilde{\mathbf{b}}_{\kappa,6} := \mathbf{0} \in \mathbb{Z}_p^{km}$$
$$\widetilde{\mathbf{b}}_\kappa := (\widetilde{\mathbf{b}}_{\kappa,1}, \ldots, \widetilde{\mathbf{b}}_{\kappa,6})$$
$$\mathbf{d}_\tau := (\mathbf{a}_{i,\tau}^\top \mathbf{S}, 0) \in \mathbb{Z}_p^{k+1},\ \widetilde{\mathbf{d}} := (\widetilde{\mathbf{s}}, 0) \in \mathbb{Z}_p^{k+1}$$
$$\mathbf{f}_1 := (\mathbf{r}, \mathbf{t}) \in \mathbb{Z}_p^{2k},\ \mathbf{f}_{2,1} = \cdots = \mathbf{f}_{2,n} := \mathbf{0} \in \mathbb{Z}_p^{m^2},\ \mathbf{f} := (\mathbf{f}_1, \mathbf{f}_{2,1}, \ldots, \mathbf{f}_{2,n}),\ h := 0$$

where $x_{i,\kappa}$ is the κ-th entry of $\mathbf{x}_i$ and $\mathbf{a}_{i,\tau}^\top$ is the τ-th row of $\mathbf{A}_i$. Then, it outputs qCT_i as follows:

$$\begin{aligned}
&\mathsf{pCT}_{\mathsf{lo}(i,\kappa)} \leftarrow \mathsf{pEnc}(\mathsf{pMSK}, (\mathbf{l}, [\mathbf{b}_\kappa]_1)),\ \mathsf{pSK}_{\mathsf{lo}(i,\kappa)} \leftarrow \mathsf{pKeyGen}(\mathsf{pMSK}, (\widetilde{\mathbf{l}}, [\widetilde{\mathbf{b}}_\kappa]_2))\\
&\mathsf{iCT}_{i,\tau} \leftarrow \mathsf{iEnc}(\mathsf{iMSK}, [\mathbf{d}_\tau]_1),\ \mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}, [\widetilde{\mathbf{d}}]_2)\\
&\mathsf{gCT}_i \leftarrow \mathsf{gEnc}(\mathsf{gMSK}, i, ([\mathbf{f}]_1, [h]_2))\\
&\mathsf{qCT}_i := (\{\mathsf{pCT}_{\mathsf{lo}(i,\kappa)}, \mathsf{pSK}_{\mathsf{lo}(i,\kappa)}\}_{\kappa\in[m]}, \{\mathsf{iCT}_{i,\tau}\}_{\tau\in[k+1]}, \mathsf{iSK}_i, \mathsf{gCT}_i).
\end{aligned} \tag{6.1}$$

$\mathsf{qKeyGen}(\mathsf{qMSK}, \mathbf{c})$**:** It outputs qSK as follows:

$$\begin{aligned}
&\widetilde{\mathbf{f}}_{i,1} := \left(\sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in[mn]}} c_{\mu,\nu} \widetilde{\mathbf{U}}_\mu \mathbf{u}_\nu, \sum_{\substack{\mu\in[mn]\\ \nu\in\mathsf{ls}(i)}} c_{\mu,\nu} \mathbf{V}_\nu \widetilde{\mathbf{v}}_\mu \right) \in \mathbb{Z}_p^{2k}\\
&\widetilde{\mathbf{f}}_{i,2,1} = \cdots = \widetilde{\mathbf{f}}_{i,2,n} := \mathbf{0} \in \mathbb{Z}_p^{m^2},\ \widetilde{\mathbf{f}}_i := (\widetilde{\mathbf{f}}_{i,1}, \widetilde{\mathbf{f}}_{i,2,1}, \ldots, \widetilde{\mathbf{f}}_{i,2,n}),\ \widetilde{h}_i := 0\\
&\mathsf{gSK} \leftarrow \mathsf{gKeyGen}(\mathsf{gMSK}, \{[\widetilde{\mathbf{f}}_i]_2, [\widetilde{h}_i]_1\}_{i\in[n]})\\
&\boldsymbol{\sigma}_{i,\theta} := \sum_{\substack{\mu\in\mathsf{ls}(i),\\ \nu\in\mathsf{ls}(\theta)}} c_{\mu,\nu} \mathbf{w}_{\mu,\nu} \in \mathbb{Z}_p^{k+1}\\
&\mathsf{qSK} := (\mathbf{c}, \mathsf{gSK}, \{\boldsymbol{\sigma}_{i,\theta}\}_{i,\theta\in[n]}).
\end{aligned}$$

$\mathsf{qDec}(\mathsf{qCT}_1, \ldots, \mathsf{qCT}_n, \mathsf{qSK})$**:** It computes

$$\begin{aligned}
&[z_1]_T := \prod_{\mu,\nu\in[mn]} \mathsf{pDec}(\mathsf{pCT}_\nu, \mathsf{pSK}_\mu)^{c_{\mu,\nu}}\\
&[\mathbf{z}_{2,i,\theta}]_T := (\mathsf{iDec}(\mathsf{iCT}_{\theta,1}, \mathsf{iSK}_i), \ldots, \mathsf{iDec}(\mathsf{iCT}_{\theta,k+1}, \mathsf{iSK}_i))\\
&[z_3]_T := \mathsf{gDec}(\mathsf{gCT}_1, \ldots, \mathsf{gCT}_n, \mathsf{gSK})\\
&[z]_T := [z_1 - \sum_{i,\theta\in[n]} \langle \mathbf{z}_{2,i,\theta}, \boldsymbol{\sigma}_{i,\theta} \rangle - z_3]_T.
\end{aligned}$$

Then, it searches for z within the range of $z \leq |m^2 n^2 C X^2|$.

Correctness. Let $x_{\mathsf{lo}(i,\kappa)} = x_{i,\kappa}$ and $\mathbf{S}_i, \widetilde{\mathbf{s}}_i, \mathbf{r}_i, \mathbf{t}_i, \mathbf{l}_i, \widetilde{\mathbf{l}}_i, \mathbf{b}_i, \widetilde{\mathbf{b}}_i$ be random elements used to generate qCT_i. Observe that $\langle \mathbf{l}_i, \widetilde{\mathbf{l}}_I \rangle = 0$ for all $i, I \in [n]$, and thus $\mathsf{pDec}(\mathsf{pCT}_i, \mathsf{pSK}_I) = \langle \mathbf{b}_i, \widetilde{\mathbf{b}}_I \rangle$. From the correctness of $\mathsf{pFE}, \mathsf{iFE}, \mathsf{gEF}$, we have

$$\begin{aligned}
z_1 &= \sum_{\mu,\nu\in[mn]} c_{\mu,\nu} (x_\mu x_\nu + \mathbf{w}_{\mu,\nu}^\top \mathbf{A}_{\mathsf{sl}(\nu)} \mathbf{S}_{\mathsf{sl}(\nu)} \widetilde{\mathbf{s}}_{\mathsf{sl}(\mu)} + \mathbf{r}_{\mathsf{sl}(\mu)}^\top \widetilde{\mathbf{U}}_\mu \mathbf{u}_\nu + \mathbf{t}_{\mathsf{sl}(\nu)}^\top \mathbf{V}_\nu \widetilde{\mathbf{v}}_\mu)\\
\sum_{i,\theta\in[n]} \langle \mathbf{z}_{2,i,\theta}, \boldsymbol{\sigma}_{i,\theta} \rangle &= \sum_{i,\theta\in[n]} \sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in\mathsf{ls}(\theta)}} c_{\mu,\nu} \mathbf{w}_{\mu,\nu}^\top \mathbf{A}_\theta \mathbf{S}_\theta \widetilde{\mathbf{s}}_i\\
&= \sum_{\mu,\nu\in[mn]} c_{\mu,\nu} \mathbf{w}_{\mu,\nu}^\top \mathbf{A}_{\mathsf{sl}(\nu)} \mathbf{S}_{\mathsf{sl}(\nu)} \widetilde{\mathbf{s}}_{\mathsf{sl}(\mu)}\\
z_3 &= \sum_{i\in[n]} \left(\sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in[mn]}} c_{\mu,\nu} \mathbf{r}_i^\top \widetilde{\mathbf{U}}_\mu \mathbf{u}_\nu + \sum_{\substack{\mu\in[mn]\\ \nu\in\mathsf{ls}(i)}} c_{\mu,\nu} \mathbf{t}_i^\top \mathbf{V}_\nu \widetilde{\mathbf{v}}_\mu \right)\\
&= \sum_{\mu,\nu\in[mn]} c_{\mu,\nu} (\mathbf{r}_{\mathsf{sl}(\mu)}^\top \widetilde{\mathbf{U}}_\mu \mathbf{u}_\nu + \mathbf{t}_{\mathsf{sl}(\nu)}^\top \mathbf{V}_\nu \widetilde{\mathbf{v}}_\mu).
\end{aligned}$$

Hence, we have $z = \sum_{\mu,\nu\in[mn]} c_{\mu,\nu} x_\mu x_\nu$.

```
$\underline{\mathsf{G}_\beta}$
$\{i, \mathbf{x}_i^{j,0}, \mathbf{x}_i^{j,1}\}_{i\in[n],j\in[q_{\mathsf{CT}}]} \leftarrow \mathcal{A}(1^\lambda)$
$\mathsf{qPP}, \mathsf{qMSK} \leftarrow \mathsf{qSetup}(1^\lambda)$
$\mathsf{qCT}_i^j \leftarrow \mathsf{qEnc}(\mathsf{qMSK}, i, \mathbf{x}_i^{j,\beta})$
$\beta' \leftarrow \mathcal{A}^{\mathsf{qKeyGen}(\mathsf{qMSK},\cdot)}(\mathsf{qPP}, \{\mathsf{qCT}_i^j\}_{i\in[n],j\in[q_{\mathsf{CT}}]})$
--------------------------------------------------------------------------
$\underline{\mathsf{H}_\iota^\eta}$
$\{i, \mathbf{x}_i^{j,0}, \mathbf{x}_i^{j,1}\}_{i\in[n],j\in[q_{\mathsf{CT}}]} \leftarrow \mathcal{A}(1^\lambda)$
$\mathsf{qPP}, \mathsf{qMSK} \leftarrow \mathsf{qSetup}(1^\lambda)$
$\mathsf{qCT}_i^j \leftarrow \widetilde{\mathsf{qEnc}}_\iota^\eta(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$
$\beta' \leftarrow \mathcal{A}^{\widetilde{\mathsf{qKeyGen}}(\mathsf{qMSK},\cdot)}(\mathsf{qPP}, \{\mathsf{qCT}_i^j\}_{i\in[n],j\in[q_{\mathsf{CT}}]})$
```

Fig 20. Security games for qFE.

6.2 Multi-input IPFE Scheme for Security Analysis

Before going to security analysis of our MQFE scheme, we recall the multi-input IPFE scheme (the MIFE scheme for $\mathcal{F}^{\mathsf{MIP}}_{m,n,\mathbb{G}}$, denoted by $\mathsf{miFE} = (\mathsf{miSetup}, \mathsf{miEnc}, \mathsf{miKeyGen}, \mathsf{miDec})$) by Abdalla *et al.* [4, Sec.4.1] that satisfies the (adaptive) message-hiding security under the MDDH assumption. Although the original scheme uses a pairing-free group for the construction, it is easy to see that their scheme can be similarly built on pairing groups where the MDDH assumption holds. We use the scheme built on the pairing groups in the security proof of our MQFE scheme. We denote the advantage of $\mathcal{A}$ against miFE by $\mathsf{Adv}^{\mathsf{miFE}}_{\mathcal{A},\mathsf{mh}}(\lambda)$. The scheme is described as follows.

$\mathsf{miSetup}(1^\lambda)$**:** It outputs $\mathsf{miPP}, \mathsf{miMSK}$ as follows:

$$\begin{aligned}&\mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda),\ \mathbf{A}_1, \ldots, \mathbf{A}_n \leftarrow \mathcal{D}_k,\ \mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow \mathbb{Z}_p^{m\times(k+1)},\ \mathbf{u}_1, \ldots, \mathbf{u}_n \leftarrow \mathbb{Z}_p^m\\ &\mathsf{miPP} := (\mathbb{G}, [\mathbf{A}_1]_1, \ldots, [\mathbf{A}_n]_1, [\mathbf{W}_1\mathbf{A}_1]_1, \ldots, [\mathbf{W}_n\mathbf{A}_n]_1),\ \mathsf{miMSK} := (\mathbf{W}_1, \ldots, \mathbf{W}_n, \mathbf{u}_1, \ldots, \mathbf{u}_n).\end{aligned}$$

$\mathsf{miEnc}(\mathsf{miMSK}, i, \mathbf{x}_i)$**:** It outputs miCT_i as follows:

$$\mathbf{s} \leftarrow \mathbb{Z}_p^k,\ \mathsf{miCT}_i := [\mathbf{c}_i]_1 = ([\mathbf{A}_i\mathbf{s}]_1, [\mathbf{W}_i\mathbf{A}_i\mathbf{s} + \mathbf{u}_i + \mathbf{x}_i]_1).$$

$\mathsf{miKeyGen}(\mathsf{miMSK}, \mathbf{y}_1, \ldots, \mathbf{y}_n)$**:** It outputs miSK as follows:

$$\mathsf{miSK}_0 := -\sum_{i\in[n]}\langle \mathbf{y}_i, \mathbf{u}_i\rangle,\ \mathsf{miSK}_i := (-\mathbf{y}_i^\top\mathbf{W}_i, \mathbf{y}_i),\ \mathsf{miSK} := (\mathsf{miSK}_0, \{\mathsf{miSK}_i\}_{i\in[n]}).$$

$\mathsf{miDec}(\mathsf{miCT}_1, \ldots, \mathsf{miCT}_n, \mathsf{miSK})$**:** It computes d where $[d]_1 = [\sum_{i\in[n]}\langle \mathbf{c}_i, \mathsf{miSK}_i\rangle + \mathsf{miSK}_0]_1$.

6.3 Security Analysis of Our Full MQFE Scheme

For security, we have the following theorem.

Theorem 6.1. *If* pFE *is partially function-hiding,* iFE *and* gFE *are function-hiding, and* $\mathcal{G}_{\mathsf{BG}}$ *outputs bilinear groups where the* $\mathcal{D}_k$*-MDDH assumption holds with overwhelming probability, then* qFE *is message-hiding.*

Proof. We prove Theorem 6.1 via a series of hybrid games H_ι^η for $\iota \in [n], \eta \in [q_{\mathsf{CT}}]$. We show that $\mathsf{G}_0 \approx_c \mathsf{H}_1^1 \approx_c \cdots \approx_c \mathsf{H}_1^{q_{\mathsf{CT}}} \approx_c \mathsf{H}_2^1 \approx_c \cdots \approx_c \mathsf{H}_n^{q_{\mathsf{CT}}} \approx_c \mathsf{G}_1$, where G_β for $\beta \in \{0, 1\}$ is the original security game. Each (hybrid) game is defined as described in Fig 20, where $\widetilde{\mathsf{qEnc}}_\iota^\eta$, and $\widetilde{\mathsf{qKeyGen}}$ work as follows. In what follows, we use a bijective query location function $\mathsf{ql} : [n] \times [q_{\mathsf{CT}}] \to [nq_{\mathsf{CT}}]$, defined as $\mathsf{ql}(x, y) := (x - 1)q_{\mathsf{CT}} + y$.

$\widetilde{\mathsf{qEnc}}^{\eta}_{\iota}(\mathsf{qMSK}, i, j, \{\mathbf{x}^{\nu,0}_{\mu}, \mathbf{x}^{\nu,1}_{\mu}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It samples vectors as follows:

$$\begin{aligned}
&\mathbf{S} \leftarrow \mathbb{Z}_p^{k\times k},\ \widetilde{\mathbf{s}}, \mathbf{r}, \mathbf{t} \leftarrow \mathbb{Z}_p^{k},\ L \leftarrow \mathbb{Z}_p\\
&\mathbf{l} := \mathbf{e}_{i/n} \otimes (1, L) \in \mathbb{Z}_p^{2n},\ \widetilde{\mathbf{l}} := \mathbf{e}_{i/n} \otimes (L, -1) \in \mathbb{Z}_p^{2n}\\
&\mathbf{b}_{\kappa,1} := (x^{j,0}_{i,\kappa}, \boxed{x^{j,1}_{i,\kappa}}) \in \mathbb{Z}_p^2,\ \mathbf{b}_{\kappa,2} := (\mathbf{w}^{\top}_{\mathsf{lo}(i,\kappa)}(\mathbf{I}_{mn} \otimes \mathbf{A}_i\mathbf{S}), \mathbf{u}_{\mathsf{lo}(i,\kappa)}) \in \mathbb{Z}_p^{(mn+1)k}\\
&\mathbf{b}_{\kappa,3} := \mathbf{t}^{\top}\mathbf{V}_{\mathsf{lo}(i,\kappa)} \in \mathbb{Z}_p^{k}\\
&\mathbf{b}_{\kappa,4} := \begin{cases} \boxed{x^{1,1}_{i,\kappa}\mathbf{x}^{1,1^{\top}}_{\iota} - x^{1,0}_{i,\kappa}\mathbf{x}^{1,0^{\top}}_{\iota}} & \text{if } i = \iota\\ \boxed{x^{j,1}_{i,\kappa}\mathbf{x}^{1,1^{\top}}_{\iota} - x^{j,0}_{i,\kappa}\mathbf{x}^{1,0^{\top}}_{\iota}} & \text{if } i \neq \iota \end{cases} \in \mathbb{Z}_p^{m}\\
&\mathbf{b}_{\kappa,5} := \mathbf{0} \in \mathbb{Z}_p^{m},\ \mathbf{b}_{\kappa,6} := \mathbf{0} \in \mathbb{Z}_p^{km},\ \mathbf{b}_{\kappa} := (\mathbf{b}_{\kappa,1}, \dots, \mathbf{b}_{\kappa,6})\\
&\widetilde{\mathbf{b}}_{\kappa,1} := \begin{cases} \boxed{(0, x^{j,1}_{i,\kappa})} & \text{if } \mathsf{ql}(i,j) \le \mathsf{ql}(\iota,\eta)\\ (x^{j,0}_{i,\kappa}, 0) & \text{if } \mathsf{ql}(i,j) > \mathsf{ql}(\iota,\eta) \end{cases} \in \mathbb{Z}_p^{2},\\
&\widetilde{\mathbf{b}}_{\kappa,2} := (\mathbf{e}_{\mathsf{lo}(i,\kappa)/mn} \otimes \widetilde{\mathbf{s}}, \mathbf{r}^{\top}\widetilde{\mathbf{U}}_{\mathsf{lo}(i,\kappa)}) \in \mathbb{Z}_p^{(mn+1)k}\\
&\widetilde{\mathbf{b}}_{\kappa,3} := \widetilde{\mathbf{v}}^{\top}_{\mathsf{lo}(i,\kappa)} \in \mathbb{Z}_p^{k},\ \widetilde{\mathbf{b}}_{\kappa,4} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j \le \eta\\ \boxed{\mathbf{e}_{\kappa/m}} & \text{if } i = \iota \wedge j > \eta \in \mathbb{Z}_p^{m}\\ \mathbf{0} & \text{if } i \neq \iota \end{cases}\\
&\widetilde{\mathbf{b}}_{\kappa,5} := \mathbf{0} \in \mathbb{Z}_p^{m},\ \widetilde{\mathbf{b}}_{\kappa,6} := \mathbf{0} \in \mathbb{Z}_p^{km},\ \widetilde{\mathbf{b}}_{\kappa} := (\widetilde{\mathbf{b}}_{\kappa,1}, \dots, \widetilde{\mathbf{b}}_{\kappa,6})\\
&\mathbf{d}_{\tau} := (\mathbf{a}^{\top}_{i,\tau}\mathbf{S}, 0) \in \mathbb{Z}_p^{k+1},\ \widetilde{\mathbf{d}} := (\widetilde{\mathbf{s}}, 0) \in \mathbb{Z}_p^{k+1}\\
&\mathbf{f}_1 := (\mathbf{r}, \mathbf{t}) \in \mathbb{Z}_p^{2k}\\
&\mathbf{f}_{2,\theta} := \begin{cases} \mathbf{0} & \text{if } \theta > \iota\\ \boxed{(\mathbf{x}^{1,1}_{i} \otimes \mathbf{x}^{1,1}_{\theta} - \mathbf{x}^{1,0}_{i} \otimes \mathbf{x}^{1,0}_{\theta})^{\top}} & \text{else if } \theta = i \vee \mathsf{ql}(i,j) \le \mathsf{ql}(\iota,\eta)\\ \boxed{(\mathbf{x}^{j,1}_{i} \otimes \mathbf{x}^{1,1}_{\theta} - \mathbf{x}^{j,0}_{i} \otimes \mathbf{x}^{1,0}_{\theta})^{\top}} & \text{else} \end{cases} \in \mathbb{Z}_p^{m^2}\\
&\mathbf{f} := (\mathbf{f}_1, \mathbf{f}_{2,1}, \dots, \mathbf{f}_{2,n}),\ h := 0.
\end{aligned}$$

Then, it computes qCT^j_i in the same way as Eq. (6.1).

$\widetilde{\mathsf{qKeyGen}}(\mathsf{qMSK}, \mathbf{c})$**:** Let $\mathbf{c}_{\mathsf{ls}(\theta),\mathsf{lo}(i,\kappa)} := (c_{\mathsf{lo}(\theta,1),\mathsf{lo}(i,\kappa)}, \dots, c_{\mathsf{lo}(\theta,m),\mathsf{lo}(i,\kappa)})$ and $\mathbf{c}_{\mathsf{ls}(\theta),\mathsf{ls}(i)} := (\mathbf{c}_{\mathsf{ls}(\theta),\mathsf{lo}(i,1)}, \dots, \mathbf{c}_{\mathsf{ls}(\theta),\mathsf{lo}(i,m)})$. It outputs qSK as follows:

$$\begin{aligned}
&\widetilde{\mathbf{f}}_{i,1} := \left(\sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in[mn]}} c_{\mu,\nu}\widetilde{\mathbf{U}}_{\mu}\mathbf{u}_{\nu}, \sum_{\substack{\mu\in[mn]\\ \nu\in\mathsf{ls}(i)}} c_{\mu,\nu}\mathbf{V}_{\nu}\widetilde{\mathbf{v}}_{\mu} \right) \in \mathbb{Z}_p^{2k}\\
&\widetilde{\mathbf{f}}_{i,2,\theta} := \boxed{\mathbf{c}_{\mathsf{ls}(\theta),\mathsf{ls}(i)}} \in \mathbb{Z}_p^{m^2}\\
&\widetilde{\mathbf{f}}_i := (\widetilde{\mathbf{f}}_{i,1}, \widetilde{\mathbf{f}}_{i,2,1}, \dots, \widetilde{\mathbf{f}}_{i,2,n}),\ \widetilde{h}_i := 0\\
&\mathsf{gSK} \leftarrow \mathsf{gKeyGen}(\mathsf{gMSK}, \{[\widetilde{\mathbf{f}}_i]_2, [\widetilde{h}_i]_1\}_{i\in[n]})\\
&\boldsymbol{\sigma}_{i,\theta} := \sum_{\substack{\mu\in\mathsf{ls}(i),\\ \nu\in\mathsf{ls}(\theta)}} c_{\mu,\nu}\mathbf{w}_{\mu,\nu} \in \mathbb{Z}_p^{k+1}\\
&\mathsf{qSK} := (\mathbf{c}, \mathsf{gSK}, \{\boldsymbol{\sigma}_{i,\theta}\}_{i,\theta\in[n]}).
\end{aligned}$$

Note that the framed parts are changed from $\mathsf{qSetup}, \mathsf{qEnc}$, or $\mathsf{qKeyGen}$. Next, we prove the indistinguishability of each pair of hybrid games. Let $\mathsf{P}(\mathcal{A}, \mathsf{G})$ be the probability that $\mathcal{A}$ outputs 1 in a security game G with the security parameter being λ, i.e., $\mathsf{P}(\mathcal{A}, \mathsf{G}_\beta) = \mathsf{P}^{\mathsf{qFE},\beta}_{\mathcal{A},\mathsf{mh}}(\lambda)$.

Lemma 6.1. *Let $\mathsf{H}^{q_{\mathsf{CT}}}_0 = \mathsf{G}_0$. For all PPT adversaries $\mathcal{A}$ and $\iota \in [n]$, there exist PPT adversaries $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that*

$$\begin{aligned}|\mathsf{P}(\mathcal{A}, \mathsf{H}^{q_{\mathsf{CT}}}_{\iota-1}) - \mathsf{P}(\mathcal{A}, \mathsf{H}^1_\iota)| \leq& 2\mathsf{Adv}^{\mathsf{pFE}}_{\mathcal{B}_1,\mathsf{pfh}}(\lambda) + 2\mathsf{Adv}^{\mathsf{gFE}}_{\mathcal{B}_2,\mathsf{fh}}(\lambda)\\ &+ 2(m + m^2 n)\mathsf{Adv}^{\mathcal{D}_k\text{-}\mathsf{MDDH}}_{\mathcal{B}_3}(\lambda) + 2^{-\Omega(\lambda)}.\end{aligned}$$

Lemma 6.2. *For all PPT adversaries $\mathcal{A}, \iota \in [n]$, and $\eta \in [2, q_{\mathsf{CT}}]$, there exists a PPT adversary $\mathcal{B}_1, \ldots, \mathcal{B}_5$ such that*

$$\begin{aligned}|\mathsf{P}(\mathcal{A}, \mathsf{H}^{\eta-1}_\iota) - \mathsf{P}(\mathcal{A}, \mathsf{H}^{\eta}_\iota)| \leq& 2\mathsf{Adv}^{\mathsf{pFE}}_{\mathcal{B}_1,\mathsf{pfh}}(\lambda) + 2\mathsf{Adv}^{\mathsf{iFE}}_{\mathcal{B}_2,\mathsf{fh}}(\lambda) + 2\mathsf{Adv}^{\mathsf{gFE}}_{\mathcal{B}_3,\mathsf{fh}}(\lambda)\\ &+ \mathsf{Adv}^{\mathsf{miFE}}_{\mathcal{B}_4,\mathsf{mh}}(\lambda) + 2(mk + 2)\mathsf{Adv}^{\mathcal{D}_k\text{-}\mathsf{MDDH}}_{\mathcal{B}_5}(\lambda) + 2^{-\Omega(\lambda)}\end{aligned}$$

Lemma 6.3. *For all PPT adversaries $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}_1, \mathcal{B}_2$ such that*

$$|\mathsf{P}(\mathcal{A}, \mathsf{H}^{q_{\mathsf{CT}}}_n) - \mathsf{P}(\mathcal{A}, \mathsf{G}_1)| \leq \mathsf{Adv}^{\mathsf{pFE}}_{\mathcal{B}_1,\mathsf{pfh}}(\lambda) + \mathsf{Adv}^{\mathsf{gFE}}_{\mathcal{B}_2,\mathsf{fh}}(\lambda).$$

Thanks to Lemmata 6.1 to 6.3, Theorem 6.1 holds. We present the proofs of these lemmata in Sec. 6.4. □

6.4 Proofs of Lemmata 6.1 to 6.3

Proof of Lemma 6.1. We introduce more hybrid games $\widehat{\mathsf{H}}_{\iota,1}, \ldots, \widehat{\mathsf{H}}_{\iota,5}$ to prove Lemma 6.1. We prove that $\mathsf{H}^{q_{\mathsf{CT}}}_{\iota-1} \approx_c \widehat{\mathsf{H}}_{\iota,1} \approx_c \cdots \approx_c \widehat{\mathsf{H}}_{\iota,5} \approx_c \mathsf{H}^1_\iota$. $\widehat{\mathsf{H}}_{\iota,\zeta}$ for $\zeta \in \{1, \ldots, 5\}$ is defined the same as $\mathsf{H}^{q_{\mathsf{CT}}}_{\iota-1}$ except that qSetup, $\widetilde{\mathsf{qEnc}}^{q_{\mathsf{CT}}}_{\iota-1}$, and $\widetilde{\mathsf{qKeyGen}}$ are replaced by $\widehat{\mathsf{qSetup}}$, $\widehat{\mathsf{qEnc}}_{\iota,\zeta}$, and $\widehat{\mathsf{qKeyGen}}$, respectively. For reference, we first describe $\widetilde{\mathsf{qEnc}}^{q_{\mathsf{CT}}}_{\iota-1}$ and $\widetilde{\mathsf{qEnc}}^1_\iota$.

$\widetilde{\mathsf{qEnc}}^{q_{\mathsf{CT}}}_{\iota-1}(\mathsf{qMSK}, i, j, \{\mathbf{x}^{\nu,0}_\mu, \mathbf{x}^{\nu,1}_\mu\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It samples vectors as follows:

$$\begin{aligned}
&\mathbf{S} \leftarrow \mathbb{Z}_p^{k\times k},\ \widetilde{\mathbf{s}}, \mathbf{r}, \mathbf{t} \leftarrow \mathbb{Z}_p^k,\ L \leftarrow \mathbb{Z}_p\\
&\mathbf{l} := \mathbf{e}_{i/n} \otimes (1, L) \in \mathbb{Z}_p^{2n},\ \widetilde{\mathbf{l}} := \mathbf{e}_{i/n} \otimes (L, -1) \in \mathbb{Z}_p^{2n}\\
&\mathbf{b}_{\kappa,1} := (x^{j,0}_{i,\kappa}, x^{j,1}_{i,\kappa}) \in \mathbb{Z}_p^2,\ \mathbf{b}_{\kappa,2} := (\mathbf{w}^\top_{\mathsf{lo}(i,\kappa)}(\mathbf{I}_{mn} \otimes \mathbf{A}_i\mathbf{S}), \mathbf{u}_{\mathsf{lo}(i,\kappa)}) \in \mathbb{Z}_p^{(mn+1)k}\\
&\mathbf{b}_{\kappa,3} := \mathbf{t}^\top \mathbf{V}_{\mathsf{lo}(i,\kappa)} \in \mathbb{Z}_p^k\\
&\mathbf{b}_{\kappa,4} := \begin{cases} x^{1,1}_{i,\kappa}\mathbf{x}^{1,1\top}_{\iota-1} - x^{1,0}_{i,\kappa}\mathbf{x}^{1,0\top}_{\iota-1} & \text{if } i = \iota - 1\\ x^{j,1}_{i,\kappa}\mathbf{x}^{1,1\top}_{\iota-1} - x^{j,0}_{i,\kappa}\mathbf{x}^{1,0\top}_{\iota-1} & \text{if } i \neq \iota - 1\end{cases} \in \mathbb{Z}_p^m\\
&\mathbf{b}_{\kappa,5} := \mathbf{0} \in \mathbb{Z}_p^m,\ \mathbf{b}_{\kappa,6} := \mathbf{0} \in \mathbb{Z}_p^{km},\ \mathbf{b}_\kappa := (\mathbf{b}_{\kappa,1}, \ldots, \mathbf{b}_{\kappa,6})\\
&\widetilde{\mathbf{b}}_{\kappa,1} := \begin{cases} (0, x^{j,1}_{i,\kappa}) & \text{if } \mathsf{ql}(i,j) \leq \mathsf{ql}(\iota-1, q_{\mathsf{CT}})\\ (x^{j,0}_{i,\kappa}, 0) & \text{if } \mathsf{ql}(i,j) > \mathsf{ql}(\iota-1, q_{\mathsf{CT}})\end{cases} \in \mathbb{Z}_p^2,\\
&\widetilde{\mathbf{b}}_{\kappa,2} := (\mathbf{e}_{\mathsf{lo}(i,\kappa)/mn} \otimes \widetilde{\mathbf{s}}, \mathbf{r}^\top \widetilde{\mathbf{U}}_{\mathsf{lo}(i,\kappa)}) \in \mathbb{Z}_p^{(mn+1)k}\\
&\widetilde{\mathbf{b}}_{\kappa,3} := \widetilde{\mathbf{v}}^\top_{\mathsf{lo}(i,\kappa)} \in \mathbb{Z}_p^k,\ \widetilde{\mathbf{b}}_{\kappa,4} = \widetilde{\mathbf{b}}_{\kappa,5} := \mathbf{0} \in \mathbb{Z}_p^m,\ \widetilde{\mathbf{b}}_{\kappa,6} := \mathbf{0} \in \mathbb{Z}_p^{km}\\
&\widetilde{\mathbf{b}}_\kappa := (\widetilde{\mathbf{b}}_{\kappa,1}, \ldots, \widetilde{\mathbf{b}}_{\kappa,6})\\
&\mathbf{d}_\tau := (\mathbf{a}^\top_{i,\tau}\widehat{\mathbf{S}}, 0) \in \mathbb{Z}_p^{k+1},\ \widetilde{\mathbf{d}} := (\widetilde{\mathbf{s}}, 0) \in \mathbb{Z}_p^{k+1}
\end{aligned}$$

$$\mathbf{f}_1 := (\mathbf{r}, \mathbf{t}) \in \mathbb{Z}_p^{2k}$$

$$\mathbf{f}_{2,\theta} := \begin{cases} \mathbf{0} & \text{if } \theta > \iota - 1 \\ (\mathbf{x}_i^{1,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{1,0} \otimes \mathbf{x}_\theta^{1,0})^\top & \text{else if } i \leq \iota \in \mathbb{Z}_p^{m^2} \\ (\mathbf{x}_i^{j,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{j,0} \otimes \mathbf{x}_\theta^{1,0})^\top & \text{else} \end{cases}$$

$$\mathbf{f} := (\mathbf{f}_1, \mathbf{f}_{2,1}, \ldots, \mathbf{f}_{2,n}),\ h := 0.$$

Then, it computes qCT_i^j in the same way as Eq. (6.1).

$\widetilde{\mathsf{qEnc}}_\iota^1(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu \in [n], \nu \in [q_{\mathsf{CT}}]})$**:** It is the same as $\widetilde{\mathsf{qEnc}}_{\iota-1}^{q_{\mathsf{CT}}}$ except the way of defining the following vectors:

$$\mathbf{b}_{\kappa,4} := \begin{cases} \boxed{x_{i,\kappa}^{1,1} \mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{1,0} \mathbf{x}_\iota^{1,0^\top}} & \text{if } i = \iota \\ \boxed{x_{i,\kappa}^{j,1} \mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{j,0} \mathbf{x}_\iota^{1,0^\top}} & \text{if } i \neq \iota \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,1} := \begin{cases} (0, x_{i,\kappa}^{j,1}) & \text{if } \mathsf{ql}(i,j) \leq \mathsf{ql}(\iota - 1, q_{\mathsf{CT}}) \\ \boxed{(0, x_{i,\kappa}^{j,1})} & \text{if } \mathsf{ql}(i,j) = \mathsf{ql}(\iota, 1) \\ (x_{i,\kappa}^{j,0}, 0) & \text{if } \mathsf{ql}(i,j) > \mathsf{ql}(\iota, 1) \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,4} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j = 1 \\ \boxed{\mathbf{e}_{\kappa/m}} & \text{if } i = \iota \wedge j > 1 \\ \mathbf{0} & \text{if } i \neq \iota \end{cases}$$

$$\mathbf{f}_{2,\theta} := \begin{cases} \mathbf{0} & \text{if } \theta > \iota \\ \boxed{(\mathbf{x}_i^{1,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{1,0} \otimes \mathbf{x}_\theta^{1,0})^\top} & \text{else if } \theta = \iota \wedge i \leq \iota \\ \boxed{(\mathbf{x}_i^{j,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{j,0} \otimes \mathbf{x}_\theta^{1,0})^\top} & \text{else if } \theta = \iota \wedge i > \iota\ \cdot \\ (\mathbf{x}_i^{1,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{1,0} \otimes \mathbf{x}_\theta^{1,0})^\top & \text{else if } i \leq \iota \\ (\mathbf{x}_i^{j,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{j,0} \otimes \mathbf{x}_\theta^{1,0})^\top & \text{else} \end{cases}$$

Note that the framed parts are changed from $\widetilde{\mathsf{qEnc}}_{\iota-1}^{q_{\mathsf{CT}}}$. Next, we describe $\widehat{\mathsf{qSetup}}$, $\widehat{\mathsf{qEnc}}_{\iota,\zeta}$, and $\widehat{\mathsf{qKeyGen}}$.

$\widehat{\mathsf{qSetup}}(1^\lambda)$**:** It works the same as qSetup except that qMSK contains additional elements as follows:

$$\boxed{\widehat{\mathbf{V}}_1, \ldots, \widehat{\mathbf{V}}_{mn} \leftarrow \mathbb{Z}_p^{k \times m}}$$

$$\mathsf{qMSK} := \begin{pmatrix} \mathbf{A}_1, \ldots, \mathbf{A}_n, \{\mathbf{w}_{i,j}\}_{i,j \in [mn]}, \{\widetilde{\mathbf{U}}_i, \mathbf{u}_i, \mathbf{V}_i, \widetilde{\mathbf{v}}_i, \boxed{\widehat{\mathbf{V}}_i}\}_{i \in [mn]} \\ \mathsf{pMSK}, \mathsf{iMSK}, \mathsf{gMSK} \end{pmatrix}.$$

$\widehat{\mathsf{qEnc}}_{\iota,1}(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu \in [n], \nu \in [q_{\mathsf{CT}}]})$**:** Let $\widetilde{\mathbf{V}}_{\mathsf{ls}(\iota)} = (\widetilde{\mathbf{v}}_{\mathsf{lo}(\iota,1)} || \cdots || \widetilde{\mathbf{v}}_{\mathsf{lo}(\iota,m)})$. It is the same as $\widetilde{\mathsf{qEnc}}_{\iota-1}^{q_{\mathsf{CT}}}$ except the way of defining the following vectors:

$$\mathbf{b}_{\kappa,4} := \boxed{\mathbf{t}^\top \mathbf{V}_{\mathsf{lo}(i,\kappa)} \widetilde{\mathbf{V}}_{\mathsf{ls}(\iota)}},\ \mathbf{b}_{\kappa,5} := \boxed{\mathbf{b}_{\kappa,4} + x_{i,\kappa}^{j,0} \mathbf{x}_\iota^{1,0^\top}}$$

$$\widetilde{\mathbf{b}}_{\kappa,1} := \begin{cases} (0, x_{i,\kappa}^{j,1}) & \text{if } \mathsf{ql}(i,j) \leq \mathsf{ql}(\iota - 1, q_{\mathsf{CT}}) \\ \boxed{(0, 0)} & \text{if } \mathsf{ql}(i,j) = \mathsf{ql}(\iota, 1) \\ (x_{i,\kappa}^{j,0}, 0) & \text{if } \mathsf{ql}(i,j) > \mathsf{ql}(\iota, 1) \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,3} := \begin{cases} \boxed{\mathbf{0}} & \text{if } i = \iota \\ \widetilde{\mathbf{v}}_{\mathsf{lo}(i,\kappa)}^\top & \text{if } i \neq \iota \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,4} := \begin{cases} \mathbf{0} & \text{if } i = \iota \vee j = 1 \\ \boxed{\mathbf{e}_{\kappa/m}} & \text{if } i = \iota \wedge j > 1 \\ \mathbf{0} & \text{if } i \neq \iota \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,5} := \begin{cases} \boxed{\mathbf{e}_{\kappa/m}} & \text{if } \mathsf{ql}(i,j) = \mathsf{ql}(\iota,1) \\ \mathbf{0} & \text{if } \mathsf{ql}(i,j) \neq \mathsf{ql}(\iota,1) \end{cases}$$

$$\mathbf{f}_{2,\theta} := \begin{cases} \mathbf{0} & \text{if } \theta > \iota \\ \boxed{(\mathbf{b}_{1,4}, \ldots, \mathbf{b}_{m,4})} & \text{else if } \theta = \iota \\ (\mathbf{x}_i^{1,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{1,0} \otimes \mathbf{x}_\theta^{1,0})^\top & \text{else if } \theta = i \vee \mathsf{ql}(i,j) \leq \mathsf{ql}(\iota - 1, q_{\mathsf{CT}}) \\ (\mathbf{x}_i^{j,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{j,0} \otimes \mathbf{x}_\theta^{1,0})^\top & \text{else} \end{cases}$$

$\widehat{\mathsf{qEnc}_{\iota,2}}(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It is the same as $\widehat{\mathsf{qEnc}_{\iota,1}}$ except the way of defining the following vectors:

$$\mathbf{b}_{\kappa,4} := \boxed{\mathbf{t}^\top \widehat{\mathbf{V}}_{\mathsf{lo}(i,\kappa)}}.$$

$\widehat{\mathsf{qEnc}_{\iota,3}}(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It is the same as $\widehat{\mathsf{qEnc}_{\iota,2}}$ except the way of defining the following vectors:

$$\boxed{\ddot{\mathbf{v}}_\kappa \leftarrow \mathbb{Z}_p^m},\ \mathbf{b}_{\kappa,4} := \boxed{\ddot{\mathbf{v}}_\kappa^\top}.$$

$\widehat{\mathsf{qEnc}_{\iota,4}}(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It is the same as $\widehat{\mathsf{qEnc}_{\iota,3}}$ except the way of defining the following vectors:

$$\ddot{\mathbf{v}}_\kappa \leftarrow \mathbb{Z}_p^m,\ \mathbf{b}_{\kappa,4} := \begin{cases} \ddot{\mathbf{v}}_\kappa^\top \boxed{+x_{i,\kappa}^{1,1}\mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{1,0}\mathbf{x}_\iota^{1,0^\top}} & \text{if } i = \iota \\ \ddot{\mathbf{v}}_\kappa^\top \boxed{+x_{i,\kappa}^{j,1}\mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{j,0}\mathbf{x}_\iota^{1,0^\top}} & \text{if } i \neq \iota \end{cases}.$$

$\widehat{\mathsf{qEnc}_{\iota,5}}(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It is the same as $\widehat{\mathsf{qEnc}_{\iota,4}}$ except the way of defining the following vectors:

$$\mathbf{b}_{\kappa,4} := \begin{cases} \boxed{\mathbf{t}^\top \mathbf{V}_{\mathsf{lo}(i,\kappa)} \widetilde{\mathbf{V}}_{\mathsf{ls}(\iota)}} + x_{i,\kappa}^{1,1}\mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{1,0}\mathbf{x}_\iota^{1,0^\top} & \text{if } i = \iota \\ \boxed{\mathbf{t}^\top \mathbf{V}_{\mathsf{lo}(i,\kappa)} \widetilde{\mathbf{V}}_{\mathsf{ls}(\iota)}} + x_{i,\kappa}^{j,1}\mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{j,0}\mathbf{x}_\iota^{1,0^\top} & \text{if } i \neq \iota \end{cases}.$$

$\widehat{\mathsf{qKeyGen}}(\mathsf{qMSK}, \mathbf{c})$**:** It outputs qSK as follows:

$$\widetilde{\mathbf{f}}_{i,1} := \left(\sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in[mn]}} c_{\mu,\nu} \widetilde{\mathbf{U}}_\mu \mathbf{u}_\nu, \boxed{\sum_{\substack{\mu\in[mn]\setminus\mathsf{ls}(\iota)\\ \nu\in\mathsf{ls}(i)}} c_{\mu,\nu} \mathbf{V}_\nu \widetilde{\mathbf{v}}_\mu} \right)$$

$$\widetilde{\mathbf{f}}_{i,2,\theta} := \mathbf{c}_{\mathsf{ls}(\theta),\mathsf{ls}(i)}$$

$$\widetilde{\mathbf{f}}_i := (\widetilde{\mathbf{f}}_{i,1}, \widetilde{\mathbf{f}}_{i,2,1}, \ldots, \widetilde{\mathbf{f}}_{i,2,n}),\ \widetilde{h}_i := 0$$

$$\mathsf{gSK} \leftarrow \mathsf{gKeyGen}(\mathsf{gMSK}, \{[\widetilde{\mathbf{f}}_i]_2, [\widetilde{h}_i]_1\}_{i\in[n]})$$

$$\boldsymbol{\sigma}_{i,\theta} := \sum_{\substack{\mu\in\mathsf{ls}(i),\\ \nu\in\mathsf{ls}(\theta)}} c_{\mu,\nu} \mathbf{w}_{\mu,\nu}$$

$$\mathsf{qSK} := (\mathbf{c}, \mathsf{gSK}, \{\boldsymbol{\sigma}_{i,\theta}\}_{i,\theta\in[n]}).$$

Thanks to Lemma 6.4 to Lemma 6.8, Lemma 6.1 holds. □

Lemma 6.4. *For all PPT adversaries $\mathcal{A}$ and $\iota \in [n]$, there exist PPT adversaries $\mathcal{B}_1, \mathcal{B}_2$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_{\iota-1}^{q_{\mathsf{CT}}}) - \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,1})| \leq \mathsf{Adv}_{\mathcal{B}_1,\mathsf{pfh}}^{\mathsf{pFE}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_2,\mathsf{fh}}^{\mathsf{gFE}}(\lambda) + 2^{-\Omega(\lambda)}$.

Proof. Since L is uniformly chosen from the exponentially large space in encryption algorithms, i.e., $\mathbb{Z}_p$, collisions do not occur in $\{L_i^j\}_{i\in[n],j\in[q_{\mathsf{CT}}]}$ with overwhelming probability. Therefore, $\langle \mathbf{l}_i^j, \widetilde{\mathbf{l}}_I^J\rangle = 0$ if $i \neq I$ or $j = J$, and $\langle \mathbf{l}_i^j, \widetilde{\mathbf{l}}_I^J\rangle \neq 0$ otherwise.

For all $(i, j, \kappa), (I, J, K) \in [n] \times [q_{\mathsf{CT}}] \times [m]$, observe that $\langle \mathbf{b}_{i,\kappa}^j, \widetilde{\mathbf{b}}_{I,K}^J\rangle$ in $\mathsf{H}_{\iota-1}^{q_{\mathsf{CT}}}$ are equal to that in $\widehat{\mathsf{H}}_{\iota,1}$ *if* $i \neq I$ or $j = J$. Thus, due to the partially function-hiding property of pFE, this implies that $\{\mathsf{pCT}_{i,\mathsf{lo}(i,\kappa)}^j, \mathsf{pSK}_{i,\mathsf{lo}(i,\kappa)}^j\}$ generated in $\mathsf{H}_{\iota-1}^{q_{\mathsf{CT}}}$ and those generated in $\widehat{\mathsf{H}}_{\iota,1}$ are computationally indistinguishable.

Similarly, we can confirm that for all $(i, j, \ell) \in [n] \times [q_{\mathsf{CT}}] \times [q_{\mathsf{SK}}]$, we have $\langle \mathbf{f}_i^j, \widetilde{\mathbf{f}}_i^\ell\rangle + \langle h_i^j, \widehat{h}_i^\ell\rangle$ in $\mathsf{H}_{\iota-1}^{q_{\mathsf{CT}}}$ are equal to that in $\widehat{\mathsf{H}}_{\iota,1}$. Thus, thanks to the function-hiding property of gFE, $\{\mathsf{gCT}_i^j, \mathsf{gSK}^\ell\}$ generated in $\mathsf{H}_{\iota-1}^{q_{\mathsf{CT}}}$ and those generated in $\widehat{\mathsf{H}}_{\iota,1}$ are computationally indistinguishable. Hence, $\mathcal{A}$'s views in $\mathsf{H}_{\iota-1}^{q_{\mathsf{CT}}}$ and $\widehat{\mathsf{H}}_{\iota,1}$ are computationally indistinguishable. □

Lemma 6.5. *For all PPT adversaries $\mathcal{A}$ and $\iota \in [n]$, there exists a PPT adversary $\mathcal{B}$ against m-fold $\mathcal{U}_{mnk,k}$-MDDH such that* $|\mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,1}) - \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,2})| \leq \mathsf{Adv}_{\mathcal{B}}^{m\text{-}\mathcal{U}_{mnk,k}\text{-}\mathsf{MDDH}}(\lambda)$.

Proof. $\mathcal{B}$ works as follows.

1. $\mathcal{B}$ takes an instance of the m-fold $\mathcal{U}_{mnk,k}$-MDDH, $(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{K}_\beta]_1)$. Recall that they are distributed as $\mathbf{M} \leftarrow \mathbb{Z}_p^{mnk\times k}$, $\mathbf{K}_0 = \mathbf{MZ} \in \mathbb{Z}_p^{mnk\times m}$ where $\mathbf{Z} \leftarrow \mathbb{Z}_p^{k\times m}$, and $\mathbf{K}_1 \leftarrow \mathbb{Z}_p^{mnk\times m}$.
2. $\mathcal{B}$ computes $\mathsf{qPP}, \mathsf{qMSK}$ in the same way as $\widehat{\mathsf{qSetup}}$ except that $\mathcal{B}$ (implicitly) defines that $\mathbf{V}_i := \mathbf{M}_i, \widehat{\mathbf{V}}_i := \mathbf{K}_{1,i}$ for $i \in [mn]$ and $\widetilde{\mathbf{V}}_{\mathsf{ls}(\iota)} := \mathbf{Z}$ for $i \in [m]$, where $\mathbf{M}_i$ and $\mathbf{K}_{\beta,i}$ are the matrices consisting of the $(i-1)k+1$ to ik-th rows of $\mathbf{M}$ and $\mathbf{K}_\beta$, respectively.
3. $\mathcal{B}$ computes qCT_i^j for $i \in [n], j \in [q_{\mathsf{CT}}]$ in the same way as $\widehat{\mathsf{qEnc}_{\iota,1}}$ except that $\mathcal{B}$ defines that $\mathbf{b}_{i,\kappa,4}^j := \mathbf{t}_i^{j\top}\mathbf{K}_{\beta,\mathsf{lo}(i,\kappa)}$ and gives $\mathsf{qPP}, \{\mathsf{qCT}_i^j\}$ to $\mathcal{A}$.
4. $\mathcal{B}$ simulates $\widehat{\mathsf{qKeyGen}}$ using qMSK, which is possible without $[\widetilde{\mathbf{V}}_{\mathsf{ls}(\iota)}]_2$.
5. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

Observe that $\mathbf{b}_{i,\kappa,4}^j = \mathbf{t}_i^{j\top}\mathbf{V}_{\mathsf{lo}(i,\kappa)}\widetilde{\mathbf{V}}_{\mathsf{ls}(\iota)}$ if $\beta = 0$ and $\mathbf{b}_{i,\kappa,4}^j = \mathbf{t}_i^{j\top}\widehat{\mathbf{V}}_{\mathsf{lo}(i,\kappa)}$ if $\beta = 1$. This concludes the proof. Note that m-fold $\mathcal{U}_{mnk,k}$-MDDH is reduced to $\mathcal{D}_k$-MDDH with the security loss of m. □

Lemma 6.6. *For all PPT adversaries $\mathcal{A}$ and $\iota \in [n]$, there exists a PPT adversary $\mathcal{B}$ against m^2n-fold $\mathcal{U}_{nq_{\mathsf{CT}},k}$-MDDH such that* $|\mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,2}) - \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,3})| \leq \mathsf{Adv}_{\mathcal{B}}^{m^2n\text{-}\mathcal{U}_{nq_{\mathsf{CT}},k}\text{-}\mathsf{MDDH}}(\lambda)$.

Proof. $\mathcal{B}$ works as follows.

1. $\mathcal{B}$ takes an instance of the m^2n-fold $\mathcal{U}_{nq_{\mathsf{CT}},k}$-MDDH, $(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{K}_\beta]_1)$. Recall that they are distributed as $\mathbf{M} \leftarrow \mathbb{Z}_p^{nq_{\mathsf{CT}}\times k}$, $\mathbf{K}_0 = \mathbf{MZ} \in \mathbb{Z}_p^{nq_{\mathsf{CT}}\times m^2n}$ where $\mathbf{Z} \leftarrow \mathbb{Z}_p^{k\times m^2n}$, and $\mathbf{K}_1 \leftarrow \mathbb{Z}_p^{nq_{\mathsf{CT}}\times m^2n}$.
2. $\mathcal{B}$ computes $\mathsf{qPP}, \mathsf{qMSK} \leftarrow \widehat{\mathsf{qSetup}}$ except that $\mathcal{B}$ implicitly defines that $\widehat{\mathbf{V}}_i := \mathbf{Z}_i$ for $i \in [mn]$ where $\mathbf{Z}_i$ is the matrix consisting of the $(i-1)m+1$ to im-th columns of $\mathbf{Z}$.
3. $\mathcal{B}$ computes qCT_i^j for $i \in [n], j \in [q_{\mathsf{CT}}]$ in the same way as $\widehat{\mathsf{qEnc}_{\iota,2}}$ except that $\mathcal{B}$ defines that $\mathbf{b}_{i,\kappa,4}^j := \mathbf{k}_{\beta,\mathsf{ql}(i,j),\mathsf{lo}(i,\kappa)}$, $\mathbf{t}_i^j := \mathbf{m}_{\mathsf{ql}(i,j)}^\top$, and $\ddot{\mathbf{v}}_{i,\kappa}^j := \mathbf{k}_{1,\mathsf{ql}(i,j),\mathsf{lo}(i,\kappa)}^\top$ where $\mathbf{k}_{\beta,\mu,\nu} \in \mathbb{Z}_p^{1\times m}$ is the (μ, ν)-th block of $\mathbf{K}_\beta$ by dividing $\mathbf{K}_\beta$ into $nq_{\mathsf{CT}} \times mn$ blocks, and $\mathbf{m}_\mu$ is the μ-th row of $\mathbf{M}$. Then, $\mathcal{B}$ gives $\mathsf{qPP}, \{\mathsf{qCT}_i^j\}$ to $\mathcal{A}$.
4. $\mathcal{B}$ simulates $\widehat{\mathsf{qKeyGen}}$ using qMSK.
5. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

Observe that $\mathbf{b}^j_{i,\kappa,4} = \mathbf{t}^{j\top}_i \widehat{\mathbf{V}}_{\mathsf{lo}(i,\kappa)}$ if $\beta = 0$ and $\mathbf{b}^j_{i,\kappa,4} = \ddot{\mathbf{v}}^{j\top}_{i,\kappa}$ if $\beta = 1$. This concludes the proof. Note that m^2n-fold $\mathcal{U}_{nq_{\mathsf{CT}},k}$-MDDH is reduced to $\mathcal{D}_k$-MDDH with the security loss of m^2n. □

Lemma 6.7. *For all PPT adversaries* $\mathcal{A}$*. we have* $\mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,3}) = \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,4})$.

Proof. By implicitly defining that

$$\ddot{\mathbf{v}}^j_{i,\kappa} := \begin{cases} \ddot{\mathbf{v}}'^j_{i,\kappa} + x^{1,1}_{i,\kappa}\mathbf{x}^{1,1}_\iota - x^{1,0}_{i,\kappa}\mathbf{x}^{1,0}_\iota & \text{if } i = \iota \\ \ddot{\mathbf{v}}'^j_{i,\kappa} + x^{j,1}_{i,\kappa}\mathbf{x}^{1,1}_\iota - x^{j,0}_{i,\kappa}\mathbf{x}^{1,0}_\iota & \text{if } i \neq \iota \end{cases}$$

where $\ddot{\mathbf{v}}'^j_{i,\kappa} \leftarrow \mathbb{Z}^m_p$, we can see that $\mathcal{A}$'s views in both hybrids are identical. This is since $\ddot{\mathbf{v}}^j_{i,\kappa} \leftarrow \mathbb{Z}^m_p$ and $\ddot{\mathbf{v}}'^j_{i,\kappa} \leftarrow \mathbb{Z}^m_p$ are identically distributed. □

Lemma 6.8. *For all PPT adversaries* $\mathcal{A}$ *and* $\iota \in [n]$*, there exist PPT adversaries* $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ *such that* $|\mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,4}) - \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,5})| \leq \mathsf{Adv}^{\mathsf{pFE}}_{\mathcal{B}_1,\mathsf{pfh}}(\lambda) + \mathsf{Adv}^{\mathsf{gFE}}_{\mathcal{B}_2,\mathsf{fh}}(\lambda) + (m + m^2n)\mathsf{Adv}^{\mathcal{D}_k\text{-MDDH}}_{\mathcal{B}_3}(\lambda) + 2^{-\Omega(\lambda)}$.

Lemma 6.8 can be proven similarly to Lemmata 6.4 to 6.6. Note that here we use the fact that $\mathbf{c}_{\mathsf{ls}(\iota),\mathsf{ls}(i)} = \mathbf{0}$ if $i < \iota$ as defined in Def. 2.4, which implies

$$\langle \mathbf{c}_{\mathsf{ls}(\iota),\mathsf{ls}(i)}, \mathbf{x}^{1,1}_i \otimes \mathbf{x}^{1,1}_\iota - \mathbf{x}^{1,0}_i \otimes \mathbf{x}^{1,0}_\iota \rangle = \langle \mathbf{c}_{\mathsf{ls}(\iota),\mathsf{ls}(i)}, \mathbf{x}^{j,1}_i \otimes \mathbf{x}^{1,1}_\iota - \mathbf{x}^{j,0}_i \otimes \mathbf{x}^{1,0}_\iota \rangle$$

for all $(i, j) \in [n] \times [q_{\mathsf{CT}}]$ if $i < \iota$.

Proof of Lemma 6.2. We introduce more hybrid games $\widehat{\mathsf{H}}^\eta_{\iota,1}, \ldots, \widehat{\mathsf{H}}^\eta_{\iota,5}$ to prove Lemma 6.2. We prove that $\mathsf{H}^{\eta-1}_\iota \approx_c \widehat{\mathsf{H}}^\eta_{\iota,1} \approx_c \cdots \approx_c \widehat{\mathsf{H}}^\eta_{\iota,5} \approx_c \mathsf{H}^\eta_\iota$. $\widehat{\mathsf{H}}^\eta_{\iota,\zeta}$ for $\zeta \in \{1, \ldots, 5\}$ is defined the same as $\mathsf{H}^{\eta-1}_\iota$ except that $\widetilde{\mathsf{qSetup}}$, $\widetilde{\mathsf{qEnc}}^{\eta-1}_\iota$, and $\widetilde{\mathsf{qKeyGen}}$ are replaced by $\widehat{\mathsf{qSetup}}$, $\widehat{\mathsf{qEnc}}^\eta_{\iota,\zeta}$, and $\widehat{\mathsf{qKeyGen}}^\eta_{\iota,\zeta}$, respectively. They are defined as follows.

$\widehat{\mathsf{qSetup}}(1^\lambda)$**:** It works the same as qSetup except that qMSK contains additional elements as follows:

$$\boxed{\{\widehat{\mathbf{u}}_{i,j}\}_{i\in[mn],j\in[m]} \leftarrow \mathbb{Z}^k_p,\ \{\ddot{\mathbf{u}}_i\}_{i\in[mn]} \leftarrow \mathbb{Z}^m_p,\ \mathbf{r}^\eta_\iota, \widetilde{\mathbf{s}}^\eta_\iota \leftarrow \mathbb{Z}^k_p}$$

$$\mathsf{qMSK} := \begin{pmatrix} \mathbf{A}_1, \ldots, \mathbf{A}_n, \{\mathbf{w}_{i,j}\}_{i,j\in[mn]}, \{\widetilde{\mathbf{U}}_i, \mathbf{u}_i, \mathbf{V}_i, \widetilde{\mathbf{v}}_i, \boxed{\{\widehat{\mathbf{u}}_{i,j}\}_{j\in[m]}, \ddot{\mathbf{u}}_i}\}_{i\in[mn]} \\ \boxed{\mathbf{r}^\eta_\iota, \widehat{\mathbf{s}}^\eta_\iota}, \mathsf{pMSK}, \mathsf{iMSK}, \mathsf{gMSK} \end{pmatrix}.$$

$\widehat{\mathsf{qEnc}}^\eta_{\iota,1}(\mathsf{qMSK}, i, j, \{\mathbf{x}^{\nu,0}_\mu, \mathbf{x}^{\nu,1}_\mu\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** Let $\mathbf{w}^\top_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)} := (\mathbf{w}_{\mathsf{lo}(\iota,1),\mathsf{lo}(i,\kappa)}, \ldots, \mathbf{w}_{\mathsf{lo}(\iota,m),\mathsf{lo}(i,\kappa)})$ and $\widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)} := (\widetilde{\mathbf{U}}_{\mathsf{lo}(\iota,1)}||\cdots||\widetilde{\mathbf{U}}_{\mathsf{lo}(\iota,m)})$. It is the same as $\widetilde{\mathsf{qEnc}}^{\eta-1}_\iota$ except the way of defining the following vectors:

$$\mathbf{b}_{\kappa,5} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j \neq \eta \\ \boxed{\begin{matrix} \mathbf{w}^\top_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}(\mathbf{I}_m \otimes \mathbf{A}_i\mathbf{S}\widehat{\mathbf{s}}^\eta_\iota) + \mathbf{u}^\top_{\mathsf{lo}(i,\kappa)}\widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)}(\mathbf{I}_m \otimes \mathbf{r}^\eta_\iota) \\ + x^{j,0}_{i,\kappa}\mathbf{x}^{\eta,0\top}_\iota + x^{1,1}_{i,\kappa}\mathbf{x}^{1,1\top}_\iota - x^{1,0}_{i,\kappa}\mathbf{x}^{1,0\top}_\iota \end{matrix}} & \text{if } i = \iota \wedge j = \eta \\ \boxed{\begin{matrix} \mathbf{w}^\top_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}(\mathbf{I}_m \otimes \mathbf{A}_i\mathbf{S}\widehat{\mathbf{s}}^\eta_\iota) + \mathbf{u}^\top_{\mathsf{lo}(i,\kappa)}\widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)}(\mathbf{I}_m \otimes \mathbf{r}^\eta_\iota) \\ + x^{j,0}_{i,\kappa}\mathbf{x}^{\eta,0\top}_\iota + x^{j,1}_{i,\kappa}\mathbf{x}^{1,1\top}_\iota - x^{j,0}_{i,\kappa}\mathbf{x}^{1,0\top}_\iota \end{matrix}} & \text{if } i \neq \iota \end{cases}$$

$$\mathbf{b}_{\kappa,6} := \boxed{\mathbf{u}^\top_{\mathsf{lo}(i,\kappa)}\widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)}}$$

$$\widetilde{\mathbf{b}}_{\kappa,1} := \begin{cases} (0, x^{j,1}_{i,\kappa}) & \text{if } \mathsf{ql}(i,j) < \mathsf{ql}(\iota,\eta) \\ \boxed{(0,0)} & \text{if } \mathsf{ql}(i,j) = \mathsf{ql}(\iota,\eta) \\ (x^{j,0}_{i,\kappa}, 0) & \text{if } \mathsf{ql}(i,j) > \mathsf{ql}(\iota,\eta) \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,2} := \begin{cases} \boxed{\mathbf{0}} & \text{if } i = \iota \wedge j = \eta \\ (\mathbf{e}_{\mathsf{lo}(i,\kappa)/mn} \otimes \widetilde{\mathbf{s}}, \boxed{\mathbf{0}}) & \text{if } i = \iota \wedge j \neq \eta \\ (\mathbf{e}_{\mathsf{lo}(i,\kappa)/mn} \otimes \widetilde{\mathbf{s}}, \mathbf{r}^\top \widetilde{\mathbf{U}}_{\mathsf{lo}(i,\kappa)}) & \text{if } i \neq \iota \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,4} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j \leq \eta - 1 \\ \boxed{\mathbf{0}} & \text{if } i = \iota \wedge j = \eta \\ \mathbf{e}_{\kappa/m} & \text{if } i = \iota \wedge j > \eta \\ \mathbf{0} & \text{if } i \neq \iota \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,5} := \begin{cases} \boxed{\mathbf{e}_{\kappa/m}} & \text{if } \mathsf{ql}(i,j) = \mathsf{ql}(\iota,1) \\ \mathbf{0} & \text{if } \mathsf{ql}(i,j) \neq \mathsf{ql}(\iota,1) \end{cases}$$

$$\widetilde{\mathbf{b}}_{\kappa,6} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j = \eta \\ \boxed{\mathbf{e}_{\kappa/m} \otimes \mathbf{r}^\top} & \text{if } i = \iota \wedge j \neq \eta \\ \mathbf{0} & \text{if } i \neq \iota \end{cases}$$

$$\mathbf{d}_\tau := (\mathbf{a}_{i,\tau}^\top \mathbf{S}, \boxed{\mathbf{a}_{i,\tau}^\top \mathbf{S} \widetilde{\mathbf{s}}_\iota^\eta}),\ \widetilde{\mathbf{d}} := \begin{cases} \boxed{(\mathbf{0}, 1)} & \text{if } \mathsf{ql}(i,j) = \mathsf{ql}(\iota,\eta) \\ (\widetilde{\mathbf{s}}, 0) & \text{if } \mathsf{ql}(i,j) \neq \mathsf{ql}(\iota,\eta) \end{cases}$$

$$\mathbf{f}_1 := \begin{cases} \boxed{(\mathbf{0}, \mathbf{t})} & \text{if } \mathsf{ql}(i,j) = \mathsf{ql}(\iota,\eta) \\ (\mathbf{r}, \mathbf{t}) & \text{if } \mathsf{ql}(i,j) \neq \mathsf{ql}(\iota,\eta) \end{cases}, \quad h := \begin{cases} \boxed{1} & \text{if } \mathsf{ql}(i,j) = \mathsf{ql}(\iota,\eta) \\ 0 & \text{if } \mathsf{ql}(i,j) \neq \mathsf{ql}(\iota,\eta) \end{cases}.$$

$\widehat{\mathsf{qEnc}}^{\eta}_{\iota,2}(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** Let $\widehat{\mathbf{u}}_i^\top := (\widehat{\mathbf{u}}_{i,1}, \ldots, \widehat{\mathbf{u}}_{i,m})$. It is the same as $\widehat{\mathsf{qEnc}}^{\eta}_{\iota,1}$ except the way of defining the following vectors:

$$\boxed{\ddot{\mathbf{s}} \leftarrow \mathbb{Z}_p^k}$$

$$\mathbf{b}_{\kappa,5} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j \neq \eta \\ \mathbf{w}_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}^\top (\mathbf{I}_m \otimes \mathbf{A}_i \boxed{\ddot{\mathbf{s}}}) + \boxed{\widehat{\mathbf{u}}_{\mathsf{lo}(i,\kappa)}^\top} (\mathbf{I}_m \otimes \mathbf{r}_\iota^\eta) & \text{if } i = \iota \wedge j = \eta \\ \quad + x_{i,\kappa}^{j,0} \mathbf{x}_\iota^{\eta,0^\top} + x_{i,\kappa}^{1,1} \mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{1,0} \mathbf{x}_\iota^{1,0^\top} & \\ \mathbf{w}_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}^\top (\mathbf{I}_m \otimes \mathbf{A}_i \boxed{\ddot{\mathbf{s}}}) + \boxed{\widehat{\mathbf{u}}_{\mathsf{lo}(i,\kappa)}^\top} (\mathbf{I}_m \otimes \mathbf{r}_\iota^\eta) & \text{if } i \neq \iota \\ \quad + x_{i,\kappa}^{j,0} \mathbf{x}_\iota^{\eta,0^\top} + x_{i,\kappa}^{j,1} \mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{j,0} \mathbf{x}_\iota^{1,0^\top} & \end{cases}$$

$$\mathbf{b}_{\kappa,6} := \boxed{\widehat{\mathbf{u}}_{\mathsf{lo}(i,\kappa)}^\top}$$

$$\mathbf{d}_\tau := (\mathbf{a}_{i,\tau}^\top \mathbf{S}, \mathbf{a}_{i,\tau}^\top \boxed{\ddot{\mathbf{s}}}).$$

$\widehat{\mathsf{qEnc}}^{\eta}_{\iota,3}(\mathsf{qMSK}, i, j, \{\mathbf{x}_\mu^{\nu,0}, \mathbf{x}_\mu^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It is the same as $\widehat{\mathsf{qEnc}}^{\eta}_{\iota,2}$ except the way of defining the following vectors:

$$\mathbf{b}_{\kappa,5} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j \neq \eta \\ \mathbf{w}_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}^\top (\mathbf{I}_m \otimes \mathbf{A}_i \ddot{\mathbf{s}}) + \boxed{\ddot{\mathbf{u}}_{\mathsf{lo}(i,\kappa)}^\top} & \text{if } i = \iota \wedge j = \eta \\ \quad + x_{i,\kappa}^{j,0} \mathbf{x}_\iota^{\eta,0^\top} + x_{i,\kappa}^{1,1} \mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{1,0} \mathbf{x}_\iota^{1,0^\top} & \\ \mathbf{w}_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}^\top (\mathbf{I}_m \otimes \mathbf{A}_i \ddot{\mathbf{s}}) + \boxed{\ddot{\mathbf{u}}_{\mathsf{lo}(i,\kappa)}^\top} & \text{if } i \neq \iota \\ \quad + x_{i,\kappa}^{j,0} \mathbf{x}_\iota^{\eta,0^\top} + x_{i,\kappa}^{j,1} \mathbf{x}_\iota^{1,1^\top} - x_{i,\kappa}^{j,0} \mathbf{x}_\iota^{1,0^\top} & \end{cases}.$$

$\widehat{\mathsf{qEnc}}^{\eta}_{\iota,4}(\mathsf{qMSK}, i, j, \{\mathbf{x}_{\mu}^{\nu,0}, \mathbf{x}_{\mu}^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It is the same as $\widehat{\mathsf{qEnc}}^{\eta}_{\iota,3}$ except the way of defining the following vectors:

$$\mathbf{b}_{\kappa,5} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j \neq \eta \\ \mathbf{w}^{\top}_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}(\mathbf{I}_m \otimes \mathbf{A}_i \ddot{\mathbf{s}}) + \ddot{\mathbf{u}}_{\kappa}^{\top} + \boxed{x^{j,1}_{i,\kappa}\mathbf{x}^{\eta,1^{\top}}_{\iota}} & \text{if } i = \iota \wedge j = \eta \\ \mathbf{w}^{\top}_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}(\mathbf{I}_m \otimes \mathbf{A}_i \ddot{\mathbf{s}}) + \ddot{\mathbf{u}}_{\kappa}^{\top} + \boxed{x^{j,1}_{i,\kappa}\mathbf{x}^{\eta,1^{\top}}_{\iota}} & \text{if } i \neq \iota \end{cases}.$$

$\widehat{\mathsf{qEnc}}^{\eta}_{\iota,5}(\mathsf{qMSK}, i, j, \{\mathbf{x}_{\mu}^{\nu,0}, \mathbf{x}_{\mu}^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It is the same as $\widehat{\mathsf{qEnc}}^{\eta}_{\iota,1}$ (*not* $\widehat{\mathsf{qEnc}}^{\eta}_{\iota,4}$) except the way of defining the following vectors:

$$\mathbf{b}_{\kappa,5} := \begin{cases} \mathbf{0} & \text{if } i = \iota \wedge j \neq \eta \\ \mathbf{w}^{\top}_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}(\mathbf{I}_m \otimes \mathbf{A}_i \boxed{\mathbf{S}\widehat{\mathbf{s}}^{\eta}_{\iota}}) + \boxed{\mathbf{u}^{\top}_{\mathsf{lo}(i,\kappa)}\widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)}(\mathbf{I}_m \otimes \mathbf{r}^{\eta}_{\iota})} + x^{j,1}_{i,\kappa}\mathbf{x}^{\eta,1^{\top}}_{\iota} & \text{if } i = \iota \wedge j = \eta \\ \mathbf{w}^{\top}_{\mathsf{ls}(\iota),\mathsf{lo}(i,\kappa)}(\mathbf{I}_m \otimes \mathbf{A}_i \boxed{\mathbf{S}\widehat{\mathbf{s}}^{\eta}_{\iota}}) + \boxed{\mathbf{u}^{\top}_{\mathsf{lo}(i,\kappa)}\widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)}(\mathbf{I}_m \otimes \mathbf{r}^{\eta}_{\iota})} + x^{j,1}_{i,\kappa}\mathbf{x}^{\eta,1^{\top}}_{\iota} & \text{if } i \neq \iota \end{cases}.$$

$\mathsf{q}\widehat{\mathsf{KeyGen}}^{\eta}_{\iota,1}(\mathsf{qMSK}, \mathbf{c})$**:** It outputs qSK as follows (the framed part is changed from $\mathsf{q}\widetilde{\mathsf{KeyGen}}$):

$$\begin{aligned} \widetilde{\mathbf{f}}_{i,1} &:= \left(\sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in[mn]}} c_{\mu,\nu}\widetilde{\mathbf{U}}_{\mu}\mathbf{u}_{\nu}, \sum_{\substack{\mu\in[mn]\\ \nu\in\mathsf{ls}(i)}} c_{\mu,\nu}\mathbf{V}_{\nu}\widetilde{\mathbf{v}}_{\mu} \right) \\ \widetilde{\mathbf{f}}_{i,2,\theta} &:= \mathbf{c}_{\mathsf{ls}(\theta),\mathsf{ls}(i)} \\ \widetilde{\mathbf{f}}_{i} &:= (\widetilde{\mathbf{f}}_{i,1}, \widetilde{\mathbf{f}}_{i,2,1}, \ldots, \widetilde{\mathbf{f}}_{i,2,n}) \\ \widetilde{h}_i &:= \begin{cases} \boxed{\sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in[mn]}} c_{\mu,\nu}\mathbf{r}^{\eta^{\top}}_{\iota}\widetilde{\mathbf{U}}_{\mu}\mathbf{u}_{\nu}} & \text{if } i = \iota \\ 0 & \text{if } i \neq \iota \end{cases} \\ \mathsf{gSK} &\leftarrow \mathsf{gKeyGen}(\mathsf{gMSK}, \{[\widetilde{\mathbf{f}}_i]_2, [\widetilde{h}_i]_1\}_{i\in[n]}) \\ \boldsymbol{\sigma}_{i,\theta} &:= \sum_{\substack{\mu\in\mathsf{ls}(i),\\ \nu\in\mathsf{ls}(\theta)}} c_{\mu,\nu}\mathbf{w}_{\mu,\nu} \\ \mathsf{qSK} &:= (\mathbf{c}, \mathsf{gSK}, \{\boldsymbol{\sigma}_{i,\theta}\}_{i,\theta\in[n]}). \end{aligned}$$

$\mathsf{q}\widehat{\mathsf{KeyGen}}^{\eta}_{\iota,2}(\mathsf{qMSK}, \mathbf{c})$**:** It is the same as $\mathsf{q}\widehat{\mathsf{KeyGen}}^{\eta}_{\iota,1}$ except that it defines

$$\widetilde{h}_i := \begin{cases} \sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in[mn]}} c_{\mu,\nu}\mathbf{r}^{\eta^{\top}}_{\iota}\boxed{\widehat{\mathbf{u}}_{\nu,\mathsf{en}(\mu)}} & \text{if } i = \iota \\ 0 & \text{if } i \neq \iota \end{cases}.$$

$\mathsf{q}\widehat{\mathsf{KeyGen}}^{\eta}_{\iota,3}(\mathsf{qMSK}, \mathbf{c})$**:** Let $\ddot{\mathbf{u}}_i^{\top} = (\ddot{u}_{i,1}, \ldots, \ddot{u}_{i,m})$. It is the same as $\mathsf{q}\widehat{\mathsf{KeyGen}}^{\eta}_{\iota,2}$ except that it defines

$$\widetilde{h}_i := \begin{cases} \sum_{\substack{\mu\in\mathsf{ls}(i)\\ \nu\in[mn]}} c_{\mu,\nu}\boxed{\ddot{u}_{\nu,\mathsf{en}(\mu)}} & \text{if } i = \iota \\ 0 & \text{if } i \neq \iota \end{cases}.$$

$\widehat{\mathsf{qKeyGen}}^{\eta}_{\iota,4}(\mathsf{qMSK}, \mathbf{c})$**:** Let $\ddot{\mathbf{u}}_i^\top = (\ddot{u}_{i,1}, \ldots, \ddot{u}_{i,m})$. It is the same as $\widehat{\mathsf{qKeyGen}}^{\eta}_{\iota,3}$ except that it defines

$$\widetilde{h}_i := \begin{cases} \displaystyle\sum_{\substack{\mu \in \mathsf{ls}(i) \\ \nu \in [mn]}} c_{\mu,\nu} \ddot{u}_{\nu,\mathsf{en}(\mu)} & \\ \boxed{\displaystyle + \sum_{\mu \in [\iota-1]} \langle \mathbf{c}_{\mathsf{ls}(\mu),\mathsf{ls}(i)}, \mathbf{x}_\iota^{\eta,0} \otimes \mathbf{x}_\mu^{1,0} - \mathbf{x}_\iota^{1,0} \otimes \mathbf{x}_\mu^{1,0} - (\mathbf{x}_\iota^{\eta,1} \otimes \mathbf{x}_\mu^{1,1} - \mathbf{x}_\iota^{1,1} \otimes \mathbf{x}_\mu^{1,1}) \rangle} & \text{if } i = \iota \\ 0 & \text{if } i \neq \iota \end{cases}.$$

$\widehat{\mathsf{qKeyGen}}^{\eta}_{\iota,5}(\mathsf{qMSK}, \mathbf{c})$**:** Let $\ddot{\mathbf{u}}_i^\top = (\ddot{u}_{i,1}, \ldots, \ddot{u}_{i,m})$. It is the same as $\widehat{\mathsf{qKeyGen}}^{\eta}_{\iota,4}$ except that it defines

$$\widetilde{h}_i := \begin{cases} \displaystyle\sum_{\substack{\mu \in \mathsf{ls}(i) \\ \nu \in [mn]}} c_{\mu,\nu} \boxed{\mathbf{r}_\iota^{\eta\top} \widetilde{\mathbf{U}}_\mu \mathbf{u}_\nu} & \\ \displaystyle + \sum_{\mu \in [\iota-1]} \langle \mathbf{c}_{\mathsf{ls}(\mu),\mathsf{ls}(i)}, \mathbf{x}_\iota^{\eta,0} \otimes \mathbf{x}_\mu^{1,0} - \mathbf{x}_\iota^{1,0} \otimes \mathbf{x}_\mu^{1,0} - (\mathbf{x}_\iota^{\eta,1} \otimes \mathbf{x}_\mu^{1,1} - \mathbf{x}_\iota^{1,1} \otimes \mathbf{x}_\mu^{1,1}) \rangle & \text{if } i = \iota \\ 0 & \text{if } i \neq \iota \end{cases}.$$

□

Lemma 6.9. *For all PPT adversaries $\mathcal{A}$, $\iota \in [n]$, and $\eta \in [2, q_{\mathsf{CT}}]$, there exist PPT adversaries $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that* $|\mathsf{P}(\mathcal{A}, \mathsf{H}_\iota^{\eta-1}) - \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}^{\eta}_{\iota,1})| \leq \mathsf{Adv}^{\mathsf{pFE}}_{\mathcal{B}_1,\mathsf{pfh}}(\lambda) + \mathsf{Adv}^{\mathsf{iFE}}_{\mathcal{B}_2,\mathsf{fh}}(\lambda) + \mathsf{Adv}^{\mathsf{gFE}}_{\mathcal{B}_3,\mathsf{fh}}(\lambda) + 2^{-\Omega(\lambda)}$.

Proof. Since L is uniformly chosen from the exponentially large space in encryption algorithms, i.e., $\mathbb{Z}_p$, collisions do not occur in $\{L_i^j\}_{i \in [n], j \in [q_{\mathsf{CT}}]}$ with overwhelming probability. Therefore, $\langle \mathbf{l}_i^j, \widetilde{\mathbf{l}}_I^J \rangle = 0$ if $i \neq I$ or $j = J$, and $\langle \mathbf{l}_i^j, \widetilde{\mathbf{l}}_I^J \rangle \neq 0$ otherwise.

For all $(i, j, \kappa), (I, J, K) \in [n] \times [q_{\mathsf{CT}}] \times [m]$, observe that $\langle \mathbf{b}_{i,\kappa}^j, \widetilde{\mathbf{b}}_{I,K}^J \rangle$ in $\mathsf{H}_\iota^{\eta-1}$ are equal to that in $\widehat{\mathsf{H}}^{\eta}_{\iota,1}$ *if* $i \neq I$ or $j = J$. Thus, due to the partially function-hiding property of pFE, this implies that $\{\mathsf{pCT}^j_{i,\mathsf{lo}(i,\kappa)}, \mathsf{pSK}^j_{i,\mathsf{lo}(i,\kappa)}\}$ generated in $\mathsf{H}_\iota^{\eta-1}$ and those generated in $\widehat{\mathsf{H}}^{\eta}_{\iota,1}$ are computationally indistinguishable.

Similarly, we can also confirm that for all $(i, j, \tau) \in [n] \times [q_{\mathsf{CT}}] \times [k]$ and $(I, J) \in [n] \times [q_{\mathsf{CT}}]$, we have $\langle \mathbf{d}_{i,\tau}^j, \widetilde{\mathbf{d}}_I^J \rangle$ in $\mathsf{H}_\iota^{\eta-1}$ are equal to that in $\widehat{\mathsf{H}}^{\eta}_{\iota,1}$. Thus, thanks to the function-hiding property of iFE, $\{\mathsf{iCT}^j_{i,\tau}, \mathsf{iSK}^j_i\}$ generated in $\mathsf{H}_\iota^{\eta-1}$ and those generated in $\widehat{\mathsf{H}}^{\eta}_{\iota,1}$ are computationally indistinguishable.

We can also confirm that for all $(i, j, \ell) \in [n] \times [q_{\mathsf{CT}}] \times [q_{\mathsf{SK}}]$, we have $\langle \mathbf{f}_i^j, \widetilde{\mathbf{f}}_i^\ell \rangle + \langle h_i^j, \widehat{h}_i^\ell \rangle$ in $\mathsf{H}_\iota^{\eta-1}$ are equal to that in $\widehat{\mathsf{H}}^{\eta}_{\iota,1}$. Thus, thanks to the function-hiding property of gFE, $\{\mathsf{gCT}_i^j, \mathsf{gSK}^\ell\}$ generated in $\mathsf{H}_\iota^{\eta-1}$ and those generated in $\widehat{\mathsf{H}}^{\eta}_{\iota,1}$ are computationally indistinguishable. Hence, $\mathcal{A}$'s views in $\mathsf{H}_\iota^{\eta-1}$ and $\widehat{\mathsf{H}}^{\eta}_{\iota,1}$ are computationally indistinguishable. □

Lemma 6.10. *For all PPT adversaries $\mathcal{A}$, $\iota \in [n]$, and $\eta \in [2, q_{\mathsf{CT}}]$, there exist PPT adversaries $\mathcal{B}_1, \mathcal{B}_2$ against mk-fold $\mathcal{U}_{mn,k}$-MDDH and $\mathcal{U}_{knq_{\mathsf{CT}},k}$-MDDH, respectively, such that* $|\mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}^{\eta}_{\iota,1}) - \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}^{\eta}_{\iota,2})| \leq \mathsf{Adv}^{mk\text{-}\mathcal{U}_{mn,k}\text{-}\mathsf{MDDH}}_{\mathcal{B}_1}(\lambda) + \mathsf{Adv}^{\mathcal{U}_{knq_{\mathsf{CT}},k}\text{-}\mathsf{MDDH}}_{\mathcal{B}_2}(\lambda)$.

Proof. We can prove the lemma with two steps. In the first step, $\widetilde{\mathbf{U}}_\mu \mathbf{u}_\nu$ for $(\mu, \nu) \in \mathsf{ls}(\iota) \times [mn]$ is changed to $\widehat{\mathbf{u}}_{\nu,\mathsf{en}(\mu)}$ via mn-fold $\mathcal{U}_{mk,k}$-MDDH. Observe that this change corresponds to the change from $\mathbf{u}^\top_{\mathsf{lo}(i,\kappa)} \widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)}$ to $\widehat{\mathbf{u}}^\top_{\mathsf{lo}(i,\kappa)}$. $\mathcal{B}_1$ works as follows.

1. $\mathcal{B}_1$ takes an instance of the mk-fold $\mathcal{U}_{mn,k}$-MDDH, $(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{K}_\beta]_1)$. Recall that they are distributed as $\mathbf{M} \leftarrow \mathbb{Z}_p^{mn \times k}$, $\mathbf{K}_0 = \mathbf{M}\mathbf{Z} \in \mathbb{Z}_p^{mn \times mk}$ where $\mathbf{Z} \leftarrow \mathbb{Z}_p^{k \times mk}$, and $\mathbf{K}_1 \leftarrow \mathbb{Z}_p^{mn \times mk}$.
2. $\mathcal{B}_1$ computes $\mathsf{qPP}, \mathsf{qMSK}$ in the same way as $\widehat{\mathsf{qSetup}}$ except that $\mathcal{B}_1$ (implicitly) defines that $\mathbf{u}_i := \mathbf{m}_i^\top, \widehat{\mathbf{u}}_i := \mathbf{k}_{1,i}^\top$ for $i \in [mn]$ and $\widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)} := \mathbf{Z}$ for $i \in [m]$, where $\mathbf{m}_i$ and $\mathbf{k}_{\beta,i}$ are the i-th rows of $\mathbf{M}$ and $\mathbf{K}_\beta$, respectively.

3. $\mathcal{B}_1$ computes qCT_i^j for $i \in [n], j \in [q_{\mathsf{CT}}]$ in the same way as $\widehat{\mathsf{qEnc}}_{\iota,1}^{\eta}$ except that $\mathcal{B}_1$ replaces $\mathbf{u}_{\mathsf{lo}(i,\kappa)}^{\top}\widetilde{\mathbf{U}}_{\mathsf{ls}(\iota)}$ in $\mathbf{b}_{\kappa,5}, \mathbf{b}_{\kappa,6}$ with $\mathbf{k}_{\beta,\mathsf{lo}(i,\kappa)}^{\top}$ and gives $\mathsf{qPP}, \{\mathsf{qCT}_i^j\}$ to $\mathcal{A}$.
4. $\mathcal{B}_1$ simulates the key generation oracle in the same way as $\widehat{\mathsf{qKeyGen}}_{\iota,1}^{\eta}$ except that $\mathcal{B}_1$ replaces $\widetilde{\mathbf{U}}_{\mu}\mathbf{u}_{\nu}$ in $\tilde{h}_i$ with $\mathbf{k}_{\beta,\nu,\mathsf{en}(\mu)}^{\top}$ where $\mathbf{k}_{\beta,i,j}^{\top}$ for $(i,j) \in [mn] \times [m]$ is the vector consisting of the $(j-1)k+1$ to jk-th entries of $\mathbf{k}_{\beta,i}^{\top}$. Note that since $\tilde{h}_i$ become an exponent of g_1, this simulation is possible.
5. $\mathcal{B}_1$ outputs $\mathcal{A}$'s output as it is.

In the second step, $\mathbf{S}\widetilde{\mathbf{s}}_{\iota}^{\eta}$ is changed to $\ddot{\mathbf{s}}$ via $\mathcal{U}_{knq_{\mathsf{CT}},k}$-MDDH. $\mathcal{B}_2$ works as follows.

1. $\mathcal{B}_2$ takes an instance of the $\mathcal{U}_{knq_{\mathsf{CT}},k}$-MDDH, $(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{k}_{\beta}]_1)$. Recall that they are distributed as $\mathbf{M} \leftarrow \mathbb{Z}_p^{knq_{\mathsf{CT}} \times k}$, $\mathbf{k}_0 = \mathbf{M}\mathbf{z} \in \mathbb{Z}_p^{knq_{\mathsf{CT}}}$ where $\mathbf{z} \leftarrow \mathbb{Z}_p^k$, and $\mathbf{k}_1 \leftarrow \mathbb{Z}_p^{knq_{\mathsf{CT}}}$.
2. $\mathcal{B}_2$ computes $\mathsf{qPP}, \mathsf{qMSK} \leftarrow \widehat{\mathsf{qSetup}}$ except that $\mathcal{B}_2$ implicitly defines $\widetilde{\mathbf{s}}_{\iota}^{\eta} := \mathbf{z}$.
3. $\mathcal{B}_2$ computes qCT_i^j for $i \in [n], j \in [q_{\mathsf{CT}}]$ in the same way as $\widehat{\mathsf{qEnc}}_{\iota,1}^{\eta}$ except that $\mathcal{B}_2$ defines $\mathbf{S}_i^j := \mathbf{M}_{\mathsf{ql}(i,j)}, \ddot{\mathbf{s}}_i^j := \mathbf{k}_{1,\mathsf{ql}(i,j)}$ and replaces $\mathbf{S}_i^j\widetilde{\mathbf{s}}_{\iota}^{\eta}$ in $\mathbf{b}_{\kappa,5}$ and $\mathbf{d}_{\tau}$ with $\mathbf{k}_{\beta,\mathsf{ql}(i,j)}$, where $\mathbf{M}_{\mu}$ for $\mu \in [nq_{\mathsf{CT}}]$ is the matrix consisting of the $(i-1)k+1$ to ik-th rows of $\mathbf{M}$, and $\mathbf{k}_{\beta,\mu}$ is the matrix consisting of the $(\mu-1)k+1$ to μk-th entries of $\mathbf{k}_{\beta}$. Then, $\mathcal{B}_2$ gives $\mathsf{qPP}, \{\mathsf{qCT}_i^j\}$ to $\mathcal{A}$.
4. $\mathcal{B}_2$ simulates the key generation oracle in the same way as $\widehat{\mathsf{qKeyGen}}_{\iota,2}^{\eta}$.
5. $\mathcal{B}_2$ outputs $\mathcal{A}$'s output as it is.

This concludes the proof. Note that mn-fold $\mathcal{U}_{mk,k}$-MDDH is reduced to $\mathcal{D}_k$-MDDH with the security loss of mk, and $\mathcal{U}_{knq_{\mathsf{CT}},k}$-MDDH is tightly reduced to $\mathcal{D}_k$-MDDH. □

Lemma 6.11. *For all PPT adversaries $\mathcal{A}$, $\iota \in [n]$, and $\eta \in [2, q_{\mathsf{CT}}]$, there exists a PPT adversary $\mathcal{B}$ against $\mathcal{U}_{m^2n,k}$-MDDH such that* $|\mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,2}^{\eta}) - \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,3}^{\eta})| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathcal{U}_{m^2n,k}\text{-}\mathsf{MDDH}}(\lambda)$.

Proof. $\mathcal{B}$ works as follows.

1. $\mathcal{B}$ takes an instance of the $\mathcal{U}_{m^2n,k}$-MDDH, $(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{k}_{\beta}]_1)$. Recall that they are distributed as $\mathbf{M} \leftarrow \mathbb{Z}_p^{m^2n \times k}$, $\mathbf{k}_0 = \mathbf{M}\mathbf{z} \in \mathbb{Z}_p^{m^2n}$ where $\mathbf{z} \leftarrow \mathbb{Z}_p^k$, and $\mathbf{k}_1 \leftarrow \mathbb{Z}_p^{m^2n}$.
2. $\mathcal{B}$ computes $\mathsf{qPP}, \mathsf{qMSK} \leftarrow \widehat{\mathsf{qSetup}}$ except that $\mathcal{B}$ (implicitly) defines that $\widehat{\mathbf{u}}_{i,j} := \mathbf{m}_{(i-1)m+j}^{\top}, \mathbf{r}_{\iota}^{\eta} := \mathbf{z}, \ddot{u}_{i,j} := k_{1,(i-1)m+j}$ for $(i,j) \in [mn] \times [m]$, where $\mathbf{m}_{\mu}$ is the μ-th row of $\mathbf{M}$, and $k_{\beta,\mu}$ is the μ-th entry of $\mathbf{k}_{\beta}$.
3. $\mathcal{B}$ computes qCT_i^j for $i \in [n], j \in [q_{\mathsf{CT}}]$ in the same way as $\widehat{\mathsf{qEnc}}_{\iota,2}^{\eta}$ except that $\mathcal{B}$ replaces $\widehat{\mathbf{u}}_{\mu,\nu}^{\top}\mathbf{r}_{\iota}^{\eta}$ for $\mu \times \nu \in [mn] \times [m]$ with $k_{\beta,(\mu-1)m+\nu}$. Then, $\mathcal{B}$ gives $\mathsf{qPP}, \{\mathsf{qCT}_i^j\}$ to $\mathcal{A}$.
4. $\mathcal{B}$ simulates the key generation oracle in the same way as $\widehat{\mathsf{qKeyGen}}_{\iota,2}^{\eta}$ except that $\mathcal{B}$ replaces ${\mathbf{r}_{\iota}^{\eta}}^{\top}\widehat{\mathbf{u}}_{\mu',\nu'}$ for $\mu' \times \nu' \in [mn] \times [m]$ with $k_{\beta,(\mu'-1)m+\nu'}$.
5. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

Observe that the encryption and key generation algorithms corresponds to $\widehat{\mathsf{qEnc}}_{\iota,2}^{\eta}$ and $\widehat{\mathsf{qKeyGen}}_{\iota,2}^{\eta}$, respectively, if $\beta = 0$, and $\widehat{\mathsf{qEnc}}_{\iota,3}^{\eta}$ and $\widehat{\mathsf{qKeyGen}}_{\iota,3}^{\eta}$, respectively, if $\beta = 1$. This concludes the proof. Note that $\mathcal{U}_{m^2n,k}$-MDDH is tightly reduced to $\mathcal{D}_k$-MDDH. □

Lemma 6.12. *For all PPT adversaries $\mathcal{A}$, $\iota \in [n]$, and $\eta \in [2, q_{\mathsf{CT}}]$, there exists a PPT adversary $\mathcal{B}$ against* miFE *in Sec. 6.2 such that* $|\mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,3}^{\eta}) - \mathsf{P}(\mathcal{A}, \widehat{\mathsf{H}}_{\iota,4}^{\eta})| \leq \mathsf{Adv}_{\mathcal{B},\mathsf{mh}}^{\mathsf{miFE}}(\lambda)$.

Proof. First, we prove that the following equality holds: for all $(\iota, \eta) \in [n] \times [q_{\mathsf{CT}}]$, $j_1, \ldots, j_n \in [q_{\mathsf{CT}}]^n$, and $\ell \in [q_{\mathsf{SK}}]$, we have

$$\begin{aligned}
&\sum_{i \in [n] \backslash \iota} \langle \mathbf{c}^{\ell}_{\mathsf{ls}(\iota),\mathsf{ls}(i)}, \mathbf{x}_i^{j_i,0} \otimes \mathbf{x}_\iota^{\eta,0} - \mathbf{x}_i^{j_i,0} \otimes \mathbf{x}_\iota^{1,0} \rangle + \langle \mathbf{c}^{\ell}_{\mathsf{ls}(\iota),\mathsf{ls}(\iota)}, \mathbf{x}_\iota^{\eta,0} \otimes \mathbf{x}_\iota^{\eta,0} - \mathbf{x}_\iota^{1,0} \otimes \mathbf{x}_\iota^{1,0} \rangle \\
&+ \sum_{i \in [\iota-1]} \langle \mathbf{c}^{\ell}_{\mathsf{ls}(i),\mathsf{ls}(\iota)}, \mathbf{x}_\iota^{\eta,0} \otimes \mathbf{x}_i^{1,0} - \mathbf{x}_\iota^{1,0} \otimes \mathbf{x}_i^{1,0} \rangle \\
= &\sum_{i \in [n] \backslash \iota} \langle \mathbf{c}^{\ell}_{\mathsf{ls}(\iota),\mathsf{ls}(i)}, \mathbf{x}_i^{j_i,1} \otimes \mathbf{x}_\iota^{\eta,1} - \mathbf{x}_i^{j_i,1} \otimes \mathbf{x}_\iota^{1,1} \rangle + \langle \mathbf{c}^{\ell}_{\mathsf{ls}(\iota),\mathsf{ls}(\iota)}, \mathbf{x}_\iota^{\eta,1} \otimes \mathbf{x}_\iota^{\eta,1} - \mathbf{x}_\iota^{1,1} \otimes \mathbf{x}_\iota^{1,1} \rangle \\
&+ \sum_{i \in [\iota-1]} \langle \mathbf{c}^{\ell}_{\mathsf{ls}(i),\mathsf{ls}(\iota)}, \mathbf{x}_\iota^{\eta,1} \otimes \mathbf{x}_i^{1,1} - \mathbf{x}_\iota^{1,1} \otimes \mathbf{x}_i^{1,1} \rangle.
\end{aligned} \tag{6.2}$$

Due to the game condition in Def. 2.3, for all $(\iota, \eta) \in [n] \times [q_{\mathsf{CT}}]$, $j_{\iota+1}, \ldots, j_n \in [q_{\mathsf{CT}}]^{n-\iota}$, and $\ell \in [q_{\mathsf{SK}}]$, we have

$$\sum_{i,\theta \in [n]} \langle \mathbf{c}^{\ell}_{\mathsf{ls}(i),\mathsf{ls}(\theta)}, \mathbf{x}_\theta^{f(\theta),0} \otimes \mathbf{x}_i^{f(i),0} \rangle = \sum_{i,\theta \in [n]} \langle \mathbf{c}^{\ell}_{\mathsf{ls}(i),\mathsf{ls}(\theta)}, \mathbf{x}_\theta^{f(\theta),1} \otimes \mathbf{x}_i^{f(i),1} \rangle \tag{6.3}$$

$$\sum_{i,\theta \in [n]} \langle \mathbf{c}^{\ell}_{\mathsf{ls}(i),\mathsf{ls}(\theta)}, \mathbf{x}_\theta^{g(\theta),0} \otimes \mathbf{x}_i^{g(i),0} \rangle = \sum_{i,\theta \in [n]} \langle \mathbf{c}^{\ell}_{\mathsf{ls}(i),\mathsf{ls}(\theta)}, \mathbf{x}_\theta^{g(\theta),1} \otimes \mathbf{x}_i^{g(i),1} \rangle \tag{6.4}$$

where

$$f(i) = \begin{cases} 1 & \text{if } i < \iota \\ \eta & \text{if } i = \iota \\ j_i & \text{if } i > \iota \end{cases}, \quad g(i) = \begin{cases} 1 & \text{if } i < \iota \\ 1 & \text{if } i = \iota \\ j_i & \text{if } i > \iota \end{cases}.$$

Then, Eq. (6.3) $-$ Eq. (6.4) results in Eq. (6.2) by reflecting the fact that $\mathbf{c}^{\ell}_{\mathsf{ls}(i),\mathsf{ls}(\theta)} = \mathbf{0}$ if $i > \theta$, which is defined in Def. 2.4.

We set the functionality of miFE as $\mathcal{F}^{\mathsf{MIP}}_{m^2,n+\iota-1}$, and let $n' = n + \iota - 1$. $\mathcal{B}$ against miFE works as follows.

1. $\mathcal{B}$ obtains $\mathsf{miPP} = (\mathbb{G}, [\mathbf{A}_1]_1, \ldots, [\mathbf{A}_{n'}]_1, [\widetilde{\mathbf{W}}_1 \mathbf{A}_1]_1, \ldots, [\widetilde{\mathbf{W}}_{n'} \mathbf{A}_{n'}]_1)$ where they are distributed as $\mathbf{A}_i \leftarrow \mathcal{D}_k, \widetilde{\mathbf{W}}_i \leftarrow \mathbb{Z}_p^{m^2 \times (k+1)}$. $\mathcal{B}$ implicitly defines $\mathbf{w}_{i,j} := \widetilde{\mathbf{w}}^{\top}_{\mathsf{sl}(j),(\mathsf{en}(j)-1)m+\mathsf{en}(i)}$ for $i \in \mathsf{ls}(\iota), j \in [mn]$ where $\widetilde{\mathbf{w}}_{\mu,\nu}$ is the ν-th row of $\widetilde{\mathbf{W}}_\mu$, and generates qPP and other elements in qMSK the same as $\widehat{\mathsf{qSetup}}$.
2. When $\mathcal{A}$ outputs the challenge ciphertexts, $\{i, \mathbf{x}_i^{j,0}, \mathbf{x}_i^{j,1}\}_{i \in [n], j \in [q_{\mathsf{CT}}]}$, $\mathcal{B}$ defines

   $$\widetilde{\mathbf{x}}_i^{j,\beta} := \begin{cases} \mathbf{x}_i^{j,\beta} \otimes \mathbf{x}_\iota^{\eta,\beta} - \mathbf{x}_i^{j,\beta} \otimes \mathbf{x}_\iota^{1,\beta} & \text{if } i \in [n] \backslash \iota \\ \mathbf{x}_\iota^{\eta,\beta} \otimes \mathbf{x}_\iota^{\eta,\beta} - \mathbf{x}_\iota^{1,\beta} \otimes \mathbf{x}_\iota^{1,\beta} & \text{if } i = \iota \\ \mathbf{x}_\iota^{\eta,\beta} \otimes \mathbf{x}_{i-n}^{1,\beta} - \mathbf{x}_\iota^{1,\beta} \otimes \mathbf{x}_{i-n}^{1,\beta} & \text{if } i \in [n+1, n'] \end{cases}$$

   and outputs $\{i, \widetilde{\mathbf{x}}_i^{j,0}, \widetilde{\mathbf{x}}_i^{j,1}\}_{i \in [n'], j \in [q'_{\mathsf{CT},i}]}$ as challenge vectors for the message-hiding game for miFE where

   $$q'_{\mathsf{CT},i} = \begin{cases} 1 & i = [\iota] \vee i \in [n+1, n'] \\ q_{\mathsf{CT}} & i \in [n] \backslash \iota \end{cases}.$$

   Then, $\mathcal{B}$ obtains $\{\mathsf{miCT}_i^j\}_{i \in [n'], j \in [q'_{\mathsf{CT},i}]}$ where $\mathsf{miCT}_i^j = ([\boldsymbol{\gamma}_i^j]_1, [\boldsymbol{\delta}_i^j]_1) = ([\mathbf{A}_i \ddot{\mathbf{s}}_i^j]_1, [\widetilde{\mathbf{W}}_i \mathbf{A}_i \ddot{\mathbf{s}}_i^j + \ddot{\mathbf{u}}_i + \widetilde{\mathbf{x}}_i^{j,\beta}]_1)$.

3. $\mathcal{B}$ generates qCT_i^j the same as $\widehat{\mathsf{qEnc}}_{\iota,3}^{\eta}$ except that it defines

$$\begin{aligned}(\mathbf{b}_{1,5},\dots,\mathbf{b}_{m,5}) &:= \begin{cases}\mathbf{0} & \text{if } i=\iota \wedge j\neq\eta\\ (\boldsymbol{\delta}_i^1+\mathbf{x}_i^{1,1}\otimes\mathbf{x}_\iota^{1,1})^\top & i=\iota\wedge j=\eta\\ (\boldsymbol{\delta}_i^j+\mathbf{x}_i^{j,1}\otimes\mathbf{x}_\iota^{1,1})^\top & i\neq\iota\end{cases}\\ \mathbf{d}_\tau &:= (\mathbf{a}_{i,\tau}^\top\mathbf{S},\gamma_{i,\tau}^j).\end{aligned}$$

4. When $\mathcal{A}$ queries the key generation oracle on $\mathbf{c}$, $\mathcal{B}$ queries the key generation oracle for miFE on $(\widetilde{\mathbf{c}}_1,\dots,\widetilde{\mathbf{c}}_{n'}) := (\mathbf{c}_{\mathsf{ls}(\iota),\mathsf{ls}(1)},\dots,\mathbf{c}_{\mathsf{ls}(\iota),\mathsf{ls}(n)},\mathbf{c}_{\mathsf{ls}(1),\mathsf{ls}(\iota)},\dots,\mathbf{c}_{\mathsf{ls}(\iota-1),\mathsf{ls}(\iota)})$ and obtains $\mathsf{miSK} = (\mathsf{miSK}_0, \{\mathsf{miSK}_i\}_{i\in[n']}) = (\sum_{i\in[n']}\langle\widetilde{\mathbf{c}}_i,\ddot{\mathbf{u}}_i\rangle, \{-\widetilde{\mathbf{c}}_i^\top\widetilde{\mathbf{W}}_i\}_{i\in[n']})$ (here we omit $\widetilde{\mathbf{c}}_i$ in miSK_i for convenience). Since we have Eq. (6.2), $\mathcal{B}$'s queries follow the security game condition for miFE. Then, $\mathcal{B}$ generates a secret key the same as $\widehat{\mathsf{qKeyGen}}_{\iota,3}^{\eta}$ except that it defines

$$\begin{aligned}\widetilde{h}_\iota &:= \mathsf{miSK}_0 - \sum_{i\in[n+1,n']}\Big(\langle\widetilde{\mathbf{c}}_i,\boldsymbol{\delta}_i^1-\widetilde{\mathbf{x}}_i^{1,0}\rangle+\langle\mathsf{miSK}_i,\boldsymbol{\gamma}_i^1\rangle\Big)\\ \boldsymbol{\sigma}_{\iota,\theta} &:= \mathsf{miSK}_\theta.\end{aligned}$$

5. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

Observe that the encryption and key generation algorithms corresponds to $\widehat{\mathsf{qEnc}}_{\iota,3}^{\eta}$ and $\widehat{\mathsf{qKeyGen}}_{\iota,3}^{\eta}$, respectively, if $\beta=0$ in the security game for miFE, and $\widehat{\mathsf{qEnc}}_{\iota,4}^{\eta}$ and $\widehat{\mathsf{qKeyGen}}_{\iota,4}^{\eta}$, respectively, if $\beta=1$. This concludes the proof. □

Lemma 6.13. *For all PPT adversaries $\mathcal{A}$, $\iota\in[n]$, and $\eta\in[2,q_{\mathsf{CT}}]$, there exist PPT adversaries $\mathcal{B}_1,\mathcal{B}_2,\mathcal{B}_3$ against mk-fold $\mathcal{U}_{mn,k}$-MDDH, $\mathcal{U}_{knq_{\mathsf{CT}},k}$-MDDH, and $\mathcal{U}_{m^2n,k}$-MDDH, respectively, such that* $|\mathsf{P}(\mathcal{A},\widehat{\mathsf{H}}_{\iota,4}^{\eta})-\mathsf{P}(\mathcal{A},\widehat{\mathsf{H}}_{\iota,5}^{\eta})| \le \mathsf{Adv}_{\mathcal{B}_1}^{mk\text{-}\mathcal{U}_{mn,k}\text{-}\mathsf{MDDH}}(\lambda)+\mathsf{Adv}_{\mathcal{B}_2}^{\mathcal{U}_{knq_{\mathsf{CT}},k}\text{-}\mathsf{MDDH}}(\lambda)+\mathsf{Adv}_{\mathcal{B}_3}^{\mathcal{U}_{m^2n,k}\text{-}\mathsf{MDDH}}(\lambda)$.

Lemma 6.13 can be proven similarly to Lemmata 6.10 and 6.11.

Lemma 6.14. *For all PPT adversaries $\mathcal{A}$, $\iota\in[n]$, and $\eta\in[2,q_{\mathsf{CT}}]$, there exist PPT adversaries $\mathcal{B}_1,\mathcal{B}_2,\mathcal{B}_3$ such that* $|\mathsf{P}(\mathcal{A},\widehat{\mathsf{H}}_{\iota,5}^{\eta})-\mathsf{P}(\mathcal{A},\mathsf{H}_\iota^{\eta})| \le \mathsf{Adv}_{\mathcal{B}_1,\mathsf{pfh}}^{\mathsf{pFE}}(\lambda)+\mathsf{Adv}_{\mathcal{B}_2,\mathsf{fh}}^{\mathsf{iFE}}(\lambda)+\mathsf{Adv}_{\mathcal{B}_3,\mathsf{fh}}^{\mathsf{gFE}}(\lambda)+2^{-\Omega(\lambda)}$.

Lemma 6.14 can be proven similarly to Lemma 6.9.

Proof of Lemma 6.3. For reference, we describe $\widetilde{\mathsf{qEnc}}_n^{q_{\mathsf{CT}}}$ and frame the parts that are different from qEnc.

$\widetilde{\mathsf{qEnc}}_n^{q_{\mathsf{CT}}}(\mathsf{qMSK},i,j,\{\mathbf{x}_\mu^{\nu,0},\mathbf{x}_\mu^{\nu,1}\}_{\mu\in[n],\nu\in[q_{\mathsf{CT}}]})$**:** It samples vectors as follows:

$$\begin{aligned}&\mathbf{S}\leftarrow\mathbb{Z}_p^{k\times k},\ \widetilde{\mathbf{s}},\mathbf{r},\mathbf{t}\leftarrow\mathbb{Z}_p^k,\ L\leftarrow\mathbb{Z}_p\\ &\mathbf{l} := \mathbf{e}_{i/n}\otimes(1,L)\in\mathbb{Z}_p^{2n},\ \widetilde{\mathbf{l}} := \mathbf{e}_{i/n}\otimes(L,-1)\in\mathbb{Z}_p^{2n}\\ &\boxed{\mathbf{b}_{\kappa,1} := (x_{i,\kappa}^{j,0},x_{i,\kappa}^{j,1})}\in\mathbb{Z}_p^2,\ \mathbf{b}_{\kappa,2} := (\mathbf{w}_{\mathsf{lo}(i,\kappa)}^\top(\mathbf{I}_{mn}\otimes\mathbf{A}_i\mathbf{S}),\mathbf{u}_{\mathsf{lo}(i,\kappa)})\in\mathbb{Z}_p^{(mn+1)k}\\ &\mathbf{b}_{\kappa,3} := \mathbf{t}^\top\mathbf{V}_{\mathsf{lo}(i,\kappa)}\in\mathbb{Z}_p^k\\ &\boxed{\mathbf{b}_{\kappa,4} := \begin{cases}x_{i,\kappa}^{1,1}\mathbf{x}_{\iota-1}^{1,1^\top}-x_{i,\kappa}^{1,0}\mathbf{x}_{\iota-1}^{1,0^\top} & \text{if } i=n\\ x_{i,\kappa}^{j,1}\mathbf{x}_{\iota-1}^{1,1^\top}-x_{i,\kappa}^{j,0}\mathbf{x}_{\iota-1}^{1,0^\top} & \text{if } i\neq n\end{cases}}\in\mathbb{Z}_p^m\\ &\mathbf{b}_{\kappa,5} := \mathbf{0}\in\mathbb{Z}_p^m,\ \mathbf{b}_{\kappa,6} := \mathbf{0}\in\mathbb{Z}_p^{km},\ \mathbf{b}_\kappa := (\mathbf{b}_{\kappa,1},\dots,\mathbf{b}_{\kappa,6})\\ &\boxed{\widetilde{\mathbf{b}}_{\kappa,1} := (0,x_{i,\kappa}^{j,1})}\in\mathbb{Z}_p^2\end{aligned}$$

$$\begin{aligned}
&\widetilde{\mathbf{b}}_{\kappa,2} := (\mathbf{e}_{\mathsf{lo}(i,\kappa)/mn} \otimes \widetilde{\mathbf{s}}, \mathbf{r}^\top \widetilde{\mathbf{U}}_{\mathsf{lo}(i,\kappa)}) \in \mathbb{Z}_p^{(mn+1)k} \\
&\widetilde{\mathbf{b}}_{\kappa,3} := \widetilde{\mathbf{v}}_{\mathsf{lo}(i,\kappa)}^\top \in \mathbb{Z}_p^k,\ \widetilde{\mathbf{b}}_{\kappa,4} = \widetilde{\mathbf{b}}_{\kappa,5} := \mathbf{0} \in \mathbb{Z}_p^m,\ \widetilde{\mathbf{b}}_{\kappa,6} := \mathbf{0} \in \mathbb{Z}_p^{km} \\
&\widetilde{\mathbf{b}}_{\kappa} := (\widetilde{\mathbf{b}}_{\kappa,1}, \ldots, \widetilde{\mathbf{b}}_{\kappa,6}) \\
&\mathbf{d}_\tau := (\mathbf{a}_{i,\tau}^\top \widehat{\mathbf{S}}, 0) \in \mathbb{Z}_p^{k+1},\ \widetilde{\mathbf{d}} := (\widetilde{\mathbf{s}}, 0) \in \mathbb{Z}_p^{k+1} \\
&\mathbf{f}_1 := (\mathbf{r}, \mathbf{t}) \in \mathbb{Z}_p^{2k} \\
&\boxed{\mathbf{f}_{2,\theta} := (\mathbf{x}_i^{1,1} \otimes \mathbf{x}_\theta^{1,1} - \mathbf{x}_i^{1,0} \otimes \mathbf{x}_\theta^{1,0})^\top} \in \mathbb{Z}_p^{m^2} \\
&\mathbf{f} := (\mathbf{f}_1, \mathbf{f}_{2,1}, \ldots, \mathbf{f}_{2,n}),\ h := 0.
\end{aligned}$$

Then, it computes qCT_i^j in the same way as Eq. (6.1).

For all $(i, j, \kappa), (I, J, K) \in [n] \times [q_{\mathsf{CT}}] \times [m]$, observe that $\langle \mathbf{b}_{i,\kappa}^j, \widetilde{\mathbf{b}}_{I,K}^J \rangle$ in $\mathsf{H}_n^{q_{\mathsf{CT}}}$ are equal to that in G_1. Thus, due to the partially function-hiding property of pFE, this implies that $\{\mathsf{pCT}_{i,\mathsf{lo}(i,\kappa)}^j, \mathsf{pSK}_{i,\mathsf{lo}(i,\kappa)}^j\}$ generated in $\mathsf{H}_n^{q_{\mathsf{CT}}}$ and those generated in G_1 are computationally indistinguishable.

Next, we confirm that, for all $\ell \in [q_{\mathsf{SK}}]$, we have

$$\sum_{i,\theta \in [n]} \langle \mathbf{c}_{\mathsf{ls}(i),\mathsf{ls}(\theta)}^\ell, \mathbf{x}_\theta^{1,1} \otimes \mathbf{x}_i^{1,1} - \mathbf{x}_\theta^{1,0} \otimes \mathbf{x}_i^{1,0} \rangle = 0.$$

This is implied by the game condition defined in Def. 2.3. Thus, for all $(j_1, \ldots, j_n, \ell) \in [q_{\mathsf{CT}}]^n \times [q_{\mathsf{SK}}]$, we have $\sum_{i \in [n]} (\langle \mathbf{f}_i^{j_i}, \widetilde{\mathbf{f}}_i^\ell \rangle + \langle h_i^{j_i}, \widehat{h}_i^\ell \rangle)$ in $\mathsf{H}_n^{q_{\mathsf{CT}}}$ are equal to that in G_1. Thus, thanks to the function-hiding property of gFE, $\{\mathsf{gCT}_i^j, \mathsf{gSK}^\ell\}$ generated in $\mathsf{H}_n^{q_{\mathsf{CT}}}$ and those generated in G_1 are computationally indistinguishable. Hence, $\mathcal{A}$'s views in $\mathsf{H}_n^{q_{\mathsf{CT}}}$ and G_1 are computationally indistinguishable. □

References

1. Abdalla, M., Benhamouda, F., Gay, R.: From single-input to multi-client inner-product functional encryption. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part III. LNCS, vol. 11923, pp. 552–582. Springer, Heidelberg (Dec 2019)
2. Abdalla, M., Benhamouda, F., Kohlweiss, M., Waldner, H.: Decentralizing inner-product functional encryption. In: Lin, D., Sako, K. (eds.) PKC 2019, Part II. LNCS, vol. 11443, pp. 128–157. Springer, Heidelberg (Apr 2019)
3. Abdalla, M., Bourse, F., De Caro, A., Pointcheval, D.: Simple functional encryption schemes for inner products. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 733–751. Springer, Heidelberg (Mar / Apr 2015)
4. Abdalla, M., Catalano, D., Fiore, D., Gay, R., Ursu, B.: Multi-input functional encryption for inner products: Function-hiding realizations and constructions without pairings. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part I. LNCS, vol. 10991, pp. 597–627. Springer, Heidelberg (Aug 2018)
5. Abdalla, M., Catalano, D., Gay, R., Ursu, B.: Inner-product functional encryption with fine-grained access control. IACR Cryptol. ePrint Arch. 2020, 577 (2020), https://eprint.iacr.org/2020/577
6. Abdalla, M., Gay, R., Raykova, M., Wee, H.: Multi-input inner-product functional encryption from pairings. In: Coron, J., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part I. LNCS, vol. 10210, pp. 601–626. Springer, Heidelberg (Apr / May 2017)
7. Agrawal, S., Clear, M., Frieder, O., Garg, S., O'Neill, A., Thaler, J.: Ad hoc multi-input functional encryption. In: Vidick, T. (ed.) ITCS 2020. vol. 151, pp. 40:1–40:41. LIPIcs (Jan 2020)
8. Agrawal, S., Libert, B., Stehlé, D.: Fully secure functional encryption for inner products, from standard assumptions. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part III. LNCS, vol. 9816, pp. 333–362. Springer, Heidelberg (Aug 2016)
9. Badrinarayanan, S., Gupta, D., Jain, A., Sahai, A.: Multi-input functional encryption for unbounded arity functions. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 27–51. Springer, Heidelberg (Nov / Dec 2015)

10. Baltico, C.E.Z., Catalano, D., Fiore, D., Gay, R.: Practical functional encryption for quadratic functions with applications to predicate encryption. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part I. LNCS, vol. 10401, pp. 67–98. Springer, Heidelberg (Aug 2017)
11. Bishop, A., Jain, A., Kowalczyk, L.: Function-hiding inner product encryption. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 470–491. Springer, Heidelberg (Nov / Dec 2015)
12. Boneh, D., Lewi, K., Raykova, M., Sahai, A., Zhandry, M., Zimmerman, J.: Semantically secure order-revealing encryption: Multi-input functional encryption without obfuscation. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 563–594. Springer, Heidelberg (Apr 2015)
13. Boneh, D., Sahai, A., Waters, B.: Functional encryption: Definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (Mar 2011)
14. Brakerski, Z., Komargodski, I., Segev, G.: Multi-input functional encryption in the private-key setting: Stronger security from weaker assumptions. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 852–880. Springer, Heidelberg (May 2016)
15. Carmer, B., Malozemoff, A.J., Raykova, M.: 5Gen-C: Multi-input functional encryption and program obfuscation for arithmetic circuits. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017. pp. 747–764. ACM Press (Oct / Nov 2017)
16. Chotard, J., Dufour Sans, E., Gay, R., Phan, D.H., Pointcheval, D.: Decentralized multi-client functional encryption for inner product. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part II. LNCS, vol. 11273, pp. 703–732. Springer, Heidelberg (Dec 2018)
17. Chotard, J., Dufour-Sans, E., Gay, R., Phan, D.H., Pointcheval, D.: Dynamic decentralized functional encryption. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2020, Part I. pp. 747–775. LNCS, Springer, Heidelberg (Aug 2020)
18. Datta, P., Dutta, R., Mukhopadhyay, S.: Functional encryption for inner product with full function privacy. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.) PKC 2016, Part I. LNCS, vol. 9614, pp. 164–195. Springer, Heidelberg (Mar 2016)
19. Datta, P., Okamoto, T., Tomida, J.: Full-hiding (unbounded) multi-input inner product functional encryption from the k-Linear assumption. In: Abdalla, M., Dahab, R. (eds.) PKC 2018, Part II. LNCS, vol. 10770, pp. 245–277. Springer, Heidelberg (Mar 2018)
20. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.L.: An algebraic framework for Diffie-Hellman assumptions. Journal of Cryptology 30(1), 242–288 (Jan 2017)
21. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer, Heidelberg (May 2013)
22. Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: 54th FOCS. pp. 40–49. IEEE Computer Society Press (Oct 2013)
23. Gay, R.: A new paradigm for public-key functional encryption for degree-2 polynomials. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part I. LNCS, vol. 12110, pp. 95–120. Springer, Heidelberg (May 2020)
24. Goldwasser, S., Gordon, S.D., Goyal, V., Jain, A., Katz, J., Liu, F.H., Sahai, A., Shi, E., Zhou, H.S.: Multi-input functional encryption. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 578–602. Springer, Heidelberg (May 2014)
25. Goyal, V., Jain, A., O'Neill, A.: Multi-input functional encryption with unbounded-message security. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 531–556. Springer, Heidelberg (Dec 2016)
26. Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from well-founded assumptions. IACR Cryptol. ePrint Arch. 2020, 1003 (2020), https://eprint.iacr.org/2020/1003
27. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (Apr 2008)
28. Kim, S., Lewi, K., Mandal, A., Montgomery, H., Roy, A., Wu, D.J.: Function-hiding inner product encryption is practical. In: Catalano, D., De Prisco, R. (eds.) SCN 18. LNCS, vol. 11035, pp. 544–562. Springer, Heidelberg (Sep 2018)
29. Libert, B., Titiu, R.: Multi-client functional encryption for linear functions in the standard model from LWE. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part III. LNCS, vol. 11923, pp. 520–551. Springer, Heidelberg (Dec 2019)
30. Lin, H.: Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 PRGs. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part I. LNCS, vol. 10401, pp. 599–629. Springer, Heidelberg (Aug 2017)

31. O'Neill, A.: Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556 (2010), http://eprint.iacr.org/2010/556
32. Tomida, J.: Tightly secure inner product functional encryption: Multi-input and function-hiding constructions. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part III. LNCS, vol. 11923, pp. 459–488. Springer, Heidelberg (Dec 2019)
33. Tomida, J., Abe, M., Okamoto, T.: Efficient functional encryption for inner-product values with full-hiding security. In: Bishop, M., Nascimento, A.C.A. (eds.) ISC 2016. LNCS, vol. 9866, pp. 408–425. Springer, Heidelberg (Sep 2016)

A Public-Key MQFE from IPFE

A.1 Definitions

Definition A.1 (Public-Key Multi-Input Functional Encryption). Let $\mathcal{F}$ be a function family such that, for all $f \in \mathcal{F}$, $f : \mathcal{X}_1 \times \cdots \times \mathcal{X}_n \to \mathcal{Z}$. An public-key MIFE scheme for $\mathcal{F}$, MIFE, consists of four algorithms.

$\mathsf{Setup}(1^\lambda)$**:** It takes a security parameter 1^λ and outputs a public parameter PP and a master secret key MSK. The other three algorithms implicitly takes PP as input.
$\mathsf{Enc}(i, x_i)$**:** It takes MSK, an index $i \in [n]$, and $x_i \in \mathcal{X}_i$ and outputs a ciphertext CT_i.
$\mathsf{KeyGen}(\mathsf{MSK}, f)$**:** It takes MSK, and $f \in \mathcal{F}$, and outputs a secret key SK.
$\mathsf{Dec}(\mathsf{CT}_1, \ldots, \mathsf{CT}_n, \mathsf{SK})$**:** It takes $\mathsf{CT}_1, \ldots, \mathsf{CT}_n$ and SK, and outputs a decryption value $d \in \mathcal{Z}$ or a symbol $\perp$.

When $n = 1$, we call it just a functional encryption (FE) scheme and omit the second argument of Enc.

Correctness. MIFE is *correct* if it satisfies the following condition. For all $\lambda \in \mathbb{N}$, $(x_1, \ldots, x_n) \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$, $f \in \mathcal{F}$, we have

$$\Pr\left[d = f(x_1, \ldots, x_n) \;\middle|\; \begin{array}{l} \mathsf{PP}, \mathsf{MSK} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{CT}_i \leftarrow \mathsf{Enc}(i, x_i) \\ \mathsf{SK} \leftarrow \mathsf{KeyGen}(\mathsf{MSK}, f) \\ d := \mathsf{Dec}(\mathsf{CT}_1, \ldots, , \mathsf{CT}_n, \mathsf{SK}) \end{array} \right] = 1.$$

Security. We define two indistinguishability-based security definitions for MIFE. For a stateful PPT adversary $\mathcal{A}$ and $\lambda \in \mathbb{N}$, let

$$\mathsf{P}^{\mathsf{MIFE},\beta}_{\mathcal{A},\mathsf{ad}}(\lambda) := \Pr\left[\beta' = 1 \;\middle|\; \begin{array}{l} \mathsf{PP}, \mathsf{MSK} \leftarrow \mathsf{Setup}(1^\lambda), \\ \beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{CT}}(\beta,\cdot), \mathsf{KeyGen}(\mathsf{MSK},\cdot)}(\mathsf{PP}, \{\mathsf{CT}^j_i\}_{i \in [n], j \in [q_{\mathsf{CT},i}]}) \end{array} \right].$$

$\mathcal{O}_{\mathsf{CT}}(\beta, \cdot)$ takes (i, x^0_i, x^1_i) and outputs $\mathsf{Enc}(i, x^\beta_i)$. Let $q_{\mathsf{CT},i}$ and q_{SK} be a number of queries to $\mathcal{O}_{\mathsf{CT}}(\beta, \cdot)$ with the form of $(i, *, *)$ and KeyGen, respectively. Let $S := \{i \in [n] \mid q_{\mathsf{CT},i} > 0\}$. We say that $\mathcal{A}$ is *admissible* if for all $I = (i_1, \ldots, i_t) \subseteq S$, $(i_{t+1}, \ldots, i_n) = [n] \backslash I$, $(j_{i_1}, \ldots, j_{i_t}) \in [q_{\mathsf{CT},i_1}] \times \cdots \times [q_{\mathsf{CT},i_t}]$, $\ell \in [q_{\mathsf{SK}}]$, $(x_{i_{t+1}}, \ldots, x_{i_n}) \in \mathcal{X}_{i_{t+1}} \times \cdots \times \mathcal{X}_{i_n}$, $\mathcal{A}$'s queries satisfy

$$f^\ell(\langle x^{j_{i_1},0}_{i_1}, \ldots, x^{j_{i_t},0}_{i_t}, x_{i_{t+1}}, \ldots, x_{i_n} \rangle) = f^\ell(\langle x^{j_{i_1},1}_{i_1}, \ldots, x^{j_{i_t},1}_{i_t}, x_{i_{t+1}}, \ldots, x_{i_n} \rangle)$$

where $\langle x_{i_1}, \ldots, x_{i_n} \rangle$ denotes a permutation such that x_i is moved to the i-th entry. MIFE is *adaptively secure* if, for all admissible PPT adversaries $\mathcal{A}$, the following advantage of $\mathcal{A}$ is negligible in λ: $\mathsf{Adv}^{\mathsf{MIFE}}_{\mathcal{A},\mathsf{ad}}(\lambda) := |\mathsf{P}^{\mathsf{MIFE},0}_{\mathcal{A},\mathsf{ad}}(\lambda) - \mathsf{P}^{\mathsf{MIFE},1}_{\mathcal{A},\mathsf{ad}}(\lambda)|$.

Definition A.2 (Bounded-Norm Inner Products over $\mathbb{Z}$). A function family $\mathcal{F}^{\mathsf{IP}}_{m,X,C}$ for bounded-norm inner products consist of functions $f : \mathcal{X}^m \to \mathbb{Z}$ where $\mathcal{X} = \{i \mid i \in \mathbb{Z}, |i| \leq X\}$. Each $f \in \mathcal{F}^{\mathsf{IP}}_{m,X,C}$ is specified by $\mathbf{c} \in \mathbb{Z}^m$ s.t. $||\mathbf{c}||_\infty \leq C$. Then, f specified by $\mathbf{c}$ is defined as $f(\mathbf{x}) := \langle \mathbf{c}, \mathbf{x} \rangle$.

A.2 Construction

Let $\mathsf{iFE} = (\mathsf{iSetup}, \mathsf{iEnc}, \mathsf{iKeyGen}, \mathsf{iDec})$ and $\mathsf{iFE}' = (\mathsf{iSetup}', \mathsf{iEnc}', \mathsf{iKeyGen}', \mathsf{iDec}')$ be an FE scheme for $\mathcal{F}^{\mathsf{IP}}_{m^2,X,C}$ and $\mathcal{F}^{\mathsf{IP}}_{m,X,C}$. For convenience, we introduce notations for computing matrix multiplication via IPFE. For $\mathbf{V} = (\mathbf{v}_1 || \cdots || \mathbf{v}_m)$, we denote $(\mathsf{iSK}_1, \dots, \mathsf{iSK}_m)$ by $\overrightarrow{\mathsf{iSK}}$ where $\mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}, \mathbf{v}_i)$ and this procedure by $\overrightarrow{\mathsf{iSK}} \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}, \mathbf{V})$. Similarly, for iCT for $\mathbf{x}$, we denote decryption of iCT with $\overrightarrow{\mathsf{iSK}}$ by $\mathsf{iDec}(\mathsf{iCT}, \overrightarrow{\mathsf{iSK}}) = (\mathsf{iDec}(\mathsf{iCT}, \mathsf{iSK}_1), \dots, \mathsf{iDec}(\mathsf{iCT}, \mathsf{iSK}_n))$. The public-key MQFE scheme $\mathsf{qFE} = (\mathsf{qSetup}, \mathsf{qEnc}, \mathsf{qKeyGen}, \mathsf{qDec})$ for $\mathcal{F}^{\mathsf{MQF}}_{m,n,X,C}$ can be constructed as follows.

$\mathsf{qSetup}(1^\lambda)$: It outputs $\mathsf{qPP}, \mathsf{qMSK}$ as follows:

$$(\mathsf{iPP}_i, \mathsf{iMSK}_i) \leftarrow \mathsf{iSetup}(1^\lambda),\ (\mathsf{iPP}'_{i,j}, \mathsf{iMSK}'_{i,j}) \leftarrow \mathsf{iSetup}'(1^\lambda)$$
$$\mathsf{qPP} := (\{\mathsf{iPP}_i\}_{i\in[n]}, \{\mathsf{iPP}'_{i,j}\}_{i,j\in[n],i\neq j}),\ \mathsf{qMSK} := (\{\mathsf{iMSK}_i\}_{i\in[n]}, \{\mathsf{iMSK}'_{i,j}\}_{i,j\in[n],i\neq j})$$

$\mathsf{qEnc}(i, \mathbf{x}_i \in \mathbb{Z}^m)$: It outputs qCT_i as follows:

$$\mathsf{iCT}_i \leftarrow \mathsf{iEnc}(\mathsf{iPP}_i, \mathbf{x}_i \otimes \mathbf{x}_i),\ \mathsf{iCT}'_{i,j} \leftarrow \mathsf{iEnc}'(\mathsf{iPP}'_{i,j}, \mathbf{x}_i)$$
$$\mathsf{qCT}_i := (\mathsf{iCT}_i, \{\mathsf{iCT}'_{i,j}\}_{j\in[n]\setminus\{i\}})$$

$\mathsf{qKeyGen}(\mathsf{qMSK}, \mathbf{c} \in \mathbb{Z}^{(mn)^2})$: Let $\mathbf{C} = \begin{pmatrix} \mathbf{C}_{1,1} & \cdots & \mathbf{C}_{1,n} \\ & \ddots & \\ \mathbf{C}_{n,1} & \cdots & \mathbf{C}_{n,n} \end{pmatrix} \in \mathbb{Z}^{mn\times mn}$ be a matrix such that $\mathbf{x}^\top \mathbf{C}\mathbf{x} = \langle \mathbf{c}, \mathbf{x} \otimes \mathbf{x}\rangle$. Let $\mathbf{c}_i$ be a vector such that $\mathbf{x}_i \mathbf{C}_{i,i} \mathbf{x}_i = \langle \mathbf{c}_i, \mathbf{x}_i \otimes \mathbf{x}_i \rangle$. It outputs qSK as follows:

$$\mathsf{iSK}_i \leftarrow \mathsf{iKeyGen}(\mathsf{iMSK}_i, \mathbf{c}_i),\ \overrightarrow{\mathsf{iSK}}'_{i,j} \leftarrow \mathsf{iKeyGen}'(\mathsf{iMSK}'_{i,j}, \mathbf{C}_{i,j} + \mathbf{C}_{j,i}^\top)$$
$$\mathsf{qSK} := (\mathbf{c}, \{\mathsf{iSK}_i\}_{i\in[n]}, \{\overrightarrow{\mathsf{iSK}}'_{i,j}\}_{i,j\in[n],i\neq j})$$

$\mathsf{qDec}(\mathsf{qCT}_1, , \dots, \mathsf{qCT}_n, \mathsf{qSK})$: Let $(\mathbf{C}_{i,j} + \mathbf{C}_{j,i}^\top)^+ \in \mathbb{Q}$ be the Moore-Penrose inverse of $\mathbf{C}_{i,j} + \mathbf{C}_{j,i}^\top$. It outputs z as follows:

$$\begin{aligned} z_i &:= \mathsf{iDec}(\mathsf{iPP}_i, \mathsf{iCT}_i, \mathsf{iSK}_i) \\ z_{i,j} &:= \mathsf{iDec}'(\mathsf{iPP}'_{i,j}, \mathsf{iCT}'_{i,j}, \overrightarrow{\mathsf{iSK}}'_{i,j})(\mathbf{C}_{i,j} + \mathbf{C}_{j,i}^\top)^+ \mathsf{iDec}'(\mathsf{iPP}'_{j,i}, \mathsf{iCT}'_{j,i}, \overrightarrow{\mathsf{iSK}}'_{j,i})^\top \\ z &:= \sum_{i\in[n]} z_i + \sum_{\substack{i,j\in[n] \\ i<j}} z_{i,j} \end{aligned}$$

Correctness. Due to the correctness of iFE and iFE', we have

$$\begin{aligned} z_i &= \mathbf{x}_i^\top \mathbf{C}_{i,i} \mathbf{x}_i \\ z_{i,j} &= \mathbf{x}_i^\top (\mathbf{C}_{i,j} + \mathbf{C}_{j,i}^\top)(\mathbf{C}_{i,j} + \mathbf{C}_{j,i}^\top)^+ (\mathbf{C}_{i,j} + \mathbf{C}_{j,i}^\top)\mathbf{x}_j = \mathbf{x}_i^\top (\mathbf{C}_{i,j} + \mathbf{C}_{j,i}^\top)\mathbf{x}_j \end{aligned}$$

Hence, we have $z = \mathbf{x}^\top \mathbf{C}\mathbf{x} = \langle \mathbf{c}, \mathbf{x} \otimes \mathbf{x} \rangle$ where $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_n)^\top$.

A.3 Security

Theorem A.1. *If* iFE *and* iFE' *are adaptively secure, then* qFE *is also adaptively secure.*

Proof (sketch). We can reduce the indistinguishability of qFE to that of iFE and iFE'. The admissibility of $\mathcal{A}$ guarantees that

$$\mathbf{x}_i^{j_i,0^\top} \mathbf{C}^\ell_{i,i} \mathbf{x}_i^{j_i,0} = \mathbf{x}_i^{j_i,1^\top} \mathbf{C}^\ell_{i,i} \mathbf{x}_i^{j_i,1}$$
$$\mathbf{x}_i^{j_i,0^\top} (\mathbf{C}^\ell_{i,\theta} + \mathbf{C}^{\ell^\top}_{\theta,i}) = \mathbf{x}_i^{j_i,1^\top} (\mathbf{C}^\ell_{i,\theta} + \mathbf{C}^{\ell^\top}_{\theta,i})$$

for all $i, \theta \in [n]$ s.t. $i \neq \theta$, $j_i \in [q_{\mathsf{CT},i}]$, $\ell \in [q_{\mathsf{SK}}]$. These conditions are exactly consistent with the query conditions in the reduction to iFE and iFE'.