Full-Hiding (Unbounded) Multi-Input Inner Product Functional Encryption from the k-Linear Assumption

Pratish Datta, Tatsuaki Okamoto, and Junichi Tomida

NTT Secure Platform Laboratories
Tokyo, 180-8585 Japan
{datta.pratish,okamoto.tatsuaki,Tomida.Junichi}@lab.ntt.co.jp

January 15, 2018

Abstract. This paper presents two *non-generic* and *practically efficient* private key *multi-input functional encryption* (MIFE) schemes for the multi-input version of the *inner product* functionality that are the *first* to achieve simultaneous message and function privacy, namely, the *full-hiding* security for a non-trivial multi-input functionality under *well-studied* cryptographic assumptions. Our MIFE schemes are built in bilinear groups of prime order, and their security is based on the standard k-*Linear* (k-LIN) assumption (along with the existence of semantically secure symmetric key encryption and pseudorandom functions). Our constructions support polynomial number of encryption slots (inputs) without incurring any super-polynomial loss in the security reduction. While the number of encryption slots in our first scheme is apriori bounded, our second scheme can withstand an *arbitrary* number of encryption slots. Prior to our work, there was no known MIFE scheme for a non-trivial functionality, even without function privacy, that can support an unbounded number of encryption slots without relying on any heavy-duty building block or little-understood cryptographic assumption.

Keywords: multi-input functional encryption, inner products, full-hiding security, unbounded arity, bilinear maps

1 Introduction

Functional encryption (FE) [BSW11,O'N10] is a new vision of modern cryptography that aims to overcome the potential limitation of the traditional encryption schemes, namely, the so called "all-or-nothing" control over decryption capabilities, i.e., parties holding the legitimate decryption key can recover the entire message encrypted within a ciphertext, whereas others can learn nothing. Specifically, FE offers additional flexibility by supporting restricted decryption keys which enable decrypters to learn specific functions of encrypted messages, without revealing any additional information. More precisely, an FE scheme for a function family $\mathcal{F}$ involves a setup authority which holds a master secret key and publishes public system parameters. An encrypter uses the public parameters (along with a secret encryption key provided by the setup authority in case of a private key scheme) to encrypt its message m belonging to some supported message space $\mathcal{M}$, creating a ciphertext CT. A decrypter may obtain a private decryption key SK corresponding to some function $f \in \mathcal{F}$ from the setup authority provided the authority deems that the decrypter is entitled for that key. Such a decryption key SK corresponding to certain decryption function f can be used to decrypt a ciphertext CT encrypting some message m to recover $f(m)$. The basic security requirement for an FE scheme is the privacy of encrypted messages against collusion of decrypters, i.e., an arbitrary number of decrypters cannot jointly retrieve any more information about an encrypted message beyond the union of what they each can learn individually.

Multi-input functional encryption (MIFE), introduced by Goldwasser et al. [GGG+14], is a generalization of FE to the setting of multi-input functions. An MIFE scheme has several encryption slots, and messages can be encrypted to different slots independently. A MIFE decryption key for an n-input function f simultaneously decrypts a set of n ciphertexts, each of which is encrypted with respect to one of the n input slots associated with f, to unveil the joint evaluation of f on the n messages encrypted within those n ciphertexts. Just like single-input FE the primary security requirement for an MIFE scheme as well is the privacy of encrypted messages against collusion attacks. However, unlike single-input FE, the formalization of this security notion in case of MIFE is somewhat subtle. In their pioneering work,

* This is the full version of an extended abstract that will appear in the proceedings of PKC 2018.

Goldwasser et al. [GGG+14] presented a rigorous framework to formally capture message privacy for MIFE, both in the public key and in the private key regimes.

MIFE is particularly useful in scenarios where informations, which need to be processed together during decryption, become available at different points of time or are supplied by different parties. In fact, MIFE can be employed in a wide range of applications pertaining to computation and mining over encrypted data coming from multiple sources. Examples include executing search queries over encrypted databases, processing encrypted streaming data, non-interactive differentially private data releases, multi-client delegation of computations to external servers, and many more. All of these applications are in fact relevant in both the public key and the private key regimes.

In view of its countless practical applications, a series of recent works have attempted to construct MIFE schemes based on various cryptographic tools. These constructions can be broadly classified into two categories. The first line of research has tried to build MIFE schemes for general multi-input functionalities, e.g., arbitrary polynomial-size circuits [GGG+14, AJ15, BKS16, GJO16, KS17] or Turing machines [BGJS15]. Unfortunately however, all such MIFE constructions rely on highly strong cryptographic primitives like indistinguishability obfuscation [BGI+01, GGH+16], single-input FE for general circuits [GGH+16, GGHZ16], or multilinear maps [GGH13, CLT13], neither of which is currently instantiable using efficient building blocks or under well-studied cryptographic assumptions. Consequently, a second line of research have emerged whose focus is to design concretely efficient MIFE schemes based on standard assumptions for specific multi-input functionalities, e.g., comparison [CLWW16,LW16,CLOZ16] or multi-input inner product [KLM+16,LL16,ARW17]. However, majority of the existing works on MIFE have concentrated merely on achieving the basic security notion, namely, message confidentiality.

Unfortunately, message confidentiality is not sufficient in several advanced applications of FE, rather privacy also needs to be ensured for the functions for which the decryption keys are issued. This is especially important in situations where the decryption functions themselves contain sensitive informations. Consider the following scenario: Suppose a hospital subscribes to an external cloud server for storing medical records of its patients. In order to ensure confidentiality of the records and, at the same time, remotely perform various computations on the outsourced data from time to time, a promising choice for the hospital is to use an FE scheme to encrypt the records locally prior to uploading to the cloud server. Now, suppose the hospital wishes to retrieve the list of all patients who is receiving treatment for a certain chronic disease from the cloud server. For this, the hospital needs to provide the cloud server a decryption key for the corresponding functionality. However, if the FE scheme used by the hospital possesses no function privacy, then the cloud server would get to know the functionality from the decryption key provided by the hospital. Thus, after performing the assigned computation, if the cloud server notices the name of some celebrity in the obtained list of patients, it would at once understand that the particular celebrity is suffering from such a chronic disease, and it may leak the information to the media possibly for financial gain. This is clearly undesirable from the privacy point of view.

In order to address such scenarios, several recent works have studied the notion of function privacy in the context of FE, both in the single-input setting [SSW09, AAB+13, BS15, ITZ15, BRS13a, BRS13b, BJK15,DDM16,TAO16,KLM+16,LV16,Lin17] and in the multi-input setting [BKS16, AJ15,KS17,Lin17]. Intuitively, function privacy demands that the decryption keys leak no additional information about the functions embedded within them, beyond what is revealed through decryption. However, it has been observed that the extent to which function privacy can be realized differs dramatically between the public key and the private key regimes. In fact, in the public key setting, where anyone can encrypt messages, only a weak form of function privacy can be realized [BRS13a,BRS13b,ITZ15]. More precisely, in order to capture function privacy for FE in the public key setting, the framework must assume that the functions come from a certain high-entropy distribution. On the contrary, function-private FE (both the single-input and the multi-input versions) has been shown to possess great potentials in the private key setting, not only as a stand-alone feature, but also as a very useful building block [ABSV15, AJ15, KSY15, LV16, Lin17, KS17]. Consequently, the research on function-private FE has been focused primarily on the private key setting. However, despite of its immense theoretical and practical significance, so far, there are only a handful of function-private FE schemes available in the literature that can be implemented in practice [BJK15, DDM16, TAO16, KLM+16, LV16, Lin17], and all of them have been designed for single-input functions, precisely, inner products. In case of function-private MIFE, the only known concrete construction is the recent one due to Lin [Lin17]. She has constructed a private key function-private MIFE scheme for computing inner products of arbitrary polynomial degree, where standard inner product is a degree 2 function. However, her construction employs multilinear maps, and thus is currently uninstantiable in practice.

In this work, our goal is to design practical private key function-private MIFE scheme supporting a polynomial number of encryption slots, incurring only polynomial loss in the security reduction. Goldwasser et al. [GGG+14] have already shown that private key MIFE for general functionalities supporting a polynomial number of encryption slots is equivalent to full-fledged indistinguishability obfuscation. Hence, it seems impossible to design such highly expressive MIFE scheme without a sub-exponential security loss [GGSW13]. In fact, all existing private key MIFE schemes for general functionalities [GGG+14, BKS16, AJ15, KS17] do suffer from at least a quasi-polynomial security loss to support even a poly-logarithmic number of encryption slots. Hence, we concentrate on a specific multi-input functionality that has a wide range of real-life applications, namely, the natural multi-input generalization of the inner product functionality. This functionality has been first considered by Abdalla et al. [ARW17]. Concretely, a multi-input inner product function $f_{\{\vec{y}_\iota\}_{\iota \in S}}$ is associated with a set S of encryption slot indices and vectors $\vec{y}_\iota \in \mathbb{Z}^m$ for all $\iota \in S$. It takes as input a set of vectors $\{\vec{x}_\iota\}_{\iota \in S}$ with the same index set S, where $\vec{x}_\iota \in \mathbb{Z}^m$ for all $\iota \in S$, and outputs $\sum_{\iota \in S} \vec{x}_\iota \cdot \vec{y}_\iota$, where $\vec{x}_\iota \cdot \vec{y}_\iota$ represents the inner product of the vectors $\vec{x}_\iota$ and $\vec{y}_\iota$ over $\mathbb{Z}$. It is required that the norm of each component inner product $\vec{x}_\iota \cdot \vec{y}_\iota$ is smaller than some upper bound $\mathscr{B}$. Observe that this functionality is different from the high-degree inner product functionality considered by Lin [Lin17]. The multi-input inner product functionality captures various important computations arising in the context of data-mining, e.g., computing weighted mean of informations supplied by different parties. Please refer to [ARW17] for a comprehensive exposure of the practical significance of the multi-input inner product functionality.

Abdalla et al. [ARW17] have presented an MIFE scheme for the multi-input inner product functionality described above in the private key setting, using bilinear groups of prime order. Their construction supports a fixed polynomial number of encryption slots and multi-input inner product functions associated with a fixed index set S of polynomial size, as well as incurs only a polynomial loss in the security reduction. Precisely, the index set S in their construction is of the form $S = [n] = \{1, \ldots, n\}$, where n is the number of encryption slots – a polynomial determined at the time of setup, for the multi-input inner product functions. Their construction achieves adaptive message privacy against arbitrary collusion, as per the framework of Goldwasser et al. [GGG+14], in the standard model under the well-studied k-*Linear* (k-LIN) assumption [Sha07]. Prior to the work of Abdalla et al. [ARW17], two independent works, namely, [KLM+16, LL16] were able to realize a two-input variant of their result, of which [KLM+16] achieved it in the generic group model. However, none of these constructions guarantee function privacy. In fact, in their paper [ARW17], Abdalla et al. have posed the construction of a function-private MIFE scheme for the multi-input inner product functionality based on the k-LIN assumption in prime order bilinear groups as an open problem.

Our Contributions

In this paper we solve the above open problem. More specifically, we construct two *concretely efficient* standard-model private key MIFE schemes for the multi-input inner product functionality in prime order bilinear groups that are the *first* to achieve *function privacy* under *well-studied* cryptographic assumptions. In fact, our constructions achieve the unified notion of message and function privacy, namely, the *full-hiding* security, formulated by Brakerski et al. [BKS16] in the context of private key MIFE by combining the corresponding notion in the context of private key single-input FE [AAB+13, BS15] with the framework for message privacy of MIFE [GGG+14], under the k-LIN assumption (along with the existence of semantically secure symmetric key encryption and pseudorandom functions). Both of our constructions support polynomial number of encryption slots and are free from any super-polynomial loss in the security reduction. Our MIFE schemes withstands any polynomial number of decryption key queries and any polynomial number of ciphertext queries for each encryption slot. We employ the elegant technique of dual pairing vector spaces (DPVS) introduced by Okamoto and Takashima [OT09, OT10], and are implementable using both symmetric and asymmetric bilinear groups. Just like [ARW17], our first construction supports an apriori fixed number of encryption slots and a fixed slot index set for the multi-input inner product functions. These limitations are removed in our second construction. More precisely, our second construction is capable of supporting an apriori *unbounded* number of encryption slots and multi-input inner product functions with *arbitrary* slot index sets of any polynomial size. In fact, this construction is the *first* MIFE scheme for a non-trivial functionality with an unbounded number of encryption slots, built using efficient cryptographic tools and under well-studied complexity assumptions. The only prior MIFE construction which achieves this feature [BGJS15] has been designed using heavy machineries and relies on little-understood cryptographic assumption like public-coin differing input obfuscation [IPS15].

Moreover, the MIFE construction of [BGJS15] has been developed in public key setting and possesses no function privacy.

Our MIFE constructions are very efficient. When instantiated under the Symmetric External Diffie-Hellman (SXDH) assumption ($k = 1$ version of the k-LIN assumption) and symmetric key encryption (SKE) whose secret key size is λ bits, the ciphertexts of our bounded MIFE scheme consist of $2m+3$ group elements and a λ-bit string, while the decryption keys consist of $n(2m+3)$ group elements. Note that these group elements are encrypted by SKE. The master secret key comprises of $n(2m+3)^2$ group elements and n λ-bit strings. The encryption incurs one time encryption of SKE and $2m+3$ exponentiations, while key generation algorithm incurs one time encryption of SKE and $n(2m+3)$ exponentiations. The decryption algorithm involves one time decryption of SKE and $n(2m+3)$ pairing operations followed by an exhaustive search step over a polynomial-size range of possible values. Here, m and n respectively denote the length of the vectors and the size of the index set associated with the multi-input inner product functionality. Observe that these figures are already in close compliance with the n-fold extension of the most efficient standard-model full-hiding single-input FE construction for inner products known till date, namely, the scheme by Lin [Lin17] (which is also designed under the SXDH assumption). The exhaustive search step in the decryption algorithm is reminiscent of all currently known bilinear-map based FE constructions for inner products, both in the single-input and in the multi-input settings. In unbounded scheme, the ciphertext size and decryption key size are the same as bounded scheme, while the master secret key consists of two pseudorandom function (PRF) keys and $(2m+3)^2$ group elements. The encryption incurs two PRF evaluations and $2m+3$ exponentiations, while the key generation algorithm incurs n times encryption of SKE, $2n$ PRF evaluations, and $n(2m+3)$ exponentiations. The decryption algorithm involves n times decryption of SKE and $n(2m+3)$ pairing operations followed by an exhaustive search step.

Our Techniques

We now explain the principal ideas underlying our MIFE constructions for the multi-input inner product functionality. In order to simplify the exposition, we ignore many technicalities in this overview.

Our bounded-arity scheme: Since, the multi-input inner product functionality is a multi-input generalization of its single-input version, a natural first step is to explore whether we can obtain a private key full-hiding n-input MIFE scheme for inner products by executing n parallel copies of a private key full-hiding FE scheme for inner products. The most efficient such scheme available in the literature is the one due to Lin [Lin17], which is based on the SXDH assumption. However, the construction is built upon the Decisional-Diffie-Hellman (DDH)-based construction of Abdalla et al. [ABDCP15] and is not readily amenable to the general k-LIN assumption. Moreover, the construction is built in a two step approach, namely, first constructing an FE scheme for inner products achieving only a weaker form of function privacy, and then bootstrapping to the full-hiding security by using the conversion of Lin and Vaikuntanathan [LV16]. We want to avoid such an approach, rather our goal is to design a direct construction of full-hiding MIFE for multi-input inner products. So, we start with the full-hiding single-input inner-product FE scheme proposed by Tomida et al. [TAO16]. This construction is direct, and while originally presented under a variant of the Decisional Linear (DLIN) assumption, seems naturally generalizable to the k-LIN assumption. Further, in terms of efficiency, this construction is next to the construction of Lin [Lin17] among the standard-model private key function-private FE constructions available in the literature [BJK15,DDM16,TAO16,Lin17]. Besides, this construction has the flexibility of being implementable in both symmetric and asymmetric bilinear groups.

First, let us briefly review the construction and proof idea of Tomida et al. [TAO16]. We assume familiarity with the DPVS framework for the rest of this section. (The background on DPVS is provided in Section 2.3.) The master secret key MSK in the construction of Tomida et al. [TAO16] consists of a pair of dual orthogonal bases $(\mathbb{B}, \mathbb{B}^*)$ of a $(2m+5)$-dimensional DPVS, where m is the length of the ciphertext and decryption key vectors. Out of the $2m+5$ dimensions, $m+4$ dimensions are utilized in the real construction, while the rest are used in performing various hybrid transitions in the security proof. Note that the use of such hidden dimensions is a powerful feature of the DPVS framework, and it has been proven to be instrumental in deducing various complex security proofs in the literature. The ciphertext CT of [TAO16] encrypting an m-dimensional vector $\vec{x}$ is given by $\text{CT} = (\vec{x}, \vec{0}^m, \vec{0}^2, \varphi_1, \varphi_2, 0)_{\mathbb{B}}$, where $\varphi_1, \varphi_2 \xleftarrow{\cup} \mathbb{F}_q$. On the other hand, the decryption key SK corresponding to some m-dimensional vector $\vec{y}$ is of the form $\text{SK} = (\vec{y}, \vec{0}^m, \gamma_1, \gamma_2, \vec{0}^2, 0)_{\mathbb{B}^*}$, where $\gamma_1, \gamma_2 \xleftarrow{\cup} \mathbb{F}_q$. Here, $(\vec{v})_{\mathbb{W}}$, for any vector $\vec{v}$ with entries

in $\mathbb{F}_q$ and any basis $\mathbb{W}$ of a DPVS, signifies the linear combination of the members of $\mathbb{W}$ using the entries of $\vec{v}$ as coefficients. The decryption algorithm works by computing $e(\mathrm{CT}, \mathrm{SK})$ followed by performing an exhaustive search step over a specified polynomial-size range to determine the output. The correctness readily follows by the dual orthogonality property of $(\mathbb{B}, \mathbb{B}^*)$.

Recall that in the full-hiding security experiment for single-input inner product FE [AAB+13, BS15], first the challenger $\mathcal{B}$ sets up the system and samples a random bit $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. Next, the adversary $\mathcal{A}$ is allowed to adaptively make any polynomial number of ciphertext and decryption key queries to $\mathcal{B}$. In order to make a ciphertext query, $\mathcal{A}$ submits a pair of message vectors $(\vec{x}_0, \vec{x}_1)$ to $\mathcal{B}$, while to make a decryption key query, $\mathcal{A}$ submits a pair of vectors $(\vec{y}_0, \vec{y}_1)$ to $\mathcal{B}$. Depending on the random bit β, $\mathcal{B}$ returns respectively an encryption of $\vec{x}_\beta$ and a decryption key for vector $\vec{y}_\beta$ to the adversary in response to the respective queries. Finally, the adversary has to correctly guess the random bit β to win the experiment. The restriction on the queries of $\mathcal{A}$ is that for all pairs of vectors $(\vec{x}_0, \vec{x}_1)$ for which a ciphertext query is made and for all pairs of vectors $(\vec{y}_0, \vec{y}_1)$ for which a decryption key query is made, it should hold that $\vec{x}_0 \cdot \vec{y}_0 = \vec{x}_1 \cdot \vec{y}_1$.

In order to prove security of the construction of [TAO16] in the above full-hiding model, the following hybrid transitions are performed: The initial hybrid is the real full-hiding experiment with the challenge bit $\beta = 0$, i.e., where the forms of the ciphertexts and decryption keys returned to $\mathcal{A}$ are respectively $\mathrm{CT}^* = (\vec{x}_0, \vec{0}^m, \vec{0}^2, \varphi_1, \varphi_2, 0)_{\mathbb{B}}$ and $\mathrm{SK}^* = (\vec{y}_0, \vec{0}^m, \gamma_1, \gamma_2, \vec{0}^2, 0)_{\mathbb{B}^*}$, while the final hybrid corresponds to the real full-hiding experiment with $\beta = 1$, i.e., where the forms of the ciphertexts and decryption keys returned to the adversary are of the form $\mathrm{CT}^* = (\vec{x}_1, \vec{0}^m, \vec{0}^2, \varphi_1, \varphi_2, 0)_{\mathbb{B}}$ and $\mathrm{SK}^* = (\vec{y}_1, \vec{0}^m, \gamma_1, \gamma_2, \vec{0}^2, 0)_{\mathbb{B}^*}$ respectively. Towards achieving this change, first, applying a combination of a computational change using the DLIN assumption, in conjunction with a conceptual transformation of the underlying bases, the form of the ciphertexts are altered one by one to $\mathrm{CT}^* = (\vec{x}_0, \vec{x}_1, \vec{0}^2, \varphi_1, \varphi_2, 0)_{\mathbb{B}}$. In the next step, applying another combination of computational and conceptual changes, the form of the queried decryption keys are changed one by one to the form $\mathrm{SK}^* = (\vec{0}^m, \vec{y}_1, \gamma_1, \gamma_2, \vec{0}^2, 0)_{\mathbb{B}^*}$. This is the most subtle transition step, and this is where we have to rely crucially on the restriction of the security model. More precisely, observe that before altering the decryption keys, decrypting the queried ciphertexts using the queried decryption keys result in $\vec{x}_0 \cdot \vec{y}_0$, whereas after the transformation, the decryption results are $\vec{x}_1 \cdot \vec{y}_1$. However, thanks to the restriction of the full-hiding security experiment, we can ensure that the decryption results in the two cases are the same, and thus the change cannot be detected through decryption. After this step, the forms of ciphertexts and decryption keys are further altered respectively to $\mathrm{CT}^* = (\vec{x}_1, \vec{x}_0, \vec{0}^2, \varphi_1, \varphi_2, 0)_{\mathbb{B}}$ and $\mathrm{SK}^* = (\vec{y}_1, \vec{0}^m, \gamma_1, \gamma_2, \vec{0}^2, 0)_{\mathbb{B}^*}$, with the help of another conceptual basis transformation. Once this step is executed, the forms of the queried ciphertexts are changed to $\mathrm{CT}^* = (\vec{x}_1, \vec{0}^m, \vec{0}^2, \varphi_1, \varphi_2, 0)_{\mathbb{B}}$ using a reverse transformation to the one used in the first step. Observe that this last step takes us to the experiment corresponding to $\beta = 1$.

Let us now consider an MIFE scheme for the n-input inner product functionality obtained by an n-fold extension of the above single-input scheme. More precisely, consider an n-input MIFE scheme having the following specifications: The master secret key MSK consists of n independently generated master secret keys for the single-input scheme, i.e., $\mathrm{MSK} = \{\mathrm{MSK}_\iota = (\mathbb{B}_\iota, \mathbb{B}_\iota^*)\}_{\iota \in [n]}$. The ciphertext of some vector $\vec{x}_\iota$ with respect to index $\iota \in [n]$ is simply a single-input FE ciphertext for $\vec{x}_\iota$ with respect to MSK_ι, i.e., the ciphertext has the form $\mathrm{CT}_\iota = (\iota, \boldsymbol{c}_\iota = (\vec{x}_\iota, \vec{0}^m, \vec{0}^2, \varphi_{\iota,1}, \varphi_{\iota,2}, 0)_{\mathbb{B}_\iota})$, where $\varphi_{\iota,1}, \varphi_{\iota,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$. On the other hand, a decryption key associated with a set of n vectors $\{\vec{y}_\iota\}_{\iota \in [n]}$ is given by a set of n decryption keys $\{\mathrm{SK}_\iota\}_{\iota \in [n]}$, where SK_ι is the single-input FE secret key for $\vec{y}_\iota$ with respect to MSK_ι, i.e., $\mathrm{SK} = \{\boldsymbol{k}_\iota = (\vec{y}_\iota, \vec{0}^m, \gamma_{\iota,1}, \gamma_{\iota,2}, \vec{0}^2, 0)_{\mathbb{B}_\iota^*}\}_{\iota \in [n]}$, where $\gamma_{\iota,1}, \gamma_{\iota,2} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for all $\iota \in [n]$. To decrypt a set of n ciphertexts $\{\mathrm{CT}_\iota\}_{\iota \in [n]}$ using a decryption key SK, one first computes $\prod_{\iota \in [n]} e(\boldsymbol{c}_\iota, \boldsymbol{k}_\iota)$, and then performs an exhaustive search step. It is easy to see that the correctness follows analogously to the single-input case.

However, one can readily observe that the above n-input extension is not secure. In particular, the construction leaks partial information. Precisely, notice that for each $\iota \in [n]$, one can easily recover $\vec{x}_\iota \cdot \vec{y}_\iota$ by computing $e(\boldsymbol{c}_\iota, \boldsymbol{k}_\iota)$, whereas ideally one should only be able to learn $\sum_{\iota \in [n]} \vec{x}_\iota \cdot \vec{y}_\iota$. Abdalla et al. [ARW17] also faced a similar challenge while constructing their MIFE scheme by building on a single input inner product FE scheme. In order to overcome this problem, they introduced additional randomness within ciphertexts and decryption keys. Precisely, in order to generate a ciphertext for vector $\vec{x}_\iota$ with respect to index $\iota \in [n]$, they encrypted the vector $(\vec{x}_\iota, z_\iota)$, where $z_1, \ldots, z_n \xleftarrow{\mathsf{U}} \mathbb{F}_q$ are included within the master secret key. Similarly, while preparing a decryption key for a set of n vectors $\{\vec{y}_\iota\}_{\iota \in [n]}$, they sampled a random value $r \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and generated single-input FE decryption keys for the vectors $(\vec{y}_\iota, r)$ for all $\iota \in$

$[n]$, and additionally create the component $k_T = g_T^{\sum_{\iota\in[n]} z_\iota r}$. We attempt to apply their trick to our setting. More precisely, we modify our MIFE construction as follows: We add one additional dimension in the dual orthogonal bases $(\mathbb{B}_\iota, \mathbb{B}_\iota^*)$ for each $\iota \in [n]$, i.e., they are now $(2m+6)$-dimensional. A ciphertext encrypting the vector $\vec{x}_\iota$ with respect to index $\iota \in [n]$ is of the form $\text{CT}_\iota = (\iota, \boldsymbol{c}_\iota = (\vec{x}_\iota, \vec{0}^m, z_\iota, \vec{0}^2, \varphi_{\iota,1}, \varphi_{\iota,2}, 0)_{\mathbb{B}_\iota})$, where $z_1, \ldots, z_n \xleftarrow{\mathsf{U}} \mathbb{F}_q$ are parts of MSK, and the decryption key corresponding to a set of n vectors $\{\vec{y}_\iota\}_{\iota\in[n]}$ is given by $\text{SK} = (\{\boldsymbol{k}_\iota = (\vec{y}_\iota, \vec{0}^m, r, \gamma_{\iota,1}, \gamma_{\iota,2}, \vec{0}^2, 0)_{\mathbb{B}_\iota^*}\}_{\iota\in[n]}, k_T = g_T^{\sum_{\iota\in[n]} z_\iota r})$. Decryption works by first computing $[\prod_{\iota\in[n]} e(\boldsymbol{c}_\iota, \boldsymbol{k}_\iota)]/k_T = g_T^{\sum_{\iota\in[n]} \vec{x}_\iota \cdot \vec{y}_\iota}$, and then performing an exhaustive search step to recover $\sum_{\iota\in[n]} \vec{x}_\iota \cdot \vec{y}_\iota$.

Let us now consider the security of the modified construction. For simplicity, assume that the adversary queries a single decryption key and a single ciphertext for each of the n encryption slots. The full-hiding security model for private key MIFE [BKS16] is an extension of its single-input counter part, but is significantly more complicated compared to it. Analogous to the single-input case, in this multi-input security model, in order to make a ciphertext query for the ι^{th} slot, the adversary has to submit a pair of vectors $(\vec{x}_{\iota,0}, \vec{x}_{\iota,1})$, whereas for making a decryption key query, the adversary has to submit a pair of sets of n vectors $(\{\vec{y}_{\iota,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,1}\}_{\iota\in[n]})$. However, unlike the single-input setting, now the restriction on the queries is that $\sum_{\iota\in[n]} \vec{x}_{\iota,0} \cdot \vec{y}_{\iota,0} = \sum_{\iota\in[n]} \vec{x}_{\iota,1} \cdot \vec{y}_{\iota,1}$. Let us try to argue security of our modified construction by taking a similar path to that taken by Tomida et al. [TAO16]. We start with the case where the challenge bit $\beta = 0$, i.e., when the ciphertexts and decryption key returned to the adversary have the form $\text{CT}_\iota^* = (\iota, \boldsymbol{c}_\iota^* = (\vec{x}_{\iota,0}, \vec{0}^m, z_\iota, \vec{0}^2, \varphi_{\iota,1}, \varphi_{\iota,2}, 0)_{\mathbb{B}_\iota})$, for $\iota \in [n]$, and $\text{SK}^* = (\{\boldsymbol{k}_\iota^* = (\vec{y}_{\iota,0}, \vec{0}^m, r, \gamma_{\iota,1}, \gamma_{\iota,2}, \vec{0}^2, 0)_{\mathbb{B}_\iota^*}\}_{\iota\in[n]}, k_T = g_T^{\sum_{\iota\in[n]} z_\iota r})$. Just like [TAO16], first, using a combination of computational changes using the DLIN assumption, in conjunction with a conceptual transformation to the underlying bases, we can alter the forms of all the ciphertexts to $\text{CT}_\iota^* = (\iota, \boldsymbol{c}_\iota^* = (\vec{x}_{\iota,0}, \vec{x}_{\iota,1}, z_\iota, \vec{0}^2, \varphi_{\iota,1}, \varphi_{\iota,2}, 0)_{\mathbb{B}_\iota})$. After this step is done, we would have to change the form of the queried decryption key SK^* so that the first $2m$ coefficients of each $\boldsymbol{k}_\iota^*$ become $(\vec{0}^m, \vec{y}_{\iota,1})$. In order to achieve this change, we first perform a computational change to $\boldsymbol{k}_\iota^*$, for each $\iota \in [n]$, with the help of the DLIN assumption to $\boldsymbol{k}_\iota^* = (\vec{y}_{\iota,0}, \vec{0}^m, r, \gamma_{\iota,1}, \gamma_{\iota,2}, \vec{0}^2, \omega_\iota)_{\mathbb{B}_\iota^*}$, where $\omega_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for all $\iota \in [n]$. Next, we need to perform a conceptual transformation to the underlying bases in each slot so that the first two m blocks of each $\boldsymbol{k}_\iota^*$ gets interchanged. However, this conceptual change would generate the term $\vec{x}_{\iota,0} \cdot \vec{y}_{\iota,0} - \vec{x}_{\iota,1} \cdot \vec{y}_{\iota,1}$ in the $(2m+6)^{\text{th}}$ coefficient of each ciphertext CT_ι. In the single-input case, such a term vanishes by the restriction on the ciphertext and decryption key queries. But, unlike the single-input case, now $\vec{x}_{\iota,0} \cdot \vec{y}_{\iota,0}$ is not guaranteed to be equal to $\vec{x}_{\iota,1} \cdot \vec{y}_{\iota,1}$ for all $\iota \in [n]$, and hence the term in the $(2m+6)^{\text{th}}$ coefficient does not vanish.

In order to overcome this problem, we modify the above construction by introducing a different randomness in each of the n component of the decryption key rather than using a same shared randomness across all the n components. More precisely, a decryption key corresponding to a set of n vectors $\{\vec{y}_\iota\}_{\iota\in[n]}$ has the form $\text{SK} = (\{\boldsymbol{k}_\iota = (\vec{y}_\iota, \vec{0}^m, r_\iota, \gamma_{\iota,1}, \gamma_{\iota,2}, \vec{0}^2, 0)_{\mathbb{B}_\iota^*}\}_{\iota\in[n]}, k_T = g_T^{\sum_{\iota\in[n]} z_\iota r_\iota})$, where $r_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for all $\iota \in [n]$. First, observe that this modification does not affect the correctness. Now, with this modification, we can resolve the above problem as follows: In the above conceptual change step, we transform the underlying bases in such a way that not only the first two m blocks of each $\boldsymbol{k}_\iota^*$ gets interchanged, but also each r_ι gets altered to $\widetilde{r}_\iota$, where $\widetilde{r}_\iota = r_\iota + [\vec{x}_{\iota,0} \cdot \vec{y}_{\iota,0} - \vec{x}_{\iota,1} \cdot \vec{y}_{\iota,1}]/z_\iota$. Observe that the $\widetilde{r}_\iota$'s are also distributed uniformly and independently over $\mathbb{F}_q$ since r_ι's are so. Also, this new basis transformation will create the additional term $[\vec{x}_{\iota,1} \cdot \vec{y}_{\iota,1} - \vec{x}_{\iota,0} \cdot \vec{y}_{\iota,0}]$ in the $(2m+6)^{\text{th}}$ coefficient of the queried ciphertext in each slot that would cancel out the term $[\vec{x}_{\iota,0} \cdot \vec{y}_{\iota,0} - \vec{x}_{\iota,1} \cdot \vec{y}_{\iota,1}]$. Further, notice that $\sum_{\iota\in[n]} z_\iota \widetilde{r}_\iota = \sum_{\iota\in[n]} z_\iota r_\iota$ by the restriction of the full-hiding security experiment of the multi-input setting, namely, $\sum_{\iota\in[n]} \vec{x}_{\iota,0} \cdot \vec{y}_{\iota,0} = \sum_{\iota\in[n]} \vec{x}_{\iota,1} \cdot \vec{y}_{\iota,1}$.

Note that our actual construction and security proof, which is presented under the general k-LIN assumption, is more subtle. In our actual construction, we observe that replacing the z_ι values with the scalar 1 and choosing the r_ι values associated with a decryption key under the restriction that $\sum_{\iota\in[n]} r_\iota = 0$ is sufficient to argue the security proof. As a result of this modification, we are able to remove the k_T

component from the decryption keys. Also, in the actual construction, we reduce the dimension of the underlying bases further by making a more careful use of the randomness.

Our unbounded-arity scheme: In our bounded-arity scheme, the setup algorithm makes n random dual orthogonal bases for n-input case, and stores them as a master secret key. The first problem is how to make these bases unboundedly from a master secret key, whose size is independent from n. Considering that our scheme is private-key MIPE, to get an idea of making them from a pseudorandom function is not difficult. That is, we prepare a randomly chosen pseudorandom function key as a master secret key in a setup phase, and in encryption or key generation, we can generate dual orthogonal bases from the pseudorandom function with its input being the slot index when they are needed. Actually, this naive idea works in a conditional full-hiding security model, where for each decryption key, all indices included in the decryption keys are queried in ciphertext query. The crucial point is that, for some decryption key queried by the adversary, if all indices that are included in the decryption key are queried in ciphertext query, then all corresponding vectors must satisfy some restrictions to avoid a trivial attack. Concretely, for each decryption key SK_S for a index set S and vectors $\{\vec{y}_\iota\}_{\iota\in S}$, all vectors $\vec{x}_\iota$ for slot $\iota \in S$ queried in ciphertext query, satisfy the following restriction s.t. $\sum_{\iota\in S} \vec{x}_{\iota,0}\cdot\vec{y}_{\iota,0} = \sum_{\iota\in S} \vec{x}_{\iota,1}\cdot\vec{y}_{\iota,1}$. When we construct our bounded-arity scheme, we first construct a scheme that is secure in the conditional full-hiding security model, and then we convert it into one that has full-hiding security with no conditions by a generic transformation, similarly to Abdalla et. al. [ARW17]. We leverage such a restriction in the proof of the underlying scheme.

In the conversion, we prepare a random bit string k_ι for each index. Next, we encrypt all decryption keys and ciphertexts of the underlying scheme with SKE using $K = \bigoplus_{\iota=1}^{n} k_\iota$ as a secret key. Then, we append the random bit string k_ι to ciphertexts for index ι. By the construction, if there exist some indices that are not queried in ciphertext query, an adversary cannot compute K and all ciphertexts and decryption keys are completely hidden from the adversary. Therefore we can exclude such a situation and focus on the conditional full-hiding security model. However, this generic transformation does not work in the unbounded arity-case, because a set of ciphertexts (or indices) needed for decryption differs by each decryption key. Then we do not know how to convert an unbounded-arity scheme secure under the conditional full-hiding security model into one with full-hiding security.

To solve this problem, we introduce a new construction and new proof techniques. Our solution inherits the spirit of the above technique due to Abdalla et. al. [ARW17], but is not completely generic. The basic scheme is that making use of pseudorandom functions as mentioned earlier. Then we introduce another pseudorandom function, which takes an index of slots ι as an input and outputs a random bit string k_ι, which is assigned for each index. Those bit strings are appended to corresponding ciphertexts like the above generic transformation, but we do not encrypt ciphertexts with SKE, or even cannot because it is impossible to decide which indices are needed for decryption in the unbounded case. Instead we encrypt each decryption key with SKE, using the all bit strings corresponding to the index set of decryption key, as a secret key of SKE in some way. We can see that if there are some indices which are not queried in ciphertext query (we call such indices as absent indices), then the decryption keys which contain absent indices will be completely hidden from the adversary. It is because to obtain the secret keys of SKE, the adversary needs all bit strings k_ι (or ciphertexts) for the corresponding indices.

In this construction, however, we cannot use a generic transformation because ciphertexts are not encrypted with SKE. Instead we consider a series of hybrids in the same manner as bounded-arity case for the security proof. During the hybrids, we encounter the problem that there are some decryption keys that have absent indices, and therefore these decryption keys and ciphertexts might not satisfy the restriction as explained above. To solve the problem, we leverage the power of SKE, and it enables us to go the hybrids ahead. More precisely, for the decryption keys that have absent indices, we use the power of SKE, and for the other decryption keys, we use the power of the basic scheme. But here, if we define the secret key of SKE to encrypt a decryption key for a set S as $\bigoplus_{\iota\in S} k_\iota$, likely to the generic transformation of the bounded case, we realize that we cannot make a reduction algorithm for SKE. This problem is mainly due to the flexibleness of decryption keys, that is, a set, which can be associated with secret keys, is not determined in the scheme. Observe that in the bounded case, the set is determined as $\{1,\ldots,n\}$. Consider the case where the adversary has a decryption key for a set $\{1,2,3\}$ (say K_{123}), one for $\{1,2\}$ (say K_{12}) and a ciphertext for index 3. Then the adversary cannot compute the secret key for these decryption keys, i.e., $K_{123} = \bigoplus_{\iota=1}^{3} k_\iota$ and $K_{12} = \bigoplus_{\iota=1}^{2} k_\iota$. However, the adversary has k_3, which is appended to the ciphertext for index 3, and knows $K_{123} = K_{12} \oplus k_3$. This correlation becomes a obstacle for the reduction. To circumvent this obstacle, we introduce another encrypting method. That

is, we iteratively encrypt a decryption key with SKE, making each bit strings k_ι be a secret key. Then such a correlation does not appear over every decryption key.

The final difficulty is that the adversary asks for decryption keys and ciphertexts in *adaptive manner*. Consequently, the challenger cannot know which type a queried decryption key will be, one that has absent indices or one does not, at the point where the decryption key is queried. Then we need to carefully construct reduction algorithms and evaluate successful probabilities of the reductions.

Concurrent Work

Concurrently and independently to our work, Abdalla et al. [ACF+17] have also considered the problem of constructing function-private MIFE scheme for the multi-input inner product functionality supporting a polynomial number of encryption slots under standard assumption. They have first presented a semi-generic scheme that achieves the full-hiding security only in a selective sense. They have subsequently overcome the selective restriction in a concrete instantiation of their semi-generic construction. However, similar to our first MIFE scheme, their construction can only support an apriori fixed number of encryption slots and a fixed slot index set for the multi-input inner product functions. Their concrete adaptively full-hiding MIFE scheme is built in prime order bilinear group setting under the k-MDDH assumption, which subsumes the k-LIN assumption used in our construction. When instantiated under the SXDH assumption, while our construction contains $4n(m^2-1)$ more field elements in the master secret key, it involves 2 and $2n+1$ less group elements in ciphertexts and decryption keys respectively compared to their scheme. On the other hand, our scheme incurs 2 and $2n+1$ less exponentiations in encryption and key generation procedures respectively, as well as requires $2n$ less pairing operations during decryption compared to theirs. Recall that m and n respectively denote the length of the vectors and the size of the index set associated with the multi-input inner product functionality.

2 Preliminaries

In this section we present various definitions and decisional problems used in this paper.

2.1 Notations

Let $\lambda \in \mathbb{N}$ denotes the security parameter and 1^λ be its unary encoding. Let $\mathbb{N}$ and $\mathbb{Z}$ denote the set of all positive integers and the set of all integers respectively, while $\mathbb{F}_q$, for any prime power $q \in \mathbb{N}$, denotes the finite field of integers modulo p. For $s \in \mathbb{N}$ and $t \in \mathbb{N} \cup \{0\}$ (with $t < s$), we let $[s] = \{1, \ldots, s\}$ and $[t, s] = \{t, \ldots, s\}$. For any set Z, $z \xleftarrow{\mathsf{U}} Z$ represents the process of uniformly sampling an element z from the set Z, and $|Z|$ signifies the size or cardinality of Z. For a probabilistic algorithm $\mathcal{R}$, we denote by $\varkappa = \mathcal{R}(\Theta; \Phi)$ the output of $\mathcal{R}$ on input Θ and the content of the random tape being Φ, while $\varkappa \xleftarrow{\mathsf{R}} \mathcal{R}(\Theta)$ represents the process of sampling $\varkappa$ from the output distribution of $\mathcal{R}$ on input Θ with a uniform random tape. On the other hand, for any deterministic algorithm $\mathcal{D}$, $\varkappa = \mathcal{D}(\Theta)$ denotes the output of $\mathcal{D}$ on input Θ. We use the abbreviation PPT to mean probabilistic polynomial-time. We assume that all the algorithms are given the unary representation 1^λ of the security parameter λ as input and will not write 1^λ explicitly as input of the algorithms when it is clear from the context. For any finite field $\mathbb{F}_q$ and $m \in \mathbb{N}$, let $\vec{v}$ denotes a vector $(v^{(1)}, \ldots, v^{(m)}) \in \mathbb{Z}^m$ or $\mathbb{F}_q^m$, where $v^{(j)} \in \mathbb{Z}$ or $\mathbb{F}_q$ respectively, for all $j \in [m]$. The all zero vectors in $\mathbb{F}_q^m$ will be denoted by $\vec{0}^m$. For any two vectors $\vec{v}, \vec{w} \in \mathbb{Z}^m$ or $\mathbb{F}_q^m$, $\vec{v} \cdot \vec{w}$ stands for the inner product of the vectors $\vec{v}$ and $\vec{w}$ over the integers, i.e., $\vec{v} \cdot \vec{w} = \sum_{j \in [m]} v^{(j)} w^{(j)} \in \mathbb{Z}$. For any multiplicative cyclic group $\mathbb{G}$ of order q and any generator $g \in \mathbb{G}$, let $\boldsymbol{u}$ represents the m-dimensional vector of group elements $(g^{v^{(1)}}, \ldots, g^{v^{(m)}}) \in \mathbb{G}^m$, for some $\vec{v} \in \mathbb{F}_q^m$. By $\mathbf{1}_{\mathbb{G}}^m$ we denote the m-dimensional vector $(1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}}) \in \mathbb{G}^m$, where $1_{\mathbb{G}}$ represents the identity element of the group $\mathbb{G}$. We use $A = (a_{j,t})_{\ell \times s}$ to represent a $\ell \times s$ matrix with entries $a_{j,t} \in \mathbb{F}_q$. By $A^\intercal$ we will signify the transpose of the matrix A, while by A^* the matrix $(A^{-1})^\intercal$. Let $\mathsf{GL}(\ell, \mathbb{F}_q)$ denotes the set of all $\ell \times \ell$ invertible matrices over $\mathbb{F}_q$. A function $\mathsf{negl} : \mathbb{N} \to \mathbb{R}^+$ is said to be *negligible* if for every $c \in \mathbb{N}$, there exists $T \in \mathbb{N}$ such that for all $\lambda \in \mathbb{N}$ with $\lambda > T$, $|\mathsf{negl}(\lambda)| < 1/\lambda^c$.

2.2 Some Essential Cryptographic Tools

Definition 2.1 (Pseudorandom Functions: PRFs): A pseudorandom function family $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$ with key space $\mathcal{K} = \{\mathcal{K}_\lambda\}_{\lambda\in\mathbb{N}}$, domain $\mathcal{X} = \{\mathcal{X}_\lambda\}_{\lambda\in\mathbb{N}}$, and range $\mathcal{Y} = \{\mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$ is a function family that consists of functions $F_\lambda : \mathcal{K}_\lambda \times \mathcal{X}_\lambda \to \mathcal{Y}_\lambda$. Let $\mathcal{R}_\lambda$ be a set of functions consists of all functions whose domain and range are $\mathcal{X}_\lambda$ and $\mathcal{Y}_\lambda$ respectively. For all PPT adversary $\mathcal{A}$, the following condition holds;

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathcal{A}}(\lambda) = \left|\mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}^{F(K,\cdot)}] - \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}^{R(\cdot)}]\right| \leq \mathsf{negl}(\lambda),$$

where $F \in \mathcal{F}_\lambda$, $K \xleftarrow{\mathsf{U}} \mathcal{K}_\lambda$, and $R \xleftarrow{\mathsf{U}} \mathcal{R}_\lambda$.

Definition 2.2 (Symmetric Key Encryption: SKE): A symmetric key encryption consists of a tuple of three PPT algorithms ($\mathsf{SKE.KeyGen}$, $\mathsf{SKE.Encrypt}$, $\mathsf{SKE.Decrypt}$). $\mathsf{SKE.KeyGen}$ takes 1^λ as an input and outputs a secret key K. $\mathsf{SKE.Encrypt}$ takes a secret key K and a message m and outputs a ciphertext c. $\mathsf{SKE.Decrypt}$ takes a secret key K and a ciphertext c and outputs a message m'. Correctness of SKE is that

$$\Pr[m = m' | K \xleftarrow{\mathsf{R}} \mathsf{SKE.KeyGen}, m' = \mathsf{SKE.Decrypt}(K, \mathsf{SKE.Encrypt}(K, m))] = 1.$$

A semantically secure symmetric key encryption scheme satisfies the following condition. For all PPT adversary $\mathcal{A}$,

$$\mathsf{Adv}^{\mathrm{SKE}}_{\mathcal{A}}(\lambda) = \left|\mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_0(\cdot)}] - \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_1(\cdot)}]\right| \leq \mathsf{negl}(\lambda),$$

where an oracle $\mathcal{O}_{\beta\in\{0,1\}}$ chooses a random secret key K as $K \xleftarrow{\mathsf{R}} \mathsf{SKE.KeyGen}$ and when it takes a pair of messages (m_0, m_1), it returns $\mathsf{SKE.Encrypt}(K, m_\beta)$.

2.3 Bilinear Groups and Dual Pairing Vector Spaces

Definition 2.3 (Bilinear Group): A bilinear group $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$ is a tuple of a prime integer $q \in \mathbb{N}$; cyclic multiplicative groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of order q each with polynomial-time computable group operations; generators $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$; and a polynomial-time computable non-degenerate bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, i.e., e satisfies the following two properties:

- *Bilinearity*: $e(g_1^\zeta, g_2^\eta) = e(g_1, g_2)^{\zeta\eta}$ for all $\zeta, \eta \in \mathbb{F}_q$.
- *Non-degeneracy*: $e(g_1, g_2) \neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ denotes the identity element of the group $\mathbb{G}_T$.

There are three types of bilinear groups according as whether efficient isomorphisms exist or not between $\mathbb{G}_1$ and $\mathbb{G}_2$ [GPS08]. In case of type 1 bilinear groups, both the isomorphisms $\phi : \mathbb{G}_2 \to \mathbb{G}_1$ and its inverse $\phi^{-1} : \mathbb{G}_1 \to \mathbb{G}_2$ can be computed efficiently, i.e., $\mathbb{G}_1 \cong \mathbb{G}_2$. For type 2 groups, the isomorphism $\phi : \mathbb{G}_2 \to \mathbb{G}_1$ is efficiently computable but its inverse $\phi^{-1} : \mathbb{G}_1 \to \mathbb{G}_2$ is not. Type 3 groups, on the other hand, have no efficient isomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$. Type 1 bilinear groups are called *symmetric* bilinear groups, while type 2 and 3 groups are called *asymmetric* bilinear groups. Let $\mathcal{G}_{\mathrm{BPG}}$ be an algorithm that on input the unary encoding 1^λ of the security parameter λ, outputs a description $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$ of a bilinear group.

Definition 2.4 (Dual Pairing Vector Spaces: DPVS [OT09, OT10]): A dual pairing vector space (DPVS) $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e)$ by the direct product of a bilinear group $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$ is a tuple of a prime integer q; m-dimensional vector spaces $\mathbb{V}_\chi = \mathbb{G}_\chi^m$ over $\mathbb{F}_q$, for $\chi \in [2]$, under vector addition '$\boxplus$' and scalar multiplication '$\circ$' defined componentwise; canonical bases $\mathbb{A}_\chi = \{\boldsymbol{a}_{\chi,j} = (\overbrace{1_{\mathbb{G}_\chi}, \ldots, 1_{\mathbb{G}_\chi}}^{j-1}, g_\chi, \overbrace{1_{\mathbb{G}_\chi}, \ldots, 1_{\mathbb{G}_\chi}}^{m-j})\}_{j\in[m]}$ of $\mathbb{V}_\chi$, for $\chi \in [2]$, where $1_{\mathbb{G}_\chi}$ is the identity element of the group $\mathbb{G}_\chi$, for $\chi \in [2]$; and a pairing $e : \mathbb{V}_1 \times \mathbb{V}_2 \to \mathbb{G}_T$ defined by $e(\boldsymbol{v}, \boldsymbol{w}) = \prod_{j\in[m]} e(g_1^{v^{(j)}}, g_2^{w^{(j)}}) \in \mathbb{G}_T$, for all $\boldsymbol{v} = (g_1^{v^{(1)}}, \ldots, g_1^{v^{(q)}}) \in \mathbb{V}_1$, $\boldsymbol{w} = (g_2^{w^{(1)}}, \ldots, g_2^{w^{(q)}}) \in \mathbb{V}_2$. Observe that the newly defined map e is also non-degenerate bilinear, i.e., e satisfies the following two properties:

- *Bilinearity*: $e(\mu \circ \boldsymbol{v}, \eta \circ \boldsymbol{w}) = e(\boldsymbol{v}, \boldsymbol{w})^{\mu\eta}$, for $\mu, \eta \in \mathbb{F}_q$, $\boldsymbol{v} \in \mathbb{V}_1$, and $\boldsymbol{w} \in \mathbb{V}_2$.
- *Non-degeneracy*: If $e(\boldsymbol{v}, \boldsymbol{w}) = 1_{\mathbb{G}_T}$ for all $\boldsymbol{w} \in \mathbb{V}_2$, then $\boldsymbol{v} = \boldsymbol{0}^m_{\mathbb{G}_1}$.

We will often omit the symbol '$\circ$' for scalar multiplication and abuse '$+$' for the vector addition '$\boxplus$' when it is clear from the context. For any set $\mathbb{W} = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ of vectors in $\mathbb{V}_\chi$, for $\chi \in [2]$, and any vector $\vec{v} \in \mathbb{F}_q^m$, let $(\vec{v})_{\mathbb{W}}$ represents the vector in $\mathbb{V}_\chi$ formed by the linear combination of the members of $\mathbb{W}$ with the entries of $\vec{v}$ as the coefficients, i.e., $(\vec{v})_{\mathbb{W}} = \sum_{j \in [m]} v^{(j)} \boldsymbol{w}_j \in \mathbb{V}_\chi$. Also, for any vector $\boldsymbol{v} \in \mathbb{V}_\chi$, for $\chi \in [2]$, and any matrix $A = (a_{j,t})_{m \times m}$ with entries $a_{j,t} \in \mathbb{F}_q$, for $j, t \in [m]$, we denote by $\boldsymbol{v}A$ the m-dimensional vector $(g_\chi^{\sum_{j\in[m]} a_{j,1}v^{(j)}}, \ldots, g_\chi^{\sum_{j\in[m]} a_{j,m}v^{(j)}}) \in \mathbb{V}_\chi$. The DPVS generation algorithm $\mathcal{G}_{\text{DPVS}}$ takes input the unary encoded security parameter 1^λ, a dimension value $m \in \mathbb{N}$, along with a bilinear group $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{BPG}}()$, and outputs a description $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e)$ of DPVS with m-dimensional $\mathbb{V}_1$ and $\mathbb{V}_2$.

We now describe random *dual orthogonal* basis generator $\mathcal{G}_{\text{OB}}$ [OT09, OT10] in Fig. 2.1. This algorithm would be utilized as a sub-routine in our constructions.

$\mathcal{G}_{\text{OB}}(m, \mathsf{params}_{\mathbb{V}}, \nu)$: This algorithm takes as input the unary encoded security parameter 1^λ, a dimension value $m \in \mathbb{N}$, a m-dimensional DPVS $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{DPVS}}(m, \mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e))$, along with a random value $\nu \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$, and performs the following operations:

1. It first samples random $B = (b_{j,t})_{m \times m} \xleftarrow{\mathsf{U}} \mathsf{GL}(m, \mathbb{F}_q)$.
2. Next, it computes $B^\bigstar = (b^*_{j,t})_{m \times m} = \nu B^*$.
3. For all $j \in [m]$, let $\vec{b}_j$ and $\vec{b}^*_j$ represent the j^{th} row-vectors of B and $B^\bigstar$ respectively. It computes $\boldsymbol{b}_j = (\vec{b}_j)_{\mathbb{A}_1}, \boldsymbol{b}^*_j = (\vec{b}^*_j)_{\mathbb{A}_2}$, for $j \in [m]$, and sets
$$\mathbb{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}, \mathbb{B}^* = \{\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_m\}.$$
Clearly $\mathbb{B}$ and $\mathbb{B}^*$ form bases of the vector spaces $\mathbb{V}_1 = \mathbb{G}_1^m$ and $\mathbb{V}_2 = \mathbb{G}_2^m$ respectively. Also, note that $\mathbb{B}$ and $\mathbb{B}^*$ are dual orthogonal in the sense that for all $j, j' \in [m]$,
$$e(\boldsymbol{b}_j, \boldsymbol{b}^*_{j'}) = \begin{cases} g_T, & \text{if } j = j' \\ 1_{\mathbb{G}_T}, & \text{otherwise} \end{cases},$$
where $g_T = e(g_1, g_2)^\nu$.
4. It returns $(\mathbb{B}, \mathbb{B}^*)$.

Fig. 2.1: Dual Orthogonal Basis Generator $\mathcal{G}_{\text{OB}}$

2.4 Complexity Assumptions

Assumption 1 (k-Linear: k-LIN [Sha07]): Fix a number $\chi \in [2]$. The k-LIN problem is to guess a bit $\hat{\beta} \xleftarrow{\mathsf{U}} \{0,1\}$ given $\varepsilon_{\hat{\beta}} = (\mathsf{params}_{\mathbb{G}}, g_\chi^{\xi_1}, \ldots, g_\chi^{\xi_k}, g_\chi^{\delta_1\xi_1}, \ldots, g_\chi^{\delta_k\xi_k}, \Re_{\hat{\beta}})$; where $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{BPG}}()$; $\xi_1, \ldots, \xi_k, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$; $\delta_1, \ldots, \delta_k \xleftarrow{\mathsf{U}} \mathbb{F}_q$; and $\Re_{\hat{\beta}} = g_\chi^{\sum_{j\in[k]} \delta_j}$ or $g_\chi^{\sigma + \sum_{j\in[k]} \delta_j}$ according as $\hat{\beta} = 0$ or 1. The k-LIN assumption states that for any PPT algorithm $\mathcal{A}$, for any security parameter λ, the advantage of $\mathcal{F}$ in deciding the k-LIN problem,
$$\mathsf{Adv}^{k\text{-LIN}}_{\mathcal{A}}(\lambda) = \left| \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}(\varepsilon_0)] - \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}(\varepsilon_1)] \right| \leq \mathsf{negl}(\lambda),$$
for some negligible function negl.

We now define a set of decisional problems. We rely on the hardness of these problems for deriving security of our constructions.

Definition 2.5 (Problem 1): Problem 1 is to guess a bit $\hat{\beta} \xleftarrow{\mathsf{U}} \{0,1\}$ given $\varrho_{\hat{\beta}} = (\mathsf{params}_{\mathbb{V}}, g_T, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota\in[n]}, \{\boldsymbol{\Upsilon}_{\iota,\hat{\beta}}\}_{\iota\in[n]})$; where $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{BPG}}()$; $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{DPVS}}(2m + 2k + 1, \mathsf{params}_{\mathbb{G}})$; $\nu \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$; $g_T = e(g_1, g_2)^\nu$;$(\mathbb{B}_\iota, \mathbb{B}^*_\iota) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{OB}}(2m + 2k + 1, \mathsf{params}_{\mathbb{V}}, \nu)$; $\widehat{\mathbb{B}}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+1}, \boldsymbol{b}_{\iota,2m+k+1}, \ldots, \boldsymbol{b}_{\iota,2m+2k}\}$, $\widehat{\mathbb{B}}^*_\iota = \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+k}\}$, for $\iota \in [n]$;

$\alpha_1, \ldots, \alpha_k \xleftarrow{\mathsf{U}} \mathbb{F}_q$; $\Im \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$; and $\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\vec{0}^{2m+k}, \alpha_1, \ldots, \alpha_k, 0)_{\mathbb{B}_\iota}$ or $(\vec{0}^{2m+k}, \alpha_1, \ldots, \alpha_k, \Im)_{\mathbb{B}_\iota}$ according as $\hat{\beta} = 0$ or 1. For any PPT algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ in deciding Problem 1 is defined as

$$\mathsf{Adv}^{\mathrm{P}_1}_{\mathcal{A}}(\lambda) = \left| \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}(\varrho_0)] - \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}(\varrho_1)] \right|.$$

Definition 2.6 (Problem 1*): Problem 1* is to guess a bit $\hat{\beta} \xleftarrow{\mathsf{U}} \{0,1\}$ given $\varrho_{\hat{\beta}} = (\mathsf{params}_{\mathbb{V}}, g_T, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota\in[n]}, \{\boldsymbol{\Upsilon}_{\iota,\hat{\beta}}\}_{\iota\in[n]})$; where $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{BPG}}()$; $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{DPVS}}(2m + 2k + 1, \mathsf{params}_{\mathbb{G}})$; $\nu \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$; $g_T = e(g_1, g_2)^\nu$; $(\mathbb{B}_\iota, \mathbb{B}^*_\iota) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{OB}}(2m + 2k + 1, \mathsf{params}_{\mathbb{V}}, \nu)$, for $\iota \in [n]$; $\widehat{\mathbb{B}}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+1}, \boldsymbol{b}_{\iota,2m+k+1}, \ldots, \boldsymbol{b}_{\iota,2m+2k}\}$, $\widehat{\mathbb{B}}^*_\iota = \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+k}, \boldsymbol{b}^*_{\iota,2m+2k+1}\}$, for $\iota \in [n]$; $\alpha_1, \ldots, \alpha_k \xleftarrow{\mathsf{U}} \mathbb{F}_q$; $\Im \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$; and $\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\vec{0}^{2m}, \alpha_1, \ldots, \alpha_k, \vec{0}^k, 0)_{\mathbb{B}^*_\iota}$ or $(\vec{0}^{2m}, \alpha_1, \ldots, \alpha_k, \vec{0}^k, \Im)_{\mathbb{B}^*_\iota}$ according as $\hat{\beta} = 0$ or 1, for $\iota \in [n]$. For any PPT algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ in deciding Problem 1* is defined as

$$\mathsf{Adv}^{\mathrm{P}_{1^*}}_{\mathcal{A}}(\lambda) = \left| \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}(\varrho_0)] - \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}(\varrho_1)] \right|.$$

In Appendix A, we will justify the reducibility of the hardness of the two decisional problems described above to that of the k-LIN problem.

2.5 Notion of Full-Hiding Multi-Input Inner Product Functional Encryption

Definition 2.7 (Multi-Input Inner Product Functionality): An unbounded-arity multi-input inner product function family $\mathcal{F}^{m,\mathscr{B}}_\lambda = \{\mathcal{F}^{m,\mathscr{B}}_S\}$, for some $m, \mathscr{B} \in \mathbb{N}$, consists of the sub-families $\mathcal{F}^{m,\mathscr{B}}_S$ of bounded-arity multi-input inner product functions, where each subfamily $\mathcal{F}^{m,\mathscr{B}}_S$ is parameterized with an index set $S \subseteq [t(\lambda)]$ for any polynomial t, and contains functions $f_{\{\vec{y}_\iota\}_{\iota\in S}} : (\mathbb{Z}^m)^{|S|} \to \mathbb{Z}$ associated with sets of vectors $\{\vec{y}_\iota\}_{\iota\in S}$ such that each vector $\vec{y}_\iota \in \mathbb{Z}^m$, where $f_{\{\vec{y}_\iota\}_{\iota\in S}}(\{\vec{x}_\iota\}_{\iota\in S}) = \sum_{\iota\in S} \vec{x}_\iota \cdot \vec{y}_\iota$, for all sets of vectors $\{\vec{x}_\iota\}_{\iota\in S}$ such that each vector $\vec{x}_\iota \in \mathbb{Z}^m$ and the norm of the inner product $|\vec{x}_\iota \cdot \vec{y}_\iota| \leq \mathscr{B}$ for all $\iota \in S$.

Without loss of generality, when dealing with MIFE for some bounded-arity multi-input inner product function family $\mathcal{F}^{m,\mathscr{B}}_S$, we consider the associated index set S to be $[n]$, and denote the function family as $\mathcal{F}^{m,\mathscr{B}}_n$, where $n = |S|$.

Definition 2.8 (Full-Hiding Private Key Bounded-Arity Multi-Input Inner Product Functional Encryption: FH-MIPE): A full-hiding private key bounded-arity multi-input inner product functional encryption scheme for an inner product function family $\mathcal{F}^{m,\mathscr{B}}_n$ consists of the following polynomial-time algorithms:

- FH-MIPE.Setup$(m, n, \mathscr{B})$: This algorithm takes as input the unary encoded security parameter 1^λ, along with the length $m \in \mathbb{N}$ of vectors, the arity $n \in \mathbb{N}$ of the multi-input inner product functionality, and the bound $\mathscr{B} \in \mathbb{N}$ on the size of each component inner products. It generates a master secret key MSK and the corresponding public parameters PP. Observe that we are considering private key setting and hence PP is not sufficient to encrypt. It merely includes some public informations required for decryption, e.g., the group description in a bilinear-map-based construction.
- FH-MIPE.KeyGen$(\mathrm{PP}, \mathrm{MSK}, \{\vec{y}_\iota\}_{\iota\in[n]})$: On input the public parameters PP, the master secret key MSK, along with a set of n vectors $\{\vec{y}_\iota\}_{\iota\in[n]}$ such that $\vec{y}_\iota \in \mathbb{Z}^m$ for all $\iota \in [n]$, this algorithm outputs a decryption key SK.
- FH-MIPE.Encrypt$(\mathrm{PP}, \mathrm{MSK}, \iota, \vec{x}_\iota)$: This algorithm upon input the public parameters PP, the master secret key MSK, an index $\iota \in [n]$, and a vector $\vec{x}_\iota \in \mathbb{Z}^m_p$, outputs a ciphertext CT_ι, which includes the index ι in the clear.
- FH-MIPE.Decrypt$(\mathrm{PP}, \mathrm{SK}, \{\mathrm{CT}_\iota\}_{\iota\in[n]})$: On input the public parameters PP, a decryption key SK, along with a set of n ciphertexts $\{\mathrm{CT}_\iota\}_{\iota\in[n]}$, where for all $\iota \in [n]$, CT_ι is a ciphertext prepared for the ι^{th} index, this algorithm either outputs a value $\Lambda \in \mathbb{Z}$ or the distinguished symbol $\perp$ indicating failure.

The algorithm FH-MIPE.Decrypt is deterministic while all the others are probabilistic. The algorithms satisfy the following correctness and security requirements.

■ **Correctness**: An FH-MIPE scheme is correct if for any security parameter $\lambda \in \mathbb{N}$, any polynomial n in λ, any $m, \mathscr{B} \in \mathbb{N}$, any two sets of n vectors $\{\vec{x}_\iota\}_{\iota\in[n]}, \{\vec{y}_\iota\}_{\iota\in[n]}$ such that $\vec{x}_\iota, \vec{y}_\iota \in \mathbb{Z}^m$ with $|\vec{x}_\iota \cdot \vec{y}_\iota| \leq \mathscr{B}$ for all $\iota \in [n]$, we have

$$\mathsf{Pr}\Big[\mathsf{FH\text{-}MIPE.Decrypt}(\mathrm{PP}, \mathrm{SK}, \{\mathrm{CT}_\iota\}_{\iota\in[n]}) = \sum_{\iota\in[n]} \vec{x}_\iota \cdot \vec{y}_\iota :$$
$$(\mathrm{PP}, \mathrm{MSK}) \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.Setup}(m, n, \mathscr{B});$$
$$\mathrm{SK} \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.KeyGen}(\mathrm{PP}, \mathrm{MSK}, \{\vec{y}_\iota\}_{\iota\in[n]});$$
$$\{\mathrm{CT}_\iota \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.Encrypt}(\mathrm{PP}, \mathrm{MSK}, \iota, \vec{x}_\iota)\}_{\iota\in[n]}\Big] \geq 1 - \mathsf{negl}(\lambda),$$

for some negligible function negl.

■ **Full-Hiding Security**: The (indistinguishability-based) full-hiding security notion for a private key bounded-arity FH-MIPE scheme is formalized through the experiment $\mathsf{Expt}_{\mathcal{A}}^{\text{FH-MIPE}}(\beta)$, for random $\beta \xleftarrow{\mathsf{U}} \{0,1\}$, which involves a PPT adversary $\mathcal{A}$ and a PPT challenger $\mathcal{B}$. The experiment is described below:

Setup: $\mathcal{B}$ generates $(\mathrm{PP}, \mathrm{MSK}) \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.Setup}(m, n, \mathscr{B})$ and provides PP to $\mathcal{A}$.

Query Phase: $\mathcal{A}$ is allowed to adaptively make any polynomial number of queries of the following two types in arbitrary order:

- *Decryption key query*: In response to the i^{th} decryption key query of $\mathcal{A}$ corresponding to a pair of sets of vectors $(\{\vec{y}_{\iota,i,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,i,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1} \in \mathbb{Z}^m$ for all $\iota \in [n]$, $\mathcal{B}$ forms a decryption key $\mathrm{SK}_i^* \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.KeyGen}(\mathrm{PP}, \mathrm{MSK}, \{\vec{y}_{\iota,i,\beta}\}_{\iota\in[n]})$ and hands SK_i^* to $\mathcal{A}$.
- *Ciphertext query*: To answer a ciphertext query of $\mathcal{A}$ for the ι^{th} index corresponding to a pair of vectors $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}) \in (\mathbb{Z}^m)^2$, $\mathcal{B}$ prepares a ciphertext $\mathrm{CT}_{\iota,t_\iota}^* \xleftarrow{\mathsf{R}} \mathsf{FH.MIPE.Encrypt}(\mathrm{PP}, \mathrm{MSK}, \vec{x}_{\iota,t_\iota,\beta})$ and gives $\mathrm{CT}_{\iota,t_\iota}^*$ to $\mathcal{A}$.

Let the total number of decryption key query made by $\mathcal{A}$ be $q_{\mathrm{KEY}}(\geq 0)$ and the total number of ciphertext query made for the ι^{th} index be $q_{\mathrm{CT},\iota}(\geq 0)$. The restrictions on the queries of $\mathcal{A}$ are that if $q_{\mathrm{CT},\iota} \geq 1$ for all $\iota \in [n]$, then for all $i \in [q_{\mathrm{KEY}}]$ and for all $(t_1, \ldots, t_n) \in [q_{\mathrm{CT},1}] \times \ldots \times [q_{\mathrm{CT},n}]$, we must have

$$\sum_{\iota\in[n]} \vec{x}_{\iota,t_\iota,0} \cdot \vec{y}_{\iota,i,0} = \sum_{\iota\in[n]} \vec{x}_{\iota,t_\iota,1} \cdot \vec{y}_{\iota,i,1}. \tag{2.1}$$

Guess: $\mathcal{A}$ eventually outputs a guess bit $\beta' \in \{0,1\}$, which is the output of the experiment.

A private key FH-MIPE scheme is said to be full-hiding if for any PPT adversary $\mathcal{A}$, for any security parameter λ, the advantage of $\mathcal{A}$ in the above experiment,

$$\mathsf{Adv}_{\mathcal{A}}^{\text{FH-MIPE}}(\lambda) = \big|\mathsf{Pr}[\mathsf{Expt}_{\mathcal{A}}^{\text{FH-MIPE}}(0) = 1] - \mathsf{Pr}[\mathsf{Expt}_{\mathcal{A}}^{\text{FH-MIPE}}(1) = 1]\big| \leq \mathsf{negl}(\lambda),$$

for some negligible function negl.

Definition 2.9 (Full-Hiding Unbounded Private Key Multi-Input Inner Product Encryption: FH-UMIPE): An unbounded full-hiding private key multi-input inner product encryption scheme for an inner product function family $\mathcal{F}_\lambda^{m,\mathscr{B}}$ consists of the following polynomial-time algorithms:

- $\mathsf{FH\text{-}UMIPE.Setup}(m, \mathscr{B})$: This algorithm takes as input the unary encoded security parameter 1^λ, along with the length $m \in \mathbb{N}$ of vectors, and the bound $\mathscr{B} \in \mathbb{N}$ of each inner product values. It generates a master secret key MSK and the corresponding public parameters PP. It publishes PP, while keeps MSK to itself.
- $\mathsf{FH\text{-}UMIPE.KeyGen}(\mathrm{PP}, \mathrm{MSK}, S, \{\vec{y}_\iota\}_{\iota\in S})$: On input the public parameters PP, the master secret key MSK, a set of indices $S \subseteq [t(\lambda)]$ where t is any polynomial, along with an $|S|$-tuple of vectors $\{\vec{y}_\iota\}_{\iota\in S} \in (\mathbb{Z}^m)^{|S|}$, this algorithm provides a decryption key SK_S including the set S explicitly.
- $\mathsf{FH\text{-}UMIPE.Encrypt}(\mathrm{PP}, \mathrm{MSK}, \iota, \vec{x}_\iota)$: On input the public parameters PP, the master secret key MSK, an index $\iota \in [2^\lambda]$, and a vector $\vec{x}_\iota \in \mathbb{Z}^m$, outputs a ciphertext CT_ι, which includes the index ι in the clear.
- $\mathsf{FH\text{-}UMIPE.Decrypt}(\mathrm{PP}, \mathrm{SK}_S, \{\mathrm{CT}_\iota\}_{\iota\in S})$: On input the public parameters PP, a decryption key SK_S associated with S, along with a tuple of $|S|$ ciphertexts $\{\mathrm{CT}_\iota\}_{\iota\in S}$, where CT_ι is a ciphertext prepared for the index ι, a decrypter either outputs a value $\Lambda \in \mathbb{N}$ or the distinguished symbol $\perp$ indicating failure.

The algorithm FH-UMIPE.Decrypt is deterministic while all the others are probabilistic. The algorithms satisfy the following correctness and security requirements.

■ **Correctness**: An FH-UMIPE scheme is correct if for any $m, \mathscr{B}, \lambda \in \mathbb{N}$, any set of indices $S \subseteq [t(\lambda)]$, where t is any polynomial, any two $|S|$-tuples of vectors $\{\vec{x}_\iota\}_{\iota \in S}, \{\vec{y}_\iota\}_{\iota \in S} \in (\mathbb{Z}^m)^{|S|}$ with $|\vec{x}_\iota \cdot \vec{y}_\iota| \leq \mathscr{B}$ for all $\iota \in S$, we have

$$\begin{aligned}\mathsf{Pr}\Big[\mathsf{FH\text{-}UMIPE.Decrypt}(\mathrm{PP}, \mathrm{SK}_S, \{\mathrm{CT}_\iota\}_{\iota \in S}) = \sum_{\iota \in S} \vec{x}_\iota \cdot \vec{y}_\iota :\\ (\mathrm{PP}, \mathrm{MSK}) \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}UMIPE.Setup}(m, \mathscr{B});\\ \mathrm{SK}_S \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}UMIPE.KeyGen}(\mathrm{PP}, \mathrm{MSK}, S, \{\vec{y}_\iota\}_{\iota \in S});\\ \{\mathrm{CT}_\iota \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}UMIPE.Encrypt}(\mathrm{PP}, \iota, \vec{x}_\iota)\}_{\iota \in S}\Big] \geq 1 - \mathsf{negl}(\lambda)\end{aligned}$$

■ **Full-Hiding Security**: The (indistinguishability-based) full-hiding security notion for a private key FH-UMIPE scheme is formalized through the experiment $\mathsf{Expt}_{\mathcal{A}}^{\text{FH-UMIPE}}(\beta)$, for random $\beta \xleftarrow{\mathsf{U}} \{0,1\}$, which involves a PPT adversary $\mathcal{A}$ and a PPT challenger $\mathcal{B}$. The experiment is described below:

Setup: $\mathcal{B}$ generates $(\mathrm{PP}, \mathrm{MSK}) \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}UMIPE.Setup}(m, \mathscr{B})$ and gives PP to $\mathcal{A}$.

Query Phase: $\mathcal{A}$ is allowed to adaptively make any polynomial number of queries of the following two types in arbitrary order:

- *Decryption key query*: In response to the i^{th} decryption key query of $\mathcal{A}$ corresponding to a set of indices $S_i \subseteq [t(\lambda)]$ for any polynomial t and a pair of $|S_i|$-tuples of vectors $\{\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1}\}_{\iota \in S_i} \in ((\mathbb{Z}^m)^{|S_i|})^2$, $\mathcal{B}$ forms a decryption key $\mathrm{SK}^*_{S_i,i} \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}UMIPE.KeyGen}(\mathrm{PP}, \mathrm{MSK}, S_i, \{\vec{y}_{\iota,i,\beta}\}_{\iota \in S_i})$ and hands $\mathrm{SK}^*_{S_i,i}$ to $\mathcal{A}$.
- *Ciphertext query*: To answer a ciphertext query of $\mathcal{A}$ for the ι^{th} index corresponding to a pair of vectors $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}) \in (\mathbb{Z}^m)^2$, $\mathcal{B}$ prepares a ciphertext $\mathrm{CT}^*_{\iota,t_\iota} \xleftarrow{\mathsf{R}} \mathsf{UFH.MIPE.Encrypt}(\mathrm{PP}, \mathrm{MSK}, \vec{x}_{\iota,t_\iota,\beta})$ and gives $\mathrm{CT}^*_{\iota,t_\iota}$ to $\mathcal{A}$.

Let the total number of decryption key query made by $\mathcal{A}$ be $q_{\text{KEY}} (\geq 0)$ and the total number of ciphertext query made for the ι^{th} index be $q_{\text{CT},\iota} (\geq 0)$. The restrictions on the queries of $\mathcal{A}$ are that for each $i \in [q_{\text{KEY}}]$, if $q_{\text{CT},\iota} \geq 1$ for all $\iota \in S_i$, then for all $\{t_\iota\}_{\iota \in S_i} \in \prod_{\iota \in S_i} [q_{\text{CT},\iota}]$ we must have $\sum_{\iota \in S_i} \vec{x}_{\iota,t_\iota,0} \cdot \vec{y}_{\iota,i,0} = \sum_{\iota \in S_i} \vec{x}_{\iota,t_\iota,1} \cdot \vec{y}_{\iota,i,1}$.

Guess: $\mathcal{A}$ eventually outputs a guess bit $\beta' \in \{0,1\}$, which is the output of the experiment.

A private key FH-UMIPE scheme is said to be full-hiding if for any PPT adversary $\mathcal{A}$, for any security parameter λ, the advantage of $\mathcal{A}$ in the above experiment,

$$\mathsf{Adv}_{\mathcal{A}}^{\text{FH-UMIPE}}(\lambda) = \left|\mathsf{Pr}[\mathsf{Expt}_{\mathcal{A}}^{\text{FH-UMIPE}}(0) = 1] - \mathsf{Pr}[\mathsf{Expt}_{\mathcal{A}}^{\text{FH-UMIPE}}(1) = 1]\right| \leq \mathsf{negl}(\lambda),$$

for some negligible function negl.

3 The Proposed Full-Hiding Bounded Multi-Input Inner Product Functional Encryption Scheme

In this section, we present our FH-MIPE scheme.

3.1 Construction

FH-MIPE.Setup$(m, n, \mathscr{B})$: This algorithm takes as input the unary encoded security parameter 1^λ, the length $m \in \mathbb{N}$ of vectors, the arity $n \in \mathbb{N}$ of the multi-input inner product functionality, and the bound $\mathscr{B} \in \mathbb{N}$ on each component inner product. It proceeds as follows:

1. First, it generates a bilinear group $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{BPG}}()$ with $q \gg n\mathscr{B}$.
2. Next, it creates $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{DPVS}}(2m + 2k + 1, \mathsf{params}_{\mathbb{G}})$.
3. Then, it samples random $\nu \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$, and computes $g_T = e(g_1, g_2)^\nu$.

4. After that, for $\iota \in [n]$, it generates $(\mathbb{B}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+2k+1}\}, \mathbb{B}^*_\iota = \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+2k+1}\}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{OB}}(2m + 2k + 1, \mathsf{params}_{\mathbb{V}}, \nu)$ and sets

$$\widehat{\mathbb{B}}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,m}, \boldsymbol{b}_{\iota,2m+1}, \boldsymbol{b}_{\iota,2m+k+1}, \ldots, \boldsymbol{b}_{\iota,2m+2k}\},$$
$$\widehat{\mathbb{B}}^*_\iota = \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,m}, \boldsymbol{b}^*_{\iota,2m+1}, \ldots, \boldsymbol{b}^*_{\iota,2m+k}\}.$$

5. It publishes the public parameters $\text{PP} = (\mathsf{params}_{\mathbb{V}}, g_T)$, while sets the master secret key $\text{MSK} = \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota \in [n]}$.

$\mathsf{FH\text{-}MIPE.KeyGen}(\text{PP}, \text{MSK}, \{\vec{y}_\iota\}_{\iota \in [n]})$: On input the public parameters PP, the master secret key MSK, along with a set of n vectors $\{\vec{y}_\iota\}_{\iota \in [n]}$ such that $\vec{y}_\iota \in \mathbb{F}_q^m$, this algorithm executes the following steps:

1. First, it samples random $r_\iota, \gamma_{\iota,1}, \ldots, \gamma_{\iota,k-1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, for $\iota \in [n]$, subject to the restriction that $\sum_{\iota \in [n]} r_\iota = 0$.
2. Next, for each $\iota \in [n]$, it computes

$$\begin{aligned}\boldsymbol{k}_\iota &= \sum_{j \in [m]} y_\iota^{(j)} \boldsymbol{b}^*_{\iota,j} + r_\iota \boldsymbol{b}^*_{\iota,2m+1} + \sum_{j \in [k-1]} \gamma_{\iota,j} \boldsymbol{b}^*_{\iota,2m+1+j} \\ &= (\vec{y}_\iota, \vec{0}^m, r_\iota, \gamma_{\iota,1}, \ldots, \gamma_{\iota,k-1}, \vec{0}^k, 0)_{\mathbb{B}^*_\iota},\end{aligned}$$

   by making use of $\widehat{\mathbb{B}}^*_\iota$ extracted from MSK.
3. It outputs the decryption key $\text{SK} = \{\boldsymbol{k}_\iota\}_{\iota \in [n]}$.

$\mathsf{FH\text{-}MIPE.Encrypt}(\text{PP}, \text{MSK}, \iota, \vec{x}_\iota)$: Taking as input the public parameters PP, the master secret key MSK, an index $\iota \in [n]$, along with a vector $\vec{x}_\iota \in \mathbb{F}_q^m$, this algorithm performs the following steps:

1. It selects random $\varphi_{\iota,1}, \ldots, \varphi_{\iota,k} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and computes

$$\begin{aligned}\boldsymbol{c}_\iota &= \sum_{j \in [m]} x_\iota^{(j)} \boldsymbol{b}_{\iota,j} + \boldsymbol{b}_{\iota,2m+1} + \sum_{j \in [k]} \varphi_{\iota,j} \boldsymbol{b}_{\iota,2m+k+j} \\ &= (\vec{x}_\iota, \vec{0}^m, 1, \vec{0}^{k-1}, \varphi_{\iota,1}, \ldots, \varphi_{\iota,k}, 0)_{\mathbb{B}_\iota},\end{aligned}$$

   by utilizing $\widehat{\mathbb{B}}_\iota$ extracted from MSK.
2. It outputs the ciphertext $\text{CT}_\iota = (\iota, \boldsymbol{c}_\iota)$.

$\mathsf{FH\text{-}MIPE.Decrypt}(\text{PP}, \text{SK}, \{\text{CT}_\iota\}_{\iota \in [n]})$: This algorithm takes as input the public parameters PP, a decryption key $\text{SK} = \{\boldsymbol{k}_\iota\}_{\iota \in [n]}$, and a set of n ciphertexts $\{\text{CT}_\iota = (\iota, \boldsymbol{c}_\iota)\}_{\iota \in [n]}$. It does the following:

1. It first computes $L_T = \prod_{\iota \in [n]} e(\boldsymbol{c}_\iota, \boldsymbol{k}_\iota)$.
2. Then, it attempts to determine a value $\Lambda \in \mathbb{Z}$ such that $g_T^\Lambda = L_T$ by performing an exhaustive search over a specified polynomial-size range of possible values. If it succeeds, then it outputs Λ. Otherwise, it outputs $\perp$ indicating failure.

We emphasize that the polynomial running time of our decryption algorithm is guaranteed by restricting the output to lie within a fixed polynomial-size range. Note that similar exhaustive search step is used to determine the output in the decryption algorithm of all bilinear-map-based IPE constructions (both single and multi-input) available in the literature.

Remark 3.1: We would like to mention here that the FH-MIPE scheme described above can be proven to achieve the full-hiding security only when the adversary makes at least one ciphertext query for each of the n encryption indices, i.e., the restriction **??** is applicable. However, using a semantically secure SKE scheme, one can generically transform any FH-MIPE scheme that achieves full-hiding security under such restriction to one that achieves the full-hiding security even when the adversary makes no ciphertext query for some of the encryption slots. The transformation is rather straightforward and is presented in Remark B.1 in Appendix B.

■ **Correctness**: The correctness of the above FH-MIPE construction can be verified as follows: Observe that for any set of n ciphertexts $\{\text{CT}_\iota = (\iota, \boldsymbol{c}_\iota)\}_{\iota\in[n]}$, where $\text{CT}_\iota = (\iota, \boldsymbol{c}_\iota)$ encrypts some vector $\vec{\boldsymbol{x}}_\iota \in \mathbb{F}_q^m$ with respect to the index ι, for $\iota \in [n]$, and any decryption key $\text{SK} = \{\boldsymbol{k}_\iota\}_{\iota\in[n]}$ corresponding to a set of n vectors $\{\vec{\boldsymbol{y}}_\iota\}_{\iota\in[n]}$ such that $\vec{\boldsymbol{y}}_\iota \in \mathbb{F}_q^m$ for all $\iota \in [n]$, we have

$$L_T = \prod_{\iota\in[n]} e(\boldsymbol{c}_\iota, \boldsymbol{k}_\iota) = g_T^{\sum\limits_{\iota\in[n]} \vec{\boldsymbol{x}}_\iota \cdot \vec{\boldsymbol{y}}_\iota}.$$

This follows from the expressions of $\boldsymbol{c}_\iota, \boldsymbol{k}_\iota$, for $\iota \in [n]$, in conjunction with the fact that for each $\iota \in [n]$, $\mathbb{B}_\iota$ and $\mathbb{B}_\iota^*$ are dual orthogonal bases. Thus, if $\sum\limits_{\iota\in[n]} \vec{\boldsymbol{x}}_\iota \cdot \vec{\boldsymbol{y}}_\iota$ is contained within the specified polynomial-size range of possible values that the decryption algorithm searches, then the decryption algorithm would definitely output $\Lambda = \sum\limits_{\iota\in[n]} \vec{\boldsymbol{x}}_\iota \cdot \vec{\boldsymbol{y}}_\iota$ as desired.

3.2 Security

Theorem 3.1 (Security of our FH-MIPE Scheme): *Assume that the k-LIN problem is hard. Then, the* FH-MIPE *construction described above achieves full-hiding security under the restriction that the adversary makes at least one ciphertext query for each encryption index. Additionally, assuming the semantic security of the* SKE *scheme employed, the* FH-MIPE *scheme obtained by applying the generic transformation of Remark B.1 to the* FH-MIPE *scheme described above achieves full-hiding security without any restriction on the number of ciphertext queries per encryption slot. More formally, for any* PPT *adversary $\mathcal{A}$ against the full-hiding security of the* FH-MIPE *construction obtained by applying the generic transformation of Remark B.1 to the* FH-MIPE *scheme described above, there exists a* PPT *algorithm $\mathcal{B}_1$ against the k-LIN problem and a* PPT *adversary $\mathcal{B}_2$ against the simantic security of* SKE *such that for any security parameter λ, we have*

$$\mathsf{Adv}_{\mathcal{A}}^{\text{FH-MIPE}}(\lambda) \leq \big[4 \sum_{\iota\in[n]} q_{\text{CT},\iota} + 2q_{\text{KEY}}\big]\mathsf{Adv}_{\mathcal{B}_1}^{k\text{-LIN}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_2}^{\text{SKE}}(\lambda).$$

Proof: Here, we only proof the hull-hiding security of the above FH-MIPE scheme under the restriction that the adversary makes at least one ciphertext query per encryption slot. The proof of the scheme obtained after applying the generic conversion is sketched in Remark B.1.

The proof is structured as a hybrid argument over a series of experiments which differ in the construction of the decryption keys and/or ciphertexts queried by the adversary $\mathcal{A}$ in the full-hiding security model described in Definition 2.8. In the first hybrid experiment, the queried decryption keys and ciphertexts are constructed as those in the security experiment $\mathsf{Expt}_{\mathcal{A}}^{\text{FH-MIPE}}(0)$. We then progressively change the ciphertexts and decryption keys in multiple hybrid steps to those in the security experiment $\mathsf{Expt}_{\mathcal{A}}^{\text{FH-MIPE}}(1)$. We prove that each hybrid is indistinguishable from the previous one, thus proving the full-hiding security of the above FH-MIPE construction. Let q_{KEY} be the number of $\mathcal{A}$'s decryption key queries and $q_{\text{CT},\iota}$ (≥ 1), for $\iota \in [n]$, be the number of $\mathcal{A}$'s ciphertext queries for the ι^{th} index. As noted earlier, we consider $q_{\text{CT},\iota} \geq 1$ for all $\iota \in [n]$. The hybrid experiments are described below. In these hybrids, a part framed by a box indicates those terms which were modified in the transition from the previous game. The sequence of hybrid experiments follow:

► Sequence of Hybrid Experiments

$\mathsf{Hyb}_\mathbf{0}$: This experiment corresponds to the experiment $\mathsf{Expt}_{\mathcal{A}}^{\text{FH-MIPE}}(0)$ described in Definition 2.8, i.e., the full-hiding security experiment where the random bit used by the challenger $\mathcal{B}$ to generate queried ciphertexts and decryption keys is $\beta = 0$. More precisely, for all $\iota \in [n], t_\iota \in [q_{\text{CT},\iota}]$, in response to the $t_\iota{}^{\text{th}}$ ciphertext query of $\mathcal{A}$ with respect to index ι corresponding to pair of vectors $(\vec{\boldsymbol{x}}_{\iota,t_\iota,0}, \vec{\boldsymbol{x}}_{\iota,t_\iota,1}) \in (\mathbb{F}_q^m)^2$, $\mathcal{B}$ returns $\text{CT}_{\iota,t_\iota}^* = (\iota, \boldsymbol{c}_{\iota,t_\iota}^*)$, where

$$\boldsymbol{c}_{\iota,t_\iota}^* = (\vec{\boldsymbol{x}}_{\iota,t_\iota,0}, \vec{0}^m, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota}, \tag{3.1}$$

and for all $i \in [q_{\text{KEY}}]$, to answer the i^{th} decryption key query of $\mathcal{A}$ corresponding to pair of sets of n vectors $(\{\vec{\boldsymbol{y}}_{\iota,i,0}\}_{\iota\in[n]}, \{\vec{\boldsymbol{y}}_{\iota,i,1}\}_{\iota\in[n]})$ such that $\vec{\boldsymbol{y}}_{\iota,i,0}, \vec{\boldsymbol{y}}_{\iota,i,1} \in \mathbb{F}_q^m$, $\mathcal{B}$ generates $\text{SK}_i^* = \{\boldsymbol{k}_{\iota,i}^*\}_{\iota\in[n]}$, where

$$\boldsymbol{k}_{\iota,i}^* = (\vec{\boldsymbol{y}}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}_\iota^*}, \text{ for } \iota \in [n]. \tag{3.2}$$

Here, $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{BPG}}()$; $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{DPVS}}(2m + 2k+1, \mathsf{params}_{\mathbb{G}})$; $\nu \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$; $(\mathbb{B}_\iota, \mathbb{B}_\iota^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\text{OB}}(2m+2k+1, \mathsf{params}_{\mathbb{V}}, \nu)$, for $\iota \in [n]$; and $\varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}$, $r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for all $\iota \in [n], t_\iota \in [q_{\text{CT},\iota}], i \in [q_{\text{KEY}}]$, such that $\sum_{\iota \in [n]} r_{\iota,i} = 0$ for all $i \in [q_{\text{KEY}}]$.

Hyb_1 Sequence

$\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ ($\iota^* \in [n], \mu_{\iota^*} \in [q_{\mathbf{ct},\iota^*}]$): $\mathsf{Hyb}_{1,0,q_{\text{CT},0},3}$ coincides with Hyb_0. This experiment is the same as $\mathsf{Hyb}_{1,\iota^*-1,q_{\text{CT},\iota^*-1},3}$, if $\mu_{\iota^*} = 1$, or $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*}-1,3}$, if $\mu_{\iota^*} > 1$, with the only exception that in response to the $\mu_{\iota^*}{}^{\text{th}}$ ciphertext query of $\mathcal{A}$ with respect to index ι^* corresponding to pair of vectors $(\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{x}_{\iota^*,\mu_{\iota^*},1}) \in (\mathbb{F}_q^m)^2$, $\mathcal{B}$ returns $\text{CT}^*_{\iota^*,\mu_{\iota^*}} = (\iota^*, \boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}})$, where

$$\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}} = (\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{0}^m, 1, \vec{0}^{k-1}, \varphi_{\iota^*,\mu_{\iota^*},1}, \ldots, \varphi_{\iota^*,\mu_{\iota^*},k}, \boxed{\rho_{\iota^*,\mu_{\iota^*}}})_{\mathbb{B}_{\iota^*}}. \tag{3.3}$$

Here, $\rho_{\iota^*,\mu_{\iota^*}} \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$, and the other variables are formed as in $\mathsf{Hyb}_{1,\iota^*-1,q_{\text{CT},\iota^*-1},3}$ or $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*}-1,3}$ according as $\mu_{\iota^*} = 1$ or $\mu_{\iota^*} > 1$.

$\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},2}$ ($\iota^* \in [n], \mu_{\iota^*} \in [q_{\mathbf{ct},\iota^*}]$): This experiment is analogous to $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ except that to answer the $\mu_{\iota^*}{}^{\text{th}}$ ciphertext query of $\mathcal{A}$ with respect to index ι^* corresponding to pair of vectors $(\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{x}_{\iota^*,\mu_{\iota^*},1}) \in (\mathbb{F}_q^m)^2$, $\mathcal{B}$ generates $\text{CT}^*_{\iota^*,\mu_{\iota^*}} = (\iota^*, \boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}})$, where

$$\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}} = (\vec{x}_{\iota^*,\mu_{\iota^*},0}, \boxed{\vec{x}_{\iota^*,\mu_{\iota^*},1}}, 1, \vec{0}^{k-1}, \varphi_{\iota^*,\mu_{\iota^*},1}, \ldots, \varphi_{\iota^*,\mu_{\iota^*},k}, \rho_{\iota^*,\mu_{\iota^*}})_{\mathbb{B}_{\iota^*}}. \tag{3.4}$$

Here, all the variables are created as in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$.

$\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},3}$ ($\iota^* \in [n], \mu_{\iota^*} \in [q_{\mathbf{ct},\iota^*}]$): This experiment is exactly identical to $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},2}$ with the only exception that in response to the $\mu_{\iota^*}{}^{\text{th}}$ ciphertext query of $\mathcal{A}$ with respect to the index ι^* corresponding to pair of vectors $(\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{x}_{\iota^*,\mu_{\iota^*},1}) \in (\mathbb{F}_q^m)^2$, $\mathcal{B}$ returns $\text{CT}^*_{\iota^*,\mu_{\iota^*}} = (\iota^*, \boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}})$, where

$$\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}} = (\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{x}_{\iota^*,\mu_{\iota^*},1}, 1, \vec{0}^{k-1}, \varphi_{\iota^*,\mu_{\iota^*},1}, \ldots, \varphi_{\iota^*,\mu_{\iota^*},k}, \boxed{0})_{\mathbb{B}_{\iota^*}}. \tag{3.5}$$

Here, all the variables are created as in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},2}$.

Hyb_2 Sequence

$\mathsf{Hyb}_{2,\upsilon,1}$ ($\upsilon \in [q_{\mathbf{key}}]$): $\mathsf{Hyb}_{2,0,3}$ coincides with $\mathsf{Hyb}_{1,n,q_{\text{CT},n},3}$. This experiment is analogous to $\mathsf{Hyb}_{2,\upsilon-1,3}$ with the only exception that in response to the υ^{th} decryption key query of $\mathcal{A}$ corresponding to the pair of sets of n vectors $(\{\vec{y}_{\iota,\upsilon,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,\upsilon,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,\upsilon,0}, \vec{y}_{\iota,\upsilon,1} \in \mathbb{F}_q^m$ for all $\iota \in [n]$, $\mathcal{B}$ gives back $\text{SK}^*_\upsilon = \{\boldsymbol{k}^*_{\iota,\upsilon}\}_{\iota\in[n]}$, where

$$\boldsymbol{k}^*_{\iota,\upsilon} = (\vec{y}_{\iota,\upsilon,0}, \vec{0}^m, r_{\iota,\upsilon}, \gamma_{\iota,\upsilon,1}, \ldots, \gamma_{\iota,\upsilon,k-1}, \vec{0}^k, \boxed{\omega_{\iota,\upsilon}})_{\mathbb{B}^*_\iota}, \text{ for } \iota \in [n]. \tag{3.6}$$

Here, $\omega_{\iota,\upsilon} \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$ for all $\iota \in [n]$, such that $\sum_{\iota\in[n]} \omega_{\iota,\upsilon} = 0$, and all the other variables are generated as in $\mathsf{Hyb}_{2,\upsilon-1,3}$.

$\mathsf{Hyb}_{2,\upsilon,2}$ ($\upsilon \in [q_{\mathbf{key}}]$): This experiment is identical to $\mathsf{Hyb}_{2,\upsilon,1}$ except that in response to the υ^{th} decryption key query of $\mathcal{A}$ corresponding to the pair of sets of n vectors $(\{\vec{y}_{\iota,\upsilon,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,\upsilon,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,\upsilon,0}, \vec{y}_{\iota,\upsilon,1} \in \mathbb{F}_q^m$, $\mathcal{B}$ returns $\text{SK}^*_\upsilon = \{\boldsymbol{k}^*_{\iota,\upsilon}\}_{\iota\in[n]}$, where

$$\boldsymbol{k}^*_{\iota,\upsilon} = (\boxed{\vec{0}^m, \vec{y}_{\iota,\upsilon,1}, \widetilde{r}_{\iota,\upsilon}}, \gamma_{\iota,\upsilon,1}, \ldots, \gamma_{\iota,\upsilon,k-1}, \vec{0}^k, \omega_{\iota,\upsilon})_{\mathbb{B}^*_\iota}, \text{ for } \iota \in [n]. \tag{3.7}$$

Here, $\widetilde{r}_{\iota,\upsilon} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for all $\iota \in [n]$, such that $\sum_{\iota\in[n]} \widetilde{r}_{\iota,\upsilon} = 0$, and all the variables are generated as in $\mathsf{Hyb}_{2,\upsilon,1}$.

$\mathsf{Hyb}_{2,\upsilon,3}$ ($\upsilon \in [q_{\mathsf{key}}]$): This experiment is analogous to $\mathsf{Hyb}_{2,\upsilon,2}$ except that to answer the υ^{th} decryption key query of $\mathcal{A}$ corresponding to the pair of sets of n vectors $(\{\vec{y}_{\iota,\upsilon,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,\upsilon,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,\upsilon,0}, \vec{y}_{\iota,\upsilon,1} \in \mathbb{F}_q^m$, $\mathcal{B}$ gives back $\mathrm{SK}^*_\upsilon = \{\boldsymbol{k}^*_{\iota,\upsilon}\}_{\iota\in[n]}$, where

$$\boldsymbol{k}^*_{\iota,\upsilon} = (\vec{0}^m, \vec{y}_{\iota,\upsilon,1}, \widetilde{r}_{\iota,\upsilon}, \gamma_{\iota,\upsilon,1}, \ldots, \gamma_{\iota,\upsilon,k-1}, \vec{0}^k, \boxed{0})_{\mathbb{B}^*_\iota}, \text{ for } \iota \in [n]. \tag{3.8}$$

Here, all the variables are generated as in $\mathsf{Hyb}_{2,\upsilon,2}$.

Hyb_3: This experiment is identical to $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$ with the only exception that for all $\iota \in [n], t_\iota \in [q_{\mathrm{CT},\iota}]$, in response to the $t_\iota{}^{\text{th}}$ ciphertext query of $\mathcal{A}$ with respect to index ι corresponding to pair of vectors $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}) \in (\mathbb{F}_q^m)^2$, $\mathcal{B}$ returns $\mathrm{CT}^*_{\iota,t_\iota} = (\iota, \boldsymbol{c}^*_{\iota,t_\iota})$, where

$$\boldsymbol{c}^*_{\iota,t_\iota} = (\boxed{\vec{x}_{\iota,t_\iota,1}, \vec{x}_{\iota,t_\iota,0}}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota}, \tag{3.9}$$

and for all $i \in [q_{\mathrm{KEY}}]$, to answer the i^{th} decryption key query of $\mathcal{A}$ corresponding to pair of sets of n vectors $(\{\vec{y}_{\iota,i,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,i,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1} \in \mathbb{F}_q^m$, $\mathcal{B}$ generates $\mathrm{SK}^*_i = \{\boldsymbol{k}^*_{\iota,i}\}_{\iota\in[n]}$, where

$$\boldsymbol{k}^*_{\iota,i} = (\boxed{\vec{y}_{\iota,i,1}, \vec{0}^m}, \widetilde{r}_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}^*_\iota}, \text{ for } \iota \in [n]. \tag{3.10}$$

Here, all the variables are generated as in $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$.

Hyb_4: This experiment corresponds to the experiment $\mathsf{Expt}^{\text{FH-MIPE}}_{\mathcal{A}}(1)$ described in Definition 2.8, i.e., the full-hiding security experiment where the random bit used by $\mathcal{B}$ to generate the ciphertexts and decryption keys queried by $\mathcal{A}$ is $\beta = 1$.

► **Analysis**

Let us now denote by $\mathsf{Adv}^{(h)}_{\mathcal{A}}(\lambda)$ the advantage of the adversary $\mathcal{A}$, i.e., $\mathcal{A}$'s probability of outputting 1 in Hyb_h, for $h \in \{0, \{1, \iota^*, \mu_{\iota^*}, \jmath\}_{\iota^*\in[n],\mu_{\iota^*}\in[q_{\mathrm{CT},\iota^*}],\jmath\in[3]}, \{2, \upsilon, \jmath\}_{\upsilon\in[q_{\mathrm{KEY}}],\jmath\in[3]}, 3, 4\}$. Then, by the definitions of hybrids, we clearly have $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) \equiv \mathsf{Pr}[\mathsf{Expt}^{\text{FH-MIPE}}_{\mathcal{A}}(0) = 1]$, $\mathsf{Adv}^{(1,0,q_{\mathrm{CT},0},3)}_{\mathcal{A}}(\lambda) \equiv \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(2,0,3)}_{\mathcal{A}}(\lambda) \equiv \mathsf{Adv}^{(1,n,q_{\mathrm{CT},n},3)}_{\mathcal{A}}(\lambda)$, and $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) \equiv \mathsf{Pr}[\mathsf{Expt}^{\text{FH-MIPE}}_{\mathcal{A}}(1) = 1]$. Also, observe that the transition from Hyb_3 to Hyb_4 is essentially the reverse transition of the Hyb_1 sequence of hybrids with $\vec{x}_{\iota^*,\mu_{\iota^*},0}$ and $\vec{x}_{\iota^*,\mu_{\iota^*},1}$ interchanged. Therefore, it follows that

$$\begin{aligned}
\mathsf{Adv}^{\text{FH-MIPE}}_{\mathcal{A}}(\lambda) \leq 2 \sum_{\iota^*\in[n]} \Big[& |\mathsf{Adv}^{(1,\iota^*-1,q_{\mathrm{CT},\iota^*-1},3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1,\iota^*,1,1)}_{\mathcal{A}}(\lambda)| \\
& + \sum_{\mu_{\iota^*}\in[2,q_{\mathrm{CT},\iota^*}]} |\mathsf{Adv}^{(1,\iota^*,\mu_{\iota^*}-1,3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1,\iota^*,\mu_{\iota^*},1)}_{\mathcal{A}}(\lambda)| \\
& + \sum_{\mu_{\iota^*}\in[q_{\mathrm{CT},\iota^*}],\jmath\in[2,3]} |\mathsf{Adv}^{(1,\iota^*,\mu_{\iota^*},\jmath-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1,\iota^*,\mu_{\iota^*},\jmath)}_{\mathcal{A}}(\lambda)| \Big] \\
& + \sum_{\upsilon\in[q_{\mathrm{KEY}}]} \Big[|\mathsf{Adv}^{(2,\upsilon-1,3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2,\upsilon,1)}_{\mathcal{A}}(\lambda)| \\
& + \sum_{\jmath\in[2,3]} |\mathsf{Adv}^{(2,\upsilon,\jmath-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2,\upsilon,\jmath)}_{\mathcal{A}}(\lambda)| \Big] \\
& + |\mathsf{Adv}^{(2,q_{\mathrm{KEY}},3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)|.
\end{aligned} \tag{3.11}$$

We will formally argue that each term on the RHS of **??** is negligible in a sequence of lemmas (Lemmas C.1–C.7) in Appendix C. This completes the proof of Theorem 3.1. □

4 The Proposed Full-Hiding Unbounded Multi-Input Inner Product Functional Encryption Scheme

In this section, we present our FH-UMIPE scheme.

4.1 Construction

For the simplicity, we consider the scheme based on the SXDH(1-Lin) in this section. However, it is clear that we can instantiate our FH-UMIPE scheme from k-Lin assumption. We also consider the case where the vector length m is polynomial in λ. Let $F_1 : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \mathbb{F}_q^{(2m+3)\times(2m+3)}$ and $F_2 : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ be pseudorandom functions and (SKE.KeyGen, SKE.Encrypt, SKE.Decrypt) be a semantically secure secret key encryption scheme whose secret key space is $\{0,1\}^\lambda$. We require that SKE.KeyGen outputs a randomly chosen λ-bit string as a secret key K, i.e., $K \xleftarrow{\mathsf{U}} \{0,1\}^\lambda$. We abuse the notation such that for a set of N vectors of M dimensional DPVS $\mathbb{D} = (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_N)$ and $W \in \mathsf{GL}(M, \mathbb{F}_q)$, $\mathbb{B} = \mathbb{D}W$ denotes $\mathbb{B} = (\boldsymbol{d}_1 W, \ldots, \boldsymbol{d}_N W)$.

FH-UMIPE.Setup$(m, \mathscr{B})$: It takes as input the unary encoded security parameter 1^λ, the length $m \in \mathbb{N}$ of vectors, and the bound $\mathscr{B} \in \mathbb{N}$. It proceeds as follows:

1. First, it generates a bilinear group $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{BPG}}()$ with q a λ-bit prime.
2. Next, it forms $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{DPVS}}(2m+3, \mathsf{params}_{\mathbb{G}})$, samples $\nu \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}$, computes $g_T = e(g_1, g_2)^\nu$, generates $(\mathbb{D}, \mathbb{D}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{OB}}(2m+3, \mathsf{params}_{\mathbb{V}}, \nu)$, and samples PRF keys $K_1, K_2 \xleftarrow{\mathsf{U}} \{0,1\}^\lambda$. Then it sets $\widehat{\mathbb{D}} = (\boldsymbol{d}_1, \ldots, \boldsymbol{d}_m, \boldsymbol{d}_{2m+1}, \boldsymbol{d}_{2m+2}), \widehat{\mathbb{D}}^* = (\boldsymbol{d}_1^*, \ldots, \boldsymbol{d}_m^*, \boldsymbol{d}_{2m+1}^*)$.
3. It publishes the public parameters $\mathrm{PP} = (\mathsf{params}_{\mathbb{V}}, g_T)$, while keeps the master secret key $\mathrm{MSK} = (K_1, K_2, \widehat{\mathbb{D}}, \widehat{\mathbb{D}}^*)$.

FH-UMIPE.KeyGen$(\mathrm{PP}, \mathrm{MSK}, S, \{\vec{y}_\iota\}_{\iota \in S})$: On input the public parameters PP, the master secret key MSK, a set of indices $S \subseteq [t(\lambda)]$ for any polynomial t, along with a $|S|$-tuple of vectors $\{\vec{y}_\iota\}_{\iota \in S} \in (\mathbb{Z}^m)^{|S|}$, this algorithm executes the following steps:

1. First, it creates random dual orthogonal bases for the index $\iota \in S$ as follows;
$$W_\iota = F_1(K_1, \iota), \ \ \mathbb{B}_\iota^* = \mathbb{D}^* W_\iota^*.$$
If W_ι for some $\iota \in S$ is not a regular matrix, then it outputs $\perp$ and halts.
2. Next, for each $\iota \in S$, it computes decryption keys similarly to the bounded case;
$$\{r_\iota\}_{\iota \in S} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S} r_\iota = 0, \quad \boldsymbol{k}_\iota = (\vec{y}_\iota, \vec{0}^m, r_\iota, \vec{0}^2)_{\mathbb{B}_\iota^*}.$$
3. Let s_j be the j^{th} element of S in ascending order. Then it iteratively encrypts the decryption keys by symmetric key encryption as
$$\begin{aligned} C_1 &= \mathsf{SKE.Encrypt}(F_2(K_2, s_1), \{\boldsymbol{k}_\iota\}_{\iota \in S}), \\ C_2 &= \mathsf{SKE.Encrypt}(F_2(K_2, s_2), C_1), \\ &\vdots \\ C_{|S|} &= \mathsf{SKE.Encrypt}(F_2(K_2, s_{|S|}), C_{|S|-1}), \end{aligned}$$
and outputs $\mathrm{SK}_S = (C_{|S|}, S)$ as a decryption key for FH-UMIPE.

FH-UMIPE.Encrypt$(\mathrm{PP}, \mathrm{MSK}, \iota, \vec{x}_\iota)$: Taking as input the public parameters PP, the master secret key MSK, an index $\iota \in [2^\lambda]$, along with a vector $\vec{x}_\iota \in \mathbb{Z}^m$, this algorithm performs the following steps:

1. First, it creates random dual orthogonal bases for the index ι as follows;
$$W_\iota = F_1(K_1, \iota), \ \ \mathbb{B}_\iota = \mathbb{D} W_\iota.$$
If W_ι is not a regular matrix, then it outputs $\perp$ and halts.
2. Otherwise, it selects random $\kappa_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q$, computes
$$\boldsymbol{c}_\iota = (\vec{x}_\iota, \vec{0}^m, 1, \kappa_\iota, 0)_{\mathbb{B}_\iota}, \quad k_\iota = F_2(K_2, \iota),$$
and outputs the ciphertext $\mathrm{CT}_\iota = (\boldsymbol{c}_\iota, k_\iota, \iota)$.

FH-UMIPE.Decrypt$(\mathrm{PP}, \mathrm{SK}_S, \{\mathrm{CT}_\iota\}_{\iota \in S})$: A decrypter takes as input the public parameters PP, a decryption key SK_S for a set S, and a tuple of $|S|$ ciphertexts $\{\mathrm{CT}_\iota\}_{\iota \in S}$. It does the following:

1. It first decrypts decryption keys as follows;

$$\begin{aligned} C'_{|S|-1} &= \mathsf{SKE.Decrypt}(k_{s_{|S|}}, C_{|S|}), \\ &\vdots \\ C'_1 &= \mathsf{SKE.Decrypt}(k_{s_2}, C'_2), \\ \{\boldsymbol{k}'_\iota\}_{\iota\in S} &= \mathsf{SKE.Decrypt}(k_{s_1}, C'_1). \end{aligned}$$

2. Next, it computes $L_T = \prod_{\iota\in S} e(\boldsymbol{c}_\iota, \boldsymbol{k}'_\iota)$.

3. Then, it attempts to determine a value $\Lambda \in \mathbb{N}$ such that $g_T^\Lambda = L_T$ by performing an exhaustive search over a specified polynomial-size range of possible values. If it succeeds, then it outputs Λ. Otherwise, it outputs $\perp$ indicating failure.

■ **Correctness**: From the fact that $C_{|S|} = \mathsf{SKE.Encrypt}(F_2(K_2, s_{|S|}), C_{|S|-1})$ and $k_{s_{|S|}} = F_2(K_2, s_{|S|})$, we can easily confirm that $C'_{|S|-1} = \mathsf{SKE.Decrypt}(k_{s_{|S|}}, C_{|S|}) = C_{|S|-1}$ by the correctness of SKE. Iteratively, it is obvious that $C'_j = C_j$ for all $j \in [|S|-2]$ and $\{\boldsymbol{k}'_\iota\}_{\iota\in S} = \{\boldsymbol{k}_\iota\}_{\iota\in S}$. Then, the correctness of the above scheme holds in the almost same way as our bounded scheme, unless there exists an index $\iota \in S$ s.t. W_ι is a singular matrix. In other words, if for all polynomial-sized set S, the probability that there exists $\iota \in S$ s.t. W_ι is a singular matrix is negligible in λ, then the correctness of above scheme holds. We consider the next two probabilities.

$$P_0(\lambda, S) = \Pr\left[\exists \iota \in S, \mathrm{det} W_\iota = 0 \;\middle|\; \begin{array}{l} K_1 \xleftarrow{\mathsf{U}} \{0,1\}^\lambda \\ \forall \iota \in S, W_\iota = F_1(K_1, \iota) \end{array}\right],$$

$$P_1(\lambda, S) = \Pr\left[\exists \iota \in S, \mathrm{det} W_\iota = 0 \;\middle|\; \begin{array}{l} R_1 \xleftarrow{\mathsf{U}} \mathcal{R}_{1,\lambda} \\ \forall \iota \in S, W_\iota = R_1(\iota) \end{array}\right],$$

where $\mathcal{R}_{1,\lambda}$ is a set of all functions that have the same domain and range as F_1. For any polynomial-sized set S, suppose $P_1(\lambda, S)$ is negligible in λ. Then if $P_0(\lambda, S)$ is non-negligible function, we can easily break the PRF property by making an adversary which outputs 1 when there exists $\iota \in S$ s.t. W_ι is a singular matrix. Consequently, the last thing we have to confirm is that $P_1(\lambda, S)$ is negligible in λ for all polynomial-sized set S.

Lemma 4.1: *For $M, q \in \mathbb{N}$ s.t. $M < q$, $\Pr[\mathrm{det} W \neq 0 | W \xleftarrow{\mathsf{U}} \mathbb{F}_q^{M\times M}] \geq 1 - \frac{M}{q}$.*

Proof: The probability that all columns of W are linearly independent in $\mathbb{F}_q$, i.e., $\mathrm{det} W \neq 0$ is

$$\prod_{i=1}^{M}(1 - \frac{1}{q^i}) \geq (1 - \frac{1}{q})^M \geq 1 - \frac{M}{q}.$$

□

Lemma 4.2: *For $M, n, q \in \mathbb{N}$ s.t. $Mn < q$, $\Pr[\forall i \in [n], \mathrm{det} W_i \neq 0 | W_1, \ldots, W_n \xleftarrow{\mathsf{U}} \mathbb{F}_q^{M\times M}] \geq 1 - \frac{Mn}{q}$.*

Proof: From Lemma 4.1,

$$\Pr[\forall i \in [n], \mathrm{det} W_i \neq 0 | W_1, \ldots, W_n \xleftarrow{\mathsf{U}} \mathbb{F}_q^{M\times M}] \geq (1 - \frac{M}{q})^n \geq 1 - \frac{Mn}{q}.$$

□

From the above lemmas, we can see that $P_1(\lambda, S) \leq \frac{(2m+3)|S|}{q}$ where m and $|S|$ are polynomial in λ while q is exponential in λ. It means that $P_1(\lambda, S)$ is negligible in λ.

4.2 Security

Theorem 4.1 (Security of Our $\mathsf{FH\text{-}UMIPE}$ Scheme): *Assume that F_1 and F_2 are pseudorandom functions, SKE is semantically secure symmetric key encryption, and SXDH problem is hard, then our $\mathsf{FH\text{-}UMIPE}$ construction achieves full-hiding security. More formally, for any PPT adversary $\mathcal{A}$ against the full-hiding*

security of the proposed FH-UMIPE *construction, there exists a* PPT *algorithm* $\mathcal{B}_1$ *against the* SXDH *problem,* $\mathcal{B}_2$ *against the symmetric key encryption scheme, and* $\mathcal{B}_3$ *and* $\mathcal{B}_4$ *against the pseudorandom functions such that for any security parameter* λ*, we have*

$$\mathsf{Adv}^{\text{FH-UMIPE}}_{\mathcal{A}}(\lambda) \leq \big[4 \sum_{\iota \in [2^\lambda]} q_{\text{CT},\iota} + 2q_{\text{KEY}}\big]\mathsf{Adv}^{\text{SXDH}}_{\mathcal{B}_1}(\lambda) + n_{max} q_{\text{KEY}} \mathsf{Adv}^{\text{SKE}}_{\mathcal{B}_2}(\lambda) + 2\mathsf{Adv}^{\text{PRF}_1}_{\mathcal{B}_3}(\lambda) + 2\mathsf{Adv}^{\text{PRF}_2}_{\mathcal{B}_4}(\lambda),$$

where $q_{\text{CT},\iota}$ *is the total number of ciphertext query for the index* ι*,* q_{KEY} *is the total number of decryption key query, and* n_{max} *is the maximum index of a decryption key that* $\mathcal{A}$ *queries, i.e.,* $S_i \subseteq [n_{max}]$ *for all* $i \in [q_{\text{SK}}]$*.*

Proof: The proof of Theorem 4.1 is structured as a hybrid argument over a series of experiments which differ in the construction of the decryption keys and/or ciphertexts queried by the adversary $\mathcal{A}$ in the full-hiding security model described in Definition 2.9. The hybrid transition is proceeded in the similar way to the bounded scheme, that is, first we gradually change the ciphertext form from $(\vec{x}_{\iota,0}, \vec{0}^m, 1, \kappa_\iota, 0)_{\mathbb{B}_\iota}$ to $(\vec{x}_{\iota,0}, \vec{x}_{\iota,1}, 1, \kappa_\iota, 0)_{\mathbb{B}_\iota}$. After that, we change the decryption key form from $(\vec{y}_{\iota,0}, \vec{0}^m, r_\iota, \vec{0}^2)_{\mathbb{B}^*_\iota}$ to $(\vec{0}^m, \vec{y}_{\iota,1}, r_\iota, \vec{0}^2)_{\mathbb{B}^*_\iota}$. Then, switch the first m coefficients with the second m coefficients and restore the ciphertexts. The proof of the ciphertexts part is almost same as that of the bounded scheme, while the decryption key part is more complicated than the bounded one. The hybrid experiments are described below. In these hybrids, a part framed by a box indicates those terms which were modified in the transition from the previous game. The sequence of hybrid experiments follow:

► Sequence of Hybrid Experiments

Hyb_0: We denote the j^{th} element of S_i in ascending order by $s_{i,j}$. This experiment is the same as $\mathsf{Expt}^{\text{FH-UMIPE}}_{\mathcal{A}}(0)$ defined in Definition 2.9. That is, when the challenger receives $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1})$ from $\mathcal{A}$ as a $t_\iota{}^{\text{th}}$ ciphertext query for index ι, it returns $\text{CT}^*_{\iota,t_\iota} = (\boldsymbol{c}^*_{\iota,t_\iota}, k_\iota, \iota)$, where

$$\begin{aligned}
&W_\iota = F_1(K_1, \iota), \;\; \mathbb{B}_\iota = \mathbb{D}W_\iota, \\
&\kappa_{\iota,t_\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{c}^*_{\iota,t_\iota} = (\vec{x}_{\iota,t_\iota,0}, \vec{0}^m, 1, \kappa_{\iota,t_\iota}, 0)_{\mathbb{B}_\iota}, \quad k_\iota = F_2(K_2, \iota).
\end{aligned}$$

On the other hand, when the challenger receives $(S_i, \{\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1}\}_{\iota \in S_i})$ for i^{th} decryption key query, it returns $\text{SK}^*_{S_i,i} = (C_{|S_i|}, S_i)$, where

$$\begin{aligned}
&r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q \;\text{ s.t. } \sum_{\iota \in S_i} r_{\iota,i} = 0, \;\; W_\iota = F_1(K_1, \iota), \;\; \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,i} = (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \vec{0}^2)_{\mathbb{B}^*_\iota} \quad \text{for } \iota \in S_i, \\
&C_{|S_i|} = \mathsf{SKE.Encrypt}(F_2(K_2, s_{i,|S_i|}), \ldots, \mathsf{SKE.Encrypt}(F_2(K_2, s_{i,1}), \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in S_i}) \ldots).
\end{aligned}$$

Hyb_1: In this hybrids, we replace pseudorandom functions $F_i(K_i, \cdot)$ for $i \in \{1, 2\}$ with random functions $R_i(\cdot) \xleftarrow{\mathsf{U}} \mathcal{R}_{i,\lambda}$, where $\mathcal{R}_{i,\lambda}$ is a set of functions consists of all functions that have the same domain and range as F_i. Observe that all dual orthogonal bases used in the ciphertexts and decryption keys queried by $\mathcal{A}$ are completely independent and random ones by each index after Hyb_1.

Hyb_2: The all replies for the ciphertext queries are changed as follows;

$$\begin{aligned}
&W_\iota = R_1(\iota), \;\; \mathbb{B}_\iota = \mathbb{D}W_\iota, \\
&\kappa_{\iota,t_\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{c}^*_{\iota,t_\iota} = (\vec{x}_{\iota,t_\iota,0}, \boxed{\vec{x}_{\iota,t_\iota,1}}, 1, \kappa_{\iota,t_\iota}, 0)_{\mathbb{B}_\iota}, \quad k_\iota = R_2(\iota),
\end{aligned}$$

and returns $\text{CT}^*_{\iota,t_\iota} = (\boldsymbol{c}^*_{\iota,t_\iota}, k_\iota, \iota)$.

Hyb_3 Sequence

$\mathsf{Hyb}_{3,\upsilon}$ ($\upsilon \in [q_{\mathsf{key}}]$): $\mathsf{Hyb}_{3,0}$ is the same as Hyb_2. The challenger replies to the first υ decryption key queries, i.e., the i^{th} decryption key query for all $i \leq \upsilon$, as

$$
\begin{aligned}
&r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_i} r_{\iota,i} = 0, \ \ W_\iota = R_1(\iota), \ \ \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,i} = (\vec{0}^m, \boxed{\vec{y}_{\iota,i,1}}, r_{\iota,i}, \vec{0}^2)_{\mathbb{B}^*_\iota} \quad \text{for } \iota \in S_i, \\
&C_{|S_i|} = \mathsf{SKE.Encrypt}(R_2(s_{i,|S_i|}), \ldots, \mathsf{SKE.Encrypt}(R_2(s_{i,1}), \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in S_i}) \ldots),
\end{aligned}
$$

and returns $\mathrm{SK}^*_{S_i,i} = (C_{|S_i|}, S_i)$. For the other decryption key queries, the challenger replies the same way as Hyb_2.

Hyb_4: In this hybrid, we switch the coefficients of 1 to m^{th} vector with those of $m+1$ to $2m^{\text{th}}$ vector in both decryption key side and ciphertext side. Namely, the replies for the ciphertext queries are $\mathrm{CT}^*_{\iota,t_\iota} = (\boldsymbol{c}^*_{\iota,t_\iota}, k_\iota, \iota)$, where

$$
\begin{aligned}
&W_\iota = R_1(\iota), \ \ \mathbb{B}_\iota = \mathbb{D} W_\iota, \\
&\kappa_{\iota,t_\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{c}^*_{\iota,t_\iota} = (\boxed{\vec{x}_{\iota,t_\iota,1}, \vec{x}_{\iota,t_\iota,0}}, 1, \kappa_{\iota,t_\iota}, 0)_{\mathbb{B}_\iota}, \quad k_\iota = R_2(\iota),
\end{aligned}
$$

and the replies for the decryption key queries are $\mathrm{SK}^*_{S_i,i} = (C_{|S_i|}, S_i)$, where

$$
\begin{aligned}
&r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_i} r_{\iota,i} = 0, \ \ W_\iota = R_1(\iota), \ \ \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,i} = (\boxed{\vec{y}_{\iota,i,1}, \vec{0}^m}, r_{\iota,i}, \vec{0}^2)_{\mathbb{B}^*_\iota} \quad \text{for } \iota \in S_i, \\
&C_{|S_i|} = \mathsf{SKE.Encrypt}(R_2(s_{i,|S_i|}), \ldots, \mathsf{SKE.Encrypt}(R_2(s_{i,1}), \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in S_i}) \ldots).
\end{aligned}
$$

Hyb_5: This hybrid is the same as $\mathsf{Expt}^{\text{FH-UMIPE}}_{\mathcal{A}}(1)$ defined in Definition 2.9. That is, the replies for the ciphertext queries are $\mathrm{CT}^*_{\iota,t_\iota} = (\boldsymbol{c}^*_{\iota,t_\iota}, k_\iota, \iota)$, where

$$
\begin{aligned}
&W_\iota = \boxed{F_1(K_1, \iota)}, \ \ \mathbb{B}_\iota = \mathbb{D} W_\iota, \\
&\kappa_{\iota,t_\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{c}^*_{\iota,t_\iota} = (\vec{x}_{\iota,t_\iota,1}, \boxed{\vec{0}^m}, 1, \kappa_{\iota,t_\iota}, 0)_{\mathbb{B}_\iota}, \quad \boxed{k_\iota = F_2(K_2, \iota)},
\end{aligned}
$$

and the replies for the decryption key queries are $\mathrm{SK}^*_{S_i,i} = (C_{|S_i|}, S_i)$, where

$$
\begin{aligned}
&r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_i} r_{\iota,i} = 0, \ \ \boxed{W_\iota = F_1(K_1, \iota)}, \ \ \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,i} = (\vec{y}_{\iota,i,1}, \vec{0}^m, r_{\iota,i}, \vec{0}^2)_{\mathbb{B}^*_\iota} \quad \text{for } \iota \in S_i, \\
&C_{|S_i|} = \mathsf{SKE.Encrypt}(\boxed{F_2(K_2, s_{i,|S_i|})}, \ldots, \mathsf{SKE.Encrypt}(\boxed{F_2(K_2, s_{i,1})}, \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in S_i}) \ldots).
\end{aligned}
$$

► Analysis

Let us now denote by $\mathsf{Adv}^{(h)}_{\mathcal{A}}(\lambda)$ the advantage of the adversary $\mathcal{A}$, i.e., $\mathcal{A}$'s probability of outputting 1 in Hyb_h. Then, we can see that

$$
\begin{aligned}
\mathsf{Adv}^{\text{FH-UMIPE}}_{\mathcal{A}}(\lambda) \leq{}& |\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| + |\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda)| \\
&+ \sum_{\upsilon=1}^{q_{\text{KEY}}} |\mathsf{Adv}^{(3,\upsilon-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3,\upsilon)}_{\mathcal{A}}(\lambda)| \qquad (4.1) \\
&+ |\mathsf{Adv}^{(3,q_{\text{KEY}})}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)| + |\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(5)}_{\mathcal{A}}(\lambda)|.
\end{aligned}
$$

We will formally argue that each term on the RHS of **??** is negligible in Appendix D. This completes the proof of Theorem 4.1. □

References

AAB+13. Shashank Agrawal, Shweta Agrawal, Saikrishna Badrinarayanan, Abishek Kumarasubramanian, Manoj Prabhakaran, and Amit Sahai. Function private functional encryption and property preserving encryption: New definitions and positive results. Cryptology ePrint Archive, Report 2013/744, 2013.

ABDCP15. Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval. Simple functional encryption schemes for inner products. In *Public Key Cryptography–PKC 2015*, pages 733–751. Springer, 2015.

ABSV15. Prabhanjan Ananth, Zvika Brakerski, Gil Segev, and Vinod Vaikuntanathan. From selective to adaptive security in functional encryption. In *Advances in Cryptology–CRYPTO 2015*, pages 657–677. Springer, 2015.

ACF+17. Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, and Bogdan Ursu. Multi-input functional encryption for inner products: Function-hiding realizations and constructions without pairings. Cryptology ePrint Archive, Report 2017/972, 2017.

AJ15. Prabhanjan Ananth and Abhishek Jain. Indistinguishability obfuscation from compact functional encryption. In *Advances in Cryptology–CRYPTO 2015*, pages 308–326. Springer, 2015.

ARW17. Michel Abdalla, Mariana Raykova, and Hoeteck Wee. Multi-input inner-product functional encryption from pairings. In *Advances in Cryptology–EUROCRYPT 2017*, pages 601–626. Springer, 2017.

BGI+01. Boaz Barak, Oded Goldreich, Rusell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im) possibility of obfuscating programs. In *Advances in Cryptology–CRYPTO 2001*, pages 1–18. Springer, 2001.

BGJS15. Saikrishna Badrinarayanan, Divya Gupta, Abhishek Jain, and Amit Sahai. Multi-input functional encryption for unbounded arity functions. In *Advances in Cryptology–ASIACRYPT 2015*, pages 27–51. Springer, 2015.

BJK15. Allison Bishop, Abhishek Jain, and Lucas Kowalczyk. Function-hiding inner product encryption. In *Advances in Cryptology–ASIACRYPT 2015*, pages 470–491. Springer, 2015.

BKS16. Zvika Brakerski, Ilan Komargodski, and Gil Segev. Multi-input functional encryption in the private-key setting: Stronger security from weaker assumptions. In *Advances in Cryptology–EUROCRYPT 2016*, pages 852–880. Springer, 2016.

BRS13a. Dan Boneh, Ananth Raghunathan, and Gil Segev. Function-private identity-based encryption: Hiding the function in functional encryption. In *Advances in Cryptology–CRYPTO 2013*, pages 461–478. Springer, 2013.

BRS13b. Dan Boneh, Ananth Raghunathan, and Gil Segev. Function-private subspace-membership encryption and its applications. In *Advances in Cryptology–ASIACRYPT 2013*, pages 255–275. Springer, 2013.

BS15. Zvika Brakerski and Gil Segev. Function-private functional encryption in the private-key setting. In *Theory of Cryptography Conference–TCC 2015*, pages 306–324. Springer, 2015.

BSW11. Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. *Theory of Cryptography–TCC 2011*, pages 253–273, 2011.

CLOZ16. David Cash, Feng-Hao Liu, Adam O'Neill, and Cong Zhang. Reducing the leakage in practical order-revealing encryption. Cryptology ePrint Archive, Report 2016/661, 2016.

CLT13. Jean-Sébastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology–CRYPTO 2013*, pages 476–493. Springer, 2013.

CLWW16. Nathan Chenette, Kevin Lewi, Stephen A Weis, and David J Wu. Practical order-revealing encryption with limited leakage. In *Fast Software Encryption–FSE 2016*, pages 474–493. Springer, 2016.

DDM16. Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay. Functional encryption for inner product with full function privacy. In *Public-Key Cryptography–PKC 2016*, pages 164–195. Springer, 2016.

GGG+14. Shafi Goldwasser, S Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou. Multi-input functional encryption. In *Advances in Cryptology–EUROCRYPT 2014*, pages 578–602. Springer, 2014.

GGH13. Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *Advances in Cryptology–EUROCRYPT 2013*, pages 1–17. Springer, 2013.

GGH+16. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *SIAM Journal on Computing*, volume 45, pages 882–929. SIAM, 2016.

GGHZ16. Sanjam Garg, Craig Gentry, Shai Halevi, and Mark Zhandry. Functional encryption without obfuscation. In *Theory of Cryptography Conference–TCC 2016*, pages 480–511. Springer, 2016.

GGSW13. Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In *symposium on Theory of computing–stoc 2013*, pages 467–476. ACM, 2013.

GJO16. Vipul Goyal, Aayush Jain, and Adam O'Neill. Multi-input functional encryption with unbounded-message security. In *Advances in Cryptology–ASIACRYPT 2016*, pages 531–556. Springer, 2016.

GPS08. Steven D Galbraith, Kenneth G Paterson, and Nigel P Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.

IPS15. Yuval Ishai, Omkant Pandey, and Amit Sahai. Public-coin differing-inputs obfuscation and its applications. In *Theory of Cryptography Conference–TCC 2015*, pages 668–697. Springer, 2015.

ITZ15. Vincenzo Iovino, Qiang Tang, and Karol Zebrowski. On the power of public-key functional encryption with function privacy. Cryptology ePrint Archive, Report 2015/470, 2015.

KLM+16. Sam Kim, Kevin Lewi, Avradip Mandal, Hart William Montgomery, Arnab Roy, and David J Wu. Function-hiding inner product encryption is practical. Cryptology ePrint Archive, Report 2016/440, 2016.

KS17. Ilan Komargodski and Gil Segev. From minicrypt to obfustopia via private-key functional encryption. In *Advances in Cryptology–EUROCRYPT 2017*, pages 122–151. Springer, 2017.

KSY15. Ilan Komargodski, Gil Segev, and Eylon Yogev. Functional encryption for randomized functionalities in the private-key setting from minimal assumptions. In *Theory of Cryptography Conference–TCC 2015*, pages 352–377. Springer, 2015.

Lin17. Huijia Lin. Indistinguishability obfuscation from sxdh on 5-linear maps and locality-5 prgs. In *Advances in Cryptology–CRYPTO 2017*, pages 599–629. Springer, 2017.

LL16. Kwangsu Lee and Dong Hoon Lee. Two-input functional encryption for inner products from bilinear maps. Cryptology ePrint Archive, Report 2016/432, 2016.

LV16. Huijia Lin and Vinod Vaikuntanathan. Indistinguishability obfuscation from ddh-like assumptions on constant-degree graded encodings. In *Foundations of Computer Science–FOCS 2016*, pages 11–20. IEEE, 2016.

LW16. Kevin Lewi and David J Wu. Order-revealing encryption: New constructions, applications, and lower bounds. In *ACM SIGSAC Conference on Computer and Communications Security–CCS 2016*, pages 1167–1178. ACM, 2016.

O'N10. Adam O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010.

OT09. Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In *Advances in Cryptology–ASIACRYPT 2009*, pages 214–231. Springer, 2009.

OT10. Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Advances in Cryptology–CRYPTO 2010*, pages 191–208. Springer, 2010.

Sha07. Hovav Shacham. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007.

SSW09. Emily Shen, Elaine Shi, and Brent Waters. Predicate privacy in encryption systems. In *Theory of Cryptography Conference–TCC 2009*, pages 457–473. Springer, 2009.

TAO16. Junichi Tomida, Masayuki Abe, and Tatsuaki Okamoto. Efficient functional encryption for inner-product values with full-hiding security. In *Information Security–ISC 2016*, pages 408–425. Springer, 2016.

Appendix

A Reducing the Hardness of Problem 1 and 1* to k-LIN

In this section, we demonstrate how to reduce the hardness of Problem 1 (Definition 2.5) and 1* (Definition 2.6) to that of the k-LIN problem. Towards this end, we first define an intermediate decisional problem, namely, Problem 0, and then reduce the hardness of Problem 1 and 1* to that of Problem 0 (Lemmas A.2 and A.3 respectively), as well as reduce the hardness of Problem 0 to that of the k-LIN problem (Lemma A.1).

Definition A.1 (Problem 0): Fix an arbitrary number $\chi \in [2]$. Problem 0 is to guess a bit $\hat{\beta} \xleftarrow{\mathsf{U}} \{0,1\}$ provided $\varsigma_{\hat{\beta}} = (\mathsf{params}_{\mathbb{G}}, \mathbb{D}, \widehat{\mathbb{D}}^*, g_\chi^\zeta, \boldsymbol{\Omega}_{\hat{\beta}})$; where $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{BPG}}()$; $\zeta, \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q\backslash\{0\}$; $\tau_1, \ldots, \tau_k \xleftarrow{\mathsf{U}} \mathbb{F}_q$; $D = (d_{j,t})_{(k+1)\times(k+1)} \xleftarrow{\mathsf{U}} \mathsf{GL}(k+1, \mathbb{F}_q)$; $D^\bigstar = (d^*_{j,t})_{(k+1)\times(k+1)} = \zeta D^*$; $\boldsymbol{d}_j = (g_\chi^{d_{j,1}}, \ldots, g_\chi^{d_{j,(k+1)}})$, $\boldsymbol{d}^*_j = (g_{3-\chi}^{d^*_{j,1}}, \ldots, g_{3-\chi}^{d^*_{j,(k+1)}})$, for $j \in [k+1]$; $\mathbb{D} = \{\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{k+1}\}$, $\widehat{\mathbb{D}}^* = \{\boldsymbol{d}^*_1\}$; and $\boldsymbol{\Omega}_{\hat{\beta}} = (\tau_1, \ldots, \tau_k, 0)_{\mathbb{D}}$ or $(\tau_1, \ldots, \tau_k, \psi)_{\mathbb{D}}$ according as $\hat{\beta} = 0$ or 1. For any PPT algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ in deciding Problem 0 is defined as

$$\mathsf{Adv}^{\mathrm{P}_0}_{\mathcal{A}}(\lambda) = \left|\mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}(\varsigma_0)] - \mathsf{Pr}[1 \xleftarrow{\mathsf{R}} \mathcal{A}(\varsigma_1)]\right|.$$

Lemma A.1: *For any* PPT *algorithm* $\mathcal{A}$ *for* Problem 0*, there exists a* PPT *algorithm* $\mathcal{B}$ *for the* k-LIN *problem such that for any security parameter* λ*, we have* $\mathsf{Adv}^{\mathrm{P}_0}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\text{k-LIN}}_{\mathcal{B}}(\lambda)$.

Proof: We construct a PPT algorithm $\mathcal{B}$ for solving the k-LIN problem using a PPT algorithm $\mathcal{A}$ for Problem 0. $\mathcal{B}$ chooses a number $\chi \in [2]$, and is given an instance of the k-LIN problem

$$\varepsilon_{\hat{\beta}} = (\mathsf{params}_{\mathbb{G}}, g_\chi^{\xi_1}, \ldots, g_\chi^{\xi_k}, g_\chi^{\delta_1\xi_1}, \ldots, g_\chi^{\delta_k\xi_k}, \Re_{\hat{\beta}}),$$

for some $\hat{\beta} \xleftarrow{\mathsf{U}} \{0,1\}$;
where $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{BPG}}()$; $\xi_1, \ldots, \xi_k, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q\backslash\{0\}$; $\delta_1, \ldots, \delta_k \xleftarrow{\mathsf{U}} \mathbb{F}_q$; and $\Re_{\hat{\beta}} = g_\chi^{\sum_{j\in[k]}\delta_j}$ or $g_\chi^{\sigma+\sum_{j\in[k]}\delta_j}$ according as $\hat{\beta} = 0$ or 1. $\mathcal{B}$ proceeds as follows:

1. First, $\mathcal{B}$ sets $g_\chi^\zeta = g_\chi^{\xi_1}$, i.e., it *implicitly* defines $\zeta = \xi_1$.
2. Next, $\mathcal{B}$ samples random $W \xleftarrow{\mathsf{U}} \mathsf{GL}(k+1, \mathbb{F}_q)$, *implicitly* sets the matrices

$$D = (d_{j,t})_{(k+1)\times(k+1)} = \begin{pmatrix} \xi_1 & & & 1 \\ & \ddots & & \vdots \\ & & \xi_k & 1 \\ & & & 1 \end{pmatrix} W,$$

$$D^\bigstar = (d^*_{j,t})_{(k+1)\times(k+1)} = \xi_1 \begin{pmatrix} \xi_1^{-1} & & & \\ & \ddots & & \\ & & & \xi_k^{-1} \\ -\xi_1^{-1} & \ldots & -\xi_k^{-1} & 1 \end{pmatrix} W^*,$$

   defines $\boldsymbol{d}_j = (g_\chi^{d_{j,1}}, \ldots, g_\chi^{d_{j,(k+1)}})$, $\boldsymbol{d}^*_j = (g_{3-\chi}^{d^*_{j,1}}, \ldots, g_{3-\chi}^{d^*_{j,(k+1)}})$, for $j \in [k+1]$, and sets

$$\mathbb{D} = \{\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{k+1}\}, \widehat{\mathbb{D}}^* = \{\boldsymbol{d}^*_1\}.$$

   Observe that since W is uniformly sampled from $\mathsf{GL}(k+1, \mathbb{F}_q)$, D is distributed uniformly over $\mathsf{GL}(k+1, \mathbb{F}_q)$ as well. Also, $D^\bigstar = \zeta D^*$. Further, note that $\mathcal{B}$ can explicitly compute $\mathbb{D}$ and $\widehat{\mathbb{D}}^*$ from the available informations.
3. After that, $\mathcal{B}$ sets

$$\boldsymbol{\Omega}_{\hat{\beta}} = (g_\chi^{\delta_1\xi_1}, \ldots, g_\chi^{\delta_k\xi_k}, \Re_{\hat{\beta}})W.$$

4. Finally, $\mathcal{B}$ hands $\varsigma_{\hat{\beta}} = (\mathsf{params}_{\mathbb{G}}, \mathbb{D}, \widehat{\mathbb{D}}^*, g_\chi^\zeta, \boldsymbol{\Omega}_{\hat{\beta}})$ to $\mathcal{A}$ and outputs $\hat{\beta}' \in \{0,1\}$ returned by $\mathcal{A}$.

Observe that if $\hat{\beta} = 0$, i.e., $\Re_{\hat{\beta}} = g_{\chi}^{\sum_{j\in[k]} \delta_j}$, then we have

$$\boldsymbol{\Omega}_{\hat{\beta}} = (\delta_1, \ldots, \delta_k, 0)_{\mathbb{D}}.$$

On the other hand, in case $\hat{\beta} = 1$, i.e., $\Re_{\hat{\beta}} = g_{\chi}^{\sigma + \sum_{j\in[k+1]} \delta_j}$, then we have

$$\boldsymbol{\Omega}_{\hat{\beta}} = (\delta_1, \ldots, \delta_k, \sigma)_{\mathbb{D}}.$$

Hence, it follows that $\varsigma_{\hat{\beta}}$ simulated by $\mathcal{B}$ is indeed an instance of Problem 0 with the challenge bit $\hat{\beta}$, where we have $\tau_j = \delta_j$ for all $j \in [k+1]$, and $\psi = \sigma$. This completes the proof of Lemma A.1. □

Lemma A.2: *For any* PPT *algorithm* $\mathcal{A}$ *for* Problem 1*, there exists a* PPT *algorithm* $\mathcal{B}$ *for* Problem 0 *such that for any security parameter* λ*, we have* $\mathsf{Adv}^{\mathrm{P1}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathrm{P0}}_{\mathcal{B}}(\lambda)$.

Proof: We construct a PPT algorithm $\mathcal{B}$ for solving Problem 0 by using a PPT algorithm $\mathcal{A}$ for Problem 1, as a sub-routine. $\mathcal{B}$ is given an instance of Problem 0 corresponding to $\chi = 1$,

$$\varsigma_{\hat{\beta}} = (\mathsf{params}_{\mathbb{G}}, \mathbb{D}, \widehat{\mathbb{D}}^*, g_1^{\zeta}, \boldsymbol{\Omega}_{\hat{\beta}}),$$

where $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{BPG}}(); \zeta, \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q \backslash \{0\}; \tau_1, \ldots, \tau_k \xleftarrow{\mathsf{U}} \mathbb{F}_q; D = (d_{j,t})_{(k+1)\times(k+1)} \xleftarrow{\mathsf{U}} \mathsf{GL}(k+1, \mathbb{F}_q)$; $D^{\bigstar} = (d^*_{j,t})_{(k+1)\times(k+1)} = \zeta D^*$; $\boldsymbol{d}_j = (g_1^{d_{j,1}}, \ldots, g_1^{d_{j,(k+1)}})$, $\boldsymbol{d}^*_j = (g_2^{d^*_{j,1}}, \ldots, g_2^{d^*_{j,(k+1)}})$, for $j \in [k+1]$; $\mathbb{D} = \{\boldsymbol{d}_1, \ldots, \boldsymbol{d}_{k+1}\}$, $\widehat{\mathbb{D}}^* = \{\boldsymbol{d}^*_1\}$; and $\boldsymbol{\Omega}_{\hat{\beta}} = (\tau_1, \ldots, \tau_k, 0)_{\mathbb{D}}$ or $(\tau_1, \ldots, \tau_k, \psi)_{\mathbb{D}}$ according as $\hat{\beta} = 0$ or 1. Then, $\mathcal{B}$ proceeds as follows:

1. $\mathcal{B}$ forms $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{DPVS}}(2m + 2k + 1, \mathsf{params}_{\mathbb{G}})$ and computes $g_T = e(g_1^{\zeta}, g_2)$.
2. Next, for each $\iota \in [n]$, $\mathcal{B}$ executes the following steps:
   i) First, $\mathcal{B}$ samples a random invertible $(2m+2k+1)\times(2m+2k+1)$ matrix $W_\iota = (w_{\iota,j,t})_{(2m+2k+1)\times(2m+2k+1)} \xleftarrow{\mathsf{U}} \mathsf{GL}(2m + 2k + 1, \mathbb{F}_q)$.
   ii) Then, $\mathcal{B}$ computes the following:

$$\begin{aligned}
\boldsymbol{b}_{\iota,j} &= (\mathbf{1}_{\mathbb{G}_1}^{j+k}, g_1^{\zeta}, \mathbf{1}_{\mathbb{G}_1}^{2m+k-j}) W_\iota, \text{for } j \in [2m+k] \\
\boldsymbol{b}_{\iota,2m+k+j} &= (\boldsymbol{d}_j, \mathbf{1}_{\mathbb{G}_1}^{2m+k}) W_\iota, \text{for } j \in [k+1] \\
\boldsymbol{b}^*_{\iota,j} &= (\mathbf{1}_{\mathbb{G}_2}^{j+k}, g_2, \mathbf{1}_{\mathbb{G}_2}^{2m+k-j}) W^*_\iota, \text{for } j \in [2m+k] \\
\boldsymbol{b}^*_{\iota,2m+k+1} &= (\boldsymbol{d}^*_1, \mathbf{1}_{\mathbb{G}_2}^{2m+k}) W^*_\iota
\end{aligned}$$

   iii) $\mathcal{B}$ also *implicitly* sets

$$\boldsymbol{b}^*_{\iota,2m+k+j} = (\boldsymbol{d}^*_j, \mathbf{1}_{\mathbb{G}_2}^{2m+k}) W^*_\iota, \text{for } j \in [2, k+1].$$

   iv) $\mathcal{B}$ sets

$$\mathbb{B}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+2k+1}\},$$

   and *implicitly* defines

$$\mathbb{B}^*_\iota = \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+2k+1}\}.$$

   It is easy to verify that $(\mathbb{B}_\iota, \mathbb{B}^*_\iota)$ are indeed dual orthogonal bases of the pair of vector spaces $(\mathbb{V}_1 = \mathbb{G}_1^{2m+2k+1}, \mathbb{V}_2 = \mathbb{G}_2^{2m+2k+1})$. Moreover, since W_ι is uniformly and independently sampled from $\mathsf{GL}(2m + 2k + 1, \mathbb{F}_q)$, $\{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}$ are distributed uniformly and independently as well. Further, $e(\boldsymbol{b}_{\iota,j}, \boldsymbol{b}^*_{\iota,j}) = g_T$, for all $j \in [2m + 2k + 1]$.
   v) $\mathcal{B}$ sets

$$\begin{aligned}
\widehat{\mathbb{B}}_\iota &= \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+1}, \boldsymbol{b}_{\iota,2m+k+1}, \ldots, \boldsymbol{b}_{\iota,2m+2k}\}, \\
\widehat{\mathbb{B}}^*_\iota &= \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+k}\}.
\end{aligned}$$

   Observe that $\mathcal{B}$ can explicitly determine $\widehat{\mathbb{B}}_\iota$ and $\widehat{\mathbb{B}}^*_\iota$ from the available informations.

vi) After that, $\mathcal{B}$ sets

$$\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\boldsymbol{\Omega}_{\hat{\beta}}, \mathbf{1}_{\mathbb{G}_1}^{2m+k}) W_\iota.$$

3. Finally, $\mathcal{B}$ hands $\varrho_{\hat{\beta}} = (\mathsf{params}_{\mathbb{V}}, g_T, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota\in[n]}, \{\boldsymbol{\Upsilon}_{\iota,\hat{\beta}}\}_{\iota\in[n]})$ to $\mathcal{A}$, and outputs $\hat{\beta}' \in \{0,1\}$ returned by $\mathcal{A}$.

   Observe that if $\hat{\beta} = 0$, i.e., $\boldsymbol{\Omega}_{\hat{\beta}} = (\tau_1, \ldots, \tau_k, 0)_{\mathbb{D}}$, then we have

$$\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\vec{0}^{2m+k}, \tau_1, \ldots, \tau_k, 0)_{\mathbb{B}_\iota} \text{ for all } \iota \in [n].$$

On the other hand, in case $\hat{\beta} = 1$, i.e., $\boldsymbol{\Omega}_{\hat{\beta}} = (\tau_1, \ldots, \tau_k, \psi)_{\mathbb{D}}$, then we have

$$\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\vec{0}^{2m+k}, \tau_1, \ldots, \tau_k, \psi)_{\mathbb{B}_\iota} \text{ for all } \iota \in [n].$$

Hence, it follows that $\varrho_{\hat{\beta}}$ simulated by $\mathcal{B}$ is indeed an instance of Problem 1 with challenge bit $\hat{\beta}$, where we have $\alpha_j = \tau_j \mathrm{b}$ for all $j \in [k]$, and $\Im = \psi$. This completes the proof of Lemma A.2. □

Lemma A.3: *For any* PPT *algorithm* $\mathcal{A}$ *for* Problem 1^**, there exists a* PPT *algorithm* $\mathcal{B}$ *for* Problem 0 *such that for any security parameter* λ*, we have* $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{P}1^*}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}}^{\mathrm{P}0}(\lambda)$.

Proof: The proof of Lemma A.3 is the same as that of Lemma A.2 except for some minor modifications that are easy to figure out. We omit the details to avoid repetition. □

B Some Remarks on the Full-Hiding Security of Bounded Multi-Input Inner Product Encryption

Remark B.1 (Zero vs Multiple Queries): Here, we show how to generically convert an FH-MIPE scheme that achieves the full-hiding security when the adversary receives at least one ciphertext for each encryption index to one that achieves full-hiding security without any restriction on the number of ciphertext queries for each encryption index, by applying a similar transformation using a standard symmetric key encryption (SKE) scheme. More formally, assume that $\Pi_{\text{FH-MIPE}} = (\mathsf{FH\text{-}MIPE.Setup}, \mathsf{FH\text{-}MIPE.KeyGen}, \mathsf{FH\text{-}MIPE.Encrypt}, \mathsf{FH\text{-}MIPE.Decrypt})$ be a private key FH-MIPE scheme for $\mathcal{F}_n^{m,\mathscr{B}}$ that achieves the full-hiding security under the model described above, and $\Pi_{\text{SKE}} = (\mathsf{SKE.KeyGen}, \mathsf{SKE.Encrypt}, \mathsf{SKE.Decrypt})$ be a symmetric key encryption scheme. Consider the private key FH-MIPE construction $\Pi'_{\text{FH-MIPE}} = (\mathsf{FH\text{-}MIPE.Setup}', \mathsf{FH\text{-}MIPE.KeyGen}', \mathsf{FH\text{-}MIPE.Encrypt}', \mathsf{FH\text{-}MIPE.Decrypt}')$ for $\mathcal{F}_n^{m,\mathscr{B}}$ described below:

$(\mathrm{PP}' = \mathrm{PP}, \mathrm{MSK}' = (\mathrm{MSK}, \{k_\iota\}_{\iota\in[1,n]})) \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.Setup}'(m, n, \mathscr{B})$:
1. $(\mathrm{PP}, \mathrm{MSK}) \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.Setup}(m, n, \mathscr{B})$
2. $K \xleftarrow{\mathsf{R}} \mathsf{SKE.KeyGen}()$
3. $k_1, \ldots, k_{n-1} \xleftarrow{\mathsf{U}} \{0,1\}^{|K|}$, $k_n = K \oplus (\bigoplus_{\iota\in[1,n-1]} k_\iota)$

$(\mathrm{SK}') \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.KeyGen}'(\mathrm{PP}', \mathrm{MSK}', (\vec{y}_1, \ldots, \vec{y}_n))$:
1. $\mathrm{SK} \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.KeyGen}(\mathrm{PP}, \mathrm{MSK}, (\vec{y}_1, \ldots, \vec{y}_n))$
2. $\mathrm{SK}' \xleftarrow{\mathsf{R}} \mathsf{SKE.Encrypt}(K, \mathrm{SK})$

$(\mathrm{CT}'_\iota, k_\iota) \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.Encrypt}'(\mathrm{PP}', \mathrm{MSK}', \iota, \vec{x}_\iota)$:
1. $\mathrm{CT}_\iota \xleftarrow{\mathsf{R}} \mathsf{FH\text{-}MIPE.Encrypt}(\mathrm{PP}, \mathrm{MSK}, \iota, \vec{x}_\iota)$
2. $\mathrm{CT}'_\iota \xleftarrow{\mathsf{R}} \mathsf{SKE.Encrypt}(K, \mathrm{CT}_\iota)$

Λ or $\perp = \mathsf{FH\text{-}MIPE.Decrypt}'(\mathrm{PP}', \mathrm{SK}', ((\mathrm{CT}'_1, k_1), \ldots, (\mathrm{CT}'_n, k_n)))$:
1. $K = \bigoplus_{\iota\in[1,n]} k_\iota$
2. $\mathrm{SK} = \mathsf{SKE.Decrypt}(K, \mathrm{SK}')$
3. $\mathrm{CT}_\iota = \mathsf{SKE.Decrypt}(K, \mathrm{CT}'_\iota), \forall \iota \in [n]$
4. Λ or $\perp = \mathsf{FH\text{-}MIPE.Decrypt}(\mathrm{PP}, \mathrm{SK}, (\mathrm{CT}_1, \ldots, \mathrm{CT}_n))$

Observe that $\Pi'_{\text{FH-MIPE}}$ achieves full-hiding security without any restriction on the number of queries of the adversary. Roughly, let us consider two cases separately:

a) $(\exists\ \iota \in [n] : q_{\text{CT},\iota} = 0)$ In this case, the corresponding k_ι is perfectly hidden from the adversary, and hence K is so as well. Then, security follows readily from the simantic security of Π_{SKE}.
b) $(q_{\text{CT},\iota} \geq 1 \forall \iota \in [n])$ In this case, security follows immediately from that of $\Pi_{\text{FH-MIPE}}$.

Remark B.2 (An equivalent formulation of the restriction on the queries of the adversary in case it makes at least one ciphertext query per encryption slot): In the full-hiding security proof of the FH-MIPE scheme proposed in Section 3.1, we consider $q_{\text{CT},\iota} \geq 1$ for all $\iota \in [n]$, i.e., the adversary $\mathcal{A}$ makes at least one ciphertext query for each of the n encryption indices. Observe that under such constraint, we can make use of an alternative equivalent formulation of the restrictions on the queries of the adversary $\mathcal{A}$ as described below. We will use this later formulation of the restriction on the adversarial queries in the security proof of our FH-MIPE scheme of Section 3.1.

Let $\{(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1})\}_{\iota\in[n],t_\iota,\in[q_{\text{CT},\iota}]}$ is the set of all ciphertext queries and $\{(\{\vec{y}_{\iota,i,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,i,1}\}_{\iota\in[n]})\}_{i\in[q_{\text{KEY}}]}$ is the set of all decryption key queries of $\mathcal{A}$. Then, it is required that for all $i \in [q_{\text{KEY}}]$,

$$\sum_{\iota\in[n]} \vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,i,0} = \sum_{\iota\in[n]} \vec{x}_{\iota,1,1} \cdot \vec{y}_{\iota,i,1}, \tag{B.1}$$

$$\text{and } \vec{x}_{\iota,t_\iota,0} \cdot \vec{y}_{\iota,i,0} - \vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,i,0} = \vec{x}_{\iota,t_\iota,1} \cdot \vec{y}_{\iota,i,1} - \vec{x}_{\iota,1,1} \cdot \vec{y}_{\iota,i,1}, \text{ for all } \iota \in [n], t_\iota \in [2, q_{\text{CT},\iota}]. \tag{B.2}$$

?? follows directly from **??** by setting $t_\iota = 1$ for all $\iota \in [n]$, while the set of equations **??** are implied by **??** as follows: By **??**, we have for all $i \in [q_{\text{KEY}}]$,

$$\vec{x}_{\iota,t_\iota,0} \cdot \vec{y}_{\iota,i,0} + \sum_{\substack{\iota'\in[n]\\ \iota'\neq\iota}} \vec{x}_{\iota',1,0} \cdot \vec{y}_{\iota',i,0} = \vec{x}_{\iota,t_\iota,1} \cdot \vec{y}_{\iota,i,1} + \sum_{\substack{\iota'\in[n]\\ \iota'\neq\iota}} \vec{x}_{\iota',1,1} \cdot \vec{y}_{\iota',i,1}, \text{ for all } \iota \in [n], t_\iota \in [q_{\text{CT},\iota}]$$

$$\implies \vec{x}_{\iota,t_\iota,0} \cdot \vec{y}_{\iota,i,0} - \vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,i,0} = \vec{x}_{\iota,t_\iota,1} \cdot \vec{y}_{\iota,i,1} - \vec{x}_{\iota,1,1} \cdot \vec{y}_{\iota,i,1}, \text{ for all } \iota \in [n], t_\iota \in [2, q_{\text{CT},\iota}].$$

On the other hand, for any $i \in [q_{\text{KEY}}]$, adding both sides of **??** and those of the set of equations **??** for $(t_1, \ldots, t_n) \in [q_{\text{CT},1}] \times \ldots \times [q_{\text{CT},n}]$, we get **??** for $(t_1, \ldots, t_n) \in [q_{\text{CT},1}] \times \ldots \times [q_{\text{CT},n}]$. We will use the alternative equivalent restriction described in this remark in the security proof of our FH-MIPE construction.

C Lemmas for the Proof of Theorem 3.1

In Lemmas C.1–C.7, we make use of the following natural order "$\prec$" defined over $(\mathbb{N} \cup \{0\})^2$ as $(s,t) \prec (s',t') \iff [s < s'] \vee [(s = s') \wedge (t < t')]$, for $(s,t), (s',t') \in (\mathbb{N} \cup \{0\})^2$. We define $(s,t) \succ (s',t') \iff (s',t') \prec (s,t)$, for $(s,t), (s',t') \in (\mathbb{N} \cup \{0\})^2$.

Lemma C.1: *For any* PPT *adversary* $\mathcal{A}$ *between* $\mathsf{Hyb}_{\iota^*,\mu_{\iota^*},1}$ *and* $\mathsf{Hyb}_{1,\iota^*-1,q_{\text{CT},\iota^*-1},3}$ *or* $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*}-1,3}$ *depending on whether* $\mu_{\iota^*} = 1$ *or* $\mu_{\iota^*} > 1$*, there exists a* PPT *algorithm* $\mathcal{B}$ *for* Problem 1 *such that for any security parameter* λ*, we have*

$$\left.\begin{aligned} \left|\mathsf{Adv}_{\mathcal{A}}^{(1,\iota^*-1,q_{\text{CT},\iota^*-1},3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1,\iota^*,\mu_{\iota^*},1)}(\lambda)\right| &\leq \mathsf{Adv}_{\mathcal{B}}^{\text{P1}}(\lambda), \text{ if } \mu_{\iota^*} = 1 \\ \left|\mathsf{Adv}_{\mathcal{A}}^{(1,\iota^*,\mu_{\iota^*}-1,3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1,\iota^*,\mu_{\iota^*},1)}(\lambda)\right| &\leq \mathsf{Adv}_{\mathcal{B}}^{\text{P1}}(\lambda), \quad \text{if } \mu_{\iota^*} > 1 \end{aligned}\right\} \forall\, \iota^* \in [n].$$

Proof: Suppose that there exists a PPT adversary $\mathcal{A}$ between $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ and $\mathsf{Hyb}_{1,\iota^*-1,q_{\text{CT},\iota^*-1},3}$ or $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*}-1,3}$ depending on whether $\mu_{\iota^*} = 1$ or $\mu_{\iota^*} > 1$. We construct a PPT algorithm $\mathcal{B}$ for Problem 1 using $\mathcal{A}$ as a sub-routine. $\mathcal{B}$ takes the role of the challenger in the full-hiding security experiment described in Definition 2.8 and interacts with $\mathcal{A}$ as follows:

- $\mathcal{B}$ is given an instance of Problem 1,

$$\varrho_{\hat{\beta}} = (\mathsf{params}_{\mathbb{V}}, g_T, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota\in[n]}, \{\boldsymbol{\Upsilon}_{\iota,\hat{\beta}}\}_{\iota\in[n]});$$

  where $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\text{R}} \mathcal{G}_{\text{BPG}}()$; $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\text{R}} \mathcal{G}_{\text{DPVS}}(2m+2k+1, \mathsf{params}_{\mathbb{G}})$; $\nu \xleftarrow{\text{U}} \mathbb{F}_q\backslash\{0\}$; $g_T = e(g_1,g_2)^\nu$; $(\mathbb{B}_\iota, \mathbb{B}^*_\iota) \xleftarrow{\text{R}} \mathcal{G}_{\text{OB}}(2m+2k+1, \mathsf{params}_{\mathbb{V}}, \nu)$, for $\iota \in [n]$; $\widehat{\mathbb{B}}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+1}, \boldsymbol{b}_{\iota,2m+k+1}, \ldots, \boldsymbol{b}_{\iota,2m+2k}\}$, $\widehat{\mathbb{B}}^*_\iota = \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+k}\}$, for $\iota \in [n]$; $\alpha_1, \ldots, \alpha_k \xleftarrow{\text{U}} \mathbb{F}_q$; $\Im \xleftarrow{\text{U}} \mathbb{F}_q\backslash\{0\}$; and $\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\vec{0}^{2m+k}, \alpha_1, \ldots, \alpha_k, 0)_{\mathbb{B}_\iota}$ or $(\vec{0}^{2m+k}, \alpha_1, \ldots, \alpha_k, \Im)_{\mathbb{B}_\iota}$ for all $\iota \in [n]$ according as $\hat{\beta} = 0$ or 1. $\mathcal{B}$ hands $\text{PP} = (\mathsf{params}_{\mathbb{V}}, g_T)$ to $\mathcal{A}$.

- For all $i \in [q_{\text{KEY}}]$, in response to the i^{th} decryption key query of $\mathcal{A}$ corresponding to pair of sets of n vectors $(\{\vec{y}_{\iota,i,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,i,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1} \in \mathbb{F}_q^m$, $\mathcal{B}$ selects random $r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, for $\iota \in [n]$, subject to the restriction that $\sum_{\iota\in[n]} r_{\iota,i} = 0$, and computes

$$\begin{aligned}\boldsymbol{k}^*_{\iota,i} &= \sum_{j\in[m]} y^{(j)}_{\iota,i,0}\boldsymbol{b}^*_{\iota,j} + r_{\iota,i}\boldsymbol{b}^*_{\iota,2m+1} + \sum_{j\in[k-1]} \gamma_{\iota,i,j}\boldsymbol{b}^*_{\iota,2m+1+j} \\ &= (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}^*_\iota}, \text{ for } \iota \in [n].\end{aligned}$$

  $\mathcal{B}$ gives $\text{SK}^*_i = \{\boldsymbol{k}^*_{\iota,i}\}_{\iota\in[n]}$ to $\mathcal{A}$.
- For $\iota \in [n], t_\iota \in [q_{\text{CT},\iota}]$, to answer the $t_\iota{}^{\text{th}}$ ciphertext query of $\mathcal{A}$ with respect to index ι corresponding to pair of vectors $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}) \in (\mathbb{F}_q^m)^2$, $\mathcal{B}$ computes $\boldsymbol{c}^*_{\iota,t_\iota}$ as follows:

  a) $((\iota,t_\iota) \prec (\iota^*,\mu_{\iota^*}))$ $\mathcal{B}$ samples random $\varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and computes $\boldsymbol{c}^*_{\iota,t_\iota}$ as

$$\begin{aligned}\boldsymbol{c}^*_{\iota,t_\iota} &= \sum_{j\in[m]} x^{(j)}_{\iota,t_\iota,0}\boldsymbol{b}_{\iota,j} + \sum_{j\in[m]} x^{(j)}_{\iota,t_\iota,1}\boldsymbol{b}_{\iota,m+j} + \boldsymbol{b}_{\iota,2m+1} + \sum_{j\in[k]} \varphi_{\iota,t_\iota,j}\boldsymbol{b}_{\iota,2m+k+j} \\ &= (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota}.\end{aligned}$$

  b) $((\iota,t_\iota) = (\iota^*,\mu_{\iota^*}))$ $\mathcal{B}$ computes $\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}}$ as

$$\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}} = \sum_{j\in[m]} x^{(j)}_{\iota^*,\mu_{\iota^*},0}\boldsymbol{b}_{\iota^*,j} + \boldsymbol{b}_{\iota^*,2m+1} + \boldsymbol{\Upsilon}_{\iota^*,\hat{\beta}}.$$

  c) $((\iota,t_\iota) \succ (\iota^*,\mu_{\iota^*}))$ $\mathcal{B}$ picks random $\varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and computes $\boldsymbol{c}^*_{\iota,t_\iota}$ as

$$\begin{aligned}\boldsymbol{c}^*_{\iota,t_\iota} &= \sum_{j\in[m]} x^{(j)}_{\iota,t_\iota,0}\boldsymbol{b}_{\iota,j} + \boldsymbol{b}_{\iota,2m+1} + \sum_{j\in[k]} \varphi_{\iota,t_\iota,j}\boldsymbol{b}_{\iota,2m+k+j} \\ &= (\vec{x}_{\iota,t_\iota,0}, \vec{0}^m, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota}.\end{aligned}$$

  $\mathcal{B}$ provides $\mathcal{A}$ with $\text{CT}^*_{\iota,t_\iota} = (\iota, \boldsymbol{c}^*_{\iota,t_\iota})$.
- $\mathcal{A}$ eventually outputs a guess bit $\beta' \in \{0,1\}$. $\mathcal{B}$ outputs $\hat{\beta}' = \beta'$ as its guess bit in its Problem 1 challenge.

  Observe that if $\hat{\beta} = 0$, i.e., $\boldsymbol{\Upsilon}_{\iota^*,\hat{\beta}} = (\vec{0}^{2m+k}, \alpha_1, \ldots, \alpha_k, 0)_{\mathbb{B}_{\iota^*}}$, then we have

$$\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}} = (\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{0}^m, 1, \vec{0}^{k-1}, \alpha_1, \ldots, \alpha_k, 0)_{\mathbb{B}_{\iota^*}},$$

which is of the same form as that in **??**, where we have $\varphi_{\iota^*,\mu_{\iota^*},j} = \alpha_j$ for all $j \in [k]$, and this is the proper form of $\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}}$ in the hybrid immediately preceding $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$. On the other hand, in case $\hat{\beta} = 1$, i.e., $\boldsymbol{\Upsilon}_{\iota^*,\hat{\beta}} = (\vec{0}^{2m+k}, \alpha_1, \ldots, \alpha_k, \Im)_{\mathbb{B}_{\iota^*}}$, then we have

$$\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}} = (\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{0}^m, 1, \vec{0}^{k-1}, \alpha_1, \ldots, \alpha_k, \Im)_{\mathbb{B}_{\iota^*}},$$

which is of the same form as in **??**, where we have $\varphi_{\iota^*,\mu_{\iota^*},j} = \alpha_j$ for all $j \in [k]$, and $\rho_{\iota^*,\mu_{\iota^*}} = \Im$, and this is the proper form of $\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}}$ in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$. For $(\iota,t_\iota) \prec (\iota^*,\mu_{\iota^*})$, $\boldsymbol{c}^*_{\iota,t_\iota}$ has the form as in **??**, while for $(\iota,t_\iota) \succ (\iota^*,\mu_{\iota^*})$, $\boldsymbol{c}^*_{\iota,t_\iota}$ is of the form as in **??**. These are indeed the proper forms of $\boldsymbol{c}^*_{\iota,t_\iota}$ in the respective cases in both $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ as well as the previous hybrid. Also, for all $i \in [q_{\text{KEY}}]$, the i^{th} answered decryption key has the form as in **??** which is their proper form in both $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ and the earlier hybrid. Thus, the view of the adversary $\mathcal{A}$ simulated by $\mathcal{B}$ is distributed as in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ or its preceding hybrid, i.e., $\mathsf{Hyb}_{1,\iota^*-1,q_{\text{CT},\iota^*-1},3}$ or $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*}-1,3}$ depending on whether $\mu_{\iota^*} = 1$ or $\mu_{\iota^*} > 1$, according as $\hat{\beta} = 0$ or 1. This completes the proof of Lemma C.1. □

Lemma C.2: *For any probabilistic adversary $\mathcal{A}$, for any security parameter λ, we have*

$$\mathsf{Adv}^{(1,\iota^*,\mu_{\iota^*},1)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(1,\iota^*,\mu_{\iota^*},2)}_{\mathcal{A}}(\lambda) \text{ for all } \iota^* \in [n], \mu_{\iota^*} \in [q_{\text{CT},\iota^*}].$$

Proof: In order to prove Lemma C.2, we demonstrate that the view of the adversary $\mathcal{A}$ in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ and that in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},2}$ are identically distributed. Towards this end, we define new sets of dual orthogonal bases $\{\mathbb{U}_\iota = \{\boldsymbol{u}_{\iota,1}, \ldots, \boldsymbol{u}_{\iota,2m+2k+1}\}, \mathbb{U}^*_\iota = \{\boldsymbol{u}^*_{\iota,1}, \ldots, \boldsymbol{u}^*_{\iota,2m+2k+1}\}\}_{\iota\in[n]}$ of the pair of vector spaces $(\mathbb{V}_1 = \mathbb{G}_1^{2m+2k+1}, \mathbb{V}_2 = \mathbb{G}_2^{2m+2k+1})$ using the sets of dual orthogonal bases $\{\mathbb{B}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+2k+1}\}, \mathbb{B}^*_\iota = \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+2k+1}\}\}_{\iota\in[n]}$ generated from $\mathcal{G}_{\mathrm{OB}}(2m+2k+1, \mathsf{params}_{\mathbb{V}}, \nu)$ in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ as follows:

$$
\begin{aligned}
\boldsymbol{u}_{\iota^*,2m+2k+1} &= \boldsymbol{b}_{\iota^*,2m+2k+1} - \sum_{j\in[m]} \frac{x^{(j)}_{\iota^*,\mu_{\iota^*},1}}{\rho_{\iota^*,\mu_{\iota^*}}} \boldsymbol{b}_{\iota^*,m+j} \\
\boldsymbol{u}_{\iota^*,j} &= \boldsymbol{b}_{\iota^*,j}, \text{ for } j \in [2m+2k] \\
\boldsymbol{u}^*_{\iota^*,m+j} &= \boldsymbol{b}^*_{\iota^*,m+j} + \frac{x^{(j)}_{\iota^*,\mu_{\iota^*},1}}{\rho_{\iota^*,\mu_{\iota^*}}} \boldsymbol{b}^*_{\iota^*,2m+2k+1}, \text{ for } j \in [m] \\
\boldsymbol{u}^*_{\iota^*,j} &= \boldsymbol{b}^*_{\iota^*,j}, \text{ for } j \in [1,m] \cup [2m+1, 2m+2k+1] \\
\boldsymbol{u}_{\iota,j} &= \boldsymbol{b}_{\iota,j}, \text{ for } \iota \in [n]\backslash\{\iota^*\}, j \in [2m+2k+1] \\
\boldsymbol{u}^*_{\iota,j} &= \boldsymbol{b}^*_{\iota,j}, \text{ for } \iota \in [n]\backslash\{\iota^*\}, j \in [2m+2k+1]
\end{aligned}
$$

Note that $\{\mathbb{U}_\iota, \mathbb{U}^*_\iota\}_{\iota\in[n]}$ is indeed a set of dual orthogonal bases since those are obtained from the set of dual orthogonal bases $\{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota\in[n]}$ by applying invertible linear transformations. Further, $\{\mathbb{U}_\iota, \mathbb{U}^*_\iota\}_{\iota\in[n]}$ are distributed uniformly at random since $\{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota\in[n]}$ are so.

Now, observe that the $\mu_{\iota^*}{}^{\mathrm{th}}$ answered ciphertext $\mathrm{CT}^*_{\iota^*,\mu_{\iota^*}} = (\iota^*, \boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}})$ for index ι^* corresponding to the pair of vectors $(\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{x}_{\iota^*,\mu_{\iota^*},1}) \in (\mathbb{F}_q^m)^2$ in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ can be expressed as

$$
\begin{aligned}
\boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}} &= (\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{0}^m, 1, \vec{0}^{k-1}, \varphi_{\iota^*,\mu_{\iota^*},1}, \ldots, \varphi_{\iota^*,\mu_{\iota^*},k}, \rho_{\iota^*,\mu_{\iota^*}})_{\mathbb{B}_{\iota^*}} \\
&= (\vec{x}_{\iota^*,\mu_{\iota^*},0}, \vec{x}_{\iota^*,\mu_{\iota^*},1}, 1, \vec{0}^{k-1}, \varphi_{\iota^*,\mu_{\iota^*},1}, \ldots, \varphi_{\iota^*,\mu_{\iota^*},k}, \rho_{\iota^*,\mu_{\iota^*}})_{\mathbb{U}_{\iota^*}},
\end{aligned}
$$

which is of the same form as that in **??** that corresponds to $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},2}$. So, the form of $\mathrm{CT}^*_{\iota^*,\mu_{\iota^*}} = (\iota^*, \boldsymbol{c}^*_{\iota^*,\mu_{\iota^*}})$ in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ is changed to that in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},2}$ through the basis transformations. Also for all $(\iota, t_\iota) \neq (\iota^*, \mu_{\iota^*})$, the $t_\iota{}^{\mathrm{th}}$ answered ciphertext $\mathrm{CT}^*_{\iota,t_\iota} = (\iota, \boldsymbol{c}^*_{\iota,t_\iota})$ for index ι corresponding to the pair of vectors $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}) \in (\mathbb{F}_q^m)^2$ in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ can be expressed as follows:

a) $((\iota, t_\iota) \prec (\iota^*, \mu_{\iota^*}))$

$$
\begin{aligned}
\boldsymbol{c}^*_{\iota,t_\iota} &= (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota} \\
&= (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{U}_\iota}
\end{aligned}
$$

b) $((\iota, t_\iota) \succ (\iota^*, \mu_{\iota^*}))$

$$
\begin{aligned}
\boldsymbol{c}^*_{\iota,t_\iota} &= (\vec{x}_{\iota,t_\iota,0}, \vec{0}^m, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota} \\
&= (\vec{x}_{\iota,t_\iota,0}, \vec{0}^m, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{U}_\iota}
\end{aligned}
$$

Thus, it follows that for all $(\iota, t_\iota) \neq (\iota^*, \mu_{\iota^*})$, the form of $\mathrm{CT}^*_{\iota,t_\iota} = (\iota, \boldsymbol{c}^*_{\iota,t_\iota})$ is preserved under the basis transformations.

On the other hand, for all $i \in [q_{\mathrm{KEY}}]$, the components of the i^{th} answered decryption key $\mathrm{SK}^*_i = \{\boldsymbol{k}^*_{\iota,i}\}_{\iota\in[n]}$ corresponding to the pair of sets of n vectors $(\{\vec{y}_{\iota,i,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,i,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1} \in \mathbb{F}_q^m$ for all $\iota \in [n]$, in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ can be expressed as follows:

$$
\begin{aligned}
\boldsymbol{k}^*_{\iota,i} &= (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}^*_\iota} \\
&= (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{U}^*_\iota}, \text{ for } \iota \in [n]
\end{aligned}
$$

Hence, we see that for all $i \in [q_{\mathrm{KEY}}]$, the forms of the components of $\mathrm{SK}^*_i = \{\boldsymbol{k}^*_{\iota,i}\}_{\iota\in[n]}$ are also preserved under the basis transformations.

Moreover, observe that $e(\boldsymbol{u}_{\iota,j}, \boldsymbol{u}^*_{\iota,j}) = e(\boldsymbol{b}_{\iota,j}, \boldsymbol{b}^*_{\iota,j}) = g_T$ for all $\iota \in [n], j \in [2m+2k+1]$, and hence the basis transformations are compatible with the public parameters $\mathrm{PP} = (\mathsf{params}_{\mathbb{V}}, g_T)$ in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ as well. Thus, it follows that the view of the adversary $\mathcal{A}$ in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},1}$ can be conceptually changed to that in $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},2}$. □

Lemma C.3: *For any* PPT *adversary* $\mathcal{A}$ *between* $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},2}$ *and* $\mathsf{Hyb}_{1,\iota^*,\mu_{\iota^*},3}$*, there exists a* PPT *algorithm* $\mathcal{B}$ *for* Problem 1 *such that for any security parameter* λ*, we have*

$$\left|\mathsf{Adv}_{\mathcal{A}}^{(1,\iota^*,\mu_{\iota^*},2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1,\iota^*,\mu_{\iota^*},3)}(\lambda)\right| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathrm{P1}}(\lambda), \text{ for } \iota^* \in [n], \mu_{\iota^*} \in [q_{\mathrm{CT},\iota^*}].$$

Proof: The proof of Lemma C.3 is the same as that of Lemma C.1, except for some readily identifiable modifications. We omit the details to avoid repetition. □

Lemma C.4: *For any* PPT *adversary* $\mathcal{A}$ *between* $\mathsf{Hyb}_{2,\upsilon-1,3}$ *and* $\mathsf{Hyb}_{2,\upsilon,1}$*, there exists a* PPT *algorithm* $\mathcal{B}$ *for* Problem 1^* *such that for any security parameter* λ*, we have*

$$\left|\mathsf{Adv}_{\mathcal{A}}^{(2,\upsilon-1,3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2,\upsilon,1)}(\lambda)\right| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathrm{P1}^*}(\lambda), \text{ for } \upsilon \in [q_{\mathrm{KEY}}].$$

Proof: Suppose there exists a PPT adversary $\mathcal{A}$ between $\mathsf{Hyb}_{2,\upsilon-1,3}$ and $\mathsf{Hyb}_{2,\upsilon,1}$. We construct a PPT algorithm $\mathcal{B}$ for Problem 1^* using $\mathcal{A}$ as a sub-routine. $\mathcal{B}$ takes the role of the challenger in the full-hiding security experiment described in Definition 2.8 and interacts with $\mathcal{A}$ as follows:

- $\mathcal{B}$ is given an instance of Problem 1^*,

$$\varrho_{\hat{\beta}} = (\mathsf{params}_{\mathbb{V}}, g_T, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}_\iota^*\}_{\iota\in[n]}, \{\boldsymbol{\Upsilon}_{\iota,\hat{\beta}}\}_{\iota\in[n]});$$

  where $\mathsf{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{BPG}}()$; $\mathsf{params}_{\mathbb{V}} = (q, \mathbb{V}_1, \mathbb{V}_2, \mathbb{G}_T, \mathbb{A}_1, \mathbb{A}_2, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{DPVS}}(2m+2k+1, \mathsf{params}_{\mathbb{G}})$; $\nu \xleftarrow{\mathsf{U}} \mathbb{F}_q\backslash\{0\}$; $g_T = e(g_1,g_2)^\nu$; $(\mathbb{B}_\iota, \mathbb{B}_\iota^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{OB}}(2m+2k+1, \mathsf{params}_{\mathbb{V}}, \nu)$, for $\iota \in [n]$; $\widehat{\mathbb{B}}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+1}, \boldsymbol{b}_{\iota,2m+k+1}, \ldots, \boldsymbol{b}_{\iota,2m+2k}\}$, $\widehat{\mathbb{B}}_\iota^* = \{\boldsymbol{b}_{\iota,1}^*, \ldots, \boldsymbol{b}_{\iota,2m+k}^*\}$, for $\iota \in [n]$; $\alpha_1, \ldots, \alpha_k \xleftarrow{\mathsf{U}} \mathbb{F}_q$; $\Im \xleftarrow{\mathsf{U}} \mathbb{F}_q\backslash\{0\}$; and $\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\vec{0}^{2m}, \alpha_1, \ldots, \alpha_k, \vec{0}^k, 0)_{\mathbb{B}_\iota^*}$ or $(\vec{0}^{2m}, \alpha_1, \ldots, \alpha_k, \vec{0}^k, \Im)_{\mathbb{B}_\iota^*}$, for $\iota \in [n]$, according as $\hat{\beta} = 0$ or 1. $\mathcal{B}$ hands $\mathrm{PP} = (\mathsf{params}_{\mathbb{V}}, g_T)$ to $\mathcal{A}$.
- For $i \in [q_{\mathrm{KEY}}]$, to answer the i^{th} decryption key query of $\mathcal{A}$ corresponding to pair of sets of n vectors $(\{\vec{y}_{\iota,i,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,i,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1} \in \mathbb{F}_q^m$, $\mathcal{B}$ generates the components of $\mathrm{SK}_i^* = \{\boldsymbol{k}_{\iota,i}^*\}_{\iota\in[n]}$ as follows:
  a) $(i < \upsilon)$ $\mathcal{B}$ selects random $\widetilde{r}_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, for $\iota \in [n]$, such that $\sum_{\iota\in[n]} \widetilde{r}_{\iota,i} = 0$, $\gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, for $\iota \in [n]$, and computes

$$\begin{aligned}\boldsymbol{k}_{\iota,i}^* &= \sum_{j\in[m]} y_{\iota,i,1}^{(j)} \boldsymbol{b}_{\iota,m+j}^* + \widetilde{r}_{\iota,i} \boldsymbol{b}_{\iota,2m+1}^* + \sum_{j\in[k-1]} \gamma_{\iota,i,j} \boldsymbol{b}_{\iota,2m+1+j}^* \\ &= (\vec{0}^m, \vec{y}_{\iota,i,1}, \widetilde{r}_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}_\iota^*}, \text{ for } \iota \in [n].\end{aligned}$$

  b) $(i = \upsilon)$ $\mathcal{B}$ samples random $\wp_{\iota,\upsilon} \xleftarrow{\mathsf{U}} \mathbb{F}_q\backslash\{0\}$, $\theta_{\iota,\upsilon} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, for $\iota \in [n]$, such that $\sum_{\iota\in[n]} \wp_{\iota,\upsilon} = \sum_{\iota\in[n]} \theta_{\iota,\upsilon} = 0$, $\kappa_{\iota,\upsilon,1}, \ldots, \kappa_{\iota,\upsilon,k-1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, for $\iota \in [n]$, and computes

$$\boldsymbol{k}_{\iota,\upsilon}^* = \sum_{j\in[m]} y_{\iota,\upsilon,0}^{(j)} \boldsymbol{b}_{\iota,j}^* + \theta_{\iota,\upsilon} \boldsymbol{b}_{\iota,2m+1}^* + \sum_{j\in[k-1]} \kappa_{\iota,\upsilon,j} \boldsymbol{b}_{\iota,2m+1+j}^* + \wp_{\iota,\upsilon} \boldsymbol{\Upsilon}_{\iota,\hat{\beta}}, \quad \text{for } \iota \in [n].$$

  c) $(i > \upsilon)$ $\mathcal{B}$ selects random $r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, for $\iota \in [n]$, such that $\sum_{\iota\in[n]} r_{\iota,i} = 0$, $\gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, for $\iota \in [n]$, and computes

$$\begin{aligned}\boldsymbol{k}_{\iota,i}^* &= \sum_{j\in[m]} y_{\iota,i,0}^{(j)} \boldsymbol{b}_{\iota,j}^* + r_{\iota,i} \boldsymbol{b}_{\iota,2m+1}^* + \sum_{j\in[k-1]} \gamma_{\iota,i,j} \boldsymbol{b}_{\iota,2m+1+j}^* \\ &= (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}_\iota^*}, \text{ for } \iota \in [n].\end{aligned}$$

  $\mathcal{B}$ gives $\mathrm{SK}_i^* = \{\boldsymbol{k}_{\iota,i}^*\}_{\iota\in[n]}$ to $\mathcal{A}$.
- For all $\iota \in [n], t_\iota \in [q_{\mathrm{CT},\iota}]$, to answer the $t_\iota{}^{\mathrm{th}}$ ciphertext query of $\mathcal{A}$ with respect to index ι corresponding to pair of vectors $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}) \in (\mathbb{F}_q^m)^2$, $\mathcal{B}$ samples random $\varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and computes

$$\begin{aligned}\boldsymbol{c}_{\iota,t_\iota}^* &= \sum_{j\in[m]} x_{\iota,t_\iota,0}^{(j)} \boldsymbol{b}_{\iota,j} + \sum_{j\in[m]} x_{\iota,t_\iota,1}^{(j)} \boldsymbol{b}_{\iota,m+j} + \boldsymbol{b}_{\iota,2m+1} + \sum_{j\in[k]} \varphi_{\iota,t_\iota,j} \boldsymbol{b}_{\iota,2m+k+j} \\ &= (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota}.\end{aligned}$$

  $\mathcal{B}$ provides $\mathcal{A}$ with $\mathrm{CT}_{\iota,t_\iota}^* = (\iota, \boldsymbol{c}_{\iota,t_\iota}^*)$.

- $\mathcal{A}$ eventually outputs a guess bit $\beta' \in \{0,1\}$. $\mathcal{B}$ outputs $\hat{\beta}' = \beta'$ as its guess bit in its Problem 1^* challenge.

  Observe that if $\hat{\beta} = 0$, i.e., $\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\vec{0}^{2m}, \alpha_1, \ldots, \alpha_k, \vec{0}^{k}, 0)_{\mathbb{B}_\iota^*}$ for all $\iota \in [n]$, then we have

$$\boldsymbol{k}^*_{\iota,\upsilon} = (\vec{y}_{\iota,\upsilon,0}, \vec{0}^{m}, \alpha_1\wp_{\iota,\upsilon} + \theta_{\iota,\upsilon}, \alpha_2\wp_{\iota,\upsilon} + \kappa_{\iota,\upsilon,1}, \ldots, \alpha_k\wp_{\iota,\upsilon} + \kappa_{\iota,\upsilon,k-1}, \vec{0}^{k}, 0)_{\mathbb{B}_\iota^*} \quad \text{for all } \iota \in [n],$$

which is of the same form as that in **??**, where we have $r_{\iota,\upsilon} = \alpha_1\wp_{\iota,\upsilon} + \theta_{\iota,\upsilon}$, and $\gamma_{\iota,\upsilon,j} = \alpha_{j+1}\wp_{\iota,\upsilon} + \kappa_{\iota,\upsilon,j}$, for $j \in [k-1]$, and this is the proper form of $\boldsymbol{k}^*_{\iota,\upsilon}$ in $\mathsf{Hyb}_{2,\upsilon-1,3}$, for all $\iota \in [n]$. On the other hand, in case $\hat{\beta} = 1$, i.e., $\boldsymbol{\Upsilon}_{\iota,\hat{\beta}} = (\vec{0}^{2m}, \alpha_1, \ldots, \alpha_k, \vec{0}^{k}, \Im)_{\mathbb{B}_\iota^*}$, then we have

$$\boldsymbol{k}^*_{\iota,\upsilon} = (\vec{y}_{\iota,\upsilon,0}, \vec{0}^{m}, \alpha_1\wp_{\iota,\upsilon} + \theta_{\iota,\upsilon}, \alpha_2\wp_{\iota,\upsilon} + \kappa_{\iota,\upsilon,1}, \ldots, \alpha_k\wp_{\iota,\upsilon} + \kappa_{\iota,\upsilon,k-1}, \vec{0}^{k}, \Im\wp_{\iota,\upsilon})_{\mathbb{B}_\iota^*} \quad \text{for all } \iota \in [n],$$

which is of the same form as in **??**, where we have $r_{\iota,\upsilon} = \alpha_1\wp_{\iota,\upsilon} + \theta_{\iota,\upsilon}$, $\gamma_{\iota,\upsilon,j} = \alpha_{j+1}\wp_{\iota,\upsilon} + \kappa_{\iota,\upsilon,j}$, for $j \in [k-1]$, and $\omega_{\iota,\upsilon} = \Im\wp_{\iota,\upsilon}$, and this is the proper form of $\boldsymbol{k}^*_{\iota,\upsilon}$ in $\mathsf{Hyb}_{2,\upsilon,1}$, for all $\iota \in [n]$. In particular, notice that $\sum_{\iota\in[n]} r_{\iota,\upsilon} = 0 = \sum_{\iota\in[n]} \omega_{\iota,\upsilon}$. For $i < \upsilon$, $\boldsymbol{k}^*_{\iota,i}$ has the form as in **??**, for all $\iota \in [n]$, while for $i > \upsilon$, $\boldsymbol{k}^*_{\iota,i}$ is of the form as in **??**, for all $\iota \in [n]$. These are indeed the proper forms of $\boldsymbol{k}^*_{\iota,i}$ in the respective cases in both $\mathsf{Hyb}_{2,\upsilon-1,3}$ as well as in $\mathsf{Hyb}_{2,\upsilon,1}$, for all $\iota \in [n]$. Further, for all $\iota \in [n], t_\iota \in [q_{\text{CT},\iota}]$, the $t_\iota{}^{\text{th}}$ answered ciphertext with respect to index ι has the form as in **??** which is their proper form in both $\mathsf{Hyb}_{2,\upsilon-1,3}$ and $\mathsf{Hyb}_{2,\upsilon,1}$. Thus, the view of the adversary $\mathcal{A}$ simulated by $\mathcal{B}$ is distributed as in $\mathsf{Hyb}_{2,\upsilon-1,3}$ or $\mathsf{Hyb}_{2,\upsilon,1}$ according as $\hat{\beta} = 0$ or 1. This completes the proof of Lemma C.4. □

Lemma C.5: *For any probabilistic adversary $\mathcal{A}$, for any security parameter λ, we have*

$$\mathsf{Adv}^{(2,\upsilon,1)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(2,\upsilon,2)}_{\mathcal{A}}(\lambda), \text{ for all } \upsilon \in [q_{\text{KEY}}].$$

Proof: In order to prove Lemma C.5, we demonstrate that the view of the adversary $\mathcal{A}$ in $\mathsf{Hyb}_{2,\upsilon,1}$ and that in $\mathsf{Hyb}_{2,\upsilon,2}$ are identically distributed. Towards this end, we define new sets of dual orthogonal bases $\{\mathbb{U}_\iota = \{\boldsymbol{u}_{\iota,1}, \ldots, \boldsymbol{u}_{\iota,2m+2k+1}\}, \mathbb{U}^*_\iota = \{\boldsymbol{u}^*_{\iota,1}, \ldots, \boldsymbol{u}^*_{\iota,2m+2k+1}\}\}_{\iota\in[n]}$ of the pair of vector spaces $(\mathbb{V}_1 = \mathbb{G}_1^{2m+2k+1}, \mathbb{V}_2 = \mathbb{G}_2^{2m+2k+1})$ using the sets of dual orthogonal bases $\{\mathbb{B}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+2k+1}\}, \mathbb{B}^*_\iota = \{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+2k+1}\}\}_{\iota\in[n]}$ generated from $\mathcal{G}_{\text{OB}}(2m+2k+1, \mathsf{params}_{\mathbb{V}}, \nu)$ in $\mathsf{Hyb}_{2,\upsilon,1}$ as follows:

$$\begin{aligned}
\boldsymbol{u}_{\iota,j} &= \boldsymbol{b}_{\iota,j} - \frac{y^{(j)}_{\iota,\upsilon,0}}{\omega_{\iota,\upsilon}}\boldsymbol{b}_{\iota,2m+2k+1}, \text{ for } \iota \in [n], j \in [m] \\
\boldsymbol{u}_{\iota,m+j} &= \boldsymbol{b}_{\iota,m+j} + \frac{y^{(j)}_{\iota,\upsilon,1}}{\omega_{\iota,\upsilon}}\boldsymbol{b}_{\iota,2m+2k+1}, \text{ for } \iota \in [n], j \in [m] \\
\boldsymbol{u}_{\iota,2m+1} &= \boldsymbol{b}_{\iota,2m+1} + \frac{\vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,\upsilon,0} - \vec{x}_{\iota,1,1} \cdot \vec{y}_{\iota,\upsilon,1}}{\omega_{\iota,\upsilon}}\boldsymbol{b}_{\iota,2m+2k+1}, \text{ for } \iota \in [n] \\
\boldsymbol{u}_{\iota,j} &= \boldsymbol{b}_{\iota,j}, \text{ for } \iota \in [n], j \in [2m+2, 2m+2k+1] \\
\boldsymbol{u}^*_{\iota,2m+2k+1} &= \boldsymbol{b}^*_{\iota,2m+2k+1} + \sum_{j\in[m]} \frac{y^{(j)}_{\iota,\upsilon,0}}{\omega_{\iota,\upsilon}}\boldsymbol{b}^*_{\iota,j} - \sum_{j\in[m]} \frac{y^{(j)}_{\iota,\upsilon,1}}{\omega_{\iota,\upsilon}}\boldsymbol{b}^*_{\iota,m+j} + \\
&\qquad \frac{\vec{x}_{\iota,1,1} \cdot \vec{y}_{\iota,\upsilon,1} - \vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,\upsilon,0}}{\omega_{\iota,\upsilon}}\boldsymbol{b}^*_{\iota,2m+1}, \text{ for } \iota \in [n] \\
\boldsymbol{u}^*_{\iota,j} &= \boldsymbol{b}^*_{\iota,j}, \text{ for } \iota \in [n], j \in [2m+2k]
\end{aligned}$$

Note that $\{\mathbb{U}_\iota, \mathbb{U}^*_\iota\}_{\iota\in[n]}$ is indeed a set of dual orthogonal bases since those are obtained from the set of dual orthogonal bases $\{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota\in[n]}$ by applying invertible linear transformations. Further, $\{\mathbb{U}_\iota, \mathbb{U}^*_\iota\}_{\iota\in[n]}$ are distributed uniformly at random since $\{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota\in[n]}$ are so.

Now, observe that the components of the υ^{th} answered decryption key $\text{SK}^*_\upsilon = \{\boldsymbol{k}^*_{\iota,\upsilon}\}_{\iota\in[n]}$ corresponding to the pair of sets of n vectors $(\{\vec{y}_{\iota,\upsilon,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,\upsilon,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,\upsilon,0}, \vec{y}_{\iota,\upsilon,1} \in \mathbb{F}_q^m$ for all $\iota \in [n]$, in $\mathsf{Hyb}_{2,\upsilon,1}$ can be expressed as

$$\begin{aligned}
\boldsymbol{k}^*_{\iota,\upsilon} &= (\vec{y}_{\iota,\upsilon,0}, \vec{0}^{m}, r_{\iota,\upsilon}, \gamma_{\iota,\upsilon,1}, \ldots, \gamma_{\iota,\upsilon,k-1}, \vec{0}^{k}, \omega_{\iota,\upsilon})_{\mathbb{B}_\iota^*} \\
&= (\vec{0}^{m}, \vec{y}_{\iota,\upsilon,1}, \widetilde{r}_{\iota,\upsilon}, \gamma_{\iota,\upsilon,1}, \ldots, \gamma_{\iota,\upsilon,k-1}, \vec{0}^{k}, \omega_{\iota,\upsilon})_{\mathbb{U}_\iota^*}, \text{ for } \iota \in [n],
\end{aligned} \tag{C.1}$$

where $\widetilde{r}_{\iota,\upsilon} = r_{\iota,\upsilon} + \dfrac{\vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,\upsilon,0} - \vec{x}_{\iota,1,1}, \vec{y}_{\iota,\upsilon,1}}{\omega_{\iota,\upsilon}}$, for all $\iota \in [n]$. Observe that $\sum_{\iota \in [n]} \widetilde{r}_{\iota,\upsilon} = 0$ holds since $\sum_{\iota \in [n]} r_{\iota,\upsilon} = 0$ and $\sum_{\iota \in [n]} \vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,\upsilon,0} = \sum_{\iota \in [n]} \vec{x}_{\iota,1,1} \cdot \vec{y}_{\iota,\upsilon,1}$ by the restriction **??** on the queries of $\mathcal{A}$. Moreover, for all $\iota \in [n]$, $\widetilde{r}_{\iota,\upsilon}$ is distributed uniformly and independently over $\mathbb{F}_q$ since $r_{\iota,\upsilon}$ is so for all $\iota \in [n]$.

Clearly, for all $\iota \in [n]$, the form of $\boldsymbol{k}^*_{\iota,\upsilon}$ in **??** is identical to that in **??** that corresponds to $\mathsf{Hyb}_{2,\upsilon,2}$. Thus, the form of the υ^{th} answered decryption key $\text{SK}^*_\upsilon = \{\boldsymbol{k}^*_{\iota,\upsilon}\}_{\iota \in [n]}$ is switched from that in $\mathsf{Hyb}_{2,\upsilon,1}$ to that in $\mathsf{Hyb}_{2,\upsilon,2}$ through the basis transformations. Further, for all $i \neq \upsilon$, the components of the i^{th} answered decryption key $\text{SK}^*_i = \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in [n]}$ corresponding to the pair of sets of n vectors $(\{\vec{y}_{\iota,i,0}\}_{\iota \in [n]}, \{\vec{y}_{\iota,i,1}\}_{\iota \in [n]})$ such that $\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1} \in \mathbb{F}_q^m$, in $\mathsf{Hyb}_{2,\upsilon,1}$ can be expressed as follows:

a) $(i < \upsilon)$

$$\begin{aligned}\boldsymbol{k}^*_{\iota,i} &= (\vec{0}^m, \vec{y}_{\iota,i,1}, \widetilde{r}_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}^*_\iota} \\ &= (\vec{0}^m, \vec{y}_{\iota,i,1}, \widetilde{r}_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{U}^*_\iota}, \text{ for } \iota \in [n]\end{aligned}$$

b) $(i > \upsilon)$

$$\begin{aligned}\boldsymbol{k}^*_{\iota,i} &= (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}^*_\iota} \\ &= (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{U}^*_\iota}, \text{ for } \iota \in [n]\end{aligned}$$

Hence, we see that for all $i \neq \upsilon$, the forms of the components of $\text{SK}^*_i = \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in [n]}$ are preserved under the basis transformations.

On the other hand, for all $\iota \in [n], t_\iota \in [q_{\text{CT},\iota}]$, the $t_\iota{}^{\text{th}}$ answered ciphertext $\text{CT}^*_{\iota,t_\iota} = (\iota, \boldsymbol{c}^*_{\iota,t_\iota})$ for index ι corresponding to the pair of vectors $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}) \in (\mathbb{F}_q^m)^2$ in $\mathsf{Hyb}_{2,\upsilon,1}$ can be expressed as follows:

$$\begin{aligned}\boldsymbol{c}^*_{\iota,t_\iota} &= (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota} \\ &= (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, [\vec{x}_{\iota,t_\iota,0} \cdot \vec{y}_{\iota,\upsilon,0} - \vec{x}_{\iota,t_\iota,1} \cdot \vec{y}_{\iota,\upsilon,1} - \\ &\quad (\vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,\upsilon,0} - \vec{x}_{\iota,1,1} \cdot \vec{y}_{\iota,\upsilon,1})]/\omega_{\iota,\upsilon})_{\mathbb{U}_\iota} \\ &= (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{U}_\iota}\end{aligned}$$

The fact that $(\vec{x}_{\iota,t_\iota,0} \cdot \vec{y}_{\iota,\upsilon,0} - \vec{x}_{\iota,t_\iota,1} \cdot \vec{y}_{\iota,\upsilon,1}) - (\vec{x}_{\iota,1,0} \cdot \vec{y}_{\iota,\upsilon,0} - \vec{x}_{\iota,1,1} \cdot \vec{y}_{\iota,\upsilon,1}) = 0$ follows directly from the restriction **??** on the queries of the adversary $\mathcal{A}$. Thus, it follows that for all $\iota \in [n], t_\iota \in [q_{\text{CT},\iota}]$, the form of $\text{CT}^*_{\iota,t_\iota} = (\iota, \boldsymbol{c}^*_{\iota,t_\iota})$ is preserved under the basis transformations.

Moreover, observe that $e(\boldsymbol{u}_{\iota,j}, \boldsymbol{u}^*_{\iota,j}) = e(\boldsymbol{b}_{\iota,j}, \boldsymbol{b}^*_{\iota,j}) = g_T$ for all $\iota \in [n], j \in [2m + 2k + 1]$, and hence the basis transformations are compatible with the public parameters $\text{PP} = (\mathsf{params}_{\mathbb{V}}, g_T)$ in $\mathsf{Hyb}_{2,\upsilon,1}$ as well. Thus, it follows that the view of the adversary $\mathcal{A}$ in $\mathsf{Hyb}_{2,\upsilon,1}$ can be conceptually changed to that in $\mathsf{Hyb}_{2,\upsilon,2}$. □

Lemma C.6: *For any* PPT *adversary* $\mathcal{A}$ *between* $\mathsf{Hyb}_{2,\upsilon,2}$ *and* $\mathsf{Hyb}_{2,\upsilon,3}$, *there exists a* PPT *algorithm* $\mathcal{B}$ *for* Problem 1^* *such that for any security parameter* λ, *we have*

$$\left|\mathsf{Adv}^{(2,\upsilon,2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2,\upsilon,3)}_{\mathcal{A}}(\lambda)\right| \leq \mathsf{Adv}^{\text{P}_1{}^*}_{\mathcal{B}}(\lambda), \text{ for } \upsilon \in [q_{\text{KEY}}].$$

Proof: The proof of Lemma C.6 is the same as that of Lemma C.4, except for some minor modifications that are easy to find out. We omit the details to avoid repetition. □

Lemma C.7: *For any probabilistic adversary* $\mathcal{A}$, *for any security parameter* λ, *we have*

$$\mathsf{Adv}^{(2,q_{\text{KEY}},3)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda).$$

Proof: In order to prove Lemma C.7, we demonstrate that the view of the adversary $\mathcal{A}$ in $\mathsf{Hyb}_{2,q_{\text{KEY}},3}$ and that in Hyb_3 are identically distributed. Towards this end, we define new sets of dual orthogonal bases $\{\mathbb{U}_\iota = \{\boldsymbol{u}_{\iota,1}, \ldots, \boldsymbol{u}_{\iota,2m+2k+1}\}, \mathbb{U}^*_\iota = \{\boldsymbol{u}^*_{\iota,1}, \ldots, \boldsymbol{u}^*_{\iota,2m+2k+1}\}\}_{\iota \in [n]}$ of the pair of vector spaces $(\mathbb{V}_1 = \mathbb{G}_1^{2m+2k+1}, \mathbb{V}_2 = \mathbb{G}_2^{2m+2k+1})$ from the sets of dual orthogonal bases $\{\mathbb{B}_\iota = \{\boldsymbol{b}_{\iota,1}, \ldots, \boldsymbol{b}_{\iota,2m+2k+1}\}, \mathbb{B}^*_\iota =$

$\{\boldsymbol{b}^*_{\iota,1}, \ldots, \boldsymbol{b}^*_{\iota,2m+2k+1}\}\}_{\iota\in[n]}$ generated from $\mathcal{G}_{\mathrm{OB}}(2m+2k+1, \mathsf{params}_{\mathbb{V}}, \nu)$ in $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$ as follows:

$$\begin{aligned}
\boldsymbol{u}_{\iota,j} &= \boldsymbol{b}_{\iota,m+j}, \text{ for } \iota \in [n], j \in [m] \\
\boldsymbol{u}_{\iota,m+j} &= \boldsymbol{b}_{\iota,j}, \text{ for } \iota \in [n], j \in [m] \\
\boldsymbol{u}_{\iota,j} &= \boldsymbol{b}_{\iota,j}, \text{ for } \iota \in [n], j \in [2m+1, 2m+2k+1] \\
\boldsymbol{u}^*_{\iota,j} &= \boldsymbol{b}^*_{\iota,m+j}, \text{ for } \iota \in [n], j \in [m] \\
\boldsymbol{u}^*_{\iota,m+j} &= \boldsymbol{b}^*_{\iota,j}, \text{ for } \iota \in [n], j \in [m] \\
\boldsymbol{u}^*_{\iota,j} &= \boldsymbol{b}^*_{\iota,j}, \text{ for } \iota \in [n], j \in [2m+1, 2m+2k+1]
\end{aligned}$$

Note that $\{\mathbb{U}_\iota, \mathbb{U}^*_\iota\}_{\iota\in[n]}$ is indeed a set of dual orthogonal bases since those are obtained from the set of dual orthogonal bases $\{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota\in[n]}$ by applying invertible linear transformations. Further, $\{\mathbb{U}_\iota, \mathbb{U}^*_\iota\}_{\iota\in[n]}$ are distributed uniformly at random since $\{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota\in[n]}$ are so.

Now, observe that for all $\iota \in [n], t_\iota \in [q_{\mathrm{CT},\iota}]$, the $t_\iota{}^{\mathrm{th}}$ answered ciphertext $\mathrm{CT}^*_{\iota,t_\iota} = (\iota, \boldsymbol{c}^*_{\iota,t_\iota})$ for index ι corresponding to the pair of vectors $(\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}) \in (\mathbb{F}_q^m)^2$ in $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$ can be expressed as

$$\begin{aligned}
\boldsymbol{c}^*_{\iota,t_\iota} &= (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{B}_\iota} \\
&= (\vec{x}_{\iota,t_\iota,1}, \vec{x}_{\iota,t_\iota,0}, 1, \vec{0}^{k-1}, \varphi_{\iota,t_\iota,1}, \ldots, \varphi_{\iota,t_\iota,k}, 0)_{\mathbb{U}_\iota},
\end{aligned}$$

which is of the same form as that in **??** that corresponds to Hyb_3. Thus, the form of $\mathrm{CT}^*_{\iota,t_\iota} = (\iota, \boldsymbol{c}^*_{\iota,t_\iota})$ in $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$ is changed to that in Hyb_3 through the basis transformations.

On the other hand, for all $i \in [q_{\mathrm{KEY}}]$, the components of the i^{th} answered decryption key $\mathrm{SK}^*_i = \{\boldsymbol{k}^*_{\iota,i}\}_{\iota\in[n]}$ corresponding to the pair of sets of n vectors $(\{\vec{y}_{\iota,i,0}\}_{\iota\in[n]}, \{\vec{y}_{\iota,i,1}\}_{\iota\in[n]})$ such that $\vec{y}_{\iota,i,0}, \vec{y}_{\iota,i,1} \in \mathbb{F}_q^m$, in $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$ can be expressed as

$$\begin{aligned}
\boldsymbol{k}^*_{\iota,i} &= (\vec{0}^m, \vec{y}_{\iota,i,1}, \widetilde{r}_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{B}^*_\iota} \\
&= (\vec{y}_{\iota,i,1}, \vec{0}^m, \widetilde{r}_{\iota,i}, \gamma_{\iota,i,1}, \ldots, \gamma_{\iota,i,k-1}, \vec{0}^k, 0)_{\mathbb{U}^*_\iota}, \text{ for } \iota \in [n].
\end{aligned}$$

Clearly, for all $\iota \in [n], i \in [q_{\mathrm{KEY}}]$, the form of $\boldsymbol{k}^*_{\iota,i}$ above is identical to that in **??** that corresponds to Hyb_3. Thus, for all $i \in [q_{\mathrm{KEY}}]$, the form of the i^{th} answered decryption key $\mathrm{SK}^*_i = \{\boldsymbol{k}^*_{\iota,i}\}_{\iota\in[n]}$ is also switched from that in $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$ to that in Hyb_3 through the basis transformations.

Moreover, observe that for all $\iota \in [n]$,

$$e(\boldsymbol{u}_{\iota,j}, \boldsymbol{u}^*_{\iota,j}) = \begin{cases} e(\boldsymbol{b}_{\iota,m+j}, \boldsymbol{b}^*_{\iota,m+j}) = g_T, \text{ for } j \in [m] \\ e(\boldsymbol{b}_{\iota,j-m}, \boldsymbol{b}^*_{\iota,j-m}) = g_T, \text{ for } j \in [m+1, 2m] \\ e(\boldsymbol{b}_{\iota,j}, \boldsymbol{b}^*_{\iota,j}) = g_T, \quad \text{for } j \in [2m+1, 2m+2k+1] \end{cases},$$

and hence the basis transformations are compatible with the public parameters $\mathrm{PP} = (\mathsf{params}_{\mathbb{V}}, g_T)$ in $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$ as well. Thus, it follows that the view of the adversary $\mathcal{A}$ in $\mathsf{Hyb}_{2,q_{\mathrm{KEY}},3}$ can be conceptually changed to that in Hyb_3. □

D Lemmas for the Proof of Theorem 4.1

Remark D.1: In some hybrids, a reduction algorithm needs to simulate random functions, which are changed from pseudorandom functions. For the simulation, the algorithm makes a list L for a random function R. When the algorithm needs to evaluate a random function with an input ι, it looks up (ι, v_ι) from L. If there is such a pair (ι, v_ι), then the algorithm uses v_ι as the output of the random function. Otherwise, it chooses a random value v_ι from its range and makes it the output of the random function. Then it adds the pair (ι, v_ι) into the list L. For ease of exposition, we express the above operation just as $v_\iota = R(\iota)$.

Lemma D.1: *For any* PPT *adversary* $\mathcal{A}$ *between* Hyb_0 *and* Hyb_1*, there exist* PPT *adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *against* PRFs *such that for any* λ*, we have*

$$|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathrm{PRF}_1}_{\mathcal{B}_1}(\lambda) + \mathsf{Adv}^{\mathrm{PRF}_2}_{\mathcal{B}_2}(\lambda).$$

Proof: This lemma directly follows from the definition of PRFs. □

Lemma D.2: *For any* PPT *adversary* $\mathcal{A}$ *between* Hyb_1 *and* Hyb_2*, there exists* PPT *adversaries* $\mathcal{B}$ *for* Problem 1 (*Definition 2.5*) *such that for any* λ*, we have*

$$|\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2)}_{\mathcal{A}}(\lambda)| \leq 2 \sum_{\iota \in [2^\lambda]} q_{\mathrm{CT},\iota} \mathsf{Adv}^{\mathrm{P1}}_{\mathcal{B}}(\lambda).$$

Proof (sketch): We can prove this lemma similarly to the Hyb_1 sequence in the bounded scheme (Section 3.2). When we embed Problem 1 into hybrids, we proceed as follows.

1. First, the challenger $\mathcal{B}$ receives an instance of Problem 1 with $n = 1$; $(\mathsf{params}_{\mathbb{V}}, g_T, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{\Upsilon}_\beta)$, and sets $(\widehat{\mathbb{D}}, \widehat{\mathbb{D}}^*) = (\widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$ as MSK.
2. When $\mathcal{B}$ is queried about a ciphertext for the index ι, it creates the basis as $W_\iota = R_1(\iota)$, $\widehat{\mathbb{B}}_\iota = \widehat{\mathbb{D}} W_\iota$. Then it encrypts the message using the basis.
3. The simulation of the decryption key query is almost same as the ciphertext query.
4. When $\mathcal{B}$ embeds the problem into the ciphertext, it uses $\boldsymbol{\Upsilon}_\beta W_\iota$ to creates the ciphertext.
5. Finally, $\mathcal{B}$ makes use of the output of the adversary.

□

Lemma D.3: *Let* n_{max} *be the maximum index of a decryption key that* $\mathcal{A}$ *queries, i.e.,* $S_i \subseteq [n_{max}]$ *for all* $i \in [q_{\mathrm{SK}}]$*. For any* PPT *adversary* $\mathcal{A}$ *between* $\mathsf{Hyb}_{3,\upsilon-1}$ *and* $\mathsf{Hyb}_{3,\upsilon}$ *for* $\upsilon \in [q_{\mathrm{KEY}}]$*, there exists* PPT *adversaries* $\mathcal{B}_1$ *for* Problem 1^* (*Definition 2.6*) *and* $\mathcal{B}_2$ *for* SKE *such that for any* λ*, we have*

$$|\mathsf{Adv}^{(3,\upsilon-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3,\upsilon)}_{\mathcal{A}}(\lambda)| \leq 2\mathsf{Adv}^{\mathrm{P1}^*}_{\mathcal{B}_1}(\lambda) + n_{max}\mathsf{Adv}^{\mathrm{SKE}}_{\mathcal{B}_2}(\lambda).$$

Proof: In $\mathsf{Hyb}_{3,\upsilon-1}$ and $\mathsf{Hyb}_{3,\upsilon}$, we can classify the experiment into the following two types with respect to the υ^{th} key query.

1. For all $\iota \in S_\upsilon$, $q_{\mathrm{CT},\iota} \geq 1$.
2. There exists $\iota \in S_\upsilon$ s.t. $q_{\mathrm{CT},\iota} = 0$.

Let X_j be a random variable over $\{1, 2\}$. We define $X_j = \ell$ if the ℓ^{th} event above occurs in the end of $\mathsf{Hyb}_{3,j}$. We also define P_j as an event that $\mathcal{A}$ outputs 1 in $\mathsf{Hyb}_{3,j}$. Namely, $\mathsf{Adv}^{(3,j)}_{\mathcal{A}}(\lambda) = \Pr[P_j]$. Then, we have

$$\begin{aligned}
&|\mathsf{Adv}^{(3,\upsilon-1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3,\upsilon)}_{\mathcal{A}}(\lambda)| = |\Pr[P_{\upsilon-1}] - \Pr[P_\upsilon]| \\
=& \left| \begin{array}{r} \Pr[X_{\upsilon-1} = 1] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 1] - \Pr[X_\upsilon = 1] \Pr[P_\upsilon | X_\upsilon = 1] \\ + \Pr[X_{\upsilon-1} = 2] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 2] - \Pr[X_\upsilon = 2] \Pr[P_\upsilon | X_\upsilon = 2] \end{array} \right|.
\end{aligned}$$

First, we consider the case of the event 1.

Lemma D.4: *For any* PPT *adversary* $\mathcal{A}$*, there exists a* PPT *adversary* $\mathcal{B}_1$ *for* Problem 1^* (*Definition 2.6*) *such that for any* λ*, we have*

$$|\Pr[X_{\upsilon-1} = 1] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 1] - \Pr[X_\upsilon = 1] \Pr[P_\upsilon | X_\upsilon = 1]| \leq 2\mathsf{Adv}^{\mathrm{P1}^*}_{\mathcal{B}_1}(\lambda).$$

Proof: Let $\mathsf{Hyb}_{3,\upsilon-1,1}, \mathsf{Hyb}_{3,\upsilon-1,2}$ be intermediate hybrids between $\mathsf{Hyb}_{3,\upsilon-1}$ and $\mathsf{Hyb}_{3,\upsilon}$, and defined as follows.

$\mathsf{Hyb}_{3,\upsilon-1,1}$ ($\upsilon \in [q_{\mathsf{key}}]$): This hybrid is identical to $\mathsf{Hyb}_{3,\upsilon-1}$ except that the υ^{th} decryption key query is replied as

$$\begin{aligned}
&r_{\iota,\upsilon}, \gamma_{\iota,\upsilon} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_\upsilon} r_{\iota,\upsilon} = \sum_{\iota \in S_\upsilon} \gamma_{\iota,\upsilon} = 0, \ \ W_\iota = R_1(\iota), \ \ \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,\upsilon} = (\vec{\boldsymbol{y}}_{\iota,\upsilon,0}, \vec{0}^m, r_{\iota,\upsilon}, 0, \boxed{\gamma_{\iota,\upsilon}})_{\mathbb{B}^*_\iota} \quad \text{for } \iota \in S_\upsilon, \\
&C_{|S_\upsilon|} = \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,|S_\upsilon|}), \ldots, \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,1}), \{\boldsymbol{k}^*_{\iota,\upsilon}\}_{\iota \in S_\upsilon}) \ldots), \\
&\mathrm{SK}^*_{S_\upsilon,\upsilon} = (C_{|S_\upsilon|}, S_\upsilon).
\end{aligned}$$

$\mathsf{Hyb}_{3,\upsilon-1,2}$ ($\upsilon \in [q_{\mathsf{key}}]$): This hybrid is identical to $\mathsf{Hyb}_{3,\upsilon-1,1}$ except that the υ^{th} decryption key query is replied as

$$
\begin{aligned}
&r_{\iota,\upsilon}, \gamma_{\iota,\upsilon} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_\upsilon} r_{\iota,\upsilon} = \sum_{\iota \in S_\upsilon} \gamma_{\iota,\upsilon} = 0, \ \ W_\iota = R_1(\iota), \ \ \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,\upsilon} = (\boxed{\vec{0}^m, \vec{y}_{\iota,\upsilon,1}}, r_{\iota,\upsilon}, 0, \gamma_{\iota,\upsilon})_{\mathbb{B}^*_\iota} \quad \text{for } \iota \in S_\upsilon, \\
&C_{|S_\upsilon|} = \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,|S_\upsilon|}), \ldots, \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,1}), \{\boldsymbol{k}^*_{\iota,\upsilon}\}_{\iota \in S_\upsilon}) \ldots), \\
&\mathrm{SK}^*_{S_\upsilon,\upsilon} = (C_{|S_\upsilon|}, S_\upsilon).
\end{aligned}
$$

Then we consider following lemmas.

Lemma D.5: *For any* PPT *adversary* $\mathcal{A}$*, there exists a* PPT *adversary* $\mathcal{B}$ *for the* Problem 1^* *such that for any* λ*, we have*

$$
\left| \begin{array}{l} \Pr[X_{\upsilon-1} = 1] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 1] \\ - \Pr[X_{\upsilon-1,1} = 1] \Pr[P_{\upsilon-1,1} | X_{\upsilon-1,1} = 1] \end{array} \right| \leq \mathsf{Adv}^{\mathrm{P}_{1^*}}_{\mathcal{B}}(\lambda).
$$

Lemma D.6: *For any* PPT *adversary* $\mathcal{A}$*, we have*

$$
\Pr[X_{\upsilon-1,1} = 1] \Pr[P_{\upsilon-1,1} | X_{\upsilon-1,1} = 1] = \Pr[X_{\upsilon-1,2} = 1] \Pr[P_{\upsilon-1,2} | X_{\upsilon-1,2} = 1].
$$

Lemma D.7: *For any* PPT *adversary* $\mathcal{A}$*, there exists a* PPT *adversary* $\mathcal{B}$ *for the* Problem 1^* *such that for any* λ*, we have*

$$
\left| \begin{array}{l} \Pr[X_{\upsilon-1,2} = 1] \Pr[P_{\upsilon-1,2} | X_{\upsilon-1,2} = 1] \\ - \Pr[X_\upsilon = 1] \Pr[P_\upsilon | X_\upsilon = 1] \end{array} \right| \leq \mathsf{Adv}^{\mathrm{P}_{1^*}}_{\mathcal{B}}(\lambda).
$$

Proof (of Lemma D.5): Let $\mathcal{B}$ behaves as follows.

1. $\mathcal{B}$ is given an instance of Problem 1^* with $n = 1$; $(\mathsf{params}_{\mathbb{V}}, g_T, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \boldsymbol{\Upsilon}_\beta)$ and sets $(\widehat{\mathbb{D}}, \widehat{\mathbb{D}}^*) = (\widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$ as MSK. It gives $(\mathsf{params}_{\mathbb{V}}, g_T)$ as PP to $\mathcal{A}$.
2. In the ciphertext query, $\mathcal{B}$ replies for $t_\iota{}^{\text{th}}$ ciphertext query for index ι as
$$
\begin{aligned}
&W_\iota = R_1(\iota), \ \ \widehat{\mathbb{B}}_\iota = \widehat{\mathbb{D}} W_\iota, \ \ \kappa_{\iota,t_\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\
&\boldsymbol{c}^*_{\iota,t_\iota} = (\vec{x}_{\iota,t_\iota,0}, \vec{x}_{\iota,t_\iota,1}, 1, \kappa_{\iota,t_\iota}, 0)_{\mathbb{B}_\iota}, \quad k_\iota = R_2(\iota), \ \ \mathrm{CT}^*_{\iota,t_\iota} = (\boldsymbol{c}^*_{\iota,t_\iota}, k_\iota, \iota).
\end{aligned}
$$
3. In the decryption key query, for all $i \leq \upsilon - 1$, $\mathcal{B}$ generates the i^{th} decryption keys as
$$
\begin{aligned}
&r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_i} r_{\iota,i} = 0, \ \ W_\iota = R_1(\iota), \ \ \widehat{\mathbb{B}}^*_\iota = \widehat{\mathbb{D}}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,i} = (\vec{0}^m, \vec{y}_{\iota,i,1}, r_{\iota,i}, \vec{0}^2)_{\mathbb{B}^*_\iota} \quad \text{for } \iota \in S_i, \\
&C_{|S_i|} = \mathsf{SKE.Encrypt}(R_2(s_{i,|S_i|}), \ldots, \mathsf{SKE.Encrypt}(R_2(s_{i,1}), \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in S_i}) \ldots), \\
&\mathrm{SK}^*_{S_i,i} = (C_{|S_i|}, S_i).
\end{aligned}
$$
4. For the υ^{th} key query, $\mathcal{B}$ makes a decryption key as
$$
\begin{aligned}
&r'_{\iota,\upsilon}, \gamma'_{\iota,\upsilon} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_\upsilon} r'_{\iota,\upsilon} = \sum_{\iota \in S_\upsilon} \gamma'_{\iota,\upsilon} = 0, \ \ W_\iota = R_1(\iota), \ \ \widehat{\mathbb{B}}^*_\iota = \widehat{\mathbb{D}}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,\upsilon,\beta} = \sum_{\eta=1}^{m} y_{\iota,\upsilon,0,\eta} \boldsymbol{b}^*_{\iota,\eta} + r'_{\iota,\upsilon} \boldsymbol{b}^*_{\iota,2m+1} + \gamma'_{\iota,\upsilon} \boldsymbol{\Upsilon}_\beta W^*_\iota \quad \text{for } \iota \in S_\upsilon, \\
&C_{|S_\upsilon|} = \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,|S_\upsilon|}), \ldots, \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,1}), \{\boldsymbol{k}^*_{\iota,\upsilon}\}_{\iota \in S_\upsilon}) \ldots), \\
&\mathrm{SK}^*_{S_\upsilon,\upsilon} = (C_{|S_\upsilon|}, S_\upsilon).
\end{aligned}
$$

   We can see that
$$
\begin{aligned}
&\boldsymbol{k}^*_{\iota,\upsilon,0} = (\vec{y}_{\iota,\upsilon,0}, \vec{0}^m, r'_{\iota,\upsilon} + \gamma'_{\iota,\upsilon}\alpha_1, 0, 0)_{\mathbb{B}^*_\iota} = (\vec{y}_{\iota,\upsilon,0}, \vec{0}^m, r_{\iota,\upsilon}, 0, 0)_{\mathbb{B}^*_\iota}, \\
&\boldsymbol{k}^*_{\iota,\upsilon,1} = (\vec{y}_{\iota,\upsilon,0}, \vec{0}^m, r'_{\iota,\upsilon} + \gamma'_{\iota,\upsilon}\alpha_1, 0, \gamma'_{\iota,\upsilon}\Im)_{\mathbb{B}^*_\iota} = (\vec{y}_{\iota,\upsilon,0}, \vec{0}^m, r_{\iota,\upsilon}, 0, \gamma_{\iota,\upsilon})_{\mathbb{B}^*_\iota},
\end{aligned}
$$
   where $r_{\iota,\upsilon} = r'_{\iota,\upsilon} + \gamma'_{\iota,\upsilon}\alpha_1$ and $\gamma_{\iota,\upsilon} = \gamma'_{\iota,\upsilon}\Im$.

5. The other key queries are replied as

$$
\begin{aligned}
&r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_i} r_{\iota,i} = 0, \ \ W_\iota = R_1(\iota), \ \ \widehat{\mathbb{B}}^*_\iota = \widehat{\mathbb{D}}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,i} = (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \vec{0}^2)_{\mathbb{B}^*_\iota} \quad \text{for } \iota \in S_i, \\
&C_{|S_i|} = \mathsf{SKE.Encrypt}(R_2(s_{i,|S_i|}), \ldots, \mathsf{SKE.Encrypt}(R_2(s_{i,1}), \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in S_i}) \ldots), \\
&\mathrm{SK}^*_{S_i,i} = (C_{|S_i|}, S_i).
\end{aligned}
$$

6. If the event 2 occurs in the end of the experiment, i.e., there exists $\iota \in S_\upsilon$ s.t. $q_{\mathrm{CT},\iota} = 0$, then $\mathcal{B}$ abort and outputs 0.
7. Finally, $\mathcal{A}$ outputs β', then $\mathcal{B}$ outputs β' as it is.

Observe that $\mathcal{A}'$s view is identical to $\mathsf{Hyb}_{3,\upsilon-1}$ if $\beta = 0$, and it is identical to $\mathsf{Hyb}_{3,\upsilon-1,1}$ if $\beta = 1$. Then if $\beta = 0$, the probability $\mathcal{B}$ outputs 1 is $\Pr[X_{\upsilon-1} = 1] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 1]$ and if $\beta = 1$, the probability is $\Pr[X_{\upsilon-1,1} = 1] \Pr[P_{\upsilon-1,1} | X_{\upsilon-1,1} = 1]$. □

Proof (Lemma D.6): The proof of this lemma is almost the same as that of Lemma C.5, so we omit the proof. Note that under the event 1, i.e., for all $\iota \in S_\upsilon$, $q_{\mathrm{CT},\iota} \geq 1$, all ciphertext queries for index $\iota \in S_\upsilon$ satisfy the conditions in Definition 2.9. That is, for all $\{t_\iota\}_{\iota \in S_\upsilon} \in \prod_{\iota \in S_\upsilon} [q_{\mathrm{CT},\iota}]$ we must have $\sum_{\iota \in S_\upsilon} \vec{x}_{\iota,t_\iota,0} \cdot \vec{y}_{\iota,\upsilon,0} = \sum_{\iota \in S_\upsilon} \vec{x}_{\iota,t_\iota,1} \cdot \vec{y}_{\iota,\upsilon,1}$. Therefore we can consider the same kind of basis change in Lemma C.5. □

Proof (Lemma D.7): The proof of this lemma is almost the same as that of Lemma D.5, so we omit the proof. □

From above lemmas, we can see that

$$
\begin{aligned}
&|\Pr[X_{\upsilon-1} = 1] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 1] - \Pr[X_\upsilon = 1] \Pr[P_\upsilon | X_\upsilon = 1]| \\
\leq &|\Pr[X_{\upsilon-1} = 1] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 1] - \Pr[X_{\upsilon-1,1} = 1] \Pr[P_{\upsilon-1,1} | X_{\upsilon-1,1} = 1]| \\
&+ |\Pr[X_{\upsilon-1,1} = 1] \Pr[P_{\upsilon-1,1} | X_{\upsilon-1,1} = 1] - \Pr[X_{\upsilon-1,2} = 1] \Pr[P_{\upsilon-1,2} | X_{\upsilon-1,2} = 1]| \\
&+ |\Pr[X_{\upsilon-1,2} = 1] \Pr[P_{\upsilon-1,2} | X_{\upsilon-1,2} = 1] - \Pr[X_\upsilon = 1] \Pr[P_\upsilon | X_\upsilon = 1]| \\
\leq &2\mathsf{Adv}^{\mathrm{P}_1*}_{\mathcal{B}_1}(\lambda).
\end{aligned}
$$

□

Next, we consider the case of the event 2.

Lemma D.8: *For any* PPT *adversary* $\mathcal{A}$*, there exists a* PPT *adversary* $\mathcal{B}_2$ *for* SKE *such that for any* λ*, we have*

$$|\Pr[X_{\upsilon-1} = 2] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 2] - \Pr[X_\upsilon = 2] \Pr[P_\upsilon | X_\upsilon = 2]| \leq n_{max} \mathsf{Adv}^{\mathrm{SKE}}_{\mathcal{B}_2}(\lambda).$$

Proof: In decryption key query, a set S queried by an adversary must be a subset of $[t(\lambda)]$ for any polynomial t. We can consider that for each adversary $\mathcal{A}$, it has some polynomial $t_\mathcal{A}$ such that all sets that $\mathcal{A}$ makes decryption key queries for are in $[t_\mathcal{A}(\lambda)]$, i.e., $n_{max} = t_\mathcal{A}(\lambda)$. Then it is sufficient to prove that there exists a (possibly different) PPT algorithm $\mathcal{B}_2$ for each $\mathcal{A}$ s.t. above inequality holds. Without loss of generality, we can assume that $\mathcal{B}_2$ knows n_{max}. Let $\mathcal{B}_2$ behaves as follows. $\mathcal{B}_2$ has an access to an SKE oracle $\mathcal{O}_\beta$, which return the encryption of m_β when it receives (m_0, m_1). Let $\widehat{S}_\upsilon$ be a subset of S_υ whose elements are indices for which $\mathcal{A}$ does not make a ciphertext query thorough the experiment.

1. First, $\mathcal{B}_2$ creates PP and bases $(\widehat{\mathbb{D}}, \widehat{\mathbb{D}}^*)$, and give PP to $\mathcal{A}$.
2. $\mathcal{B}_2$ chooses $\iota' \xleftarrow{\mathsf{U}} [n_{max}]$ as a conjecture of the minimum element of $\widehat{S}_\upsilon$.
3. In ciphertext query, $\mathcal{B}_2$ encrypts messages in the same way as Hyb_2. If a ciphertext for index ι' is queried, then $\mathcal{B}_2$ aborts and outputs 0.
4. For $i < \upsilon$, $\mathcal{B}_2$ replies for the i^{th} key query with a set S_i as follows. We denote the j^{th} element of S_i in ascending order by $s_{i,j}$.
   – Let $\boldsymbol{k}^*_{\iota,i}$ for all $\iota \in S_i$ be

$$
\begin{aligned}
&r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_i} r_{\iota,i} = 0, \ \ W_\iota = R_1(\iota), \ \ \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\
&\boldsymbol{k}^*_{\iota,i} = (\vec{0}^m, \vec{y}_{\iota,i,1}, r_{\iota,i}, \vec{0}^2)_{\mathbb{B}^*_\iota}.
\end{aligned}
$$

– If $\iota' \notin S_i$, $\mathcal{B}_2$ computes $C_{|S_i|}$ as

$$\begin{aligned} C_1 =& \mathsf{SKE.Encrypt}(R_2(s_{i,1}), \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in S_i}) \\ C_2 =& \mathsf{SKE.Encrypt}(R_2(s_{i,2}), C_1), \\ & \vdots \\ C_{|S_i|} =& \mathsf{SKE.Encrypt}(R_2(s_{i,|S_i|}), C_{|S_i|-1}). \end{aligned}$$

If $\iota' \in S_i$, $\mathcal{B}_2$ computes $C_{|S_i|}$ as follows. First, $\mathcal{B}_2$ computes C_j by iterating encryption as above, where j is the maximum index s.t. $s_{i,j} < \iota'$, i.e., $\iota' = s_{i,j+1}$. Namely,

$$\begin{aligned} C_1 =& \mathsf{SKE.Encrypt}(R_2(s_{i,1}), \{\boldsymbol{k}^*_{\iota,i}\}_{\iota \in S_i}) \\ C_2 =& \mathsf{SKE.Encrypt}(R_2(s_{i,2}), C_1), \\ & \vdots \\ C_j =& \mathsf{SKE.Encrypt}(R_2(s_{i,j}), C_{j-1}). \end{aligned}$$

Then it inputs a pair of the identical two messages (C_j, C_j) into $\mathcal{O}_\beta$ and defines the output as C_{j+1}. Finally, if $|S_i| > j+1$, continues encryption of SKE as

$$\begin{aligned} C_{j+2} =& \mathsf{SKE.Encrypt}(R_2(s_{i,j+2}), C_{j+1}), \\ & \vdots \\ C_{|S_i|} =& \mathsf{SKE.Encrypt}(R_2(s_{i,|S_i|}), C_{|S_i|-1}). \end{aligned}$$

– $\mathcal{B}_2$ returns $\mathrm{SK}^*_{S_i,i} = (C_{|S_i|}, S_i)$ to $\mathcal{A}$.

5. For the υ^{th} key query with a set S_υ, if $\iota' \notin S_\upsilon$, $\mathcal{B}_2$ aborts and outputs 0. Otherwise, it proceeds as follows.
   – For all $\iota \in S_\upsilon$ and $\beta \in \{0,1\}$, let $\boldsymbol{k}^*_{\iota,\upsilon,\beta}$ be

$$\begin{aligned} & r_{\iota,\upsilon} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_\upsilon} r_{\iota,\upsilon} = 0, \ \ W_\iota = R_1(\iota), \ \ \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\ & \boldsymbol{k}^*_{\iota,\upsilon,0} = (\vec{y}_{\iota,\upsilon,0}, \vec{0}^m, r_{\iota,\upsilon}, \vec{0}^2)_{\mathbb{B}^*_\iota}, \quad \boldsymbol{k}^*_{\iota,\upsilon,1} = (\vec{0}^m, \vec{y}_{\iota,\upsilon,1}, r_{\iota,\upsilon}, \vec{0}^2)_{\mathbb{B}^*_\iota}. \end{aligned}$$

   – $\mathcal{B}_2$ computes $C_{|S_\upsilon|,\beta}$ as follows. Let j be the maximum index s.t. $s_{\upsilon,j} < \iota'$. First, it computes $C_{j,0}$ and $C_{j,1}$ as

$$\begin{aligned} C_{1,\beta} =& \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,1}), \{\boldsymbol{k}^*_{\iota,\upsilon,\beta}\}_{\iota \in S_\upsilon}) \\ C_{2,\beta} =& \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,2}), C_{1,\beta}), \\ & \vdots \\ C_{j,\beta} =& \mathsf{SKE.Encrypt}(R_2(s_{\upsilon,j}), C_{j-1,\beta}) \quad \text{for } \beta \in \{0,1\}. \end{aligned}$$

   Then it inputs a pair of two messages $(C_{j,0}, C_{j,1})$ into $\mathcal{O}_\beta$ and defines the output as $C_{j+1,\beta}$. If $|S_\upsilon| > j+1$, it iteratively encrypts $C_{j+1,\beta}$ until getting $C_{|S_\upsilon|,\beta}$ in the same way as step 4.
   – $\mathcal{B}_2$ returns $\mathrm{SK}^*_{S_\upsilon,\upsilon,\beta} = (C_{|S_\upsilon|,\beta}, S_\upsilon)$ to $\mathcal{A}$.

6. For $i > \upsilon$, $\mathcal{B}_2$ replies for the i^{th} key query with a set S_i as follows.
   – Let $\boldsymbol{k}^*_{\iota,i}$ for all $\iota \in S_i$ be

$$\begin{aligned} & r_{\iota,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ \text{ s.t. } \sum_{\iota \in S_i} r_{\iota,i} = 0, \ \ W_\iota = R_1(\iota), \ \ \mathbb{B}^*_\iota = \mathbb{D}^* W^*_\iota, \\ & \boldsymbol{k}^*_{\iota,i} = (\vec{y}_{\iota,i,0}, \vec{0}^m, r_{\iota,i}, \vec{0}^2)_{\mathbb{B}^*_\iota}. \end{aligned}$$

   – The remaining procedure is the same as step 4.

7. During the experiment, if the event 1 occurs i.e., for all $\iota \in S_\upsilon$, $q_{\mathrm{CT},\iota} \geq 1$, then $\mathcal{B}_2$ aborts and outputs 0.
8. In the end of the experiment, if ι' is not the minimum element of $\widehat{S}_\upsilon$, then $\mathcal{B}_2$ aborts and outputs 0.
9. Finally, $\mathcal{A}$ outputs β', then $\mathcal{B}_2$ outputs β' as it is.

$\mathcal{B}_2$ implicitly sets $R_2(\iota') = K_{\mathcal{O}_\beta}$, where $K_{\mathcal{O}_\beta}$ is a secret key used in $\mathcal{O}_\beta$. Observe that $\mathcal{A}'$s view is identical to $\mathsf{Hyb}_{3,\upsilon-1}$ if $\beta = 0$, and it is identical to $\mathsf{Hyb}_{3,\upsilon}$ if $\beta = 1$. Then if $\beta = 0$, the probability $\mathcal{B}_2$ outputs 1 is $\Pr[X_{\upsilon-1} = 2] \Pr[P_{\upsilon-1} \wedge \iota' = \min \widehat{S}_\upsilon | X_{\upsilon-1} = 2]$ and if $\beta = 1$, the probability is $\Pr[X_\upsilon = 2] \Pr[P_\upsilon \wedge \iota' = \min \widehat{S}_\upsilon | X_\upsilon = 2]$. Note that $P_{\upsilon-1}$ (resp. P_υ) and $\iota' = \min \widehat{S}_\upsilon$ under $X_{\upsilon-1} = 2$ (resp. $X_\upsilon = 2$) are independent events, and ι' is uniformly chosen from $[n_{max}]$. Then, we have

$$\begin{aligned}
&\Pr[X_{\upsilon-1} = 2] \Pr[P_{\upsilon-1} \wedge \iota' = \min \widehat{S}_\upsilon | X_{\upsilon-1} = 2] \\
=&\Pr[X_{\upsilon-1} = 2] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 2] \Pr[\iota' = \min \widehat{S}_\upsilon | X_{\upsilon-1} = 2] \\
=&\frac{1}{n_{max}} \Pr[X_{\upsilon-1} = 2] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 2], \\
&\Pr[X_\upsilon = 2] \Pr[P_\upsilon \wedge \iota' = \min \widehat{S}_\upsilon | X_\upsilon = 2] \\
=&\frac{1}{n_{max}} \Pr[X_\upsilon = 2] \Pr[P_\upsilon | X_\upsilon = 2].
\end{aligned}$$

Consequently,

$$|\Pr[X_{\upsilon-1} = 2] \Pr[P_{\upsilon-1} | X_{\upsilon-1} = 2] - \Pr[X_\upsilon = 2] \Pr[P_\upsilon | X_\upsilon = 2]| \leq n_{max} \mathsf{Adv}^{\mathrm{SKE}}_{\mathcal{B}_2}(\lambda).$$

□

From Lemma D.4 and D.8, Lemma D.3 holds. □

Lemma D.9: *For any* PPT *adversary* $\mathcal{A}$ *between* $\mathsf{Hyb}_{3,q_{\mathrm{KEY}}}$ *and* Hyb_4*, we have*

$$\mathsf{Adv}^{(3,q_{\mathrm{KEY}})}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda).$$

Proof: This lemma can be proven similarly to Lemma C.7.

Lemma D.10: *For any* PPT *adversary* $\mathcal{A}$ *between* Hyb_4 *and* Hyb_5*, there exist* PPT *adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *against* PRFs *and* $\mathcal{B}_3$ *for* Problem 1 *such that for any* λ*, we have*

$$|\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(5)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathrm{PRF}_1}_{\mathcal{B}_1}(\lambda) + \mathsf{Adv}^{\mathrm{PRF}_2}_{\mathcal{B}_2}(\lambda) + 2 \sum_{\iota \in [2^\lambda]} q_{\mathrm{CT},\iota} \mathsf{Adv}^{\mathrm{P}_1}_{\mathcal{B}_3}(\lambda).$$

Proof: The hybrid sequence of Hyb_4 to Hyb_5 is just the reverse of Hyb_0 to Hyb_2.

□