Registered Functional Encryptions from Pairings★

Ziqi Zhu[1], Jiangtao Li[2], Kai Zhang[3], Junqing Gong[1,4,✉], and Haifeng Qian[1,✉]

[1] East China Normal University
52275902001@stu.ecnu.edu.cn
jqgong@sei.ecnu.edu.cn
hfqian@cs.ecnu.edu.cn
[2] Shanghai University
lijiangtao@shu.edu.cn
[3] Shanghai University of Electric Power
kzhang@shiep.edu.cn
[4] Shanghai Qi Zhi Institute

Abstract. This work initiates the study of *concrete* registered functional encryption (Reg-FE) beyond "all-or-nothing" functionalities:

– We build the first Reg-FE for linear function or inner-product evaluation (Reg-IPFE) from pairings. The scheme achieves adaptive IND-security under k-Lin assumption in the prime-order bilinear group. A minor modification yields the first Registered Inner-Product Encryption (Reg-IPE) scheme from k-Lin assumption. Prior work achieves the same security in the generic group model.
– We build the first Reg-FE for quadratic function (Reg-QFE) from pairings. The scheme achieves *very selective* simulation-based security (SIM-security) under bilateral k-Lin assumption in the prime-order bilinear group. Here, "very selective" means that the adversary claims challenge messages, all quadratic functions to be registered and all corrupted users at the beginning.

Besides focusing on the compactness of the master public key and helper keys, we also aim for compact ciphertexts in Reg-FE. Let L be the number of slots and n be the input size. Our first Reg-IPFE has *weakly compact* ciphertexts of size $O(n \cdot \log L)$ while our second Reg-QFE has *compact* ciphertexts of size $O(n+\log L)$. Technically, for our first Reg-IPFE, we employ *nested* dual-system method within the context of Reg-IPFE; for our second Reg-QFE, we follow Wee's "IPFE-to-QFE" transformation [TCC' 20] but devise a set of new techniques that make our *pairing-based* Reg-IPFE compatible. Along the way, we introduce a new notion named *Pre-Constrained Registered IPFE* which generalizes slotted Reg-IPFE by constraining the form of functions that can be registered.

Contents

1 Introduction

In *Registered Functional Encryption* (Reg-FE) [FFM+23,DP23], a trusted party generates a common reference string crs and then can go offline. The system is maintained by *curator* who holds crs but *no secret values*. When a user

★ This work is partially supported by National Natural Science Foundation of China (62372175, 62372285), Shanghai Rising-Star Program (22QA1403800), Science and Technology on Communication Security Laboratory Foundation (6142103022208), Innovation Program of Shanghai Municipal Education Commission (2021-01-07-00-08-E00101) and the "Digital Silk Road" Shanghai International Joint Lab of Trustworthy Intelligent Software (22510750100).

registers public key pk with a specific function f, the curator updates the master public key mpk and sends a helper key hsk to the new user. This hsk allows the user's secret key sk to decrypt a ciphertext ct of x under this new mpk to $f(x)$. Additionally, the registration process might also update helper keys for existing users in the system. Two crucial features of RFE are: (1) all actions performed by the curator are deterministic and auditable, and (2) mpk and hsk should be compact and update procedure must be efficient; ideally, objective sizes and algorithm costs are polylogarithmic in the number of registered users in the system.

Conceptually, Reg-FE covers the notion of registered attribute-based encryption (Reg-ABE) [HLWW23]. In particular, each user registers a predicate p instead of a function f, and a ciphertext encrypts message m with respect to an attribute a; decrypting the ciphertext using the secret key sk corresponding to predicate p recovers m if $p(a) = 1$. The most fundamental instance of Reg-ABE is called registration-based encryption (RBE) [GHMR18] corresponding to IBE [BF01,BB04,Wat05].

Historically, several constructions for RBE were first proposed via non-black-box technique based on garbling scheme [GHMR18,GHM+19,GV20,CES21]. Constructions via black-box technique were recently proposed based on bilinear maps [GKMR22] and learning with error (LWE) [DKL+23]. Almost simultaneously, Reg-ABE that goes beyond RBE was realized using bilinear maps [HLWW23,FFM+23,ZZGQ23] and witness encryption [FWW23]. However, for more general Reg-FE, we only see two recent work that presented schemes based on iO [FFM+23,DP23].

In this work, we will focus on Reg-FE for *concrete* functionalities instead of *general* functions in [FFM+23,DP23] and pursue *pairing-based* constructions from standard assumptions, notably k-Lin assumption and variants.

1.1 Results

Our main results are two-fold:

(1) We build the first Reg-FE for linear functions or inner-product evaluation (Reg-IPFE) from pairings: Each user is allowed to register pk with a linear function represented by a vector $\mathbf{y}$; decrypting a ciphertext of vector $\mathbf{x}$ gives $\mathbf{x}\mathbf{y}^{\top}$. The scheme achieves adaptive indistinguishability-based security (IND-security) under k-Lin assumption in the prime-order bilinear group.

(2) We build the first Reg-FE for quadratic functions (Reg-QFE) from pairings: Each user is allowed to register pk with a quadratic function represented by a vector $\mathbf{f}$; decrypting a ciphertext of $(\mathbf{x}_1, \mathbf{x}_2)$ gives $(\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^{\top}$. The scheme achieves *very selective* simulation-based security (SIM-security) under bilateral k-Lin assumption in the prime-order bilinear group. Here, "very selective" means that the adversary claims challenge messages, all quadratic functions to be registered, and all corrupted users at the beginning.

This is the first time we have concrete Reg-FE from standard assumptions with functionalities beyond "all-or-nothing" decryption. As prior pairing-based schemes [HLWW23,FFM+23,ZZGQ23], all our Reg-FE schemes support *bounded* number of slots, have a *structural* crs and require a specific procedure checking the validity of public key in the registration. Let L be the number of slots and n be the input size (which refers to $|\mathbf{x}|$ in Reg-IPFE and $|\mathbf{x}_1|$, $|\mathbf{x}_2|$ in Reg-QFE, respectively). Our schemes respectively have compact mpk of size $O(n \cdot \log L)$ and $O(n + \log L)$, and both schemes have compact hsk of size $O(n \cdot \log L)$. By contrast with RBE and Reg-ABE, we also concern ciphertext size in terms of n and L: our first Reg-IPFE has *weak compact* ct of size $O(n \cdot \log L)$ while our second Reg-QFE has *compact* ct of size $O(n + \log L)$. We summarize our results in Figure 1.

More Results. Our first Reg-IPFE scheme implies the following results:

(i) A minor modification to our Reg-IPFE scheme yields the first Registered Inner-Product Encryption (Reg-IPE) scheme that supports full attribute-hiding feature from k-Lin assumption. Prior work [FFM+23] achieves the

Scheme	Function	Security	Assumptions	$\vert\mathsf{mpk}\vert$	$\vert\mathsf{hsk}\vert$	$\vert\mathsf{ct}\vert$
[DP23],[FFM+23]	General	Ad-IND	iO + SSB	1	1	$n \log L$
result **(1)**	Linear	Ad-IND	k-Lin	$n \log L$	$n \log L$	$n \log L$
result **(ii)**	Linear	Sel-IND	k-Lin	$n + \log L$	$\log L$	$n + \log L$
	Linear	Sel*-SIM	bi-k-Lin	$n + \log L$	$\log L$	$n + \log L$
result **(2)**	Quadratic	Sel*-SIM	bi-k-Lin	$n + \log L$	$n \log L$	$n + \log L$

Fig. 1: Summary of existing registered functional encryption beyond Reg-ABE. Here n is the message size, and L is the maximum number of slots in the system. In the column **Security**, "Ad", "Sel" and "Sel*" stand for "adaptive", "selective" and "very selective"; "IND" and "SIM" indicate IND- and SIM-security. In column **Assumptions**, "SSB" stands for "somewhere statistically binding hash functions" while "bi-k-Lin" means "bilateral k-Lin assumption".

same security in the generic group model; this resolved the open problem posed in [FFM+23]. The scheme is similar to the Reg-ABE for zero inner-product predicate in [ZZGQ23] (and IPE in [OT12,CGKW18,CGW18]). However their *generic* framework failed to give a proof for full attribute-hiding; our work show that, for the *concrete* scheme, it is actually feasible to give a proof from k-Lin.

Along the way to our second Reg-QFE scheme, we obtain the following results which can be of independent interest:

(ii) We obtain two Reg-IPFE schemes with compact ciphertext of size $O(n + \log L)$ and shorter hsk of size independent of n but weaker security guarantee; the selectively IND-secure scheme is based on k-Lin assumption while the very selectively SIM-secure scheme is based on bi-k-Lin assumption. See Figure 1. We believe they will find more theoretical applications in the future.

(iii) We introduce a new notion *Pre-Constrained Registered IPFE* (PReg-IPFE) which generalizes slotted Reg-IPFE. It generates crs with a set of matrices $\mathbf{M}_1, \ldots, \mathbf{M}_L$ and decryption gives $\mathbf{x}\mathbf{M}_i\mathbf{f}_i^\top$ for slot i that is with $\mathbf{f}_i$. We conceptually consider $\mathbf{y}_i^\top = \mathbf{M}_i\mathbf{f}_i^\top$ as the linear function related to slot i. Imagine $\mathbf{M}$ is a "tall" matrix, we are forcing $\mathbf{y}_i^\top \in \mathsf{span}(\mathbf{M}_i)$. We believe this will motivate the study of *registration patterns* orthogonal to functionalities.

Open Problems. We list some open problems:

- We consider pre-constrained Reg-IPFE as a theoretical tool for a specific task. We believe it is worthwhile to investigate more general definitions, security, and constructions. They can be of independent interest even in real-world applications. Here we mention a related notion called *Pre-Constrained Encryption* [AJJM22] which has many theoretical implications. It is also nice to clarify the relation between these two notions.
- For Reg-IPFE, our work suggests that compact ciphertext and adaptive security can not be achieved simultaneously. One can disprove this conjecture by showing a Reg-IPFE scheme with both properties or providing an impossibility result to confirm it.
- Our Reg-QFE has crs of size $n^2 \cdot L^2 \cdot \log L$ where n is the input size and L is the number of slots. It is unclear whether such a huge crs is inevitable and is nice to have a more efficient Reg-QFE scheme with $|\mathsf{crs}| = n \cdot L^2 \cdot \log L$.

Related Work. We mention several recent work on RBE. [FKdP23] proposed a new black-box construction of RBE from Cuckoo hashing, which supports unbounded identity spaces based on pairings. [MQR22] found the trade-off between the size of public parameters and the number of decryption updates in RBE, they find out that the optimal number of decryption updates is $\Omega(\log L / \log\log L)$, when the size of public parameters is at most $\mathrm{poly}(\log L)$. They prove their result by constructing a polynomial-time adversary with the "good" identities tuples for attack, when the RBE scheme is beyond the trade-off they claim. [MQ23] constructed an RBE that achieves the optimal number of decryption updates with an online merger. In particular, they constructed an (approximately) optimal online merger, and applied it to the iO-based construction of [GHMR18] to achieve the optimal decryption update of RBE. In [HMQS23], Hajiabadi *et al.* showed the impossibility of black-box construction of RBE solely based on the idealized models of random trapdoor permutations (TDP) or Shoup's generic group model, without any other concrete assumption. With the black-box equivalence between RBE and public-key compression (PKCom), they proved their impossibility by showing there exists an adversary with polynomial queries, who breaks any PKCom which is solely based on either TDP model or Shoup's GGM. Their impossibility holds even if the size of crs is growing with the number of registered users.

Concurrent Work. As an independent work, Datta et al. [DPY23] (which is an updated version of [DP23]) provided a pairing-based Reg-IPFE from (plain) IPFE proposed by Abdalla et al. [ABDP15], and extended their Reg-IPFE to support fine-grained access control with linear secret sharing access structure (LSSS) policy. Their schemes are secure in the generic bilinear group model.

1.2 Slotted Reg-IPFE from k-Lin

Thanks to "powers-of-two" transformation [GHMR18,HLWW23,FFM+23], we focus on slotted Reg-IPFE where we do not worry about the complex update procedure. Let lower-case boldface denote *row* vectors and upper-case boldface denote matrices. An L-slotted Reg-IPFE simplifies Reg-IPFE for L users as follows: *After collecting all* $\mathsf{R} = ((\mathsf{pk}_1, \mathbf{y}_1), \ldots, (\mathsf{pk}_L, \mathbf{y}_L))$, the *aggregator* generates a master public key mpk for encryption and a set of helper keys $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ for all registered users. Conceptually[5], the adaptive security requires that the adversary cannot distinguish the ciphertext ct^* of message $\mathbf{x}_0^*$ and $\mathbf{x}_1^*$ given $\mathsf{mpk}, \mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ and secret keys sk_i from adversarially chosen slots with the restriction $\mathbf{x}_0^* \mathbf{y}_i^\top = \mathbf{x}_1^* \mathbf{y}_i^\top$. In this overview, we assume all $\mathsf{pk}_1, \ldots, \mathsf{pk}_L$ are generated by the challenger and the case with malicious keys can be handled via quasi-adaptive NIZK [ZZGQ23].

Recap: ABDP IPFE [ABDP15]. Assume $\mathbb{G}$ is a finite cyclic group of prime order p with generator g. Write $[x] = g^x \in \mathbb{G}$ for $x \in \mathbb{Z}_p$. Our starting point is the IPFE scheme for n dimensional space from [ABDP15]:

$$\mathsf{mpk} = [\mathbf{w}]; \quad \mathsf{ct} = [s, s\mathbf{w} + \mathbf{x}]; \quad \mathsf{sk} = \mathbf{w}\mathbf{y}^\top \tag{1}$$

where $\mathbf{w} \leftarrow \mathbb{Z}_p^n$ and $s \leftarrow \mathbb{Z}_p$. The correctness uses the equality

$$\overbrace{(s\mathbf{w} + \mathbf{x})}^{\mathsf{ct}} \cdot \mathbf{y}^\top - \overbrace{s}^{\mathsf{ct}} \cdot \overbrace{\mathbf{w}\mathbf{y}^\top}^{\mathsf{sk}} = \mathbf{x}\mathbf{y}^\top \tag{2}$$

The selective security of the scheme is based on DDH assumption. We omit the proof here since it is not quite related to our final proof for slotted Reg-IPFE.

Warm-up. We employ the strategy in [ZZGQ23] and [HLWW23] to build a one-slot Reg-IPFE and then extend it to a L-slotted Reg-IPFE. Let us give a slightly detailed explanation. Based on the correctness of equation (2), we first enables a user with an ElGamal-type key pair $(\mathsf{pk}, \mathsf{sk})$ to register $(\mathsf{pk}, \mathbf{y})$, as follows:

- $\mathsf{crs} = [\mathbf{w}]$ is basically the mpk of ABDP IPFE (1) and the key pair of user is $(\mathsf{pk}, \mathsf{sk}) = ([u], u)$ with $u \leftarrow \mathbb{Z}_p$.

[5] Formally, the adversary is given crs that allows it to derive $\mathsf{mpk}, \mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ on its own; our conceptual definition gives a simple mind model analogous to FE.

– To register $\mathsf{R} = (\mathsf{pk}, \mathbf{y})$, the aggregator generates the corresponding master public key $\mathsf{mpk}_\mathsf{R} = [u + \mathbf{w}\mathbf{y}^\top, \mathbf{w}]$.
– Under this mpk_R, we encrypt $\mathbf{x}$ as $\mathsf{ct} = [s, su + s\mathbf{w}\mathbf{y}^\top, s\mathbf{w} + \mathbf{x}]$ where $s \leftarrow \mathbb{Z}_p$.

The main idea above is to embed the decryption shown in (2) into the ciphertext and use an ElGamal encryption to hide the key $\mathbf{w}\mathbf{y}^\top$. The correctness uses

$$\overbrace{(s\mathbf{w} + \mathbf{x})}^{\mathsf{ct}} \cdot \mathbf{y}^\top - \overbrace{(su + s\mathbf{w}\mathbf{y}^\top)}^{\mathsf{ct}} + \overbrace{s}^{\mathsf{ct}} \cdot \overbrace{u}^{\mathsf{sk}} = \mathbf{x}\mathbf{y}^\top. \tag{3}$$

The security roughly follows from the case study below.

– When $\mathsf{sk} = u$ is secret, DDH assumption implies that $\mathsf{ct}^* \approx [s, \tilde{u} + \mathbf{w}\mathbf{y}^\top, \mathbf{w} + \mathbf{x}_b^*]$ where $\tilde{u}$ are independent and uniformly distributed, and the security follows from the fact that $(\tilde{u} + \mathbf{w}\mathbf{y}^\top, \mathbf{w} + \mathbf{x}_b^*) \equiv (\tilde{u}, \mathbf{w} + \mathbf{x}_b^*) \equiv (\tilde{u}, \mathbf{w})$ hides $\mathbf{x}_b^*$ in its entirety.
– When $\mathsf{sk} = u$ is leaked, DDH assumption implies that $\mathsf{ct} \approx [s, su + \tilde{\mathbf{w}}\mathbf{y}^\top, \tilde{\mathbf{w}} + \mathbf{x}_b^*]$ where we cannot change su to $\tilde{u}$ as before. In this case, we do not expect that ct hides $\mathbf{x}_b^*$; instead, we can argue that that $(\tilde{\mathbf{w}}\mathbf{y}^\top, \tilde{\mathbf{w}} + \mathbf{x}_0^*) \approx_s (\tilde{\mathbf{w}}\mathbf{y}^\top, \tilde{\mathbf{w}} + \mathbf{x}_1^*)$ since $\mathbf{x}_0^*\mathbf{y}^\top = \mathbf{x}_1^*\mathbf{y}^\top$.

This simple scheme is the so-called *one-slot* Reg-IPFE. The L-slot Reg-IPFE is the "sum" of L parallel instances of the above one-slot Reg-IPFE (namely, with fresh $\mathbf{w}$ for each slot) that ensures compact mpk (and ct as well):

– $\mathsf{crs} = [\mathbf{w}_1, \ldots, \mathbf{w}_L]$ is the concatenation of crs's from L fresh one-slot Reg-IPFE instances, i.e., $\mathsf{crs}_i = [\mathbf{w}_i]$ for all $i \in [L]$, and the i-th user has key pair $(\mathsf{pk}_i, \mathsf{sk}_i) = ([u_i], u_i)$ with $u_i \leftarrow \mathbb{Z}_p^n$ for all $i \in [L]$.
– To register $\mathsf{R} = ((\mathsf{pk}_1, \mathbf{y}_1), \ldots, (\mathsf{pk}_L, \mathbf{y}_L))$, the aggregator generates the corresponding master public key $\mathsf{mpk}_\mathsf{R} = [\sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top), \sum_j \mathbf{w}_j]$ where index j ranges from 1 to L; this sums up all $\mathsf{mpk}_{\mathsf{pk}_i, \mathbf{y}_i}$ in the one-slot Reg-IPFE with crs_i for all $i \in [L]$.
– Under this mpk_R, one encrypts $\mathbf{x}$ as $\mathsf{ct} = [s, s\sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top), s\sum_j \mathbf{w}_j + \mathbf{x}]$; this is analogous to the encryption procedure in the one-slot scheme.

However "addition" of L one-slot Reg-IPFE breaks the correctness: a user even holding the correct secret key cannot decrypt as in the one-slot setting. Analogous to [ZZGQ23], we turn to bilinear groups and use source group $\mathbb{G}_2$ to accommodate the helper keys. Let $\mathbb{G}_1 = \langle g_1 \rangle, \mathbb{G}_2 = \langle g_2 \rangle$ be finite cyclic source groups of bilinear maps e and $\mathbb{G}_T$ be the target group; the order of all groups is prime p. We place the above parallel instances over $\mathbb{G}_1$, and define helper keys:

$$\mathsf{hsk}_i = [r_i, r_i \textstyle\sum_{j \neq i}(u_j + \mathbf{w}_j\mathbf{y}_j^\top), r_i \sum_{j \neq i} \mathbf{w}_j]_2, \quad i \in [L].$$

Observe that, for each $i \in [L]$, hsk_i over $\mathbb{G}_2$ helps to recover a ciphertext of the same message $\mathbf{x}$ over $\mathbb{G}_T$ in the *one-slot* Reg-IPFE instance under $\mathsf{mpk}_{\mathsf{pk}_i, \mathbf{y}_i}$ (generated from crs_i and $\mathsf{pk}_i, \mathbf{y}_i$) with random coin sr_i instead of s:

$$\begin{aligned}
\overbrace{r_i}^{\mathsf{hsk}_i} \cdot \overbrace{(s\textstyle\sum_j \mathbf{w}_j + \mathbf{x})}^{\mathsf{ct}} \quad &- \overbrace{s}^{\mathsf{ct}} \cdot \overbrace{(r_i \textstyle\sum_{j \neq i} \mathbf{w}_j)}^{\mathsf{hsk}_i} &&= sr_i\mathbf{w}_i + \mathbf{x} \\
r_i \cdot (s\textstyle\sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top)) &- s \cdot (r_i \textstyle\sum_{j \neq i}(u_j + \mathbf{w}_j\mathbf{y}_j^\top)) &&= sr_i(u_i + \mathbf{w}_i\mathbf{y}_i^\top)
\end{aligned}$$

Given $\mathsf{sk}_i = u_i$ and $\mathbf{y}_i$, decryption then works as in the one-slot scheme over $\mathbb{G}_T$, cf. (3). Note that the helper keys $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ are generated by the curator during the registration and crs will contain terms $[r_i, r_i\mathbf{w}_j]_2$, where i, j ranges from 1 to L with the restriction that $i \neq j$; this ensures that all helper keys can be computed *publicly and deterministically*.

Proof: Strategy. The dual-system method used in [HLWW23,ZZGQ23] is not sufficient for proving our warm-up Reg-IPFE. In previous dual-system proofs for Reg-ABE, one conceptually changes $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ one-by-one and then changes ct^* in the last step. In our setting for Reg-IPFE, each time we "touch" an hsk_i, we change ct^* from an encryption of $\mathbf{x}_0^*$ to an encryption of $\mathbf{x}_1^*$. Therefore we employ the so-called *nested dual-system method* [LW11]; this has extensive applications in IPE with full attribute-hiding features [OT12,CGKW18,CGW18]. In this overview, we will explain the idea using bilinear group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ of *composite order* $N = p_1p_2p_3p_4$ where p_1, p_2, p_3, p_4 are prime. For each $\gamma \in \{1, 2, T\}$, group $\mathbb{G}_\gamma$ can be decomposed as $\mathbb{G}_{\gamma,1} \times \mathbb{G}_{\gamma,2} \times \mathbb{G}_{\gamma,3} \times \mathbb{G}_{\gamma,4}$ where the four subgroups have orders p_1, p_2, p_3, p_4, respectively. For $\sigma \in [4]$, let $\mathbb{G}_{\gamma,\sigma} = \langle g_{\gamma,\sigma}\rangle$. We will use implicit representation analogous to the prime-order group: for each $\gamma \in \{1, 2, T\}$ and $S \subseteq \{1, 2, 3, 4\}$, we will write $[x]_\gamma^S = \prod_{\sigma\in S} g_{\gamma,\sigma}^x$. As usual, this applies to matrices and vectors. When $|S| = 1$, i.e., $S = \{\sigma\}$, we may simplify the notation as $[x]_\gamma^\sigma$. We quickly review properties of composite-order bilinear groups:

- orthogonality: for $\sigma, \delta \in \{1, 2, 3, 4\}$, we have $e([1]_1^\sigma, [1]_2^\delta) = [0]_T$ when $\sigma \neq \delta$;
- non-degenerate: for $\sigma, \delta \in \{1, 2, 3, 4\}$, we have $e([1]_1^\sigma, [1]_2^\delta) \neq [0]_T$ when $\sigma = \delta$.

The common computational assumption is *subgroup decision assumption* indicating indistinguishability between random samples from two specific subgroups. We will give concrete assumptions when we use them in the proof.

Proof in Composite-order Groups. We embed our warm-up scheme into subgroups of order p_1 and p_4:

$$\begin{aligned}
\mathsf{crs} &= [\mathbf{w}_j]_1^1, \quad \forall j \in [L] \\
&\quad [r_i, r_i\mathbf{w}_j]_2^{\{1,4\}}, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\
\mathsf{mpk}_\mathsf{R} &= [\textstyle\sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top), \sum_j \mathbf{w}_j]_1^1 \\
\mathsf{hsk}_i &= [r_i, r_i \textstyle\sum_{j\neq i}(u_j + \mathbf{w}_j\mathbf{y}_j^\top), r_i \sum_{j\neq i} \mathbf{w}_j]_2^{\{1,4\}} \\
\mathsf{ct} &= [s, s\textstyle\sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top), s\sum_j \mathbf{w}_j + \boxed{s\mathbf{x}}]_1^1
\end{aligned}$$

where $\mathsf{sk}_i = u_i \leftarrow \mathbb{Z}_N$ and $\mathsf{pk}_i = ([u_i]_1^1, \{[r_j u_i]_2^{\{1,4\}}\}_{j\neq i})$ for all $i \in [L]$. Here we replace $\mathbf{x}$ with $s\mathbf{x}$, highlighted with a dashed box; the reader will see the reason later. Also, we will assume that the message $\mathbf{x}$ is sufficiently small so that $\mathbf{x} \bmod p_1 = \mathbf{x} \bmod p_2 = \mathbf{x} \bmod p_3 = \mathbf{x} \bmod p_4$ (e.g., $\mathbf{x} \in B^n$ where $B = \{1, \ldots, \min\{p_1, p_2, p_3, p_4\}\}$). This is a restriction applied to our composite-order group but not to our prime-order scheme.

<u>*Dual-system Method.*</u> Recall that $\mathbf{x}_0^*, \mathbf{x}_1^*$ are challenge messages. Let $([u_i]_1, \mathbf{y}_i)$ be with slot $i \in [L]$ and assume $u_1, \ldots, u_L$ are all honestly chosen (but can be leaked to the adversary later). From a very high level, we will follow the dual-system method, see Fig 2a. We begin with a challenge ciphertext of $\mathbf{x}_b^*$ where b is the secret bit, see G_0.

- First, we change the challenge ciphertext as below, which corresponds to G_2:

$$\boxed{[s, s\textstyle\sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top), s\sum_j \mathbf{w}_j + s\mathbf{x}_0^*]_1^2} \cdot [s, s\textstyle\sum_j (u_j + \mathbf{w}_j\mathbf{y}_j^\top), s\sum_j \mathbf{w}_j + s\mathbf{x}_b^*]_1^{\{3,4\}}.$$

- Second, we change all hsk_i's to the following form, which corresponds to G_3:

$$\boxed{[r_i, r_i \textstyle\sum_{j\neq i}(u_j + \mathbf{w}_j\mathbf{y}_j^\top), r_i\sum_{j\neq i} \mathbf{w}_j]_2^2} \cdot [r_i, r_i \textstyle\sum_{j\neq i}(u_j + \mathbf{w}_j\mathbf{y}_j^\top), r_i\sum_{j\neq i} \mathbf{w}_j]_2^1.$$

By this, we let ct and all hsk_i interplay only through p_2-subgroup where $\mathbf{x}_0^*$ is in the place of $\mathbf{x}_b^*$. This allows us to reach a challenge ciphertext of $\mathbf{x}_0^*$, i.e., G_4, via a simple argument that makes use of the absence of p_3- and p_4-components in $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$. To complete the proof, we need to justify the above two bullets. The first bullet follows from (a) subgroup decision assumption $[s]_1^{\{1\}} \approx_c [s]_1^{\{2,3,4\}}$ given $[1]_1^1, [1]_2^{\{1,4\}}$ that "moves" p_1-component of ct^* to $p_2p_3p_4$-subgroup, i.e., $\mathsf{G}_0 \mapsto \mathsf{G}_1$, and (b) the same argument above but over p_2-subgroup instead of p_3- and p_4-subgroup, see $\mathsf{G}_1 \mapsto \mathsf{G}_2$. The second bullet is intended to work in a one-by-one fashion and uses *nested dual-system method* sketched below.

Gm	Grp	ct*	hsk_i	Remark
G_0	p_1	$\mathbf{x}_b^*$	✓	Real Game
	p_2	—	—	
	p_3	—	—	
	p_4	—	✓	
G_1	p_1	—	✓	SD: $p_1 \to p_2p_3p_4$
	p_2	$\mathbf{x}_b^*$	—	
	p_3	$\mathbf{x}_b^*$	—	
	p_4	$\mathbf{x}_b^*$	✓	
G_2	p_1	—	✓	Statistical
	p_2	$\mathbf{x}_0^*$	—	
	p_3	$\mathbf{x}_b^*$	—	
	p_4	$\mathbf{x}_b^*$	✓	
G_3	p_1	—	✓	Fig. 2b
	p_2	$\mathbf{x}_0^*$	✓	
	p_3	$\mathbf{x}_b^*$	—	
	p_4	$\mathbf{x}_b^*$	—	
G_4	p_1	—	✓	Statistical
	p_2	$\mathbf{x}_0^*$	✓	
	p_3	$\mathbf{x}_0^*$	—	
	p_4	$\mathbf{x}_0^*$	—	

(a) Games for dual-system method with $i \in [L]$.

Gm	Grp	ct*	$\mathsf{hsk}_{i<\ell}$	hsk_ℓ	$\mathsf{hsk}_{i>\ell}$	Remark
$\mathsf{G}_{3.\ell.0}$	p_1	—	✓	✓	✓	$\mathsf{G}_{3.1.0} = \mathsf{G}_2$
	p_2	$\mathbf{x}_0^*$	✓	—	—	
	p_3	$\mathbf{x}_b^*$	—	—	—	$\mathsf{G}_{3.L+1.0} = \mathsf{G}_3$
	p_4	$\mathbf{x}_b^*$	—	✓	✓	
$\mathsf{G}_{3.\ell.1}$	p_1	—	✓	✓	✓	SD: $p_4 \to p_3$
	p_2	$\mathbf{x}_0^*$	✓	—	—	
	p_3	$\mathbf{x}_b^*$	—	✓	—	
	p_4	$\mathbf{x}_b^*$	—	—	✓	
$\mathsf{G}_{3.\ell.2}$	p_1	—	✓	✓	✓	Statistical
	p_2	$\mathbf{x}_0^*$	✓	—	—	
	p_3	$\mathbf{x}_0^*$	—	✓	—	
	p_4	$\mathbf{x}_b^*$	—	—	✓	
$\mathsf{G}_{3.\ell.3}$	p_1	—	✓	✓	✓	SD: $p_3 \to p_2$
	p_2	$\mathbf{x}_0^*$	✓	✓	—	
	p_3	$\mathbf{x}_0^*$	—	—	—	
	p_4	$\mathbf{x}_b^*$	—	—	✓	
$\mathsf{G}_{3.\ell.4}$	p_1	—	✓	✓	✓	Statistical
	p_2	$\mathbf{x}_0^*$	✓	✓	—	
	p_3	$\mathbf{x}_b^*$	—	—	—	$\mathsf{G}_{3.\ell.4} = \mathsf{G}_{3.\ell+1.0}$
	p_4	$\mathbf{x}_b^*$	—	—	✓	

(b) Games for nested dual-system method where $\ell \in [L]$.

Fig. 2: Game sequence in the composite-order group. For each game, we show the challenge ciphertext ct* and helper keys hsk_ℓ in the template: $\prod_{\sigma \in S}[s, s\sum_j(u_j + \mathbf{w}_j\mathbf{y}_j^\top), s\sum_j \mathbf{w}_j + s\mathbf{x}_\sigma]_1^\sigma$ and $[r_i, r_i\sum_{j\neq i}(u_j + \mathbf{w}_j\mathbf{y}_j^\top), r_i\sum_{j\neq i}\mathbf{w}_j]_2^{S_i}$ where $S, S_1, \ldots, S_L \in 2^{[4]}$. In column ct*, we show $\mathbf{x}_\sigma$ in row p_σ for all $\sigma \in S$ and put a symbol "—" in row p_σ when $\sigma \notin S$. In column hsk_i, we put a symbol "✓" in row p_σ when $\sigma \in S_i$, otherwise leave "—".

Nested Dual-System Method. For each $\ell \in [L]$, we change hsk_ℓ in the form

$$[r_\ell, r_\ell\textstyle\sum_{j\neq\ell}(u_j + \mathbf{w}_j\mathbf{y}_j^\top), r_\ell\sum_{j\neq\ell}\mathbf{w}_j]_2^{S_\ell}$$

one-by-one via the following transitions:

$$S_\ell : \{1,4\} \longmapsto \{1,3\} \longmapsto \{1,2\}$$

where they corresponds to $\mathsf{G}_{3.\ell.0}$, $\mathsf{G}_{3.\ell.1}$ (also, $\mathsf{G}_{3.\ell.3}$), and $\mathsf{G}_{3.\ell.4}$, respectively, in Figure 2b. We cannot achieve $\{1,4\} \longmapsto \{1,2\}$ directly (as in standard dual-system proof) since we have $\mathbf{x}_0^*$ in the p_2-component of ct (see the boxed term in ct) but $\mathbf{x}_b^*$ in the p_4-component of ct*, subgroup decision assumption $[r]_2^{\{4\}} \approx_c [r]_2^{\{2\}}$ cannot apply. Here we use p_3-subgroup as a step-stone: We first apply the subgroup decision assumption $[r_\ell]_2^{\{4\}} \approx_c [r_\ell]_2^{\{3\}}$ given $[1]_1^{\{3,4\}}$ that "moves" p_4-component of hsk_ℓ to p_3-subgroup. Observe that only hsk_ℓ interplays with ct* through p_3-subgroup, the following case study switches $\mathbf{x}_b^*$ in the p_3-component of ct* to $\mathbf{x}_0^*$:

- If slot ℓ is honest, then u_ℓ mod p_3 is hidden and thus $\mathbf{w}_\ell$ mod p_3 hides $\mathbf{x}_b^*$.
- If slot ℓ is corrupted, then we have $\mathbf{w}_\ell\mathbf{y}_\ell^\top, \mathbf{w}_\ell + \mathbf{x}_b^* \equiv \mathbf{w}_\ell\mathbf{y}_\ell^\top, \mathbf{w}_\ell + \mathbf{x}_0^*$ mod p_3 with the restriction $\mathbf{x}_0^*\mathbf{y}_\ell^\top = \mathbf{x}_1^*\mathbf{y}_\ell$.

This corresponds to $\mathsf{G}_{3.\ell.1} \mapsto \mathsf{G}_{3.\ell.3}$ in Figure 2b. By this, we have $\mathbf{x}_0^*$ over both p_2- and p_3-subgroup, and the subgroup decision assumption $[r_\ell]_2^{\{3\}} \approx_c [r_\ell]_2^{\{2\}}$ given $[1]_1^{\{2,3\}}$ gives desired form of hsk_ℓ. Finally, we roll back the p_3-component of ct to encrypt $\mathbf{x}_b^*$ for future use, i.e., for handling $\mathsf{hsk}_{\ell+1}$ in the next loop.

Our Scheme in the Prime-order Group. Neglecting subscripts i, j, we do the following substitution with basis $\mathbf{A} \in \mathbb{Z}_p^{k\times(k+1)}$ and $\mathbf{B} \in \mathbb{Z}_p^{(2k+1)\times k}$ as in [CGW18]:

$$\begin{aligned} \mathbf{w} \in \mathbb{Z}_N^n &\mapsto \mathbf{W} \in \mathbb{Z}_p^{(k+1)\times(2k+1)n} \\ [s]_1^1 \in \mathbb{G}_{1,1}, [r]_2^{\{1,4\}} \in \mathbb{G}_{2,1} \times \mathbb{G}_{2,4} &\mapsto [\mathbf{sA}]_1 \in \mathbb{G}_1^{1\times(k+1)}, [\mathbf{Br}^\top]_2 \in \mathbb{G}_2^{2k+1} \\ [\mathbf{w}]_1 \in \mathbb{G}_{1,1}^n, [s\mathbf{w}]_1^1 \in \mathbb{G}_{1,1}^n &\mapsto [\mathbf{AW}]_1 \in \mathbb{G}_1^{k\times(2k+1)n}, [\mathbf{sAW}]_1 \in \mathbb{G}_1^{1\times(2k+1)n} \\ [r\mathbf{w}]_2^{\{1,4\}} \in (\mathbb{G}_{2,1} \times \mathbb{G}_{2,4})^n &\mapsto [\mathbf{W}(\mathbf{I}_n \otimes \mathbf{Br}^\top)]_2 \in \mathbb{G}_2^{(k+1)\times n} \end{aligned}$$

This yields our L-slotted Reg-IPFE scheme in the prime-order group:

$$\begin{aligned} \mathsf{crs} &= [\mathbf{AV}]_1, [\mathbf{AW}_j]_1, \quad \forall j \in [L] \\ &\quad [\mathbf{Br}_i^\top, \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_i^\top)]_2, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\ \mathsf{mpk}_\mathsf{R} &= [\textstyle\sum_j (\mathbf{AU}_j + \mathbf{AW}_j(\mathbf{y}_j^\top \otimes \mathbf{I}_{2k+1})), \sum_j \mathbf{AW}_j, \mathbf{AV}]_1 \\ \mathsf{hsk}_i &= [\mathbf{Br}_i^\top, \textstyle\sum_{j\neq i} (\mathbf{U}_j \mathbf{Br}_i^\top + \mathbf{W}_j(\mathbf{y}_j^\top \otimes \mathbf{Br}_i^\top)), \sum_{j\neq i} \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_i^\top)]_2 \\ \mathsf{ct} &= [\mathbf{sA}, \mathbf{s}\textstyle\sum_j (\mathbf{AU}_j + \mathbf{AW}_j(\mathbf{y}_j^\top \otimes \mathbf{I}_{2k+1})), \mathbf{s}\sum_j \mathbf{AW}_j + \mathbf{x} \otimes \mathbf{sAV}, \mathbf{sAV}]_1 \end{aligned} \tag{4}$$

where $\mathsf{sk}_i = \mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)}$ and $\mathsf{pk}_i = ([\mathbf{AU}_i]_1, \{[\mathbf{U}_i\mathbf{Br}_j^\top]_2\}_{j\neq i})$ for all $i \in [L]$. This is almost the final scheme except for some extra elements for handling malicious public keys. All subgroup decision assumptions we used can be replaced by MDDH assumption. Roughly, basis $\mathbf{B}$ corresponds to a $(2k+1)$-dimensional space; we use two k-dimensional subspaces to simulate p_3, p_4-subgroup, respectively, and the remaining 1-dimensional subspace to simulate p_2-subgroup. We leave more details to Section 3. For simplicity, we will continue our technical overview based on this slightly weaker scheme.

Extension to Reg-IPE. Recall that the proof of our slotted Reg-IPFE is motivated by that for IPE with full attribute hiding [OT12,CGKW18,CGW18]. This similarity inspires the following L-slotted Reg-IPE:

$$\begin{aligned} \mathsf{crs} &= \boxed{[\mathbf{Ak}^\top]_T}, [\mathbf{AV}]_1, \boxed{[\mathbf{AW}_0]_1}, [\mathbf{AW}_j]_1, \quad \forall j \in [L] \\ &\quad [\mathbf{Br}_i^\top, \boxed{\mathbf{W}_0\mathbf{Br}_i^\top + \mathbf{k}^\top}, \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_i^\top)]_2, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\ \mathsf{mpk}_\mathsf{R} &= [\boxed{\mathbf{AW}_0} + \textstyle\sum_j (\mathbf{AU}_j + \mathbf{AW}_j(\mathbf{y}_j^\top \otimes \mathbf{I}_{2k+1})), \sum_j \mathbf{AW}_j, \mathbf{AV}]_1 \\ \mathsf{hsk}_i &= [\mathbf{Br}_i^\top, \textstyle\sum_{j\neq i} (\mathbf{U}_j \mathbf{Br}_i^\top + \mathbf{W}_j(\mathbf{y}_j^\top \otimes \mathbf{Br}_i^\top)), \sum_{j\neq i} \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_i^\top), \boxed{\mathbf{W}_0\mathbf{Br}_i^\top + \mathbf{k}^\top}]_2 \\ \mathsf{ct} &= [\mathbf{sA}, \boxed{\mathbf{sAW}_0} + \mathbf{s}\textstyle\sum_j (\mathbf{AU}_j + \mathbf{AW}_j(\mathbf{y}_j^\top \otimes \mathbf{I}_{2k+1})), \mathbf{s}\sum_j \mathbf{AW}_j + \mathbf{x} \otimes \mathbf{sAV}]_1, \boxed{[\mathbf{sAk}^\top]_T \cdot m} \end{aligned}$$

where sk_i and pk_i are as in (4). We highlight the difference between our slotted Reg-IPFE and the slotted Reg-IPE above. The "powers-of-two" technique finally gives us a Reg-IPFE scheme. We leave all details to Appendix B.

1.3 Reg-QFE from Bilateral k-Lin

This section explains our Reg-QFE where each user registers a quadratic function $\mathbf{f} \in \mathbb{Z}_p^{n_1\times n_2}$ so that decrypting a ciphertext of $(\mathbf{x}_1, \mathbf{x}_2) \in \mathbb{Z}_p^{n_1} \times \mathbb{Z}_p^{n_2}$ recovers $(\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^\top$. Given (a) our slotted Reg-IPFE in Section 1.2 and Section 3, (b) Wee's "IPFE-to-QFE" transformation [Wee20] and (c) "powers-of-two" transformation [GHMR18,HLWW23,FFM+23,DP23], we want to follow the technical line:

$$\text{slotted Reg-IPFE} \overset{(a)}{} \overset{(b)}{\Longrightarrow} \text{slotted Reg-QFE} \overset{(c)}{\Longrightarrow} \text{Reg-QFE}. \tag{5}$$

This defers complicated update procedure to the very last stage and keeps most steps simple. Only the first " $\Longrightarrow$ " in technical line (5) can be problematic since the transformation is not for Reg-FE but FE. Let us begin with a sketch of Wee's transformation.

Recap. Given an IPFE (iKey, iEnc)[6], the QFE scheme from [Wee20] works as follows:

$$\mathsf{mpk} = [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \qquad \mathsf{ct} = [\mathbf{y}_1]_1, [\mathbf{y}_2]_2, \mathsf{iEnc}(\mathbf{x}), \qquad \mathsf{sk}_{\mathbf{f}} = \mathsf{iKey}([\mathbf{M}\mathbf{f}^\top]_2)$$

where we sample random coins $\mathbf{s}_1, \mathbf{s}_2$ and set $\mathbf{y}_1 = \mathbf{x}_1 + \mathbf{s}_1\mathbf{A}_1$, $\mathbf{y}_2 = \mathbf{x}_2 + \mathbf{s}_2\mathbf{A}_2$, $\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$ and

$$\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I}_{n_2} \\ \mathbf{I}_{n_1} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}.$$

Note that this is slightly different from the original scheme in [Wee20] but they are essentially the same. The correctness follows from

$$(\mathbf{y}_1 \otimes \mathbf{y}_2)\mathbf{f}^\top = (\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^\top + \mathbf{x}\mathbf{M}\mathbf{f}^\top \tag{6}$$

The *selective SIM-security* requires a simulator $(\widetilde{\mathsf{iEnc}}, \widetilde{\mathsf{iKey}})$ so that we can carry out the following argument:

$$\begin{aligned}
& [\mathbf{y}_1]_1,\ [\mathbf{y}_2]_2,\ \mathsf{iEnc}(\mathbf{x}),\ \mathsf{iKey}([\mathbf{M}\mathbf{f}^\top]_2) \\
\approx_c\ & [\mathbf{y}_1]_1,\ [\mathbf{y}_2]_2,\ \widetilde{\mathsf{iEnc}}(),\quad \widetilde{\mathsf{iKey}}([\mathbf{M}\mathbf{f}^\top]_2, [\mathbf{x}\mathbf{M}\mathbf{f}^\top]_2) && \text{// IPFE} \\
\equiv\ & [\mathbf{y}_1]_1,\ [\mathbf{y}_2]_2,\ \widetilde{\mathsf{iEnc}}(),\quad \widetilde{\mathsf{iKey}}([\mathbf{M}\mathbf{f}^\top]_2, [(\mathbf{y}_1 \otimes \mathbf{y}_2)\mathbf{f}^\top - (\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^\top]_2) && \text{// (6)} \\
\approx_c\ & [\widetilde{\mathbf{y}}_1]_1,\ [\widetilde{\mathbf{y}}_2]_2,\ \widetilde{\mathsf{iEnc}}(),\quad \widetilde{\mathsf{iKey}}([\mathbf{M}\mathbf{f}^\top]_2, [(\widetilde{\mathbf{y}}_1 \otimes \widetilde{\mathbf{y}}_2)\mathbf{f}^\top - (\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^\top]_2) && \text{// bi-MDDH}
\end{aligned}$$

where $\widetilde{\mathbf{y}}_1 \leftarrow \mathbb{Z}_p^{n_1}$ and $\widetilde{\mathbf{y}}_2 \leftarrow \mathbb{Z}_p^{n_2}$ are independently and uniformly distributed. Here, the first $\approx_c$ uses the simulator over groups to embed the result $z' = \mathbf{x}\mathbf{M}\mathbf{f}^\top$ into the simulated key; the second $\equiv$ follows from the equation for correctness; the third $\approx_c$ is ensured by bilateral MDDH assumption w.r.t. $\mathbf{A}_1$ and $\mathbf{A}_2$.

Challenges. The first " $\Longrightarrow$ " in technical line (5) is expected to apply a similar transformation to our slotted Reg-IPFE in Section 1.2 and Section 3. However, there are three main challenges pertinent to both correctness and security:

- **Challenge 1: Decryption with Fixed Base.** Our slotted Reg-IPFE gives decryption result in the form of $[b, zb]_T$ where z is the result and base $b = \mathbf{s}\mathbf{A}\mathbf{V}\mathbf{B}\mathbf{r}_i^\top$; here b varies with the user who are decrypting. This is fine in the case of small z since brute-force search recovers z. For the use in Wee's QFE, z involves random coins $\mathbf{s}_1, \mathbf{s}_2$ and can be quite large, more precisely, $z \in \mathbb{Z}_p$; clearly, we cannot extract $[z]_T$ from $[b, zb]_T$ in this case. Therefore, we need a slotted Reg-IPFE that recovers $[z]_T$ for *all* slots, i.e., with fixed base $[1]_T$.
- **Challenge 2: Group-friendly Registration.** A subtly point in Wee's scheme is that we need to encode $\mathbf{M}\mathbf{f}^\top$ (and also $\mathbf{y}_1, \mathbf{y}_2$) over proper groups in order to apply bi-MDDH assumption later. In the context of slotted Reg-IPFE, this means that a user can register a function of the form $[\mathbf{M}\mathbf{f}^\top]_2$ over $\mathbb{G}_2$. However our slotted Reg-IPFE already has crs and mpk, $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ over $\mathbb{G}_1, \mathbb{G}_2$, there is no space to use pairing which seems to be inevitable if we want to "multiply" $\mathbf{M}\mathbf{f}^\top$ with terms from crs. Therefore, we need a slotted Reg-IPFE with *group-friendly* registration.
- **Challenge 3: Simulation-based Security.** In the first step of Wee's proof, we make use of the simulator to assemble $\mathbf{x}$ and $\mathbf{M}\mathbf{f}^\top$ in $\mathsf{sk}_{\mathbf{f}}$. In fact, when serving as a building block, we prefer an IPFE with SIM-security. However, our slotted Reg-IPFE scheme only achieves strictly weaker IND-security. Furthermore, Wee's QFE requires that the simulator takes $[\mathbf{M}\mathbf{f}^\top]_2$ and $[\mathbf{x}\mathbf{M}\mathbf{f}^\top]_2$ as well; this is a requirement related to **Challenge 2**. Therefore, we need a slotted Reg-IPFE achieving *SIM-security* with *group-based* simulator.

We will explain our solutions to all three challenges. Note that, in [Wee20], all above are easy to satisfy since the underlying IPFE [ALS16] is pairing-free and embedding it into a bilinear group simply works; however, our slotted Reg-IPFE already uses bilinear groups and those embedding tricks fail.

[6] Here we hardcode the master public key and master secret key inside iEnc and iKey, respectively, for notation simplicity.

Solution 1: Decryption with Fixed Base. Let us review the structure of ciphertext in our slotted Reg-IPFE (4):

$$[\mathbf{sA}, \mathbf{s}\sum_j(\mathbf{AU}_j + \mathbf{AW}_j(\mathbf{y}_j^\top \otimes \mathbf{I})), \boxed{\mathbf{s}\sum_j \mathbf{AW}_j + \mathbf{x} \otimes \mathbf{sAV}}, \mathbf{sAV}]_1$$

The reason of decryption with variable base is that we put $\mathbf{x}$ with term $\sum_j \mathbf{sAW}_j$, highlighted in the gray box, which involves terms from all slots; during the decryption, it interplays with $\mathbf{Br}_i^\top$ depending on the user/slot. Our revision starts from the following substitution:

$$\boxed{\mathbf{s}\sum_j \mathbf{AW}_j + \mathbf{x} \otimes \mathbf{sAV}} \longmapsto \boxed{\mathbf{sAW} + \mathbf{x}}$$

namely, we simply hide $\mathbf{x}$ using $\mathbf{sAW}$ where $\mathbf{W}$ is conceptually shared by all users/slots. In fact, this is exactly the ciphertext by Agrawal *et al.*'s IPFE [ALS16] that is compatible with Wee's QFE. This breaks the correctness, but a minor modification saves us: we remove terms involving $\mathbf{V}$ and we put $\boxed{[\mathbf{AW}]_1}$ into crs and mpk for encryption; the most crucial change is the substitution

$$\mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_i^\top) \longmapsto \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_i^\top) + \boxed{\mathbf{W}}$$

which connects the two terms in the ciphertext. This yields the following scheme with new terms highlighted in the boxes:

$$\begin{aligned}
\mathsf{crs} &= \boxed{[\mathbf{AW}]_1}, [\mathbf{AW}_j]_1, \quad \forall j \in [L] \\
&\quad [\mathbf{Br}_i^\top, \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_i^\top), \mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{Br}_i^\top) + \boxed{\mathbf{W}}]_2, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\
\mathsf{mpk}_{\mathsf{R}} &= [\textstyle\sum_j(\mathbf{AU}_j + \mathbf{AW}_j(\mathbf{y}_j^\top \otimes \mathbf{I})), \boxed{\mathbf{AW}}]_1 \\
\mathsf{hsk}_i &= [\mathbf{Br}_i^\top, \textstyle\sum_{j\neq i}(\mathbf{U}_j\mathbf{Br}_i^\top + \mathbf{W}_j(\mathbf{y}_j^\top \otimes \mathbf{Br}_i^\top)), \mathbf{W}_i(\mathbf{y}_i^\top \otimes \mathbf{Br}_i^\top) + \boxed{\mathbf{Wy}_i^\top}]_2 \\
\mathsf{ct} &= [\mathbf{sA}, \mathbf{s}\textstyle\sum_j(\mathbf{AU}_j + \mathbf{AW}_j(\mathbf{y}_j^\top \otimes \mathbf{I})), \boxed{\mathbf{sAW} + \mathbf{x}}]_1
\end{aligned} \tag{7}$$

where $(\mathsf{pk}_i, \mathsf{sk}_i)$ is in the same form as in (4). Here we leave some $\mathbf{I}$'s with dimension undefined for now. For correctness, revised terms (with boxes) in hsk_i and ct now interplay as below during decryption:

$$-\mathbf{sA} \cdot (\mathbf{W}_i(\mathbf{y}_i^\top \otimes \mathbf{Br}_i^\top) + \boxed{\mathbf{Wy}_i^\top}) + (\boxed{\mathbf{sAW} + \mathbf{x}}) \cdot \mathbf{y}_i^\top = -\mathbf{sAW}_i(\mathbf{y}_i^\top \otimes \mathbf{Br}_i^\top) + \mathbf{xy}_i^\top$$

while the remaining unchanged terms give $\mathbf{sAU}_i\mathbf{Br}_i^\top + \mathbf{sAW}_i(\mathbf{y}_i^\top \otimes \mathbf{Br}_i^\top)$ as before; they are sufficient to recover $\mathbf{xy}_i^\top$ for the legitimate user holding $\mathsf{sk}_i = \mathbf{U}_i$. For security, our revised scheme only achieves a selective variant where the adversary claims the challenge message before seeing crs. The good news is we will not need the complex "nested dual-system" technique — the standard dual-system method is already sufficient as in prior Reg-ABE [HLWW23,ZZGQ23]. In a bit more detail, after changing the challenge ciphertext to the form:

$$\mathsf{ct}^* = [\boxed{\mathbf{c}}, \textstyle\sum_j(\boxed{\mathbf{c}}\mathbf{U}_j + \boxed{\mathbf{c}}\mathbf{W}_j(\mathbf{y}_j^\top \otimes \mathbf{I})), \boxed{\mathbf{c}}\mathbf{W} + \mathbf{x}_b^*]_1$$

via MDDH assumption w.r.t. $\mathbf{A}$, we can "embded" $\mathbf{x}_b^*$ to crs via the substitution: $\mathbf{W} \mapsto \mathbf{W} - \mathbf{c}^\perp\mathbf{x}_b^*$ where $\mathbf{cc}^\perp = 1$ but $\mathbf{cA} = \mathbf{0}$. Then, we can prove the security via the dual-system method: $\mathbf{x}_b^*$ now conceptually locates in $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ and we can handle them one-by-one. Therefore, we only need $\mathbf{B}$ to be a vector of dimension $k+1$ following [CGW15] and this requires the size of $\mathbf{I}$ to be $(k+1) \times (k+1)$. (Sizes of related matrices should be changed accordingly.) One can see that embedding $\mathbf{x}_b^*$ into crs is what renders the scheme selectively secure. This addresses **Challenge 1** at the cost of weaker security. Even though, this is sufficient for our purpose; in fact, we do not know how to achieve adaptive security even for plain QFE (from standard assumptions).

Solution 2: Pre-Constrained Registered IPFE. Recall that **Challenge 2** requires group-friendly registration. We believe this problem is quite hard *in general* and focus on functions in the *specific form* $[\mathbf{Mf}^\top]_2$. Observe that

– $\mathbf{M}$ is fully determined by $\mathbf{A}_1$ and $\mathbf{A}_2$; this is the part that must be encoded over groups, but they are shared by all users/slots and determined at the very beginning under no control of any users;
– $\mathbf{f}$ is fully controlled by the users but not necessary to be encoded over the group at all; in fact, it should be public according to the functionality.

This does not help to give a group-friendly registration, but suggests a way to circumvent this technical issue:

> *We do not need to wait and ask the curator to register* $[\mathbf{M}\mathbf{f}^\top]_2$*; instead, we can embed the "troublemaker"* $[\mathbf{M}]_2$ *over group into crs beforehand in the setup phase and ask the curator to register only* $\mathbf{y}$ *over integers.*

We capture this idea by introducing a new notion called *Pre-Constrained Registered IPFE* (PReg-IPFE):

– crs is generated with $\mathbf{M}$ where $\mathbf{M}$ is sampled from a pre-defined distribution.
– For each $i \in [L]$, the user holding $(\mathsf{pk}_i, \mathsf{sk}_i)$ can register $(\mathsf{pk}_i, \mathbf{f}_i)$ to slot i.
– Given a ciphertext of $\mathbf{x}$, decrypting it using sk_i (and hsk_i) gives $[\mathbf{x}\mathbf{M}\mathbf{f}_i^\top]_T$.

This generalizes the notion of slotted Reg-IPFE. Conceptually, $\mathbf{y}_i = \mathbf{M}\mathbf{f}_i$ is the function for slot i. Imagine that $\mathbf{M}$ is a "tall" matrix defining a subspace. Our PReg-IPFE forces that all user's functions $\mathbf{y}_1, \ldots, \mathbf{y}_L$ should be in $\mathsf{span}(\mathbf{M})$. Our slotted Reg-IPFE with fixed base, i.e, (7), can be easily modified to give an instance of PReg-IPFE:

$$\begin{aligned}
\mathsf{crs}_{\mathbf{M}} &= [\mathbf{A}\mathbf{W}]_1, [\mathbf{A}\mathbf{W}_j(\boxed{\mathbf{M} \otimes \mathbf{I}_{k+1}})]_1 \quad \forall j \in [L] \\
&\quad [\mathbf{B}\mathbf{r}_i^\top, \mathbf{W}_j(\boxed{\mathbf{M}} \otimes \mathbf{B}\mathbf{r}_i^\top), \mathbf{W}_i(\boxed{\mathbf{M}} \otimes \mathbf{B}\mathbf{r}_i^\top) + \mathbf{W}\boxed{\mathbf{M}}]_2, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\
\mathsf{mpk}_{\mathsf{R}} &= [\textstyle\sum_j (\mathbf{A}\mathbf{U}_j + \mathbf{A}\mathbf{W}_j(\boxed{\mathbf{M}}\mathbf{f}_j^\top \otimes \mathbf{I}_{k+1})), \mathbf{A}\mathbf{W}]_1 \\
\mathsf{hsk}_i &= [\mathbf{B}\mathbf{r}_i^\top, \textstyle\sum_{j \neq i}(\mathbf{U}_j\mathbf{B}\mathbf{r}_i^\top + \mathbf{W}_j(\boxed{\mathbf{M}}\mathbf{f}_j^\top \otimes \mathbf{B}\mathbf{r}_i^\top)), \mathbf{W}_i(\boxed{\mathbf{M}}\mathbf{f}_i^\top \otimes \mathbf{B}\mathbf{r}_i^\top) + \mathbf{W}\boxed{\mathbf{M}}\mathbf{f}_i^\top]_2 \\
\mathsf{ct} &= [\mathbf{s}\mathbf{A}, \mathbf{s}\textstyle\sum_j (\mathbf{A}\mathbf{U}_j + \mathbf{A}\mathbf{W}_j(\boxed{\mathbf{M}}\mathbf{f}_j^\top \otimes \mathbf{I}_{k+1})), \mathbf{s}\mathbf{A}\mathbf{W} + \mathbf{x}]_1
\end{aligned} \tag{8}$$

where $(\mathsf{pk}_i, \mathsf{sk}_i)$ is as in (7) and we highlight the difference with (7) using boxes. To reach this scheme from (7), we simply set $\mathbf{y}_i^\top = \mathbf{M}\mathbf{f}_i^\top$ for all $i \in [L]$ in hsk_i and ct from (7) and rebuild $\mathsf{crs}_{\mathbf{M}}$ and $\mathsf{mpk}_{\mathsf{R}}$ with $\mathbf{M}$ embedded. In fact, one can see that setting $\mathbf{M} = \mathbf{I}_n$ degrades it to the original scheme (7). Clearly, correctness and selective security can be proved analogously, but the registration now only involves crs and $\mathsf{R} = ((\mathsf{pk}_1, \mathbf{f}_1), \ldots, (\mathsf{pk}_L, \mathbf{f}_L))$ and has nothing to do with $\mathbf{M}$. Furthermore, we can check that if we publish $[\mathbf{M}]_2$ in crs and $[\mathbf{M}\mathbf{f}_i^\top]_2$ in hsk_i (which is used to compute $[(\mathbf{s}\mathbf{A}\mathbf{W} + \mathbf{x}) \cdot \mathbf{M}\mathbf{f}_i^\top]_T$ during decryption), then all occurrences of $\mathbf{M}$ have been encoded over groups. This addresses **Challenge 2**.

Solution 3.1: Defining Simulation-based Security. We begin to work on **Challenge 3**. This is the first time to consider simulation-based security (SIM-security) in the context of Reg-FE. Since we will work on scheme (8), our discussion will be restricted to PReg-IPFE and we will not pursue security stronger than selective security. Another technical reason is that there is no IPFE scheme supporting group-based functions with adaptive SIM-security. Assume $\mathbf{x}^*$ is the challenge message and registration $\mathsf{R} = ((\mathsf{pk}_1, \mathbf{f}_1), \ldots, (\mathsf{pk}_L, \mathbf{f}_L))$, the SIM-secure PReg-IPFE requires a simulator that can simulate the view of adversary using $Z = \{\mathbf{x}^*\mathbf{M}\mathbf{f}_i^\top\}_{i \in C}$ where $C \in [L]$ is the set of corrupted slots. Inspired by the selective SIM-security of plain IPFE, we expect the simulator to embed Z into $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$. However, in the PReg-IPFE system, $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ is generated by aggregator *under the supervision of adversary*, hence the simulator has no chance to embed anything inside $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$. In this work, we embed Z into crs which is fully controlled by the simulator and is used to generate $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$; we note that this will also require the adversary to claim the challenge $\mathbf{x}^*$, the set C along with corresponding $\mathbf{f}_i, i \in C$ at the beginning so that Z is well-defined during the setup phase. This is analogous to the *very selective* security in the setting of ABE [AMY19] where the adversary claims the challenge and all key queries at the beginning. We finally mention that the adversary is still free to choose $\mathsf{pk}_1, \ldots, \mathsf{pk}_L$ after seeing crs.

Solution 3.2: Simulation-based Security via PReg-IPFE. Roughly, we will make use of pre-constrained registration in (8) to implement the idea of function-hiding IPFE [LV16] and slotted IPFE [LL20]: instead of embedding a private "slot" into a key, we will embed this private "slot" into $\mathbf{M}$ in crs. (Note that the "slot" here has different means with the slots in the context of Reg-IPFE.) For this, we first extend the notion of *pre-constrained registration*:

- crs is generated along with $\boxed{\mathbf{M}_1, \ldots, \mathbf{M}_L}$ for the L slots, respectively.
- Decrypting a ciphertext of $\mathbf{x}$ using sk_i for slot i gives $[\mathbf{x}\boxed{\mathbf{M}_i}\mathbf{f}_i^{\top}]_T$ for all $i \in [L]$.

A minor revision of (8) below already works with analogous correctness and selective IND-security.

$$\begin{aligned}
\mathsf{crs} &= [\mathbf{AW}]_1, [\mathbf{AW}_j(\boxed{\mathbf{M}_j} \otimes \mathbf{I}_{k+1})]_1, \boxed{[\mathbf{M}_j]_2}, \quad \forall j \in [L] \\
&\quad [\mathbf{Br}_i^{\top}, \mathbf{W}_j(\boxed{\mathbf{M}_j} \otimes \mathbf{Br}_i^{\top}), \mathbf{W}_i(\boxed{\mathbf{M}_i} \otimes \mathbf{Br}_i^{\top}) + \mathbf{W}\boxed{\mathbf{M}_i}]_2, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\
\mathsf{mpk}_{\mathsf{R}} &= [\textstyle\sum_j (\mathbf{AU}_j + \mathbf{AW}_j(\boxed{\mathbf{M}_j}\mathbf{f}_j^{\top} \otimes \mathbf{I}_{k+1})), \mathbf{AW}]_1 \qquad (9) \\
\mathsf{hsk}_i &= [\mathbf{Br}_i^{\top}, \textstyle\sum_{j \neq i} (\mathbf{U}_j \mathbf{Br}_i^{\top} + \mathbf{W}_j(\boxed{\mathbf{M}_j}\mathbf{f}_j^{\top} \otimes \mathbf{Br}_i^{\top})), \mathbf{W}_i(\boxed{\mathbf{M}_i}\mathbf{f}_i^{\top} \otimes \mathbf{Br}_i^{\top}) + \mathbf{W}\boxed{\mathbf{M}_i}\mathbf{f}_i^{\top}, \boxed{\mathbf{M}_i\mathbf{f}_i^{\top}}]_2 \\
\mathsf{ct} &= [\mathbf{sA}, \mathbf{s}\textstyle\sum_j (\mathbf{AU}_j + \mathbf{AW}_j(\boxed{\mathbf{M}_j}\mathbf{f}_j^{\top} \otimes \mathbf{I}_{k+1})), \mathbf{sAW} + \mathbf{x}]_1
\end{aligned}$$

where $(\mathsf{pk}_i, \mathsf{sk}_i)$ is as in (8).

Scheme. We achieve SIM-security from IND-security as follows: we use the scheme (9) with the following special $[\mathbf{M}_1, \ldots, \mathbf{M}_L]_2$ in crs:

$$[\mathbf{M}_i]_2 = \begin{pmatrix} [\mathbf{M}]_2 & [0]_2 \\ [\mathbf{0}]_2 & \mathsf{Enc}(\mathsf{pk}, 0) \end{pmatrix} \qquad \text{where} \qquad (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$$

where $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a PKE with *linear decryption* whose message space serves as the private "slot". For concreteness, we leave formal definition in Section 2.5 and mention that ElGamal PKE with ciphertexts over $\mathbb{G}_2$ suffices:

$$\mathsf{pk} = [\mathbf{A}, \mathbf{wA}]_2, \quad \mathsf{sk} = (-\mathbf{w}, 1) \in \mathbb{Z}_p^{1 \times (k+2)}, \quad \mathsf{Enc}(\mathsf{pk}, x) = \begin{pmatrix} [\mathbf{As}^{\top}]_2 \\ [x + \mathbf{wAs}^{\top}]_2 \end{pmatrix} \in \mathbb{G}_2^{k+2}$$

where $\mathbf{A} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{w} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$, $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and it is easy to verify the linear decryption. Accordingly,

- in the registration phase, given $\mathsf{R} = ((\mathsf{pk}_1, \mathbf{f}_1), \ldots, (\mathsf{pk}_L, \mathbf{f}_L))$, we register extended $\overline{\mathsf{R}} = ((\mathsf{pk}_1, \overline{\mathbf{f}}_1), \ldots, (\mathsf{pk}_L, \overline{\mathbf{f}}_L))$ where $\overline{\mathbf{f}}_i = (\mathbf{f}_i \| 1)$ for all $i \in [L]$;
- to encrypt $\mathbf{x}$, we encrypt extended message $\overline{\mathbf{x}} = (\mathbf{x} \| 0)$.

The correctness follows from the fact that $\overline{\mathbf{x}}\mathbf{M}_i\overline{\mathbf{f}}_i^{\top} = \mathbf{xMf}_i^{\top}$ for all $i \in [L]$.

Simulator & Proof. Let us sketch the idea to simulator. Given $\mathbf{f}_i$ and $\mathbf{xMf}_i^{\top}$ for all $i \in C$, we first change $\mathbf{M}_i$ to $\widetilde{\mathbf{M}}_i$ for all $i \in C$ and then switch $\overline{\mathbf{x}}$ to $\widetilde{\mathbf{x}}$ where

$$\widetilde{\mathbf{M}}_i = \begin{pmatrix} \mathbf{M} & 0 \\ \mathbf{0} & \boxed{\mathsf{Enc}(\mathsf{pk}, \mathbf{xMf}_i^{\top})} \end{pmatrix} \quad \text{and} \quad \widetilde{\mathbf{x}} = (\mathbf{0} \| \mathsf{sk})$$

Here, the first $\mathbf{M}_i \mapsto \widetilde{\mathbf{M}}_i$ step follows from the security of $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, the second $\overline{\mathbf{x}} \mapsto \widetilde{\mathbf{x}}$ step follows from the selective IND-security of (9) by the fact that, for all $i \in C$, we have

$$\widetilde{\mathbf{x}}\widetilde{\mathbf{M}}_i\overline{\mathbf{f}}_i^{\top} = \mathsf{sk} \cdot \mathsf{Enc}(\mathsf{pk}, \mathbf{xMf}_i^{\top}) = \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, \mathbf{xMf}_i^{\top})) = \mathbf{xMf}_i^{\top} = \overline{\mathbf{x}}\widetilde{\mathbf{M}}_i\overline{\mathbf{f}}_i^{\top}$$

Here we do not need to maintain a similar relation for the case $i \in H$. At this point, we can simulate everything without knowing $\mathbf{x}$ but $\mathbf{xMf}_i^{\top}$ for all $i \in C$. This yields a very selective simulator. Furthermore, we embed the results Z into $\mathbf{M}_1, \ldots, \mathbf{M}_L$ which are over groups as in (8). This addresses **Challenge 3**.

Final Scheme with Compact Ciphertexts. Putting all these together, the technical line depicted in (5) works but leads to a Reg-QFE with ciphertexts of size $O(n \cdot \log L)$. The reason is: to move from L-slotted Reg-QFE to Reg-QFE with L slots, "powers-of-two" transformation runs $\log L$ parallel instances of slotted Reg-QFE. This means we encrypt the same message $(\mathbf{x}_1, \mathbf{x}_2)$ of size $2n$ for $\log L$ times (in the worst case). To avoid this, we let all $\log L$ instances have shared $\mathbf{A}_1$ and $\mathbf{A}_2$ in crs and encrypt the message *once for all*. However this is not enough: the $\log L$ underlying slotted PReg-IPFE instances encrypt the same $\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$ for $\log L$ times. To fix this, we let all instances share $\mathbf{W}$ in crs and encrypt $\mathbf{x}$ *once for all* with shared random coin $\mathbf{s}$; by this, all instances share the term $\mathbf{sAW} + \mathbf{x}$ in ciphertexts, cf. (9). Formally, we introduce the *multi-instance* variants of scheme (9) and update the technical line (5) as follows:

$$\begin{aligned} &\textit{multi-instance} \text{ slotted PReg-IPFE} \\ \Longrightarrow\quad &\textit{multi-instance} \text{ slotted Reg-QFE} \\ \Longrightarrow\quad &\textit{compact} \text{ Reg-QFE} \end{aligned} \tag{10}$$

This line gives Reg-QFE with ciphertexts of size $O(n + \log L)$ and we consider this as our main result **(2)**.

More Results & Roadmap. In Section 5, we treat the second " $\Longrightarrow$ " in the new technical line (10) as a general transformation. For more details, we give the definitions of multi-instance slotted Reg-FE for *general* functions in Section 5.1; and present the transformation from multi-instance slotted Reg-FE to compact Reg-FE for *general* functions in Section 5.2. This leads to result **(ii)**:

- Setting $\mathbf{M}_i = \mathbf{I}$ for all $i \in [L]$ (i.e., scheme (7)) gives IND-secure multi-instance slotted Reg-IPFE scheme, with fixed decryption base, c.f. Section 6.5. With the generic transformation in Section 5.2, it leads to the IND-secure compact Reg-IPFE.
- Setting $\mathbf{M} = \mathbf{I}$ gives us the SIM-secure multi-instance slotted Reg-IPFE scheme, c.f. Section 6.4. With the generic transformation in Section 5.2, it leads to the SIM-secure compact Reg-IPFE.

We summarize the roadmap of this part in Fig. 3, where "mi" means "multi-instance" for short.

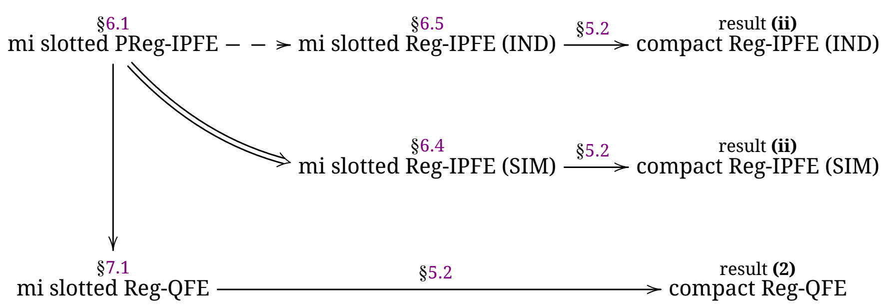

Fig. 3: Roadmap of the technical part. Here "mi" stands for "multi-instance". Those solid arrows show transformations proposed in this work; the dashed arrow means a mild adaptation; the double-line arrow indicates an implication.

2 Preliminaries

Notations. For a finite set S, we use $s \leftarrow S$ to denote the procedure of sampling s from S uniformly. For an ordered list or array $\mathcal{L}$, we use $|\mathcal{L}|$ to denote its size (i.e., the number of entries in the list) and use $\mathcal{L}[i]$ to refer to its i-th entry. When $i > |\mathcal{L}|$ or $i < 1$, we define $\mathcal{L}[i] = \perp$; when we append x to $\mathcal{L}$, we set $\mathcal{L}[|\mathcal{L}|+1] = x$. We use $\star$ as a wildcard. Let $\approx_s$ (resp. $\approx_c$) stand for two distributions being statistically (resp. computationally) indistinguishable. We use lower-case boldface to denote *row* vectors (e.g., $\mathbf{a}$) and upper-case boldface to denote matrices (e.g. $\mathbf{M}$). We use $\mathsf{span}(\mathbf{M})$ to denote the row span of $\mathbf{M}$, and use $\mathsf{basis}(\mathbf{M})$ to denote a basis of the column space of $\mathbf{M}$. Let $\mathbb{F}$ be a field. We use $\mathbf{A} \otimes \mathbf{B}$ to denote *Kronecker Product* for matrices $\mathbf{A} \in \mathbb{F}^{\ell \times m}$ and $\mathbf{B} \in \mathbb{F}^{n \times p}$. For matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}$ of proper sizes, we have: $(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = \mathbf{AC} \otimes \mathbf{BD}$. We use $n \oplus m$ to denote *XOR* for numbers $n, m \in \mathbb{N}$.

2.1 Prime-Order Bilinear Groups

Assume an efficient $\mathcal{G}$ that takes as input a security parameter 1^λ and outputs $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. Here $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are cyclic groups of prime order p, $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a non-degenerate bilinear map, and all group operations and bilinear map are efficient. Let $\mathbb{G}_1 = \langle g_1 \rangle$, $\mathbb{G}_2 = \langle g_2 \rangle$ and $g_T = e(g_1, g_2)$, we employ *implicit representation* of group elements: for a matrix $\mathbf{M} = (m_{ij})$ over $\mathbb{Z}_p$, define $[\mathbf{M}]_s = g_s^{\mathbf{M}} = (g_s^{m_{ij}})$ for all $s \in \{1, 2, T\}$; given $[\mathbf{A}]_1, [\mathbf{B}]_2$, we write $e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{AB}]_T$.

Assumption 1 *((k, ℓ, d)-MDDH [EHK+13] over $\mathbb{G}_s$, $s \in \{1, 2\}$) Let $k, \ell, d \in \mathbb{N}$. We say that the (k, ℓ, d)-MDDH assumption holds[7] in $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}^{\text{MDDH}}_{\mathcal{A},s,k,\ell,d}(\lambda) = \left| \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_s, [\mathbf{SM}]_s) = 1] - \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_s, [\mathbf{U}]_s) = 1] \right|$$

where $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$, $\mathbf{M} \leftarrow \mathbb{Z}_p^{k \times \ell}$, $\mathbf{S} \leftarrow \mathbb{Z}_p^{d \times k}$ and $\mathbf{U} \leftarrow \mathbb{Z}_p^{d \times \ell}$.

It is shown that the assumption is implied by k-Lin [EHK+13]. The *bilateral MDDH* assumption is defined analogously with the advantage function:

$$\mathsf{Adv}^{\text{bi-MDDH}}_{\mathcal{A},s,k,\ell,d}(\lambda) = \left| \Pr[\mathcal{A}(\mathbb{G}, \{[\mathbf{M}]_s, [\mathbf{SM}]_s\}_{s \in \{1,2\}}) = 1] - \Pr[\mathcal{A}(\mathbb{G}, \{[\mathbf{M}]_s, [\mathbf{U}]_s\}_{s \in \{1,2\}}) = 1] \right|$$

2.2 Registered Functional Encryption (Reg-FE)

Algorithms. A *registered functional encryption* [FFM+23,DP23] (Reg-FE for short) for functionality $F = \{f : X \to Z\}$ consists of six algorithms:

- $\mathsf{Setup}(1^\lambda, 1^L, F) \to \mathsf{crs}$: It takes as input security parameter 1^λ, maximum number of users 1^L, functionality F, outputs a common reference string crs.
- $\mathsf{Gen}(\mathsf{crs}, \mathsf{aux}) \to (\mathsf{pk}, \mathsf{sk})$: It takes as input crs and state aux, outputs key pair $(\mathsf{pk}, \mathsf{sk})$.
- $\mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f) \to (\mathsf{mpk}, \mathsf{aux}')$: It takes as input crs, aux, and pk along with function $f \in F$, outputs master public key mpk and updated state aux'.
- $\mathsf{Enc}(\mathsf{mpk}, x) \to \mathsf{ct}$: It takes as input mpk, $x \in X$, outputs a ciphertext ct.
- $\mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}) \to \mathsf{hsk}$: It take as input $\mathsf{crs}, \mathsf{aux}, \mathsf{pk}$, outputs a helper key hsk.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, \mathsf{ct}) \to z/\perp/\mathtt{getupd}$: It take as input $\mathsf{sk}, \mathsf{hsk}, \mathsf{ct}$ and outputs $z \in Z$ or a special symbol $\perp$ to indicate a decryption failure, or a special flag $\mathtt{getupd}$ to indicate the need of an updated helper key.

Correctness, Compactness and Update Efficiency. *Correctness* means, for all stateful (unbounded) adversary $\mathcal{A}$ making a polynomial number of oracle queries (defined below) and all L, the following advantage function is negligible in λ:

$$\Pr[b = 1 | \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F); b = 0; \mathcal{A}^{\mathsf{ORegNT}(\cdot,\cdot), \mathsf{ORegT}(\cdot), \mathsf{OEnc}(\cdot,\cdot), \mathsf{ODec}(\cdot)}(\mathsf{crs})]$$

where oracles work as follows with $\mathsf{aux} = \perp$, $\mathcal{E} = \emptyset$, $\mathcal{R} = \emptyset$ and $t = \perp$:

[7] The (k, ℓ, d)-MDDH assumption holds *unconditionally* when $\ell > k$.

- $\mathsf{ORegNT}(\mathsf{pk}, f)$: run $(\mathsf{mpk}, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f)$, update $\mathsf{aux} = \mathsf{aux}'$, append $(\mathsf{mpk}, \mathsf{aux})$ to $\mathcal{R}$ and return $(|\mathcal{R}|, \mathsf{mpk}, \mathsf{aux})$;
- $\mathsf{ORegT}(f^*)$: run $(\mathsf{pk}^*, \mathsf{sk}^*) \leftarrow \mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$, $(\mathsf{mpk}, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*, f^*)$, update $\mathsf{aux} = \mathsf{aux}'$, compute $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*)$, append $(\mathsf{mpk}, \mathsf{aux})$ to $\mathcal{R}$, return $(t = |\mathcal{R}|, \mathsf{mpk}, \mathsf{aux}, \mathsf{pk}^*, \mathsf{sk}^*, \mathsf{hsk}^*)$;
- $\mathsf{OEnc}(i, x)$: let $\mathcal{R}[i] = (\mathsf{mpk}, \star)$, run $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x)$, append (x, ct) to $\mathcal{E}$ and return $(|\mathcal{E}|, \mathsf{ct})$;
- $\mathsf{ODec}(j)$: let $\mathcal{E}[j] = (x_j, \mathsf{ct}_j)$, compute $z_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$; if $z_j = \texttt{getupd}$, run $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*)$ and recompute $z_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$. Set $b = 1$ when $z_j \neq f^*(x_j)$.

with the following restrictions:

- there are at most $L-1$ queries to ORegNT and there is exactly one query to ORegT; therefore, we will consider $f^*, \mathsf{pk}^*, \mathsf{sk}^*, \mathsf{hsk}^*$ to be global;
- for query (i, x) to OEnc, it holds that $i \geq t$, $\mathcal{R}[i] \neq \perp$;
- for query (j) to ODec, it holds that $\mathcal{E}[j] \neq \perp$.

Compactness means that, for all mpk and hsk in the above, we have

$$|\mathsf{mpk}| = \mathsf{poly}(\lambda, \mathsf{par}, \log L), \quad |\mathsf{hsk}| = \mathsf{poly}(\lambda, \mathsf{par}, \log L);$$

where par is a parameter depending on the functionality F. Furthermore, *update efficiency* means that the number of invocations of Upd in ODec is at most $O(\log |\mathcal{R}|)$ and each invocation costs $\mathsf{poly}(\log |\mathcal{R}|)$ time.

Indistinguishability-based Security (IND-security). For all stateful PPT adversary $\mathcal{A}$, the adaptive (resp., selective) indistinguishability-based security requires the advantage function $\mathsf{IndAdv}_{\mathcal{A}}^{\text{Ad-Reg-FE}}$ (resp., $\mathsf{IndAdv}_{\mathcal{A}}^{\text{Sel-Reg-FE}}$) defined as follows is negligible in λ:

$$\mathsf{IndAdv}_{\mathcal{A}}^{\text{Ad-Reg-FE}}(\lambda) = \Pr\left[b = b' \left| \begin{array}{l} \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, F); \\ x_0^*, x_1^* \leftarrow \mathcal{A}^{\mathsf{ORegCK}(\cdot,\cdot), \mathsf{ORegHK}(\cdot), \mathsf{OCorHK}(\cdot)}(\mathsf{crs}); \\ b \leftarrow \{0,1\}, \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, x_b^*), b' \leftarrow \mathcal{A}(\mathsf{ct}^*) \end{array} \right. \right] - 1/2,$$

where the oracles work as follows with initial setting $\mathsf{aux} = \perp$, $\mathsf{mpk} = \perp$, $\mathcal{H} = \emptyset$, $C = \emptyset$ and $\mathcal{D}$ being a dictionary with $\mathcal{D}[\mathsf{pk}] = \emptyset$ for all possible pk:

- $\mathsf{ORegCK}(\mathsf{pk}, f)$: run $(\mathsf{mpk}', \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f)$, update $\mathsf{mpk} = \mathsf{mpk}'$, $\mathsf{aux} = \mathsf{aux}'$, $\mathcal{D}[\mathsf{pk}] = \mathcal{D}[\mathsf{pk}] \cup \{f\}$, append pk to C and return $(\mathsf{mpk}, \mathsf{aux})$;
- $\mathsf{ORegHK}(f)$: run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$ and $(\mathsf{mpk}', \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f)$, update $\mathsf{mpk} = \mathsf{mpk}'$, $\mathsf{aux} = \mathsf{aux}'$, $\mathcal{D}[\mathsf{pk}] = \mathcal{D}[\mathsf{pk}] \cup \{f\}$, append $(\mathsf{pk}, \mathsf{sk})$ to $\mathcal{H}$ and return $(|\mathcal{H}|, \mathsf{mpk}, \mathsf{aux}, \mathsf{pk})$;
- $\mathsf{OCorHK}(i)$: let $\mathcal{H}[i] = (\mathsf{pk}, \mathsf{sk})$, append pk to C and return sk;

with the following restrictions:

- for query i to OCorHK, it holds that $\mathcal{H}[i] \neq \perp$;
- for all $f \in \bigcup_{\mathsf{pk} \in C} \mathcal{D}[\mathsf{pk}]$, it holds that $f(x_0^*) = f(x_1^*)$.

The selective IND-security is analogous to above definition of adaptive security, except that $\mathcal{A}$ claim the challenge x_0^*, x_1^* at the begining.

2.3 Slotted Registered Functional Encryption

Algorithms. A slotted Reg-FE (sReg-FE for short) for functionality $F = \{f : X \to Z\}$ consists of six efficient algorithms:

- $\mathsf{Setup}(1^\lambda, 1^L, F) \to \mathsf{crs}$: It takes as input security parameter 1^λ, maximum number of slots 1^L, functionality F, outputs a common reference string crs.
- $\mathsf{Gen}(\mathsf{crs}, i) \to (\mathsf{pk}_i, \mathsf{sk}_i)$: It takes as input crs and slot number $i \in [L]$, outputs key pair $(\mathsf{pk}_i, \mathsf{sk}_i)$.
- $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) \to 0/1$: It takes as input crs, i, pk_i and outputs a bit.
- $\mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, f_i)_{i\in[L]}) \to (\mathsf{mpk}, (\mathsf{hsk}_j)_{j\in[L]})$:[8] It takes as input crs and a series of pk_i with $f_i \in F$ for all $i \in [L]$, outputs master public key mpk and a series of helper keys hsk_j for all $j \in [L]$.
- $\mathsf{Enc}(\mathsf{mpk}, x) \to \mathsf{ct}$: It takes as input mpk, $x \in X$, outputs a ciphertext ct.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, \mathsf{ct}) \to z/\perp$: It takes as input sk, hsk, ct and outputs $z \in Z$ or a special symbol $\perp$.

We require that Agg and Dec are deterministic.

Completeness. For all $\lambda, L \in \mathbb{N}$, all F, and all $i \in [L]$, we have

$$\Pr\left[\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1 \,\middle|\, \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F);\ (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)\right] = 1.$$

Correctness. For all $\lambda, L \in \mathbb{N}$, all F, all $i^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i^*)$, all $\{\mathsf{pk}_i\}_{i\in[L]\setminus\{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, all $x \in X$ and $f_1, \ldots, f_L \in F$, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{i^*}, \mathsf{hsk}_{i^*}, \mathsf{ct}) = f_{i^*}(x) \,\middle|\, \begin{array}{l} (\mathsf{mpk}, (\mathsf{hsk}_j)_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, f_i)_{i\in[L]}) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x) \end{array}\right] = 1.$$

Compactness. For all $\lambda, L \in \mathbb{N}$, all P, and all $i \in [L]$, we have

$$|\mathsf{mpk}| = \mathrm{poly}(\lambda, P, \log L) \quad \text{and} \quad |\mathsf{hsk}_i| = \mathrm{poly}(\lambda, P, \log L).$$

Indistinguishability-based Security (IND-security). For all stateful PPT adversary $\mathcal{A}$, the adaptive (resp., selective) indistinguishability-based security requires the advantage function $\mathsf{IndAdv}_{\mathcal{A}}^{\text{Ad-sReg-FE}}$ (resp., $\mathsf{IndAdv}_{\mathcal{A}}^{\text{Sel-sReg-FE}}$) defined as follows is negligible in λ:

$$\mathsf{IndAdv}_{\mathcal{A}}^{\text{Ad-sReg-FE}}(\lambda) = \Pr\left[b = b' \,\middle|\, \begin{array}{l} L \leftarrow \mathcal{A}(1^\lambda);\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F) \\ (\mathsf{pk}_i^*, f_i^*)_{i\in[L]}, x_0^*, x_1^* \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot), \mathsf{OCor}(\cdot)}(\mathsf{crs}) \\ (\mathsf{mpk}, \ldots) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_1^*, f_1^*), \ldots, (\mathsf{pk}_L^*, f_L^*)) \\ b \leftarrow \{0,1\}, \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, x_b^*), b' \leftarrow \mathcal{A}(\mathsf{ct}^*) \end{array}\right] - 1/2,$$

where the oracles work as follows with the initial setting $C = \emptyset$ and $\mathcal{D}_i = \emptyset$ for all $i \in [L]$:

- $\mathsf{OGen}(i)$: run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)$, set $\mathcal{D}_i[\mathsf{pk}] = \mathsf{sk}$ and return pk.
- $\mathsf{OCor}(i, \mathsf{pk})$: return $\mathcal{D}_i[\mathsf{pk}]$ and update $C = C \cup \{(i, \mathsf{pk})\}$.

and for all $i \in [L]$, we require that

$$\mathcal{D}_i[\mathsf{pk}_i^*] = \perp \implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1 \quad \text{and} \quad (i, \mathsf{pk}_i^*) \in C \vee \mathcal{D}_i[\mathsf{pk}_i^*] = \perp \implies f_i^*(x_0^*) = f_i^*(x_1^*).$$

The selective IND-security is analogous to above definition of adaptive security, except that $\mathcal{A}$ claim the challenge x_0^*, x_1^* at the begining. Analogous to sReg-ABE [HLWW23], there is no need to give mpk and $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ to $\mathcal{A}$ explicitly and to consider post-challenge queries.

[8] Note that we use two difference indices i and j for pk_i and hsk_j, respectively; both of them range from 1 to L.

2.4 Quasi-Adaptive Non-Interactive Zero-Knowledge Argument

Algorithms. A Quasi-adaptive Non-interactive Zero-knowledge Argument (QA-NIZK) for linear space over bilinear group $\mathbb{G}$ [JR13,KW15] consists of four efficient algorithms:

- $\mathsf{LGen}(1^\lambda, 1^n, 1^m, 1^\ell, [\mathbf{M}]_1) \to (\mathsf{crs}, \mathsf{td})$: It takes as input the security parameter 1^λ, language parameter $1^n, 1^m, 1^\ell$, and a matrix $[\mathbf{M}]_1 \leftarrow \mathbb{G}_1^{n\times m}$ defining a linear space, outputs common reference string crs and trapdoor td.
- $\mathsf{LPrv}(\mathsf{crs}, [\mathbf{Y}]_1, \mathbf{X}) \to \pi$: It takes as input crs, a matrix $[\mathbf{Y}]_1 \in \mathbb{G}_1^{n\times \ell}$ along with $\mathbf{X} \in \mathbb{Z}_p^{m\times \ell}$ such that $\mathbf{Y} = \mathbf{MX}$, outputs a proof π.
- $\mathsf{LVer}(\mathsf{crs}, [\mathbf{Y}]_1, \pi) \to 0/1$: It takes as input crs, $[\mathbf{Y}]_1$ and π, outputs a bit showing the validity of π.
- $\mathsf{LSim}(\mathsf{crs}, \mathsf{td}, [\mathbf{Y}]_1) \to \widetilde{\pi}$: It takes as input crs, td, $[\mathbf{Y}]_1$, outputs a simulated proof $\widetilde{\pi}$.

Perfect Completeness. For all λ, $\mathbf{M}$, and all $\mathbf{X}, \mathbf{Y}$ such that $\mathbf{Y} = \mathbf{MX}$:

$$\Pr\left[\mathsf{LVer}(\mathsf{crs}, [\mathbf{Y}]_1, \pi) = 1 \,\middle|\, \begin{array}{l} (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{LGen}(1^\lambda, 1^n, 1^m, 1^\ell, [\mathbf{M}]_1) \\ \pi \leftarrow \mathsf{LPrv}(\mathsf{crs}, [\mathbf{Y}]_1, \mathbf{X}) \end{array}\right] = 1.$$

Perfect Zero-knowledge. For all λ, $\mathbf{M}$, $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{LGen}(1^\lambda, 1^n, 1^m, 1^\ell, [\mathbf{M}]_1)$, and all $\mathbf{X}, \mathbf{Y}$ such that $\mathbf{Y} = \mathbf{MX}$:

$$\mathsf{LPrv}(\mathsf{crs}, [\mathbf{Y}]_1, \mathbf{X}) \equiv \mathsf{LSim}(\mathsf{crs}, \mathsf{td}, [\mathbf{Y}]_1).$$

Unbounded Simulation Soundness. For all adversary $\mathcal{A}$, the advantage

$$\Pr\left[\begin{array}{l} ([\mathbf{Y}^*]_1, \pi) \notin Q \quad \wedge \\ \mathbf{Y}^* \notin \mathsf{span}(\mathbf{M}) \quad \wedge \\ \mathsf{LVer}(\mathsf{crs}, [\mathbf{Y}^*]_1, \pi^*) = 1 \end{array} \,\middle|\, \begin{array}{l} \mathbf{M} \leftarrow \mathbb{Z}_p^{n\times m} \\ (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{LGen}(1^\lambda, 1^n, 1^m, 1^\ell, [\mathbf{M}]_1) \\ ([\mathbf{Y}^*]_1, \pi^*) \leftarrow \mathcal{A}^{\mathsf{LSim}(\mathsf{crs}, \mathsf{td}, \cdot)}(1^\lambda, \mathsf{crs}, \mathbf{M}) \end{array}\right]$$

is negligible in λ, where Q records all queries to $\mathsf{LSim}(\mathsf{crs}, \mathsf{td}, \cdot)$ along with response. We use $\mathsf{Adv}^{\mathrm{USS}}_{\mathcal{A},n,m,\ell}(\lambda)$ to denote the advantage function. Note that our definition is stronger in the sense that the adversary is given $\mathbf{M}$ instead of $[\mathbf{M}]_1$.

Scheme from Pairings. It is shown in [KW15] that there exists QA-NIZK scheme for $\ell = 1$ in the prime-order bilinear group whose enhanced soundness (defined above) relies on MMDH assumption (see Assumption 1). For general $\ell > 1$, we simply employ ℓ parallel fresh instances. See [ZZGQ23] for more details.

2.5 Bilateral Public-Key Encryption with Linear Decryption

Algorithms. A *bilateral public-key encryption* (Bi-PKE) over bilinear group $\mathbb{G}$ consists of three efficient algorithms:

- $\mathsf{Gen}(1^\lambda) \to ([\mathsf{pk}]_1, [\mathsf{pk}]_2, \mathsf{sk})$: It takes as input the security parameter 1^λ, outputs public keys $[\mathsf{pk}]_1$ (over $\mathbb{G}_1$) and $[\mathsf{pk}]_2$ (over $\mathbb{G}_2$) and a secret key sk (over $\mathbb{Z}_p$).
- $\mathsf{Enc}([\mathsf{pk}]_1, [\mathsf{pk}]_2, \mathsf{m}) \to ([\mathsf{ct}]_1, [\mathsf{ct}]_2)$: It takes as input $[\mathsf{pk}]_1, [\mathsf{pk}]_2$ and a message $\mathsf{m} \in \mathbb{Z}_p$, outputs ciphertext $[\mathsf{ct}]_1$ (over $\mathbb{G}_1$) and $[\mathsf{ct}]_2$ (over $\mathbb{G}_2$).
- $\mathsf{Dec}_s([\mathsf{ct}]_s, \mathsf{sk}) \to \mathsf{m}'$, $s \in \{1, 2\}$: It takes as input a (partial) ciphertext $[\mathsf{ct}]_s$ over $\mathbb{G}_s$ and a secret key sk, outputs m'.

Correctness. For all $\lambda \in \mathbb{N}$, all $\mathsf{m} \in \mathbb{Z}_p$ all $s \in \{1, 2\}$, we have:

$$\Pr\left[\mathsf{Dec}_s([\mathsf{ct}]_s, \mathsf{sk}) = \mathsf{m} \,\middle|\, \begin{array}{l} ([\mathsf{pk}]_1, [\mathsf{pk}]_2, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \\ ([\mathsf{ct}]_1, [\mathsf{ct}]_2) \leftarrow \mathsf{Enc}([\mathsf{pk}]_1, [\mathsf{pk}]_2, \mathsf{m}) \end{array}\right] = 1.$$

Linear Decryption. For all $\lambda \in \mathbb{N}$, all $\mathsf{m} \in \mathbb{Z}_p$, we have $[\mathsf{ct}]_1$, $[\mathsf{ct}]_2$ and sk are vectors with same size (respectively over $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{Z}_p$), and for all $s \in \{1, 2\}$, we have:

$$\mathsf{sk} \cdot \mathsf{ct}^\top = \mathsf{Dec}_s([\mathsf{ct}]_s, \mathsf{sk}).$$

Security. For all stateful $\mathcal{A}$, the following advantage function is negligible

$$\mathsf{Adv}_{\mathcal{A}}^{\text{Bi-PKE}} = \Pr\left[b = b' \,\middle|\, \begin{array}{l} ([\mathsf{pk}]_1, [\mathsf{pk}]_2, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \\ m_0^*, m_1^* \leftarrow \mathcal{A}([\mathsf{pk}]_1, [\mathsf{pk}]_2) \\ b \leftarrow \{0, 1\}, ([\mathsf{ct}^*]_1, [\mathsf{ct}^*]_2) \leftarrow \mathsf{Enc}([\mathsf{pk}]_1, [\mathsf{pk}]_2, m_b^*) \\ b' \leftarrow \mathcal{A}([\mathsf{pk}]_1, [\mathsf{pk}]_2, [\mathsf{ct}^*]_1, [\mathsf{ct}^*]_2) \end{array}\right] - 1/2.$$

Group-based Encryption. For all $([\mathsf{pk}]_1, [\mathsf{pk}]_2) \in \mathsf{Gen}(1^\lambda)$, there exists a group-based algorithm Enc' such that

$$\mathsf{Enc}'([\mathsf{pk}]_1, [\mathsf{pk}]_2, [\mathsf{m}]_1, [\mathsf{m}]_2) \equiv \mathsf{Enc}([\mathsf{pk}]_1, [\mathsf{pk}]_2, \mathsf{m})$$

A Concrete Bi-PKE. We present a Bi-PKE transformed from ElGamal PKE:

– $\mathsf{Gen}(1^\lambda)$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k \times (k+1)}, \ \mathbf{w} \leftarrow \mathbb{Z}_p^{1 \times (k+1)}$$

Output:

$$[\mathsf{pk}]_1 = [\mathbf{A}, \mathbf{A}\mathbf{w}^\top]_1, [\mathsf{pk}]_2 = [\mathbf{A}, \mathbf{A}\mathbf{w}^\top]_2 \quad \text{and} \quad \mathsf{sk} = (-\mathbf{w}, 1)$$

– $\mathsf{Enc}([\mathsf{pk}]_1, [\mathsf{pk}]_2, \mathsf{m})$: Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$, output

$$[\mathsf{ct}]_1 = [\mathbf{sA}, \mathbf{sA}\mathbf{w}^\top + \mathsf{m}]_1, \ [\mathsf{ct}]_2 = [\mathbf{sA}, \mathbf{sA}\mathbf{w}^\top + \mathsf{m}]_2$$

– $\mathsf{Dec}([\mathsf{ct}]_s, \mathsf{sk})$: Compute

$$[z]_s = [\mathsf{sk} \cdot \mathsf{ct}^\top]_s$$

Recover z from $[z]_s$ via brute-force DLOG and output z.

3 Slotted Registered Inner-product Functional Encryption

In this section, we present our slotted Reg-IPFE scheme for the inner product functionality which is defined by $X = \mathbb{Z}_p^{1 \times n}$, $Z = \mathbb{Z}_p$ and

$$\mathrm{IP}_n = \{\mathbf{y} : \mathbf{x} \mapsto \mathbf{x}\mathbf{y}^\top\}$$

The scheme achieves the adaptive IND-security defined in Section 2.3 under the k-Lin assumption. Applying generic transformation [HLWW23,FFM+23,DP23] gives our Reg-IPFE scheme. Let us define dual basis and show related facts and assumptions.

Dual Basis. Let $\ell_1, \ell_2, \ell_3 \geq 1$ and $\ell := \ell_1 + \ell_2 + \ell_3$. We use basis

$$\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{\ell\times\ell_1},\ \mathbf{B}_2 \leftarrow \mathbb{Z}_p^{\ell\times\ell_2},\ \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{\ell\times\ell_3},$$

we denote $\mathbf{B}_1^{\|}, \mathbf{B}_2^{\|}, \mathbf{B}_3^{\|}$ as its dual basis, for all $\sigma, \delta \in \{1,2,3\}$, it holds that:

$$\mathbf{B}_\sigma^\top \mathbf{B}_\delta^{\|} = \begin{cases} \mathbf{I} & \text{when } \sigma = \delta \quad \text{(non-degeneracy)} \\ \mathbf{0} & \text{when } \sigma \neq \delta \quad \text{(orthogonality)} \end{cases}$$

Facts. With basis $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$ and its dual basis $\mathbf{B}_1^{\|}, \mathbf{B}_2^{\|}, \mathbf{B}_3^{\|}$, for all $\mathbf{v} \in \mathbb{Z}_p^{1\times n\ell}$, we can uniquely decompose $\mathbf{v}$ as

$$\mathbf{v} = \sum_{\sigma\in\{1,2,3\}} \mathbf{v}^{(\sigma)} \quad \text{where} \quad \mathbf{v}^{(\sigma)} \in \mathsf{span}(\mathbf{I}_n \otimes (\mathbf{B}_\sigma^{\|})^\top)$$

Note that for all $\sigma \in \{1,2,3\}$ and $n \in \mathbb{N}$, $\mathbf{v}^{(\sigma)}$ can be seen as the projection of $\mathbf{v}$ onto $\mathsf{span}(\mathbf{I}_n \otimes (\mathbf{B}_\sigma^{\|})^\top)$, and for each $S \subseteq \{1,2,3\}$, we write $\mathbf{v}^S = \sum_{\sigma\in S} \mathbf{s}^{(\sigma)}$. Moreover, it holds that:

$$\mathbf{v}\mathbf{B}_\sigma = \mathbf{v}^{(\sigma)}\mathbf{B}_\sigma, \quad \text{and} \quad \left\{\mathbf{v}^{(\sigma)}, \{\mathbf{v}^{(\delta)}\}_{\delta\neq\sigma}\right\} \equiv \left\{\mathbf{v}^*, \{\mathbf{v}^{(\delta)}\}_{\delta\neq\sigma}\right\}$$

where $\mathbf{v}^* \leftarrow \mathsf{span}(\mathbf{I}_n \otimes (\mathbf{B}_\sigma^{\|})^\top)$.

Assumption 2 *($\mathsf{SD}^{\mathbb{G}_s}_{\mathbf{B}_1\mapsto\mathbf{B}_2}$ for $s \in \{1,2\}$) Let $\ell_1, \ell_2, \ell_3 \geq 1$ and $\ell := \ell_1 + \ell_2 + \ell_3$. We say that the subspace decision assumption $\mathsf{SD}^{\mathbb{G}_s}_{\mathbf{B}_1\mapsto\mathbf{B}_2}$ holds in $\mathbb{G}_s$ if there exist an efficient sampler outputting random $[\mathbf{B}_1]_s \in \mathbb{G}_s^{\ell\times\ell_1}$, $[\mathbf{B}_2]_s \in \mathbb{G}_s^{\ell\times\ell_2}$, $[\mathbf{B}_3]_s \in \mathbb{G}_s^{\ell\times\ell_3}$ along with its dual basis: $\mathbf{B}_1^{\|}, \mathbf{B}_2^{\|}, \mathbf{B}_3^{\|}$ such that for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}^{\mathsf{SD}^{\mathbb{G}_s}_{\mathbf{B}_1\mapsto\mathbf{B}_2}}_{\mathcal{A},s,\ell_1,\ell_2,\ell_3} = |\Pr[\mathcal{A}(\mathbb{G}, D, [\mathbf{t}_0^\top]_s) = 1] - \Pr[\mathcal{A}(\mathbb{G}, D, [\mathbf{t}_1^\top]_s) = 1]|$$

where $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$, $D := \left([\mathbf{B}_1]_s, [\mathbf{B}_2]_s, [\mathbf{B}_3]_s, \mathsf{basis}(\mathbf{B}_1^{\|}, \mathbf{B}_2^{\|}), \mathsf{basis}(\mathbf{B}_3^{\|})\right)$ and $\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{B}_1^\top)$, $\mathbf{t}_1 \leftarrow \mathsf{span}(\mathbf{B}_2^\top)$.

3.1 Scheme

Assuming QA-NIZK $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ for linear space over bilinear groups, see Section 2.4, our slotted Reg-IPFE scheme in prime-order bilinear groups works as follows:

– $\mathsf{Setup}(1^\lambda, 1^n, 1^L)$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k},\ \mathbf{V} \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)}.$$

For all $i \in [L]$, sample

$$\mathbf{W}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)n},\ \mathbf{R}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)},\ \mathbf{r}_i \leftarrow \mathbb{Z}_p^{1\times k}.$$

For all $i \in [L]$, write $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{R}_i} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$, run

$$(\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1).$$

Output

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AV}]_1, \left\{[\mathbf{B}_1\mathbf{r}_j^\top]_2\right\}_{j\in[L]} \\ \left\{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{AW}_i]_1\right\}_{i\in[L]} \\ \left\{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\right\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$

Note that we do not use $\mathsf{td}_1, \ldots, \mathsf{td}_L$ in the actual scheme.

– $\mathsf{Gen}(\mathsf{crs}, i)$: Sample $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)}$. Define $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i} = \binom{\mathbf{A}\mathbf{U}_i}{\mathbf{R}_i\mathbf{U}_i} = \mathbf{A}_i\mathbf{U}_i \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$ and run

$$\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i).$$

Fetch $\{[\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[L]\setminus\{i\}}$ from crs and output

$$\mathsf{pk}_i = \big([\underbrace{\mathbf{A}\mathbf{U}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{R}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{[\underbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big) \quad \text{and} \quad \mathsf{sk}_i = \mathbf{U}_i.$$

– $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i)$: Parse $\mathsf{pk}_i = \big([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{h}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$. Write $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i}$ and check

$$\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \pi_i) \stackrel{?}{=} 1.$$

For each $j \in [L] \setminus \{i\}$, check

$$e([\mathbf{A}]_1, [\mathbf{h}_{i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_i]_1, [\mathbf{B}_1\mathbf{r}_j^\top]_2).$$

If all these checks pass, output 1; otherwise, output 0.

– $\mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, \mathbf{y}_i)_{i\in[L]})$: For all $i \in [L]$, parse $\mathsf{pk}_i = \big([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{h}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$. Output:

$$\mathsf{mpk} = \left(\left[\mathbf{A}, \sum_{i\in[L]}(\mathbf{T}_i + \mathbf{A}\mathbf{W}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1})), \sum_{i\in[L]}\mathbf{A}\mathbf{W}_i, \mathbf{A}\mathbf{V}\right]_1\right)$$

and for all $j \in [L]$

$$\mathsf{hsk}_j = \left(\left[\underbrace{\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i\in[L]\setminus\{j\}}(\mathbf{h}_{i,j} + \mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)\mathbf{y}_i^\top)}_{\mathbf{k}_1^\top}, \underbrace{\sum_{i\in[L]\setminus\{j\}}\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)}_{\mathbf{K}_2}\right]_2\right).$$

– $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x})$: Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$. Output:

$$\mathsf{ct} = \left(\left[\underbrace{\mathbf{s}\mathbf{A}}_{\mathbf{c}_0}, \underbrace{\sum_{i\in[L]}(\mathbf{s}\mathbf{T}_i + \mathbf{s}\mathbf{A}\mathbf{W}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1}, \underbrace{\mathbf{x} \otimes \mathbf{s}\mathbf{A}\mathbf{V} + \sum_{i\in[L]}\mathbf{s}\mathbf{A}\mathbf{W}_i}_{\mathbf{c}_2}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{V}}_{\mathbf{c}_3}\right]_1\right).$$

– $\mathsf{Dec}(\mathsf{sk}_{i^*}, \mathsf{hsk}_{i^*}, \mathsf{ct})$: Parse

$$\mathsf{sk}_{i^*} = \mathbf{U}_{i^*}, \quad \mathsf{hsk}_{i^*} = ([\mathbf{k}_0^\top, \mathbf{k}_1^\top, \mathbf{K}_2]_2), \quad \mathsf{ct} = ([\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3]_1).$$

Recover

$$\begin{aligned}
&[\mathbf{z}_1]_T = e([\mathbf{c}_2]_1, [\mathbf{I}_n \otimes \mathbf{k}_0^\top]_2), && [\mathbf{z}_2]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_2]_2);\\
&[z_3]_T = e([\mathbf{c}_1]_1, [\mathbf{k}_0^\top]_2), && [z_4]_T = e([\mathbf{c}_0]_1, [\mathbf{k}_1^\top]_2);\\
&[z_5]_T = e([\mathbf{c}_0\mathbf{U}_{i^*}]_1, [\mathbf{k}_0^\top]_2), &&\\
&[z_6]_T = e([\mathbf{c}_3]_1, [\mathbf{k}_0^\top]_2). &&
\end{aligned}$$

Compute

$$[z']_T = [(\mathbf{z}_1 - \mathbf{z}_2)\mathbf{y}_{i^*}^\top - (z_3 - z_4 - z_5)]_T.$$

Recover z from $[z']_T$ over $[z_6]_T$ via brute-force DLOG and output z.

Completeness. For all $\lambda, L, n \in \mathbb{N}$, all $i \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^n, 1^L)$ and $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)$, we have

$$\mathsf{pk}_i = \left([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{h}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\right) = \left([\mathbf{A}\mathbf{U}_i, \mathbf{R}_i\mathbf{U}_i]_1, \{[\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\right)$$

for some $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)}$ and $\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{A}_i\mathbf{U}_i]_1, \mathbf{U}_i)$ where $(\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$ and $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{R}_i}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$, $\mathbf{R}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}$. Then

- Write $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i} = \binom{\mathbf{A}\mathbf{U}_i}{\mathbf{R}_i\mathbf{U}_i}$, we have $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \pi_i) = 1$ by the perfect completeness of Π_0 (see Section 2.4) and the fact that $\mathbf{F}_i = \mathbf{A}_i\mathbf{U}_i$;
- For each $j \in [L] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top]_2) = e([\mathbf{A}\mathbf{U}_i]_1, [\mathbf{B}_1\mathbf{r}_j^\top]_2)$ by the definition of bilinear map e (see Section 2.1) and the fact that $\mathbf{A}\cdot\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top = \mathbf{A}\mathbf{U}_i\cdot\mathbf{B}_1\mathbf{r}_j^\top$.

This ensures that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$ by the specification of Ver and readily proves the completeness.

Correctness. For all $\lambda, L, n \in \mathbb{N}$, , all $i^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^n, 1^L)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i^*)$, all $\{\mathsf{pk}_i\}_{i\in[L]\setminus\{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, for all $\mathbf{y}_1, \ldots, \mathbf{y}_L \in \mathbb{Z}_p^n$ and $\mathbf{x} \in \mathbb{Z}_p^n$, we have:

$$\begin{aligned}
\mathsf{sk}_{i^*} &= \mathbf{U}_{i^*},\\
\mathsf{ct} &= \left(\left[\underbrace{\mathbf{sA}}_{\mathbf{c}_0}, \underbrace{\sum_{i\in[L]}(\mathbf{sT}_i + \mathbf{sAW}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1}, \underbrace{\mathbf{x}\otimes\mathbf{sAV} + \sum_{i\in[L]}\mathbf{sAW}_i}_{\mathbf{c}_2}, \underbrace{\mathbf{sAV}}_{\mathbf{c}_3}\right]_1\right)\\
\mathsf{hsk}_{i^*} &= \left(\left[\underbrace{\mathbf{B}_1\mathbf{r}_{i^*}^\top}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i\in[L]\setminus\{i^*\}}(\mathbf{h}_{i,i^*} + \mathbf{W}_i(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_i^\top)}_{\mathbf{k}_1^\top}, \underbrace{\sum_{i\in[L]\setminus\{i^*\}}\mathbf{W}_i(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top)}_{\mathbf{K}_2}\right]_2\right)
\end{aligned}$$

where

$$\mathbf{A}\mathbf{h}_{i,i^*} = \mathbf{T}_i\mathbf{B}_1\mathbf{r}_{i^*}^\top \quad \forall i \in [L]\setminus\{i^*\} \quad \text{and} \quad \mathbf{A}\mathbf{U}_{i^*} = \mathbf{T}_{i^*}.$$

Note that here we actually consider hsk_j for $j = i^*$ and sk_i for $i = i^*$ and all above equalities are ensured by Ver and Gen. we have

$$\begin{aligned}
\mathbf{z}_1 &= (\mathbf{x}\otimes\mathbf{sAV})(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top) + \sum_{i\in[L]}\mathbf{sAW}_i(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top)\\
&= \mathbf{sAV}(\mathbf{x}\otimes\mathbf{I}_{2k+1})(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top) + \sum_{i\in[L]}\mathbf{sAW}_i(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top)\\
&= \mathbf{sAVB}_1\mathbf{r}_{i^*}^\top\mathbf{x} + \sum_{i\in[L]}\mathbf{sAW}_i(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top) \qquad (11)\\
\mathbf{z}_2 &= \sum_{i\in[L]\setminus\{i^*\}}\mathbf{sAW}_i(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top)\\
z_3 &= \sum_{i\in[L]}(\mathbf{sT}_i\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{sAW}_i(\mathbf{y}_i^\top\otimes\mathbf{I}_{2k+1})\mathbf{B}_1\mathbf{r}_{i^*}^\top)\\
&= \sum_{i\in[L]}(\mathbf{sT}_i\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{sAW}_i(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_i^\top) \qquad (12)\\
z_4 &= \sum_{i\in[L]\setminus\{i^*\}}(\mathbf{sAh}_{i,i^*} + \mathbf{sAW}_i(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_i^\top)\\
z_5 &= \mathbf{sAU}_{i^*}\mathbf{B}_1\mathbf{r}_{i^*}^\top\\
z_6 &= \mathbf{sAVB}_1\mathbf{r}_{i^*}^\top
\end{aligned}$$

and then

$$
\begin{aligned}
[z']_T &= [(\mathbf{z}_1 - \mathbf{z}_2)\mathbf{y}_{i^*}^\top - (z_3 - z_4 - z_5)]_T \\
&= [(\mathbf{sAVB}_1\mathbf{r}_{i^*}^\top \cdot \mathbf{xy}_{i^*}^\top + \mathbf{sAW}_{i^*}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_{i^*}^\top) - (\mathbf{sT}_{i^*}\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{sAW}_{i^*}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_{i^*}^\top - \mathbf{sAU}_{i^*}\mathbf{B}_1\mathbf{r}_{i^*}^\top)]_T \qquad (13) \\
&= [\mathbf{sAVB}_1\mathbf{r}_{i^*}^\top \cdot \mathbf{xy}_{i^*}^\top]_T \qquad (14)
\end{aligned}
$$

Here, equality (11) and equality (12) follows from the property of tensor product: $(\mathbf{M} \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{a}^\top) = \mathbf{M} \otimes \mathbf{a}^\top = (\mathbf{I} \otimes \mathbf{a}^\top)\mathbf{M}$ for matrices of proper size; equality (13) follows from the fact that $\mathbf{Ah}_{i,i^*} = \mathbf{T}_i\mathbf{B}_1\mathbf{r}_{i^*}^\top$ for all $i \in [L] \setminus \{i^*\}$; equality (14) follows from the fact that $\mathbf{T}_{i^*} = \mathbf{AU}_{i^*}$. Treat $[z_6]_T = [\mathbf{sAVB}_1\mathbf{r}_{i^*}^\top]_T$ as the basis, and recover z from $[z']_T = [\mathbf{sAVB}_1\mathbf{r}_{i^*}^\top \cdot \mathbf{xy}_{i^*}^\top]_T$ via brute-force DLOG, we have

$$z = \mathbf{xy}_{i^*}^\top$$

This proves the correctness.

Compactness and Efficiency. Our slotted Reg-IPFE has the following properties:

$$|\mathsf{crs}| = L^2 \cdot n \cdot \mathsf{poly}(\lambda); \quad |\mathsf{mpk}| = n \cdot \mathsf{poly}(\lambda); \quad |\mathsf{hsk}_j| = n \cdot \mathsf{poly}(\lambda); \quad |\mathsf{ct}| = n \cdot \mathsf{poly}(\lambda).$$

Note that the total size of $\{\mathsf{crs}_i\}_{i\in[L]}$ is $L \cdot \mathsf{poly}(\lambda)$ according to the efficiency of the pairing-based QA-NIZK scheme by Kiltz and Wee [KW15] and the fact that the size of language description is $\mathsf{poly}(\lambda)$.

Security. We have the following theorem. Given pairing-based QA-NIZK in [KW15] with unbounded simulation soundness under MDDH assumption and the fact that MDDH assumption implies subspace decision assumption [CGKW18], our slotted Reg-IPFE scheme achieves adaptive IND-security from MDDH assumption.

Theorem 1. *Assume* $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ *is a QA-NIZK with perfect completeness, perfect zero-knowledge and unbounded simulation soundness for linear space defined in Section 2.4, our slotted Reg-IPFE scheme achieves the adaptive IND-security defined in Section 2.3 under MDDH assumption and subspace decision assumption.*

3.2 Proof

We prove the following technical lemma; this immediately proves Theorem 1.

Lemma 1. *For all adversaries* $\mathcal{A}$*, there exist adversaries* $\mathcal{B}_1$*,* $\mathcal{B}_2$*,* $\mathcal{B}_3$ *and* $\mathcal{B}_4$ *such that:*

$$\mathsf{IndAdv}_{\mathcal{A}}^{\textit{Ad-sReg-IPFE}}(\lambda) \le L \cdot \mathsf{Adv}_{\mathcal{B}_1}^{\textit{USS}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_2}^{\textit{MDDH}}(\lambda) + L \cdot \mathsf{Adv}_{\mathcal{B}_3}^{\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_3}}(\lambda) + L \cdot \mathsf{Adv}_{\mathcal{B}_4}^{\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_2}}(\lambda) + \mathsf{negl}(\lambda)$$

where L *is the number of slots and* $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3), \mathsf{Time}(\mathcal{B}_4) \approx \mathsf{Time}(\mathcal{A})$.

Game Sequence. Suppose that crs is the common reference string, $(\mathbf{x}_0^*, \mathbf{x}_1^*)$ is the challenge pair, $\{\mathsf{pk}_i^*, \mathbf{y}_i^*\}_{i\in[L]}$ are challenge public keys along with challenge functions to be registered. For all $i \in [L]$, define $D_i = \{\mathsf{pk}_i : \mathcal{D}_i[\mathsf{pk}_i] = \mathsf{sk}_i \neq \bot\}$ be responses to $\mathsf{OGen}(i)$ and $C_i = \{\mathsf{pk}_i : (i, \mathsf{pk}_i) \in C\}$ records public keys in D_i that have been sent to $\mathsf{OCor}(i, \cdot)$. Recall that, for each $i \in [L]$, we require that

$$\mathsf{pk}_i^* \notin D_i \implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1, \quad \mathsf{pk}_i^* \in C_i \vee \mathsf{pk}_i^* \notin D_i \implies \mathbf{x}_0^*(\mathbf{y}_i^*)^\top = \mathbf{x}_1^*(\mathbf{y}_i^*)^\top.$$

Note that pk_i serves as a *general* entry in D_i while pk_i^* is the *specific* challenge public for slot i; there can be more than one assignments for pk_i since the adversary can invoke $\mathsf{OGen}(i)$ for many times. We prove the Lemma 1 via nested dual-system method using the following game sequence.

– G_0: This is the real game, recall that we have

- crs is in the form:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AV}]_1, \left\{[\mathbf{B}_1\mathbf{r}_j^\top]_2\right\}_{j\in[L]} \\ \left\{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{AW}_i]_1\right\}_{i\in[L]} \\ \left\{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\right\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$

  where $\mathsf{crs}_i \in \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$, $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{R}_i}$.
- For each $i \in [L]$, each $\mathsf{pk}_i, \in D_i$ is in the form:

$$\mathsf{pk}_i = \big([\underbrace{\mathbf{AU}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{R}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{[\underbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$$

  where $\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i)$, $\mathbf{F}_i = \binom{\mathbf{AU}_i}{\mathbf{R}_i\mathbf{U}_i}$, and $\mathbf{U}_i$ is the corresponding sk_i.
- For all $i \in [L]$, pk_i^* is in the form:

$$\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{h}_{i,j}^*]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$$

  such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1$ which means $\mathsf{LVer}\left(\mathsf{crs}_i, \begin{bmatrix}\mathbf{T}_i^* \\ \mathbf{Q}_i^*\end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{Ah}_{i,j}^* = \mathbf{T}_i^*\mathbf{B}_1\mathbf{r}_j^\top$ for each $j \in [L]\setminus\{i\}$.
- ct^* for $(\mathbf{x}_0^*, \mathbf{x}_1^*)$ is in the form:

$$\mathsf{ct}^* = \left(\left[\underbrace{\mathbf{sA}}_{\mathbf{c}_0^*}, \underbrace{\sum_{i\in[L]}(\mathbf{sT}_i + \mathbf{sAW}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1^*}, \underbrace{\mathbf{x}_b^* \otimes \mathbf{sAV} + \sum_{i\in[L]}\mathbf{sAW}_i}_{\mathbf{c}_2^*}, \underbrace{\mathbf{sAV}}_{\mathbf{c}_3^*}\right]_1\right).$$

  where $b \leftarrow \{0,1\}$ is the secret bit.

– G_1: Identical to G_0 except that, for all $i \in [L]$ and all $\mathsf{pk}_i \in D_i$, we replace π_i with

$$\widetilde{\pi}_i \leftarrow \boxed{\mathsf{LSim}}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{F}_i]_1) \quad \text{where} \quad \mathbf{F}_i = \begin{pmatrix}\mathbf{AU}_i \\ \mathbf{R}_i\mathbf{U}_i\end{pmatrix}.$$

We have $\mathsf{G}_1 \equiv \mathsf{G}_0$. This follows from the perfect zero-knowledge of Π_0.

– G_2: Identical to G_1 except that we sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ along with $\mathbf{A}$ and replace all $\mathbf{R}_i$ in crs with

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix}\mathbf{sA} \\ \mathbf{I}_{2k+1}\end{pmatrix}, \quad \widetilde{\mathbf{R}}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}.$$

We have $\mathsf{G}_2 \equiv \mathsf{G}_1$. This follows from the fact that both $\mathbf{R}_i$ (in G_1) and $\widehat{\mathbf{R}}_i$ (in G_2) are truly random since matrix $\binom{\mathbf{sA}}{\mathbf{I}_{2k+1}}$ is full-rank.

– G_3: Identical to G_2 except that we generate the $\mathbf{c}_1^*$ as follows:

$$\mathbf{c}_1^* = \sum_{i\in[L]}(\boxed{\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*} + \mathbf{sAW}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1})).$$

We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from stronger unbounded simulation soundness of Π_0 along with the fact that $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i^*], \pi_i^*) = 1$ for all $i \in [L]$ where $\mathbf{F}_i^* = \begin{pmatrix}\mathbf{T}_i^* \\ \mathbf{Q}_i^*\end{pmatrix}$. Assume $\mathsf{pk}_{i^*}^* \notin D_{i^*}$, i.e., $\mathsf{pk}_{i^*}^*$ is malicious. In the reduction, we guess $i^* \leftarrow [L]$ and obtain $\mathbf{A}, \widehat{\mathbf{R}}_{i^*}, \mathsf{crs}_{i^*}$ as input; we simulate honestly as in G_3 except that for all $\mathsf{pk}_{i^*} \in D_{i^*}$, we make an oracle query $[\mathbf{F}_{i^*}]_1$ and get $\widetilde{\pi}_{i^*}$ in it; we finally output $([\mathbf{F}_{i^*}^*]_1, \pi_{i^*}^*)$ in $\mathsf{pk}_{i^*}^* \notin D_{i^*}$. Observe that once it happens that $\mathbf{e}_1\widetilde{\mathbf{R}}_{i^*}^{-1}\mathbf{Q}_{i^*}^* \neq \mathbf{sT}_{i^*}^*$, we must have $\mathbf{F}_{i^*}^* \notin \mathsf{span}(\mathbf{A}_{i^*})$. When $\mathsf{pk}_{i^*}^* \in D_{i^*}$, we always have $\mathsf{G}_3 \equiv \mathsf{G}_2$.

– G_4: Identical to G_3 except that we replace all $\mathbf{sA}$ with $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$; in particular, we generate $\widehat{\mathbf{R}}_i$ as follows:

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix} \boxed{\mathbf{c}} \\ \mathbf{I}_{2k+1} \end{pmatrix}, \quad \widetilde{\mathbf{R}}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}$$

and generate the challenge ciphertext as follows:

$$\mathsf{ct}^* = \left(\left[\underbrace{\boxed{\mathbf{c}}}_{\mathbf{c}_0^*}, \underbrace{\sum_{i\in[L]} (\mathbf{e}_1 \widetilde{\mathbf{R}}_i^{-1} \mathbf{Q}_i^* + \boxed{\mathbf{c}} \mathbf{W}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1^*}, \underbrace{\mathbf{x}_b^* \otimes \boxed{\mathbf{c}}\mathbf{V} + \sum_{i\in[L]} \boxed{\mathbf{c}}\mathbf{W}_i}_{\mathbf{c}_2^*}, \underbrace{\boxed{\mathbf{c}}\mathbf{V}}_{\mathbf{c}_3^*} \right]_1 \right).$$

We have $\mathsf{G}_4 \approx_c \mathsf{G}_3$. This follows from MDDH assumption which ensures that $([\mathbf{A}]_1, [\mathbf{sA}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{c}]_1)$ when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}, \mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$.

– G_5: Identical to G_4 except that for all $i \in [L]$, we replace $\mathbf{AV}$ in crs with

$$\widetilde{\mathbf{V}} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$$

we replace $\mathbf{cV}$ in challenge ciphertext with

$$\mathbf{v} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$$

In particular, we generate crs as below:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \boxed{\widetilde{\mathbf{V}}}]_1, \{[\mathbf{B}_1 \mathbf{r}_j^\top]_2\}_{j\in[L]} \\ \{\mathsf{crs}_i, [\widehat{\mathbf{R}}_i, \mathbf{AW}_i]_1\}_{i\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1 \mathbf{r}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix},$$

and generate the challenge ciphertext as

$$\mathsf{ct}^* = \left(\left[\underbrace{\mathbf{c}}_{\mathbf{c}_0^*}, \underbrace{\sum_{i\in[L]} (\mathbf{e}_1 \widetilde{\mathbf{R}}^{-1} \mathbf{Q}_i^* + \mathbf{c} \mathbf{W}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1^*}, \underbrace{\mathbf{x}_b^* \otimes \boxed{\mathbf{v}} + \sum_{i\in[L]} \mathbf{c}\mathbf{W}_i}_{\mathbf{c}_2^*}, \underbrace{\boxed{\mathbf{v}}}_{\mathbf{c}_3^*} \right]_1 \right).$$

We have $\mathsf{G}_5 \equiv \mathsf{G}_4$. This follows from the fact that when $\mathbf{V}$ is uniformly sampled from $\mathbb{Z}_p^{(2k+1)\times(2k+1)}$ and not published elsewhere, $(\mathbf{AV}, \mathbf{cV})$ (in G_4) is statically equivalent with the uniformly sampled $(\widetilde{\mathbf{V}}, \mathbf{v})$ where $\widetilde{\mathbf{V}} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{v} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$ (in G_5) , since both $\mathbf{A}$ and $\mathbf{c}$ are full row rank (with overwhelming probability).

– G_6: Identical to G_5 except that we randomly sample $\mathbf{B}_2 \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, and compute the dual basis $\mathbf{B}_1^{\|}, \mathbf{B}_2^{\|}, \mathbf{B}_3^{\|}$. And we change $\mathbf{c}_2^*$ as follows:

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1,3)} + \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]} \mathbf{cW}_i$$

We have $\mathsf{G}_6 \equiv \mathsf{G}_5$. This follows from the following argument for $b' = b$ (in G_5) or $b' = 0$ (in G_6):

$$\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]} (\mathbf{cW}_i)^{(2)} \equiv \sum_{i\in[L]} (\mathbf{cW}_i)^{(2)}$$

This argument follows from the fact that the basis $\mathbf{B}_2$ and dual basis $\mathbf{B}_2^{\|}$ are not revealed, so we have $(\mathbf{cW}_i)^{(2)}$ is hidden, this can imply that $\sum_{i\in[L]} (\mathbf{cW}_i)^{(2)}$ hides $\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(2)}$.

– $\mathsf{G}_{7,\ell}, (\ell \in [0, L])$: Identical to G_6 except that for all $j \in [\ell]$ we replace all $\mathbf{B}_1 \mathbf{r}_j^\top$ in crs with

$$\mathbf{d}_j^\top \quad \text{where} \quad \boxed{\mathbf{d}_j \leftarrow \mathsf{span}(\mathbf{B}_2^\top)}$$

We have that

- $\mathsf{G}_{7,0} = \mathsf{G}_6$; the two games are actually identical, since $[0] = \emptyset$;
- $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$ for all $\ell \in [L]$, we will employ a sub-sequence of games for the proof described later.

– G_8: Identical to $\mathsf{G}_{7,L}$ except that we generate the $\mathbf{c}_2^*$ as follows:

$$\mathbf{c}_2^* = \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(1,3)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]} \mathbf{c}\mathbf{W}_i$$

We have $\mathsf{G}_8 \equiv \mathsf{G}_{7,L}$. The proof is analogous to that of $\mathsf{G}_6 \equiv \mathsf{G}_5$, with the fact that basis $\mathbf{B}_1, \mathbf{B}_3$ and dual basis $\mathbf{B}_1^{\|}, \mathbf{B}_3^{\|}$ are not revealed in $\mathsf{G}_{7,L}$, we have the following argument for $b' = b$ (in $\mathsf{G}_{7,L}$) or $b' = 0$ (in G_8):

$$\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(1,3)} + \sum_{i\in[L]} (\mathbf{c}\mathbf{W}_i)^{(1,3)} \equiv \sum_{i\in[L]} (\mathbf{c}\mathbf{W}_i)^{(1,3)}$$

Observe that, in the final game G_8 the challenge ciphertext ct is independent of the random bit b and the adversary's advantage is exactly 0.

From $\mathsf{G}_{7,\ell-1}$ to $\mathsf{G}_{7,\ell}$. We are ready to prove $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$ and this will complete the proof of Lemma 1. For this, we need the following sub-sequence of games for each $\ell \in [L]$:

– $\mathsf{G}_{7,\ell-1,0}$: Identical to $\mathsf{G}_{7,\ell-1}$ where we recall crs, $\mathsf{pk}_i \in D_i$ and $\mathbf{c}_2^*$, with highlighting relevant terms in the following sub-sequence with dashed boxes as follows:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \{[\mathbf{d}_j^\top]_2\}_{j\in[\ell-1]}, \boxed{[\mathbf{B}_1\mathbf{r}_\ell^\top]_2}, \{[\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[L]\setminus[\ell]} \\ \{\mathsf{crs}_i, [\widehat{\mathbf{R}}_i, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{d}_j^\top)]_2\}_{j\in[\ell-1], i\in[L]\setminus\{j\}}, \\ \{\boxed{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_\ell^\top)]_2}\}_{i\in[L]\setminus\{\ell\}}, \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L]\setminus[\ell], i\in[L]\setminus\{j\}} \end{pmatrix},$$

$$\mathsf{pk}_i = \begin{cases} ([\overbrace{\mathbf{A}\mathbf{U}_i}^{\mathbf{T}_i}, \overbrace{\widehat{\mathbf{R}}_i\mathbf{U}_i}^{\mathbf{Q}_i}]_1, \{[\overbrace{\mathbf{U}_i\mathbf{d}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j\in[\ell-1]\setminus\{i\}}, \boxed{[\overbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{r}_\ell^\top}^{\mathbf{h}_{i,\ell}}]_2}, \{[\overbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus[i,\ell]}, \widetilde{\pi}_i) & \text{if } i \neq \ell \\ ([\underbrace{\mathbf{A}\mathbf{U}_\ell}_{\mathbf{T}_\ell}, \underbrace{\widehat{\mathbf{R}}_i\mathbf{U}_\ell}_{\mathbf{Q}_\ell}]_1, \{[\underbrace{\mathbf{U}_\ell\mathbf{d}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j\in[\ell-1]}, \{[\underbrace{\mathbf{U}_\ell\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j\in[L]\setminus[\ell]}, \widetilde{\pi}_\ell) & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_i$$

Where $\mathbf{d}_j \leftarrow \mathsf{span}(\mathbf{B}_2^\top)$ for all $j \in [\ell-1]$. We have $\mathsf{G}_{7,\ell-1,0} = \mathsf{G}_{7,\ell-1}$; all changes are conceptual.

– $\mathsf{G}_{7,\ell-1,1}$: Identical to $\mathsf{G}_{7,\ell-1,0}$ except that we replace all $\mathbf{B}_1\mathbf{r}_\ell^\top$ in crs with

$$\mathbf{d}_\ell^\top \quad \text{where} \quad \boxed{\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_3^\top)}.$$

In particular, we change the dashed boxed term in crs and pk_i as follows:

$$[\boxed{\mathbf{d}_\ell^\top}]_2, \{[\mathbf{W}_i(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top})]_2, [\mathbf{U}_i\boxed{\mathbf{d}_\ell^\top}]_2\}_{i\in[L]\setminus\{\ell\}}$$

We have $\mathsf{G}_{7,\ell-1,1} \approx_c \mathsf{G}_{7,\ell-1,0}$. This follow from the $\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_1\mapsto\mathbf{B}_3}$ assumption which ensure that

$$[\mathbf{t}_0]_2 \approx_c [\mathbf{t}_1]_2 \quad \text{given} \quad [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_1^{\|}, \mathbf{B}_3^{\|}), \mathsf{basis}(\mathbf{B}_2^{\|})$$

Where $\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{B}_1^\top)$ corresponding to $\mathsf{G}_{7,\ell-1,0}$, and $\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_3^\top)$ corresponding to $\mathsf{G}_{7,\ell-1,1}$.

– $\mathsf{G}_{7,\ell-1,2}$: Identical to $\mathsf{G}_{7,\ell-1,1}$ except that we generate the $\mathbf{c}_2^*$ as follows:

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell + \sum_{i \in [L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_i$$

We have $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$. We provide an overview of the proof in Section 3.3.

– $\mathsf{G}_{7,\ell-1,3}$: Identical to $\mathsf{G}_{7,\ell-1,2}$ except that we replace all $\mathbf{d}_\ell^\top$ in crs with

$$\mathbf{d}_\ell^\top \quad \text{where} \quad \boxed{\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_2^\top)}$$

In particular, we change the dashed boxed term in crs and pk_i as follows:

$$[\boxed{\mathbf{d}_\ell^\top}]_2, \{[\mathbf{W}_i(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top})]_2, [\mathbf{U}_i \boxed{\mathbf{d}_\ell^\top}]_2\}_{i \in [L]\setminus\{\ell\}}$$

We have $\mathsf{G}_{7,\ell-1,3} \approx_c \mathsf{G}_{7,\ell-1,2}$. This follow from the $\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_2}$ assumption which ensure that

$$[\mathbf{t}_0]_2 \approx_c [\mathbf{t}_1]_2 \quad \text{given} \quad [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel), \mathsf{basis}(\mathbf{B}_1^\parallel)$$

Where $\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{B}_3^\top)$ corresponding to $\mathsf{G}_{7,\ell-1,2}$, and $\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_2^\top)$ corresponding to $\mathsf{G}_{7,\ell-1,3}$.

– $\mathsf{G}_{7,\ell-1,4}$: Identical to $\mathsf{G}_{7,\ell-1,3}$ except that we generate the $\mathbf{c}_2^*$ as follows:

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell + \sum_{i \in [L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_i$$

We have $\mathsf{G}_{7,\ell-1,4} \approx_c \mathsf{G}_{7,\ell-1,3}$. The proof is identical to that for $\mathsf{G}_{7,\ell-1,2} \approx \mathsf{G}_{7,\ell-1,1}$.

Observe that $\mathsf{G}_{7,\ell-1,4} = \mathsf{G}_{7,\ell}$ and this prove $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$.

3.3 From $\mathsf{G}_{7,\ell-1,1}$ to $\mathsf{G}_{7,\ell-1,2}$

We review $\mathsf{G}_{7,\ell-1,1}$ and $\mathsf{G}_{7,\ell-1,2}$ in the following form. Here we use solid box to indicate the difference between two games and use dashed boxes to highlight those terms that are relevant to our proof. For all $j \in [\ell-1]$, we rewrite $\mathbf{d}_j \leftarrow \mathsf{span}(\mathbf{B}_2^\top)$ with $\mathbf{B}_2^\top r_j$, for some $r_j \leftarrow \mathbb{Z}_p$.

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \{[\mathbf{B}_2 r_j]_2\}_{j \in [\ell-1]}, [\mathbf{d}_\ell^\top]_2, \{[\mathbf{B}_1 \mathbf{r}_j^\top]_2\}_{j \in [L]\setminus[\ell]} \\ \{\mathsf{crs}_i, [\widehat{\mathbf{R}}_i, \mathbf{A}\mathbf{W}_i]_1\}_{i \in [L]} \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_2 r_j)]_2\}_{j \in [\ell-1], i \in [L]\setminus\{j\}}, \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top)]_2\}_{i \in [L]\setminus\{\ell\}}, \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1 \mathbf{r}_j^\top)]_2\}_{j \in [L]\setminus[\ell], i \in [L]\setminus\{j\}} \end{pmatrix},$$

$$\mathsf{pk}_i = \begin{cases} \big([\overbrace{\mathbf{A}\mathbf{U}_i}^{\mathbf{T}_i}, \overbrace{\widehat{\mathbf{R}}_i \mathbf{U}_i}^{\mathbf{Q}_i}]_1, \{\overbrace{[\mathbf{U}_i \mathbf{B}_2 r_j]_2}^{\mathbf{h}_{i,j}}\}_{j \in [\ell-1]\setminus\{i\}}, \overbrace{[\mathbf{U}_i \mathbf{d}_\ell^\top]_2}^{\mathbf{h}_{i,\ell}}, \{\overbrace{[\mathbf{U}_i \mathbf{B}_1 \mathbf{r}_j^\top]_2}^{\mathbf{h}_{i,j}}\}_{j \in [L]\setminus[i,\ell]}, \widetilde{\pi}_i\big) & \text{if } i \neq \ell \\ \big([\underbrace{\mathbf{A}\mathbf{U}_\ell}_{\mathbf{T}_\ell}, \underbrace{\widehat{\mathbf{R}}_i \mathbf{U}_\ell}_{\mathbf{Q}_\ell}]_1, \{\underbrace{[\mathbf{U}_\ell \mathbf{B}_2 r_j]_2}_{\mathbf{h}_{\ell,j}}\}_{j \in [\ell-1]}, \qquad \{\underbrace{[\mathbf{U}_\ell \mathbf{B}_1 \mathbf{r}_j^\top]_2}_{\mathbf{h}_{\ell,j}}\}_{j \in [L]\setminus[\ell]}, \widetilde{\pi}_\ell\big) & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_1^* = (\mathbf{e}_1 \widetilde{\mathbf{R}}_\ell^{-1} \mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1})) + \sum_{i \in [L]\setminus\{\ell\}} (\mathbf{e}_1 \widetilde{\mathbf{R}}_i^{-1} \mathbf{Q}_i^* + \mathbf{c}\mathbf{W}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{2k+1}))$$

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell + \sum_{i \in [L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_i$$

where $\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_3^\top)$. We define $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$ and $\mathbf{c}\mathbf{c}^\perp = 1$. With the orthogonality of dual basis, for all $\mathbf{v}^{(3)} \in \mathsf{span}((\mathbf{B}_3^\|)^\top)$, we have:

$$\mathbf{v}^{(3)}\mathbf{B}_1 = \mathbf{0}, \quad \mathbf{v}^{(3)}\mathbf{B}_2 = \mathbf{0}.$$

We will proof $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$ by considering two cases: (1) pk_ℓ^* is honest; (2) pk_ℓ^* is corrupted or maliciously generated by the adversary.

Useful Lemma. Before we proceed, we prepare the following lemma.

Lemma 2. *For all basis $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B}_2 \leftarrow \mathbb{Z}_p^{(2k+1)}$, $\mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, and its dual basis $\mathbf{B}_1^\|, \mathbf{B}_2^\|, \mathbf{B}_3^\|$. For all $\mathbf{d}^\perp \in \mathsf{span}((\mathbf{B}_3^\|)^\top)$ such that $\mathbf{d}^\perp\mathbf{B}_1 = \mathbf{0}$ and $\mathbf{d}^\perp\mathbf{B}_2 = 0$. For any adversary $\mathcal{A}$, there exist an adversary $\mathcal{B}_2$ such that*

$$\begin{aligned}
&\big| \Pr[\mathcal{A}(\mathbf{A}, \mathbf{c}, [\mathbf{R}]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\perp, \mathbf{AU}, \mathbf{cU}, [\mathbf{RU}]_1, \qquad\qquad \mathbf{UB}_1, \mathbf{UB}_2) = 1] - \\
&\quad \Pr[\mathcal{A}(\mathbf{A}, \mathbf{c}, [\mathbf{R}]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\perp, \mathbf{AU}, \mathbf{cU}, [\mathbf{RU} + \boxed{\mathbf{u}^\top\mathbf{d}^\perp}]_1, \mathbf{UB}_1, \mathbf{UB}_2) = 1] \big| \\
\leq\ & 2 \cdot \mathsf{Adv}_{\mathcal{B}_2}^{MDDH} + \mathsf{negl}(\lambda)
\end{aligned}$$

where $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$, $\mathbf{R} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}$, $\mathbf{U} \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)}$ and $\mathbf{u} \leftarrow \mathbb{Z}_p^{1\times(2k+2)}$.

Honest Case. In this case, we have $\mathsf{pk}_\ell^* = ([\mathbf{T}_\ell^*, \mathbf{Q}_\ell^*]_1, \{[\mathbf{h}_{\ell,j}^*]_2\}_{j\in[L]\setminus\{\ell\}}, \pi_\ell^*) \in D_\ell \setminus C_\ell$. Namely, we know $\mathbf{U}_\ell^*$ (such that $\mathbf{T}_\ell^* = \mathbf{AU}_\ell^*$ and $\mathbf{Q}_\ell^* = \widehat{\mathbf{R}}_\ell\mathbf{U}_\ell^*$) and $\mathbf{U}_\ell^*$ is hidden from the adversary. We can write the dashboxed terms in $\mathbf{c}_1^*$ as follows:

$$\boxed{\mathbf{cU}_\ell^*} + \mathbf{cW}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1})$$

and replace $\widehat{\mathbf{R}}_\ell$ in crs with a random $\mathbf{R}_\ell$ as in G_1.

Let's use $\mathbf{x}_{b'}^*$ to denote the challenge message, which is $\mathbf{x}_b^*$ in $\mathsf{G}_{7,\ell-1,1}$ and $\mathbf{x}_0^*$ in $\mathsf{G}_{7,\ell-1,2}$ respectively. We have the following argument holds for both $b' = b$ (in $\mathsf{G}_{7,\ell-1,1}$) and $b' = 0$ (in $\mathsf{G}_{7,\ell-1,2}$), which proves that $\mathsf{G}_{7,\ell-1,1} \approx_c \mathsf{G}_{7,\ell-1,2}$ in the honest case:

$$\begin{aligned}
& \mathbf{A}, \mathbf{c}^\perp, [\mathbf{R}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{AW}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) && /\!/\mathsf{crs},\ \mathsf{pk}_\ell \\
& \mathbf{c}, \mathbf{cU}_\ell^* + \mathbf{cW}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}), \mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)} + \mathbf{cW}_\ell && /\!/\mathsf{ct}^* \\
& \mathbf{AU}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^*]_1, \mathbf{U}_\ell^*\mathbf{B}_1, \mathbf{U}_\ell^*\mathbf{B}_2 && /\!/\mathsf{pk}_\ell^* \\
\approx_c\ & \mathbf{A}, \mathbf{c}^\perp, [\mathbf{R}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{AW}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{cU}_\ell^* + \mathbf{cW}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}), \mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)} + \mathbf{cW}_\ell \\
& \mathbf{AU}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \boxed{\widehat{\mathbf{u}}^\top\mathbf{v}^{(3)}}]_1, \mathbf{U}_\ell^*\mathbf{B}_1, \mathbf{U}_\ell^*\mathbf{B}_2 \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, [\mathbf{R}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{AW}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{cU}_\ell^* + \mathbf{cW}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}) + \boxed{u_\ell\mathbf{v}^{(3)} + \mathbf{w}_\ell(\mathbf{y}_\ell^*)^\top\mathbf{v}^{(3)}}, \mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)} + \mathbf{cW}_\ell + \boxed{\mathbf{w}_\ell \otimes \mathbf{v}^{(3)}} \\
& \mathbf{AU}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \boxed{\mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{v}^{(3)}} + \widehat{\mathbf{u}}^\top\mathbf{v}^{(3)}]_1, \mathbf{U}_\ell^*\mathbf{B}_1, \mathbf{U}_\ell^*\mathbf{B}_2 \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, [\mathbf{R}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{AW}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{cU}_\ell^* + \mathbf{cW}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}) + u_\ell\mathbf{v}^{(3)} + \mathbf{w}_\ell(\mathbf{y}_\ell^*)^\top\mathbf{v}^{(3)}, \cancel{\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)}} + \mathbf{cW}_\ell + \mathbf{w}_\ell \otimes \mathbf{v}^{(3)} \\
& \mathbf{AU}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{v}^{(3)} + \widehat{\mathbf{u}}^\top\mathbf{v}^{(3)}]_1, \mathbf{U}_\ell^*\mathbf{B}_1, \mathbf{U}_\ell^*\mathbf{B}_2
\end{aligned}$$

where $\widehat{\mathbf{u}} \leftarrow \mathbb{Z}_p^{1\times(2k+2)}$ and $u_\ell \leftarrow \mathbb{Z}_p$, $\mathbf{w}_\ell \leftarrow \mathbb{Z}_p^{1\times n}$. We justify each step as below: The first $\approx_c$ uses Lemma 2 with $\mathbf{R} = \mathbf{R}_\ell$, $\mathbf{U} = \mathbf{U}_\ell^*$, $\mathbf{u} = \widehat{\mathbf{u}}$ and $\mathbf{d}^\perp = \mathbf{v}^{(3)}$. The second $\approx_s$ uses change of variables

$$\mathbf{W}_\ell \mapsto \mathbf{W}_\ell + \mathbf{c}^\perp(\mathbf{w}_\ell \otimes \mathbf{v}^{(3)}) \quad \text{and} \quad \mathbf{U}_\ell^* \mapsto \mathbf{U}_\ell^* + \mathbf{c}^\perp u_\ell \mathbf{v}^{(3)}$$

The last $\approx_s$ follows from the fact that $\widehat{\mathbf{u}}$ hides $\mathbf{R}\mathbf{c}^\perp u_\ell$, this implies that u_ℓ can hide $\mathbf{w}_\ell(\mathbf{y}_\ell^*)^\top$ in $\mathbf{c}_1^*$, and $\mathbf{w}_\ell$ hides $\mathbf{x}_{b'}^*$ in $\mathbf{c}_2^*$.

Corrupted & Malicious Case. In this case, we have $\mathsf{pk}_\ell^* = ([\mathbf{T}_\ell^*, \mathbf{Q}_\ell^*]_1, \{[\mathbf{h}_{\ell,j}^{*\top}]_2\}_{j\in[L]\setminus\{\ell\}}, \pi_\ell^*) \in C_\ell \cup \overline{D}_\ell$. It is required that $\mathbf{x}_0^*(\mathbf{y}_i^*)^\top = \mathbf{x}_1^*(\mathbf{y}_i^*)^\top$. We prove $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$ in this case using the following argument for all $b \in \{0,1\}$:

$$\begin{aligned}
&\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) && //\mathsf{crs}\\
&\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}), \mathbf{x}_b^* \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell && //\mathsf{ct}^* \text{ in } \mathsf{G}_{7,\ell-1,1}\\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2)\\
&\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}) - \boxed{\mathbf{x}_b^*(\mathbf{y}_\ell^*)^\top\mathbf{v}^{(3)}}, \cancel{\mathbf{x}_b^* \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_\ell\\
=\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2)\\
&\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}) - \boxed{\mathbf{x}_0^*(\mathbf{y}_\ell^*)^\top\mathbf{v}^{(3)}}, \mathbf{c}\mathbf{W}_\ell\\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) && //\mathsf{crs}\\
&\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}) + \cancel{\mathbf{x}_0^*(\mathbf{y}_\ell^*)^\top\mathbf{v}^{(3)}}, \boxed{\mathbf{x}_0^* \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_\ell && //\mathsf{ct}^* \text{ in } \mathsf{G}_{7,\ell-1,2}
\end{aligned}$$

We justify each step as follows: the first $\approx_s$ uses the change of variables

$$\mathbf{W}_\ell \mapsto \mathbf{W}_\ell - \mathbf{c}^\perp(\mathbf{x}_b^* \otimes \mathbf{v}^{(3)})$$

The second = uses the fact that $\mathbf{x}_b^*(\mathbf{y}_\ell^*)^\top = \mathbf{x}_0^*(\mathbf{y}_\ell^*)^\top$ in this case. The last $\approx_s$ uses the change of variables

$$\mathbf{W}_\ell \mapsto \mathbf{W}_\ell + \mathbf{c}^\perp(\mathbf{x}_0^* \otimes \mathbf{v}^{(3)})$$

4 Simulation-based Security for Reg-FE

In this section, we define the notion of simulation-based security in the context of Reg-FE. We give both the adaptive variant and the very selective variant followed by several remarks.

4.1 Adaptive SIM-security for Reg-FE

Definition. For all stateful PPT adversary $\mathcal{A}$, there exists simulator $(\widetilde{\mathsf{Setup}}, \widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Enc}})$ such that:

$$\left[\begin{array}{l}
\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F);\\
x^* \leftarrow \mathcal{A}^{\mathsf{ORegCK}(\cdot,\cdot),\mathsf{ORegHK}(\cdot),\mathsf{OCorHK}(\cdot)}(\mathsf{crs});\\
\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*);\\
\mathcal{A}^{\mathsf{OCorHK}(\cdot)}(\mathsf{ct}^*), \alpha \leftarrow \mathcal{A}(\mathsf{ct}^*)
\end{array}\right] \approx_c \left[\begin{array}{l}
(\widetilde{\mathsf{crs}}, \mathsf{td}) \leftarrow \widetilde{\mathsf{Setup}}(1^\lambda, 1^L, F);\\
x^* \leftarrow \mathcal{A}^{\mathsf{ORegCK}(\cdot,\cdot),\mathsf{ORegHK}(\cdot),\mathsf{OCorHK}(\cdot)}(\widetilde{\mathsf{crs}});\\
\widetilde{\mathsf{ct}}^* \leftarrow \widetilde{\mathsf{Enc}}((\mathsf{pk}_1^*, \ldots, \mathsf{pk}_{L'}^*); \mathsf{td})\\
\mathcal{A}^{\mathsf{OCorHK}(\cdot)}(\widetilde{\mathsf{ct}}^*), \alpha \leftarrow \mathcal{A}(\widetilde{\mathsf{ct}}^*)
\end{array}\right]$$

Here, in the real world (on the left-hand side), the oracles work as follows with initial setting $\mathsf{aux} = \perp$, $\mathsf{mpk} = \perp$, $\mathcal{H} = \emptyset$, $C = \emptyset$ and $\mathcal{D}$ being a dictionary with $\mathcal{D}[\mathsf{pk}] = \emptyset$ for all possible pk:

- $\mathsf{ORegCK}(\mathsf{pk}, f)$: run $(\mathsf{mpk}', \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f)$, update $\mathsf{mpk} = \mathsf{mpk}'$, $\mathsf{aux} = \mathsf{aux}'$, $\mathcal{D}[\mathsf{pk}] = \mathcal{D}[\mathsf{pk}] \cup \{f\}$, append pk to $\mathcal{C}$ and return $(\mathsf{mpk}, \mathsf{aux})$;
- $\mathsf{ORegHK}(f)$: run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$ and $(\mathsf{mpk}', \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f)$, update $\mathsf{mpk} = \mathsf{mpk}'$, $\mathsf{aux} = \mathsf{aux}'$, $\mathcal{D}[\mathsf{pk}] = \mathcal{D}[\mathsf{pk}] \cup \{f\}$, append $(\mathsf{pk}, \mathsf{sk})$ to $\mathcal{H}$ and return $(|\mathcal{H}|, \mathsf{mpk}, \mathsf{aux}, \mathsf{pk})$;
- $\mathsf{OCorHK}(i)$: let $\mathcal{H}[i] = (\mathsf{pk}, \mathsf{sk})$, append pk to $\mathcal{C}$ and return sk;

with the following restrictions:

- for query i to OCorHK, it holds that $\mathcal{H}[i] \neq \perp$.

In the ideal world (on the right-hand side), the oracles are analogous to that in the real world; except that they use $\widetilde{\mathsf{crs}}$ simulated by $\widetilde{\mathsf{Setup}}$ instead of crs, and ORegHK invokes $\widetilde{\mathsf{Gen}}$ instead of Gen.

4.2 Very Selective SIM-security for Reg-FE

In the very selective setting, the adversary claims the challenge, challenge functions, and the types of challenge public keys at the beginning. The specific definition is as follows:

Definition. For all stateful PPT adversary $\mathcal{A}$, there exists simulator $(\widetilde{\mathsf{Setup}}, \widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Enc}})$ such that:

$$\begin{bmatrix} L, L', x^*, \{f_i^*\}_{i\in[L']}, CK, HK, CH \leftarrow \mathcal{A}(1^\lambda); \\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F); \\ \mathcal{A}^{\mathsf{O}(\mathsf{crs}, \{f_i^*\}_{i\in[L']}, CK, HK, CH, \cdot, \cdot)}(\mathsf{crs}); \\ \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*), \alpha \leftarrow \mathcal{A}(\mathsf{ct}^*) \end{bmatrix} \approx_c \begin{bmatrix} L, L', x^*, \{f_i^*\}_{i\in[L']}, CK, HK, CH \leftarrow \mathcal{A}(1^\lambda); \\ (\widetilde{\mathsf{crs}}, \mathsf{td}) \leftarrow \widetilde{\mathsf{Setup}}(1^\lambda, 1^L, F; \{f_i^*\}_{i\in CK\cup HK}, \{f_i^*(x^*)\}_{i\in CK\cup CH}); \\ \mathcal{A}^{\mathsf{O}(\widetilde{\mathsf{crs}}, \{f_i^*\}_{i\in[L']}, CK, HK, CH, \cdot, \cdot)}(\widetilde{\mathsf{crs}}); \\ \widetilde{\mathsf{ct}}^* \leftarrow \widetilde{\mathsf{Enc}}((\mathsf{pk}_1^*, \ldots, \mathsf{pk}_{L'}^*); \mathsf{td}), \alpha \leftarrow \mathcal{A}(\widetilde{\mathsf{ct}}^*) \end{bmatrix}$$

where $CK, HK \subseteq [L']$, $CK \cup HK = [L']$ for some $L' \leq L$, $CH \subseteq HK$ and $CK \cap HK = \emptyset$, and O works as follows with a counter $\ell = 1$ and the same set of auxiliary data structure as in the definition of IND-security: on input (i, pk_i^*), return $\perp$ when $i \neq \ell$, otherwise set $\ell = \ell + 1$ and do

- when $i \in CK$, return $\mathsf{ORegCK}(\mathsf{pk}_i^*, f_i^*)$;
- when $i \in HK$, return $\mathsf{ORegHK}(f_i^*)$; furthermore, if $i \in CH$, return $\mathsf{OCorHK}(|HK \cap [i]|)$.

Here ORegCK and ORegHK invoke Reg in both cases: in the real world (on the left-hand side), they use crs generated by Setup and ORegHK invokes Gen; in the ideal world (on the right-hand side), they use $\widetilde{\mathsf{crs}}$ simulated by $\widetilde{\mathsf{Setup}}$ and ORegHK invokes $\widetilde{\mathsf{Gen}}$.

Remark. We give several remarks on our formalization.

- We do *not* require simulated version of Reg and Upd since both of them are public.
- We allow the adversary to choose pk_i^* at any point, only functions f_i and *types* of public keys (i.e., honest, malicious, honest but corrupted) are chosen "very selectively".
- The set CH does *not* give the timing to invoke OCorHK. One could let the adversary make an explicit query; however we call the oracle automatically just after invocation of ORegHK. This gives a simple but not weaker model in the very selective setting. In the definition, $|HK \cap [i]|$ is the first item of the response of $\mathsf{ORegHK}(f_i^*)$.
- In very selective SIM-security, there is no need to consider post-challenge queries. This relies on the fact that the adversary should state the set CH at the beginning, so the pre-challenge and post-challenge corruption queries are equivalent in the very-selective SIM-security setting.

5 Compact Reg-FE from Multi-instance Slotted Reg-FE

In this section, we define *multi-instance* slotted Reg-FE and give a transformation to get *compact* Reg-FE. Our transformation works well for both IND and SIM security.

5.1 Multi-instance Slotted Reg-FE

Algorithms. A *multi-instance slotted Reg-FE* for the functionality $F = \{f : Y \to Z\}$, consists of eight efficient algorithms:

- $\mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, F) \to \mathsf{crs}$: It takes as input security parameter 1^λ, maximum instance index 1^m, maximum slot indices $1^{L_1}, \ldots, 1^{L_m}$ of every instances and functionalities F, outputs common reference string crs.
- $\mathsf{Gen}(\mathsf{crs}, q, i) \to (\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i})$: It takes as input crs, instance index $q \in [m]$, and slot index $i \in [L_q]$, outputs key pair $(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i})$.
- $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i}) \to 0/1$: It takes as input crs, $q \in [m]$, $i \in [L_q]$ and $\mathsf{pk}_{q,i}$, outputs a bit.
- $\mathsf{Agg}_+(\mathsf{crs}) \to \mathsf{mpk}_+$: It takes as input crs, outputs the shared parts of master public key mpk_+.
- $\mathsf{Agg}(\mathsf{crs}, q, (\mathsf{pk}_{q,i}, f_{q,i})_{i\in[L_q]}) \to (\mathsf{mpk}_q, (\mathsf{hsk}_{q,j})_{j\in[L_q]})$: It takes as input crs, $q \in [m]$, a series of $\mathsf{pk}_{q,i}$ with $f_{q,i} \in F$ for all $i \in [L_q]$, outputs master public key mpk_q and helper keys $\mathsf{hsk}_{q,j}$ for instance q.
- $\mathsf{Enc}_+(\mathsf{mpk}_+, x) \to \mathsf{ct}_+$: It takes mpk_+ and message $x \in X$ as input, outputs ciphertext ct_+.
- $\mathsf{Enc}(\mathsf{mpk}_q) \to \mathsf{ct}_q$: It takes as input mpk_q (for some $q \in [m]$), outputs ciphertext ct_q.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, (\mathsf{ct}_+, \mathsf{ct}_q)) \to z/\perp$: It takes as input sk, hsk, ct_+ and ct_q (for some $q \in [m]$), outputs $z \in \mathbb{Z}_p$ or a special symbol $\perp$.

We require that Agg_+, Agg and Dec are deterministic, and Enc_+ and Enc share the random coin space Coin. And we allow the case that some instance q^* to be empty, namely $\mathsf{Agg}(\mathsf{crs}, q^*, \cdot)$ takes $(\mathsf{pk}_{q^*,i}, f_{q^*,i}) = (\perp, \perp)$ for all $i \in [L_{q^*}]$ as input, and return $\mathsf{mpk}_{q^*} = \perp$ and $\mathsf{hsk}_{q^*,j} = \perp$ for all $j \in [L_{q^*}]$, and we allow Enc to take $\mathsf{mpk}_{q^*} = \perp$ as input and output $\mathsf{ct}_{q^*} = \perp$.

Completeness. For all $\lambda, m, L_1, \ldots, L_m \in \mathbb{N}$, all F, all $q \in [m]$ and $i \in [L_q]$, we have

$$\Pr\left[\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i}) = 1 \,\middle|\, \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, F);\ (\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q, i)\right] = 1.$$

Correctness. For all $\lambda, m, L_1, \ldots, L_m \in \mathbb{N}$, all F, all $q^* \in [m]$ and $i^* \in [L_{q^*}]$; all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, F)$, all $(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q^*, i^*)$; all $\{\mathsf{pk}_{q^*,i}\}_{i\in[L_{q^*}]\setminus\{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, q^*, i, \mathsf{pk}_{q^*,i}) = 1$; for all $x \in X$, $f_{q^*,i} \in F$, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{q^*,i^*}, \mathsf{hsk}_{q^*,i^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*})) = f_{q^*,i^*}(x) \,\middle|\, \begin{array}{l} \mathsf{mpk}_+ \leftarrow \mathsf{Agg}_+(\mathsf{crs}); \\ (\mathsf{mpk}_{q^*}, (\mathsf{hsk}_{q^*,j})_{j\in[L_{q^*}]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, q^*, (\mathsf{pk}_{q^*,i}, f_{q^*,i})_{i\in[L_{q^*}]}) \\ s \leftarrow \mathsf{Coin};\ \mathsf{ct}_+ \leftarrow \mathsf{Enc}_+(\mathsf{mpk}_+, x; s);\ \mathsf{ct}_{q^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}_{q^*}; s) \end{array}\right] = 1.$$

Ciphertext Compactness. For all $\lambda, m, L_1, \ldots, L_m \in \mathbb{N}$, all F, all $q \in [m]$ and $i \in [L_q]$; all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, F)$, all $(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q, i)$ such that $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i}) = 1$; for all $x \in X$, $f_{q,i} \in F$; all $\mathsf{mpk}_+ \leftarrow \mathsf{Agg}_+(\mathsf{crs})$, all $(\mathsf{mpk}_q, (\mathsf{hsk}_{q,j})_{j\in[L_q]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, q, (\mathsf{pk}_{q,i}, f_{q,i})_{i\in[L_q]})$, all $\mathsf{ct}_+ \leftarrow \mathsf{Enc}_+(\mathsf{mpk}_+, x)$, all $\mathsf{ct}_q \leftarrow \mathsf{Enc}(\mathsf{mpk}_q)$, we have

$$|\mathsf{ct}_+| = |x| + \mathsf{poly}(\lambda) \quad \text{and} \quad |\mathsf{ct}_q| = \mathsf{poly}(\lambda).$$

IND-security in Joint Challenge Setting. For all stateful PPT adversary $\mathcal{A}$, the following advantage function is negligible in λ:

$$\mathsf{IndAdv}^{\text{miReg-FE}}_{\mathcal{A}}(\lambda) = \Pr\left[b = b' \left| \begin{array}{l} m, L_1, \ldots, L_m \leftarrow \mathcal{A}(1^\lambda);\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, F) \\ (\mathsf{pk}^*_{q,i}, f^*_{q,i})_{q\in[m], i\in[L_m]}, x^*_0, x^*_1 \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot,\cdot),\mathsf{OCor}(\cdot,\cdot,\cdot)}(\mathsf{crs}) \\ \mathsf{mpk}_+ \leftarrow \mathsf{Agg}_+(\mathsf{crs}) \\ (\mathsf{mpk}_q, \ldots) \leftarrow \mathsf{Agg}(\mathsf{crs}, q, (\mathsf{pk}^*_{q,1}, f^*_{q,1}), \ldots, (\mathsf{pk}^*_{q,L_q}, f^*_{q,L_q})),\ \forall q \in [m] \\ b \leftarrow \{0,1\},\ s \leftarrow \mathsf{Coin},\ \mathsf{ct}^*_+ \leftarrow \mathsf{Enc}_+(\mathsf{mpk}_+, x^*_b; s),\ \mathsf{ct}^*_q \leftarrow \mathsf{Enc}(\mathsf{mpk}_q; s), \forall q \in [m] \\ b' \leftarrow \mathcal{A}(\mathsf{ct}^*_+, \mathsf{ct}^*_1, \ldots, \mathsf{ct}^*_q) \end{array} \right.\right] - 1/2$$

where the oracles work as follows with the initial setting $C = \emptyset$ and $\mathcal{D}_{q,i} = \emptyset$ for all $q \in [m], i \in [L_q]$:

- $\mathsf{OGen}(q, i)$: run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q, i)$, set $\mathcal{D}_{q,i}[\mathsf{pk}] = \mathsf{sk}$ and return pk.
- $\mathsf{OCor}(q, i, \mathsf{pk})$: return $\mathcal{D}_{q,i}[\mathsf{pk}]$ and update $C = C \cup \{(q, i, \mathsf{pk})\}$.

and for all $q \in [m], i \in [L_q]$, we require that

$$\mathcal{D}_{q,i}[\mathsf{pk}^*_{q,i}] = \perp \implies \mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}^*_{q,i}) = 1 \quad \text{and} \quad (q, i, \mathsf{pk}^*_{q,i}) \in C \vee \mathcal{D}_{q,i}[\mathsf{pk}^*_{q,i}] = \perp \implies f^*_{q,i}(x^*_0) = f^*_{q,i}(x^*_1).$$

In IND-security model, we allow the case that some instance q^* to be empty, namely $\mathcal{A}$ submit the challenge pairs $(\mathsf{pk}^*_{q^*,i}, f^*_{q^*,i}) = (\perp, \perp)$ for all $i \in [L_{q^*}]$, and challenge ciphertext $\mathsf{ct}^*_{q^*} = \perp$. We use $\mathsf{IndAdv}^{\text{miReg-FE}}_{\mathcal{A}}(\lambda)$ to denote the advantage function. Analogous to sReg-ABE [HLWW23], there is no need to give mpk and $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ to $\mathcal{A}$ explicitly and to consider post-challenge queries.

Very Selective SIM-security in Joint Challenge Setting. For all stateful PPT adversary $\mathcal{A}$, there exists simulator $(\widetilde{\mathsf{Setup}}, \widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Enc}}_+, \widetilde{\mathsf{Enc}})$ such that the following distributions are indistinguishable

$$\left[\begin{array}{l} x^*, \{L_q, \mathcal{M}^*_q, C^*_q, \{f^*_{q,i}\}_{i\in[L_q]}\}_{q\in[m]} \leftarrow \mathcal{A}(1^\lambda); \\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, F); \\ \{\mathsf{pk}^*_{q,i}\}_{q\in[m], i\in[L_q]} \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot,\cdot),\mathsf{OCor}(\cdot,\cdot,\cdot)}(\mathsf{crs}); \\ \mathsf{mpk}_+ \leftarrow \mathsf{Agg}_+(\mathsf{crs}),\ (\mathsf{mpk}_q, \ldots) \leftarrow \mathsf{Agg}(\mathsf{crs}, q, (\mathsf{pk}^*_{q,1}, f^*_{q,1}), \ldots, (\mathsf{pk}^*_{q,L_q}, f^*_{q,L_q})),\ \forall q \in [m] \\ s \leftarrow \mathsf{Coin},\ \mathsf{ct}^*_+ \leftarrow \mathsf{Enc}_+(\mathsf{mpk}_+, x^*; s),\ \mathsf{ct}^*_q \leftarrow \mathsf{Enc}(\mathsf{mpk}_q; s), \forall q \in [m] \\ \alpha \leftarrow \mathcal{A}(\mathsf{ct}^*_+, \mathsf{ct}^*_1, \ldots, \mathsf{ct}^*_q) \end{array} \right]$$

$$\approx_c \left[\begin{array}{l} x^*, \{L_q, \mathcal{M}^*_q, C^*_q, \{f^*_{q,i}\}_{i\in[L_q]}\}_{q\in[m]} \leftarrow \mathcal{A}(1^\lambda); \\ (\widetilde{\mathsf{crs}}, \mathsf{td}) \leftarrow \widetilde{\mathsf{Setup}}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, F; \{\{f^*_{q,i}\}_{i\in[L_q]}, \{f^*_{q,i}(x^*)\}_{i\in\mathcal{M}^*_q\cup C^*_q}\}_{q\in[m]}); \\ \{\mathsf{pk}^*_{q,i}\}_{q\in[m], i\in[L_q]} \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot,\cdot),\mathsf{OCor}(\cdot,\cdot,\cdot)}(\widetilde{\mathsf{crs}}); \\ \widetilde{\mathsf{ct}}^*_+ \leftarrow \widetilde{\mathsf{Enc}}_+(\mathsf{td}),\ \widetilde{\mathsf{ct}}^*_q \leftarrow \widetilde{\mathsf{Enc}}((\mathsf{pk}^*_{q,1}, \ldots, \mathsf{pk}^*_{q,L_q}); \mathsf{td}), \forall q \in [m] \\ \alpha \leftarrow \mathcal{A}(\widetilde{\mathsf{ct}}^*_+, \widetilde{\mathsf{ct}}^*_1, \ldots, \widetilde{\mathsf{ct}}^*_q) \end{array} \right]$$

where $\mathcal{M}^*_q, C^*_q \subseteq [L_q]$ for $q \in [m]$ denote the sets of malicious and corrupted slots in instance q, and the oracles work as follows with initial setting $C_q = \emptyset$ and $\mathcal{D}_{q,i} = \emptyset$ for all $i \in [L_q]$ and $q \in [m]$:

- $\mathsf{OGen}(q, i)$: run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q, i)$, set $\mathcal{D}_{q,i}[\mathsf{pk}] = \mathsf{sk}$ and return pk.
- $\mathsf{OCor}(q, i, \mathsf{pk})$: return $\mathcal{D}_{q,i}[\mathsf{pk}]$ and update $C_q = C_q \cup \{(i, \mathsf{pk})\}$.

In the ideal world, OGen invokes $\widetilde{\mathsf{Gen}}$ instead of Gen; and the following restrictions: for all $q \in [m]$,

$$\begin{aligned} i \in \mathcal{M}^*_q &\implies \mathcal{D}_{q,i}[\mathsf{pk}^*_{q,i}] = \perp \wedge \mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}^*_{q,i}) = 1 \\ i \in C^*_q &\implies (i, \mathsf{pk}^*_{q,i}) \in C_q \\ i \in [L_q] \setminus (\mathcal{M}^*_q \cup C^*_q) &\implies \mathcal{D}_{q,i}[\mathsf{pk}^*_{q,i}] \neq \perp \wedge (i, \mathsf{pk}^*_{q,i}) \notin C_q \end{aligned}$$

In SIM-security model, we allow the case that some instance q^* to be empty, namely $\mathcal{A}$ gives $\mathcal{M}^*_{q^*}, C^*_{q^*} = \emptyset$, and the challenge functions $f^*_{q^*,i} = \perp$, challenge public keys $\mathsf{pk}^*_{q^*,i} = \perp$ for all $i \in [L_{q^*}]$, and we have challenge ciphertext $\mathsf{ct}^*_{q^*} = \perp$ (resp. $\widetilde{\mathsf{ct}}^*_{q^*} = \perp$) in real (resp. ideal) world. We use $\mathsf{Adv}^{\text{miReg-FE}}_{\mathcal{A}}$ to denote the advantage function. Similarly, there is no need to give $\mathsf{mpk}_+, \{\mathsf{mpk}_q, \mathsf{hsk}_{q,1}, \dots \mathsf{hsk}_{q,L_q}\}_{q\in[m]}$ to $\mathcal{A}$ explicitly in real game (or explicitly in simulation game) and consider post-challenge queries.

5.2 Compact Reg-FE

We give a generic transformation from multi-instance slotted Reg-FE to Reg-FE (c.f. Section 2.2) with compact ciphertext. Here we will apply a conceptual change to multi-instance slotted Reg-FE: we will always add an instance with index 0 and count slot index from 0 instead of 1. Namely, Setup that takes 1^m and $1^{L_0}, 1^{L_1}, \dots, 1^{L_m}$ as input will give us $m+1$ instances indexed by $0, 1, \dots, m$; for each $q \in [0, m]$, the q-th instance has L_q slots indexed by $0, 1, \dots, L_q - 1$. Clearly, this does not change correctness and security. Note that in the remaining subsections of Section 5, we use two difference indices i and j, respectively referring to the global range from 0 to $L-1$ and instances' internal ranges from 0 to $L_q - 1$ (for each $q \in [0, m]$).

Auxiliary Data Structure. We will count users from 0 and set $\mathsf{aux} = (\mathsf{ctr}, \mathcal{D}_1, \mathcal{D}_2, \mathsf{mpk})$:

- Counter $\mathsf{ctr} \in [0, L]$ is the current number of registered users in the system, or the index of the next user.
- $\mathcal{D}_1$ is a dictionary that maps $q \in [0, m]$ and $j \in [0, 2^q - 1]$ to public key $\mathsf{pk}_{q,j}$ and function $f_{q,j}$.
- $\mathcal{D}_2$ is a dictionary that maps $q \in [0, m]$ and $i \in [0, L-1]$ to a helper key hsk.
- mpk will be in the form $(\mathsf{ctr}, \mathsf{mpk}_+, \mathsf{mpk}_0, \dots, \mathsf{mpk}_m)$.

Initially, we set $\mathsf{ctr} = 0$, $\mathcal{D}_1 = \emptyset$, $\mathcal{D}_2 = \emptyset$, $\mathsf{mpk} = (0, \perp, \dots, \perp)$; the system is overloaded when $\mathsf{ctr} = L$.

Generic Transformation. Our Reg-FE with compact ciphertext works as follows with multi-instance slotted Reg-FE $(\mathsf{mSetup}, \mathsf{mGen}, \mathsf{mVer}, \mathsf{mAgg}_+, \mathsf{mAgg}, \mathsf{mEnc}_+, \mathsf{mEnc}, \mathsf{mDec})$:

- $\mathsf{Setup}(1^\lambda, 1^L, F)$: Compute $m = \log L$, output
$$\mathsf{crs} \leftarrow \mathsf{mSetup}(1^\lambda, 1^m, 1^{2^0}, \dots, 1^{2^m}, F)$$
- $\mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$: Parse $\mathsf{aux} = (\mathsf{ctr}, \mathcal{D}_1, \mathcal{D}_2, \mathsf{mpk})$ and run
$$(\mathsf{pk}^{\mathsf{ctr}}_q, \mathsf{sk}^{\mathsf{ctr}}_q) \leftarrow \mathsf{mGen}(\mathsf{crs}, q, \mathsf{ctr} \bmod 2^q), \quad \forall q \in [0, m]$$
  Output
$$\mathsf{pk} = (\mathsf{ctr}, \mathsf{pk}^{\mathsf{ctr}}_0, \dots, \mathsf{pk}^{\mathsf{ctr}}_m) \quad \text{and} \quad \mathsf{sk} = (\mathsf{ctr}, \mathsf{sk}^{\mathsf{ctr}}_0, \dots, \mathsf{pk}^{\mathsf{ctr}}_m).$$
- $\mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f)$: Parse $\mathsf{aux} = (\mathsf{ctr}, \mathcal{D}_1, \mathcal{D}_2, \mathsf{mpk})$ where $\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_+, \mathsf{mpk}_0, \dots, \mathsf{mpk}_m)$ and $\mathsf{pk} = (\mathsf{ctr}_{\mathsf{pk}}, \mathsf{pk}^{\mathsf{ctr}}_0, \dots, \mathsf{pk}^{\mathsf{ctr}}_m)$. Abort if the following does not hold:
$$\mathsf{ctr} = \mathsf{ctr}_{\mathsf{pk}} \quad \text{and} \quad \mathsf{mVer}(\mathsf{crs}, q, \mathsf{ctr} \bmod 2^q, \mathsf{pk}^{\mathsf{ctr}}_q) = 1, \quad \forall q \in [0, m]$$
  For each $q \in [0, m]$, update $\mathcal{D}_1[q, \mathsf{ctr} \bmod 2^q] = (\mathsf{pk}^{\mathsf{ctr}}_q, f)$; furthermore, if $\mathsf{ctr} + 1 = 0 \bmod 2^q$, run
$$(\mathsf{mpk}'_q, \mathsf{hsk}'_{q,0}, \dots, \mathsf{hsk}'_{q,2^q-1}) \leftarrow \mathsf{mAgg}(\mathsf{crs}, q, \mathcal{D}_1[q, 0], \dots, \mathcal{D}_1[q, 2^q - 1])$$
  and update $\mathcal{D}_2[q, \mathsf{ctr} - 2^q + 1 + j] = \mathsf{hsk}'_{q,j}$ for all $j \in [0, 2^q - 1]$; otherwise, set $\mathsf{mpk}'_q = \mathsf{mpk}_q$. Output
$$\mathsf{mpk} = (\mathsf{ctr} + 1, \mathsf{mpk}_+, \mathsf{mpk}'_0, \dots, \mathsf{mpk}'_m) \quad \text{and} \quad \mathsf{aux} = (\mathsf{ctr} + 1, \mathcal{D}_1, \mathcal{D}_2, \mathsf{mpk}).$$

– $\mathsf{Enc}(\mathsf{mpk}, x)$: Parse $\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_+, \mathsf{mpk}_0, \ldots, \mathsf{mpk}_m)$. Sample $s \leftarrow \mathsf{Coin}$ and compute

$$\mathsf{ct}_+ \leftarrow \mathsf{mEnc}_+(\mathsf{mpk}_+, x; s) \quad \text{and} \quad \mathsf{ct}_q \leftarrow \mathsf{mEnc}(\mathsf{mpk}_q; s), \quad \forall q \in [0, m]$$

Output

$$\mathsf{ct} = (\mathsf{ctr}, \mathsf{ct}_+, \mathsf{ct}_0, \ldots, \mathsf{ct}_m).$$

– $\mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk})$: Parse $\mathsf{aux} = (\mathsf{ctr}, \mathcal{D}_1, \mathcal{D}_2, \mathsf{mpk})$ and $\mathsf{pk} = (\mathsf{ctr}_{\mathsf{pk}}, \mathsf{pk}_0^{\mathsf{ctr}}, \ldots, \mathsf{pk}_m^{\mathsf{ctr}})$. Abort if $\mathsf{ctr}_{\mathsf{pk}} \geq \mathsf{ctr}$; otherwise, output

$$\mathsf{hsk} = (\mathcal{D}_2[0, \mathsf{ctr}_{\mathsf{pk}} + 1], \ldots, \mathcal{D}_2[m, \mathsf{ctr}_{\mathsf{pk}} + 1]).$$

– $\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, \mathsf{ct})$: Parse $\mathsf{sk} = (\mathsf{ctr}_{\mathsf{sk}}, \mathsf{sk}_0, \ldots, \mathsf{sk}_m)$, $\mathsf{hsk} = (\mathsf{hsk}_0, \ldots, \mathsf{hsk}_m)$ and $\mathsf{ct} = (\mathsf{ctr}_{\mathsf{ct}}, \mathsf{ct}_+, \mathsf{ct}_0, \ldots, \mathsf{ct}_m)$. Abort if $\mathsf{ctr}_{\mathsf{sk}} \geq \mathsf{ctr}_{\mathsf{ct}}$. Find the largest $q^* \in [0, m]$ such that $2^{q^*} \leq (\mathsf{ctr}_{\mathsf{ct}} \oplus \mathsf{ctr}_{\mathsf{sk}})$ Output

$$z = \begin{cases} \mathtt{getupd} & \text{if } \mathsf{hsk}_{q^*} = \perp \\ \mathsf{mDec}(\mathsf{sk}_{q^*}, \mathsf{hsk}_{q^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*})) & \text{otherwise} \end{cases}$$

Correctness, Update Efficiency and Compactness. Our generic transformation employs "power-of-two" technique in [HLWW23]. The analysis in [HLWW23] can be adapted to show the correctness, update efficiency and compactness of ours. We omit the details and mention that

$$|\mathsf{crs}| = O(L^2 \cdot |x|^2) \cdot \mathsf{poly}(\lambda), \quad |\mathsf{hsk}| = O(|x| \cdot \log L) \cdot \mathsf{poly}(\lambda), \quad |\mathsf{mpk}| = O(|x| + \log L) \cdot \mathsf{poly}(\lambda).$$

Furthermore, by the ciphertext compactness of multi-instance slotted Reg-FE, our transformation achieves:

$$|\mathsf{ct}| = |\mathsf{ct}_+| + |\mathsf{ct}_0| + \ldots + |\mathsf{ct}_{\log L}| = O(|x|) + O(\log L) \cdot \mathsf{poly}(\lambda)$$

IND-security. Analogous to [HLWW23], we have the following theorem. The proof is analogous to [HLWW23], except that we don't need to build a series of hybrid experiments and reduce the security to $m+1$ parallel instances one-by-one, we can directly reduce the security to the multi-instance slotted scheme at once time.

Theorem 2. *Assume* $(\mathsf{mSetup}, \mathsf{mGen}, \mathsf{mVer}, \mathsf{mAgg}_+, \mathsf{mAgg}, \mathsf{mEnc}_+, \mathsf{mEnc}, \mathsf{mDec})$ *is a multi-instance slotted Reg-FE with adaptive (resp. selective) IND-security, our Reg-FE scheme generates via above transformation achieves adaptive (resp. selective) IND-security.*

5.3 SIM-security

We have the following theorem. Given multi-instance slotted Reg-QFE with very selective SIM-security under MDDH assumption, our Reg-QFE scheme uses prime-order bilinear group and the very selective SIM-security can be reduced to Bi-MDDH assumption.

Theorem 3. *Assume* $(\mathsf{mSetup}, \mathsf{mGen}, \mathsf{mVer}, \mathsf{mAgg}_+, \mathsf{mAgg}, \mathsf{mEnc}_+, \mathsf{mEnc}, \mathsf{mDec})$ *is a multi-instance slotted Reg-FE, with completeness, correctness and very selective SIM-security, our Reg-FE scheme generate via above transformation achieves the very selective SIM-security, under bi-MDDH assumption.*

Let $(\widetilde{\mathsf{mSetup}}, \widetilde{\mathsf{mGen}}, \widetilde{\mathsf{mEnc}_+}, \widetilde{\mathsf{mEnc}})$ be the simulator of multi-instance slotted Reg-FE, to build the simulator of the Reg-FE, we need the following auxiliary data structure and deterministic algorithm which simulate the slot filling procedure in Reg, to determine the slots' filling state after all users have registered.

Auxiliary Data Structure.

- D, R are dictionaries that map $q \in [0, m]$ and $j \in [0, 2^q - 1]$ to index i.
- $\mathcal{M}_q^*, C_q^*$ are the same sets as the definition of SIM-security of multi-instance slotted Reg-FE.

Initially, we set $D = \emptyset, R = \emptyset$ and $\mathcal{M}_q^*, C_q^* = \emptyset$ for all $q \in [0, m]$.

Auxiliary Algorithm. Assume the Reg-FE mostly supports $L = 2^m$ users, and $CK, HK \subseteq [0, L' - 1]$, $CH \cup HK = [0, L' - 1]$ for some $L' \leq L$, the algorithms works as follow:

- $\mathsf{Fillslot}(CK, HK, CH)$: For all $i \in [0, L' - 1]$: for each $q \in [0, m]$, update $D[q, i \bmod 2^q] = i$; furthermore, if $i + 1 = 0 \bmod 2^q$, update

$$R[q, j] = D[q, j] \quad \forall j \in [0, 2^q - 1].$$

  Output R.

Simulator. The simulator of our multi-instance Reg-QFE is as follows:

- $\widetilde{\mathsf{Setup}}(1^\lambda, 1^L, F; \{f_i\}_{i \in CK \cup HK}, \{\mu_i\}_{i \in CK \cup CH})$: Let $m = \log L$, run $R \leftarrow \mathsf{Fillslot}(CK, HK, CH)$. For all $q \in [0, m]$:
  - If $2^q \leq L'$, for all $j \in [0, 2^q - 1]$: fetch $R[q, j] = i$ and output $f_{q,j} = f_i$, furthermore, if $i \in CK \cup CH$, output $\mu_{q,j} = \mu_i$ and update

$$\begin{cases} \mathcal{M}_q^* = \mathcal{M}_q^* \cup \{j\} & \text{if } i \in CK \\ C_q^* = C_q^* \cup \{j\} & \text{if } i \in CH \end{cases}$$

  - If $2^q > L'$, for all $j \in [0, 2^q - 1]$, output $f_{q,j} = \perp$.

  And run

$$(\widetilde{\mathsf{crs}}, \mathsf{mtd}) \leftarrow \mathsf{m}\widetilde{\mathsf{Setup}}(1^\lambda, 1^m, 1^{2^0}, \ldots, 1^{2^m}, F, \{\{f_{q,j}\}_{j \in [0, 2^q - 1]}, \{\mu_{q,j}\}_{j \in \mathcal{M}_q \cup C_q}\}_{q \in [0, m]})$$

  Output $\widetilde{\mathsf{crs}}$, and set trapdoor as $\mathsf{td} = \mathsf{mtd} \cup R$.
- $\widetilde{\mathsf{Gen}}(\widetilde{\mathsf{crs}}, \mathsf{aux}; \mathsf{td})$: Parse $\mathsf{aux} = (\mathsf{ctr}, \mathcal{D}_1, \mathcal{D}_2, \mathsf{mpk})$ and run

$$(\widetilde{\mathsf{pk}}_q, \widetilde{\mathsf{sk}}_q) \leftarrow \mathsf{m}\widetilde{\mathsf{Gen}}(\widetilde{\mathsf{crs}}, q, \mathsf{ctr} \bmod 2^q; \mathsf{td}), \quad \forall q \in [0, m]$$

  Output

$$\mathsf{pk} = (\mathsf{ctr}, \widetilde{\mathsf{pk}}_0, \ldots, \widetilde{\mathsf{pk}}_m) \quad \text{and} \quad \mathsf{sk} = (\mathsf{ctr}, \widetilde{\mathsf{sk}}_0, \ldots, \widetilde{\mathsf{pk}}_m).$$

- $\widetilde{\mathsf{Enc}}((\mathsf{pk}_1, \ldots, \mathsf{pk}_{L'}); \mathsf{td})$: Parse $\mathsf{td} = (\mathsf{mtd}, R)$ and $\mathsf{pk}_i = (i, \mathsf{pk}_0^i, \ldots, \mathsf{pk}_m^i)$. For all $q \in [0, m]$:
  - If $2^q \leq L'$, for all $j \in [0, 2^q - 1]$: fetch $R[q, j] = i$ and set $\mathsf{pk}_{q,j} = \mathsf{pk}_q^i$
  - If $2^q > L'$, for all $j \in [0, 2^q - 1]$, set $\mathsf{pk}_{q,j} = \perp$.

  Compute

$$\widetilde{\mathsf{ct}}_+ \leftarrow \mathsf{m}\widetilde{\mathsf{Enc}}_+(\mathsf{mtd}) \quad \text{and} \quad \widetilde{\mathsf{ct}}_q \leftarrow \mathsf{m}\widetilde{\mathsf{Enc}}((\mathsf{pk}_{q,0}, \ldots, \mathsf{pk}_{q,2^q-1}); \mathsf{mtd}), \quad \forall q \in [0, m]$$

  Output

$$\widetilde{\mathsf{ct}} = (\mathsf{ctr}, \widetilde{\mathsf{ct}}_+, \widetilde{\mathsf{ct}}_0, \ldots, \widetilde{\mathsf{ct}}_m).$$

The reader can find the sanity check in Appendix D.

5.4 Proof

We prove the following technical lemma this immediately proves Theorem 3.

Lemma 3. *For all adversaries $\mathcal{A}$, there exist adversary $\mathcal{B}$ such that:*

$$\mathsf{Adv}_{\mathcal{A}}^{\textit{Reg-FE}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}}^{\textit{miReg-FE}}(\lambda) + \mathsf{negl}(\lambda)$$

where $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$.

Game Sequence. Suppose that crs is the common reference string. x^* is the challenge, with some $L' \leq L$, $\{f_i^*\}_{i\in[0,L'-1]}$ are challenge functions that chosen at the beginning. CK, HK and CH are the set of register corrupted (malicious) key index, register honest key index and corrupted honest key index such that $CK, HK \subseteq [0, L'-1]$, $CK \cup HK = [0, L'-1]$, $CH \subseteq HK$ and $CK \cap HK = \emptyset$. $\{\mathsf{pk}_i^*\}_{i\in[0,L']}$ are challenge public keys with the form of $\mathsf{pk}_i^* = (i, (\mathsf{pk}_0^i)^*, \ldots, (\mathsf{pk}_m^i)^*)$. Recall that $\mathcal{H}$ record the $(\mathsf{pk}_i^*, \mathsf{sk}_i^*)_{i\in HK}$ that generated in $\mathsf{ORegHK}(\cdot)$.

- G_0: This is the real game, recall that we have
  - crs is in the form of
  $$\mathsf{crs} \leftarrow \mathsf{mSetup}(1^\lambda, 1^m, 1^{2^0}, \ldots, 1^{2^m}, F)$$
  - For each $i \in HK$, each $(\mathsf{pk}_i^*, \mathsf{sk}_i^*) \in \mathcal{H}$ is in the form of
  $$\mathsf{pk}_i^* = (i, (\mathsf{pk}_0^i)^*, \ldots, (\mathsf{pk}_m^i)^*) \quad \text{and} \quad \mathsf{sk}_i^* = (i, (\mathsf{sk}_0^i)^*, \ldots, (\mathsf{sk}_m^i)^*).$$
  where $(\mathsf{pk}_{q,i}^*, \mathsf{sk}_{q,i}^*) \leftarrow \mathsf{mGen}(\mathsf{crs}, q, i \bmod 2^q)$, for all $q \in [0, m]$.
  - ct^* for x^* is in the form of
  $$\mathsf{ct}^* = (L, \mathsf{ct}_+^*, \mathsf{ct}_0^*, \ldots, \mathsf{ct}_m^*)$$
  where $\mathsf{ct}_+^* \leftarrow \mathsf{mEnc}_+(\mathsf{mpk}_+, x^*; s)$, and $\mathsf{ct}_q^* \leftarrow \mathsf{mEnc}(\mathsf{mpk}_q; s)$ for all $q \in [0, m]$, with the same random coin $s \leftarrow \mathsf{Coin}$.
- G_1: Identical to G_0 except that we replace $(\mathsf{mSetup}, \mathsf{mGen}, \mathsf{mEnc}_+, \mathsf{mEnc})$ with $(\widetilde{\mathsf{mSetup}}, \widetilde{\mathsf{mGen}}, \widetilde{\mathsf{mEnc}}_+, \widetilde{\mathsf{mEnc}})$. In particular:
  - crs is replaced with $\boxed{\widetilde{\mathsf{crs}}}$, where
  $$(\widetilde{\mathsf{crs}}, \mathsf{mtd}) \leftarrow \boxed{\widetilde{\mathsf{mSetup}}}(1^\lambda, 1^m, 1^{2^0}, \ldots, 1^{2^m}, F, \{\{f_{q,j}^*\}_{j\in[0,2^q-1]}, \{f_{q,j}^*(x^*)\}_{j\in\mathcal{M}_q^*\cup C_q^*}\}_{q\in[0,m]})$$
  where
  $$f_{q,j}^* = \begin{cases} f_{R[q,j]}^* & \text{if } 2^q \leq L' \\ \perp & \text{if } 2^q > L' \end{cases}$$
  with $R \leftarrow \mathsf{Fillslot}(CK, HK, CH)$.
  - For each $i \in HK$, each $(\mathsf{pk}_i^*, \mathsf{sk}_i^*) \in \mathcal{H}$ is in the form of
  $$\mathsf{pk}_i^* = (i, \boxed{(\widetilde{\mathsf{pk}}_0^i)^*, \ldots, (\widetilde{\mathsf{pk}}_m^i)^*}) \quad \text{and} \quad \mathsf{sk}_i^* = (i, \boxed{(\widetilde{\mathsf{sk}}_0^i)^*, \ldots, (\widetilde{\mathsf{sk}}_m^i)^*}).$$
  where $((\widetilde{\mathsf{pk}}_q^i)^*, (\widetilde{\mathsf{sk}}_q^i)^*) \leftarrow \boxed{\widetilde{\mathsf{mGen}}}(\mathsf{crs}, q, i \bmod 2^q; \mathsf{td})$, for all $q \in [0, m]$.
  - ct^* for x^* is in the form of
  $$\mathsf{ct}^* = (L', \boxed{\widetilde{\mathsf{ct}}_+^*, \widetilde{\mathsf{ct}}_0^*, \ldots, \widetilde{\mathsf{ct}}_m^*})$$
  where $\widetilde{\mathsf{ct}}_+^* \leftarrow \boxed{\widetilde{\mathsf{mEnc}}_+}(\mathsf{td})$, and $\widetilde{\mathsf{ct}}_q^* \leftarrow \boxed{\widetilde{\mathsf{mEnc}}}((\mathsf{pk}_{q,0}^*, \ldots, \mathsf{pk}_{q,2^q-1}^*); \mathsf{td})$ for all $q \in [0, m]$. With
  $$\mathsf{pk}_{q,j}^* = \begin{cases} (\mathsf{pk}_q^{R[q,j]})^* & \text{if } 2^q \leq L' \\ \perp & \text{if } 2^q > L' \end{cases}$$

We reduce the security to multi-instance slotted Reg-FE, where the instances $q^* \in \{q : 2^q > L'\}$ are empty: we have $f^*_{q^*,j}, \mathsf{pk}^*_{q^*,j} = \perp$ for all $j \in [0, 2^{q^*} - 1]$, and $\mathcal{M}^*_{q^*}, C^*_{q^*} = \emptyset$. Observe that the game G_1 can be simulated using the simulator by setting $\mu_i = f^*_i(x^*)$

6 Pre-Constrained Slotted Reg-IPFE

In this section, we introduce the notion of pre-constrained slotted Reg-IPFE; the definition for general functionality is deferred to Appendix A. We present our pairing-based construction with very selective SIM-security in Section 6.1. We explain how this implies (standard, without pre-constrain) slotted Reg-IPFE with very selective SIM-security in Section 6.4 and how this derives (standard, without pre-constrain) slotted Reg-IPFE with selective IND-security in Section 6.5.

Functionality and Definition. A *Pre-constrained* Slotted Reg-IPFE is a generalized slotted Reg-FE for linear functionality:

$$F = \{\mathbf{f} : \mathbf{x} \to \mathbf{x}\mathbf{f}^\top\}$$

where $\mathbf{x}, \mathbf{f} \in \mathbb{Z}_p^{1\times n}$. The generalization in multi-instance version is in the following four aspects:

- Algorithm: Setup takes as input security parameter 1^λ, maximum instance index 1^m, maximum slot indices $1^{L_1}, \ldots, 1^{L_m}$ of every instances, function parameter $1^{n_1}, 1^{n_2}$ and pre-constrained matrix $\mathbf{M} \in \mathbb{Z}_p^{n_1\times n_2}$, outputs common reference string crs.
- Correctness: for all $\lambda, m, L_1, \ldots, L_m, n_1, n_2 \in \mathbb{N}$, all $q^* \in [m]$ and $i^* \in [L_{q^*}]$; all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2}, \mathbf{M})$, all $(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q^*, i^*)$; all $\{\mathsf{pk}_{q^*,i}\}_{i\in[L_{q^*}]\setminus\{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, q^*, i, \mathsf{pk}_{q^*,i}) = 1$; for all $\mathbf{x} \in \mathbb{Z}_p^{1\times n_1}$, $\mathbf{f}_{q^*,i} \in \mathbb{Z}_p^{1\times n_2}$, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{q^*,i^*}, \mathsf{hsk}_{q^*,i^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*})) = \mathbf{x}\mathbf{M}\mathbf{f}^\top_{q^*,i^*} \;\middle|\; \begin{array}{l} \mathsf{mpk}_+ \leftarrow \mathsf{Agg}_+(\mathsf{crs}); \\ (\mathsf{mpk}_{q^*}, (\mathsf{hsk}_{q^*,j})_{j\in[L_{q^*}]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, q^*, (\mathsf{pk}_{q^*,i}, \mathbf{f}_{q^*,i})_{i\in[L_{q^*}]}) \\ s \leftarrow \mathsf{Coin};\ \mathsf{ct}_+ \leftarrow \mathsf{Enc}_+(\mathsf{mpk}_+, \mathbf{x}; s);\ \mathsf{ct}_{q^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}_{q^*}; s) \end{array}\right] = 1.$$

- IND-security: We let the adversary to choose $\mathbf{M}$ at the beginning and require that $\mathbf{x}^*_0\mathbf{M}(\mathbf{f}^*_{q,i})^\top = \mathbf{x}^*_1\mathbf{M}(\mathbf{f}^*_{q,i})^\top$ for the case "$(q, i, \mathsf{pk}^*_{q,i}) \in C \vee \mathcal{D}_{q,i}[\mathsf{pk}^*_{q,i}] = \perp$".
- SIM-security: We let the adversary to choose $\mathbf{M}$ at the beginning and give $\mathbf{M}$ and $\{\mathbf{x}^*\mathbf{M}(\mathbf{f}^*_{q,i})\}_{i\in\mathcal{M}^*_q\cup C^*_q}$ to $\widetilde{\mathsf{Setup}}$.

It is straightforward to verify that setting $n_1 = n_2 = n$ and $\mathbf{M} = \mathbf{I}_n$ yields standard slotted Reg-IPFE defined above.

Group-based Simulator. We also require the existence of the group-based simulator $\widetilde{\mathsf{Setup}}_{\mathbb{G}}$. For all $\lambda, m, n_1, n_2 \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $\mathcal{M}^*_q, C^*_q \subseteq [L_q]$, all $\mathbf{M} \in \mathbb{Z}_p^{n_1\times n_2}$, all $\mathbf{f}_{q,1}, \ldots, \mathbf{f}_{q,L_q} \in \mathbb{Z}_p^{1\times n_2}$ and $\mu_{q,i} \in \mathbb{Z}_p$, there exist a group-based algorithm $\widetilde{\mathsf{Setup}}_g$ such that

$$\begin{aligned} &\widetilde{\mathsf{Setup}}_{\mathbb{G}}(1^\lambda, 1^m, 1^{n_1}, 1^{n_2}, [\mathbf{M}]_1, [\mathbf{M}]_2; \{1^{L_q}, \{\mathbf{f}_{q,i}\}_{i\in[L_q]}, \{[\mu_{q,i}]_1, [\mu_{q,i}]_2\}_{i\in\mathcal{M}^*_q\cup C^*_q}\}_{q\in[m]}) \\ \equiv\ &\widetilde{\mathsf{Setup}}(1^\lambda, 1^m, 1^{n_1}, 1^{n_2}, \mathbf{M}; \{1^{L_q}, \{\mathbf{f}_{q,i}\}_{i\in[L_q]}, \{\mu_{q,i}\}_{i\in\mathcal{M}^*_q\cup C^*_q}\}_{q\in[m]}) \end{aligned}$$

For simplicity, for the group-based simulator, we do not distinguish the notation of $\widetilde{\mathsf{Setup}}_{\mathbb{G}}$ and $\widetilde{\mathsf{Setup}}$.

6.1 Scheme

Assuming a QA-NIZK $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ for linear space over bilinear groups, see Section 2.4; a Bi-PKE $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ with linear decryption over bilinear groups, see Section 2.5. Assuming that $|\mathsf{ict}| = |\mathsf{isk}| = n$, our multi-instance slotted PReg-IPFE scheme, with a shared pre-constrained $\mathbf{M} \in \mathbb{Z}_p^{n_1 \times n_2}$ works as follows in the prime-order bilinear group:

- $\mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2}, \mathbf{M})$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$, $([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mathsf{isk}) \leftarrow \mathsf{Gen}_1(1^\lambda)$. Sample shared parts:
$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k \times (2k+1)}, \ \mathbf{W} \leftarrow \mathbb{Z}_p^{(2k+1) \times (n_1 + n)}.$$
For each instance $q \in [m]$, sample $\mathbf{B}_q \leftarrow \mathbb{Z}_p^{(k+1) \times k}$, and for all $i \in [L_q]$, do following operations:
  - Run $([\mathsf{ict}_{q,i}]_1, [\mathsf{ict}_{q,i}]_2) \leftarrow \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0)$, for $s \in \{1, 2\}$, set
$$[\mathbf{M}_{q,i}]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}_{q,i}^\top \end{bmatrix}_s \in \mathbb{G}_s^{(n_1+n) \times (n_2+1)}.$$
  - Sample
$$\mathbf{W}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1) \times (k+1)(n_1+n)}, \ \mathbf{R}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+2) \times (2k+1)}, \ \mathbf{r}_{q,i} \leftarrow \mathbb{Z}_p^{1 \times k}.$$
  - Run $(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_{q,i}]_1)$, where $\mathbf{A}_{q,i} = \binom{\mathbf{A}}{\mathbf{R}_{q,i}} \in \mathbb{Z}_p^{(3k+2) \times (2k+1)}$.

  Output[9]
$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \mathbf{AW}]_1, \\ \left\{ \begin{array}{l} \{\mathsf{crs}_{q,i}, [\mathbf{R}_{q,i}, \mathbf{AW}_{q,i}(\mathbf{M}_{q,i} \otimes \mathbf{I}_{k+1}), \mathbf{AW}_{q,i}]_1\}_{i \in [L_q]} \\ \{[\mathbf{M}_{q,j}, \mathbf{B}_q \mathbf{r}_{q,j}^\top, \mathbf{W}_{q,j}(\mathbf{M}_{q,j} \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top) + \mathbf{WM}_{q,j}]_2\}_{j \in [L_q]} \\ \{[\mathbf{W}_{q,i}(\mathbf{M}_{q,i} \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top)]_2\}_{j \in [L_q], i \in [L_q] \setminus \{j\}} \end{array} \right\}_{q \in [m]} \end{array} \right).$$
- $\mathsf{Gen}(\mathsf{crs}, q, i)$: Sample $\mathbf{U}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1) \times (k+1)}$. Define $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}} = \binom{\mathbf{AU}_{q,i}}{\mathbf{R}_{q,i}\mathbf{U}_{q,i}} = \mathbf{A}_{q,i}\mathbf{U}_{q,i} \in \mathbb{Z}_p^{(3k+2) \times (2k+1)}$ and run
$$\pi_{q,i} \leftarrow \mathsf{LPrv}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \mathbf{U}_{q,i}).$$
Fetch $\{[\mathbf{B}_q \mathbf{r}_{q,j}^\top]_2\}_{j \in [L_q] \setminus \{i\}}$ from crs and output
$$\mathsf{pk}_{q,i} = \big([\underbrace{\mathbf{AU}_{q,i}}_{\mathbf{T}_{q,i}}, \underbrace{\mathbf{R}_{q,i}\mathbf{U}_{q,i}}_{\mathbf{Q}_{q,i}}]_1, \{[\underbrace{\mathbf{U}_{q,i}\mathbf{B}_q \mathbf{r}_{q,j}^\top}_{\mathbf{h}_{q,i,j}}]_2\}_{j \in [L_q] \setminus \{i\}}, \pi_{q,i}\big) \quad \text{and} \quad \mathsf{sk}_{q,i} = \mathbf{U}_{q,i}.$$
- $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i})$: Parse $\mathsf{pk}_{q,i} = \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j \in [L_q] \setminus \{i\}}, \pi_{q,i}\big)$. Write $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}}$ and check
$$\mathsf{LVer}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \pi_{q,i}) \stackrel{?}{=} 1.$$
For each $j \in [L_q] \setminus \{i\}$, check
$$e([\mathbf{A}]_1, [\mathbf{h}_{q,i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_{q,i}]_1, [\mathbf{B}_q \mathbf{r}_{q,j}^\top]_2).$$
If all these checks pass, output 1; otherwise, output 0.
- $\mathsf{Agg}_+(\mathsf{crs})$: Output:
$$\mathsf{mpk}_+ = ([\mathbf{A}, \mathbf{AW}]_1).$$

[9] Note that we employ i as the index for $\mathbf{W}_q$'s and $\mathbf{M}_q$'s while j is the index for $\mathbf{r}_q$'s; both of them range from 1 to L_q. One exception is the terms with $\mathbf{W}_q$, which is conceptually $\mathbf{W}_{q,i}(\mathbf{M}_{q,i} \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top)$ with $i = j$. Note that we do not use $\mathsf{td}_{q,1}, \ldots, \mathsf{td}_{q,L_q}$ and isk in the actual scheme.

– $\mathsf{Agg}(\mathsf{crs}, q, (\mathsf{pk}_{q,i}, \mathbf{f}_{q,i})_{i\in[L_q]})$: If q is an empty instance, on input $(\mathsf{pk}_{q,i}, \mathbf{f}_{q,i}) = (\perp, \perp)$ for all $i \in [L_q]$, abort and return $\mathsf{mpk}_q = \perp$, $\mathsf{hsk}_{q,j} = \perp$ for all $j \in [L_q]$. For all $i \in [L_q]$, parse $\mathsf{pk}_{q,i} = \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_{q,i}\big)$, and set $\overline{\mathbf{f}}_{q,i} = (\mathbf{f}_{q,i}\|1) \in \mathbb{Z}_p^{1\times(n_2+1)}$. Output:

$$\mathsf{mpk}_q = \left[\sum_{i\in[L_q]} (\mathbf{T}_{q,i} + \mathbf{A}\mathbf{W}_{q,i}(\mathbf{M}_{q,i}\overline{\mathbf{f}}_{q,i}^{\top} \otimes \mathbf{I}_{k+1}))\right]_1,$$

and for all $j \in [L_q]$

$$\mathsf{hsk}_{q,j} = \Bigg(\Bigg[\underbrace{\mathbf{B}_q\mathbf{r}_{q,j}^{\top}}_{\mathbf{k}_0^{\top}}, \underbrace{\sum_{i\in[L_q]\setminus\{j\}} (\mathbf{h}_{q,i,j} + \mathbf{W}_{q,i}(\mathbf{M}_{q,i}\overline{\mathbf{f}}_{q,i}^{\top} \otimes \mathbf{B}_q\mathbf{r}_{q,j}^{\top}))}_{\mathbf{k}_1^{\top}}, \underbrace{\mathbf{W}_{q,j}(\mathbf{M}_{q,j}\overline{\mathbf{f}}_{q,j}^{\top} \otimes \mathbf{B}_q\mathbf{r}_{q,j}^{\top}) + \mathbf{W}\mathbf{M}_{q,j}\overline{\mathbf{f}}_{q,j}^{\top}}_{\mathbf{k}_2^{\top}}, \underbrace{\mathbf{M}_{q,j}\overline{\mathbf{f}}_{q,j}^{\top}}_{\mathbf{k}_3^{\top}}\Bigg]_2\Bigg).$$

– $\mathsf{Enc}_+(\mathsf{mpk}_+, \mathbf{x})$: Set $\overline{\mathbf{x}} = (\mathbf{x}\|\mathbf{0}_n) \in \mathbb{Z}_p^{1\times(n_1+n)}$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$. Output:

$$\mathsf{ct}_+ = ([\underbrace{\mathbf{s}\mathbf{A}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{W} + \overline{\mathbf{x}}}_{\mathbf{c}_{+,1}}]_1).$$

– $\mathsf{Enc}(\mathsf{mpk}_q)$: Abort and return $\perp$ if $\mathsf{mpk}_q = \perp$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$, output

$$\mathsf{ct}_q = \underbrace{\left[\sum_{i\in[L_q]} (\mathbf{s}\mathbf{T}_{q,i} + \mathbf{s}\mathbf{A}\mathbf{W}_{q,i}(\mathbf{M}_{q,i}\overline{\mathbf{f}}_{q,i}^{\top} \otimes \mathbf{I}_{k+1}))\right]_1}_{\mathbf{c}_q}.$$

– $\mathsf{Dec}(\mathsf{sk}_{q^*,i^*}, \mathsf{hsk}_{q^*,i^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*}))$: Abort and return $\perp$ if $\mathsf{ct}_{q^*} = \perp$. Parse

$$\mathsf{sk}_{q^*,i^*} = \mathbf{U}_{q^*,i^*}, \quad \mathsf{hsk}_{q^*,i^*} = ([\mathbf{k}_0^{\top}, \mathbf{k}_1^{\top}, \mathbf{k}_2^{\top}, \mathbf{k}_3^{\top}]_2), \quad (\mathsf{ct}_+, \mathsf{ct}_{q^*}) = ([\mathbf{c}_{+,0}, \mathbf{c}_{+,1}, \mathbf{c}_{q^*}]_1).$$

Recover

$$\begin{aligned}
&[z_1]_T = e([\mathbf{c}_{q^*}]_1, [\mathbf{k}_0^{\top}]_2), && [z_2]_T = e([\mathbf{c}_{+,0}]_1, [\mathbf{k}_1^{\top}]_2),\\
&[z_3]_T = e([\mathbf{c}_{+,0}\mathbf{U}_{q^*,i^*}]_1, [\mathbf{k}_0^{\top}]_2), && [z_4]_T = e([\mathbf{c}_{+,0}]_1, [\mathbf{k}_2^{\top}]_2),\\
&[z_5]_T = e([\mathbf{c}_{+,1}]_1, [\mathbf{k}_3^{\top}]_2).
\end{aligned}$$

Compute

$$[z]_T = [z_1 - z_2 - z_3 - z_4 + z_5]_T.$$

Recover z from $[z]_T$ via brute-force DLOG and output z.

Completeness. For all $\lambda, m, n_1, n_2 \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $\mathbf{M} \in \mathbb{Z}_p^{n_1\times n_2}$, all $q \in [m]$ and $i \in [L_q]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^{\lambda}, 1^m, 1^{n_1}, 1^{n_2}, \mathbf{M}, 1^{L_1}, \ldots, 1^{L_m})$, and $(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q, i)$, we have

$$\begin{aligned}
\mathsf{pk}_{q,i} &= \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j\in[L_q]\setminus\{i\}}, \pi_{q,i}\big)\\
&= \big([\mathbf{A}\mathbf{U}_{q,i}, \mathbf{R}_{q,i}\mathbf{U}_{q,i}]_1, \{[\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^{\top}]_2\}_{j\in[L_q]\setminus\{i\}}, \pi_{q,i}\big)
\end{aligned}$$

for some $\mathbf{U}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$ and $\pi_{q,i} \leftarrow \mathsf{LPrv}(\mathsf{crs}_{q,i}, [\mathbf{A}_{q,i}\mathbf{U}_i]_1, \mathbf{U}_i)$ where $(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}) \leftarrow \mathsf{LGen}(1^{\lambda}, \mathbb{G}_1, [\mathbf{A}_{q,i}]_1)$ and $\mathbf{A}_{q,i} = \binom{\mathbf{A}}{\mathbf{R}_{q,i}}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$, $\mathbf{R}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}$. Then

– Write $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}} = \binom{\mathbf{A}\mathbf{U}_{q,i}}{\mathbf{R}_{q,i}\mathbf{U}_{q,i}}$, we have $\mathsf{LVer}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \pi_{q,i}) = 1$ by the perfect completeness of Π_0 (see Section 2.4) and the fact that $\mathbf{F}_{q,i} = \mathbf{A}_{q,i}\mathbf{U}_{q,i}$;
– For each $j \in [L_q] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^{\top}]_2) = e([\mathbf{A}\mathbf{U}_{q,i}]_1, [\mathbf{B}_q\mathbf{r}_{q,j}^{\top}]_2)$ by the definition of bilinear map e (see Section 2.1) and the fact that $\mathbf{A} \cdot \mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^{\top} = \mathbf{A}\mathbf{U}_{q,i} \cdot \mathbf{B}_q\mathbf{r}_{q,j}^{\top}$.

This ensures that $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i}) = 1$ by the specification of Ver and readily proves the completeness.

Correctness. For all $\lambda, m, n_1, n_2 \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $\mathbf{M} \in \mathbb{Z}_p^{n_1 \times n_2}$, all $q^* \in [m]$ and $i^* \in [L_{q^*}]$; all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{n_1}, 1^{n_2}, \mathbf{M}, 1^{L_1}, \ldots, 1^{L_m})$, all $(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q^*, i^*)$; all $\{\mathsf{pk}_{q^*,i}\}_{i \in [L_{q^*}] \setminus \{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, q^*, i, \mathsf{pk}_{q^*,i}) = 1$; all $\mathbf{x} \in \mathbb{Z}_p^{1 \times n_1}$ and $\mathbf{f}_{q^*,i} \in \mathbb{Z}_p^{1 \times n_2}$; for $s \in \{1, 2\}$, we have:

$$\overline{\mathbf{x}} = (\mathbf{x} \| \mathbf{0}_n), \quad \overline{\mathbf{f}}_{q^*,i^*} = (\mathbf{f}_{q^*,i^*} \| 1), \quad [\mathbf{M}_{q^*,i^*}]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}_{q^*,i^*}^\top \end{bmatrix}_s \tag{15}$$

where $[\mathsf{ict}_{q^*,i^*}]_s \in \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0)$ and $([\mathsf{ipk}]_1, [\mathsf{ipk}]_2) \in \mathsf{Gen}_1(1^\lambda)$. And for all $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$, we have

$$\begin{aligned}
\mathsf{sk}_{q^*,i^*} &= \mathbf{U}_{q^*,i^*}, \\
(\mathsf{ct}_+, \mathsf{ct}_{q^*}) &= \left(\left[\underbrace{\mathbf{sA}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{sAW} + \overline{\mathbf{x}}}_{\mathbf{c}_{+,1}}, \underbrace{\sum_{i \in [L_q]} (\mathbf{sT}_{q^*,i} + \mathbf{sAW}_{q^*,i}(\mathbf{M}_{q^*,i}\overline{\mathbf{f}}_{q^*,i}^\top \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_{q^*}} \right]_1 \right) \\
\mathsf{hsk}_{q^*,i^*} &= \Bigg(\Bigg[\underbrace{\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i \in [L_{q^*}] \setminus \{i^*\}} (\mathbf{h}_{q^*,i,i^*} + \mathbf{W}_{q^*,i}(\mathbf{M}_{q^*,i}\overline{\mathbf{f}}_{q^*,i}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top)),}_{\mathbf{k}_1^\top} \\
&\qquad \underbrace{\mathbf{W}_{q^*,i^*}(\mathbf{M}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top) + \mathbf{WM}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top,}_{\mathbf{k}_2^\top}, \underbrace{\mathbf{M}_{q,i^*}\overline{\mathbf{f}}_{q \cdot i^*}^\top}_{\mathbf{k}_3^\top} \Bigg]_2 \Bigg).
\end{aligned}$$

where

$$\mathbf{Ah}_{q^*,i,i^*} = \mathbf{T}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top \quad \forall i \in [L_{q^*}] \setminus \{i^*\} \quad \text{and} \quad \mathbf{AU}_{q^*,i^*} = \mathbf{T}_{q^*,i^*}.$$

Note that here we actually consider $\mathsf{hsk}_{q^*,j}$ for $j = i^*$ and $\mathsf{sk}_{q^*,i}$ for $i = i^*$ and all above equalities are ensured by Ver and Gen. We have

$$\begin{aligned}
z_1 &= \sum_{i \in [L_{q^*}]} (\mathbf{sT}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top + \mathbf{sAW}_{q^*,i}(\mathbf{M}_{q^*,i}\overline{\mathbf{f}}_{q^*,i}^\top \otimes \mathbf{I}_{k+1})\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top) \\
&= \sum_{i \in [L_{q^*}]} (\mathbf{sT}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top + \mathbf{sAW}_{q^*,i}(\mathbf{M}_{q^*,i}\overline{\mathbf{f}}_{q^*,i}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top)) \\
z_2 &= \sum_{i \in [L_{q^*}] \setminus \{i^*\}} (\mathbf{sAh}_{q^*,i,i^*} + \mathbf{sAW}_{q^*,i}(\mathbf{M}_{q^*,i}\overline{\mathbf{f}}_{q^*,i}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top)) \\
z_3 &= \mathbf{sAU}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top \\
z_4 &= \mathbf{sAW}_{q^*,i^*}(\mathbf{M}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top) + \mathbf{sAWM}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top \\
z_5 &= \mathbf{sAWM}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top + \overline{\mathbf{x}}\mathbf{M}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top
\end{aligned} \tag{16}$$

and then

$$\begin{aligned}
z &= z_1 - z_2 - z_3 - z_4 + z_5 \\
&= \mathbf{sT}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top + \mathbf{sAW}_{q^*,i^*}(\mathbf{M}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top) - \mathbf{sAU}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top \\
&\quad -(\mathbf{sAW}_{q^*,i^*}(\mathbf{M}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top) + \mathbf{sAWM}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top) \\
&\quad +(\mathbf{sAWM}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top + \overline{\mathbf{x}}\mathbf{M}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top) && (17) \\
&= \overline{\mathbf{x}}\mathbf{M}_{q^*,i^*}\overline{\mathbf{f}}_{q^*,i^*}^\top && (18) \\
&= (\mathbf{x} \| \mathbf{0}_n) \begin{pmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}_{q^*,i^*}^\top \end{pmatrix} \begin{pmatrix} \mathbf{f}_{q^*,i^*}^\top \\ 1 \end{pmatrix} && (19) \\
&= \mathbf{xMf}_{q^*,i^*}^\top
\end{aligned}$$

Here, equality (16) follows from the property of tensor product: $(\mathbf{a}^\top \otimes \mathbf{I})\mathbf{M} = \mathbf{a}^\top \otimes \mathbf{M}$ for matrices of proper size; equality (17) follows from the fact that $\mathbf{A}\mathbf{h}_{q^*,i,i^*} = \mathbf{T}_i \mathbf{B}_{q^*} \mathbf{r}^\top_{q^*,i^*}$ for all $i \in [L_{q^*}] \setminus \{i^*\}$; equality (18) follows from the fact that $\mathbf{T}_{q^*,i^*} = \mathbf{A}\mathbf{U}_{q^*,i^*}$; equality (19) follows from the fact (15). This proves the correctness.

Compactness and Efficiency. Our multi-instance PReg-IPFE has the following properties:

$$
\begin{aligned}
|\mathsf{crs}| &= O(L^2 \cdot n_1 \cdot n_2) \cdot \mathsf{poly}(\lambda), & |\mathsf{hsk}_{q,j}| &= O(n_1) \cdot \mathsf{poly}(\lambda),\\
|\mathsf{mpk}_+| &= O(n_1)\mathsf{poly}(\lambda), & |\mathsf{mpk}_q| &= \mathsf{poly}(\lambda),\\
|\mathsf{ct}_+| &= O(n_1) + \mathsf{poly}(\lambda), & |\mathsf{ct}_q| &= \mathsf{poly}(\lambda),
\end{aligned}
$$

where $L = L_1 + \cdots + L_m$. Note that the total size of $\{\mathsf{crs}_i\}_{i\in[L]}$ is $L \cdot \mathsf{poly}(\lambda)$ according to the efficiency of the pairing-based QA-NIZK scheme by Kiltz and Wee [KW15] and the fact that the size of language description is $\mathsf{poly}(\lambda)$.

Security. We have the following theorem. Given pairing-based QA-NIZK in [KW15] with unbounded simulation soundness under MDDH assumption, given Bi-PKE with linear decryption and IND-security under bi-MDDH assumption, our multi-instance slotted PReg-IPFE scheme uses prime-order bilinear group and the security can be reduced to bi-MDDH assumption.

Theorem 4. *Assume $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ is a QA-NIZK with perfect completeness, perfect zero-knowledge and unbounded simulation soundness for linear space defined in Section 2.4, assuming $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ is a Bi-PKE with correctness, linear decryption and IND-security defined in Section 2.5, our multi-instance slotted PReg-IPFE scheme achieves the very selective SIM-security as the definition in Section 5.1, under bi-MDDH assumption.*

6.2 Simulator

Recall that we allow some instance q^* to be empty, namely $\mathcal{M}^*_{q^*} = \emptyset, C^*_{q^*} = \emptyset$ and $\mathbf{f}_{q^*,i} = \perp, \mathsf{pk}_{q^*,i} = \perp$ for all $i \in [L_{q^*}]$. Our simulator is as follows:

- $\widetilde{\mathsf{Setup}}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2}, \mathbf{M}; \{\{\mathbf{f}_{q,i}\}_{i\in[L_q]}, \{\mu_{q,i}\}_{i\in\mathcal{M}^*_q \cup C^*_q}\}_{q\in[m]})$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$, $([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mathsf{isk}) \leftarrow \mathsf{Gen}_1(1^\lambda)$. Sample shared parts:

  $$\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)},\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{W} \leftarrow \mathbb{Z}_p^{(2k+1)\times(n_1+n)}.$$

  For each instance $q \in [m]$, sample $\mathbf{B}_q \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, for all $i \in [L_q]$, $s \in \{1, 2\}$, set

  $$[\widetilde{\mathbf{M}}_{q,i}]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}^\top_{n_1} \\ \mathbf{0}_{n\times n_2} & \mathsf{ict}^\top_{q,i} \end{bmatrix}_s \quad \text{where} \quad [\mathsf{ict}_{q,i}]_s \in \begin{cases} \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0) & \text{if } i \in [L_q] \setminus (\mathcal{M}^*_q \cup C^*_q) \\ \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mu_{q,i}) & \text{if } i \in \mathcal{M}^*_q \cup C^*_q \end{cases}$$

  and for all $i \in [L_q]$, do following operations:

  - Sample

    $$\mathbf{W}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)(n_1+n)},\ \widetilde{\mathbf{R}}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)},\ \mathbf{r}_{q,i} \leftarrow \mathbb{Z}_p^{1\times k}.$$

    and compute

    $$\widehat{\mathbf{R}}_{q,i} = \widetilde{\mathbf{R}}_{q,i} \begin{pmatrix} \mathbf{c} \\ \mathbf{I}_{2k+1} \end{pmatrix}.$$

  - Run $(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_{q,i}]_1)$, where $\mathbf{A}_{q,i} = \binom{\mathbf{A}}{\widehat{\mathbf{R}}_{q,i}} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$.

Output

$$\widetilde{\mathsf{crs}} = \left(\begin{array}{l} [\mathbf{A}, \mathbf{AW}]_1, \\ \left\{ \begin{array}{l} \{\mathsf{crs}_{q,i}, [\widehat{\mathbf{R}}_{q,i}, \mathbf{AW}_{q,i}(\widetilde{\mathbf{M}}_{q,i} \otimes \mathbf{I}_{k+1}), \mathbf{AW}_{q,i}]_1\}_{i\in[L_q]} \\ \{[\widetilde{\mathbf{M}}_{q,j}, \mathbf{B}_q\mathbf{r}_{q,j}^\top, \mathbf{W}_{q,j}(\widetilde{\mathbf{M}}_{q,j} \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{W}\widetilde{\mathbf{M}}_{q,j}]_2\}_{j\in[L_q]} \\ \{[\mathbf{W}_{q,i}(\widetilde{\mathbf{M}}_{q,i} \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top)]_2\}_{j\in[L_q], i\in[L_q]\setminus\{j\}} \end{array} \right\}_{q\in[m]} \end{array} \right).$$

And set the trapdoor as

$$\mathsf{td} = \left(\{(\widetilde{\mathbf{R}}_{q,i}, \mathsf{td}_{q,i})_{i\in[L_q]}, \}_{q\in[m]}, [\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mathsf{isk}, \mathbf{c}, \mathbf{W}\right)$$

for all $q \in [m]$, if q is not an empty instance, update

$$\mathsf{td} = \mathsf{td} \cup \left\{ \sum_{i\in[L_q]} \mathbf{cW}_{q,i}(\widetilde{\mathbf{M}}_q\overline{\mathbf{f}}_{q,i}^\top \otimes \mathbf{I}_{k+1}) \right\}$$

where $\overline{\mathbf{f}}_{q,i} = (\mathbf{f}_{q,i}\|1)$.

- $\widetilde{\mathsf{Gen}}(\widetilde{\mathsf{crs}}, q, i; \mathsf{td})$: Fetch $\mathsf{td}_{q,i}$ from td. Sample $\mathbf{U}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$. Define $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}} = \binom{\mathbf{AU}_{q,i}}{\widehat{\mathbf{R}}_{q,i}\mathbf{U}_{q,i}} = \mathbf{A}_{q,i}\mathbf{U}_{q,i} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$ and run

$$\widetilde{\pi}_{q,i} \leftarrow \mathsf{LSim}(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}, [\mathbf{F}_{q,i}]_1).$$

Fetch $\{[\mathbf{B}_q\mathbf{r}_{q,j}^\top]_2\}_{j\in[L_q]\setminus\{i\}}$ from $\widetilde{\mathsf{crs}}$ and output

$$\widetilde{\mathsf{pk}}_{q,i} = ([\underbrace{\mathbf{AU}_{q,i}}_{\mathbf{T}_{q,i}}, \underbrace{\widehat{\mathbf{R}}_{q,i}\mathbf{U}_{q,i}}_{\mathbf{Q}_{q,i}}]_1, \{[\underbrace{\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^\top}_{\mathbf{h}_{q,i,j}}]_2\}_{j\in[L_q]\setminus\{i\}}, \widetilde{\pi}_{q,i}) \quad \text{and} \quad \widetilde{\mathsf{sk}}_{q,i} = \mathbf{U}_{q,i}.$$

- $\widetilde{\mathsf{Enc}}_+(\mathsf{td})$: Fetch $\mathbf{c}, \mathbf{W}$, isk from td, set $\widetilde{\mathbf{x}} = (\mathbf{0}_{n_1}\|\mathsf{isk})$. Output

$$\widetilde{\mathsf{ct}}_+ = ([\underbrace{\mathbf{c}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{cW} + \widetilde{\mathbf{x}}}_{\mathbf{c}_{+,1}}]_1)$$

- $\widetilde{\mathsf{Enc}}((\mathsf{pk}_{q,1}, \ldots, \mathsf{pk}_{q,L_q}); \mathsf{td})$: If q is an empty instance, on input $\mathsf{pk}_{q,i} = \perp$ for all $i \in [L_q]$, abort and return $\widetilde{\mathsf{ct}}_q = \perp$. For all $i \in [L_q]$, parse $\mathsf{pk}_{q,i} = ([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_{q,i})$. Fetch $\{\widetilde{\mathbf{R}}_{q,i}\}_{i\in[L_q]}$ and $\sum_{i\in[L_q]} \mathbf{cW}_{q,i}(\widetilde{\mathbf{M}}_q\overline{\mathbf{f}}_{q,i}^\top \otimes \mathbf{I}_{k+1})$ from td. Output:

$$\widetilde{\mathsf{ct}}_q = \underbrace{\left[\sum_{i\in[L_q]} (\mathbf{e}_1\widetilde{\mathbf{R}}_{q,i}^{-1}\mathbf{Q}_{q,i} + \mathbf{cW}_{q,i}(\widetilde{\mathbf{M}}_q\overline{\mathbf{f}}_{q,i}^\top \otimes \mathbf{I}_{k+1})) \right]_1}_{\mathbf{c}_q}.$$

It is easy to see that with a group-based Bi-PKE (c.f. Section 2.5), our simulator above is a group-based simulator: it can still simulate even if replace $\mathbf{M}, \mu_{q,i}$ with $[\mathbf{M}, \mu_{q,i}]_1$, $[\mathbf{M}, \mu_{q,i}]_2$ in the input of $\widetilde{\mathsf{Setup}}$. The reader can find the sanity check in Appendix D.

6.3 Proof

We prove the following technical lemma this immediately proves Theorem 4.

Lemma 4. *For all adversaries $\mathcal{A}$, there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ such that:*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathit{miPReg\text{-}IPFE}}(\lambda) \leq L \cdot \mathsf{Adv}_{\mathcal{B}_1}^{\mathit{USS}}(\lambda) + L \cdot \mathsf{Adv}_{\mathcal{B}_2}^{\mathit{Bi\text{-}PKE}}(\lambda) + (2L + 2L \cdot Q + 1)\mathsf{Adv}_{\mathcal{B}_3}^{\mathit{MDDH}}(\lambda) + \mathsf{negl}(\lambda)$$

where $L = L_1 + \ldots + L_m$ is the number of slots, Q is the maximum number of queries on a slot made by $\mathcal{A}$ and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3) \approx \mathsf{Time}(\mathcal{A})$.

For simplicity, we prove Lemma 4 in the case of nonempty 1-instance and remove the index q in the following proof. For an empty instance, we only need to remove the terms about ct_1^* and all pk_i^* in the following game sequence, and notice that $\mathcal{M}^*, \mathcal{C}^* = \emptyset$ for empty instance. In the case of m-instance, it only needs to add back index q and apply sub-sequence $\mathsf{G}_{7,\ell-1,0}, \ldots, \mathsf{G}_{7,\ell-1,3}$ to each instance.

Game Sequence. Suppose that crs is the common reference string, $\mathbf{M}$ is the pre-constrained matrix, $\mathbf{x}^*$ is the challenge, $\{\mathsf{pk}_i^*, \mathbf{f}_i^*\}_{i\in[L]}$ are challenge public keys along with challenge functions to be registered, $\mathcal{M}^*, \mathcal{C}^* \subseteq [L]$ are the sets of malicious and corrupted slots. For all $i \in [L]$, define $D_i = \{\mathsf{pk}_i : \mathcal{D}_{1,i}[\mathsf{pk}_i] = \mathsf{sk}_i \neq \perp\}$ be responses to $\mathsf{OGen}(i)$ and $C_i = \{\mathsf{pk}_i : (i, \mathsf{pk}_i) \in \mathcal{C}_1\}$ records public keys in D_i that have been sent to $\mathsf{OCor}(i, \cdot)$. Recall that, for each $i \in [L]$, we require

$$\begin{aligned} i \in \mathcal{M}^* &\implies \mathsf{pk}_i^* \notin D_i \wedge \mathsf{Ver}(\mathsf{crs}, 1, i, \mathsf{pk}_i^*) = 1 \\ i \in \mathcal{C}^* &\implies \mathsf{pk}_i^* \in C_i \\ i \in [L] \setminus (\mathcal{M}^* \cup \mathcal{C}^*) &\implies \mathsf{pk}_i^* \in D_i \wedge \mathsf{pk}_i^* \notin C_i \end{aligned}$$

Note that pk_i serves as a *general* entry in D_i while pk_i^* is the *specific* challenge public for slot i; there can be more than one assignment for pk_i since the adversary can invoke $\mathsf{OGen}(i)$ for many times. We prove the Lemma 4 via dual-system method using the following game sequence.

- G_0: This is the real game, recall that we have
  - crs is in the form:
$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AW}]_1 \\ \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{AW}_i(\mathbf{M}_i \otimes \mathbf{I}_{k+1}), \mathbf{AW}_i]_1\}_{i\in[L]} \\ \{[\mathbf{M}_j, \mathbf{Br}_j^\top, \mathbf{W}_j(\mathbf{M}_j \otimes \mathbf{Br}_j^\top) + \mathbf{WM}_j]_2\}_{j\in[L]} \\ \{[\mathbf{W}_i(\mathbf{M}_i \otimes \mathbf{Br}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$
    where $[\mathbf{M}_i]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n\times n_2} & \mathsf{ict}_i^\top \end{bmatrix}_s$, $[\mathsf{ict}_i]_s \in \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0)$ for $s \in \{1, 2\}$, $([\mathsf{ipk}]_1, [\mathsf{ipk}]_2) \in \mathsf{Gen}_1(1^\lambda)$; and $\mathsf{crs}_i \in \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$, with $\mathbf{A}_i = \begin{pmatrix} \mathbf{A} \\ \mathbf{R}_i \end{pmatrix}$.
  - For each $i \in [L]$, each $\mathsf{pk}_i \in D_i$ is in the form
$$\mathsf{pk}_i = ([\underbrace{\mathbf{AU}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{R}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{[\underbrace{\mathbf{U}_i\mathbf{Br}_j^\top}_{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i)$$
    where $\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i)$, $\mathbf{F}_i = \binom{\mathbf{AU}_i}{\mathbf{RU}_i}$, and $\mathbf{U}_i$ is the corresponding sk_i.
  - For all $i \in [L]$, pk_i^* is in the form:
$$\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{h}_{i,j}^*]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$$
    such that $\mathsf{Ver}(\mathsf{crs}, 1, i, \mathsf{pk}_i^*) = 1$ which means $\mathsf{LVer}\left(\mathsf{crs}_i, \begin{bmatrix} \mathbf{T}_i^* \\ \mathbf{Q}_i^* \end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{Ah}_{i,j}^* = \mathbf{T}_i^*\mathbf{Br}_j^\top$ for each $j \in [L] \setminus \{i\}$.
  - $(\mathsf{ct}_+^*, \mathsf{ct}_1^*)$ for $\mathbf{x}^*$ is in the form:
$$(\mathsf{ct}_+^*, \mathsf{ct}_1^*) = \left(\left[\underbrace{\mathbf{sA}}_{\mathbf{c}_{+,0}^*}, \underbrace{\mathbf{sAW} + \overline{\mathbf{x}}^*}_{\mathbf{c}_{+,1}^*}, \underbrace{\sum_{i\in[L]} (\mathbf{sT}_i + \mathbf{sAW}_i(\mathbf{M}_i(\overline{\mathbf{f}}_i^*)^\top \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_1^*}\right]_1\right).$$

where $\overline{\mathbf{f}}_i^* = (\mathbf{f}_i^* \| 1)$ and $\overline{\mathbf{x}}^* = (\mathbf{x}^* \| \mathbf{0}_n)$.

– G_1: Identical to G_0, except that for all $i \in [L]$ and $s \in \{1,2\}$, we replace $[\mathbf{M}_i]_s$ with

$$[\widetilde{\mathbf{M}}_i]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}_i^\top \end{bmatrix}_s \quad \text{where} \quad [\mathsf{ict}_i]_s \in \begin{cases} \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \boxed{0}) & \text{if } i \in [L] \setminus (\mathcal{M} \cup \mathcal{C}) \\ \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \boxed{\mathbf{x}^* \mathbf{M}(\mathbf{f}_i^*)^\top}) & \text{if } i \in \mathcal{M} \cup \mathcal{C} \end{cases}$$

In particuar, we generate crs as

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AW}]_1 \\ \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{AW}_i(\widetilde{\mathbf{M}}_i \otimes \mathbf{I}_{k+1}), \mathbf{AW}_i]_1\}_{i \in [L]} \\ \{[\widetilde{\mathbf{M}}_j, \mathbf{Br}_j^\top, \mathbf{W}_j(\widetilde{\mathbf{M}}_j \otimes \mathbf{Br}_j^\top) + \mathbf{W}\widetilde{\mathbf{M}}_j]_2\}_{j \in [L]} \\ \{[\mathbf{W}_i(\widetilde{\mathbf{M}}_i \otimes \mathbf{Br}_j^\top)]_2\}_{j \in [L], i \in [L] \setminus \{j\}} \end{pmatrix},$$

and generate challenge ciphertext as

$$(\mathsf{ct}_+^*, \mathsf{ct}_1^*) = \left(\left[\underbrace{\mathbf{sA}}_{\mathbf{c}_{+,0}^*}, \underbrace{\mathbf{sAW} + \overline{\mathbf{x}}^*}_{\mathbf{c}_{+,1}^*}, \underbrace{\sum_{i \in [L]} (\mathbf{sT}_i + \mathbf{sAW}_i(\widetilde{\mathbf{M}}_i(\overline{\mathbf{f}}_i^*)^\top \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_1^*} \right]_1 \right).$$

We have $\mathsf{G}_1 \approx_c \mathsf{G}_0$. This follows from the security of Π_1.

– G_2: Identical to G_1 except that for all $i \in [L]$ and all $\mathsf{pk}_i \in D_i$, we replace π_i with

$$\widetilde{\pi}_i \leftarrow \boxed{\mathsf{LSim}}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{F}_i]_1) \quad \text{where} \quad \mathbf{F}_i = \begin{pmatrix} \mathbf{AU}_i \\ \mathbf{R}_i \mathbf{U}_i \end{pmatrix}.$$

We have $\mathsf{G}_2 \equiv \mathsf{G}_1$. This follows from the perfect zero-knowledge of Π_0.

– G_3: Identical to G_2 except that we sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$ along with $\mathbf{A}$ and replace all $\mathbf{R}_i$ in crs with

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix} \mathbf{sA} \\ \mathbf{I}_{2k+1} \end{pmatrix}, \quad \widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+2) \times (2k+2)}.$$

We have $\mathsf{G}_3 \equiv \mathsf{G}_2$. This follows from the fact that both $\mathbf{R}_i$ (in G_2) and $\widehat{\mathbf{R}}_i$ (in G_3) are truly random since matrix $\binom{\mathbf{sA}}{\mathbf{I}_{2k+1}}$ is full-rank.

– G_4: Identical to G_3 except that we generate the $\mathbf{c}_1^*$ as follows:

$$\mathbf{c}_1^* = \sum_{i \in [L]} (\boxed{\mathbf{e}_1 \widetilde{\mathbf{R}}_i^{-1} \mathbf{Q}_i^*} + \mathbf{sAW}_i(\mathbf{M}_i(\overline{\mathbf{f}}_i^*)^\top \otimes \mathbf{I}_{k+1}))$$

We have $\mathsf{G}_4 \approx_c \mathsf{G}_3$. This follows from stronger unbounded simulation soundness of Π_0 along with the fact that $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i^*], \pi_i^*) = 1$ for all $i \in [L]$ where $\mathbf{F}_i^* = \begin{pmatrix} \mathbf{T}_i^* \\ \mathbf{Q}_i^* \end{pmatrix}$. The details are identical to that in game G_3 of our sReg-IPFE (c.f. Section 3).

– G_5: Identical to G_4 except that we replace all $\mathbf{sA}$ with $\mathbf{c} \leftarrow \mathbb{Z}_p^{1 \times (2k+1)}$; in particular, we generate $\widehat{\mathbf{R}}_i$ as follows:

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix} \boxed{\mathbf{c}} \\ \mathbf{I}_{2k+1} \end{pmatrix}, \quad \widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+2) \times (2k+2)}$$

and generate the challenge ciphertext as follows:

$$(\mathsf{ct}_+^*, \mathsf{ct}_1^*) = \left(\left[\underbrace{\boxed{\mathbf{c}}}_{\mathbf{c}_{+,0}^*}, \underbrace{\boxed{\mathbf{c}}\mathbf{W} + \overline{\mathbf{x}}^*}_{\mathbf{c}_{+,1}^*}, \underbrace{\sum_{i \in [L]} (\mathbf{e}_1 \widetilde{\mathbf{R}}_i^{-1} \mathbf{Q}_i^* + \boxed{\mathbf{c}}\mathbf{W}_i(\widetilde{\mathbf{M}}_i(\overline{\mathbf{f}}_i^*)^\top \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_1^*} \right]_1 \right).$$

We have $\mathsf{G}_5 \approx_c \mathsf{G}_4$. This follows from MDDH assumption which ensures that $([\mathbf{A}]_1, [\mathbf{sA}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{c}]_1)$ when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}, \mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$.

- G_6: Identical to G_5 except that
  - we generate $\mathbf{c}^*_{+,1}$ as follows:
$$\mathbf{c}^*_{+,1} = \mathbf{cW} + \boxed{\widetilde{\mathbf{x}}^*}$$
    where $\widetilde{\mathbf{x}}^* = (\mathbf{0}_{n_1} \| \mathsf{isk})$, $\mathsf{isk} \in \mathsf{Gen}_1(1^\lambda)$;
  - in crs, we change $[\mathbf{W}_j(\widetilde{\mathbf{M}}_j \otimes \mathbf{Br}_j^\top) + \mathbf{W}\widetilde{\mathbf{M}}_j]_2$ for all $j \in [L]$ as follows:
$$[\mathbf{W}_j(\widetilde{\mathbf{M}}_j \otimes \mathbf{Br}_j^\top) + \mathbf{W}\widetilde{\mathbf{M}}_j + \boxed{\mathbf{c}^\perp \mathbf{a}_j}]_2$$
    where $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{cc}^\perp = 1$ and $\mathbf{Ac}^\perp = \mathbf{0}$; and
$$\mathbf{a}_j = \begin{cases} (-\mathbf{x}^*\mathbf{M} \| 0) & \text{if } \ j \in [L] \setminus (\mathcal{M}^* \cup \mathcal{C}^*) \\ (-\mathbf{x}^*\mathbf{M} \| \mathbf{x}^*\mathbf{M}(\mathbf{f}_j^*)^\top) & \text{if } \ j \in \mathcal{M}^* \cup \mathcal{C}^* \end{cases}$$

  We have $\mathsf{G}_6 \approx_s \mathsf{G}_5$. This follows from the change of variable $\mathbf{W} \mapsto \mathbf{W} + \mathbf{c}^\perp(-\mathbf{x}^* \| \mathsf{isk})$. With above variable substitution, we have
$$\begin{aligned} & \mathbf{cW} + (\mathbf{x}^* \| \mathbf{0}_n) && /\!/ \ \mathbf{c}^*_{+,1} \text{ in } \mathsf{G}_5 \\ \approx_s \ & \mathbf{cW} + (-\mathbf{x}^* \| \mathsf{isk}) + (\mathbf{x}^* \| \mathbf{0}_n) \\ = \ & \mathbf{cW} + \boxed{(\mathbf{0}_{n_1} \| \mathsf{isk})} && /\!/ \ \mathbf{c}^*_{+,1} \text{ in } \mathsf{G}_6 \end{aligned}$$
  For all $j \in \mathcal{M}^* \cup \mathcal{C}^*$, we have
$$\begin{aligned} & [\mathbf{W}\widetilde{\mathbf{M}}_j]_2 && /\!/ \ \mathsf{crs} \text{ in } \mathsf{G}_5 \\ \approx_s \ & \left[\mathbf{W}\widetilde{\mathbf{M}}_j + \mathbf{c}^\perp(-\mathbf{x}^* \| \mathsf{isk}) \begin{pmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n\times n_2} & \mathsf{ict}_j^\top \end{pmatrix}\right]_2 \\ = \ & [\mathbf{W}\widetilde{\mathbf{M}}_j + \mathbf{c}^\perp(\mathbf{x}^*\mathbf{M} \| \boxed{\mathbf{x}^*\mathbf{M}(\mathbf{f}_j^*)^\top})]_2 && /\!/ \ \mathsf{crs} \text{ in } \mathsf{G}_6 \end{aligned}$$
  the third "=" follows from the fact that $[\mathsf{ict}_j]_2 \in \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mathbf{x}^*\mathbf{M}(\mathbf{f}_j^*)^\top)$ for $j \in \mathcal{M}^* \cup \mathcal{C}^*$, and the linear decryption of Π_1 (defined in Section 2.5). And for all $j \in [L] \setminus (\mathcal{M}^* \cup \mathcal{C}^*)$, we have
$$\begin{aligned} & [\mathbf{W}\widetilde{\mathbf{M}}_j]_2 && /\!/ \ \mathsf{crs} \text{ in } \mathsf{G}_5 \\ \approx_s \ & \left[\mathbf{W}\widetilde{\mathbf{M}}_j + \mathbf{c}^\perp(-\mathbf{x}^* \| \mathsf{isk}) \begin{pmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n\times n_2} & \mathsf{ict}_j^\top \end{pmatrix}\right]_2 \\ = \ & [\mathbf{W}\widetilde{\mathbf{M}}_j + \mathbf{c}^\perp(\mathbf{x}^*\mathbf{M} \| \boxed{0})]_2 && /\!/ \ \mathsf{crs} \text{ in } \mathsf{G}_6 \end{aligned}$$
  the third "=" follows from the fact that $[\mathsf{ict}_j]_2 \in \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0)$ for $j \in [L] \setminus (\mathcal{M}^* \cup \mathcal{C}^*)$, and the linear decryption of Π_1 (defined in Section 2.5).
- $\mathsf{G}_{7,\ell}$, $(\ell \in [0, L])$: Identical to G_6 except that for all $j \in [\ell]$, we change $[\mathbf{W}_j(\widetilde{\mathbf{M}}_j \otimes \mathbf{Br}_j^\top) + \mathbf{W}\mathbf{M}_j + \mathbf{c}^\perp \mathbf{a}_j]_2$ in crs as follows:
$$[\mathbf{W}_j(\widetilde{\mathbf{M}}_j \otimes \mathbf{Br}_j^\top) + \mathbf{W}\mathbf{M}_j + \cancel{\mathbf{c}^\perp \mathbf{a}_j}]_2$$
  We have that
  - $\mathsf{G}_{7,0} = \mathsf{G}_6$; the two games are actually identical, since $[0] = \emptyset$;
  - $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$ for all $\ell \in [L]$, we will employ a sub-sequence of games for the proof described later.

Observe that in the final game $\mathsf{G}_{7,L}$ can be simulated using the simulator by setting $\mu_i = \mathbf{x}^*\mathbf{M}(\mathbf{f}_i^*)^\top$, where we embed $\mathbf{x}^*\mathbf{M}(\mathbf{f}_i^*)^\top$ into crs so that hsk_i for all $i \in \mathcal{M}^* \cup \mathcal{C}^*$ and remove $\mathbf{x}^*$ from ct^*.

From $\mathsf{G}_{7,\ell-1}$ to $\mathsf{G}_{7,\ell}$. We are ready to prove $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$ and this will complete the proof of Lemma 4. For this, we need the following sub-sequence of games for each $\ell \in [L]$:

– $\mathsf{G}_{7,\ell-1,0}$: Identical to $\mathsf{G}_{7,\ell-1}$ where we recall $\mathsf{crs}, \mathsf{pk}_i \in D_i$ and $\mathbf{c}_1^*$, with highlighting relevant terms in the following sub-sequence with dashed boxes as follows:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{A}\mathbf{W}]_1, \{\mathsf{crs}_i, [\widehat{\mathbf{R}}_i, \mathbf{A}\mathbf{W}_i(\widetilde{\mathbf{M}}_i \otimes \mathbf{I}_{k+1}), \mathbf{A}\mathbf{W}_i]_1, [\widetilde{\mathbf{M}}_i]_2\}_{i \in [L]} \\ \{[\mathbf{B}\mathbf{r}_j^\top, \mathbf{W}_j(\widetilde{\mathbf{M}}_j \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{W}\widetilde{\mathbf{M}}_j]_2\}_{j \in [\ell-1]} \\ \boxed{[\mathbf{B}\mathbf{r}_\ell^\top, \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{B}\mathbf{r}_\ell^\top) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \mathbf{c}^\perp \mathbf{a}_\ell]_2} \\ \{[\mathbf{B}\mathbf{r}_j^\top, \mathbf{W}_j(\widetilde{\mathbf{M}}_j \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{W}\widetilde{\mathbf{M}}_j + \mathbf{c}^\perp \mathbf{a}_j]_2\}_{j \in [L] \setminus [\ell]} \\ \{[\mathbf{W}_i(\widetilde{\mathbf{M}}_i \otimes \mathbf{B}\mathbf{r}_j^\top)]_2\}_{j \in [L] \setminus \{\ell\}, i \in [L] \setminus \{j\}}, \boxed{\{[\mathbf{W}_i(\widetilde{\mathbf{M}}_i \otimes \mathbf{B}\mathbf{r}_\ell^\top)]_2\}_{i \in [L] \setminus \{\ell\}}} \end{pmatrix}$$

$$\mathsf{pk}_i = \begin{cases} \big([\overbrace{\mathbf{A}\mathbf{U}_i}^{\mathbf{T}_i}, \overbrace{\widehat{\mathbf{R}}_i\mathbf{U}_i}^{\mathbf{Q}_i}]_1, \{[\overbrace{\mathbf{U}_i\mathbf{d}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j \in [\ell-1] \setminus \{i\}}, \boxed{[\overbrace{\mathbf{U}_i\mathbf{B}\mathbf{r}_\ell^\top}^{\mathbf{h}_{i,\ell}}]_2}, \{[\overbrace{\mathbf{U}_i\mathbf{B}\mathbf{r}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j \in [L] \setminus [i,\ell]}, \widetilde{\pi}_i\big) & \text{if } i \neq \ell \\ \big([\underbrace{\mathbf{A}\mathbf{U}_\ell}_{\mathbf{T}_\ell}, \underbrace{\widehat{\mathbf{R}}_i\mathbf{U}_\ell}_{\mathbf{Q}_\ell}]_1, \{[\underbrace{\mathbf{U}_\ell\mathbf{d}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j \in [\ell-1]}, \qquad \{[\underbrace{\mathbf{U}_\ell\mathbf{B}\mathbf{r}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j \in [L] \setminus [\ell]}, \widetilde{\pi}_\ell\big) & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_1^* = \boxed{\mathbf{e}_1 \widetilde{\mathbf{R}}_\ell^{-1} \mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}_\ell^*)^\top \otimes \mathbf{I}_{k+1})} + \sum_{i \in [L] \setminus \{\ell\}} (\mathbf{e}_1 \widetilde{\mathbf{R}}_i^{-1} \mathbf{Q}_i^* + \mathbf{c}\mathbf{W}_i(\widetilde{\mathbf{M}}_i(\overline{\mathbf{f}}_i^*)^\top \otimes \mathbf{I}_{k+1}))$$

where $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{c}\mathbf{c}^\perp = 1$, $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$. For all $i \in [L]$, $s \in \{1, 2\}$, recall that $[\widetilde{\mathbf{M}}_i]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}_i^\top \end{bmatrix}_s$, where

$$[\mathsf{ict}_i]_s \in \begin{cases} \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0) & \text{if } i \in [L] \setminus (\mathcal{M}^* \cup \mathcal{C}^*) \\ \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mathbf{x}^*\mathbf{M}(\mathbf{f}_i^*)^\top) & \text{if } i \in \mathcal{M}^* \cup \mathcal{C}^* \end{cases}$$

For all $j \in [L] \setminus [\ell - 1]$, recall that

$$\mathbf{a}_j = \begin{cases} (-\mathbf{x}^*\mathbf{M} \| 0) & \text{if } j \in [L] \setminus (\mathcal{M}^* \cup \mathcal{C}^*) \\ (-\mathbf{x}^*\mathbf{M} \| \mathbf{x}^*\mathbf{M}(\mathbf{f}_j^*)^\top) & \text{if } j \in \mathcal{M}^* \cup \mathcal{C}^* \end{cases}$$

– $\mathsf{G}_{7,\ell-1,1}$: Identical to $\mathsf{G}_{7,\ell-1,0}$ except that we replace all $\mathbf{B}\mathbf{r}_\ell^\top$ with $\mathbf{d}_\ell^\top \leftarrow \mathbb{Z}_p^{k+1}$ in crs; in particular, we change the dashed boxed term in crs and pk_i as follows:

$$[\boxed{\mathbf{d}_\ell^\top}, \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \boxed{\mathbf{d}_\ell^\top}) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \mathbf{c}^\perp \mathbf{a}_\ell]_2, \{[\mathbf{W}_i(\widetilde{\mathbf{M}}_i \otimes \boxed{\mathbf{d}_\ell^\top})]_2, [\mathbf{U}_i \boxed{\mathbf{d}_\ell^\top}]_2\}_{i \in [L] \setminus \{\ell\}}$$

We have $\mathsf{G}_{7,\ell-1,1} \approx_c \mathsf{G}_{7,\ell-1,0}$. This follows from MDDH assumption w.r.t. $[\mathbf{B}]_2$ which ensures that $([\mathbf{B}]_2, [\mathbf{B}\mathbf{r}_\ell^\top]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{d}_\ell^\top]_2)$ when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1) \times k}$, $\mathbf{r}_\ell \leftarrow \mathbb{Z}_p^{1 \times k}$, $\mathbf{d}_\ell \leftarrow \mathbb{Z}_p^{1 \times (k+1)}$.

– $\mathsf{G}_{7,\ell-1,2}$: Identical to $\mathsf{G}_{7,\ell-1,1}$, except that we replace $\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}_\ell^\top) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \mathbf{c}^\perp \mathbf{a}_\ell$ with

$$\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}_\ell^\top) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \cancel{\mathbf{c}^\perp \mathbf{a}_\ell}$$

We have $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$. With defining $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ and $\mathbf{d}^\perp \in \mathbb{Z}_p^{1 \times (k+1)}$ such that $\mathbf{c}\mathbf{c}^\perp = 1$, $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$ and $\mathbf{d}^\perp \mathbf{d}_\ell^\top = 1$, $\mathbf{d}^\perp \mathbf{B} = \mathbf{0}$. We consider two cases

- Honest case ($\ell \in [L] \setminus (\mathcal{M}^* \cup \mathcal{C}^*)$): In this case, for all $s \in \{1, 2\}$, with $[\mathsf{ict}_\ell]_s \in \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0)$, we have

$$\mathbf{a}_\ell = (-\mathbf{x}^*\mathbf{M} \| 0), \quad [\mathbf{M}_\ell]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}_\ell^\top \end{bmatrix}_s$$

And we have $\mathsf{pk}^*_\ell = ([\mathbf{T}^*_\ell, \mathbf{Q}^*_\ell]_1, \{[\mathbf{h}^{*\,\top}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}}, \pi^*_\ell) \in D_\ell \setminus C_\ell$ in this case. Namely, we know $\mathbf{U}^*_\ell$ (such that $\mathbf{T}^*_\ell = \mathbf{A}\mathbf{U}^*_\ell$ and $\mathbf{Q}^*_\ell = \widehat{\mathbf{R}}_\ell\mathbf{U}^*_\ell$) and $\mathbf{U}^*_\ell$ is hidden from the adversary. We can write the dash boxed terms in $\mathbf{c}^*_1$ as follows:

$$\boxed{\mathbf{c}\mathbf{U}^*_\ell} + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top \otimes \mathbf{I}_{k+1})$$

and replace $\widehat{\mathbf{R}}_\ell$ in crs with a random $\mathbf{R}_\ell$ as in G_3. And we can proof $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$ in this case using the following argument for all $b \in \{0,1\}$:

$$\begin{aligned}
&\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{B}), \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + b\mathbf{c}^\perp\mathbf{a}_\ell]_2; && /\!/\mathsf{crs},\ \mathsf{pk}_\ell\\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top \otimes \mathbf{I}_{k+1})]_1, \mathbf{A}\mathbf{U}^*_\ell, [\mathbf{R}_\ell\mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell\mathbf{B} && /\!/\mathsf{ct}^*,\ \mathsf{pk}^*_\ell\\
\approx_c\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{B}), \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + b\mathbf{c}^\perp\mathbf{a}_\ell]_2;\\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top \otimes \mathbf{I}_{k+1})]_1, \mathbf{A}\mathbf{U}^*_\ell, [\mathbf{R}_\ell\mathbf{U}^*_\ell + \boxed{\widehat{\mathbf{u}}^\top\mathbf{d}^\perp}]_1, \mathbf{U}^*_\ell\mathbf{B}\\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{B}), \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \boxed{\mathbf{c}^\perp(\mathbf{w}_\ell\mathbf{M}\|0)} + b\mathbf{c}^\perp\mathbf{a}_\ell]_2;\\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top \otimes \mathbf{I}_{k+1}) + \boxed{u_\ell\mathbf{d}^\perp + \mathbf{w}_\ell\mathbf{M}(\mathbf{f}^*_\ell)^\top\mathbf{d}^\perp}]_1, \mathbf{A}\mathbf{U}^*_\ell, [\mathbf{R}_\ell\mathbf{U}^*_\ell + \boxed{\mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{d}^\perp} + \widehat{\mathbf{u}}^\top\mathbf{d}^\perp]_1, \mathbf{U}^*_\ell\mathbf{B}\\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{B}), \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \mathbf{c}^\perp(\mathbf{w}_\ell\mathbf{M}\|0) + \cancel{b\mathbf{c}^\perp\mathbf{a}_\ell}]_2;\\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top \otimes \mathbf{I}_{k+1}) + u_\ell\mathbf{d}^\perp + \mathbf{w}_\ell\mathbf{M}(\mathbf{f}^*_\ell)^\top\mathbf{d}^\perp]_1, \mathbf{A}\mathbf{U}^*_\ell, [\mathbf{R}_\ell\mathbf{U}^*_\ell + \mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{d}^\perp + \widehat{\mathbf{u}}^\top\mathbf{d}^\perp]_1, \mathbf{U}^*_\ell\mathbf{B}
\end{aligned}$$

where $\widehat{\mathbf{u}} \leftarrow \mathbb{Z}_p^{1\times(2k+2)}$, $u_\ell \leftarrow \mathbb{Z}_p$ and $\mathbf{w}_\ell \leftarrow \mathbb{Z}_p^{n_1}$. We justify each step as below: The first $\approx_c$ follows the argument:

$$\begin{aligned}
&(\mathbf{A}, \mathbf{c}, [\mathbf{R}_\ell]_1, \mathbf{B}, \mathbf{d}^\perp, \mathbf{A}\mathbf{U}_\ell, \mathbf{c}\mathbf{U}_\ell[\mathbf{R}\mathbf{U}_\ell]_1, \qquad\qquad \mathbf{U}_\ell\mathbf{B})\\
\approx_c\ &(\mathbf{A}, \mathbf{c}, [\mathbf{R}_\ell]_1, \mathbf{B}, \mathbf{d}^\perp, \mathbf{A}\mathbf{U}_\ell, \mathbf{c}\mathbf{U}_\ell, [\mathbf{R}_\ell\mathbf{U}_\ell + \boxed{\mathbf{u}^\top\mathbf{d}^\perp}]_1, \mathbf{U}_\ell\mathbf{B})
\end{aligned}$$

which is analogous to the Lemma 2 in [ZZGQ23]. The second $\approx_s$ uses the change of variables:

$$\mathbf{U}^*_\ell \mapsto \mathbf{U}^*_\ell + \mathbf{c}^\perp u_\ell\mathbf{d}^\perp \quad \text{and} \quad \mathbf{W}_\ell \mapsto \mathbf{W}_\ell + \mathbf{c}^\perp((\mathbf{w}_\ell\|\mathbf{0}_n) \otimes \mathbf{d}^\perp)$$

The last $\approx_s$ is straight-forward with the observation that $\widehat{\mathbf{u}}^\top$ hides $\mathbf{R}_\ell\mathbf{c}^\perp u_\ell$, this implies that u_ℓ hides $\mathbf{w}_\ell\mathbf{M}(\mathbf{f}^*_\ell)^\top$, and $(\mathbf{w}_\ell\mathbf{M}\|0)$ is sufficient to hide $\mathbf{a}_\ell = (-\mathbf{x}^*\mathbf{M}\|0)$.

$$\mathbf{a}_\ell = (-\mathbf{x}^*\mathbf{M}\|\mathbf{x}^*\mathbf{M}(\mathbf{f}^*_j)^\top), \quad [\mathbf{M}_\ell]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}^\top_{n_1} \\ \mathbf{0}_{n\times n_2} & \mathsf{ict}^\top_\ell \end{bmatrix}_s \tag{20}$$

- Corrupted & Malicious Case ($\ell \in (\mathcal{M}^* \cup \mathcal{C}^*)$): And in this case, we have $\mathsf{pk}^*_\ell = ([\mathbf{T}^*_\ell, \mathbf{Q}^*_\ell]_1, \{[\mathbf{h}^{*\,\top}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}}, \pi^*_\ell) \in C_\ell \cup \overline{D}_\ell$. We prove $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$ in this case using the following argument:

$$\begin{aligned}
&\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{B}), \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \mathbf{c}^\perp\mathbf{a}_\ell]_2; && /\!/\mathsf{crs}\\
&[\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top \otimes \mathbf{I}_{2k+1})]_1 && /\!/\mathsf{ct}^* \text{ in } \mathsf{G}_{7,\ell-1,1}\\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{B}), \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \boxed{\mathbf{c}^\perp(\mathbf{x}^*\| -\mathsf{isk})\widetilde{\mathbf{M}}_\ell} + \mathbf{c}^\perp\mathbf{a}_\ell]_2;\\
&[\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top \otimes \mathbf{I}_{2k+1}) + \boxed{(\mathbf{x}^*\| -\mathsf{isk})\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top\mathbf{d}^\perp}]_1\\
=\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{B}), \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}\widetilde{\mathbf{M}}_\ell + \cancel{\mathbf{c}^\perp(\mathbf{x}^*\| -\mathsf{isk})\widetilde{\mathbf{M}}_\ell} + \cancel{\mathbf{c}^\perp\mathbf{a}_\ell}]_2; && /\!/\mathsf{crs}\\
&[\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top \otimes \mathbf{I}_{2k+1}) + \cancel{(\mathbf{x}^*\| -\mathsf{isk})\widetilde{\mathbf{M}}_\ell(\overline{\mathbf{f}}^*_\ell)^\top\mathbf{d}^\perp}]_1 && /\!/\mathsf{ct}^* \text{ in } \mathsf{G}_{7,\ell-1,2}
\end{aligned}$$

where $\mathsf{isk} \in \mathsf{Gen}_1(1^\lambda)$. We justify each step as follows: The first $\approx_s$ uses the change of variable:

$$\mathbf{W}_\ell \mapsto \mathbf{W}_\ell + \mathbf{c}^\perp((\mathbf{x}^* \| - \mathsf{isk}) \otimes \mathbf{d}^\perp)$$

The second = follows from the fact in equility (20), $\overline{\mathbf{f}}^*_\ell = (\mathbf{f}^*_\ell \| 1)$ and the linear decryption of Π_1 (defined in Section 2.5), which ensure that

$$\left[(\mathbf{x}^* \| - \mathsf{isk}) \begin{pmatrix} \mathbf{M} & \mathbf{0}^\top_{n_1} \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}^\top_\ell \end{pmatrix} (\mathbf{f}^*_\ell \| 1)^\top\right]_1 = [0]_1, \left[(\mathbf{x}^* \| - \mathsf{isk}) \begin{pmatrix} \mathbf{M} & \mathbf{0}^\top_{n_1} \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}^\top_\ell \end{pmatrix} + (-\mathbf{x}^*\mathbf{M} \| \mathbf{x}^*\mathbf{M}(\mathbf{f}^*_j)^\top)\right]_2 = [0]_2$$

– $\mathsf{G}_{7,\ell-1,3}$: Identical to $\mathsf{G}_{7,\ell-1,2}$ except that we replace all $\mathbf{d}^\top_\ell$ with $\mathbf{B}\mathbf{r}^\top_\ell$ where $\mathbf{r}^\top_\ell \leftarrow \mathbb{Z}_p^k$ in crs; in particular, we change the dashed boxed term in crs and pk_i as follows:

$$[\boxed{\mathbf{B}\mathbf{r}^\top_\ell}, \mathbf{W}_\ell(\widetilde{\mathbf{M}}_\ell \otimes \boxed{\mathbf{B}\mathbf{r}^\top_\ell}) + \mathbf{W}\widetilde{\mathbf{M}}_\ell]_2, \{[\mathbf{W}_i(\widetilde{\mathbf{M}}_i \otimes \boxed{\mathbf{B}\mathbf{r}^\top_\ell})]_2, [\mathbf{U}_i \boxed{\mathbf{B}\mathbf{r}^\top_\ell}]_2\}_{i \in [L] \setminus \{\ell\}}$$

We have $\mathsf{G}_{7,\ell-1,1} \approx_c \mathsf{G}_{7,\ell-1,0}$. This follows from MDDH assumption w.r.t. $[\mathbf{B}]_2$ which ensures that $([\mathbf{B}]_2, [\mathbf{B}\mathbf{r}^\top_\ell]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{d}^\top_\ell]_2)$ when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{r}_\ell \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{d}_\ell \leftarrow \mathbb{Z}_p^{1\times(k+1)}$.

6.4 Implication: Slotted Reg-IPFE with Very Selective SIM-Security

Setting the constraint $\mathbf{M}$ as $\mathbf{I}$, we immediately have a multi-instance slotted Reg-IPFE which implies a Reg-IPFE with compact ciphertext. The scheme achieves very selective simulation-based security as our PReg-IPFE. And we delay the concrete scheme and proof in Appendix C.

6.5 A Variant: Slotted Reg-IPFE with Selective IND-security

The scheme is basically the same with our pre-constrained Reg-IPFE except that we set $\mathbf{M}_i$ as $\mathbf{I}$ and remove the extra components for simulation-based security.

Scheme. Assuming QA-NIZK $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ for linear space over bilinear groups, see Section 2.4, our slotted Reg-IPFE scheme in prime-order bilinear groups works as follows:

– $\mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \cdots, 1^{L_m}, 1^n)$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \ \mathbf{W} \leftarrow \mathbb{Z}_p^{(2k+1)\times n}.$$

For each $q \in [m]$, sample

$$\mathbf{B}_q \leftarrow \mathbb{Z}_p^{(k+1)\times k},$$

and for all $i \in [L_q]$, sample

$$\mathbf{W}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)n}, \ \mathbf{R}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}, \ \mathbf{r}_{q,i} \leftarrow \mathbb{Z}_p^{1\times k}.$$

Run

$$(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_{q,i}]_1),$$

where $\mathbf{A}_{q,i} = \binom{\mathbf{A}}{\mathbf{R}_{q,i}} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$ for all $q \in [m]$ and $i \in [L_q]$. Output

$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \mathbf{A}\mathbf{W}]_1, \\ \left\{ \begin{array}{l} \{\mathsf{crs}_{q,i}, [\mathbf{R}_{q,i}, \mathbf{A}\mathbf{W}_{q,i}]_1\}_{i\in[L_q]} \\ \{[\mathbf{B}_q\mathbf{r}^\top_{q,j}, \mathbf{W}_{q,j}(\mathbf{I}_n \otimes \mathbf{B}_q\mathbf{r}^\top_{q,j}) + \mathbf{W}]_2]_2\}_{j\in[L_q]} \\ \{[\mathbf{W}_{q,i}(\mathbf{I}_n \otimes \mathbf{B}_q\mathbf{r}^\top_{q,j})\}_{j\in[L_q], i\in[L_q]\setminus\{j\}} \end{array} \right\}_{q\in[m]} \end{array} \right).$$

– $\mathsf{Gen}(\mathsf{crs}, q, i)$: Sample $\mathbf{U}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$. Define $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}} = \binom{\mathbf{A}\mathbf{U}_{q,i}}{\mathbf{R}_{q,i}\mathbf{U}_{q,i}} = \mathbf{A}_{q,i}\mathbf{U}_{q,i} \in \mathbb{Z}_p^{(3k+2)\times(k+1)}$ and run

$$\pi_{q,i} \leftarrow \mathsf{LPrv}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \mathbf{U}_{q,i}).$$

Fetch $\{[\mathbf{B}_q\mathbf{r}_{q,j}^\top]_2\}_{j\in[L_q]\setminus\{i\}}$ from crs and output

$$\mathsf{pk}_{q,i} = \big([\underbrace{\mathbf{A}\mathbf{U}_{q,i}}_{\mathbf{T}_{q,i}}, \underbrace{\mathbf{R}_{q,i}\mathbf{U}_{q,i}}_{\mathbf{Q}_{q,i}}]_1, \{[\underbrace{\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^\top}_{\mathbf{h}_{q,i,j}}]_2\}_{j\in[L_q]\setminus\{i\}}, \pi_{q,i}\big) \quad \text{and} \quad \mathsf{sk}_{q,i} = \mathbf{U}_{q,i}.$$

– $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i})$: Parse $\mathsf{pk}_{q,i} = \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{i,j}]_2\}_{j\in[L_q]\setminus\{i\}}, \pi_{q,i}\big)$. Write $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}}$ and check

$$\mathsf{LVer}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \pi_{q,i}) \stackrel{?}{=} 1.$$

For each $j \in [L_q] \setminus \{i\}$, check

$$e([\mathbf{A}]_1, [\mathbf{h}_{i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_{q,i}]_1, [\mathbf{B}_q\mathbf{r}_{q,j}^\top]_2).$$

If all these checks pass, output 1; otherwise, output 0.

– $\mathsf{Agg}_+(\mathsf{crs})$: Output:

$$\mathsf{mpk}_+ = ([\mathbf{A},\ \mathbf{A}\mathbf{W}]_1)$$

– $\mathsf{Agg}(\mathsf{crs}, q, (\mathsf{pk}_{q,i}, \mathbf{y}_{q,i})_{i\in[L_q]})$: If q is an empty instance, on input $(\mathsf{pk}_{q,i}, \mathbf{f}_{q,i}) = (\perp, \perp)$ for all $i \in [L_q]$, abort and return $\mathsf{mpk}_q = \perp$, $\mathsf{hsk}_{q,j} = \perp$ for all $j \in [L_q]$. For all $i \in [L_q]$, parse $\mathsf{pk}_{q,i} = \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{i,j}]_2\}_{j\in[L_q]\setminus\{i\}}, \pi_{q,i}\big)$. Output:

$$\mathsf{mpk}_q = \left(\left[\sum_{i\in[L_q]} (\mathbf{T}_{q,i} + \mathbf{A}\mathbf{W}_{q,i}(\mathbf{y}_{q,i}^\top \otimes \mathbf{I}_{k+1}))\right]_1\right)$$

and for all $j \in [L_q]$

$$\mathsf{hsk}_{q,j} = \left(\left[\underbrace{\mathbf{B}_q\mathbf{r}_{q,j}^\top}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i\in[L_q]\setminus\{j\}} (\mathbf{h}_{q,i,j} + \mathbf{W}_{q,i}(\mathbf{I}_n \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top)\mathbf{y}_{q,i}^\top)}_{\mathbf{k}_1^\top}, \underbrace{\mathbf{W}_{q,j}(\mathbf{y}_{q,j}^\top \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{W}\mathbf{y}_{q,j}^\top}_{\mathbf{k}_2^\top}\right]_2\right).$$

– $\mathsf{Enc}_+(\mathsf{mpk}_+, \mathbf{x})$: Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$. Output:

$$\mathsf{ct}_+ = ([\underbrace{\mathbf{s}\mathbf{A}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{W} + \mathbf{x}}_{\mathbf{c}_{+,1}}]_1)$$

– $\mathsf{Enc}(\mathsf{mpk}_q)$: Abort and return $\perp$ if $\mathsf{mpk}_q = \perp$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$. Output:

$$\mathsf{ct}_q = \Bigg[\underbrace{\sum_{i\in[L_q]} (\mathbf{s}\mathbf{T}_{q,i} + \mathbf{s}\mathbf{A}\mathbf{W}_{q,i}(\mathbf{y}_{q,i}^\top \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_q}\Bigg]_1.$$

– $\mathsf{Dec}(\mathsf{sk}_{q^*,i^*}, \mathsf{hsk}_{q^*,i^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*}))$: Abort and return $\perp$ if $\mathsf{ct}_{q^*} = \perp$. Parse

$$\mathsf{sk}_{q^*,i^*} = \mathbf{U}_{q,i^*}, \quad \mathsf{hsk}_{q^*,i^*} = ([\mathbf{k}_0^\top, \mathbf{k}_1^\top, \mathbf{K}_2]_2), \quad (\mathsf{ct}_+, \mathsf{ct}_{q^*}) = ([\mathbf{c}_{+,0}, \mathbf{c}_{+,1}, \mathbf{c}_{q^*}]_1).$$

Recover

$$\begin{aligned} [z_1]_T &= e([\mathbf{c}_{q^*}]_1, [\mathbf{k}_0^\top]_2), & [z_2]_T &= e([\mathbf{c}_{+,0}]_1, [\mathbf{k}_1^\top]_2); \\ [z_3]_T &= e([\mathbf{c}_{+,0}\mathbf{U}_{q^*,i^*}]_1, [\mathbf{k}_0^\top]_2), & [z_4]_T &= e([\mathbf{c}_{+,0}]_1, [\mathbf{k}_2^\top]_2); \\ [z_5]_T &= e([\mathbf{c}_{+,1}]_1, [\mathbf{y}_{q^*,i^*}^\top]_2), \end{aligned}$$

Compute

$$[z]_T = [z_1 - z_2 - z_3 - z_4 + z_5]_T.$$

Recover z from $[z]_T$ via brute-force DLOG and output z.

Completeness. For all $\lambda, m, n \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all all $q \in [m]$ and $i \in [L_q]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^n, 1^{L_1}, \ldots, 1^{L_m})$, and $(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q, i)$, we have

$$\begin{aligned}\mathsf{pk}_{q,i} &= \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j\in[L_q]\setminus\{i\}}, \pi_{q,i}\big)\\ &= \big([\mathbf{A}\mathbf{U}_{q,i}, \mathbf{R}_{q,i}\mathbf{U}_{q,i}]_1, \{[\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^\top]_2\}_{j\in[L_q]\setminus\{i\}}, \pi_{q,i}\big)\end{aligned}$$

for some $\mathbf{U}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$ and $\pi_{q,i} \leftarrow \mathsf{LPrv}(\mathsf{crs}_{q,i}, [\mathbf{A}_{q,i}\mathbf{U}_i]_1, \mathbf{U}_i)$ where $(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_{q,i}]_1)$ and $\mathbf{A}_{q,i} = \binom{\mathbf{A}}{\mathbf{R}_{q,i}}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$, $\mathbf{R}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}$. Then

- Write $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}} = \binom{\mathbf{A}\mathbf{U}_{q,i}}{\mathbf{R}_{q,i}\mathbf{U}_{q,i}}$, we have $\mathsf{LVer}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \pi_{q,i}) = 1$ by the perfect completeness of Π_0 (see Section 2.4) and the fact that $\mathbf{F}_{q,i} = \mathbf{A}_{q,i}\mathbf{U}_{q,i}$;
- For each $j \in [L_q] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^\top]_2) = e([\mathbf{A}\mathbf{U}_{q,i}]_1, [\mathbf{B}_q\mathbf{r}_{q,j}^\top]_2)$ by the definition of bilinear map e (see Section 2.1) and the fact that $\mathbf{A} \cdot \mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^\top = \mathbf{A}\mathbf{U}_{q,i} \cdot \mathbf{B}_q\mathbf{r}_{q,j}^\top$.

This ensures that $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i}) = 1$ by the specification of Ver and readily proves the completeness.

Correctness. For all $\lambda, m, n \in \mathbb{N}$, all $q^* \in [m]$ and $i^* \in [L_{q^*}]$; all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^n, 1^{L_1}, \ldots, 1^{L_m})$, all $(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q^*, i^*)$; all $\{\mathsf{pk}_{q^*,i}\}_{i\in[L_{q^*}]\setminus\{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, q^*, i, \mathsf{pk}_{q^*,i}) = 1$; all $\mathbf{x} \in \mathbb{Z}_p^{1\times n}$ and $\mathbf{y}_{q^*,i} \in \mathbb{Z}_p^{1\times n}$, for all $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$, we have

$$\begin{aligned}\mathsf{sk}_{q^*,i^*} &= \mathbf{U}_{q^*,i^*},\\ (\mathsf{ct}_+, \mathsf{ct}_{q^*}) &= \Bigg(\Bigg[\underbrace{\mathbf{sA}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{sAW} + \mathbf{x}}_{\mathbf{c}_{+,1}}, \underbrace{\sum_{i\in[L_q]} (\mathbf{sT}_{q^*,i} + \mathbf{sAW}_{q^*,i}(\mathbf{y}_{q^*,i^*}^\top \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_{q^*}}\Bigg]_1\Bigg)\\ \mathsf{hsk}_{q^*,i^*} &= \Bigg(\Bigg[\underbrace{\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i\in[L_{q^*}]\setminus\{i^*\}} (\mathbf{h}_{q^*,i,i^*} + \mathbf{W}_{q^*,i}(\mathbf{y}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top))}_{\mathbf{k}_1^\top}, \underbrace{\mathbf{W}_{q^*,i^*}(\mathbf{y}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top) + \mathbf{W}\mathbf{y}_{q^*,i^*}^\top}_{\mathbf{k}_2^\top}\Bigg]_2\Bigg).\end{aligned}$$

where

$$\mathbf{A}\mathbf{h}_{q^*,i,i^*} = \mathbf{T}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top \quad \forall i \in [L_{q^*}] \setminus \{i^*\} \quad \text{and} \quad \mathbf{A}\mathbf{U}_{q^*,i^*} = \mathbf{T}_{q^*,i^*}.$$

Note that here we actually consider $\mathsf{hsk}_{q^*,j}$ for $j = i^*$ and $\mathsf{sk}_{q^*,i}$ for $i = i^*$ and all above equalities are ensured by Ver and Gen. We have

$$\begin{aligned} z_1 &= \sum_{i\in[L_{q^*}]} (\mathbf{sT}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top + \mathbf{sAW}_{q^*,i}(\mathbf{y}_{q^*,i^*}^\top \otimes \mathbf{I}_{k+1})\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top)\\ &= \sum_{i\in[L_{q^*}]} (\mathbf{sT}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top + \mathbf{sAW}_{q^*,i}(\mathbf{y}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top)) \qquad (21)\\ z_2 &= \sum_{i\in[L_{q^*}]\setminus\{i^*\}} (\mathbf{sA}\mathbf{h}_{q^*,i,i^*} + \mathbf{sAW}_{q^*,i}(\mathbf{y}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top))\\ z_3 &= \mathbf{sAU}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top\\ z_4 &= \mathbf{sAW}_{q^*,i^*}(\mathbf{y}_{q^*,i^*}^\top \otimes \mathbf{B}_{q^*}\mathbf{r}_{q^*,i^*}^\top) + \mathbf{sAW}\mathbf{y}_{q^*,i^*}^\top\\ z_5 &= \mathbf{sAW}\mathbf{y}_{q^*,i^*}^\top + \mathbf{x}\mathbf{y}_{q^*,i^*}^\top\end{aligned}$$

and then

$$\begin{aligned}
z &= z_1 - z_2 - z_3 - z_4 + z_5 \\
&= \mathbf{sT}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} + \mathbf{sAW}_{q^*,i^*}(\mathbf{y}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) - \mathbf{sAU}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} \\
&\quad -(\mathbf{sAW}_{q^*,i^*}(\mathbf{y}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{sAWy}^\top_{q^*,i^*}) \\
&\quad +(\mathbf{sAWy}^\top_{q^*,i^*} + \mathbf{xy}^\top_{q^*,i^*}) \qquad (22) \\
&= \mathbf{xy}^\top_{q^*,i^*} \qquad (23)
\end{aligned}$$

Here, equality (21) follows from the property of tensor product: $(\mathbf{a}^\top \otimes \mathbf{I})\mathbf{M} = \mathbf{a}^\top \otimes \mathbf{M}$ for matrices of proper size; equality (22) follows from the fact that $\mathbf{Ah}_{q^*,i,i^*} = \mathbf{T}_i\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}$ for all $i \in [L_{q^*}] \setminus \{i^*\}$; equality (23) follows from the fact that $\mathbf{T}_{q^*,i^*} = \mathbf{AU}_{q^*,i^*}$. This proves the correctness.

Compactness and Efficiency. Our multi-instance Reg-IPFE has the following properties:

$$\begin{aligned}
|\mathsf{crs}| &= O(L^2 \cdot n) \cdot \mathsf{poly}(\lambda), & |\mathsf{hsk}_{q,j}| &= \mathsf{poly}(\lambda), \\
|\mathsf{mpk}_+| &= O(n) \cdot \mathsf{poly}(\lambda), & |\mathsf{mpk}_q| &= \mathsf{poly}(\lambda), \\
|\mathsf{ct}_+| &= O(n) + \mathsf{poly}(\lambda), & |\mathsf{ct}_q| &= \mathsf{poly}(\lambda),
\end{aligned}$$

where $L = L_1 + \cdots + L_m$, $\mathsf{mpk} = (\mathsf{mpk}_s, (\mathsf{mpk}_q)_{q\in[m]})$. Note that the total size of $\{\mathsf{crs}_i\}_{i\in[L]}$ is $L \cdot \mathsf{poly}(\lambda)$ according to the efficiency of the pairing-based QA-NIZK scheme by Kiltz and Wee [KW15] and the fact that the size of language description is $\mathsf{poly}(\lambda)$.

Security. We have the following theorem. Given pairing-based QA-NIZK in [KW15] with unbounded simulation soundness under MDDH assumption and the fact that MDDH assumption implies subspace assumption [CGKW18], our slotted Reg-IPFE scheme achieves selective security from MDDH assumption.

Theorem 5. *Assume $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ is a QA-NIZK with perfect completeness, perfect zero-knowledge and unbounded simulation soundness for linear space defined in Section 2.4, our slotted Reg-IPFE scheme achieves the selective IND-security defined in Section 2.3 under MDDH assumption and subspace decision assumption.*

Proof We prove the following technical lemma this immediately proves Theorem 5.

Lemma 5. *For all adversaries $\mathcal{A}$, there exist adversaries $\mathcal{B}_1, \mathcal{B}_2$ such that:*

$$\mathsf{Adv}^{miReg\text{-}IPFE}_{\mathcal{A}}(\lambda) \leq L \cdot \mathsf{Adv}^{USS}_{\mathcal{B}_1}(\lambda) + (2L + 2L \cdot Q + 1)\mathsf{Adv}^{MDDH}_{\mathcal{B}_2}(\lambda) + \mathsf{negl}(\lambda)$$

where $L = L_1 + \ldots + L_m$ is the number of slots, Q is the maximum number of queries on a slot made by $\mathcal{A}$ and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2) \approx \mathsf{Time}(\mathcal{A})$.

For simplicity, we prove Lemma 4 in the case of nonempty 1-instance and remove the index q in the following proof. For an empty instance, we only need to remove the terms about ct^*_1 and all pk^*_i in the following game sequence and notice there only exists "honest case" for empty instance. In the case of m-instance, it only needs to add back index q and apply sub-sequence $\mathsf{G}_{6,\ell-1,0}, \ldots, \mathsf{G}_{6,\ell-1,3}$ to each instance.

Game Sequence. Suppose that crs is the common reference string, $\mathbf{x}_b^*$ is the challenge, $\{\mathsf{pk}_i^*, \mathbf{y}_i^*\}_{i\in[L]}$ are challenge public keys along with challenge functions to be registered, . For all $i \in [L]$, define $D_i = \{\mathsf{pk}_i : \mathcal{D}_{1,i}[\mathsf{pk}_i] = \mathsf{sk}_i \neq \perp\}$ be responses to $\mathsf{OGen}(i)$ and $C_i = \{\mathsf{pk}_i : (i, \mathsf{pk}_i) \in \mathcal{C}_1\}$ records public keys in D_i that have been sent to $\mathsf{OCor}(i,\cdot)$. Recall that, for each $i \in [L]$, we require that

$$\mathsf{pk}_i^* \notin D_i \implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1, \quad \mathsf{pk}_i^* \in C_i \vee \mathsf{pk}_i^* \notin D_i \implies \mathbf{x}_0^*(\mathbf{y}_i^*)^\top = \mathbf{x}_1^*(\mathbf{y}_i^*)^\top.$$

Note that pk_i serves as a *general* entry in D_i while pk_i^* is the *specific* challenge public for slot i; there can be more than one assignment for pk_i since the adversary can invoke $\mathsf{OGen}(i)$ for many times. We prove the Lemma 4 via dual-system method using the following game sequence.

- G_0: This is the real game, recall that we have
  - crs is in the form:
$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AW}]_1, \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{AW}_i]_1\}_{i\in[L]} \\ \{[\mathbf{Br}_j^\top, \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{W}]_2]_2\}_{j\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{Br}_j^\top)\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$
    where $\mathsf{crs}_i \in \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$, $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{R}_i}$.
  - For each $i \in [L]$, each $(\mathsf{pk}_i, \mathsf{sk}_i) \in D_i$ is in the form
$$\mathsf{pk}_i = ([\underbrace{\mathbf{AU}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{R}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{[\underbrace{\mathbf{U}_i\mathbf{Br}_j^\top}_{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i) \quad \text{and} \quad \mathsf{sk}_i = \mathbf{U}_i$$
    where $\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i)$, $\mathbf{F}_i = \binom{\mathbf{AU}_i}{\mathbf{RU}_i}$.
  - For all $i \in [L]$, pk_i^* is in the form:
$$\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{h}_{i,j}^*]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$$
    such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1$ which means $\mathsf{LVer}\left(\mathsf{crs}_i, \begin{bmatrix} \mathbf{T}_i^* \\ \mathbf{Q}_i^* \end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{Ah}_{i,j}^* = \mathbf{T}_i^*\mathbf{Br}_j^\top$ for each $j \in [L] \setminus \{i\}$.
  - $(\mathsf{ct}_+^*, \mathsf{ct}_1^*)$ for $\mathbf{x}_b^*$ is in the form:
$$(\mathsf{ct}_+^*, \mathsf{ct}_1^*) = \left(\left[\underbrace{\mathbf{sA}}_{\mathbf{c}_{+,0}^*}, \underbrace{\mathbf{sAW} + \mathbf{x}_b^*}_{\mathbf{c}_{+,1}^*}, \underbrace{\sum_{i\in[L]} (\mathbf{sT}_i + \mathbf{sAW}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_1^*}\right]_1\right).$$
- G_1: Identical to G_0 except that for all $i \in [L]$ and all $(\mathsf{pk}_i, \mathsf{sk}_i) \in D_i$, we replace π_i with
$$\widetilde{\pi}_i \leftarrow \boxed{\mathsf{LSim}}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{F}_i]_1) \quad \text{where} \quad \mathbf{F}_i = \begin{pmatrix} \mathbf{AU}_i \\ \mathbf{R}_i\mathbf{U}_i \end{pmatrix}.$$
  We have $\mathsf{G}_1 \equiv \mathsf{G}_0$. This follows from the perfect zero-knowledge of Π_0.
- G_2: Identical to G_1 except that we sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ along with $\mathbf{A}$ and replace all $\mathbf{R}_i$ in crs with
$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix} \mathbf{sA} \\ \mathbf{I}_{2k+1} \end{pmatrix}, \quad \widetilde{\mathbf{R}}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}.$$
  We have $\mathsf{G}_2 \equiv \mathsf{G}_1$. This follows from the fact that both $\mathbf{R}_i$ (in G_2) and $\widehat{\mathbf{R}}_i$ (in G_3) are truly random since matrix $\binom{\mathbf{sA}}{\mathbf{I}_{2k+1}}$ is full-rank.

– G_3: Identical to G_2 except that we generate the $\mathbf{c}_1^*$ as follows:

$$\mathbf{c}_1^* = \sum_{i\in[L]} (\boxed{\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*} + \mathbf{sAW}_i(\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{k+1}))$$

We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from stronger unbounded simulation soundness of Π along with the fact that $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i^*], \pi_i^*) = 1$ for all $i \in [L]$ where $\mathbf{F}_i^* = \begin{pmatrix}\mathbf{T}_i^* \\ \mathbf{Q}_i^*\end{pmatrix}$. Assume $\mathsf{pk}_{i^*}^* \notin D_{i^*}$, i.e., $\mathsf{pk}_{i^*}^*$ is malicious. In the reduction, we guess $i^* \leftarrow [L]$ and obtain $\mathbf{A}, \widehat{\mathbf{R}}_{i^*}, \mathsf{crs}_{i^*}$ as input; we simulate honestly as in G_3 except that for all $\mathsf{pk}_{i^*} \in D_{i^*}$, we make an oracle query $[\mathbf{F}_{i^*}]_1$ and get $\widetilde{\pi}_{i^*}$ in it; we finally output $([\mathbf{F}_{i^*}^*]_1, \pi_{i^*}^*)$ in $\mathsf{pk}_{i^*}^* \notin D_{i^*}$. Observe that once it happens that $\mathbf{e}_1\widetilde{\mathbf{R}}_{i^*}^{-1}\mathbf{Q}_{i^*}^* \neq \mathbf{sT}_{i^*}^*$, we must have $\mathbf{F}_{i^*}^* \notin \mathsf{span}(\mathbf{A}_{i^*})$. When $\mathsf{pk}_{i^*}^* \in D_{i^*}$, we always have $\mathsf{G}_4 \equiv \mathsf{G}_3$.

– G_4: Identical to G_3 except that we replace all $\mathbf{sA}$ with $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$; in particular, we generate $\widehat{\mathbf{R}}$ as follows:

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix} \boxed{\mathbf{c}} \\ \mathbf{I}_{2k+1}\end{pmatrix}, \quad \widetilde{\mathbf{R}}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+2)}$$

and generate the challenge ciphertext as follows:

$$\mathsf{ct}^* = \Bigg(\Bigg[\underbrace{\boxed{\mathbf{c}}}_{\mathbf{c}_{+,0}^*}, \underbrace{\boxed{\mathbf{c}}\mathbf{W} + \mathbf{x}_b^*}_{\mathbf{c}_{+,1}^*}, \underbrace{\sum_{i\in[L]} (\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^* + \boxed{\mathbf{c}}\mathbf{W}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_1^*}\Bigg]_1\Bigg).$$

We have $\mathsf{G}_4 \approx_c \mathsf{G}_3$. This follows from MDDH assumption which ensures that $([\mathbf{A}]_1, [\mathbf{sA}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{c}]_1)$ when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}, \mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$.

– G_5: Identical to G_4 except that

- we generate $\mathbf{c}_{+,1}^*$ as follows:

$$\mathbf{c}_{+,1}^* = [\mathbf{cW} + \boxed{\mathbf{x}_0^*}]_1$$

- in crs, we make the following change for all $j \in [L]$:

$$[\mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{W} + \boxed{\mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)}]_2$$

where $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{cc}^\perp = 1$, $\mathbf{Ac}^\perp = \mathbf{0}$.

We have $\mathsf{G}_5 \approx_s \mathsf{G}_4$ which follows from the fact that we can utilize the change of variable $\mathbf{W} \mapsto \mathbf{W} + \mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)$.

– $\mathsf{G}_{6,\ell}(\ell \in [0,L])$: Identical to G_5 except that for all $j \in [\ell]$, we change $[\mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \boxed{\mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)}]_2$ in crs as follows:

$$[\mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{W} + \cancel{\mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)}]_2$$

We have that

- $\mathsf{G}_{6,0} = \mathsf{G}_5$; the two games are actually identical, since $[0] = \emptyset$;
- $\mathsf{G}_{6,\ell-1} \approx_c \mathsf{G}_{6,\ell}$ for all $\ell \in [L]$, we will employ a sub-sequence of games for the proof described later.

From $\mathsf{G}_{6,\ell-1}$ to $\mathsf{G}_{6,\ell}$. We are ready to prove $\mathsf{G}_{6,\ell-1} \approx_c \mathsf{G}_{6,\ell}$ and this will complete the proof of Lemma 5. For this, we need the following sub-sequence of games for each $\ell \in [L]$:

– $\mathsf{G}_{6,\ell-1,0}$: Identical to $\mathsf{G}_{6,\ell-1}$ where we recall crs, $\mathsf{pk}_i \in D_i$ and $\mathbf{c}_1^*$, with highlighting relevant terms in the following sub-sequence with dashed boxes as follows:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AW}]_1, \left\{\mathsf{crs}_i, [\widehat{\mathbf{R}}_i, \mathbf{AW}_i]_1\right\}_{i\in[L]} \\ \left\{[\mathbf{Br}_j^\top, \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{W}]_2\right\}_{j\in[\ell-1]} \\ \boxed{[\mathbf{Br}_\ell^\top, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{Br}_\ell^\top) + \mathbf{W} + \mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)]_2} \\ \left\{[\mathbf{Br}_j^\top, \mathbf{W}_j(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{W} + \mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)]_2\right\}_{j\in[L]\setminus[\ell]} \\ \left\{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{Br}_j^\top)]_2\right\}_{j\in[L]\setminus\{\ell\}, i\in[L]\setminus\{j\}}, \boxed{\left\{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{Br}_\ell^\top)]_2\right\}_{i\in[L]\setminus\{\ell\}}} \end{pmatrix}$$

$$\mathsf{pk}_i = \begin{cases} \Big([\overbrace{\mathbf{AU}_i}^{\mathbf{T}_i}, \overbrace{\widehat{\mathbf{R}}_i\mathbf{U}_i}^{\mathbf{Q}_i}]_1, \{[\overbrace{\mathbf{U}_i\mathbf{d}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j\in[\ell-1]\setminus\{i\}}, \boxed{[\overbrace{\mathbf{U}_i\mathbf{Br}_\ell^\top}^{\mathbf{h}_{i,\ell}}]_2}, \{[\overbrace{\mathbf{U}_i\mathbf{Br}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus[i,\ell]}, \widetilde{\pi}_i\Big) & \text{if } i \neq \ell \\ \Big([\underbrace{\mathbf{AU}_\ell}_{\mathbf{T}_\ell}, \underbrace{\widehat{\mathbf{R}}_i\mathbf{U}_\ell}_{\mathbf{Q}_\ell}]_1, \{[\underbrace{\mathbf{U}_\ell\mathbf{d}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j\in[\ell-1]}, \qquad \{[\underbrace{\mathbf{U}_\ell\mathbf{Br}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j\in[L]\setminus[\ell]}, \widetilde{\pi}_\ell\Big) & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_1^* = \boxed{\mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{cW}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1})} + \sum_{i\in[L]\setminus\{\ell\}} (\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^* + \mathbf{cW}_i((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1}))$$

where $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{cc}^\perp = 1$, $\mathbf{Ac}^\perp = \mathbf{0}$.

– $\mathsf{G}_{6,\ell-1,1}$: Identical to $\mathsf{G}_{6,\ell-1,0}$ except that we replace all $\mathbf{Br}_\ell^\top$ with $\mathbf{d}_\ell^\top \leftarrow \mathbb{Z}_p^{k+1}$ in crs; in particular, we change the dashed boxed term in crs and pk_i as follows:

$$[\boxed{\mathbf{d}_\ell^\top}, \mathbf{W}_\ell(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top}) + \mathbf{W} + \mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)]_2, \{[\mathbf{W}_i(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top})]_2, [\mathbf{U}_i\boxed{\mathbf{d}_\ell^\top}]_2\}_{i\in[L]\setminus\{\ell\}}$$

We have $\mathsf{G}_{6,\ell-1,1} \approx_c \mathsf{G}_{6,\ell-1,0}$. This follows from MDDH assumption w.r.t. $[\mathbf{B}]_2$ which ensures that $([\mathbf{B}]_2, [\mathbf{Br}_\ell^\top]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{d}_\ell^\top]_2)$ when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{r}_\ell \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{d}_\ell \leftarrow \mathbb{Z}_p^{1\times(k+1)}$.

– $\mathsf{G}_{6,\ell-1,2}$: Identical to $\mathsf{G}_{6,\ell-1,1}$, except that we make the following change of crs

$$[\mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{W} + \cancel{\mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)}]_2$$

We have $\mathsf{G}_{6,\ell-1,2} \approx_c \mathsf{G}_{6,\ell-1,1}$. With defining $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{cc}^\perp = 1$, $\mathbf{Ac}^\perp = \mathbf{0}$. We consider two cases

- Honest case: In this case, we have $\mathsf{pk}_\ell^* = ([\mathbf{T}_\ell^*, \mathbf{Q}_\ell^*]_1, \{[\mathbf{h}_{\ell,j}^{*\top}]_2\}_{j\in[L]\setminus\{\ell\}}, \pi_\ell^*) \in D_\ell \setminus C_\ell$. Namely, we know $\mathbf{U}_\ell^*$ (such that $\mathbf{T}_\ell^* = \mathbf{AU}_\ell^*$ and $\mathbf{Q}_\ell^* = \widehat{\mathbf{R}}_\ell\mathbf{U}_\ell^*$) and $\mathbf{U}_\ell^*$ is hidden from the adversary. We can write the dash boxed terms in $\mathbf{c}_1^*$ as follows:

$$\boxed{\mathbf{cU}_\ell^*} + \mathbf{cW}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1})$$

and replace $\widehat{\mathbf{R}}_\ell$ in crs with a random $\mathbf{R}_\ell$ as in G_2. And we can prove $\mathsf{G}_{6,\ell-1,2} \approx_c \mathsf{G}_{6,\ell-1,1}$ in this case using the following argument for all $b' \in \{0,1\}$:

$$\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{W} + b'\mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)]_2; \quad \text{//crs, pk}_\ell$$

$$[\mathbf{c}, \mathbf{c}\mathbf{U}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1})]_1, \mathbf{A}\mathbf{U}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^*]_1, \mathbf{U}_\ell^*\mathbf{B}; \quad \text{//ct}^*,\ \text{pk}_\ell^*$$

$$\approx_c \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{W} + b'\mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)]_2;$$

$$[\mathbf{c}, \mathbf{c}\mathbf{U}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1})]_1, \mathbf{A}\mathbf{U}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \boxed{\widehat{\mathbf{u}}^\top\mathbf{d}^\perp}]_1, \mathbf{U}_\ell^*\mathbf{B};$$

$$\approx_s \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{W} + \cancel{b'\mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)}];$$

$$[\mathbf{c}, \mathbf{c}\mathbf{U}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1}) + \boxed{u_\ell\mathbf{d}^\perp - b(\mathbf{x}_0^* - \mathbf{x}_b^*)(\mathbf{y}_\ell^*)^\top\mathbf{d}^\perp}]_1, \mathbf{A}\mathbf{U}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \boxed{\mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{d}^\perp} + \widehat{\mathbf{u}}^\top\mathbf{d}^\perp]_1, \mathbf{U}_\ell^*\mathbf{B};$$

$$\approx_s \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{W}]_2;$$

$$[\mathbf{c}, \mathbf{c}\mathbf{U}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1}) + u_\ell\mathbf{d}^\perp - \cancel{b'(\mathbf{x}_0^* - \mathbf{x}_b^*)(\mathbf{y}_\ell^*)^\top\mathbf{d}^\perp}]_1, \mathbf{A}\mathbf{U}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{d}^\perp + \widehat{\mathbf{u}}^\top\mathbf{d}^\perp]_1, \mathbf{U}_\ell^*\mathbf{B};$$

where $\widehat{\mathbf{u}} \leftarrow \mathbb{Z}_p^{1\times(2k+2)}$, $u_\ell \leftarrow \mathbb{Z}_p$, and $\mathbf{d}^\perp \in \mathbb{Z}_p^{1\times(k+1)}$ such that $\mathbf{d}^\perp\mathbf{d}_\ell^\top = 1$, $\mathbf{d}^\perp\mathbf{B} = \mathbf{0}$. We justify each step as below: The first $\approx_c$ follows the argument:

$$(\mathbf{A}, \mathbf{c}, [\mathbf{R}_\ell]_1, \mathbf{B}, \mathbf{d}^\perp, \mathbf{A}\mathbf{U}_\ell, \mathbf{c}\mathbf{U}_\ell[\mathbf{R}\mathbf{U}_\ell]_1, \qquad \mathbf{U}_\ell\mathbf{B})$$
$$\approx_c (\mathbf{A}, \mathbf{c}, [\mathbf{R}_\ell]_1, \mathbf{B}, \mathbf{d}^\perp, \mathbf{A}\mathbf{U}_\ell, \mathbf{c}\mathbf{U}_\ell, [\mathbf{R}_\ell\mathbf{U}_\ell + \boxed{\mathbf{u}^\top\mathbf{d}^\perp}]_1, \mathbf{U}_\ell\mathbf{B})$$

which is analogous to the Lemma 2 in [ZZGQ23]. The second $\approx_s$ uses the change of variables:

$$\mathbf{U}_\ell^* \mapsto \mathbf{U}_\ell^* + \mathbf{c}^\perp u_\ell\mathbf{d}^\perp \quad \text{and} \quad \mathbf{W}_\ell \mapsto \mathbf{W}_\ell - b'\mathbf{c}^\perp((\mathbf{x}_0^* - \mathbf{x}_b^*) \otimes \mathbf{d}^\perp)$$

The last $\approx_s$ is straight-forward with the observation that $\widehat{\mathbf{u}}^\top$ hides $\mathbf{R}_\ell\mathbf{c}^\perp u_\ell$, this implies that u_ℓ hides $b'(\mathbf{x}_0^* - \mathbf{x}_b^*)\mathbf{y}_\ell^{*\top}$.

- Corrupted & Malicious Case: In this case, we have $\mathsf{pk}_\ell^* = ([\mathbf{T}_\ell^*, \mathbf{Q}_\ell^*]_1, \{[\mathbf{h}_{\ell,j}^{*}{}^\top]_2\}_{j\in[L]\setminus\{\ell\}}, \pi_\ell^*) \in C_\ell \cup \overline{D}_\ell$. We prove $\mathsf{G}_{6,\ell-1,2} \approx_c \mathsf{G}_{6,\ell-1,1}$ in this case using the following argument:

$$\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{W} + \mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)]_2; \quad \text{//crs}$$

$$[\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1})]_1; \quad \text{//ct}^* \text{ in } \mathsf{G}_{6,\ell-1,1}$$

$$\approx_s \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{W} + \cancel{\mathbf{c}^\perp(\mathbf{x}_0^* - \mathbf{x}_b^*)}]_2;$$

$$[\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1}) + \boxed{(\mathbf{x}_0^* - \mathbf{x}_b^*)(\mathbf{y}_\ell^*)^\top\mathbf{d}^\perp}]_1;$$

$$\approx_s \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, [\mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{W}]_2; \quad \text{//crs}$$

$$[\mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{k+1}) + \cancel{(\mathbf{x}_0^* - \mathbf{x}_b^*)(\mathbf{y}_\ell^*)^\top\mathbf{d}^\perp}]_1; \quad \text{//ct}^* \text{ in } \mathsf{G}_{6,\ell-1,2}$$

We justify each step as follows: The first $\approx_s$ uses the change of variable:

$$\mathbf{W}_\ell \mapsto \mathbf{W}_\ell - \mathbf{c}^\perp((\mathbf{x}_0^* - \mathbf{x}_b^*) \otimes \mathbf{d}^\perp)$$

The second $\approx_s$ uses the fact that $(\mathbf{x}_0^* - \mathbf{x}_b^*)\mathbf{y}_\ell = 0$ in this case.

– $\mathsf{G}_{6,\ell-1,3}$: Identical to $\mathsf{G}_{6,\ell-1,2}$ except that we replace all $\mathbf{d}_\ell^\top$ with $\mathbf{B}\mathbf{r}_\ell^\top$ where $\mathbf{r}_\ell^\top \leftarrow \mathbb{Z}_p^k$ in crs; in particular, we change the dashed boxed term in crs and pk_i as follows:

$$[\boxed{\mathbf{B}\mathbf{r}_\ell^\top}, \mathbf{W}_\ell(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top}) + \mathbf{W}]_2, \{[\mathbf{W}_i(\mathbf{I}_n \otimes \boxed{\mathbf{B}\mathbf{r}_\ell^\top})]_2, [\mathbf{U}_i\boxed{\mathbf{B}\mathbf{r}_\ell^\top}]_2\}_{i\in[L]\setminus\{\ell\}}$$

We have $\mathsf{G}_{6,\ell-1,3} \approx_c \mathsf{G}_{6,\ell-1,2}$. This follows from MDDH assumption w.r.t. $[\mathbf{B}]_2$ which ensures that $([\mathbf{B}]_2, [\mathbf{B}\mathbf{r}_\ell^\top]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{d}_\ell^\top]_2)$ when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{r}_\ell \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{d}_\ell \leftarrow \mathbb{Z}_p^{1\times(k+1)}$.

7 Registered Quadratic Functional Encryption

In this section, we present our Reg-QFE scheme for the quadratic functionality which is defined by $X = \mathbb{Z}_p^{1\times n_1} \times \mathbb{Z}_p^{1\times n_2}$, $Z = \mathbb{Z}_p$ and

$$\mathsf{QF}_{n_1 n_2} = \{\mathbf{f} : (\mathbf{x}_1, \mathbf{x}_2) \mapsto (\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^\top\},$$

where $\mathbf{f} \in \mathbb{Z}_p^{1\times n_1 n_2}$. We first present the multi-instance slotted Reg-QFE by working on our multi-instance slotted PReg-IPFE scheme in Section 6; with the multi-instance Reg-QFE, we finally lead to the compact Reg-QFE which achieve the very selective SIM-security defined in Section 2.2.

7.1 Multi-instance slotted Reg-QFE

With the multi-instance slotted PReg-IPFE $\Pi_2 = (\mathsf{iSetup}, \mathsf{iGen}, \mathsf{iVer}, \mathsf{iAgg}_+, \mathsf{iAgg}, \mathsf{iEnc}_+, \mathsf{iEnc}, \mathsf{iDec})$ in Section 6, over prime-order bilinear group $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$; our multi-instance slotted Reg-QFE works as follows in the bilinear group $\mathbb{G}$:

– $\mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2})$: Sample $\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k\times n_1}$, $\mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k\times n_2}$. Set $n'_1 = k(n_1 + n_2 + k)$, $n'_2 = n_1 n_2$, run

$$\mathsf{icrs} \leftarrow \mathsf{iSetup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n'_1}, 1^{n'_2}, \mathbf{M}) \quad \text{where} \quad \mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I}_{n_2} \\ \mathbf{I}_{n_1} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}.$$

Output

$$\mathsf{crs} = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathsf{icrs})$$

– $\mathsf{Gen}(\mathsf{crs}, q, i)$: Sample $(\mathsf{ipk}_{q,i}, \mathsf{isk}_{q,i}) \leftarrow \mathsf{iGen}(\mathsf{icrs}, q, i)$, output

$$(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) = (\mathsf{ipk}_{q,i}, \mathsf{isk}_{q,i})$$

– $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i})$: Parse $\mathsf{pk}_{q,i} = \mathsf{ipk}_{q,i}$, output

$$\mathsf{iVer}(\mathsf{icrs}, q, i, \mathsf{ipk}_{q,i}).$$

– $\mathsf{Agg}_+(\mathsf{crs})$: Sample $\mathsf{impk}_+ \leftarrow \mathsf{iAgg}_+(\mathsf{icrs})$, output

$$\mathsf{mpk}_+ = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathsf{impk}_+).$$

– $\mathsf{Agg}(\mathsf{crs}, q, (\mathsf{pk}_{q,i}, \mathbf{f}_{q,i})_{i\in[L_q]})$: If q is an empty instance, namely $(\mathsf{pk}_{q,i}, \mathbf{f}_{q,i}) = (\perp, \perp)$ for all $i \in [L_q]$, abort and return $\mathsf{mpk}_q = \perp$, $\mathsf{hsk}_{q,j} = \perp$ for all $j \in [L_q]$. Sample $(\mathsf{impk}_q, (\mathsf{ihsk}_{q,j})_{j\in[L_q]}) \leftarrow \mathsf{iAgg}(\mathsf{icrs}, q, (\mathsf{ipk}_{q,i}, \mathbf{f}_{q,i})_{i\in[L_q]})$, output

$$\mathsf{mpk}_q = \mathsf{impk}_q,$$

and for all $j \in [L_q]$

$$\mathsf{hsk}_{q,j} = \mathsf{ihsk}_{q,j}.$$

– $\mathsf{Enc}_+(\mathsf{mpk}_+, (\mathbf{x}_1, \mathbf{x}_2))$: Sample $\mathbf{s}_1, \mathbf{s}_2 \leftarrow \mathbb{Z}_p^{1\times k}$. Run

$$\mathsf{ict}_+ \leftarrow \mathsf{iEnc}_+((\mathsf{impk}_+, \mathbf{x}),$$

where $\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$. Output

$$\mathsf{ct}_+ = ([\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2}_{\mathbf{y}_2}]_2, \mathsf{ict}_+)$$

– $\mathsf{Enc}(\mathsf{mpk}_q)$: Abort and return $\mathsf{ct}_q = \perp$ if $\mathsf{mpk}_q = \perp$. Run

$$\mathsf{ict}_q \leftarrow \mathsf{iEnc}(\mathsf{impk}_q),$$

Output

$$\mathsf{ct}_q = \mathsf{ict}_q.$$

– $\mathsf{Dec}(\mathsf{sk}_{q^*,i^*}, \mathsf{hsk}_{q^*,i^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*}))$: Abort and return $\perp$ if $\mathsf{ict}_{q^*} = \perp$. Parse

$$\mathsf{sk}_{q^*,i^*} = \mathsf{isk}_{q^*,i^*}, \quad \mathsf{hsk}_{q^*,i^*} = \mathsf{ihsk}_{q^*,i^*}, \quad (\mathsf{ct}_+, \mathsf{ct}_{q^*}) = ([\mathbf{y}_1]_1, [\mathbf{y}_2]_2, \mathsf{ict}_+, \mathsf{ict}_{q^*}).$$

Compute

$$[z]_T = [(\mathbf{y}_1 \otimes \mathbf{y}_2)\mathbf{f}^{\top}_{q^*,i^*} - \mathsf{iDec}(\mathsf{isk}_{q^*,i^*}, \mathsf{ihsk}_{q^*,i^*}, (\mathsf{ict}_s, \mathsf{ict}_{q^*}))]_T$$

Recover z from $[z]_T$ via brute-force DLOG and output z.

Completeness. For all $\lambda, m, n_1, n_2 \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $q \in [m]$ and $i \in [L_q]$; all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2})$, and $(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q, i)$, we have

$$\mathsf{crs} = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathsf{icrs}) \quad \text{and} \quad (\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) = (\mathsf{ipk}_{q,i}, \mathsf{isk}_{q,i})$$

where $(\mathsf{ipk}_{q,i}, \mathsf{isk}_{q,i}) \leftarrow \mathsf{iGen}(\mathsf{icrs}, q, i)$ and $\mathsf{icrs} \leftarrow \mathsf{iSetup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n'_1}, 1^{n'_2}, \mathbf{M})$, with $n'_1 = k(n_1 + n_2 + k)$, $n'_2 = n_1 n_2$. With the completeness of Π_2 (c.f. Section 6.1), we have $\mathsf{iVer}(\mathsf{icrs}, q, i, \mathsf{ipk}_{q,i}) = 1$. This ensures that $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i}) = 1$ by the specification of Ver and readily proves the completeness.

Correctness. For all $\lambda, m, n_1, n_2 \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $q^* \in [m]$ and $i^* \in [L_{q^*}]$; all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2})$, all $(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q^*, i^*)$; all $(\mathbf{x}_1, \mathbf{x}_2) \in \mathbb{Z}_p^{1\times n_1} \times \mathbb{Z}_p^{1\times n_2}$ and $\mathbf{f}_{q^*,i} \in \mathbb{Z}_p^{1\times n_1 n_2}$; we have:

$$\begin{aligned}
(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) &= (\mathsf{ipk}_{q^*,i^*}, \mathsf{isk}_{q^*,i^*}) \\
\mathsf{hsk}_{q^*,i^*} &= \mathsf{ihsk}_{q^*,i^*} \\
(\mathsf{ct}_+, \mathsf{ct}_{q^*}) &= ([\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2}_{\mathbf{y}_2}]_2, \mathsf{ict}_+, \mathsf{ict}_{q^*})
\end{aligned}$$

where

$$\begin{aligned}
\mathsf{ict}_+ &\leftarrow \mathsf{iEnc}_+(\mathsf{impk}_+, \mathbf{x}; s) \\
\mathsf{ict}_{q^*} &\leftarrow \mathsf{iEnc}(\mathsf{impk}_{q^*}; s) \\
\mathsf{impk}_+ &\leftarrow \mathsf{iAgg}_+(\mathsf{icrs}) \\
(\mathsf{impk}_{q^*}, \mathsf{ihsk}_{q^*,i^*}) &\in \mathsf{iAgg}(\mathsf{icrs}, q^*, (\mathsf{pk}_{q^*,i}, \mathbf{f}_{q^*,i})_{i\in[L_{q^*}]}) \\
(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) &\leftarrow \mathsf{iGen}(\mathsf{icrs}, q^*, i^*) \\
\mathsf{icrs} &\leftarrow \mathsf{iSetup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n'_1}, 1^{n'_2}, \mathbf{M})
\end{aligned}$$

with $n'_1 = k(n_1 + n_2 + k)$, $n'_2 = n_1 n_2$ and $s \leftarrow \mathsf{Coin}$. Note that all above equalities are ensured by the specification of Ver. We have

$$\begin{aligned}
z &= ((\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2))\mathbf{f}^{\top}_{q^*,i^*} - \mathsf{iDec}(\mathsf{isk}_{q^*,i^*}, \mathsf{ihsk}_{q^*,i^*}, (\mathsf{ict}_s, \mathsf{ict}_{q^*})) \\
&= ((\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2))\mathbf{f}^{\top}_{q^*,i^*} - \mathbf{x}\mathbf{M}\mathbf{f}^{\top}_{q^*,i^*} \qquad (24) \\
&= (\mathbf{s}_1\mathbf{A}_1 \otimes \mathbf{s}_2\mathbf{A}_2 + \mathbf{s}_1\mathbf{A}_1 \otimes \mathbf{x}_2 + \mathbf{x}_1 \otimes \mathbf{s}_2\mathbf{A}_2)\mathbf{f}^{\top}_{q^*,i^*} + (\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^{\top}_{q^*,i^*} - \mathbf{x}\mathbf{M}\mathbf{f}^{\top}_{q^*,i^*} \\
&= (\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^{\top}_{q^*,i^*} \qquad (25)
\end{aligned}$$

where equality (24) follows from the correctness of Π_2, which is ensure by iVer and iGen; equality (25) follows from the fact that $\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I}_{n_2} \\ \mathbf{I}_{n_1} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}$ and $\mathbf{x} = (\mathbf{s}_1 \otimes \mathbf{x}_2 \| \mathbf{x}_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$. This proves the correctness.

Compactness and Efficiency. Our multi-instance slotted Reg-QFE has the following properties:

$$\begin{aligned} |\mathsf{crs}| &= O(L^2 \cdot n^2) \cdot \mathsf{poly}(\lambda), & |\mathsf{hsk}_{q,j}| &= O(n) \cdot \mathsf{poly}(\lambda), \\ |\mathsf{mpk}_+| &= O(n) \cdot \mathsf{poly}(\lambda), & |\mathsf{mpk}_q| &= \mathsf{poly}(\lambda), \\ |\mathsf{ct}_+| &= O(n) + \mathsf{poly}(\lambda), & |\mathsf{ct}_q| &= \mathsf{poly}(\lambda), \end{aligned}$$

where $L = L_1 + \cdots + L_m$, $n = n_1 + n_2$.

Security. We have the following theorem. Given multi-instance slotted PReg-IPFE with very selective SIM-security under MDDH assumption, our multi-instance slotted Reg-QFE scheme uses prime-order bilinear group and the security can be reduced to bi-MDDH assumption.

Theorem 6. *Assume* $\Pi_2 = (\mathsf{iSetup}, \mathsf{iGen}, \mathsf{iVer}, \mathsf{iAgg}_+, \mathsf{iAgg}, \mathsf{iEnc}_+, \mathsf{iEnc}, \mathsf{iDec})$ *is a multi-instance slotted PReg-IPFE with completeness, correctness, very selective SIM-security and has group-based simulator defined in Section 6, our multi-instance slotted Reg-QFE scheme achieves the very selective SIM-security, under bi-MDDH assumption.*

7.2 Simulator

Recall that we allow some instance q^* to be empty, namely $\mathcal{M}^*_{q^*}, C^*_{q^*} = \emptyset$ and $\mathbf{f}_{q^*,i} = \perp$, $\mathsf{pk}_{q^*,i} = \perp$ for all $i \in [L_{q^*}]$. Let $(\widetilde{\mathsf{iSetup}}, \widetilde{\mathsf{iGen}}, \widetilde{\mathsf{iEnc}}_+, \widetilde{\mathsf{iEnc}})$ be the group-based simulator of multi-instance slotted PReg-IPFE Π_2, the simulator of our multi-instance slotted Reg-QFE is as follows:

- $\widetilde{\mathsf{Setup}}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2}, \{\{\mathbf{f}_{q,i}\}_{i \in [L_q]}, \{\mu_{q,i}\}_{\mathcal{M}^*_q \cup C^*_q}\}_{q \in [m]})$: Sample
$$\widetilde{\mathbf{y}}_1 \leftarrow \mathbb{Z}_p^{1 \times n_1},\ \widetilde{\mathbf{y}}_2 \leftarrow \mathbb{Z}_p^{1 \times n_2},\ \mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k \times n_1},\ \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n_2}$$
Set $n'_1 = k(n_1 + n_2 + k)$, $n'_2 = n_1 n_2$ and $\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I}_{n_1} \\ \mathbf{I}_{n_2} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}$, run
$(\widetilde{\mathsf{icrs}}, \mathsf{itd}) \leftarrow \widetilde{\mathsf{iSetup}}(1^\lambda, 1^m, \{1^{L_q}\}_{q \in [m]}, 1^{n'_1}, 1^{n'_2}, \{[\mathbf{M}]_s\}_{s \in \{1,2\}}; \{\{\mathbf{f}_{q,i}\}_{i \in [L_q]}, \{\{[(\widetilde{\mathbf{y}}_1 \otimes \widetilde{\mathbf{y}}_2)\mathbf{f}^\top_{q,i} - \mu_{q,i}]_s\}_{s \in \{1,2\}}\}_{i \in \mathcal{M}^*_q \cup C^*_q}\}_{q \in [m]})$
Output
$$\widetilde{\mathsf{crs}} = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \widetilde{\mathsf{icrs}})$$
And set $\mathsf{td} = (\mathbf{y}_1, \mathbf{y}_2, \mathsf{itd})$.
- $\widetilde{\mathsf{Gen}}(\widetilde{\mathsf{crs}}, q, i; \mathsf{td})$: Fetch itd from td, sample $(\widetilde{\mathsf{ipk}}_{q,i}, \widetilde{\mathsf{isk}}_{q,i}) \leftarrow \widetilde{\mathsf{iGen}}(\widetilde{\mathsf{icrs}}, q, i; \mathsf{itd})$, output
$$(\widetilde{\mathsf{pk}}_{q,i}, \widetilde{\mathsf{sk}}_{q,i}) = (\widetilde{\mathsf{ipk}}_{q,i}, \widetilde{\mathsf{isk}}_{q,i})$$
- $\widetilde{\mathsf{Enc}}_+(\mathsf{td})$: Parse $\mathsf{td} = (\widetilde{\mathbf{y}}_1, \widetilde{\mathbf{y}}_2, \mathsf{itd})$, sample $\widetilde{\mathsf{ict}}_+ \leftarrow \widetilde{\mathsf{iEnc}}_+(\mathsf{itd})$. Output
$$\widetilde{\mathsf{ct}}_+ = ([\widetilde{\mathbf{y}}_1]_1, [\widetilde{\mathbf{y}}_2]_2, \widetilde{\mathsf{ict}}_+),$$
- $\widetilde{\mathsf{Enc}}((\mathsf{pk}_{q,1}, \ldots, \mathsf{pk}_{q,L_q}); \mathsf{td})$: If q is an empty instance, on input $\mathsf{pk}_{q,i} = \perp$ for all $i \in [L_q]$, abort and return $\widetilde{\mathsf{ct}}_q = \perp$. For all $i \in [L_q]$, parse $\mathsf{pk}_{q,i} = \mathsf{ipk}_{q,i}$. Fetch itd from td, sample $\widetilde{\mathsf{ict}}_q \leftarrow \widetilde{\mathsf{iEnc}}((\mathsf{ipk}_{q,1}, \ldots, \mathsf{ipk}_{q,L_q}); \mathsf{itd})$. Output
$$\widetilde{\mathsf{ct}}_q = \widetilde{\mathsf{ict}}_q.$$

The reader can find the sanity check in Appendix D.

7.3 Proof

We prove the following technical lemma this immediately proves Theorem 6.

Lemma 6. *For all adversaries $\mathcal{A}$, there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ such that:*

$$\mathsf{Adv}^{\textit{miReg-QFE}}_{\mathcal{A}}(\lambda) \leq L \cdot \mathsf{Adv}^{\textit{miPReg-IPFE}}_{\mathcal{B}_1}(\lambda) + 2 \cdot \mathsf{Adv}^{\textit{bi-MDDH}}_{\mathcal{B}_2}(\lambda) + \mathsf{negl}(\lambda)$$

where $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2) \approx \mathsf{Time}(\mathcal{A})$.

For simplicity, we prove Lemma 6 in the case that all instances are not empty. For empty instance q^*, we simply change $\mathsf{ct}^*_{q^*}$ and $\mathsf{pk}^*_{q^*,i}$ to $\perp$, and we have $\mathcal{M}^*_{q^*}, \mathcal{C}^*_{q^*} = \emptyset$ in following game sequence.

Game Sequence. Suppose that crs is the common reference string, $(\mathbf{x}^*_1, \mathbf{x}^*_2)$ is the challenge; for each instance $q \in [m]$, $\{\mathsf{pk}^*_{q,i}, \mathbf{f}^*_{q,i}\}_{i\in[L_q]}$ are challenge public keys along with challenge functions to be registered, and $\mathcal{M}^*_q, \mathcal{C}^*_q \subseteq [L_q]$ are the sets of malicious and corrupted slots. For all $q \in [m]$, $i \in [L_q]$, define $D_{q,i} = \{\mathsf{pk}_{q,i} : \mathcal{D}_{q,i}[\mathsf{pk}_{q,i}] = \mathsf{sk}_{q,i} \neq \perp\}$ be responses to $\mathsf{OGen}(q,i)$ and $C_{q,i} = \{\mathsf{pk}_{q,i} : (i, \mathsf{pk}_{q,i}) \in \mathcal{C}_q\}$ records public keys in D_i that have been sent to $\mathsf{OCor}(q,i,\cdot)$. Recall that, for each $q \in [m]$, $i \in [L_q]$, we require that

$$\begin{aligned} i \in \mathcal{M}^*_q &\implies \mathsf{pk}^*_{q,i} \notin D_{q,i} \wedge \mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}^*_{q,i}) = 1 \\ i \in \mathcal{C}^*_q &\implies \mathsf{pk}^*_{q,i} \in C_{q,i} \\ i \in [L_q] \setminus (\mathcal{M}^*_q \cup \mathcal{C}^*_q) &\implies \mathsf{pk}^*_{q,i} \in D_{q,i} \wedge \mathsf{pk}^*_i \notin C_{q,i} \end{aligned}$$

Note that $\mathsf{pk}_{q,i}$ serves as a *general* entry in $D_{q,i}$ while $\mathsf{pk}^*_{q,i}$ is the *specific* challenge public for slot i in instance q; there can be more than one assignments for $\mathsf{pk}_{q,i}$ since the adversary can invoke $\mathsf{OGen}(q,i)$ (or $\widetilde{\mathsf{OGen}}(q,i)$) for many times. We prove Lemma 6 using the following game sequence.

- G_0: This is the real game, recall that we have
  - crs is in the form of
    $$\mathsf{crs} = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathsf{icrs})$$
    where
    $$\mathsf{icrs} \leftarrow \mathsf{iSetup}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n'_1}, 1^{n'_2}, \mathbf{M}),$$
    with $n'_1 = k(n_1 + n_2 + k)$, $n'_2 = n_1 n_2$ and $\mathbf{M} = \begin{pmatrix} \mathbf{A}_1 \otimes \mathbf{I}_{n_2} \\ \mathbf{I}_{n_1} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2 \end{pmatrix}$.
  - For each $q \in [m]$, $i \in [L_q]$, each $\mathsf{pk}_{q,i} \in D_{q,i}$ and its corresponding $\mathsf{sk}_{q,i}$ are
    $$(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) = (\mathsf{ipk}_{q,i}, \mathsf{isk}_{q,i}) \quad \text{where} \quad (\mathsf{ipk}_{q,i}, \mathsf{isk}_{q,i}) \leftarrow \mathsf{iGen}(\mathsf{icrs}, q, i)$$
  - $(\mathsf{ct}^*_+, (\mathsf{ct}^*_q)_{q\in[m]})$ for $(\mathbf{x}^*_1, \mathbf{x}^*_2)$ is in the form:
    $$(\mathsf{ct}^*_+, (\mathsf{ct}^*_q)_{q\in[m]}) = ([\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1}_{\mathbf{y}^*_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}^*_2}_{\mathbf{y}^*_2}]_2, \mathsf{ict}^*_+, (\mathsf{ict}^*_q)_{q\in[m]})$$
    where $\mathsf{ict}^*_+ \leftarrow \mathsf{iEnc}(\mathsf{impk}_+, \mathbf{x}^*; s)$, $\mathsf{ict}^*_q \leftarrow \mathsf{iEnc}(\mathsf{impk}_q; s)$ with $\mathbf{x}^* = (\mathbf{s}_1 \otimes \mathbf{x}^*_2 \| \mathbf{x}^*_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)$ and $s \leftarrow \mathsf{Coin}$.
- G_1: Identical to G_0, except that we replace $(\mathsf{iSetup}, \mathsf{iGen}, \mathsf{iEnc}_+, \mathsf{iEnc})$ with $(\widetilde{\mathsf{iSetup}}, \widetilde{\mathsf{iGen}}, \widetilde{\mathsf{iEnc}}_+, \widetilde{\mathsf{iEnc}})$. In particular:

- crs is generated as

$$\mathsf{crs} = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \boxed{\widetilde{\mathsf{icrs}}})$$

where

$$(\widetilde{\mathsf{icrs}}, \mathsf{itd}) \leftarrow \boxed{\widetilde{\mathsf{iSetup}}}(1^\lambda, 1^m, \{1^{L_q}\}_{q\in[m]}, 1^{n_1'}, 1^{n_2'}, \{[\mathbf{M}]_s\}_{s\in\{1,2\}}; \{\{\mathbf{f}^*_{q,i}\}_{i\in[L_q]}, \{\{[\theta^*_{q,i}]_s\}_{s\in\{1,2\}}\}_{i\in\mathcal{M}^*_q\cup\mathcal{C}^*_q}\}_{q\in[m]})$$

with $\theta^*_{q,i} = \mathbf{x}^*\mathbf{M}(\mathbf{f}^*_{q,i})^\top$.

- For each $q \in [m]$, $i \in [L_q]$, each $\mathsf{pk}_{q,i} \in D_{q,i}$ and its corresponding $\mathsf{sk}_{q,i}$ are generated as

$$(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) = (\boxed{\widetilde{\mathsf{ipk}}_{q,i}, \widetilde{\mathsf{isk}}_{q,i}}) \quad \text{where} \quad (\widetilde{\mathsf{ipk}}_{q,i}, \widetilde{\mathsf{isk}}_{q,i}) \leftarrow \boxed{\widetilde{\mathsf{iGen}}}(\widetilde{\mathsf{icrs}}, q, i; \mathsf{itd})$$

- $(\mathsf{ct}^*_+, (\mathsf{ct}^*_q)_{q\in[m]})$ for $(\mathbf{x}^*_1, \mathbf{x}^*_2)$ is in the form:

$$(\mathsf{ct}^*_+, (\mathsf{ct}^*_q)_{q\in[m]}) = ([\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1}_{\mathbf{y}^*_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}^*_2}_{\mathbf{y}^*_2}]_2, \boxed{\widetilde{\mathsf{ict}}^*_+, (\widetilde{\mathsf{ict}}^*_q)_{q\in[m]}})$$

where $\widetilde{\mathsf{ict}}^*_+ \leftarrow \boxed{\widetilde{\mathsf{iEnc}}_+}(\mathsf{itd})$ and $\widetilde{\mathsf{ict}}^*_q \leftarrow \boxed{\widetilde{\mathsf{iEnc}}}((\mathsf{ipk}^*_{q,i}, \ldots, \mathsf{ipk}^*_{q,L_q}); \mathsf{itd})$.

We have $\mathsf{G}_1 \approx_c \mathsf{G}_0$. This follows from the very selective SIM-security of Π_2 with the group-based simulator.

– G_2: Identical to G_1, except that we replace $\widetilde{\mathsf{icrs}}$ in crs with

$$\widetilde{\mathsf{icrs}} \in \widetilde{\mathsf{iSetup}}(1^\lambda, 1^m, \{1^{L_q}\}_{q\in[m]}, 1^{n_1'}, 1^{n_2'}, \{[\mathbf{M}]_s\}_{s\in\{1,2\}}; \{\{\mathbf{f}^*_{q,i}\}_{i\in[L_q]}, \{\{[\boxed{\theta^*_{q,i}}]_s\}_{s\in\{1,2\}}\}_{i\in\mathcal{M}^*_q\cup\mathcal{C}^*_q}\}_{q\in[m]})$$

where

$$\theta^*_{q,i} = \boxed{(\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1) \otimes (\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1)(\mathbf{f}^*_{q,i})^\top - (\mathbf{x}^*_1 \otimes \mathbf{x}^*_2)(\mathbf{f}^*_{q,i})^\top}$$

We have $\mathsf{G}_2 \equiv \mathsf{G}_1$. This follows from the fact that

$$\begin{aligned}\mathbf{x}^*\mathbf{M} &= (\mathbf{s}_1 \otimes \mathbf{x}^*_2 \| \mathbf{x}^*_1 \otimes \mathbf{s}_2 \| \mathbf{s}_1 \otimes \mathbf{s}_2)\begin{pmatrix}\mathbf{A}_1 \otimes \mathbf{I}_{n_2} \\ \mathbf{I}_{n_1} \otimes \mathbf{A}_2 \\ \mathbf{A}_1 \otimes \mathbf{A}_2\end{pmatrix} \\ &= (\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1) \otimes (\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1) - (\mathbf{x}^*_1 \otimes \mathbf{x}^*_2)\end{aligned}$$

– G_3: Identical to G_2, except that we replace all $\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1$ with $\widetilde{\mathbf{y}}_1 \leftarrow \mathbb{Z}_p^{n_1}$. In particular, we have

$$\widetilde{\mathsf{icrs}} \in \widetilde{\mathsf{iSetup}}(1^\lambda, 1^m, \{1^{L_q}\}_{q\in[m]}, 1^{n_1'}, 1^{n_2'}, \{[\mathbf{M}]_s\}_{s\in\{1,2\}}; \{\{\mathbf{f}^*_{q,i}\}_{i\in[L_q]}, \{\{[\boxed{\theta^*_{q,i}}]_s\}_{s\in\{1,2\}}\}_{i\in\mathcal{M}^*_q\cup\mathcal{C}^*_q}\}_{q\in[m]})$$

where

$$[\theta^*_{q,i}]_s = [(\boxed{\widetilde{\mathbf{y}}_1}) \otimes (\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1)(\mathbf{f}^*_{q,i})^\top - (\mathbf{x}^*_1 \otimes \mathbf{x}^*_2)(\mathbf{f}^*_{q,i})^\top]_s \quad (\forall s \in \{1,2\})$$

And we have

$$\mathsf{ct}^*_+ = ([\boxed{\widetilde{\mathbf{y}}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}^*_2}_{\mathbf{y}_2}]_2, \widetilde{\mathsf{ict}}^*_+)$$

We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from the bi-MDDH assumption w.r.t. $\mathbf{A}_1$ which ensure that $([\mathbf{A}_1]_1, [\mathbf{A}_1]_2, [\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1]_1, [\mathbf{s}_1\mathbf{A}_1 + \mathbf{x}^*_1]_2) \approx_c ([\mathbf{A}_1]_1, [\mathbf{A}_1]_2, [\widetilde{\mathbf{y}}_1]_1, [\widetilde{\mathbf{y}}_1]_2)$ when $\mathbf{s}_1 \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k\times n_1}$, $\mathbf{x}_1, \widetilde{\mathbf{y}}_1 \leftarrow \mathbb{Z}_p^{1\times n_1}$.

– G_4: Identical to G_3, except that we replace all $\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}^*_2$ with $\widetilde{\mathbf{y}}_2 \leftarrow \mathbb{Z}_p^{n_2}$. In particular, we have

$$\widetilde{\mathsf{icrs}} \in \widetilde{\mathsf{iSetup}}(1^\lambda, 1^m, \{1^{L_q}\}_{q\in[m]}, 1^{n_1'}, 1^{n_2'}, \{[\mathbf{M}]_s\}_{s\in\{1,2\}}; \{\{\mathbf{f}^*_{q,i}\}_{i\in[L_q]}, \{\{[\boxed{\theta^*_{q,i}}]_s\}_{s\in\{1,2\}}\}_{i\in\mathcal{M}^*_q\cup\mathcal{C}^*_q}\}_{q\in[m]})$$

where

$$[\theta^*_{q,i}]_s = [(\widetilde{\mathbf{y}}_1 \otimes \boxed{\widetilde{\mathbf{y}}_2})(\mathbf{f}^*_{q,i})^\top - (\mathbf{x}^*_1 \otimes \mathbf{x}^*_2)(\mathbf{f}^*_{q,i})^\top]_s \quad (\forall s \in \{1,2\})$$

And we have

$$\mathsf{ct}_+^* = ([\widetilde{\mathbf{y}}_1]_1, [\boxed{\widetilde{\mathbf{y}}_2}]_2, \widetilde{\mathsf{ict}}_+^*)$$

We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from the bi-MDDH assumption w.r.t. $\mathbf{A}_1$ which ensure that $([\mathbf{A}_2]_1, [\mathbf{A}_2]_2, [\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2^*]_1, [\mathbf{s}_2\mathbf{A}_2 + \mathbf{x}_2^*]_2) \approx_c ([\mathbf{A}_2]_1, [\mathbf{A}_2]_2, [\widetilde{\mathbf{y}}_2]_1, [\widetilde{\mathbf{y}}_2]_2)$ when $\mathbf{s}_2 \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k\times n_2}$, $\mathbf{x}_2, \widetilde{\mathbf{y}}_2 \leftarrow \mathbb{Z}_p^{1\times n_2}$.

Observe that in the final game G_4 can be simulated using the simulator by setting $\mu_{q,i} = (\mathbf{x}_1^* \otimes \mathbf{x}_2^*)(\mathbf{f}_{q,i}^*)^\top$

References

ABDP15. Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval. Simple functional encryption schemes for inner products. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 733–751. Springer, Heidelberg, March / April 2015. 4

AJJM22. Prabhanjan Ananth, Abhishek Jain, Zhengzhong Jin, and Giulio Malavolta. Pre-constrained encryption. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 4:1–4:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. 3

ALS16. Shweta Agrawal, Benoît Libert, and Damien Stehlé. Fully secure functional encryption for inner products, from standard assumptions. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 333–362. Springer, Heidelberg, August 2016. 9, 10

AMY19. Shweta Agrawal, Monosij Maitra, and Shota Yamada. Attribute based encryption for deterministic finite automata from DLIN. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part II*, volume 11892 of *LNCS*, pages 91–117. Springer, Heidelberg, December 2019. 11

BB04. Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 443–459. Springer, Heidelberg, August 2004. 2

BF01. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Heidelberg, August 2001. 2

CES21. Kelong Cong, Karim Eldefrawy, and Nigel P. Smart. Optimizing registration based encryption. *IACR Cryptol. ePrint Arch.*, page 499, 2021. 2

CGKW18. Jie Chen, Junqing Gong, Lucas Kowalczyk, and Hoeteck Wee. Unbounded ABE via bilinear entropy expansion, revisited. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 503–534. Springer, Heidelberg, April / May 2018. 3, 6, 8, 22, 50

CGW15. Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Heidelberg, April 2015. 10

CGW18. Jie Chen, Junqing Gong, and Hoeteck Wee. Improved inner-product encryption with adaptive security and full attribute-hiding. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 673–702. Springer, Heidelberg, December 2018. 3, 6, 8

DKL+23. Nico Döttling, Dimitris Kolonelos, Russell W. F. Lai, Chuanwei Lin, Giulio Malavolta, and Ahmadreza Rahimi. Efficient laconic cryptography from learning with errors. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 417–446. Springer, Heidelberg, April 2023. 2

DP23. Pratish Datta and Tapas Pal. Registration-based functional encryption. Cryptology ePrint Archive, Paper 2023/457, 2023. `https://eprint.iacr.org/archive/2023/457/20230330:055744`. 1, 2, 3, 4, 8, 14, 18

DPY23. Pratish Datta, Tapas Pal, and Shota Yamada. Registered fe beyond predicates: (attribute-based) linear functions and more. Cryptology ePrint Archive, Paper 2023/457, 2023. `https://eprint.iacr.org/2023/457`. 4

EHK+13. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013. 14

FFM+23. Danilo Francati, Daniele Friolo, Monosij Maitra, Giulio Malavolta, Ahmadreza Rahimi, and Daniele Venturi. Registered (inner-product) functional encryption. Asiacrypt 2023, 2023. https://eprint.iacr.org/2023/395. 1, 2, 3, 4, 8, 14, 18

FKdP23. Dario Fiore, Dimitris Kolonelos, and Paola de Perthuis. Cuckoo commitments: Registration-based encryption and key-value map commitments for large spaces. Cryptology ePrint Archive, Paper 2023/1389, 2023. https://eprint.iacr.org/2023/1389. 3

FWW23. Cody Freitag, Brent Waters, and David J. Wu. How to use (plain) witness encryption: Registered abe, flexible broadcast, and more. CRYPTO 2023, 2023. https://eprint.iacr.org/2023/812. 2

GHM+19. Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, Ahmadreza Rahimi, and Sruthi Sekar. Registration-based encryption from standard assumptions. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 63–93. Springer, Heidelberg, April 2019. 2

GHMR18. Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, and Ahmadreza Rahimi. Registration-based encryption: Removing private-key generator from IBE. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018, Part I*, volume 11239 of *LNCS*, pages 689–718. Springer, Heidelberg, November 2018. 2, 4, 8

GKMR22. Noemi Glaeser, Dimitris Kolonelos, Giulio Malavolta, and Ahmadreza Rahimi. Efficient registration-based encryption. Cryptology ePrint Archive, Report 2022/1505, 2022. https://eprint.iacr.org/2022/1505. 2

GV20. Rishab Goyal and Satyanarayana Vusirikala. Verifiable registration-based encryption. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 621–651. Springer, Heidelberg, August 2020. 2

HLWW23. Susan Hohenberger, George Lu, Brent Waters, and David J. Wu. Registered attribute-based encryption. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 511–542. Springer, Heidelberg, April 2023. 2, 4, 6, 8, 10, 16, 18, 31, 33, 66

HMQS23. Mohammad Hajiabadi, Mohammad Mahmoody, Wei Qi, and Sara Sarfaraz. Lower bounds on assumptions behind registration-based encryption. In Guy N. Rothblum and Hoeteck Wee, editors, *Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part II*, volume 14370 of *Lecture Notes in Computer Science*, pages 306–334. Springer, 2023. 4

JR13. Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, Heidelberg, December 2013. 17

KW15. Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, April 2015. 17, 22, 40, 50, 69, 79

LL20. Huijia Lin and Ji Luo. Compact adaptively secure ABE from k-Lin: Beyond NC^1 and towards NL. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 247–277. Springer, Heidelberg, May 2020. 12

LV16. Huijia Lin and Vinod Vaikuntanathan. Indistinguishability obfuscation from DDH-like assumptions on constant-degree graded encodings. In Irit Dinur, editor, *57th FOCS*, pages 11–20. IEEE Computer Society Press, October 2016. 12

LW11. Allison B. Lewko and Brent Waters. Unbounded HIBE and attribute-based encryption. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 547–567. Springer, 2011. 6

MQ23. Mohammad Mahmoody and Wei Qi. Online mergers and applications to registration-based encryption and accumulators. In Kai-Min Chung, editor, *4th Conference on Information-Theoretic Cryptography, ITC 2023, June 6-8, 2023, Aarhus University, Aarhus, Denmark*, volume 267 of *LIPIcs*, pages 15:1–15:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. 4

MQR22. Mohammad Mahmoody, Wei Qi, and Ahmadreza Rahimi. Lower bounds for the number of decryption updates in registration-based encryption. Cryptology ePrint Archive, Paper 2022/1285, 2022. https://eprint.iacr.org/2022/1285. 3

OT12. Tatsuaki Okamoto and Katsuyuki Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 591–608. Springer, Heidelberg, April 2012. 3, 6, 8

Wat05. Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer, Heidelberg, May 2005. 2

Wee20. Hoeteck Wee. Functional encryption for quadratic functions from *k*-lin, revisited. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part I*, volume 12550 of *LNCS*, pages 210–228. Springer, Heidelberg, November 2020. 8, 9

ZZGQ23. Ziqi Zhu, Kai Zhang, Junqing Gong, and Haifeng Qian. Registered abe via predicate encodings. In *Asiacrypt*, 2023. 2, 3, 4, 5, 6, 10, 17, 46, 54, 74, 86

Appendix

A Pre-constrained Reg-FE

In this section, we give the definition of pre-constrained Reg-FE for general functionality and its slotted variant.

A.1 Pre-Constrained Reg-FE

Algorithms. A pre-constrained registered functional encryption, with the functionalities: $G = \{g : X \to Y\}$, $F = \{f : Y \to Z\}$ and a pre-constrained $g_0 \in G$, consists of six efficient algorithms:

- $\mathsf{Setup}(1^\lambda, F, G, g_0, 1^L) \to \mathsf{crs}$: It takes as input the security parameter 1^λ, the description of functionalities F, G, a pre-constrained $g_0 \in G$ and the bounded number of user 1^L, outputs a common reference string crs.
- $\mathsf{Gen}(\mathsf{crs}, \mathsf{aux}) \to (\mathsf{pk}, \mathsf{sk})$: It takes as input crs and the public state aux, outputs key pair $(\mathsf{pk}, \mathsf{sk})$.
- $\mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f) \to (\mathsf{mpk}, \mathsf{aux}')$: It takes as input $\mathsf{crs}, \mathsf{aux}$, and pk along with $f \in F$, outputs master public key mpk and updated state aux'.
- $\mathsf{Enc}(\mathsf{mpk}, x) \to \mathsf{ct}$: It takes as input mpk, $x \in X$, outputs a ciphertext ct.
- $\mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}) \to \mathsf{hsk}$: It take as input $\mathsf{crs}, \mathsf{aux}, \mathsf{pk}$, outputs a helper key hsk.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, \mathsf{ct}) \to z/\bot/\mathtt{getupd}$: It take as input $\mathsf{sk}, \mathsf{hsk}, \mathsf{ct}$ and outputs $z \in Z$ or a special symbol $\bot$ to indicate a decryption failure, or a special flag getupd to indicate the need of an updated helper key.

Correctness. For all stateful adversary $\mathcal{A}$, the following advantage function is negligible in λ:

$$\Pr\left[b = 1 \middle| \begin{array}{l} L \leftarrow \mathcal{A}; \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, F, G, g_0, 1^L); \\ b = 0; \mathcal{A}^{\mathsf{ORegNT}(\cdot,\cdot),\mathsf{ORegT}(\cdot),\mathsf{OEnc}(\cdot,\cdot),\mathsf{ODec}(\cdot)}(\mathsf{crs}) \end{array} \right]$$

the oracles work as follows with initial setting $\mathsf{aux} = \bot$, $\mathsf{ctr} = 0$, $\mathcal{E} = \emptyset$, $\mathcal{R} = \emptyset$ and $t = \bot$:

- $\mathsf{ORegNT}(\mathsf{pk}, f)$: run $(\mathsf{mpk}, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, f)$, update $\mathsf{aux} = \mathsf{aux}'$, $\mathsf{ctr} = \mathsf{ctr} + 1$, append $(\mathsf{mpk}, \mathsf{aux})$ to $\mathcal{R}$ and return $(|\mathcal{R}|, \mathsf{mpk}, \mathsf{aux})$;
- $\mathsf{ORegT}(f^*)$: run $(\mathsf{pk}^*, \mathsf{sk}^*) \leftarrow \mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$, $(\mathsf{mpk}, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*, f^*)$, update $\mathsf{aux} = \mathsf{aux}'$, $\mathsf{ctr} = \mathsf{ctr} + 1$ and set $\mathsf{ctr}^* = \mathsf{ctr}$, compute $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*)$, append $(\mathsf{mpk}, \mathsf{aux})$ to $\mathcal{R}$, return $(t = |\mathcal{R}|, \mathsf{mpk}, \mathsf{aux}, \mathsf{pk}^*, \mathsf{sk}^*, \mathsf{hsk}^*)$;
- $\mathsf{OEnc}(i, x)$: let $\mathcal{R}[i] = (\mathsf{mpk}, \star)$, run $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x)$, append (x, ct) to $\mathcal{E}$ and return $(|\mathcal{E}|, \mathsf{ct})$;
- $\mathsf{ODec}(j)$: let $\mathcal{E}[j] = (x_j, \mathsf{ct}_j)$, compute $z'_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$; if $z'_j = \mathtt{getupd}$, run $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*)$ and recompute $z'_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$. Set $b = 1$ when $z'_j \neq f^* \circ g_0(x_j)$.

with the following restrictions:

- for query to above oracles, it holds that $\mathsf{ctr} \leq L$;
- there exists one query to ORegT; (we can consider $g_1^*, \ldots, g_L^*, f^*, \mathsf{pk}^*, \mathsf{sk}^*, \mathsf{hsk}^*$ to be global;)
- for query (i, x) to OEnc, it holds that $i \geq t$, $\mathcal{R}[i] \neq \bot$;
- for query (j) to ODec, it holds that $\mathcal{E}[j] \neq \bot$.

Compactness and Efficiency. *Compactness* means that

$$|\mathsf{mpk}| = \mathsf{poly}(\lambda, \mathsf{par}, \log L), \quad |\mathsf{hsk}_i| = \mathsf{poly}(\lambda, \mathsf{par}, \log L);$$

where par is a parameter depending on the functionalities F, G. Furthermore, *update efficiency* means that the number of invocations of Upd in ODec is at most $O(\log |\mathcal{R}|)$ and each invocation costs $\mathsf{poly}(\log |\mathcal{R}|)$ time (in RAM model).

Very Selective Simulation-based Security (SIM-security). For all stateful adversary $\mathcal{A}$, there exist simulator $(\widetilde{\mathsf{Setup}}, \widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Enc}})$ such that:

$$\begin{bmatrix} L, L', x^*, g_0, \{f_i^*\}_{i\in[L']}, CK, HK, CH \leftarrow \mathcal{A}(1^\lambda); \\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, F, G, g_0, 1^L); \\ \mathcal{A}^{\mathsf{O}(\mathsf{crs}, \{f_i^*\}_{i\in[L']}, CK, HK, CH, \cdot, \cdot)}(\mathsf{crs}); \\ \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*), \alpha \leftarrow \mathcal{A}(\mathsf{ct}^*) \end{bmatrix}$$
$$\approx_c \begin{bmatrix} L, L', x^*, g_0, \{f_i^*\}_{i\in[L']}, CK, HK, CH \leftarrow \mathcal{A}(1^\lambda); \\ \widetilde{\mathsf{crs}} \leftarrow \widetilde{\mathsf{Setup}}(1^\lambda, F, G, g_0, 1^L; \{f_i^*\}_{i\in CK\cup HK}, \{f_i^* \circ g_0(x^*)\}_{i\in CK\cup CH}); \\ \mathcal{A}^{\mathsf{O}(\widetilde{\mathsf{crs}}, \{f_i^*\}_{i\in[L']}, CK, HK, CH, \cdot, \cdot)}(\widetilde{\mathsf{crs}}); \\ \widetilde{\mathsf{ct}}^* \leftarrow \widetilde{\mathsf{Enc}}((\mathsf{pk}_1^*, \dots, \mathsf{pk}_{L'}^*); \mathsf{td}), \alpha \leftarrow \mathcal{A}(\widetilde{\mathsf{ct}}^*) \end{bmatrix}$$

where $CK, HK \subseteq [L']$, $CK \cup HK = [L']$ for some $L' \leq L$, $CH \subseteq HK$ and $CK \cap HK = \emptyset$, and O works as follows with a counter $\ell = 1$ and the same set of auxiliary data structure as in the definition of IND-security: on input (i, pk_i^*), return $\perp$ when $i \neq \ell$, otherwise set $\ell = \ell + 1$ and do

- when $i \in CK$, return $\mathsf{ORegCK}(\mathsf{pk}_i^*, f_i^*)$;
- when $i \in HK$, return $\mathsf{ORegHK}(f_i^*)$; furthermore, if $i \in CH$, return $\mathsf{OCorHK}(|HK \cap [i]|)$.

Here ORegCK and ORegHK invoke Reg in both cases: in the real world (on the left-hand side), they use crs generated by Setup and ORegHK invokes Gen; in the ideal world (on the right-hand side), they use $\widetilde{\mathsf{crs}}$ simulated by $\widetilde{\mathsf{Setup}}$ and ORegHK invokes $\widetilde{\mathsf{Gen}}$.

Remark. We give several remarks on our formalization.

- We do *not* require simulated version of Reg and Upd since both of them are public.
- We allow the adversary to choose pk_i^* at any point, only functions f_i and *types* of public keys (i.e., honest, malicious, honest but corrupted) are chosen "very selectively".
- The set CH does *not* give the timing to invoke OCorHK. One could let the adversary make an explicit query; however we call the oracle automatically just after the invocation of ORegHK. This gives a simple but not weaker model in the very selective setting. In the definition, $|HK \cap [i]|$ is the first item of the response of $\mathsf{ORegHK}(f_i^*)$.
- In very selective SIM-security, there is no need to consider post-challenge queries. This relies on the fact that adversary should state the set CH at the beginning, so the pre-challenge and post-challenge corruption queries are equivalent in the very-selective SIM-security setting.

A.2 Pre-Constrained Slotted Reg-FE

Algorithms. A slotted pre-constrained registered functional encryption, with the functionalities: $G = \{g : X \to Y\}$, $F = \{f : Y \to Z\}$ and a pre-constrained $g_0 \in G$, consists of six efficient algorithms:

- $\mathsf{Setup}(1^\lambda, F, G, g_0, 1^L) \to \mathsf{crs}$: It takes as input the security parameter 1^λ, the description of functionalities F, G, a pre-constrained $g_0 \in G$ and the upper bound 1^L of the slot numbers, outputs a common reference string crs.
- $\mathsf{Gen}(\mathsf{crs}, i) \to (\mathsf{pk}_i, \mathsf{sk}_i)$: It takes as input crs and slot number $i \in [L]$, outputs key pair $(\mathsf{pk}_i, \mathsf{sk}_i)$.
- $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) \to 0/1$: It takes as input $\mathsf{crs}, i, \mathsf{pk}_i$ and outputs a bit.
- $\mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, f_i)_{i\in[L]}) \to (\mathsf{mpk}, (\mathsf{hsk}_j)_{j\in[L]})$: It takes as input crs and a series of pk_i with $f_i \in F$ for all $i \in [L]$, outputs master public key mpk and a series of helper keys hsk_j for all $j \in [L]$. This algorithm is deterministic.

- $\mathsf{Enc}(\mathsf{mpk}, x) \to \mathsf{ct}$: It takes as input mpk, $x \in X$, outputs a ciphertext ct.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, \mathsf{ct}) \to z/\bot$: It takes as input sk, hsk, ct and outputs $z \in Z$ or a special symbol $\bot$.

We require that Agg and Dec are deterministic.

Completeness. For all $\lambda, L \in \mathbb{N}$, all F, G, all $g_0 \in G$ and all $i \in [L]$, we have

$$\Pr\left[\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1 \,\middle|\, \begin{array}{l} \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, F, G, g_0, 1^L) \\ (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{crs}, i) \end{array}\right] = 1.$$

Correctness. For all $\lambda, L \in \mathbb{N}$, all F, G, all $g_0 \in G$, all $i^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, F, G, g_0, 1^L)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i^*)$, all $\{\mathsf{pk}_i\}_{i \in [L] \setminus \{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, all $x \in X$ and $f_1, \ldots, f_L \in F$, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{i^*}, \mathsf{hsk}_{i^*}, \mathsf{ct}) = f_{i^*} \circ g_0(x) \,\middle|\, \begin{array}{l} (\mathsf{mpk}, (\mathsf{hsk}_j)_{j \in [L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, f_i)_{i \in [L]}) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x) \end{array}\right] = 1.$$

Very Selective Simulation-based Security (SIM-security). For all stateful adversary $\mathcal{A}$, there exist simulator $(\widetilde{\mathsf{Setup}}, \widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Enc}})$ such that

$$\begin{bmatrix} L, x^*, \mathcal{M}^*, C^*, \{f_i^*\}_{i \in [L]} \leftarrow \mathcal{A}(1^\lambda); \\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, F, G, g_0, 1^L); \\ \{\mathsf{pk}_i^*\}_{i \in [L]} \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot), \mathsf{OCor}(\cdot)}(\mathsf{crs}); \\ (\mathsf{mpk}, \ldots) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i^*, f_i^*)_{i \in [L]}); \\ \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*), \alpha \leftarrow \mathcal{A}(\mathsf{ct}^*) \end{bmatrix}$$
$$\approx_c \begin{bmatrix} L, x^*, \mathcal{M}^*, C^*, \{f_i^*\}_{i \in [L]} \leftarrow \mathcal{A}(1^\lambda); \\ (\widetilde{\mathsf{crs}}, \mathsf{td}) \leftarrow \widetilde{\mathsf{Setup}}(1^\lambda, F, G, g_0, 1^L; \{f_i^*\}_{i \in [L]}, \{f_i^* \circ g_0(x^*)\}_{i \in \mathcal{M}^*, C^*}); \\ \{\mathsf{pk}_i^*\}_{i \in [L]} \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot), \mathsf{OCor}(\cdot)}(\widetilde{\mathsf{crs}}); \\ \widetilde{\mathsf{ct}}^* \leftarrow \widetilde{\mathsf{Enc}}(\mathsf{pk}_1^*, \ldots, \mathsf{pk}_L^*; \mathsf{td}), \alpha \leftarrow \mathcal{A}(\widetilde{\mathsf{ct}}^*) \end{bmatrix}$$

where $\mathcal{M}^*, C^* \subseteq [L]$ denote the sets of malicious and corrupted slots, and the oracles work as follows with initial setting $C = \emptyset$ and $\mathcal{D}_i = \emptyset$ for all $i \in [L]$ and $q \in [m]$:

- $\mathsf{OGen}(i)$: run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)$, set $\mathcal{D}_i[\mathsf{pk}] = \mathsf{sk}$ and return pk.
- $\mathsf{OCor}(i, \mathsf{pk})$: return $\mathcal{D}_i[\mathsf{pk}]$ and update $C = C \cup \{(i, \mathsf{pk})\}$.

In the ideal world, OGen invokes $\widetilde{\mathsf{Gen}}$ instead of Gen; and the following restrictions:

$$\begin{aligned} i \in \mathcal{M}^* &\implies \mathcal{D}_i[\mathsf{pk}_i^*] = \bot \wedge \mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1 \\ i \in C^* &\implies (i, \mathsf{pk}_i^*) \in C \\ i \in [L] \setminus (\mathcal{M}^* \cup C^*) &\implies \mathcal{D}_i[\mathsf{pk}_i^*] \neq \bot \wedge (i, \mathsf{pk}_i^*) \notin C \end{aligned}$$

Similarly, there is no need to give $\mathsf{mpk}, \mathsf{hsk}_1, \ldots \mathsf{hsk}_L$ to $\mathcal{A}$ explicitly in real game (or explicitly in simulation game) and consider post-challenge queries.

B Registered Inner-product Encryption with Full Attribute Hiding

In this section, we present the slotted Reg-IPE with full attribute hiding, motivated by our slotted Reg-IPFE in Section 3.

Algorithms. A slotted registered inner-product encryption consists of six efficient algorithms:

- $\mathsf{Setup}(1^\lambda, 1^n, 1^L) \to \mathsf{crs}$: It takes as input the security parameter 1^λ, the size of vector 1^n and the upper bound 1^L of the number of slots, outputs a common reference string crs.
- $\mathsf{Gen}(\mathsf{crs}, i) \to (\mathsf{pk}_i, \mathsf{sk}_i)$: It takes as input crs and slot number $i \in [L]$, outputs key pair $(\mathsf{pk}_i, \mathsf{sk}_i)$.
- $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) \to 0/1$: It takes as input crs, i, pk_i and outputs a bit indicating whether pk_i is valid.
- $\mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, \mathbf{y}_i)_{i\in[L]}) \to (\mathsf{mpk}, (\mathsf{hsk}_j)_{j\in[L]})$: It takes as input crs and a series of pk_i with $\mathbf{y}_i \in \mathbb{Z}_p^n$ for all $i \in [L]$, outputs master public key mpk and a series of helper keys hsk_j for all $j \in [L]$. This algorithm is deterministic.
- $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, \mathsf{m}) \to \mathsf{ct}$: It takes as input mpk, $\mathbf{x} \in \mathbb{Z}_p^n$ and message m, outputs a ciphertext ct.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, \mathsf{ct}) \to \mathsf{m}/\bot$: It takes as input sk, hsk, ct and outputs m or a special symbol $\bot$.

Completeness. For all $\lambda, L, n \in \mathbb{N}$, and all $i \in [L]$, we have

$$\Pr\left[\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1 \,\middle|\, \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^n, 1^L);\ (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)\right] = 1.$$

Correctness. For all $\lambda, L, n \in \mathbb{N}$, all $i^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^n, 1^L)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i^*)$, all $\{\mathsf{pk}_i\}_{i\in[L]\setminus\{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, all $\mathbf{x} \in \mathbb{Z}_p^n$ and $\mathbf{y}_1, \ldots, \mathbf{y}_L \in \mathbb{Z}_p^n$ such that $\mathbf{x}\mathbf{y}_{i^*}^\top = 0$, and all m, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{i^*}, \mathsf{hsk}_{i^*}, \mathsf{ct}) = \mathsf{m} \,\middle|\, (\mathsf{mpk}, (\mathsf{hsk}_j)_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, \mathbf{y}_i)_{i\in[L]});\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, \mathsf{m})\right] = 1.$$

Attribute Hiding Security. For all stateful adversary $\mathcal{A}$, the advantage

$$\Pr\left[b = b' \,\middle|\, \begin{array}{l} L \leftarrow \mathcal{A}(1^\lambda);\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^n, 1^L) \\ (\mathsf{pk}_i^*, \mathbf{y}_i^*)_{i\in[L]}, \mathbf{x}_0^*, \mathbf{x}_1^*, \mathsf{m}_0^*, \mathsf{m}_1^* \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot),\mathsf{OCor}(\cdot)}(\mathsf{crs}) \\ (\mathsf{mpk}, (\mathsf{hsk}_j)_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i^*, \mathbf{y}_i^*)_{i\in[L]}) \\ b \leftarrow \{0,1\}, \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}_b^*, \mathsf{m}_b^*);\ b' \leftarrow \mathcal{A}(\mathsf{ct}^*) \end{array}\right] - \frac{1}{2}$$

is negligible in λ, where the oracles work as follows with initial setting $C = \emptyset$ and $\mathcal{D}_i = \emptyset$ for all $i \in [L]$:

- $\mathsf{OGen}(i)$: run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)$, set $\mathcal{D}_i[\mathsf{pk}] = \mathsf{sk}$ and return pk.
- $\mathsf{OCor}(i, \mathsf{pk})$: return $\mathcal{D}_i[\mathsf{pk}]$ and update $C = C \cup \{(i, \mathsf{pk})\}$.

and, for all $i \in [L]$, we require that

$$\mathcal{D}_i[\mathsf{pk}_i^*] = \bot \implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1,$$

if $\mathsf{m}_0^* \neq \mathsf{m}_1^*$, we require that

$$(i, \mathsf{pk}_i^*) \in C \lor \mathcal{D}_i[\mathsf{pk}_i^*] = \bot \implies \mathbf{x}_0^*(\mathbf{y}_i^*)^\top \neq 0 \land \mathbf{x}_1^*(\mathbf{y}_i^*)^\top \neq 0$$

if $\mathsf{m}_0^* = \mathsf{m}_1^*$, we require that

$$(i, \mathsf{pk}_i^*) \in C \lor \mathcal{D}_i[\mathsf{pk}_i^*] = \bot \implies \left(\mathbf{x}_0^*(\mathbf{y}_i^*)^\top \neq 0 \land \mathbf{x}_1^*(\mathbf{y}_i^*)^\top \neq 0\right) \lor \left(\mathbf{x}_0^*(\mathbf{y}_i^*)^\top = \mathbf{x}_1^*(\mathbf{y}_i^*)^\top = 0\right)$$

We use $\mathsf{Adv}_{\mathcal{A}}^{\text{sReg-IPE}}(\lambda)$ to denote the advantage function. Note that [HLWW23] showed that there is no need to give mpk and $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ to $\mathcal{A}$ explicitly and to consider post-challenge queries.

B.1 Scheme

Assuming a QA-NIZK $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ for linear space over bilinear groups, our slotted Reg-IPE scheme works as follows in the prime-order bilinear group:

– $\mathsf{Setup}(1^\lambda, 1^n, 1^L)$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k},\ \mathbf{V} \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)},\ \mathbf{W}_0 \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)},\ \mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}.$$

For all $i \in [L]$, sample

$$\mathbf{W}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)n},\ \mathbf{R}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)},\ \mathbf{r}_i \leftarrow \mathbb{Z}_p^{1\times k}.$$

For all $i \in [L]$, write $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{R}_i} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$, run

$$(\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1).$$

Output

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AV}, \mathbf{AW}_0]_1,\ [\mathbf{Ak}^\top]_T \\ \{\mathsf{crs}_i,\ [\mathbf{R}_i, \mathbf{AW}_i]_1\}_{i\in[L]} \\ \{[\mathbf{B}_1\mathbf{r}_j^\top, \mathbf{W}_0\mathbf{B}_1\mathbf{r}_j^\top + \mathbf{k}^\top]_2\}_{j\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$

Note that we do not use $\mathsf{td}_1, \ldots, \mathsf{td}_L$ in the actual scheme.

– $\mathsf{Gen}(\mathsf{crs}, i)$: Sample $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)}$. Define $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i} = \binom{\mathbf{AU}_i}{\mathbf{R}_i\mathbf{U}_i} = \mathbf{A}_i\mathbf{U}_i \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$ and run

$$\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i).$$

Fetch $\{[\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[L]\setminus\{i\}}$ from crs and output

$$\mathsf{pk}_i = \Big([\underbrace{\mathbf{AU}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{R}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{[\underbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\Big) \quad \text{and} \quad \mathsf{sk}_i = \mathbf{U}_i.$$

– $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i)$: Parse $\mathsf{pk}_i = \big([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{h}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$. Write $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i}$ and check

$$\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \pi_i) \stackrel{?}{=} 1.$$

For each $j \in [L] \setminus \{i\}$, check

$$e([\mathbf{A}]_1, [\mathbf{h}_{i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_i]_1, [\mathbf{B}_1\mathbf{r}_j^\top]_2).$$

If all these checks pass, output 1; otherwise, output 0.

– $\mathsf{Agg}(\mathsf{crs}, (\mathsf{pk}_i, \mathbf{y}_i)_{i\in[L]})$: For all $i \in [L]$, parse $\mathsf{pk}_i = \big([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{h}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$. Output:

$$\mathsf{mpk} = \left(\left[\mathbf{A},\ \mathbf{AW}_0 + \sum_{i\in[L]}(\mathbf{T}_i + \mathbf{AW}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1})),\ \sum_{i\in[L]}\mathbf{AW}_i,\ \mathbf{AV}\right]_1\right)$$

and for all $j \in [L]$

$$\mathsf{hsk}_j = \left(\left[\underbrace{\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{k}_0^\top},\ \underbrace{\sum_{i\in[L]\setminus\{j\}}(\mathbf{h}_{i,j} + \mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)\mathbf{y}_i^\top)}_{\mathbf{k}_1^\top},\ \underbrace{\sum_{i\in[L]\setminus\{j\}}\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)}_{\mathbf{K}_2},\ \underbrace{\mathbf{W}_0\mathbf{B}_1\mathbf{r}_j^\top + \mathbf{k}^\top}_{\mathbf{k}_3^\top}\right]_2\right).$$

– $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, \mathsf{m})$: Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$. Output:

$$\mathsf{ct} = \Bigg(\Bigg[\underbrace{\mathbf{sA}}_{\mathbf{c}_0}, \underbrace{\mathbf{sAW}_0 + \sum_{i\in[L]} (\mathbf{sT}_i + \mathbf{sAW}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1}, \underbrace{\mathbf{x} \otimes \mathbf{sAV} + \sum_{i\in[L]} \mathbf{sAW}_i}_{\mathbf{c}_2}\Bigg]_1, \underbrace{[\mathbf{sAk}^\top]_T \cdot \mathsf{m}}_{C}\Bigg).$$

– $\mathsf{Dec}(\mathsf{sk}_{i^*}, \mathsf{hsk}_{i^*}, \mathsf{ct})$: Parse

$$\mathsf{sk}_{i^*} = \mathbf{U}_{i^*}, \quad \mathsf{hsk}_{i^*} = ([\mathbf{k}_0^\top, \mathbf{k}_1^\top, \mathbf{K}_2, \mathbf{k}_3^\top]_2), \quad \mathsf{ct}_x = ([\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2]_1, C).$$

Recover

$$\begin{aligned} [\mathbf{z}_1]_T &= e([\mathbf{c}_2]_1, [\mathbf{I}_n \otimes \mathbf{k}_0^\top]_2), & [\mathbf{z}_2]_T &= e([\mathbf{c}_0]_1, [\mathbf{K}_2]_2); \\ [z_3]_T &= e([\mathbf{c}_1]_1, [\mathbf{k}_0^\top]_2), & [z_4]_T &= e([\mathbf{c}_0]_1, [\mathbf{k}_1^\top]_2); \\ [z_5]_T &= e([\mathbf{c}_0\mathbf{U}_{i^*}]_1, [\mathbf{k}_0^\top]_2), & [z_6]_T &= e([\mathbf{c}_0]_1, [\mathbf{k}_3^\top]_2). \end{aligned}$$

Compute

$$z = [(z_3 - z_4 - z_5) - (\mathbf{z}_1 - \mathbf{z}_2)\mathbf{y}_{i^*}^\top - z_6]_T \cdot C.$$

Completeness. For all $\lambda, L, n \in \mathbb{N}$, all $i \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^n, 1^L)$ and $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)$, we have

$$\mathsf{pk}_i = \big([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{h}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big) = \big([\mathbf{AU}_i, \mathbf{R}_i\mathbf{U}_i]_1, \{[\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$$

for some $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)}$ and $\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{A}_i\mathbf{U}_i]_1, \mathbf{U}_i)$ where $(\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$ and $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{R}_i}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$, $\mathbf{R}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}$. Then

– Write $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i} = \binom{\mathbf{AU}_i}{\mathbf{R}_i\mathbf{U}_i}$, we have $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \pi_i) = 1$ by the perfect completeness of Π_0 (see Section 2.4) and the fact that $\mathbf{F}_i = \mathbf{A}_i\mathbf{U}_i$;
– For each $j \in [L] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top]_2) = e([\mathbf{AU}_i]_1, [\mathbf{B}_1\mathbf{r}_j^\top]_2)$ by the definition of bilinear map e (see Section 2.1) and the fact that $\mathbf{A} \cdot \mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top = \mathbf{AU}_i \cdot \mathbf{B}_1\mathbf{r}_j^\top$.

This ensures that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$ by the specification of Ver and readily proves the completeness.

Correctness. For all $\lambda, L, n \in \mathbb{N}$, , all $i^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^n, 1^L)$, all $(\mathsf{pk}_{i^*}, \mathsf{sk}_{i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i^*)$, all $\{\mathsf{pk}_i\}_{i\in[L]\setminus\{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1$, for all $\mathbf{y}_1, \ldots, \mathbf{y}_L \in \mathbb{Z}_p^n$ and $\mathbf{x} \in \mathbb{Z}_p^n$ such that $\mathbf{xy}_{i^*}^\top = 0$, we have:

$$\begin{aligned} \mathsf{sk}_{i^*} &= \mathbf{U}_{i^*}, \\ \mathsf{ct} &= \Bigg(\Bigg[\underbrace{\mathbf{sA}}_{\mathbf{c}_0}, \underbrace{\mathbf{sAW}_0 + \sum_{i\in[L]} (\mathbf{sT}_i + \mathbf{sAW}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1}, \underbrace{\mathbf{x} \otimes \mathbf{sAV} + \sum_{i\in[L]} \mathbf{sAW}_i}_{\mathbf{c}_2}\Bigg]_1, \underbrace{[\mathbf{sAk}^\top]_T \cdot \mathsf{m}}_{C}\Bigg) \\ \mathsf{hsk}_{i^*} &= \Bigg(\Bigg[\underbrace{\mathbf{B}_1\mathbf{r}_{i^*}^\top}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i\in[L]\setminus\{i^*\}} (\mathbf{h}_{i,i^*} + \mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_i^\top)}_{\mathbf{k}_1^\top}, \underbrace{\sum_{i\in[L]\setminus\{i^*\}} \mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top)}_{\mathbf{K}_2}, \underbrace{\mathbf{W}_0\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{k}^\top}_{\mathbf{k}_3^\top}\Bigg]_2\Bigg) \end{aligned}$$

where

$$\mathbf{Ah}_{i,i^*} = \mathbf{T}_i\mathbf{B}_1\mathbf{r}_{i^*}^\top \quad \forall i \in [L] \setminus \{i^*\} \quad \text{and} \quad \mathbf{AU}_{i^*} = \mathbf{T}_{i^*}.$$

Note that here we actually consider hsk_j for $j = i^*$ and sk_i for $i = i^*$ and all above equalities are ensured by Ver and Gen. we have

$$\begin{aligned}
\mathbf{z}_1 &= (\mathbf{x} \otimes \mathbf{sAV})(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top) + \sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top) \\
&= \mathbf{sAV}(\mathbf{x} \otimes \mathbf{I}_{2k+1})(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top) + \sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top) \\
&= \mathbf{sAVB}_1\mathbf{r}_{i^*}^\top\mathbf{x} + \sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top) \qquad (26) \\
\mathbf{z}_2 &= \sum_{i\in[L]\setminus\{i^*\}} \mathbf{sAW}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top) \\
z_3 &= \mathbf{sAW}_0 + \sum_{i\in[L]} (\mathbf{sT}_i\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{sAW}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1})\mathbf{B}_1\mathbf{r}_{i^*}^\top) \\
&= \mathbf{sAW}_0 + \sum_{i\in[L]} (\mathbf{sT}_i\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{sAW}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_i^\top) \qquad (27) \\
z_4 &= \sum_{i\in[L]\setminus\{i^*\}} (\mathbf{sAh}_{i,i^*} + \mathbf{sAW}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_i^\top) \\
z_5 &= \mathbf{sAU}_{i^*}\mathbf{B}_1\mathbf{r}_{i^*}^\top \\
z_6 &= \mathbf{sAW}_0\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{sAk}^\top
\end{aligned}$$

and then

$$\begin{aligned}
z &= [(z_3 - z_4 - z_5) - (\mathbf{z}_1 - \mathbf{z}_2)\mathbf{y}_{i^*}^\top - z_6]_T \cdot C \\
&= [(\mathbf{sAW}_0\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{sT}_{i^*}\mathbf{B}_1\mathbf{r}_{i^*}^\top + \mathbf{sAW}_{i^*}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_{i^*}^\top - \mathbf{sAU}_{i^*}\mathbf{B}_1\mathbf{r}_{i^*}^\top) - \\
&\quad (\mathbf{sAVB}_1\mathbf{r}_{i^*}^\top \cdot \mathbf{xy}_{i^*}^\top + \mathbf{sAW}_{i^*}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_{i^*}^\top)\mathbf{y}_{i^*}^\top) \\
&\quad -\mathbf{sAW}_0\mathbf{B}_1\mathbf{r}_{i^*}^\top - \mathbf{sAk}^\top]_T \cdot [\mathbf{sAk}^\top]_T \cdot \mathsf{m} \qquad (28) \\
&= [-\mathbf{sAVB}_1\mathbf{r}_{i^*}^\top \cdot \mathbf{xy}_{i^*}^\top]_T \cdot \mathsf{m} \qquad (29) \\
&= \mathsf{m} \qquad (30)
\end{aligned}$$

Here, equality (26) and equality (27) follows from the property of tensor product: $(\mathbf{M}\otimes\mathbf{I})(\mathbf{I}\otimes\mathbf{a}^\top) = \mathbf{M}\otimes\mathbf{a}^\top = (\mathbf{I}\otimes\mathbf{a}^\top)\mathbf{M}$ for matrices of proper size; equality (28) follows from the fact that $\mathbf{Ah}_{i,i^*} = \mathbf{T}_i\mathbf{B}_1\mathbf{r}_{i^*}^\top$ for all $i \in [L] \setminus \{i^*\}$; equality (29) follows from the fact that $\mathbf{T}_{i^*} = \mathbf{AU}_{i^*}$; equality (30) follows from the fact that $\mathbf{xy}_{i^*}^\top = 0$. This proves the correctness.

Compactness and Efficiency. Our slotted Reg-IPFE has the following properties:

$$|\mathsf{crs}| = L^2 \cdot n \cdot \mathsf{poly}(\lambda); \quad |\mathsf{mpk}| = n \cdot \mathsf{poly}(\lambda); \quad |\mathsf{hsk}_j| = n \cdot \mathsf{poly}(\lambda); \quad |\mathsf{ct}| = n \cdot \mathsf{poly}(\lambda).$$

Note that the total size of $\{\mathsf{crs}_i\}_{i\in[L]}$ is $L \cdot \mathsf{poly}(\lambda)$ according to the efficiency of the pairing-based QA-NIZK scheme by Kiltz and Wee [KW15] and the fact that the size of language description is $\mathsf{poly}(\lambda)$.

Security. We have the following theorem. Given pairing-based QA-NIZK in [KW15] with unbounded simulation soundness under MDDH assumption, our slotted Reg-IPFE scheme uses prime-order bilinear group and the security can be reduced to MDDH assumption and subgroup decision assumption.

Theorem 7. *Assume* $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ *is a QA-NIZK with perfect completeness, perfect zero-knowledge and unbounded simulation soundness for linear space defined in Section 2.4, our slotted Reg-IPE scheme achieves the attribute hiding security under MDDH assumption and subspace decision assumption.*

B.2 Proof

We prove the following technical lemma; this immediately proves Theorem 7.

Lemma 7. *For all adversaries $\mathcal{A}$, there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ and $\mathcal{B}_4$ such that:*

$$\mathsf{Adv}_{\mathcal{A}}^{sReg\text{-}IPE}(\lambda) \le L \cdot \mathsf{Adv}_{\mathcal{B}_1}^{USS}(\lambda) + \mathsf{Adv}_{\mathcal{B}_2}^{MDDH} + L \cdot \mathsf{Adv}_{\mathcal{B}_3}^{\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_3}} + L \cdot \mathsf{Adv}_{\mathcal{B}_4}^{\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_2}} \mathsf{negl}(\lambda)$$

where L is the number of slots and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3), \mathsf{Time}(\mathcal{B}_4) \approx \mathsf{Time}(\mathcal{A})$.

Game Sequence. Suppose that crs is the common reference string, $(\mathbf{x}_0^*, \mathbf{x}_1^*)$ and $(\mathsf{m}_0^*, \mathsf{m}_1^*)$ are the challenge pair, $\{\mathsf{pk}_i^*, \mathbf{y}_i^*\}_{i\in[L]}$ are challenge public keys along with challenge functions to be registered. Let $D_i = \{(\mathsf{pk}_i, \mathsf{sk}_i) : \mathcal{D}_i[\mathsf{pk}_i] = \mathsf{sk}_i \neq \bot\}$ be responses to $\mathsf{OGen}(i)$ and C records public keys in $D_1, \ldots, D_L$ that have been sent to OCor. Recall that, for challenge public keys $\{\mathsf{pk}_i^*, \mathbf{y}_i^*\}_{i\in[L]}$, we require that

$$\mathcal{D}_i[\mathsf{pk}_i^*] = \bot \implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1,$$

and if $\mathsf{m}_0^* \neq \mathsf{m}_1^*$, we require that

$$(i, \mathsf{pk}_i^*) \in C \vee \mathcal{D}_i[\mathsf{pk}_i^*] = \bot \implies \mathbf{x}_0^*(\mathbf{y}_i^*)^\top \neq 0 \wedge \mathbf{x}_1^*(\mathbf{y}_i^*)^\top \neq 0.$$

if $\mathsf{m}_0^* = \mathsf{m}_1^*$, we require that

$$(i, \mathsf{pk}_i^*) \in C \vee \mathcal{D}_i[\mathsf{pk}_i^*] = \bot \implies (\mathbf{x}_0^*(\mathbf{y}_i^*)^\top \neq 0 \wedge \mathbf{x}_1^*(\mathbf{y}_i^*)^\top \neq 0) \vee (\mathbf{x}_0^*(\mathbf{y}_i^*)^\top = \mathbf{x}_1^*(\mathbf{y}_i^*)^\top = 0).$$

Note that pk_i serves as a *general* entry in D_i while pk_i^* is the *specific* challenge public for slot i; there can be more than one assignments for pk_i since the adversary can invoke $\mathsf{OGen}(i)$ for many times. We prove the Lemma 7 via nested dual-system method using the following game sequence.

- G_0: This is the real game, recall that we have
  - crs is in the form:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AV}, \mathbf{AW}_0]_1, [\mathbf{A}\mathbf{k}^\top]_T \\ \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{AW}_i]_1\}_{i\in[L]} \\ \{[\mathbf{B}_1\mathbf{r}_j^\top, \mathbf{W}_0\mathbf{B}_1\mathbf{r}_j^\top + \mathbf{k}^\top]_2\}_{j\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$

    where $\mathsf{crs}_i \in \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$, $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{R}_i}$.
  - For each $i \in [L]$, each $(\mathsf{pk}_i, \mathsf{sk}_i) \in D_i$ is in the form:

$$\mathsf{pk}_i = \big([\underbrace{\mathbf{AU}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{R}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{[\underbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big) \quad \text{and} \quad \mathsf{sk}_i = \mathbf{U}_i$$

    where $\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i)$, $\mathbf{F}_i = \binom{\mathbf{AU}_i}{\mathbf{RU}_i}$.
  - For all $i \in [L]$, pk_i^* is in the form:

$$\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{h}_{i,j}^*]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$$

    such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i^*) = 1$ which means $\mathsf{LVer}\left(\mathsf{crs}_i, \begin{bmatrix} \mathbf{T}_i^* \\ \mathbf{Q}_i^* \end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{A}\mathbf{h}_{i,j}^* = \mathbf{T}_i^*\mathbf{B}_1\mathbf{r}_j^\top$ for each $j \in [L]\setminus\{i\}$.

- ct^* for $(\mathbf{x}_0^*, \mathbf{x}_1^*)$ and $(\mathsf{m}_0^*, \mathsf{m}_1^*)$ is in the form:

$$\mathsf{ct}^* = \left(\left[\underbrace{\mathbf{sA}}_{\mathbf{c}_0^*}, \underbrace{\mathbf{sAW}_0 + \sum_{i\in[L]}(\mathbf{sT}_i + \mathbf{sAW}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1^*}, \underbrace{\mathbf{x}_b^* \otimes \mathbf{sAV} + \sum_{i\in[L]}\mathbf{sAW}_i}_{\mathbf{c}_2^*}, \underbrace{[\mathbf{sAk}^\top]_T \cdot \mathsf{m}_b^*}_{C^*}\right]\right).$$

where $b \leftarrow \{0,1\}$ is the secret bit.

– G_1: Identical to G_0 except that, for all $i \in [L]$ and all $(\mathsf{pk}_i, \mathsf{sk}_i) \in D_i$, we replace π_i with

$$\widetilde{\pi}_i \leftarrow \boxed{\mathsf{LSim}}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{F}_i]_1) \quad \text{where} \quad \mathbf{F}_i = \begin{pmatrix}\mathbf{AU}_i \\ \mathbf{R}_i\mathbf{U}_i\end{pmatrix}.$$

We have $\mathsf{G}_1 \equiv \mathsf{G}_0$. This follows from the perfect zero-knowledge of Π_0.

– G_2: Identical to G_1 except that we sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ along with $\mathbf{A}$ and replace all $\mathbf{R}_i$ in crs with

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i\begin{pmatrix}\mathbf{sA} \\ \mathbf{I}_{2k+1}\end{pmatrix}, \quad \widetilde{\mathbf{R}}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}.$$

We have $\mathsf{G}_2 \equiv \mathsf{G}_1$. This follows from the fact that both $\mathbf{R}_i$ (in G_1) and $\widehat{\mathbf{R}}_i$ (in G_2) are truly random since matrix $\binom{\mathbf{sA}}{\mathbf{I}_{2k+1}}$ is full-rank.

– G_3: Identical to G_2 except that we generate the $\mathbf{c}_1^*$ as follows:

$$\mathbf{c}_1^* = \mathbf{sAW}_0 + \sum_{i\in[L]}(\boxed{\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*} + \mathbf{sAW}_i(\mathbf{y}_i^\top \otimes \mathbf{I}_{2k+1})).$$

We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from stronger unbounded simulation soundness of Π_0 along with the fact that $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i^*], \pi_i^*) = 1$ for all $i \in [L]$ where $\mathbf{F}_i^* = \begin{pmatrix}\mathbf{T}_i^* \\ \mathbf{Q}_i^*\end{pmatrix}$. Assume $\mathsf{pk}_{i^*}^* \notin D_{i^*}$, i.e., $\mathsf{pk}_{i^*}^*$ is malicious. In the reduction, we guess $i^* \leftarrow [L]$ and obtain $\mathbf{A}, \widehat{\mathbf{R}}_{i^*}, \mathsf{crs}_{i^*}$ as input; we simulate honestly as in G_3 except that for all $\mathsf{pk}_{i^*} \in D_{i^*}$, we make an oracle query $[\mathbf{F}_{i^*}]_1$ and get $\widetilde{\pi}_{i^*}$ in it; we finally output $([\mathbf{F}_{i^*}^*]_1, \pi_{i^*}^*)$ in $\mathsf{pk}_{i^*}^* \notin D_{i^*}$. Observe that once it happens that $\mathbf{e}_1\widetilde{\mathbf{R}}_{i^*}^{-1}\mathbf{Q}_{i^*}^* \neq \mathbf{sT}_{i^*}^*$, we must have $\mathbf{F}_{i^*}^* \notin \mathsf{span}(\mathbf{A}_{i^*})$. When $\mathsf{pk}_{i^*}^* \in D_{i^*}$, we always have $\mathsf{G}_3 \equiv \mathsf{G}_2$.

– G_4: Identical to G_3 except that we replace all $\mathbf{sA}$ with $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$; in particular, we generate $\widehat{\mathbf{R}}_i$ as follows:

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i\begin{pmatrix}\boxed{\mathbf{c}} \\ \mathbf{I}_{2k+1}\end{pmatrix}, \quad \widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}$$

and generate the challenge ciphertext as follows:

$$\mathsf{ct}^* = \left(\left[\underbrace{\boxed{\mathbf{c}}}_{\mathbf{c}_0^*}, \underbrace{\boxed{\mathbf{c}}\mathbf{W}_0 + \sum_{i\in[L]}(\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^* + \boxed{\mathbf{c}}\mathbf{W}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1^*}, \underbrace{\mathbf{x}_b^* \otimes \boxed{\mathbf{c}}\mathbf{V} + \sum_{i\in[L]}\boxed{\mathbf{c}}\mathbf{W}_i}_{\mathbf{c}_2^*}\right]_1, \underbrace{[\boxed{\mathbf{c}}\mathbf{k}^\top]_T \cdot \mathsf{m}_b^*}_{C^*}\right).$$

We have $\mathsf{G}_4 \approx_c \mathsf{G}_3$. This follows from MDDH assumption which ensures that $([\mathbf{A}]_1, [\mathbf{sA}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{c}]_1)$ when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}, \mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$.

– G_5: Identical to G_4 except that for all $i \in [L]$, we replace $\mathbf{AV}$ in crs with

$$\widetilde{\mathbf{V}} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$$

we replace $\mathbf{cV}$ in challenge ciphertext with

$$\mathbf{v} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$$

In particular, we generate crs as below:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \boxed{\widetilde{\mathbf{V}}}, \mathbf{A}\mathbf{W}_0]_1, [\mathbf{A}\mathbf{k}^\top]_T \\ \{\mathsf{crs}_i, [\widehat{\mathbf{R}}_i, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\mathbf{B}_1\mathbf{r}_j^\top, \mathbf{W}_0\mathbf{B}_1\mathbf{r}_j^\top + \mathbf{k}^\top]_2\}_{j\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$

and generate the challenge ciphertext as

$$\mathsf{ct}^* = \left(\left[\underbrace{\mathbf{c}}_{\mathbf{c}_0^*}, \underbrace{\mathbf{c}\mathbf{W}_0 + \sum_{i\in[L]}(\mathbf{e}_1\widetilde{\mathbf{R}}^{-1}\mathbf{Q}_i^* + \mathbf{c}\mathbf{W}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1^*}, \underbrace{\mathbf{x}_b^* \otimes \boxed{\mathbf{v}} + \sum_{i\in[L]}\mathbf{c}\mathbf{W}_i}_{\mathbf{c}_2^*}\right]_1, \underbrace{[\mathbf{c}\mathbf{k}^\top]_T \cdot \mathsf{m}_b^*}_{C^*}\right).$$

We have $\mathsf{G}_5 \equiv \mathsf{G}_4$. This follows from the fact that when $\mathbf{V}$ is uniformly sampled from $\mathbb{Z}_p^{(2k+1)\times(2k+1)}$ and not published elsewhere, $(\mathbf{A}\mathbf{V}, \mathbf{c}\mathbf{V})$ (in G_4) is statically equivalent with the uniformly sampled $(\widetilde{\mathbf{V}}, \mathbf{v})$ where $\widetilde{\mathbf{V}} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{v} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$ (in G_5) , since both $\mathbf{A}$ and $\mathbf{c}$ are full row rank (with overwhelming probability).

– G_6: Identical to G_5 except that we randomly sample $\mathbf{B}_2 \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, and compute the dual basis $\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel$. And we change $\mathbf{c}_2^*$ as follows:

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1,3)} + \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]}\mathbf{c}\mathbf{W}_i$$

We have $\mathsf{G}_6 \equiv \mathsf{G}_5$. This follows from the following argument for $b' = b$ (in G_5) or $b' = 0$ (in G_6):

$$\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]}(\mathbf{c}\mathbf{W}_i)^{(2)} \equiv \sum_{i\in[L]}(\mathbf{c}\mathbf{W}_i)^{(2)}$$

This argument follows from the fact that the basis $\mathbf{B}_2$ and dual basis $\mathbf{B}_2^\parallel$ are not revealed, so we have $(\mathbf{c}\mathbf{W}_i)^{(2)}$ is hidden, this can imply that $\sum_{i\in[L]}(\mathbf{c}\mathbf{W}_i)^{(2)}$ hides $\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(2)}$.

– $\mathsf{G}_{7,\ell}$, $(\ell \in [0, L])$: Identical to G_6 except that for all $j \in [\ell]$ we replace all $\mathbf{B}_1\mathbf{r}_j^\top$ and $\mathbf{W}_0\mathbf{B}_1\mathbf{r}_j^\top + \mathbf{k}^\top$ in crs with

$$\boxed{\mathbf{d}_j^\top} \quad \text{and} \quad \mathbf{W}_0\boxed{\mathbf{d}_j^\top} + \mathbf{k}^\top + \boxed{\mathbf{c}^\perp\alpha}$$

where $\mathbf{d}_j \leftarrow \mathsf{span}(\mathbf{B}_2^\top)$, $\alpha \leftarrow \mathbb{Z}_p$ and $\mathbf{c} \leftarrow \mathbb{Z}_p^{2k+1}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}, \mathbf{c}\mathbf{c}^\perp = 1$. We have that

- $\mathsf{G}_{7,0} = \mathsf{G}_6$; the two games are actually identical, since $[0] = \emptyset$;
- $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$ for all $\ell \in [L]$, we will employ a sub-sequence of games for the proof described later.

– G_8: Identical to $\mathsf{G}_{7,L}$ except that we generate the $\mathbf{c}_2^*$ as follows:

$$\mathbf{c}_2^* = \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(1,3)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]}\mathbf{c}\mathbf{W}_i$$

We have $\mathsf{G}_8 \equiv \mathsf{G}_{7,L}$. The proof is analogous to that of $\mathsf{G}_6 \equiv \mathsf{G}_5$, with the fact that basis $\mathbf{B}_1, \mathbf{B}_3$ and dual basis $\mathbf{B}_1^\parallel, \mathbf{B}_3^\parallel$ are not revealed in $\mathsf{G}_{7,L}$, we have the following argument for $b' = b$ (in $\mathsf{G}_{7,L}$) or $b' = 0$ (in G_8):

$$\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(1,3)} + \sum_{i\in[L]}(\mathbf{c}\mathbf{W}_i)^{(2)} \equiv \sum_{i\in[L]}(\mathbf{c}\mathbf{W}_i)^{(1,3)}$$

– G_9: Identical to G_8 except that we replace terms C^* in ct^* as $\boxed{C^* \leftarrow \mathbb{G}_T}$. We have $\mathsf{G}_9 \equiv \mathsf{G}_8$. This follows from the following statistical argument:

$$(\overbrace{\mathbf{A}\mathbf{k}^\top, \mathbf{k}^\top + \mathbf{c}^\perp\alpha}^{\mathsf{crs}}, \overbrace{\mathbf{c}\mathbf{k}^\top}^{C^* \text{ in } \mathsf{ct}^*}) \equiv (\mathbf{A}\mathbf{k}^\top, \mathbf{k}^\top, \mathbf{c}\mathbf{k}^\top - \alpha)$$

when $\mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$ and the fact that $[\alpha]_T$ only appears in C^*. We can prove the statement via change of variable $\mathbf{k}^\top \mapsto \mathbf{k}^\top - \mathbf{c}^\perp\alpha$.

Observe that, in the final game G_9 the challenge ciphertext ct is independent of the random bit b and the adversary's advantage is exactly 0.

From $\mathsf{G}_{7,\ell-1}$ to $\mathsf{G}_{7,\ell}$. We are ready to prove $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$ and this will complete the proof of Lemma 7. For this, we need the following sub-sequence of games for each $\ell \in [L]$:

- $\mathsf{G}_{7,\ell-1,0}$: Identical to $\mathsf{G}_{7,\ell-1}$ where we recall crs, $\mathsf{pk}_i \in D_i$ and $\mathbf{c}_1^*, \mathbf{c}_2^*$, with highlighting relevant terms in the following sub-sequence with dashed boxes as follows:

$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \widetilde{\mathbf{V}}, \mathbf{A}\mathbf{W}_0]_1, [\mathbf{A}\mathbf{k}^\top]_T, \left\{\mathsf{crs}_i, [\widehat{\mathbf{R}}_i, \mathbf{A}\mathbf{W}_i]_1\right\}_{i\in[L]} \\ \left\{[\mathbf{d}_j^\top, \mathbf{W}_0\mathbf{d}_j^\top + \mathbf{k}^\top + \mathbf{c}^\perp\alpha]_2\right\}_{j\in[\ell-1]}, \boxed{[\mathbf{B}_1\mathbf{r}_\ell^\top, \mathbf{W}_0\mathbf{B}_1\mathbf{r}_\ell^\top + \mathbf{k}^\top]_2}, \\ \left\{[\mathbf{B}_1\mathbf{r}_j^\top, \mathbf{W}_0\mathbf{B}_1\mathbf{r}_j^\top + \mathbf{k}^\top]_2\right\}_{j\in[L]\setminus[\ell]} \\ \left\{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{d}_j^\top)]_2\right\}_{j\in[\ell-1], i\in[L]\setminus\{j\}}, \left\{\boxed{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_\ell^\top)]_2}\right\}_{i\in[L]\setminus\{\ell\}}, \\ \left\{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\right\}_{j\in[L]\setminus[\ell], i\in[L]\setminus\{j\}} \end{array}\right),$$

$$\mathsf{pk}_i = \begin{cases} \Big([\overbrace{\mathbf{A}\mathbf{U}_i}^{\mathbf{T}_i}, \overbrace{\widehat{\mathbf{R}}_i\mathbf{U}_i}^{\mathbf{Q}_i}]_1, \{[\overbrace{\mathbf{U}_i\mathbf{d}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j\in[\ell-1]\setminus\{i\}}, \boxed{[\overbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{r}_\ell^\top}^{\mathbf{h}_{i,\ell}}]_2}, \{[\overbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{r}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus[i,\ell]}, \widetilde{\pi}_i\Big) & \text{if } i \neq \ell \\ \Big([\underbrace{\mathbf{A}\mathbf{U}_\ell}_{\mathbf{T}_\ell}, \underbrace{\widehat{\mathbf{R}}_i\mathbf{U}_\ell}_{\mathbf{Q}_\ell}]_1, \{[\underbrace{\mathbf{U}_\ell\mathbf{d}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j\in[\ell-1]}, \{[\underbrace{\mathbf{U}_\ell\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j\in[L]\setminus[\ell]}, \widetilde{\pi}_\ell\Big) & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_1^* = \boxed{(\mathbf{c}\mathbf{W}_0 + \mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{2k+1}))} + \sum_{i\in[L]\setminus\{\ell\}} (\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^* + \mathbf{c}\mathbf{W}_i((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{2k+1}))$$

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*} \otimes \mathbf{v}^{(3)} + \boxed{\mathbf{c}\mathbf{W}_\ell} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_i$$

  Where $\mathbf{d}_j \leftarrow \mathsf{span}(\mathbf{B}_2^\top)$ for all $j \in [\ell-1]$. We have $\mathsf{G}_{7,\ell-1,0} = \mathsf{G}_{7,\ell-1}$; all changes are conceptual.
- $\mathsf{G}_{7,\ell-1,1}$: Identical to $\mathsf{G}_{7,\ell-1,0}$ except that we replace all $\mathbf{B}_1\mathbf{r}_\ell^\top$ in crs with

$$\mathbf{d}_\ell^\top \quad \text{where} \quad \boxed{\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_3^\top)}.$$

  In particular, we change the dashed boxed term in crs and pk_i as follows:

$$[\boxed{\mathbf{d}_\ell^\top, \mathbf{W}_0\mathbf{d}_\ell^\top + \mathbf{k}^\top}]_2, \{[\mathbf{W}_i(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top})]_2, [\mathbf{U}_i\boxed{\mathbf{d}_\ell^\top}]_2\}_{i\in[L]\setminus\{\ell\}}$$

  We have $\mathsf{G}_{7,\ell-1,1} \approx_c \mathsf{G}_{7,\ell-1,0}$. This follow from the $\mathrm{SD}^{\mathbb{G}_2}_{\mathbf{B}_1\mapsto\mathbf{B}_3}$ assumption which ensure that

$$[\mathbf{t}_0]_2 \approx_c [\mathbf{t}_1]_2 \quad \text{given} \quad [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_1^\parallel, \mathbf{B}_3^\parallel), \mathsf{basis}(\mathbf{B}_2^\parallel)$$

  Where $\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{B}_1^\top)$ corresponding to $\mathsf{G}_{7,\ell-1,0}$, and $\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_3^\top)$ corresponding to $\mathsf{G}_{7,\ell-1,1}$.
- $\mathsf{G}_{7,\ell-1,2}$: Identical to $\mathsf{G}_{7,\ell-1,1}$ except that we change the dashed boxed term in crs and pk_i as follows:

$$[\mathbf{d}_\ell^\top, \mathbf{W}_0\mathbf{d}_\ell^\top + \mathbf{k}^\top + \boxed{\mathbf{c}^\perp\alpha}]_2, \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top)]_2, [\mathbf{U}_i\mathbf{d}_\ell^\top]_2\}_{i\in[L]\setminus\{\ell\}}$$

  We have $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$. We provide some details in Section B.3.
- $\mathsf{G}_{7,\ell-1,3}$: Identical to $\mathsf{G}_{7,\ell-1,2}$ except that we generate the $\mathbf{c}_2^*$ as follows:

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_i$$

  We have $\mathsf{G}_{7,\ell-1,3} \approx_c \mathsf{G}_{7,\ell-1,3}$. The proof in "honest case" is analogous to that in Section 3.3, the "corrupted or malicious case" has some difference and we provide it in Section B.4.

– $\mathsf{G}_{7,\ell-1,4}$: Identical to $\mathsf{G}_{7,\ell-1,3}$ except that we replace all $\mathbf{d}_\ell^\top$ in crs with

$$\mathbf{d}_\ell^\top \quad \text{where} \quad \boxed{\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_2^\top)}$$

In particular, we change the dashed boxed term in crs and pk_i as follows:

$$[\boxed{\boxed{\mathbf{d}_\ell^\top}, \mathbf{W}_0\mathbf{d}_\ell^\top + \mathbf{k}^\top + \mathbf{c}^\perp\alpha}]_2, \{[\mathbf{W}_i(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top})]_2, [\mathbf{U}_i\boxed{\mathbf{d}_\ell^\top}]_2\}_{i\in[L]\setminus\{\ell\}}$$

We have $\mathsf{G}_{7,\ell-1,4} \approx_c \mathsf{G}_{7,\ell-1,3}$. This follow from the $\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_3\mapsto\mathbf{B}_2}$ assumption which ensure that

$$[\mathbf{t}_0]_2 \approx_c [\mathbf{t}_1]_2 \quad \text{given} \quad [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_2^{\|}, \mathbf{B}_3^{\|}), \mathsf{basis}(\mathbf{B}_1^{\|})$$

Where $\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{B}_3^\top)$ corresponding to $\mathsf{G}_{7,\ell-1,2}$, and $\mathbf{d}_\ell \leftarrow \mathsf{span}(\mathbf{B}_2^\top)$ corresponding to $\mathsf{G}_{7,\ell-1,3}$.

– $\mathsf{G}_{7,\ell-1,5}$: Identical to $\mathsf{G}_{7,\ell-1,4}$ except that we generate the $\mathbf{c}_2^*$ as follows:

$$\mathbf{c}_2^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_i$$

We have $\mathsf{G}_{7,\ell-1,5} \approx_c \mathsf{G}_{7,\ell-1,4}$. The proof is identical to that for $\mathsf{G}_{7,\ell-1,3} \approx \mathsf{G}_{7,\ell-1,2}$.

Observe that $\mathsf{G}_{7,\ell-1,5} = \mathsf{G}_{7,\ell}$ and this prove $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$.

B.3 From $\mathsf{G}_{7,\ell-1,1}$ to $\mathsf{G}_{7,\ell-1,2}$

The proof idea is analogous to that in Section 3.3 and [ZZGQ23]: For all $j \in [\ell-1]$, we rewrite $\mathbf{d}_j \leftarrow \mathsf{span}(\mathbf{B}_2^\top)$ with $\mathbf{B}_2^\top r_j$, for some $r_j \leftarrow \mathbb{Z}_p$. And we we define $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$ and $\mathbf{c}\mathbf{c}^\perp = 1$. With the orthogonality of dual basis, we can define $\mathbf{d}^\perp \in \mathsf{span}((\mathbf{B}_3^{\|})^\top)$ such that:

$$\mathbf{d}^\perp\mathbf{B}_1 = \mathbf{0}, \quad \mathbf{d}^\perp\mathbf{B}_2 = \mathbf{0}, \quad \mathbf{d}^\perp\mathbf{d}_\ell^\top = 1.$$

With Lemma 2, we also need to consider following two cases:

Honest Case. In this case, we have $\mathsf{pk}_\ell^* = ([\mathbf{T}_\ell^*, \mathbf{Q}_\ell^*]_1, \{[\mathbf{h}_{\ell,j}^{*\top}]_2\}_{j\in[L]\setminus\{\ell\}}, \pi_\ell^*) \in D_\ell \setminus C_\ell$. Namely, we know $\mathbf{U}_\ell^*$ (such that $\mathbf{T}_\ell^* = \mathbf{A}\mathbf{U}_\ell^*$ and $\mathbf{Q}_\ell^* = \widehat{\mathbf{R}}_\ell\mathbf{U}_\ell^*$) and $\mathbf{U}_\ell^*$ is hidden from the adversary. We can write the $\mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}$ in $\mathbf{c}_1^*$ as $\boxed{\mathbf{c}\mathbf{U}_\ell^*}$, and replace $\widehat{\mathbf{R}}_\ell$ in crs with a random $\mathbf{R}_\ell$ as in G_1. We prove $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$ in this case using the following argument for $b' = 1$ (in $\mathsf{G}_{7,\ell-1,1}$) or $b' = 0$ (in $\mathsf{G}_{7,\ell-1,2}$):

$$\begin{aligned}
&\mathbf{A}, \mathbf{c}^\perp, [\mathbf{R}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_0, \mathbf{W}_0\mathbf{B}_1, \mathbf{W}_0\mathbf{B}_2, \mathbf{W}_0\mathbf{d}_\ell^\top + b'\mathbf{c}^\perp\alpha \\
&\mathbf{c}, \mathbf{c}\mathbf{W}_0 + \mathbf{c}\mathbf{U}_\ell^*, \mathbf{A}\mathbf{U}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^*]_1, \mathbf{U}_\ell^*\mathbf{B}_1, \mathbf{U}_\ell^*\mathbf{B}_2 \\
\approx_c\ &\mathbf{A}, \mathbf{c}^\perp, [\mathbf{R}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_0, \mathbf{W}_0\mathbf{B}_1, \mathbf{W}_0\mathbf{B}_2, \mathbf{W}_0\mathbf{d}_\ell^\top + b'\mathbf{c}^\perp\alpha \\
&\mathbf{c}, \mathbf{c}\mathbf{W}_0 + \mathbf{c}\mathbf{U}_\ell^*, \mathbf{A}\mathbf{U}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \boxed{\widehat{\mathbf{u}}^\top\mathbf{d}^\perp}]_1, \mathbf{U}_\ell^*\mathbf{B}_1, \mathbf{U}_\ell^*\mathbf{B}_2 \\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, [\mathbf{R}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_0, \mathbf{W}_0\mathbf{B}_1, \mathbf{W}_0\mathbf{B}_2, \mathbf{W}_0\mathbf{d}_\ell^\top + b'\mathbf{c}^\perp\alpha + \boxed{\mathbf{c}^\perp w} \\
&\mathbf{c}, \mathbf{c}\mathbf{W}_0 + \mathbf{c}\mathbf{U}_\ell^* + \boxed{w\mathbf{d}^\perp + u_\ell\mathbf{d}^\perp}, \mathbf{A}\mathbf{U}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \boxed{\mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{d}^\perp} + \widehat{\mathbf{u}}^\top\mathbf{d}^\perp]_1, \mathbf{U}_\ell^*\mathbf{B}_1, \mathbf{U}_\ell^*\mathbf{B}_2 \\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, [\mathbf{R}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_0, \mathbf{W}_0\mathbf{B}_1, \mathbf{W}_0\mathbf{B}_2, \mathbf{W}_0\mathbf{d}_\ell^\top + \cancel{b'\mathbf{c}^\perp\alpha} + \mathbf{c}^\perp w \\
&\mathbf{c}, \mathbf{c}\mathbf{W}_0 + \mathbf{c}\mathbf{U}_\ell^* + w\mathbf{d}^\perp + u_\ell\mathbf{d}^\perp, \mathbf{A}\mathbf{U}_\ell^*, [\mathbf{R}_\ell\mathbf{U}_\ell^* + \mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{d}^\perp + \widehat{\mathbf{u}}^\top\mathbf{d}^\perp]_1, \mathbf{U}_\ell^*\mathbf{B}_1, \mathbf{U}_\ell^*\mathbf{B}_2
\end{aligned}$$

where $\widehat{\mathbf{u}} \leftarrow \mathbb{Z}_p^{1\times(2k+2)}$ and $u_\ell \leftarrow \mathbb{Z}_p$, $\mathbf{w}_\ell \leftarrow \mathbb{Z}_p^{1\times n}$. We justify each step as below: The first $\approx_c$ uses Lemma 2 with $\mathbf{M} = \binom{\mathbf{A}}{\mathbf{c}}$, $\mathbf{R} = \mathbf{R}_\ell$, $\mathbf{U} = \mathbf{U}_\ell^*$, $\mathbf{u} = \widehat{\mathbf{u}}$. The second $\approx_s$ uses change of variables

$$\mathbf{W}_0 \mapsto \mathbf{W}_0 + \mathbf{c}^\perp w\mathbf{d}^\perp \quad \text{and} \quad \mathbf{U}_\ell \mapsto \mathbf{U}_\ell + \mathbf{c}^\perp u_\ell\mathbf{d}^\perp$$

The last $\approx_s$ follows from the fact that $\widehat{\mathbf{u}}$ hides $\mathbf{R}\mathbf{c}^\perp u_\ell$, this implies that u_ℓ can hide w in $\mathbf{c}_1^*$, and w hides $b'\alpha$ in crs.

Corrupted & Malicious Case. In this case, we have $\mathsf{pk}^*_\ell \in \mathcal{C}_\ell \cup \overline{\mathcal{D}}_\ell$. And we only consider $\mathsf{m}^*_0 \neq \mathsf{m}^*_1$ here, since we don't need to handle $\mathbf{k}^\top$ to hide m^*_b if they are equal. It is required that $\mathbf{x}^*_0(\mathbf{y}^*_\ell)^\top \neq 0 \wedge \mathbf{x}^*_1(\mathbf{y}^*_\ell)^\top \neq 0$. We prove $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$ in this case using the following argument for $b' = 1$ (in $\mathsf{G}_{7,\ell-1,1}$) or $b' = 0$ (in $\mathsf{G}_{7,\ell-1,2}$):

$$
\begin{aligned}
& \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{A}\mathbf{W}_0, \mathbf{W}_0\mathbf{B}_1, \mathbf{W}_0\mathbf{B}_2, \mathbf{W}_0\mathbf{d}^\top_\ell + b'\mathbf{c}^\perp\alpha \\
& \mathbf{c}, \mathbf{c}\mathbf{W}_0 + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}^*_\ell)^\top \otimes \mathbf{I}_{2k+1}), \mathbf{x}^*_b \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{A}\mathbf{W}_0, \mathbf{W}_0\mathbf{B}_1, \mathbf{W}_0\mathbf{B}_2, \mathbf{W}_0\mathbf{d}^\top_\ell + b'\mathbf{c}^\perp\alpha + \boxed{w\mathbf{d}^\perp} \\
& \mathbf{c}, \mathbf{c}\mathbf{W}_0 + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}^*_\ell)^\top \otimes \mathbf{I}_{2k+1}) + \boxed{w\mathbf{d}^\perp - \mathbf{x}^*_b(\mathbf{y}^*_\ell)^\top\mathbf{v}^{(3)}}, \cancel{\mathbf{x}^*_b \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_\ell \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{A}\mathbf{W}_0, \mathbf{W}_0\mathbf{B}_1, \mathbf{W}_0\mathbf{B}_2, \mathbf{W}_0\mathbf{d}^\top_\ell + \cancel{b'\mathbf{c}^\perp\alpha} + w\mathbf{d}^\perp \\
& \mathbf{c}, \mathbf{c}\mathbf{W}_0 + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}^*_\ell)^\top \otimes \mathbf{I}_{2k+1}) + w\mathbf{d}^\perp - \mathbf{x}^*_b(\mathbf{y}^*_\ell)^\top\mathbf{v}^{(3)}, \mathbf{c}\mathbf{W}_\ell
\end{aligned}
$$

We justify each step as follows: the first $\approx_s$ uses the change of variables

$$\mathbf{W}_\ell \mapsto \mathbf{W}_\ell - \mathbf{c}^\perp(\mathbf{x}^*_b \otimes \mathbf{v}^{(3)}) \quad \text{and} \quad \mathbf{W}_0 \mapsto \mathbf{W}_0 + \mathbf{c}^\perp w\mathbf{d}^\perp$$

The second $\approx_s$ uses the fact that $\mathbf{v}$ is hidden and $\mathbf{x}_b(\mathbf{y}^*_\ell)^\top \neq 0$ (which is different to our slotted Reg-IPFE), so that $\mathbf{x}^*_b(\mathbf{y}^*_\ell)^\top\mathbf{v}^{(3)}$ hides w, so we have $b'\alpha$ is hidden.

B.4 From $\mathsf{G}_{7,\ell-1,2}$ to $\mathsf{G}_{7,\ell-1,3}$ in Corrupted & Malicious Case

In this section, we present the proof of "corrupted & malicious case" in $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,3}$, which is different to that in Section 3.3; and we omit the proof of "honest case", which is identical to that in Section 3.3. In the "corrupted & malicious case", we have $\mathsf{pk}^*_\ell \in \mathcal{C}_\ell \cup \overline{\mathcal{D}}_\ell$. It is required that $\mathbf{x}^*_0(\mathbf{y}^*_\ell)^\top \neq 0 \wedge \mathbf{x}^*_1(\mathbf{y}^*_\ell)^\top \neq 0$ or $\mathbf{x}^*_0(\mathbf{y}^*_\ell)^\top = \mathbf{x}^*_1(\mathbf{y}^*_\ell)^\top = 0$. We prove $\mathsf{G}_{7,\ell-1,3} \approx_c \mathsf{G}_{7,\ell-1,2}$ in this case using the following argument for $b' = b$ (in $\mathsf{G}_{7,\ell-1,2}$) or $b' = 0$ (in $\mathsf{G}_{7,\ell-1,3}$):

$$
\begin{aligned}
& \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}^*_\ell)^\top \otimes \mathbf{I}_{2k+1}), \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}^*_\ell)^\top \otimes \mathbf{I}_{2k+1}) - \boxed{\mathbf{x}^*_{b'}(\mathbf{y}^*_\ell)^\top\mathbf{v}^{(3)}}, \cancel{\mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_\ell \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{R}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell((\mathbf{y}^*_\ell)^\top \otimes \mathbf{I}_{2k+1}) - \cancel{\mathbf{x}^*_{b'}(\mathbf{y}^*_\ell)^\top\mathbf{v}^{(3)}}, \mathbf{c}\mathbf{W}_\ell
\end{aligned}
$$

We justify each step as follows: the first $\approx_s$ uses the change of variables

$$\mathbf{W}_\ell \mapsto \mathbf{W}_\ell - \mathbf{c}^\perp(\mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)})$$

The second $\approx_s$ uses the fact that $\mathbf{v}^{(3)}$ is hidden (which is different to that in slotted Reg-IPFE c.f. Section 3.3), so that $\mathbf{x}^*_{b'}(\mathbf{y}^*_\ell)^\top\mathbf{v}^{(3)}$ can be hidden by $\mathbf{v}^{(3)}$ no matter $\mathbf{x}^*_{b'}(\mathbf{y}^*_\ell)^\top \neq 0$ or $\mathbf{x}^*_{b'}(\mathbf{y}^*_\ell)^\top = 0$.

C Slotted Reg-IPFE with Very Selective SIM-Security

This section gives a self-contained description of our slotted Reg-IPFE with very selective SIM-security which is implied by our pre-constrained slotted Reg-IPFE in Section 6.

C.1 Scheme

Assuming a QA-NIZK $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ for linear space over bilinear groups, see Section 2.4; our multi-instance slotted Reg-IPFE scheme, works as follows in the prime-order bilinear group:

– $\mathsf{Setup}(1^\lambda, 1^m, 1^n, 1^{L_1}, \ldots, 1^{L_m})$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample shared parts:

$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{V}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times n},\ \mathbf{V}_2 \leftarrow \mathbb{Z}_p^{(2k+1)\times k+1},\ \mathbf{v} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}.$$

And sample

$$\mathbf{D} \leftarrow \mathbb{Z}_p^{(k+1)\times k},\ \mathbf{w} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$$

For each instance $q \in [m]$, sample $\mathbf{B}_q \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, and for all $i \in [L_q]$, do following operations:

- Sample $\mathbf{t}_{q,i} \leftarrow \mathbb{Z}_p^{1\times k}$, for $s \in \{1, 2\}$, set

$$[\mathbf{M}_{q,i}]_s = \begin{bmatrix} \mathbf{I}_n & \mathbf{0}_n^\top \\ \mathbf{0}_{(k+1)\times n} & \mathbf{D}\mathbf{t}_{q,i}^\top \\ \mathbf{0}_n & \mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top \end{bmatrix}_s \in \mathbb{G}_s^{(n_1+n)\times(n_2+1)}.$$

- Sample

$$\mathbf{W}_{1,q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times n(k+1)},\ \mathbf{W}_{2,q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)(k+1)},\ \mathbf{W}_{3,q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)},$$

  and

$$\mathbf{R}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)},\ \mathbf{r}_{q,i} \leftarrow \mathbb{Z}_p^{1\times k},\ \mathbf{t}_{q,i} \leftarrow \mathbb{Z}_p^{1\times k}.$$

- Run $(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_{q,i}]_1)$, where

$$\mathbf{A}_{q,i} = \begin{pmatrix} \mathbf{A} \\ \mathbf{R}_{q,i} \end{pmatrix} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}.$$

Output[10]

$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \mathbf{A}\mathbf{V}_1, \mathbf{A}\mathbf{V}_2, \mathbf{A}\mathbf{v}^\top]_1, \\ \left\{ \begin{array}{l} \{\mathsf{crs}_{q,i}, [\mathbf{R}_{q,i}, \mathbf{A}\mathbf{W}_{1,q,i}, \mathbf{A}\mathbf{W}_{2,q,i}, \mathbf{A}\mathbf{W}_{3,q,i}, \mathbf{A}(\mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q,i}(\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}))]_1\}_{i\in[L_q]} \\ \{[\mathbf{D}\mathbf{t}_{q,j}^\top, \mathbf{w}\mathbf{D}\mathbf{t}_{q,j}^\top, \mathbf{B}_q\mathbf{r}_{q,j}^\top, \mathbf{W}_{1,q,j}(\mathbf{I}_n \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{V}_1]_2\}_{j\in[L_q]}, \\ \{[\mathbf{W}_{2,q,j}(\mathbf{D}\mathbf{t}_{q,j}^\top \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{W}_{3,q,j}(\mathbf{w}\mathbf{D}\mathbf{t}_{q,j}^\top \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{V}_2\mathbf{D}\mathbf{t}_{q,j}^\top + \mathbf{v}^\top\mathbf{w}\mathbf{D}\mathbf{t}_{q,j}^\top]_2\}_{j\in[L_q]} \\ \{[\mathbf{W}_{1,q,i}(\mathbf{I}_n \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top), \mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{W}_{3,q,i}(\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top)]_2\}_{j\in[L_q], i\in[L_q]\setminus\{j\}} \end{array} \right\}_{q\in[m]} \end{array} \right).$$

– $\mathsf{Gen}(\mathsf{crs}, q, i)$: Sample $\mathbf{U}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$. Define $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}} = \binom{\mathbf{A}\mathbf{U}_{q,i}}{\mathbf{R}_{q,i}\mathbf{U}_{q,i}} = \mathbf{A}_{q,i}\mathbf{U}_{q,i} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$ and run

$$\pi_{q,i} \leftarrow \mathsf{LPrv}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \mathbf{U}_{q,i}).$$

Fetch $\{[\mathbf{B}_q\mathbf{r}_{q,j}^\top]_2\}_{j\in[L_q]\setminus\{i\}}$ from crs and output

$$\mathsf{pk}_{q,i} = ([\underbrace{\mathbf{A}\mathbf{U}_{q,i}}_{\mathbf{T}_{q,i}}, \underbrace{\mathbf{R}_{q,i}\mathbf{U}_{q,i}}_{\mathbf{Q}_{q,i}}]_1, \{[\underbrace{\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^\top}_{\mathbf{h}_{q,i,j}}]_2\}_{j\in[L_q]\setminus\{i\}}, \pi_{q,i}) \quad \text{and} \quad \mathsf{sk}_{q,i} = \mathbf{U}_{q,i}.$$

[10] Note that we employ i as the index for $\mathbf{W}_q$'s and $\mathbf{M}_q$'s while j is the index for $\mathbf{r}_q$'s; both of them range from 1 to L_q. One exception is the terms with $\mathbf{W}_q$, which is conceptually $\mathbf{W}_{q,i}(\mathbf{M}_{q,i} \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top)$ with $i = j$. Note that we do not use $\mathsf{td}_{q,1}, \ldots, \mathsf{td}_{q,L_q}$ and isk in the actual scheme.

– $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i})$: Parse $\mathsf{pk}_{q,i} = \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j \in [L_q] \setminus \{i\}}, \pi_{q,i}\big)$. Write $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}}$ and check

$$\mathsf{LVer}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \pi_{q,i}) \stackrel{?}{=} 1.$$

For each $j \in [L_q] \setminus \{i\}$, check

$$e([\mathbf{A}]_1, [\mathbf{h}_{q,i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_{q,i}]_1, [\mathbf{B}_q \mathbf{r}_{q,j}^\top]_2).$$

If all these checks pass, output 1; otherwise, output 0.

– $\mathsf{Agg}_+(\mathsf{crs})$: Output:

$$\mathsf{mpk}_+ = ([\mathbf{A}, \mathbf{A}\mathbf{V}_1, \mathbf{A}\mathbf{V}_2, \mathbf{A}\mathbf{v}^\top]_1).$$

– $\mathsf{Agg}(\mathsf{crs}, q, (\mathsf{pk}_{q,i}, \mathbf{y}_{q,i})_{i \in [L_q]})$: If q is an empty instance, on input $(\mathsf{pk}_{q,i}, \mathbf{y}_{q,i}) = (\perp, \perp)$ for all $i \in [L_q]$, abort and return $\mathsf{mpk}_q = \perp$, $\mathsf{hsk}_{q,j} = \perp$ for all $j \in [L_q]$. For all $i \in [L_q]$, parse $\mathsf{pk}_{q,i} = \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j \in [L] \setminus \{i\}}, \pi_{q,i}\big)$, and set $\overline{\mathbf{y}}_{q,i} = (\mathbf{y}_{q,i} \| 1) \in \mathbb{Z}_p^{1 \times (n_2+1)}$. Output:

$$\mathsf{mpk}_q = \left[\sum_{i \in [L_q]} (\mathbf{T}_{q,i} + \mathbf{A}(\mathbf{W}_{1,q,i}(\mathbf{y}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q,i}(\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}))) \right]_1,$$

and for all $j \in [L_q]$

$$\mathsf{hsk}_{q,j} = \Bigg(\Bigg[\underbrace{\mathbf{B}_q \mathbf{r}_{q,j}^\top}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i \in [L_q] \setminus \{j\}} (\mathbf{h}_{q,i,j} + \mathbf{W}_{1,q,i}(\mathbf{y}_{q,i}^\top \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top) + \mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top) + \mathbf{W}_{3,q,i}(\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top)),}_{\mathbf{k}_1^\top}$$

$$\underbrace{\mathbf{W}_{1,q,j}(\mathbf{y}_{q,j}^\top \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top) + \mathbf{W}_{2,q,j}(\mathbf{D}\mathbf{t}_{q,j}^\top \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top) + \mathbf{W}_{3,q,j}(\mathbf{w}\mathbf{D}\mathbf{t}_{q,j}^\top \otimes \mathbf{B}_q \mathbf{r}_{q,j}^\top) + \mathbf{V}_1 \mathbf{y}_{q,j}^\top + \mathbf{V}_2 \mathbf{D}\mathbf{t}_{q,j}^\top + \mathbf{v}^\top \mathbf{w}\mathbf{D}\mathbf{t}_{q,j}^\top,}_{\mathbf{k}_2^\top}$$

$$\underbrace{\mathbf{D}\mathbf{t}_{q,j}^\top}_{\mathbf{k}_3^\top}, \underbrace{\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top}_{k_4} \Bigg]_2\Bigg).$$

– $\mathsf{Enc}_+(\mathsf{mpk}_+, \mathbf{x})$: Set $\overline{\mathbf{x}} = (\mathbf{x} \| \mathbf{0}_n) \in \mathbb{Z}_p^{1 \times (n_1+n)}$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$. Output:

$$\mathsf{ct}_+ = ([\underbrace{\mathbf{s}\mathbf{A}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{V}_1 + \mathbf{x}}_{\mathbf{c}_{+,1}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{V}_2}_{\mathbf{c}_{+,2}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{v}^\top}_{c_{+,3}}]_1).$$

– $\mathsf{Enc}(\mathsf{mpk}_q)$: Abort and return $\perp$ if $\mathsf{mpk}_q = \perp$. Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$, output

$$\mathsf{ct}_q = \Bigg[\underbrace{\sum_{i \in [L_q]} (\mathbf{s}\mathbf{T}_{q,i} + \mathbf{s}\mathbf{A}(\mathbf{W}_{1,q,i}(\mathbf{y}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q,i}(\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1})))}_{\mathbf{c}_q} \Bigg]_1.$$

– $\mathsf{Dec}(\mathsf{sk}_{q^*,i^*}, \mathsf{hsk}_{q^*,i^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*}))$: Abort and return $\perp$ if $\mathsf{ct}_{q^*} = \perp$. Parse

$$\mathsf{sk}_{q^*,i^*} = \mathbf{U}_{q^*,i^*}, \quad \mathsf{hsk}_{q^*,i^*} = ([\mathbf{k}_0^\top, \mathbf{k}_1^\top, \mathbf{k}_2^\top, \mathbf{k}_3^\top, k_4]_2), \quad (\mathsf{ct}_+, \mathsf{ct}_{q^*}) = ([\mathbf{c}_{+,0}, \mathbf{c}_{+,1}, \mathbf{c}_{+,2}, c_{+,3}, \mathbf{c}_{q^*}]_1).$$

Recover

$$\begin{aligned} [z_1]_T &= e([\mathbf{c}_{q^*}]_1, [\mathbf{k}_0^\top]_2), & [z_2]_T &= e([\mathbf{c}_{+,0}]_1, [\mathbf{k}_1^\top]_2), \\ [z_3]_T &= e([\mathbf{c}_{+,0}\mathbf{U}_{q^*,i^*}]_1, [\mathbf{k}_0^\top]_2), & [z_4]_T &= e([\mathbf{c}_{+,0}]_1, [\mathbf{k}_2^\top]_2), \\ [z_5]_T &= e([\mathbf{c}_{+,1}]_1, [\mathbf{y}_{q^*,i^*}^\top]_2), & [z_6]_T &= e([\mathbf{c}_{+,2}]_1, [\mathbf{k}_3^\top]_2), \\ [z_7]_T &= e([c_{+,3}]_1, [k_4]_2). \end{aligned}$$

Compute

$$[z]_T = [z_1 - z_2 - z_3 - z_4 + z_5 + z_6 + z_7]_T.$$

Recover z from $[z]_T$ via brute-force DLOG and output z.

Completeness. For all $\lambda, m, n \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $q \in [m]$ and $i \in [L_q]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^n, 1^{L_1}, \ldots, 1^{L_m})$, and $(\mathsf{pk}_{q,i}, \mathsf{sk}_{q,i}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q, i)$, we have

$$\begin{aligned}\mathsf{pk}_{q,i} &= \big([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j \in [L_q] \setminus \{i\}}, \pi_{q,i}\big) \\ &= \big([\mathbf{A}\mathbf{U}_{q,i}, \mathbf{R}_{q,i}\mathbf{U}_{q,i}]_1, \{[\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}^\top_{q,j}]_2\}_{j \in [L_q] \setminus \{i\}}, \pi_{q,i}\big)\end{aligned}$$

for some $\mathbf{U}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$ and $\pi_{q,i} \leftarrow \mathsf{LPrv}(\mathsf{crs}_{q,i}, [\mathbf{A}_{q,i}\mathbf{U}_i]_1, \mathbf{U}_i)$ where $(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_{q,i}]_1)$ and $\mathbf{A}_{q,i} = \binom{\mathbf{A}}{\mathbf{R}_{q,i}}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$, $\mathbf{R}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}$. Then

- Write $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}} = \binom{\mathbf{A}\mathbf{U}_{q,i}}{\mathbf{R}_{q,i}\mathbf{U}_{q,i}}$, we have $\mathsf{LVer}(\mathsf{crs}_{q,i}, [\mathbf{F}_{q,i}]_1, \pi_{q,i}) = 1$ by the perfect completeness of Π_0 (see Section 2.4) and the fact that $\mathbf{F}_{q,i} = \mathbf{A}_{q,i}\mathbf{U}_{q,i}$;
- For each $j \in [L_q] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}^\top_{q,j}]_2) = e([\mathbf{A}\mathbf{U}_{q,i}]_1, [\mathbf{B}_q\mathbf{r}^\top_{q,j}]_2)$ by the definition of bilinear map e (see Section 2.1) and the fact that $\mathbf{A} \cdot \mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}^\top_{q,j} = \mathbf{A}\mathbf{U}_{q,i} \cdot \mathbf{B}_q\mathbf{r}^\top_{q,j}$.

This ensures that $\mathsf{Ver}(\mathsf{crs}, q, i, \mathsf{pk}_{q,i}) = 1$ by the specification of Ver and readily proves the completeness.

Correctness. For all $\lambda, m, n \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $q^* \in [m]$ and $i^* \in [L_{q^*}]$; all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^m, 1^n, 1^{L_1}, \ldots, 1^{L_m})$, all $(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, q^*, i^*)$; all $\{\mathsf{pk}_{q^*,i}\}_{i \in [L_{q^*}] \setminus \{i^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, q^*, i, \mathsf{pk}_{q^*,i}) = 1$; all $\mathbf{x} \in \mathbb{Z}_p^{1\times n}$ and $\mathbf{y}_{q^*,i} \in \mathbb{Z}_p^{1\times n}$; for $s \in \{1, 2\}$, we have:

$$\begin{aligned}
\mathsf{sk}_{q^*,i^*} &= \mathbf{U}_{q^*,i^*}, \\
\mathsf{ct}_+ &= ([\underbrace{\mathbf{s}\mathbf{A}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{V}_1 + \mathbf{x}}_{\mathbf{c}_{+,1}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{V}_2}_{\mathbf{c}_{+,2}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{v}^\top}_{c_{+,3}}]_1), \\
\mathsf{ct}_{q^*} &= \Bigg[\underbrace{\sum_{i \in [L_{q^*}]} (\mathbf{s}\mathbf{T}_{q^*,i} + \mathbf{s}\mathbf{A}(\mathbf{W}_{1,q^*,i}(\mathbf{y}^\top_{q^*,i} \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,q^*,i}(\mathbf{D}\mathbf{t}^\top_{q^*,i} \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q^*,i}(\mathbf{w}\mathbf{D}\mathbf{t}^\top_{q^*,i} \otimes \mathbf{I}_{k+1})))}_{\mathbf{c}_{q^*}}\Bigg]_1,
\end{aligned}$$

$$\begin{aligned}
\mathsf{hsk}_{q^*,i^*} = \Bigg(\Bigg[&\underbrace{\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i \in [L_{q^*}] \setminus \{i^*\}} (\mathbf{h}_{q^*,i,i^*} + \mathbf{W}_{1,q^*,i}(\mathbf{y}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{2,q^*,i}(\mathbf{D}\mathbf{t}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{3,q^*,i}(\mathbf{w}\mathbf{D}\mathbf{t}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}))}_{\mathbf{k}_1^\top}, \\
&\underbrace{\mathbf{W}_{1,q^*,i^*}(\mathbf{y}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{2,q^*,i^*}(\mathbf{D}\mathbf{t}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{3,q^*,i^*}(\mathbf{w}\mathbf{D}\mathbf{t}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{V}_1\mathbf{y}^\top_{q^*,i^*} + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_{q^*,i^*} + \mathbf{v}^\top\mathbf{w}\mathbf{D}\mathbf{t}^\top_{q^*,i^*}}_{\mathbf{k}_2^\top}, \\
&\underbrace{\mathbf{D}\mathbf{t}^\top_{q^*,i^*}}_{\mathbf{k}_3^\top}, \underbrace{\mathbf{w}\mathbf{D}\mathbf{t}^\top_{q^*,i^*}}_{k_4}\Bigg]_2\Bigg).
\end{aligned}$$

where

$$\mathbf{A}\mathbf{h}_{q^*,i,i^*} = \mathbf{T}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} \quad \forall i \in [L_{q^*}] \setminus \{i^*\} \quad \text{and} \quad \mathbf{A}\mathbf{U}_{q^*,i^*} = \mathbf{T}_{q^*,i^*}.$$

Note that here we actually consider $\mathsf{hsk}_{q^*,j}$ for $j = i^*$ and $\mathsf{sk}_{q^*,i}$ for $i = i^*$ and all above equalities are ensured by Ver and Gen. We have

$$
\begin{aligned}
z_1 &= \sum_{i \in [L_{q^*}]} (\mathbf{sT}_{q^*,i} + \mathbf{sA}(\mathbf{W}_{1,q^*,i}(\mathbf{y}^\top_{q^*,i} \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,q^*,i}(\mathbf{Dt}^\top_{q^*,i} \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q^*,i}(\mathbf{wDt}^\top_{q^*,i} \otimes \mathbf{I}_{k+1})))\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} \\
&= \sum_{i \in [L_{q^*}]} (\mathbf{sT}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} + \mathbf{sA}(\mathbf{W}_{1,q^*,i}(\mathbf{y}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{2,q^*,i}(\mathbf{Dt}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{3,q^*,i}(\mathbf{wDt}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*})) \quad (31) \\
z_2 &= \sum_{i \in [L_{q^*}] \setminus \{i^*\}} (\mathbf{sAh}_{q^*,i,i^*} + \mathbf{sA}(\mathbf{W}_{1,q^*,i}(\mathbf{y}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{2,q^*,i}(\mathbf{Dt}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{3,q^*,i}(\mathbf{wDt}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}))))\\
z_3 &= \mathbf{sAU}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} \\
z_4 &= \mathbf{sA}(\mathbf{W}_{1,q^*,i^*}(\mathbf{y}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{2,q^*,i^*}(\mathbf{Dt}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{3,q^*,i^*}(\mathbf{wDt}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*})) \\
&\quad + \mathbf{sA}(\mathbf{V}_1\mathbf{y}^\top_{q^*,i^*} + \mathbf{V}_2\mathbf{Dt}^\top_{q^*,i^*} + \mathbf{v}^\top\mathbf{wDt}^\top_{q^*,i^*})) \\
z_5 &= \mathbf{sAV}_1\mathbf{y}^\top_{q^*,i^*} + \mathbf{xy}^\top_{q^*,i^*} \\
z_6 &= \mathbf{sAV}_2\mathbf{Dt}^\top_{q^*,i^*} \\
z_7 &= \mathbf{sAv}^\top\mathbf{wDt}^\top_{q^*,i^*}
\end{aligned}
$$

and then

$$
\begin{aligned}
z &= z_1 - z_2 - z_3 - z_4 + z_5 + z_6 + z_7 \\
&= \mathbf{sT}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} + \mathbf{sA}(\mathbf{W}_{1,q^*,i^*}(\mathbf{y}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{2,q^*,i^*}(\mathbf{Dt}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{3,q^*,i^*}(\mathbf{wDt}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) \\
&\quad - \mathbf{sAU}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} - \mathbf{sA}(\mathbf{W}_{1,q^*,i^*}(\mathbf{y}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{2,q^*,i^*}(\mathbf{Dt}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}_{3,q^*,i^*}(\mathbf{wDt}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*})) \\
&\quad - \mathbf{sA}(\mathbf{V}_1\mathbf{y}^\top_{q^*,i^*} + \mathbf{V}_2\mathbf{Dt}^\top_{q^*,i^*} + \mathbf{v}^\top\mathbf{wDt}^\top_{q^*,i^*})) \\
&\quad + \mathbf{sAV}_1\mathbf{y}^\top_{q^*,i^*} + \mathbf{xy}^\top_{q^*,i^*} + \mathbf{sAV}_2\mathbf{Dt}^\top_{q^*,i^*} + \mathbf{sAv}^\top\mathbf{wDt}^\top_{q^*,i^*} \quad (32) \\
&= \mathbf{xy}^\top_{q^*,i^*} \quad (33)
\end{aligned}
$$

Here, equality (31) follows from the property of tensor product: $(\mathbf{a}^\top \otimes \mathbf{I})\mathbf{M} = \mathbf{a}^\top \otimes \mathbf{M}$ for matrices of proper size; equality (32) follows from the fact that $\mathbf{Ah}_{q^*,i,i^*} = \mathbf{T}_i\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}$ for all $i \in [L_{q^*}] \setminus \{i^*\}$; equality (33) follows from the fact that $\mathbf{T}_{q^*,i^*} = \mathbf{AU}_{q^*,i^*}$.

Compactness and Efficiency. Our multi-instance PReg-IPFE has the following properties:

$$
\begin{aligned}
|\mathsf{crs}| &= O(L^2 \cdot n) \cdot \mathsf{poly}(\lambda), & |\mathsf{hsk}_{q,j}| &= \mathsf{poly}(\lambda), \\
|\mathsf{mpk}_+| &= O(n)\mathsf{poly}(\lambda), & |\mathsf{mpk}_q| &= \mathsf{poly}(\lambda), \\
|\mathsf{ct}_+| &= O(n) + \mathsf{poly}(\lambda), & |\mathsf{ct}_q| &= \mathsf{poly}(\lambda),
\end{aligned}
$$

where $L = L_1 + \cdots + L_m$. Note that the total size of $\{\mathsf{crs}_i\}_{i \in [L]}$ is $L \cdot \mathsf{poly}(\lambda)$ according to the efficiency of the pairing-based QA-NIZK scheme by Kiltz and Wee [KW15] and the fact that the size of language description is $\mathsf{poly}(\lambda)$.

Security. We have the following theorem. Given pairing-based QA-NIZK in [KW15] with unbounded simulation soundness under MDDH assumption, our multi-instance slotted Reg-IPFE scheme uses prime-order bilinear group and the security can be reduced to MDDH assumption.

Theorem 8. *Assume* $\Pi_0 = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ *is a QA-NIZK with perfect completeness, perfect zero-knowledge and unbounded simulation soundness for linear space defined in Section 2.4, our multi-instance slotted Reg-IPFE scheme achieves the very selective SIM-security as the definition in Section 5.1, under bi-MDDH assumption.*

C.2 Simulator

Recall that we allow some instance q^* to be empty, namely $\mathcal{M}_{q^*}, C_{q^*} = \perp$ and $\mathbf{y}_{q^*,i} = \perp$, $\mathsf{pk}_{q^*,i} = \perp$ for all $i \in [L_{q^*}]$. Our simulator is as follows:

– $\widetilde{\mathsf{Setup}}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^n; \{\{\mathbf{y}_{q,i}\}_{i\in[L_q]}, \{\mu_{q,i}\}_{i\in\mathcal{M}_q\cup C_q}\}_{q\in[m]})$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample shared parts:

$$\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)},\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{V}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times n},\ \mathbf{V}_2 \leftarrow \mathbb{Z}_p^{(2k+1)\times k+1},\ \mathbf{v} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}.$$

And sample

$$\mathbf{D} \leftarrow \mathbb{Z}_p^{(k+1)\times k},\ \mathbf{w} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$$

For each instance $q \in [m]$, sample $\mathbf{B}_q \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, for all $i \in [L_q]$, $s \in \{1,2\}$, set

$$[\widetilde{\mathbf{M}}_{q,i}]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}_{n_1}^\top \\ \mathbf{0}_{n\times n_2} & \mathsf{ict}_{q,i}^\top \end{bmatrix}_s \quad \text{where} \quad [\mathsf{ict}_{q,i}]_s \in \begin{cases} \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0) & \text{if } i \in [L_q] \setminus (\mathcal{M}_q \cup C_q) \\ \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mu_{q,i}) & \text{if } i \in \mathcal{M}_q \cup C_q \end{cases}$$

and for all $i \in [L_q]$, do following operations:

- Set
$$\theta_{q,i} = \begin{cases} 0 & \text{if } i \in [L_q] \setminus (\mathcal{M}_q \cup C_q) \\ \mu_{q,i} & \text{if } i \in \mathcal{M}_q \cup C_q \end{cases}$$
- Sample
$$\mathbf{W}_{1,q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times n(k+1)},\ \mathbf{W}_{2,q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)(k+1)},\ \mathbf{W}_{3,q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)},$$
  and
$$\widetilde{\mathbf{R}}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)},\ \mathbf{r}_{q,i} \leftarrow \mathbb{Z}_p^{1\times k},\ \mathbf{t}_{q,i} \leftarrow \mathbb{Z}_p^{1\times k}.$$
  and compute
$$\widehat{\mathbf{R}}_{q,i} = \widetilde{\mathbf{R}}_{q,i} \begin{pmatrix} \mathbf{c} \\ \mathbf{I}_{2k+1} \end{pmatrix}.$$
- Run $(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_{q,i}]_1)$, where
$$\mathbf{A}_{q,i} = \begin{pmatrix} \mathbf{A} \\ \widehat{\mathbf{R}}_{q,i} \end{pmatrix} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}.$$

Output

$$\widetilde{\mathsf{crs}} = \left(\begin{array}{l} [\mathbf{A}, \mathbf{A}\mathbf{V}_1, \mathbf{A}\mathbf{V}_2, \mathbf{A}\mathbf{v}^\top]_1, \\ \left\{ \begin{array}{l} \{\mathsf{crs}_{q,i}, [\widehat{\mathbf{R}}_{q,i}, \mathbf{A}\mathbf{W}_{1,q,i}, \mathbf{A}\mathbf{W}_{2,q,i}, \mathbf{A}\mathbf{W}_{3,q,i}, \mathbf{A}(\mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q,i}((\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top + \theta_{q,i}) \otimes \mathbf{I}_{k+1}))]_1\}_{i\in[L_q]} \\ \{[\mathbf{D}\mathbf{t}_{q,j}^\top, \mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top + \theta_{q,i}, \mathbf{B}_q\mathbf{r}_{q,j}^\top, \mathbf{W}_{1,q,j}(\mathbf{I}_n \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{V}_1]_2\}_{j\in[L_q]}, \\ \{[\mathbf{W}_{2,q,j}(\mathbf{D}\mathbf{t}_{q,j}^\top \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{W}_{3,q,j}((\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top + \theta_{q,i}) \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{V}_2\mathbf{D}\mathbf{t}_{q,j}^\top + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top + \theta_{q,i})]_2\}_{j\in[L_q]} \\ \{[\mathbf{W}_{1,q,i}(\mathbf{I}_n \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top), \mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top) + \mathbf{W}_{3,q,i}((\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top + \theta_{q,i}) \otimes \mathbf{B}_q\mathbf{r}_{q,j}^\top)]_2\}_{j\in[L_q], i\in[L_q]\setminus\{j\}} \end{array} \right\}_{q\in[m]} \end{array} \right).$$

And set the trapdoor as

$$\mathsf{td} = \left(\mathbf{c}, \mathbf{V}_1, \mathbf{V}_2, \mathbf{v}, \mathbf{w}, \left\{ \{\widetilde{\mathbf{R}}_{q,i}, \mathsf{td}_{q,i}\}_{i\in[L_q]} \right\}_{q\in[m]} \right)$$

for all $q \in [m]$, if q is not empty instance, update

$$\mathsf{td} = \mathsf{td} \cup \left\{ \sum_{i\in[L_q]} \mathbf{c}(\mathbf{W}_{1,q,i}(\mathbf{y}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q,i}((\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top + \theta_{q,i}) \otimes \mathbf{I}_{k+1})) \right\}$$

– $\widetilde{\mathsf{Gen}}(\widetilde{\mathsf{crs}}, q, i; \mathsf{td})$: Fetch $\mathsf{td}_{q,i}$ from td. Sample $\mathbf{U}_{q,i} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$. Define $\mathbf{F}_{q,i} = \binom{\mathbf{T}_{q,i}}{\mathbf{Q}_{q,i}} = \binom{\mathbf{A}\mathbf{U}_{q,i}}{\widehat{\mathbf{R}}_{q,i}\mathbf{U}_{q,i}} = \mathbf{A}_{q,i}\mathbf{U}_{q,i} \in \mathbb{Z}_p^{(3k+2)\times(2k+1)}$ and run

$$\widetilde{\pi}_{q,i} \leftarrow \mathsf{LSim}(\mathsf{crs}_{q,i}, \mathsf{td}_{q,i}, [\mathbf{F}_{q,i}]_1).$$

Fetch $\{[\mathbf{B}_q\mathbf{r}_{q,j}^\top]_2\}_{j\in[L_q]\setminus\{i\}}$ from $\widetilde{\mathsf{crs}}$ and output

$$\widetilde{\mathsf{pk}}_{q,i} = \big([\underbrace{\mathbf{A}\mathbf{U}_{q,i}}_{\mathbf{T}_{q,i}}, \underbrace{\widehat{\mathbf{R}}_{q,i}\mathbf{U}_{q,i}}_{\mathbf{Q}_{q,i}}]_1, \{[\underbrace{\mathbf{U}_{q,i}\mathbf{B}_q\mathbf{r}_{q,j}^\top}_{\mathbf{h}_{q,i,j}}]_2\}_{j\in[L_q]\setminus\{i\}}, \widetilde{\pi}_{q,i}\big) \quad \text{and} \quad \widetilde{\mathsf{sk}}_{q,i} = \mathbf{U}_{q,i}.$$

– $\widetilde{\mathsf{Enc}}_+(\mathsf{td})$: Fetch $\mathbf{c}, \mathbf{V}_1, \mathbf{V}_2, \mathbf{v}, \mathbf{w}$ from td, set $\widetilde{\mathbf{x}} = (\mathbf{0}_{n_1}\|\mathsf{isk})$. Output

$$\widetilde{\mathsf{ct}}_+ = ([\underbrace{\mathbf{c}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{c}\mathbf{V}_1}_{\mathbf{c}_{+,1}}, \underbrace{\mathbf{c}\mathbf{V}_2 - \mathbf{w}}_{\mathbf{c}_{+,2}}, \underbrace{\mathbf{c}\mathbf{v}^\top + 1}_{c_{+,3}}]_1)$$

– $\widetilde{\mathsf{Enc}}((\mathsf{pk}_{q,1}, \ldots, \mathsf{pk}_{q,L_q}); \mathsf{td})$: If q is an empty instance, on input $\mathsf{pk}_{q,i} = \perp$ for all $i \in [L_q]$, abort and return $\widetilde{\mathsf{ct}}_q = \perp$. For all $i \in [L_q]$, parse $\mathsf{pk}_{q,i} = ([\mathbf{T}_{q,i}, \mathbf{Q}_{q,i}]_1, \{[\mathbf{h}_{q,i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_{q,i})$. Fetch $\{\widetilde{\mathbf{R}}_{q,i}\}_{i\in[L_q]}$ and $\sum_{i\in[L_q]} \mathbf{c}(\mathbf{W}_{1,q,i}(\mathbf{y}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q,i}((\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top + \theta_{q,i}) \otimes \mathbf{I}_{k+1}))$ from td. Output:

$$\widetilde{\mathsf{ct}}_q = \Bigg[\underbrace{\sum_{i\in[L_q]} (\mathbf{e}_1\widetilde{\mathbf{R}}_{q,i}^{-1}\mathbf{Q}_{q,i} + \mathbf{c}(\mathbf{W}_{1,q,i}(\mathbf{y}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,q,i}(\mathbf{D}\mathbf{t}_{q,i}^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,q,i}((\mathbf{w}\mathbf{D}\mathbf{t}_{q,i}^\top + \theta_{q,i}) \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_q}\Bigg]_1.$$

C.3 Proof

We prove the following technical lemma this immediately proves Theorem 8.

Lemma 8. *For all adversaries $\mathcal{A}$, there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ such that:*

$$\mathsf{Adv}_{\mathcal{A}}^{\textit{miReg-IPFE}}(\lambda) \le L \cdot \mathsf{Adv}_{\mathcal{B}_1}^{\textit{USS}}(\lambda) + (3L + 2L\cdot Q + 1)\mathsf{Adv}_{\mathcal{B}_2}^{\textit{MDDH}}(\lambda) + \mathsf{negl}(\lambda)$$

where $L = L_1 + \ldots + L_m$ is the number of slots, Q is the maximum number of queries on a slot made by $\mathcal{A}$ and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2) \approx \mathsf{Time}(\mathcal{A})$.

For simplicity, we prove Lemma 8 in the case of nonempty 1-instance and remove the index q in the following proof. For an empty instance, we only need to remove the terms about ct_1^* and all pk_i^* in following game sequence, and notice that $\mathcal{M}^*, \mathcal{C}^* = \emptyset$ for empty instance. In the case of m-instance, it only needs to add back index q and apply sub-sequence $\mathsf{G}_{8,\ell-1,0}, \ldots, \mathsf{G}_{8,\ell-1,3}$ to each instance.

Game Sequence. Suppose that crs is the common reference string, $\mathbf{x}^*$ is the challenge, $\{\mathsf{pk}_i^*, \mathbf{y}_i^*\}_{i\in[L]}$ are challenge public keys along with challenge functions to be registered, $\mathcal{M}^*, \mathcal{C}^* \subseteq [L]$ are the sets of malicious and corrupted slots. For all $i \in [L]$, define $D_i = \{\mathsf{pk}_i : \mathcal{D}_{1,i}[\mathsf{pk}_i] = \mathsf{sk}_i \neq \perp\}$ be responses to $\mathsf{OGen}(i)$ and $C_i = \{\mathsf{pk}_i : (i, \mathsf{pk}_i) \in \mathcal{C}_1\}$ records public keys in D_i that have been sent to $\mathsf{OCor}(i, \cdot)$. Recall that, for each $i \in [L]$, we require that

$$\begin{aligned} i \in \mathcal{M}^* &\implies \mathsf{pk}_i^* \notin D_i \wedge \mathsf{Ver}(\mathsf{crs}, 1, i, \mathsf{pk}_i^*) = 1 \\ i \in \mathcal{C}^* &\implies \mathsf{pk}_i^* \in C_i \\ i \in [L] \setminus (\mathcal{M}^* \cup \mathcal{C}^*) &\implies \mathsf{pk}_i^* \in D_i \wedge \mathsf{pk}_i^* \notin C_i \end{aligned}$$

Note that pk_i serves as a *general* entry in D_i while pk_i^* is the *specific* challenge public for slot i; there can be more than one assignment for pk_i since the adversary can invoke $\mathsf{OGen}(i)$ for many times. We prove the Lemma 4 via dual-system method using the following game sequence.

– G_0: This is the real game, recall that we have

- crs is in the form:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{A}\mathbf{V}_1, \mathbf{A}\mathbf{V}_2, \mathbf{A}\mathbf{v}^\top]_1, \\ \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{A}\mathbf{W}_{1,i}, \mathbf{A}\mathbf{W}_{2,i}, \mathbf{A}\mathbf{W}_{3,i}, \mathbf{A}(\mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,i}(\mathbf{wDt}_i^\top \otimes \mathbf{I}_{k+1}))]_1\}_{i\in[L]} \\ \{[\mathbf{Dt}_j^\top, \mathbf{wDt}_j^\top, \mathbf{Br}_j^\top, \mathbf{W}_{1,j}(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{V}_1]_2\}_{j\in[L]}, \\ \{[\mathbf{W}_{2,j}(\mathbf{Dt}_j^\top \otimes \mathbf{Br}_j^\top) + \mathbf{W}_{3,j}(\mathbf{wDt}_j^\top \otimes \mathbf{Br}_j^\top) + \mathbf{V}_2\mathbf{Dt}_j^\top + \mathbf{v}^\top\mathbf{wDt}_j^\top]_2\}_{j\in[L]} \\ \{[\mathbf{W}_{1,i}(\mathbf{I}_n \otimes \mathbf{Br}_j^\top), \mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{Br}_j^\top) + \mathbf{W}_{3,i}(\mathbf{wDt}_i^\top \otimes \mathbf{Br}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$

where $\mathsf{crs}_i \in \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$, with $\mathbf{A}_i = \begin{pmatrix} \mathbf{A} \\ \mathbf{R}_i \end{pmatrix}$.

- For each $i \in [L]$, each $\mathsf{pk}_i \in D_i$ is in the form

$$\mathsf{pk}_i = \big([\underbrace{\mathbf{A}\mathbf{U}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{R}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{[\underbrace{\mathbf{U}_i\mathbf{Br}_j^\top}_{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$$

where $\pi_i \longleftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i)$, $\mathbf{F}_i = \binom{\mathbf{A}\mathbf{U}_i}{\mathbf{R}\mathbf{U}_i}$, and $\mathbf{U}_i$ is the corresponding sk_i.

- For all $i \in [L]$, pk_i^* is in the form:

$$\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{h}_{i,j}^*]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$$

such that $\mathsf{Ver}(\mathsf{crs}, 1, i, \mathsf{pk}_i^*) = 1$ which means $\mathsf{LVer}\left(\mathsf{crs}_i, \begin{bmatrix} \mathbf{T}_i^* \\ \mathbf{Q}_i^* \end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{A}\mathbf{h}_{i,j}^* = \mathbf{T}_i^*\mathbf{Br}_j^\top$ for each $j \in [L] \setminus \{i\}$.

- ct_+^* for $\mathbf{x}^*$ is in the form:

$$\mathsf{ct}_+^* = ([\underbrace{\mathbf{sA}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{sAV}_1 + \mathbf{x}^*}_{\mathbf{c}_{+,1}}, \underbrace{\mathbf{sAV}_2}_{\mathbf{c}_{+,2}}, \underbrace{\mathbf{sAv}^\top}_{c_{+,3}}]_1).$$

- ct_1^* for $\mathbf{x}^*$ is in the form:

$$\mathsf{ct}_1^* = \underbrace{\left[\sum_{i\in[L_q]} (\mathbf{sT}_i + \mathbf{sA}(\mathbf{W}_{1,i}(\mathbf{y}_i^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,i}(\mathbf{wDt}_i^\top \otimes \mathbf{I}_{k+1})))\right]_1}_{\mathbf{c}_q}.$$

– G_1: Identical to G_0, except that for all $i \in [L]$, we replace $\mathbf{wDt}_i^\top$ in crs with

$$\mathbf{wDt}_i^\top + \boxed{\theta_i} \quad \text{where} \quad \theta_i = \begin{cases} 0 & \text{if } i \in [L_q] \setminus (\mathcal{M}_q \cup \mathcal{C}_q) \\ \boxed{\mathbf{x}^*(\mathbf{y}_i^*)^\top} & \text{if } i \in \mathcal{M}_q \cup \mathcal{C}_q \end{cases}$$

In particuar, we generate crs as

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{A}\mathbf{V}_1, \mathbf{A}\mathbf{V}_2, \mathbf{A}\mathbf{v}^\top]_1, \\ \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{A}\mathbf{W}_{1,i}, \mathbf{A}\mathbf{W}_{2,i}, \mathbf{A}\mathbf{W}_{3,i}, \mathbf{A}(\mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,i}((\mathbf{wDt}_i^\top + \boxed{\theta_i}) \otimes \mathbf{I}_{k+1}))]_1\}_{i\in[L]} \\ \{[\mathbf{Dt}_j^\top, (\mathbf{wDt}_j^\top + \boxed{\theta_j}), \mathbf{Br}_j^\top, \mathbf{W}_{1,j}(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{V}_1]_2\}_{j\in[L]}, \\ \{[\mathbf{W}_{2,j}(\mathbf{Dt}_j^\top \otimes \mathbf{Br}_j^\top) + \mathbf{W}_{3,j}((\mathbf{wDt}_j^\top + \boxed{\theta_j}) \otimes \mathbf{Br}_j^\top) + \mathbf{V}_2\mathbf{Dt}_j^\top + \mathbf{v}^\top(\mathbf{wDt}_j^\top + \boxed{\theta_j})]_2\}_{j\in[L]} \\ \{[\mathbf{W}_{1,i}(\mathbf{I}_n \otimes \mathbf{Br}_j^\top), \mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{Br}_j^\top) + \mathbf{W}_{3,i}((\mathbf{wDt}_i^\top + \boxed{\theta_i}) \otimes \mathbf{Br}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix},$$

and generate challenge ciphertext ct_1^* as

$$\Bigg[\underbrace{\sum_{i\in[L_q]}(\mathbf{s}\mathbf{T}_i + \mathbf{s}\mathbf{A}(\mathbf{W}_{1,i}(\mathbf{y}_i^\top\otimes\mathbf{I}_{k+1}) + \mathbf{W}_{2,i}(\mathbf{D}\mathbf{t}_i^\top\otimes\mathbf{I}_{k+1}) + \mathbf{W}_{3,i}((\mathbf{w}\mathbf{D}\mathbf{t}_i^\top + \boxed{\theta_i})\otimes\mathbf{I}_{k+1})))}_{\mathbf{c}_q}\Bigg]_1.$$

We have $\mathsf{G}_1 \approx_c \mathsf{G}_0$. This follows from MDDH assumption which ensures that $([\mathbf{D}]_1, [\mathbf{w}\mathbf{D}\mathbf{t}_i^\top]_1) \approx_c ([\mathbf{D}]_1, [\mathbf{w}\mathbf{D}\mathbf{t}_i^\top + \theta_i]_1)$ when $\mathbf{D} \leftarrow \mathbb{Z}_p^{(k+1)\times k}, \mathbf{t}_i \leftarrow \mathbb{Z}_p^{1\times k}, \mathbf{w} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$.

– G_2: Identical to G_1 except that for all $i \in [L]$ and all $\mathsf{pk}_i \in D_i$, we replace π_i with

$$\widetilde{\pi}_i \leftarrow \boxed{\mathsf{LSim}}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{F}_i]_1) \quad \text{where} \quad \mathbf{F}_i = \begin{pmatrix}\mathbf{A}\mathbf{U}_i\\ \mathbf{R}_i\mathbf{U}_i\end{pmatrix}.$$

We have $\mathsf{G}_2 \equiv \mathsf{G}_1$. This follows from the perfect zero-knowledge of Π_0.

– G_3: Identical to G_2 except that we sample $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ along with $\mathbf{A}$ and replace all $\mathbf{R}_i$ in crs with

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i\begin{pmatrix}\mathbf{s}\mathbf{A}\\ \mathbf{I}_{2k+1}\end{pmatrix}, \quad \widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}.$$

We have $\mathsf{G}_3 \equiv \mathsf{G}_2$. This follows from the fact that both $\mathbf{R}_i$ (in G_2) and $\widehat{\mathbf{R}}_i$ (in G_3) are truly random since matrix $\binom{\mathbf{s}\mathbf{A}}{\mathbf{I}_{2k+1}}$ is full-rank.

– G_4: Identical to G_3 except that we generate the $\mathbf{c}_1^*$ as follows:

$$\mathbf{c}_1^* = \sum_{i\in[L]}(\boxed{\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*} + \mathbf{s}\mathbf{A}(\mathbf{W}_{1,i}(\mathbf{y}_i^\top\otimes\mathbf{I}_{k+1}) + \mathbf{W}_{2,i}(\mathbf{D}\mathbf{t}_i^\top\otimes\mathbf{I}_{k+1}) + \mathbf{W}_{3,i}((\mathbf{w}\mathbf{D}\mathbf{t}_i^\top + \theta_i)\otimes\mathbf{I}_{k+1})))$$

We have $\mathsf{G}_4 \approx_c \mathsf{G}_3$. This follows from stronger unbounded simulation soundness of Π_0 along with the fact that $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i^*], \pi_i^*) = 1$ for all $i \in [L]$ where $\mathbf{F}_i^* = \begin{pmatrix}\mathbf{T}_i^*\\ \mathbf{Q}_i^*\end{pmatrix}$. The details are identical to that in game G_3 of our sReg-IPFE (c.f. Section 3).

– G_5: Identical to G_4 except that we replace all $\mathbf{s}\mathbf{A}$ with $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$; in particular, we generate $\widehat{\mathbf{R}}_i$ as follows:

$$\widehat{\mathbf{R}}_i = \widetilde{\mathbf{R}}_i\begin{pmatrix}\boxed{\mathbf{c}}\\ \mathbf{I}_{2k+1}\end{pmatrix}, \quad \widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}$$

and generate the challenge ciphertext ct_+^* as follows:

$$\mathsf{ct}_+^* = ([\underbrace{\boxed{\mathbf{c}}}_{\mathbf{c}_{+,0}}, \underbrace{\boxed{\mathbf{c}}\mathbf{V}_1 + \mathbf{x}^*}_{\mathbf{c}_{+,1}}, \underbrace{\boxed{\mathbf{c}}\mathbf{V}_2}_{\mathbf{c}_{+,2}}, \underbrace{\boxed{\mathbf{c}}\mathbf{v}^\top}_{c_{+,3}}]_1).$$

generate the challenge ciphertext ct_1^* as follows:

$$\mathsf{ct}_1^* = \left(\Bigg[\underbrace{\sum_{i\in[L]}(\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^* + \boxed{\mathbf{c}}(\mathbf{W}_{1,i}(\mathbf{y}_i^\top\otimes\mathbf{I}_{k+1}) + \mathbf{W}_{2,i}(\mathbf{D}\mathbf{t}_i^\top\otimes\mathbf{I}_{k+1}) + \mathbf{W}_{3,i}((\mathbf{w}\mathbf{D}\mathbf{t}_i^\top + \theta_i)\otimes\mathbf{I}_{k+1})))}_{\mathbf{c}_1^*}\Bigg]_1\right).$$

We have $\mathsf{G}_5 \approx_c \mathsf{G}_4$. This follows from MDDH assumption which ensures that $([\mathbf{A}]_1, [\mathbf{s}\mathbf{A}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{c}]_1)$ when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}, \mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$.

– G_6: Identical to G_5 except that

- we generate $\mathbf{c}_+^*$ as follows:

$$\mathsf{ct}_+^* = ([\underbrace{\mathbf{c}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{c}\mathbf{V}_1 + \cancel{\mathbf{x}^*}}_{\mathbf{c}_{+,1}}, \underbrace{\mathbf{c}\mathbf{V}_2}_{\mathbf{c}_{+,2}}, \underbrace{\mathbf{c}\mathbf{v}^\top}_{c_{+,3}}]_1).$$

- In crs, we change $[\mathbf{W}_{1,j}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{V}_1]_2$ for all $j \in [L]$ as follows:

$$[\mathbf{W}_{1,j}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{V}_1 + \boxed{\mathbf{c}^\perp(-\mathbf{x}^*)}]_2.$$

  where $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{c}\mathbf{c}^\perp = 1$ and $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$.

  We have $\mathsf{G}_6 \approx_s \mathsf{G}_5$. This follows from the change of variable $\mathbf{V}_1 \mapsto \mathbf{V}_1 + \mathbf{c}^\perp(-\mathbf{x}^*)$.

- G_7: Identical to G_6, except that

  - we generate $\mathbf{c}_+^*$ as follows:

$$\mathsf{ct}_+^* = ([\underbrace{\mathbf{c}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{c}\mathbf{V}_1}_{\mathbf{c}_{+,1}}, \underbrace{\mathbf{c}\mathbf{V}_2 + \boxed{-\mathbf{w}}}_{\mathbf{c}_{+,2}}, \underbrace{\mathbf{c}\mathbf{v}^\top + \boxed{1}}_{c_{+,3}}]_1).$$

  - In crs, we change $[\mathbf{W}_{2,j}(\mathbf{D}\mathbf{t}_j^\top \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{W}_{3,j}((\mathbf{w}\mathbf{D}\mathbf{t}_j^\top + \theta_j) \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{V}_2\mathbf{D}\mathbf{t}_j^\top + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}_j^\top + \theta_j)]_2$ for all $j \in [L]$ as follow:

$$[\mathbf{W}_{2,j}(\mathbf{D}\mathbf{t}_j^\top \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{W}_{3,j}((\mathbf{w}\mathbf{D}\mathbf{t}_j^\top + \theta_j) \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{V}_2\mathbf{D}\mathbf{t}_j^\top + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}_j^\top + \theta_j) + \boxed{\mathbf{c}^\perp\theta_j}]_2$$

  where $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{c}\mathbf{c}^\perp = 1$ and $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$.

  We have $\mathsf{G}_7 \approx_s \mathsf{G}_6$. This follows from the change of variable $\mathbf{V}_2 \mapsto \mathbf{V}_2 + \mathbf{c}^\perp(-\mathbf{w})$ and $\mathbf{v} \mapsto \mathbf{v} + \mathbf{c}^\perp$.

- $\mathsf{G}_{8,\ell}$, ($\ell \in [0, L]$): Identical to G_8 except that for all $j \in [\ell]$, we change $[\mathbf{W}_{1,j}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{V}_1 + \mathbf{c}^\perp(-\mathbf{x}^*)]_2$ in crs as follows:

$$[\mathbf{W}_{1,j}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{V}_1 + \cancel{\mathbf{c}^\perp(-\mathbf{x}^*)}]_2.$$

  and change $[\mathbf{W}_{2,j}(\mathbf{D}\mathbf{t}_j^\top \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{W}_{3,j}((\mathbf{w}\mathbf{D}\mathbf{t}_j^\top + \theta_j) \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{V}_2\mathbf{D}\mathbf{t}_j^\top + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}_j^\top + \theta_j) + \mathbf{c}^\perp\theta_j]_2$ in crs as follows:

$$[\mathbf{W}_{2,j}(\mathbf{D}\mathbf{t}_j^\top \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{W}_{3,j}((\mathbf{w}\mathbf{D}\mathbf{t}_i^\top + \theta_i) \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{V}_2\mathbf{D}\mathbf{t}_j^\top + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}_i^\top + \theta_i) + \cancel{\mathbf{c}^\perp\theta_i}]_2$$

  We have that

  - $\mathsf{G}_{8,0} = \mathsf{G}_8$; the two games are actually identical, since $[0] = \emptyset$;
  - $\mathsf{G}_{8,\ell-1} \approx_c \mathsf{G}_{8,\ell}$ for all $\ell \in [L]$, we will employ a sub-sequence of games for the proof described later.

Observe that in the final game $\mathsf{G}_{8,L}$ can be simulated using the simulator by setting $\mu_i = \mathbf{x}^*(\mathbf{y}_i^*)^\top$, where we embed $\mathbf{x}^*(\mathbf{y}_i^*)^\top$ into crs so that hsk_i for all $i \in \mathcal{M}^* \cup \mathcal{C}^*$ and remove $\mathbf{x}^*$ from ct^*.

From $\mathsf{G}_{8,\ell-1}$ to $\mathsf{G}_{8,\ell}$. We are ready to prove $\mathsf{G}_{8,\ell-1} \approx_c \mathsf{G}_{8,\ell}$ and this will complete the proof of Lemma 4. For this, we need the following sub-sequence of games for each $\ell \in [L]$:

– $\mathsf{G}_{8,\ell-1,0}$: Identical to $\mathsf{G}_{8,\ell-1}$ where we recall crs, $\mathsf{pk}_i \in D_i$ and $\mathbf{c}_1^*$, with highlighting relevant terms in the following sub-sequence with dashed boxes as follows:

$$\mathsf{crs} = \left(\begin{array}{l}
[\mathbf{A}, \mathbf{AV}_1, \mathbf{AV}_2, \mathbf{Av}^\top]_1, \{[\mathbf{Dt}_j^\top, (\mathbf{wDt}_j^\top + \theta_j)]_2\}_{j\in[L]} \\
\left\{\mathsf{crs}_i, [\widehat{\mathbf{R}}_i, \mathbf{AW}_{1,i}, \mathbf{AW}_{2,i}, \mathbf{AW}_{3,i}, \mathbf{A}(\mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,i}((\mathbf{wDt}_i^\top + \theta_i) \otimes \mathbf{I}_{k+1}))]_1\right\}_{i\in[L]} \\
\left\{[\mathbf{Br}_j^\top, \mathbf{W}_{1,j}(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{V}_1]_2\right\}_{j\in[\ell-1]} \\
\boxed{[\mathbf{Br}_\ell^\top, \mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{Br}_\ell^\top) + \mathbf{V}_1 + \mathbf{c}^\perp(-\mathbf{x}^*)]_2} \\
\left\{[\mathbf{Br}_j^\top, \mathbf{W}_{1,j}(\mathbf{I}_n \otimes \mathbf{Br}_j^\top) + \mathbf{V}_1 + \mathbf{c}^\perp(-\mathbf{x}^*)]_2\right\}_{j\in[L]\setminus[\ell]} \\
\left\{[\mathbf{W}_{2,j}(\mathbf{Dt}_j^\top \otimes \mathbf{Br}_j^\top) + \mathbf{W}_{3,j}((\mathbf{wDt}_j^\top + \theta_j) \otimes \mathbf{Br}_j^\top) + \mathbf{V}_2\mathbf{Dt}_j^\top + \mathbf{v}^\top(\mathbf{wDt}_j^\top + \theta_j)]_2\right\}_{j\in[\ell-1]} \\
\boxed{[\mathbf{W}_{2,\ell}(\mathbf{Dt}_\ell^\top \otimes \mathbf{Br}_\ell^\top) + \mathbf{W}_{3,\ell}((\mathbf{wDt}_\ell^\top + \theta_\ell) \otimes \mathbf{Br}_\ell^\top) + \mathbf{V}_2\mathbf{Dt}_\ell^\top + \mathbf{v}^\top(\mathbf{wDt}_\ell^\top + \theta_\ell) + \mathbf{c}^\perp\theta_\ell]_2} \\
\left\{[\mathbf{W}_{2,j}(\mathbf{Dt}_j^\top \otimes \mathbf{Br}_j^\top) + \mathbf{W}_{3,j}((\mathbf{wDt}_j^\top + \theta_j) \otimes \mathbf{Br}_j^\top) + \mathbf{V}_2\mathbf{Dt}_j^\top + \mathbf{v}^\top(\mathbf{wDt}_j^\top + \theta_j) + \mathbf{c}^\perp\theta_j]_2\right\}_{j\in[L]\setminus[\ell]} \\
\left\{[\mathbf{W}_{1,i}(\mathbf{I}_n \otimes \mathbf{Br}_j^\top), \mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{Br}_j^\top) + \mathbf{W}_{3,i}((\mathbf{wDt}_i^\top + \theta_i) \otimes \mathbf{Br}_j^\top)]_2\right\}_{j\in[L]\setminus\{\ell\}, i\in[L]\setminus\{j\}}, \\
\boxed{\left\{[\mathbf{W}_{1,i}(\mathbf{I}_n \otimes \mathbf{Br}_\ell^\top), \mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{Br}_\ell^\top) + \mathbf{W}_{3,i}((\mathbf{wDt}_i^\top + \theta_i) \otimes \mathbf{Br}_\ell^\top)]_2\right\}_{i\in[L]\setminus\{\ell\}}}
\end{array}\right)$$

$$\mathsf{pk}_i = \begin{cases} ([\overbrace{\mathbf{AU}_i}^{\mathbf{T}_i}, \overbrace{\widehat{\mathbf{R}}_i\mathbf{U}_i}^{\mathbf{Q}_i}]_1, \{[\overbrace{\mathbf{U}_i\mathbf{d}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j\in[\ell-1]\setminus\{i\}}, \boxed{[\overbrace{\mathbf{U}_i\mathbf{Br}_\ell^\top}^{\mathbf{h}_{i,\ell}}]_2}, \{[\overbrace{\mathbf{U}_i\mathbf{Br}_j^\top}^{\mathbf{h}_{i,j}}]_2\}_{j\in[L]\setminus[i,\ell]}, \widetilde{\pi}_i) & \text{if } i \neq \ell \\ ([\underbrace{\mathbf{AU}_\ell}_{\mathbf{T}_\ell}, \underbrace{\widehat{\mathbf{R}}_i\mathbf{U}_\ell}_{\mathbf{Q}_\ell}]_1, \{[\underbrace{\mathbf{U}_\ell\mathbf{d}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j\in[\ell-1]}, \{[\underbrace{\mathbf{U}_\ell\mathbf{Br}_j^\top}_{\mathbf{h}_{\ell,j}}]_2\}_{j\in[L]\setminus[\ell]}, \widetilde{\pi}_\ell) & \text{if } i = \ell \end{cases}$$

$$\begin{aligned}\mathbf{c}_1^* = {} & \boxed{\mathbf{e}_1\widetilde{\mathbf{R}}_\ell^{-1}\mathbf{Q}_\ell^* + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}_\ell^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{Dt}_\ell^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{wDt}_\ell^\top + \theta_\ell) \otimes \mathbf{I}_{k+1}))} \\ & + \sum_{i\in[L]\setminus\{\ell\}} (\mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^* + \mathbf{c}(\mathbf{W}_{1,i}(\mathbf{y}_i^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,i}((\mathbf{wDt}_i^\top + \theta_i) \otimes \mathbf{I}_{k+1})))\end{aligned}$$

where $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ such that $\mathbf{cc}^\perp = 1$, $\mathbf{Ac}^\perp = \mathbf{0}$. For all $i \in [L]$, recall that

$$\theta_i = \begin{cases} 0 & \text{if } i \in [L] \setminus (\mathcal{M} \cup \mathcal{C}) \\ \mathbf{x}^*(\mathbf{y}_i^*)^\top & \text{if } i \in \mathcal{M} \cup \mathcal{C} \end{cases}$$

– $\mathsf{G}_{8,\ell-1,1}$: Identical to $\mathsf{G}_{8,\ell-1,0}$ except that we replace all $\mathbf{Br}_\ell^\top$ with $\mathbf{d}_\ell^\top \leftarrow \mathbb{Z}_p^{k+1}$ in crs; in particular, we change the dashed boxed term in crs and pk_i as follows:

$$\begin{array}{l}
[\boxed{\mathbf{d}_\ell^\top}, \mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top}) + \mathbf{V}_1 + \mathbf{c}^\perp(-\mathbf{x}^*)]_2 \\
[\mathbf{W}_{2,\ell}(\mathbf{Dt}_\ell^\top \otimes \boxed{\mathbf{d}_\ell^\top}) + \mathbf{W}_{3,\ell}((\mathbf{wDt}_\ell^\top + \theta_\ell) \otimes \boxed{\mathbf{d}_\ell^\top}) + \mathbf{V}_2\mathbf{Dt}_\ell^\top + \mathbf{v}^\top(\mathbf{wDt}_\ell^\top + \theta_\ell) + \mathbf{c}^\perp\theta_\ell]_2 \\
\left\{[\mathbf{W}_{1,i}(\mathbf{I}_n \otimes \boxed{\mathbf{d}_\ell^\top}), \mathbf{W}_{2,i}(\mathbf{Dt}_i^\top \otimes \boxed{\mathbf{d}_\ell^\top}) + \mathbf{W}_{3,i}((\mathbf{wDt}_i^\top + \theta_i) \otimes \boxed{\mathbf{d}_\ell^\top})]_2\right\}_{i\in[L]\setminus\{\ell\}}
\end{array}$$

We have $\mathsf{G}_{8,\ell-1,1} \approx_c \mathsf{G}_{8,\ell-1,0}$. This follows from MDDH assumption w.r.t. $[\mathbf{B}]_2$ which ensures that $([\mathbf{B}]_2, [\mathbf{Br}_\ell^\top]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{d}_\ell^\top]_2)$ when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{r}_\ell \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{d}_\ell \leftarrow \mathbb{Z}_p^{1\times(k+1)}$.

– $\mathsf{G}_{8,\ell-1,2}$: Identical to $\mathsf{G}_{8,\ell-1,1}$, except that we replace $\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{V}_1 + \mathbf{c}^\perp(-\mathbf{x}^*)$ with

$$\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}_\ell^\top) + \mathbf{V}_1 + \cancel{\mathbf{c}^\perp(-\mathbf{x}^*)}$$

and replace $\mathbf{W}_{2,\ell}(\mathbf{Dt}_\ell^\top \otimes \mathbf{d}_\ell^\top) + \mathbf{W}_{3,\ell}((\mathbf{wDt}_\ell^\top + \theta_\ell) \otimes \mathbf{d}_\ell^\top) + \mathbf{V}_2\mathbf{Dt}_\ell^\top + \mathbf{v}^\top(\mathbf{wDt}_\ell^\top + \theta_\ell) + \mathbf{c}^\perp\theta_\ell$ with

$$\mathbf{W}_{2,\ell}(\mathbf{Dt}_\ell^\top \otimes \mathbf{d}_\ell^\top) + \mathbf{W}_{3,\ell}((\mathbf{wDt}_\ell^\top + \theta_\ell) \otimes \mathbf{d}_\ell^\top) + \mathbf{V}_2\mathbf{Dt}_\ell^\top + \mathbf{v}^\top(\mathbf{wDt}_\ell^\top + \theta_\ell) + \cancel{\mathbf{c}^\perp\theta_\ell}$$

We have $\mathsf{G}_{8,\ell-1,2} \approx_c \mathsf{G}_{8,\ell-1,1}$. With defining $\mathbf{c}^\perp \in \mathbb{Z}_p^{2k+1}$ and $\mathbf{d}^\perp \in \mathbb{Z}_p^{1\times(k+1)}$ such that $\mathbf{cc}^\perp = 1$, $\mathbf{Ac}^\perp = \mathbf{0}$ and $\mathbf{d}^\perp\mathbf{d}_\ell^\top = 1$, $\mathbf{d}^\perp\mathbf{B} = \mathbf{0}$. We consider two cases

- Honest case ($\ell \in [L]\backslash(\mathcal{M}^*\cup\mathcal{C}^*)$): In this case, we have $\theta_\ell = 0$, and we have $\mathsf{pk}^*_\ell = ([\mathbf{T}^*_\ell, \mathbf{Q}^*_\ell]_1, \{[\mathbf{h}^{*\top}_{\ell,j}]_2\}_{j\in[L]\backslash\{\ell\}}, \pi^*_\ell) \in D_\ell \setminus C_\ell$. Namely, we know $\mathbf{U}^*_\ell$ (such that $\mathbf{T}^*_\ell = \mathbf{A}\mathbf{U}^*_\ell$ and $\mathbf{Q}^*_\ell = \widehat{\mathbf{R}}_\ell\mathbf{U}^*_\ell$) and $\mathbf{U}^*_\ell$ is hidden from the adversary. We can write the dash boxed terms in $\mathbf{c}^*_1$ as follows:

$$\boxed{\mathbf{c}\mathbf{U}^*_\ell} + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{I}_{k+1}))$$

and replace $\widehat{\mathbf{R}}_\ell$ in crs with a random $\mathbf{R}_\ell$ as in G_3. And we can proof $\mathsf{G}_{8,\ell-1,2} \approx_c \mathsf{G}_{8,\ell-1,1}$ in this case using the following argument for all $b \in \{0,1\}$:

$$\begin{aligned}
&\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_{1,\ell}, \mathbf{A}\mathbf{W}_{2,\ell}, \mathbf{A}\mathbf{W}_{3,\ell}, [\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_1 + b\mathbf{c}^\perp(-\mathbf{x}^*)]_2 \\
&[\mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) + b\mathbf{c}^\perp\theta_\ell]_2; \qquad /\!/\mathsf{crs},\ \mathsf{pk}_\ell \\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{I}_{k+1}))]_1 \\
&\mathbf{A}\mathbf{U}^*_\ell, [\mathbf{R}_\ell\mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell\mathbf{B} \qquad /\!/\mathsf{ct}^*,\ \mathsf{pk}^*_\ell \\
\approx_c\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_{1,\ell}, \mathbf{A}\mathbf{W}_{2,\ell}, \mathbf{A}\mathbf{W}_{3,\ell}, [\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_1 + b\mathbf{c}^\perp(-\mathbf{x}^*)]_2 \\
&[\mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) + b\mathbf{c}^\perp\theta_\ell]_2; \\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{I}_{k+1}))]_1 \\
&\mathbf{A}\mathbf{U}^*_\ell, [\mathbf{R}_\ell\mathbf{U}^*_\ell + \boxed{\widehat{\mathbf{u}}^\top\mathbf{d}^\perp}]_1, \mathbf{U}^*_\ell\mathbf{B} \\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_{1,\ell}, \mathbf{A}\mathbf{W}_{2,\ell}, \mathbf{A}\mathbf{W}_{3,\ell}, [\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_1 + \boxed{\mathbf{c}^\perp\mathbf{w}_\ell} + b\mathbf{c}^\perp(-\mathbf{x}^*)]_2, \\
&[\mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) + b\mathbf{c}^\perp\theta_\ell]_2; \\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{I}_{k+1})) + \boxed{u_\ell\mathbf{d}^\perp + \mathbf{w}_\ell(\mathbf{y}^*_\ell)^\top\mathbf{d}^\perp}]_1 \\
&\mathbf{A}\mathbf{U}^*_\ell, [\mathbf{R}_\ell\mathbf{U}^*_\ell + \boxed{\mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{d}^\perp} + \widehat{\mathbf{u}}^\top\mathbf{d}^\perp]_1, \mathbf{U}^*_\ell\mathbf{B} \\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{R}_\ell]_1, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_{1,\ell}, \mathbf{A}\mathbf{W}_{2,\ell}, \mathbf{A}\mathbf{W}_{3,\ell}, [\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_1 + \mathbf{c}^\perp\mathbf{w}_\ell + \cancel{b\mathbf{c}^\perp(-\mathbf{x}^*)}]_2, \\
&[\mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) + \cancel{b\mathbf{c}^\perp\theta_\ell}]_2; \\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{I}_{k+1})) + u_\ell\mathbf{d}^\perp + \mathbf{w}_\ell(\mathbf{y}^*_\ell)^\top\mathbf{d}^\perp]_1 \\
&\mathbf{A}\mathbf{U}^*_\ell, [\mathbf{R}_\ell\mathbf{U}^*_\ell + \mathbf{R}_\ell\mathbf{c}^\perp u_\ell\mathbf{d}^\perp + \widehat{\mathbf{u}}^\top\mathbf{d}^\perp]_1, \mathbf{U}^*_\ell\mathbf{B}
\end{aligned}$$

where $\widehat{\mathbf{u}} \leftarrow \mathbb{Z}_p^{1\times(2k+2)}$, $u_\ell \leftarrow \mathbb{Z}_p$ and $\mathbf{w}_\ell \leftarrow \mathbb{Z}_p^{n_1}$. We justify each step as below: The first $\approx_c$ follows the argument:

$$\begin{aligned}
&(\mathbf{A}, \mathbf{c}, [\mathbf{R}_\ell]_1, \mathbf{B}, \mathbf{d}^\perp, \mathbf{A}\mathbf{U}_\ell, \mathbf{c}\mathbf{U}_\ell[\mathbf{R}\mathbf{U}_\ell]_1, \qquad \mathbf{U}_\ell\mathbf{B}) \\
\approx_c\ &(\mathbf{A}, \mathbf{c}, [\mathbf{R}_\ell]_1, \mathbf{B}, \mathbf{d}^\perp, \mathbf{A}\mathbf{U}_\ell, \mathbf{c}\mathbf{U}_\ell, [\mathbf{R}_\ell\mathbf{U}_\ell + \boxed{\mathbf{u}^\top\mathbf{d}^\perp}]_1, \mathbf{U}_\ell\mathbf{B})
\end{aligned}$$

which is analogous to the Lemma 2 in [ZZGQ23]. The second $\approx_s$ uses the change of variables:

$$\mathbf{U}^*_\ell \mapsto \mathbf{U}^*_\ell + \mathbf{c}^\perp u_\ell\mathbf{d}^\perp \quad \text{and} \quad \mathbf{W}_{1,\ell} \mapsto \mathbf{W}_{1,\ell} + \mathbf{c}^\perp(\mathbf{w}_\ell \otimes \mathbf{d}^\perp)$$

The last $\approx_s$ is straight-forward with

  * the fact that $\theta_\ell = 0$ in this case;
  * the observation that $\widehat{\mathbf{u}}^\top$ hides $\mathbf{R}_\ell\mathbf{c}^\perp u_\ell$, this implies that u_ℓ hides $\mathbf{w}_\ell(\mathbf{y}^*_\ell)^\top$, and $\mathbf{w}_\ell$ is sufficient to hide $\mathbf{x}^*$.

- Corrupted & Malicious Case ($\ell \in (\mathcal{M}^* \cup C^*)$): And in this case, we have $\theta_\ell = \mathbf{x}^*(\mathbf{y}^*_\ell)^\top$, and we have $\mathsf{pk}^*_\ell = ([\mathbf{T}^*_\ell, \mathbf{Q}^*_\ell]_1, \{[\mathbf{h}^{*\top}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}}, \pi^*_\ell) \in C_\ell \cup \overline{D}_\ell$. We prove $\mathsf{G}_{8,\ell-1,2} \approx_c \mathsf{G}_{8,\ell-1,1}$ in this case using the following argument:

$$\begin{aligned}
&\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{A}\mathbf{W}_{1,\ell}, \mathbf{A}\mathbf{W}_{2,\ell}, \mathbf{A}\mathbf{W}_{3,\ell}, [\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_1 + \mathbf{c}^\perp(-\mathbf{x}^*)]_2\\
&[\mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) + \mathbf{c}^\perp\theta_\ell]_2;\\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{I}_{k+1}))]_1\\
\approx_s\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{A}\mathbf{W}_{1,\ell}, \mathbf{A}\mathbf{W}_{2,\ell}, \mathbf{A}\mathbf{W}_{3,\ell}, [\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_1 + \boxed{\mathbf{c}^\perp\mathbf{x}^*} + \mathbf{c}^\perp(-\mathbf{x}^*)]_2\\
&[\mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) + \boxed{\mathbf{c}^\perp\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{c}^\perp(-\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell - \theta_\ell)} + \mathbf{c}^\perp\theta_\ell]_2;\\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{I}_{k+1})) + \boxed{\mathbf{x}^*(\mathbf{y}^*_\ell)^\top\mathbf{d}^\perp + \mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell\mathbf{d}^\perp + (-\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell - \theta_\ell)\mathbf{d}^\perp}]_1\\
=\ &\mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{A}\mathbf{W}_{1,\ell}, \mathbf{A}\mathbf{W}_{2,\ell}, \mathbf{A}\mathbf{W}_{3,\ell}, [\mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_1 + \cancel{\mathbf{c}^\perp\mathbf{x}^* + \mathbf{c}^\perp(-\mathbf{x}^*)}]_2\\
&[\mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{d}^\top_\ell) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{d}^\top_\ell) + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) + \cancel{\mathbf{c}^\perp\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{c}^\perp(-\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell - \theta_\ell) + \mathbf{c}^\perp\theta_\ell}]_2;\\
&[\mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}(\mathbf{W}_{1,\ell}(\mathbf{y}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \mathbf{I}_{k+1}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \mathbf{I}_{k+1})) + \cancel{\mathbf{x}^*(\mathbf{y}^*_\ell)^\top\mathbf{d}^\perp + \mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell\mathbf{d}^\perp + (-\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell - \theta_\ell)\mathbf{d}^\perp}]_1
\end{aligned}$$

We justify each step as follows: The first $\approx_s$ uses the change of variables:

$$\mathbf{W}_{1,\ell} \mapsto \mathbf{W}_{1,\ell} + \mathbf{c}^\perp(\mathbf{x}^* \otimes \mathbf{d}^\perp), \quad \mathbf{W}_{2,\ell} \mapsto \mathbf{W}_{2,\ell} + \mathbf{c}^\perp(\mathbf{w} \otimes \mathbf{d}^\perp), \quad \mathbf{W}_{3,\ell} \mapsto \mathbf{W}_{3,\ell} + \mathbf{c}^\perp((-1) \otimes \mathbf{d}^\perp)$$

The second = follows from the fact that $\theta_\ell = \mathbf{x}^*(\mathbf{y}^*_\ell)^\top$ in this case.

– $\mathsf{G}_{8,\ell-1,3}$: Identical to $\mathsf{G}_{8,\ell-1,2}$ except that we replace all $\mathbf{d}^\top_\ell$ with $\mathbf{B}\mathbf{r}^\top_\ell$ where $\mathbf{r}^\top_\ell \leftarrow \mathbb{Z}_p^k$ in crs; in particular, we change the dashed boxed term in crs and pk_i as follows:

$$\begin{aligned}
&[\boxed{\mathbf{B}\mathbf{r}^\top_\ell}, \mathbf{W}_{1,\ell}(\mathbf{I}_n \otimes \boxed{\mathbf{B}\mathbf{r}^\top_\ell}) + \mathbf{V}_1 + \mathbf{c}^\perp(-\mathbf{x}^*)]_2\\
&[\mathbf{W}_{2,\ell}(\mathbf{D}\mathbf{t}^\top_\ell \otimes \boxed{\mathbf{B}\mathbf{r}^\top_\ell}) + \mathbf{W}_{3,\ell}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) \otimes \boxed{\mathbf{B}\mathbf{r}^\top_\ell}) + \mathbf{V}_2\mathbf{D}\mathbf{t}^\top_\ell + \mathbf{v}^\top(\mathbf{w}\mathbf{D}\mathbf{t}^\top_\ell + \theta_\ell) + \mathbf{c}^\perp\theta_\ell]_2\\
&\{[\mathbf{W}_{1,i}(\mathbf{I}_n \otimes \boxed{\mathbf{B}\mathbf{r}^\top_\ell}), \mathbf{W}_{2,i}(\mathbf{D}\mathbf{t}^\top_i \otimes \boxed{\mathbf{B}\mathbf{r}^\top_\ell}) + \mathbf{W}_{3,i}((\mathbf{w}\mathbf{D}\mathbf{t}^\top_i + \theta_i) \otimes \boxed{\mathbf{B}\mathbf{r}^\top_\ell})]_2\}_{i\in[L]\setminus\{\ell\}}
\end{aligned}$$

We have $\mathsf{G}_{8,\ell-1,1} \approx_c \mathsf{G}_{8,\ell-1,0}$. This follows from MDDH assumption w.r.t. $[\mathbf{B}]_2$ which ensures that $([\mathbf{B}]_2, [\mathbf{B}\mathbf{r}^\top_\ell]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{d}^\top_\ell]_2)$ when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{r}_\ell \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{d}_\ell \leftarrow \mathbb{Z}_p^{1\times(k+1)}$.

D Sanity Check of the Simulators

This section provides sanity check for all simulators appeared in this paper.

D.1 Sanity Check of the simulator in Section 6.2

In this section, we show that the simulator of our multi-instance slotted PReg-IPFE in Section 6.2 can pass the sanity check. The simulated $\widetilde{\mathsf{crs}}$ has the full capacity as the crs of the scheme in Section 6.1. For all $\lambda, m, n_1, n_2 \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $\mathbf{M} \in \mathbb{Z}_p^{n_1\times n_2}$, all $\{\mathcal{M}^*_q, C^*_q\}_{q\in[m]}$, all $\mathbf{f}'_{q,i} \in \mathbb{Z}_p^{1\times n_2}$, $\mu_{q,i} \in \mathbb{Z}_p$, all $q^* \in [m]$ and $i^* \in [L_{q^*}]$; all

$$\widetilde{\mathsf{crs}} \leftarrow \widetilde{\mathsf{Setup}}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2}, \mathbf{M}; \{\{\mathbf{f}'_{q,i}\}_{i\in[L_q]}, \{\mu_{q,i}\}_{i\in\mathcal{M}^*_q\cup C^*_q}\}_{q\in[m]}),$$

all $(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) \leftarrow \mathsf{Gen}(\widetilde{\mathsf{crs}}, q^*, i^*)$; all $\{\mathsf{pk}_{q^*,i}\}_{i \in [L_{q^*}] \setminus \{i^*\}}$ such that $\mathsf{Ver}(\widetilde{\mathsf{crs}}, q^*, i, \mathsf{pk}_{q^*,i}) = 1$; all $\mathbf{x} \in \mathbb{Z}_p^{1 \times n_1}$ and $\mathbf{f}_{q^*,i} \in \mathbb{Z}_p^{1 \times n_2}$; we have:

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{q^*,i^*}, \mathsf{hsk}_{q^*,i^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*})) = \mathbf{x}\mathbf{M}\mathbf{f}^\top_{q^*,i^*} \left| \begin{array}{l} \mathsf{mpk}_+ \leftarrow \mathsf{Agg}_+(\widetilde{\mathsf{crs}}); \\ (\mathsf{mpk}_{q^*}, (\mathsf{hsk}_{q^*,j})_{j \in [L_{q^*}]}) \leftarrow \mathsf{Agg}(\widetilde{\mathsf{crs}}, q^*, (\mathsf{pk}_{q^*,i}, \mathbf{f}_{q^*,i})_{i \in [L_{q^*}]}) \\ s \leftarrow \mathsf{Coin};\ \mathsf{ct}_+ \leftarrow \mathsf{Enc}_+(\mathsf{mpk}_+, \mathbf{x}; s);\ \mathsf{ct}_{q^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}_{q^*}; s) \end{array}\right.\right] = 1.$$

This follows from the fact that the analysis of correctness in Section 6.1: for $s \in \{1, 2\}$, we have:

$$\overline{\mathbf{x}} = (\mathbf{x} \| \mathbf{0}_n), \quad \overline{\mathbf{f}}_{q^*,i^*} = (\mathbf{f}_{q^*,i^*} \| 1)$$

and

$$[\widetilde{\mathbf{M}}_{q^*,i^*}]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}^\top_{n_1} \\ \mathbf{0}_{n \times n_2} & \mathsf{ict}^\top_{q^*,i^*} \end{bmatrix}_s \quad \text{where} \quad [\mathsf{ict}_{q^*,i^*}]_s \in \begin{cases} \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0) & \text{if } i^* \in [L_{q^*}] \setminus (\mathcal{M}^*_{q^*} \cup \mathcal{C}^*_{q^*}) \\ \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mu_{q^*,i^*}) & \text{if } i \in \mathcal{M}^*_{q^*} \cup \mathcal{C}^*_{q^*} \end{cases}$$

with $([\mathsf{ipk}]_1, [\mathsf{ipk}]_2) \in \mathsf{Gen}_1(1^\lambda)$. And for all $\mathbf{s} \leftarrow \mathbb{Z}_p^{1 \times k}$, we have

$$\begin{aligned}
\mathsf{sk}_{q^*,i^*} &= \mathbf{U}_{q^*,i^*}, \\
(\mathsf{ct}_+, \mathsf{ct}_{q^*}) &= \left(\left[\underbrace{\mathbf{s}\mathbf{A}}_{\mathbf{c}_{+,0}}, \underbrace{\mathbf{s}\mathbf{A}\mathbf{W} + \overline{\mathbf{x}}}_{\mathbf{c}_{+,1}}, \underbrace{\sum_{i \in [L_q]} (\mathbf{s}\mathbf{T}_{q^*,i} + \mathbf{s}\mathbf{A}\mathbf{W}_{q^*,i}(\widetilde{\mathbf{M}}_{q^*,i}\overline{\mathbf{f}}^\top_{q^*,i} \otimes \mathbf{I}_{k+1}))}_{\mathbf{c}_{q^*}}\right]_1\right) \\
\mathsf{hsk}_{q^*,i^*} &= \left(\left[\underbrace{\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}}_{\mathbf{k}_0^\top}, \underbrace{\sum_{i \in [L_{q^*}] \setminus \{i^*\}} (\mathbf{h}_{q^*,i,i^*} + \mathbf{W}_{q^*,i}(\widetilde{\mathbf{M}}_{q^*,i}\overline{\mathbf{f}}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}))}_{\mathbf{k}_1^\top},\right.\right. \\
&\qquad \left.\left.\underbrace{\mathbf{W}_{q^*,i^*}(\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{W}\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*}}_{\mathbf{k}_2^\top}, , \underbrace{\widetilde{\mathbf{M}}_{q,i^*}\overline{\mathbf{f}}^\top_{q,i^*}}_{\mathbf{k}_3^\top}\right]_2\right).
\end{aligned}$$

where

$$\mathbf{A}\mathbf{h}_{q^*,i,i^*} = \mathbf{T}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} \quad \forall i \in [L_{q^*}] \setminus \{i^*\} \quad \text{and} \quad \mathbf{A}\mathbf{U}_{q^*,i^*} = \mathbf{T}_{q^*,i^*}.$$

Note that here we actually consider $\mathsf{hsk}_{q^*,j}$ for $j = i^*$ and $\mathsf{sk}_{q^*,i}$ for $i = i^*$ and all above equalities are ensured by Ver and Gen. We have

$$\begin{aligned}
z_1 &= \sum_{i \in [L_{q^*}]} (\mathbf{s}\mathbf{T}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} + \mathbf{s}\mathbf{A}\mathbf{W}_{q^*,i}(\widetilde{\mathbf{M}}_{q^*,i}\overline{\mathbf{f}}^\top_{q^*,i} \otimes \mathbf{I}_{k+1})\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) \\
&= \sum_{i \in [L_{q^*}]} (\mathbf{s}\mathbf{T}_{q^*,i}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} + \mathbf{s}\mathbf{A}\mathbf{W}_{q^*,i}(\widetilde{\mathbf{M}}_{q^*,i}\overline{\mathbf{f}}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*})) \\
z_2 &= \sum_{i \in [L_{q^*}] \setminus \{i^*\}} (\mathbf{s}\mathbf{A}\mathbf{h}_{q^*,i,i^*} + \mathbf{s}\mathbf{A}\mathbf{W}_{q^*,i}(\widetilde{\mathbf{M}}_{q^*,i}\overline{\mathbf{f}}^\top_{q^*,i} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*})) \\
z_3 &= \mathbf{s}\mathbf{A}\mathbf{U}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} \\
z_4 &= \mathbf{s}\mathbf{A}\mathbf{W}_{q^*,i^*}(\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{s}\mathbf{A}\mathbf{W}\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*} \\
z_5 &= \mathbf{s}\mathbf{A}\mathbf{W}\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*} + \overline{\mathbf{x}}\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*}
\end{aligned}$$

and then

$$
\begin{aligned}
z &= z_1 - z_2 - z_3 - z_4 + z_5 \\
&= \mathbf{s}\mathbf{T}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} + \mathbf{s}\mathbf{A}\mathbf{W}_{q^*,i^*}(\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) - \mathbf{s}\mathbf{A}\mathbf{U}_{q^*,i^*}\mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*} \\
&\quad -(\mathbf{s}\mathbf{A}\mathbf{W}_{q^*,i^*}(\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*} \otimes \mathbf{B}_{q^*}\mathbf{r}^\top_{q^*,i^*}) + \mathbf{s}\mathbf{A}\mathbf{W}\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*}) \\
&\quad +(\mathbf{s}\mathbf{A}\mathbf{W}\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*} + \overline{\mathbf{x}}\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*}) \\
&= \overline{\mathbf{x}}\widetilde{\mathbf{M}}_{q^*,i^*}\overline{\mathbf{f}}^\top_{q^*,i^*} \\
&= (\mathbf{x}\|\mathbf{0}_n)\begin{pmatrix} \widetilde{\mathbf{M}} & \mathbf{0}^\top_{n_1} \\ \mathbf{0}_{n\times n_2} & \mathsf{ict}^\top_{q^*,i^*} \end{pmatrix}\begin{pmatrix} \mathbf{f}^\top_{q^*,i^*} \\ 1 \end{pmatrix} \\
&= \mathbf{x}\widetilde{\mathbf{M}}\mathbf{f}^\top_{q^*,i^*}
\end{aligned}
$$

Here, equalities hold analogous to the analysis of correctness in Section 6.1, and the last equality holds even if we replace $[\mathbf{M}_{q^*,i^*}]_s$ with

$$
[\widetilde{\mathbf{M}}_{q^*,i^*}]_s = \begin{bmatrix} \mathbf{M} & \mathbf{0}^\top_{n_1} \\ \mathbf{0}_{n\times n_2} & \mathsf{ict}^\top_{q^*,i^*} \end{bmatrix}_s \quad \text{where} \quad [\mathsf{ict}_{q^*,i^*}]_s \in \begin{cases} \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, 0) & \text{if } i \in [L_{q^*}] \setminus (\mathcal{M}^*_{q^*} \cup \mathcal{C}^*_{q^*}) \\ \mathsf{Enc}_1([\mathsf{ipk}]_1, [\mathsf{ipk}]_2, \mu_{q^*,i^*}) & \text{if } i \in \mathcal{M}^*_{q^*} \cup \mathcal{C}^*_{q^*} \end{cases}
$$

D.2 Sanity Check of the simulator in Section 7.2

In this section, we show that the simulator of our multi-instance slotted Reg-QFE can pass the sanity check. The simulated $\widetilde{\mathsf{crs}}$ has the full capacity as the crs of the scheme in Section 7.1. For all $\lambda, m, n_1, n_2 \in \mathbb{N}$, all $L_1, \ldots, L_m \in \mathbb{N}$, all $\{\mathcal{M}^*_q, \mathcal{C}^*_q\}_{q\in[m]}$, all $\mathbf{f}'_{q,i} \in \mathbb{Z}_p^{1\times n_1 n_2}$, $\mu_{q,i} \in \mathbb{Z}_p$, all $q^* \in [m]$ and $i^* \in [L_{q^*}]$; all

$$
\widetilde{\mathsf{crs}} \leftarrow \widetilde{\mathsf{Setup}}(1^\lambda, 1^m, 1^{L_1}, \ldots, 1^{L_m}, 1^{n_1}, 1^{n_2}, \{\{\mathbf{f}'_{q,i}\}_{i\in[L_q]}, \{\mu_{q,i}\}_{\mathcal{M}^*_q\cup\mathcal{C}^*_q}\}_{q\in[m]}),
$$

all $(\mathsf{pk}_{q^*,i^*}, \mathsf{sk}_{q^*,i^*}) \leftarrow \mathsf{Gen}(\widetilde{\mathsf{crs}}, q^*, i^*)$; all $\{\mathsf{pk}_{q^*,i}\}_{i\in[L_{q^*}]\setminus\{i^*\}}$ such that $\mathsf{Ver}(\widetilde{\mathsf{crs}}, q^*, i, \mathsf{pk}_{q^*,i}) = 1$; all $\mathbf{x}_1 \in \mathbb{Z}_p^{1\times n_1}, \mathbf{x}_2 \in \mathbb{Z}_p^{1\times n_2}$ and $\mathbf{f}_{q^*,i} \in \mathbb{Z}_p^{1\times n_1 n_2}$; we have:

$$
\Pr\left[\mathsf{Dec}(\mathsf{sk}_{q^*,i^*}, \mathsf{hsk}_{q^*,i^*}, (\mathsf{ct}_+, \mathsf{ct}_{q^*})) = (\mathbf{x}_1 \otimes \mathbf{x}_2)\mathbf{f}^\top_{q^*,i^*} \middle| \begin{array}{l} \mathsf{mpk}_+ \leftarrow \mathsf{Agg}_+(\widetilde{\mathsf{crs}}); \\ (\mathsf{mpk}_{q^*}, (\mathsf{hsk}_{q^*,j})_{j\in[L_{q^*}]}) \leftarrow \mathsf{Agg}(\widetilde{\mathsf{crs}}, q^*, (\mathsf{pk}_{q^*,i}, \mathbf{f}_{q^*,i})_{i\in[L_{q^*}]}) \\ s \leftarrow \mathsf{Coin};\ \mathsf{ct}_+ \leftarrow \mathsf{Enc}_+(\mathsf{mpk}_+, (\mathbf{x}_1, \mathbf{x}_2); s);\ \mathsf{ct}_{q^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}_{q^*}; s) \end{array}\right] = 1.
$$

This follows from the analysis of correctness in Section 7.1 and the fact that the simulator of our multi-instance slotted PReg-IPFE $(\widetilde{\mathsf{iSetup}}, \widetilde{\mathsf{iGen}}, \widetilde{\mathsf{iEnc}}_+, \widetilde{\mathsf{iEnc}})$ can pass the sanity check as shown in Appendix D.1.

D.3 Sanity Check of the simulator in Section 5.3

In this Section, we show that when apply our multi-instance slotted Reg-QFE in Section 7.1 to the transformation in Section 5.2, the simulator of the compact Reg-QFE can pass the sanity check. The simulated $\widetilde{\mathsf{crs}}$ has the full capacity as the crs. For all $L \in \mathbb{N}$, all $f'_i \in F, \mu_i \in Z$ and all CK, HK, CH such that $CK, HK \subseteq [0, L'-1], CH \cup HK = [0, L'-1]$ for some $L' \leq L$. For all stateful adversary $\mathcal{A}$ making a polynomial number of oracle queries (defined as in Section 2.2) and all L, we have the following advantage function is negligible in λ:

$$
\Pr[b = 1 | \widetilde{\mathsf{crs}} \leftarrow \widetilde{\mathsf{Setup}}(1^\lambda, 1^L, F; \{f'_i\}_{i\in CK\cup HK}, \{\mu_i\}_{i\in CK\cup CH}); b = 0; \mathcal{A}^{\mathsf{ORegNT}(\cdot,\cdot),\mathsf{ORegT}(\cdot),\mathsf{OEnc}(\cdot,\cdot),\mathsf{ODec}(\cdot)}(\widetilde{\mathsf{crs}})]
$$

we recall that oracles work as follows with $\mathsf{aux} = \perp, \mathcal{E} = \emptyset, \mathcal{R} = \emptyset$ and $t = \perp$:

- $\mathsf{ORegNT}(\mathsf{pk}, f)$: run $(\mathsf{mpk}, \mathsf{aux}') \leftarrow \mathsf{Reg}(\widetilde{\mathsf{crs}}, \mathsf{aux}, \mathsf{pk}, f)$, update $\mathsf{aux} = \mathsf{aux}'$, append $(\mathsf{mpk}, \mathsf{aux})$ to $\mathcal{R}$ and return $(|\mathcal{R}|, \mathsf{mpk}, \mathsf{aux})$;
- $\mathsf{ORegT}(f^*)$: run $(\mathsf{pk}^*, \mathsf{sk}^*) \leftarrow \mathsf{Gen}(\widetilde{\mathsf{crs}}, \mathsf{aux})$, $(\mathsf{mpk}, \mathsf{aux}') \leftarrow \mathsf{Reg}(\widetilde{\mathsf{crs}}, \mathsf{aux}, \mathsf{pk}^*, f^*)$, update $\mathsf{aux} = \mathsf{aux}'$, compute $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\widetilde{\mathsf{crs}}, \mathsf{aux}, \mathsf{pk}^*)$, append $(\mathsf{mpk}, \mathsf{aux})$ to $\mathcal{R}$, return $(t = |\mathcal{R}|, \mathsf{mpk}, \mathsf{aux}, \mathsf{pk}^*, \mathsf{sk}^*, \mathsf{hsk}^*)$;
- $\mathsf{OEnc}(i, x)$: let $\mathcal{R}[i] = (\mathsf{mpk}, \star)$, run $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x)$, append (x, ct) to $\mathcal{E}$ and return $(|\mathcal{E}|, \mathsf{ct})$;
- $\mathsf{ODec}(j)$: let $\mathcal{E}[j] = (x_j, \mathsf{ct}_j)$, compute $z_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$; if $z_j = \texttt{getupd}$, run $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\widetilde{\mathsf{crs}}, \mathsf{aux}, \mathsf{pk}^*)$ and recompute $z_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$. Set $b = 1$ when $z_j \neq f^*(x_j)$.

with the following restrictions:

- there are at most $L - 1$ queries to ORegNT and there is exactly one query to ORegT; therefore, we will consider $f^*, \mathsf{pk}^*, \mathsf{sk}^*, \mathsf{hsk}^*$ to be global;
- for query (i, x) to OEnc, it holds that $i \geq t, \mathcal{R}[i] \neq \perp$;
- for query (j) to ODec, it holds that $\mathcal{E}[j] \neq \perp$.

This follows from the analysis of correctness in Section 5.2, and the fact that the simulator of our multi-instance slotted Reg-QFE $(\widetilde{\mathsf{mSetup}}, \widetilde{\mathsf{mGen}}, \widetilde{\mathsf{mEnc}}_+, \widetilde{\mathsf{mEnc}})$ can pass the sanity check as shown in Appendix D.2.