When KGC Meets Curator: New Paradigm of Registered ABE and FE*

Ziqi Zhu[1], Jun Zhao[1], Kai Zhang[2], Junqing Gong[1,3,✉], and Haifeng Qian[1,✉]

[1] East China Normal University
ziqizhu00@stu.ecnu.edu.cn
junzhao@szut.edu.cn
jqgong@sei.ecnu.edu.cn
hfqian@cs.ecnu.edu.cn
[2] Shanghai University of Electric Power
kzhang@shiep.edu.cn
[3] Shanghai Qi Zhi Institute

Abstract. Functional encryption (FE) which covers the notion of attribute-based encryption (ABE), is the cryptographic tool to realize fine-grained control on the accessibility of encrypted data. The traditional FE requires a central *trusted* authority to issue secret keys. It depends on the *full-trust model*, and is vulnerable to the security issue caused by key-escrow. While the registered FE (Reg-FE) achieves the *zero-trust model* and addresses the security issue by removing the use of central authority. It allows users to generate secret keys themselves and join the system by registering corresponding public keys to a curator.

This work introduces delegated Reg-FE, which is a primitive with a new registration paradigm. It allows the registration of certain authorities that can issue secret keys for their respective classical FE sub-systems, beyond the prior work of registering plain users. Delegated Reg-FE implements a hybrid trust model within a two-level hierarchy. By redefining key escrow as a *functional mechanism* rather than a security concern, this model employs a zero-trust upper level which removes key-escrow, while the subsystem of each authority is locally full-trust and retains key-escrow mechanism.

We construct four delegated Reg-FE schemes for functionalities that can be described as the 2×2 combinations of *linear function* and *policy check*. Namely, Delegated Reg-IPFE, Delegated Reg-ABE, Reg-IPFE with delegated ABE, and Reg-ABE with delegated IPFE. All concrete schemes support bounded registrations and delegations, and achieve standard *adaptive* security under MDDH assumption on prime-order bilinear group. Furthermore, these schemes only rely on *black-box* techniques. Technically, these schemes rely on dual-system techniques as prior registration-based works. And we devise a new "hierarchically invoked dual-system" technique on schemes which have sub-ABE delegation systems.

Furthermore, we present a generic construction of Delegated Reg-FE from the combination of Reg-FE and FE. The instantiations of this generic construction demonstrate the feasibility of delegated Reg-FE, supporting arbitrary functions as well as unbounded numbers of registrations and delegations. However, this approach requires non-black-box techniques and achieves weaker semi-adaptive security without malicious registration, where the semi-adaptive means the adversary claims the challenge after seeing common reference string but before making any query. Its security relies solely on the underlying assumptions of the Reg-FE and FE components.

* This work is partially supported by National Natural Science Foundation of China (62572189,62372175,62372285), Innovation Program of Shanghai Municipal Education Commission (2021-01-07-00-08-E00101), the “Digital Silk Road” Shanghai International Joint Lab of Trustworthy Intelligent Software (22510750100), Shanghai Pilot Program for Basic Research (TQ20240212), Fundamental Research Funds for the Central Universities (40500-20104-222609).

1 Introduction

The cryptographic primitives supporting fine-grained access control have a long line of work on attribute-based encryption (ABE) [Sha84,SW05,GPSW06] and functional encryption (FE) [BSW11,O'N10]. More concretely, in an FE scheme, an *trusted authority* generates a master public key mpk and a master secret key msk, where the ciphertext encrypts a message x is generated from mpk, the secret key issued by the authority is generated from msk and is associated with functions f. The user holding the secret key with f will only learn $f(x)$ from the ciphertext of x. In the case of ABE covered by FE, a secret key is associated with a predicate p, instead of functions f, and the ciphertext for message x is bound to an attribute a. The decryption will reveal x if and only if $p(a) = 1$. There has been a long line of work on ABE and FE, however, both of them suffer from the key-escrow problem: the system requires a trusted central authority holding msk to generate and issue secret keys, it will be vulnerable when the central authority is corrupted by an adversary.

To overcome the key-escrow problem and remove the use of trusted central party, the pioneering work [GHMR18] initiated the line of registered encryption in the setting of identity-based encryption (IBE) [Sha84], and lead to the notion of registered IBE (RBE). Following this line, [HLWW23] generalized the notion to registered attribute-based encryption (Reg-ABE) and [FFM+23,DPY24] further extended it to registered functional encryption (Reg-FE). In Reg-FE, the central authority is replaced by a *curator*, who holds a common reference string crs without any secret. It allow a user to generate his/her own key pair $(\mathsf{pk}, \mathsf{sk})$ and register pk along with a function f into the system. The registration procedure is executed by the curator in a deterministic and public method and will update a mpk for encryption. And the user can recover $f(x)$ from the ciphertext of x, using his/her own sk along with a helper key hsk updated by the curator in registration process. In addition, it requires that the size of mpk, hsk and the costs of the update procedure are bounded by polylogarithmic in the number of registered users in the system. Such as standard ABE, Reg-ABE and RBE are the special cases of Reg-FE for the functionalities derived by predicates. In the historical line of work, [GHMR18,GHM+19,GV20,CES21,DKL+23,GKMR23,FKdP23,DMQ25] proposed several constructions of RBE and [HLWW23,FWW23,ZZGQ23,FFM+23,GLWW24,AT24,CHW25,ZZC+25] realized a series of constructions of Reg-ABE for complex policies. The study of concrete Reg-FE [ZLZ+24,DPY24,BLM+24] showed how to achieve some concrete functions (e.g. linear/quadratic functions, linear functions with access control) in the bilinear pairing groups, and [FFM+23,DPY24,ZCHZ24] proposed some constructions for general functions based on indistinguishable obfuscation (iO) [BGI+12,GGH+13,JLS22] or garbling scheme [Yao82,BHR12].

Motivation: Trust Model v.s. Key-escrow. Theoretically, we could consider key-escrow as a mechanism of supervisory, rather than a security issue. The traditional FE employs *full-trust model* with an authority who has *full key-escrow mechanism* to supervise all users. While the Reg-FE employs *zero-trust model* with a curator who has *no key-escrow mechanism* and registers users in a public way. Namely, in both standard FE and Reg-FE, we only have an "all-or-nothing" type of control on trust-level and key-escrow. This motivates the question:

Can we find an interpolation between FE and Reg-FE, that realizes the fine-grained control on trust-level requirement and key-escrow mechanism?

In some practical application scenarios, the fine-grained type of control on trust level and key-escrow is desirable. For example, in some stream media platforms that support family subscriptions and age rating (such as Netflix and Disney+), we consider content-supply and subscription services consisting the public domain, and the family of each subscriber as a private domain. In particular, content-supply plays the role of encryptor[1] that offer data encrypted with some policies (e.g. subscribers set and age rating), and

[1] Note that we don't consider the attack on content supply in this scenario.

– *within the public domain:* the key-escrow is undesirable, the subscription service is preferred being trustless and keeping no secret of subscribers;
– *within the private domain:* the key-escrow is necessary in some sense, the parents desire to have capacity of issuing keys to children, that with some attributes (e.g. age).

Notice that neither standard FE or Reg-FE can achieve the above scenario. Obviously, the regular FE with trusted central authority cannot keep no key-escrow and zero-trust model within the public domain. While using a Reg-FE cannot realize the key-escrow in the family's private domain. Moreover, simply registering separate keys for children will make some sensitive attributes (e.g. children's age) be transparent to those entities in the public domain the public domain, such as content-supply and other registered users, this is undesirable for most parents. To achieve the goal in this practical scenario, we need to explore a new line between FE and Reg-FE, that combine the trustless feature of curator and the key-escrow feature of authority.

1.1 Results

A New Registration Paradigm. In this work, we initiate the study of the *interpolation* between FE and Reg-FE by introducing a new registration paradigm. The new paradigm allows the registration of authorities that can issue secret keys and delegate decryption. This paradigm inspires a primitive called *delegated Reg-FE* that combine the features of curator and authority. In a Reg-FE system, the registration object is initially a plain user with only decryption capacity. We replace this user with an authority that maintains an FE sub-system. The registered authority is locally trusted with the capacity to issue secret keys and supervise the users within its sub-system (refers to the private domain). The registration-based superstructure ensures that, within the up-system (refers to the public domain), the Reg-FE's curator does not maintain any secrets of registered authorities, thereby employing the zero-trust model. Moreover, a compromised registered authority will only corrupt its own private domain, but will not affect other authorities and their sub-systems. This new primitive implements fine-grained control on trust model and key-escrow in the sense that: (1) the public domain is employed zero-trust environment, whereas private domains are locally employed trusted model; (2) key-escrow is forbidden in the public domain but possible in the private domain.

In more detail, a delegated Reg-FE for functionalities $G : X \to Y$ and $F : Y \to Z$ is established by a common reference string crs, and maintained by a curator as in Reg-FE. While the user in Reg-FE is replaced by a entity who plays the role as an authority of FE and can generate his/her own master key pair $(\mathsf{mpk}, \mathsf{msk})$. Similar to Reg-FE, this entity register (mpk, g) for some $g \in G$ into the system, the curator updates a *global* master public key mpk_+ for encryption and sends back a helper key hsk. In delegated Reg-FE, we allow this entity to issue secret key for some $f \in F$ with his/her msk and hsk. With this secret key, a user can decrypt the ciphertext for $x \in X$ and reveal the composite function value $f \circ g(x)$. The efficiency requirements are similar to Reg-ABE, we require the size of mpk_+, hsk and the costs of updating algorithms are all polylogarithmic in the number of registered authorities.

Conceptually, delegated Reg-FE interpolates between standard FE and Reg-FE and covers their notions. In particular, a delegated Reg-FE will collapse to regular FE when there exists only one registered authority and G is the identity functionality; and a delegated Reg-FE will collapse to Reg-FE when each registered authority maintains a one-key FE sub-system and F is the identity functionality. Furthermore, just as standard/registered FE encompass standard/registered ABE, the delegated Reg-FE can derive notions of *delegated Reg-ABE*, *Reg-FE with delegated ABE*, and *Reg-ABE with delegated FE*. By specifying the functionality as access control functions of the up-system or sub-system.

Similar to the slotted version of registration encryption [HLWW23], we can also define a weaker slotted version of our new primitive. In a slotted delegated Reg-FE for L registered authorities, the up-system is a slotted Reg-FE

instead of the Reg-FE, where each authority is associated with a slot index $i \in [L]$, and the curator is replaced with an public and deterministic aggregator. The aggregator can collect (mpk, g) for all L slots and generate mpk_+ and hsk once for all.

Constructions. Our constructive results are two-fold:

- First, we focus on *concrete* delegated Reg-FE, and propose four pairing-based schemes that support different concrete functionalities via *black-box* technique.
  (1) We build the first delegated Reg-FE for dual access control functionalities. Specifically, it's the first delegated Reg-ABE scheme for predicates $P : X \times Y \to \{0,1\}$ and $P' : X' \times Y' \to \{0,1\}$ via predicate encoding [Wee14,CGW15]: each authority is allowed to register mpk with a $y \in Y$ and allowed to issue secret keys for some $y' \in Y$; decryption of a ciphertext of (x, x') will pass if and only if $P(x, y) = 1 \wedge P'(x', y') = 1$. The scheme is a generic framework that supports a large class of predicates such as span program (ASP) and arithmetic branching program (ABP).
  (2) We build the first delegated Reg-FE scheme for linear functionalities $G = \{\mathbf{M} : \mathbf{x} \to \mathbf{xM}\}$ and $F = \{\mathbf{f} : \mathbf{y} \to \mathbf{yf}^\top\}$: each authority is allowed to register mpk with a function represented by a matrix $\mathbf{M}$ and allowed to issue secret keys for some functions represented by some vectors $\mathbf{f}$; decrypting a ciphertext of $\mathbf{x}$ recovers composite function value $\mathbf{xMf}^\top$.
  (3) We build the first delegated Reg-FE for access control and linear functionalities. Specifically, it's the first Reg-ABE with delegated FE for predicate $P : X \times Y \to \{0,1\}$ and linear functionality via predicate encoding [Wee14,CGW15]: each authority is allowed to register mpk with a $y \in Y$ and allowed to issue secret keys for some functions represented by some vector $\mathbf{y}$; decrypting a ciphertext for $(x, \mathbf{x})$ recovers $\mathbf{xy}^\top$ if and only if $P(x, y) = 1$. The scheme is a generic framework that supports a large class of predicates such as ASP and ABP.
  (4) We build the first delegated Reg-FE for linear and access control functionalities. Specifically, it's the first Reg-FE with delegated ABE for linear functionality and predicate $P : X \times Y \to \{0,1\}$ via predicate encoding [Wee14,CGW15]: each authority is allowed to register a function represented by a vector $\mathbf{y}$ and allowed to issue secret keys for some $y \in Y$; decrypting a ciphertext for $(\mathbf{x}, x)$ recovers $\mathbf{xy}^\top$ if and only if $P(x, y) = 1$. The scheme is a generic framework that supports a large class of predicates such as ASP and ABP.

  Considering *indistinguishability-based* (IND) security model adapted from that in Reg-FE (or FE), which ensures that any adversary cannot distinguish challenge ciphertexts even given some secret keys of users and master secret keys of registered authorities. All of these concrete schemes achieve *adaptive* IND-security under *standard* assumptions (e.g. MDDH assumption), and work over the prime-order bilinear group. As the previous pairing-based Reg-ABE/Reg-IPFE schemes [HLWW23,FFM+23,ZZGQ23,ZLZ+24] and pairing-based ABE/IPFE [CGW15,ABDP15], all of them support *bounded* number of authority registrations, *bounded* number of user delegations, have *structural* crs and need a specific verification procedure of master public key during registration.
- Second, we consider the feasibility of constructing delegated Reg-FE that supports *general* functions and *unbounded* numbers of registrations and delegations.
  (5) We build the first delegated Reg-FE scheme for arbitrary class of functions $G : X \to Y$ and $F : Y \to Z$, it's constructed from general Reg-FE and FE via non-black-box technique. When instantiated with unbounded Reg-FE and FE, this scheme serves as a feasibility result for delegated Reg-FE supporting general functions, enabling *unbounded* registrations and delegations.

  This generic scheme achieves *semi-adaptive* IND-security without malicious registration. Here, "semi-adaptive" means the adversary claims the challenge message after receiving crs before making any query. The generic construction relies solely on the assumptions underlying its base Reg-FE and FE, without requiring additional

Scheme	Function	Assumption	Security	Black-Box	Malicious	Unbounded
result **(1)**, § 5.1	Predicate ↑ Predicate ↓	MDDH	AD	✓	✓	Registration ✗ Delegation ✗
result **(2)**, § 6.1	Linear ↑ Linear ↓	MDDH	AD	✓	✓	Registration ✗ Delegation ✗
result **(3)**, § 7.1	Predicate ↑ Linear ↓	MDDH	AD	✓	✓	Registration ✗ Delegation ✗
result **(4)**, § 8.1	Linear ↑ Predicate ↓	MDDH	AD	✓	✓	Registration ✗ Delegation ✗
result **(5)**, § 9.1	General ↑ General ↓	iO + SSB	semi-AD	✗	✗	Registration ✓ Delegation ✓

Fig. 1: Summary of constructive results. Here, in the column **Scheme**, we use a instantiation of result **(5)** with the Reg-FE in [FFM+23,DPY24] and the FE in [GGH+13,Wat15]. In the column, **Function**, we use the symbols ↑ and ↓ to indicate the functionalities of the up- and sub-system, respectively. In the column **Security**, "AD", "semi-AD" stand for "adaptive" and "semi-adaptive" IND-security. The column **Black-Box** indicates the usage of the black-box technique, and the column **Malicious** indicates the permission of malicious registration. In the column **Unbounded**, "Registration", "Delegation" stand for "unbounded authority registrations" and "unbounded use delegations".

assumptions. However, a limitation is that the generic construction heavily relies on the general Reg-FE, which only appeared in [FFM+23,DPY24][2] and relies on iO. Instantiating the construction with the Reg-FE in [FFM+23,DPY24] and the FE in [GGH+13,Wat15] yields a general delegated Reg-FE scheme, that is based on iO [BGI+12,GGH+13,JLS22] and somewhere statistically binding hash functions (SSB) [HW15]. And this instantiation supports *unbounded* number of authority registrations and *unbounded* number of user-delegations.

We summarize our constructive results in Figure 1 for more details.

Conceptual Benefits. The primitive from the new registration paradigm can be seen as the combination of a Reg-FE up-system and some FE sub-systems, and it has the following benefits:

- **Batch User Registration:** In a delegated Reg-FE, the registered object is an authority that can maintain a many-key FE sub-system. In some sense, it is a Reg-FE that allows batch user registration. Concretely, when we let F be the identity functionality, the registration for authority can be seen as the batch registration for all potential users in its FE's private domain, and all these users register the same function $g \in G$ as their authority. Moreover, in the slotted version, the batch user registration feature can be seen as "one-slot for many-user", meaning that it enables filling many users with the same y into a single slot.
- **Partial Registration:** In a delegated Reg-FE supports the composite functionalities, where a user's function consists of its authority's part $g \in G$ and the own part $f \in F$. In some sense, it realizes a Reg-FE for composite functionality that allows partial function registration. Namely, when each authority holds a one-key FE sub-system, we can treat that user with authority to be the same entity with functions (g, f). Each "authority-user" entity will only partially register the function g instead of the whole (g, f). In addition, the entity only reveals the partial function g to the public domain, but keeps the function f in its private domain.

[2] Here, we don't mention the general Reg-FE in [BLM+24,ZCHZ24] for the brevity of discussion, since they are bounded collusion-resistant, which is not considered in our work.

– **Trade-off between Robustness and Efficiency:** In the study of registration-based systems, we concern space efficiency (crs/ct/hsk size) and time efficiency (update cost) in terms of the number L of users. In contrast of direct registration in Reg-FE, users in delegated Reg-FE "register" into the system through some prior registered authorities who can independently manage multiple users. Therefore, delegated Reg-FE can be more efficient (in both space and time) than Reg-FE at the cost of a higher risk of key leakage (since the authority could lose its msk). For example, in a Reg-FE that mostly supports L users, the update costs are polylogarithmic in L. Its system is zero-trust, ensuring that the curator cannot be compromised, and each corruption only affects one user. In contrast, we consider a delegated Reg-FE that mostly supports $\sqrt{L}$ registered authorities, and each authority manages $\sqrt{L}$ users. This yields a system totally accommodates $L = \sqrt{L} \times \sqrt{L}$ users. Such delegated Reg-FE decrease the security robustness, where each corruption (on authority) affects $\sqrt{L}$ users; however, it achieves advantage in the update efficiency, where the updation costs are polylogarithmic in $\sqrt{L}$.

1.2 Discussions

Related Works. We mention some previous works that our registration paradigm is related to. [GS02,HL02] introduced the notion of *hierarchical identity-based encryption* (HIBE). In a HIBE scheme, the system is structured as a hierarchy tree, enabling users to delegate secret keys to users in children nodes. In addition, some existing works [SW08,OT09,LOS+10,GVW13,BGG+14] also considered the delegation mechanism for the predicate encryption and attribute-based encryption, and extended the notions to *hierarchical predicate encryption* (HPE) and delegatable ABE. Further, [ABG+13] introduced the notion of *hierarchical functional encryption* (HFE) and [BS15] presented a generic transformation from general-purpose FE to HFE. All of these primitives share some kinds of hierarchical structures and implement delegation capabilities. Despite differing motivations, our delegated Reg-FE framework exhibits a similar hierarchical structure of the type "curator-authority-user". Our new notion can be interpreted as introducing hierarchy and delegation into the registration paradigm; or alternatively, as replacing the top tier of a (three-tier) hierarchy with a curator.

Concurrent Works. We note that [DKL+23] mentioned the possibility of hybrid IBE/RBE but offered neither a formal definition or construction. As their description, hybrid IBE/RBE enables the users in RBE to delegate decryption of some identities, which is analogous to our notion of delegated Reg-FE (for specific identity-based predicates). Recently, [LWW25] also proposed a new paradigm of registration by considering multiple key curators instead of a unique one. They introduced the notion of multi-authority Reg-ABE (MA-Reg-ABE), which combines the features of registration and multi-authority settings. In a MA-Reg-ABE model, there exists more than one key curator. Each curator manages their sets of attributes, and users can register into any curators. Similar to multi-authority ABE, one can specify a policy over attributes from different curators during encryption of MA-Reg-ABE.

Open problems. Beyond some natural open problems about constructing delegated Reg-FE for different functionalities, under different assumptions (e.g. LWE) and enhancing the security of general delegated Reg-FE, there are also various interesting problems on the new line, which explore fine-grained control on trust level and key-escrow mechanism. We have some discussions as below.

– Can we instantiate the public domain (trustless) and private domain (locally trusted) using other cryptographic primitives? For example, it's interesting to find a combined primitive that localizes the encryption within the private domains, which may be naturally extended to multi-input/multi-client setting. Notice that the "local encryption" idea seems far from the sense of registration, which requires encryption under a publicly aggregated mpk. And it may be realized by the interpretation between FE and some other decentralized primitives.

– Can we consider some extensions of our model? We consider the extensions in some senses as follows. (1) In the current model, all registered entities are the authorities of the FE sub-systems for the same functionality. We can consider the mixed registration, which allows registered entities to play different roles. For instance, we could allow some registered entities to be plain users and others to be authorities with FE subsystems for different functionalities. (2) We can consider the extended model that supports both "global encryption" and "local encryption" (mentioned above). Roughly, the "global encryption" is under the global mpk_+, while "local encryption" is under a registered authority's mpk. And the security should ensure the "local ciphertexts" within one sub-system cannot be decrypted by the authorities and users in different sub-systems. We believe that formalizing these extended models would yield interesting results.
– Our new model achieves the fine-grained control of trust model and key-escrow, in the sense of public/private domain. Is it possible to realize that goal in other senses? For example, can we consider a fine-grained control in the sense of time, where the whole system may be fully trusted with key-escrow capacity before a given time point, and be trustless without any key-escrow after this time point.

Organization. This paper is organized as follows: In Section 2, we provide the technical overviews of delegated Reg-ABE and generic construction in slotted version, and present the informal constructions of other concrete works. We review some background knowledge in Section 3. And present the formal definition of delegated Reg-FE in both full-fledged and slotted versions in Section 4. In Section 5, 6, 7 and 8, we respectively propose the concrete constructions of slotted delegated Reg-ABE, slotted delegated Reg-IPFE, slotted Reg-ABE with delegated IPFE, and slotted delegated Reg-IPFE with delegated ABE. Except slotted delegated Reg-IPFE, other three construction are generic frameworks for all predicates with predicate encodings. And in Section 9, we give the generic construction of delegated Reg-FE. In Section 10, we present the generic transformation from slotted delegated Reg-FE to full-fledged delegated Reg-FE.

2 Technical Overview

Acknowledgement. We want to thank the anonymous reviewer#B from Crypto 2025 for his/her insightful comment and inspiring recommendation, which significantly contributed to our generic construction.

Strategy. We follow a similar blueprint as that in Reg-ABE by [HLWW23]. We first define and focus on a weaker primitive named slotted delegated Reg-FE. A slotted delegated Reg-FE for L slots replaces the curator in delegated Reg-FE with an *aggregator*, the aggregator collects all $(\mathsf{mpk}_1, g_1), \ldots, (\mathsf{mpk}_L, g_L)$ at once, generates mpk_+ and hsk's for all slots. In a slotted delegated Reg-FE, we don't need to concern with updating operations. And we propose a generic transformation adapted from the "power-of-two" method in [HLWW23], to transform any slotted delegated Reg-FE to a delegated Reg-FE. And in our technical overview, we first neglect the case where mpk_i is malicious, and explain how to deal with malicious mpk later.

This work mainly focuses on four concrete delegated Reg-FE schemes, with a generic scheme included to demonstrate feasibility in our setting. Due to space limitations, in this section, we (1) explain how to construct the one for access control functionalities, namely delegated Reg-ABE, as it is the most technologically representative one of concrete schemes; (2) present a brief explanation of generic construction. Additionally, we directly provide the informal version of remaining concrete constructions. We summarize our roadmap of delegated Reg-ABE as follows:

Recap: ZZGQ sReg-ABE [ZZGQ23] and Dual-system ABE. Let lower-case boldface denote *row* vectors and upper-case boldface denote matrices. We review the definition of predicate encoding and dual-system ABE [Wee14,CGW15]

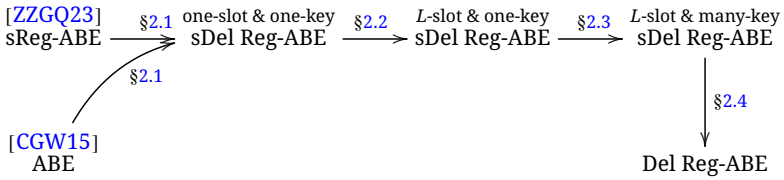

Fig. 2: Roadmap of the delegated Reg-ABE. Here "sReg-ABE" stands for "slotted Reg-ABE", "sDel Reg-ABE" and "Del Reg-ABE" respectively stands for "delegated Reg-ABE" in slotted and full-fledged version.

[ABS17,ACGU20]. A predicate $P : X \times Y \to \{0,1\}$ has an (n, n_c, n_k)-predicate encoding (PE) if: For all $x \in X$, $y \in Y$, one can efficiently and deterministically find

$$\mathbf{C}_x \in \mathbb{Z}_p^{n \times n_c},\ \mathbf{K}_y \in \mathbb{Z}_p^{n \times n_k},\ \mathbf{a}_y \in \mathbb{Z}_p^{1 \times n_k},\ \mathbf{d}_{x,y} \in \mathbb{Z}_p^{n_c+n_k}$$

that forms $\mathbf{M}_{x,y} = \begin{pmatrix} \mathbf{a}_y & \mathbf{0}_{n_c} \\ \mathbf{K}_y & \mathbf{C}_x \end{pmatrix}$ such that

α-reconstruction: when $P(x,y) = 1$, we have $\mathbf{M}_{x,y}\mathbf{d}_{x,y}^\top = \mathbf{e}_1^\top$;
α-privacy: when $P(x,y) = 0$, we have $\{x, y, \alpha, (\alpha \| \mathbf{w})\mathbf{M}_{x,y}\} \approx_s \{x, y, \alpha, (0 \| \mathbf{w})\mathbf{M}_{x,y}\}$ where $\mathbf{w} \leftarrow \mathbb{Z}_p^n$.

α-reconstruction and α-privacy are used to ensure correctness and security of ABE, respectively. (For the reader who is familiar with the notations in [CGW15], $\mathbf{C}_x, \mathbf{K}_y, \mathbf{a}_y$ refer to sE, rE, kE, and $\mathbf{d}_{x,y}$ corresponds to sD, rD.) Let $\mathbb{G}$ be a finite cyclic group with generator g and denote $[x] = g^x$, one of the start point is the one-slot Reg-ABE in [ZZGQ23] for predicate P with predicate encoding $(\mathbf{C}_x, \mathbf{K}_y, \mathbf{a}_y, \mathbf{d}_{x,y})$:

$$\begin{aligned} \mathsf{crs} &= [\mathbf{w}, \alpha]; \\ \mathsf{pk}, \mathsf{sk} &= [\alpha'], \alpha'; \\ \mathsf{mpk}_{\mathsf{pk},y} &= [(\alpha + \alpha')\mathbf{a}_y + \mathbf{w}\mathbf{K}_y, \mathbf{w}, \alpha]; \\ \mathsf{ct}_x &= [s, s(\alpha + \alpha')\mathbf{a}_y + s\mathbf{w}\mathbf{K}_y, s\mathbf{w}\mathbf{C}_x], [s\alpha] \cdot \mathsf{m}. \end{aligned} \tag{1}$$

Decryption relies on the following equation:

$$(s \cdot ((\alpha + \alpha')\mathbf{a}_y + \mathbf{w}\mathbf{K}_y) \| s\mathbf{w}\mathbf{C}_x)\mathbf{d}_{x,y}^\top = (s(\alpha + \alpha') \| s\mathbf{w})\mathbf{M}_{x,y}\mathbf{d}_{x,y}^\top = (s(\alpha + \alpha') \| s\mathbf{w})\mathbf{e}_1^\top = s(\alpha + \alpha'). \tag{2}$$

where the second equation use the α-reconstruction of PE; and with $\mathsf{sk} = \alpha'$, the user can recover $s\alpha$. For security, it considers two cases:

- When $\mathsf{sk} = \alpha'$ is leaked, we require $P(x,y) = 0$. DDH assumption implies $\mathsf{ct}_x \approx [s, (\tilde{\alpha} + s\alpha')\mathbf{a}_y + \tilde{\mathbf{w}}\mathbf{K}_y, \tilde{\mathbf{w}}\mathbf{C}_x], [\tilde{\alpha}] \cdot \mathsf{m}$. And with the α-privacy of predicate encoding, the α is hidden by $(\tilde{\alpha}\mathbf{a}_y + \tilde{\mathbf{w}}\mathbf{K}_y, \tilde{\mathbf{w}}\mathbf{C}_x) \approx (0 \cdot \mathbf{a}_y + \tilde{\mathbf{w}}\mathbf{K}_y, \tilde{\mathbf{w}}\mathbf{C}_x)$.
- When $\mathsf{sk} = \alpha'$ is secret, the security follows from the fact that $[s\alpha']$ can hide $[s\alpha]$ with the analogous reason in ElGamal encryption.

Another start point is the one-key plain ABE in [CGW15] for predicate P' with predicate encoding $(\mathbf{C}'_{x'}, \mathbf{K}'_{y'}, \mathbf{a}'_{y'}, \mathbf{d}'_{x'y'})$:

$$\begin{aligned} \mathsf{mpk}, \mathsf{msk} &= ([\mathbf{w}', \alpha']), (\mathbf{w}', \alpha'); \\ \mathsf{ct}_{x'} &= [s, s\mathbf{w}'\mathbf{C}'_{x'}], [s\alpha'] \cdot \mathsf{m}; \\ \mathsf{sk}_{y'} &= \alpha'\mathbf{a}'_{y'} + \mathbf{w}'\mathbf{K}'_{y'}. \end{aligned} \tag{3}$$

Decryption relies on the following equation:

$$(s \cdot (\alpha'\mathbf{a}'_{y'} + \mathbf{w}'\mathbf{K}'_{y'}) \| s\mathbf{w}'\mathbf{C}'_{x'})\mathbf{d}'^\top_{x',y'} = (s\alpha' \| s\mathbf{w}')\mathbf{M}'_{x',y'}\mathbf{d}'^\top_{x',y'} = (s\alpha' \| s\mathbf{w}')\mathbf{e}_1^\top = s\alpha'. \tag{4}$$

where the second equation uses the α-reconstruction of PE; security follows from the α-privacy of PE. The actual proof needs a composite-order group with subgroup decision assumption.

2.1 One-slot & One-key Scheme

We consider conjunction of predicates P and P', where P and P' respectively have predicate encodings $(\mathbf{C}_x, \mathbf{K}_y, \mathbf{a}_y, \mathbf{d}_{x,y})$ and $(\mathbf{C}'_{x'}, \mathbf{K}'_{y'}, \mathbf{a}'_{y'}, \mathbf{d}'_{x',y'})$. We employ the [CGW15] one-key ABE and [ZZGQ23] one-slot Reg-ABE. With a brief explanation, we enable the authority in that slot to generate the [CGW15] ABE-type master key pair: $\mathsf{mpk} = ([\mathbf{w}', \alpha'])$, $\mathsf{msk} = (\mathbf{w}', \alpha')$. To register this authority, $[\alpha']$ in mpk will additionally play the role as original pk in [ZZGQ23] one-slot Reg-ABE, in order to series connect the sReg-ABE and [CGW15] one-key ABE sub-system. In more detail, the one-slot & one-key schemes works as follows:

$$\begin{aligned} \mathsf{crs} &= [\mathbf{w}, \alpha]; \\ \mathsf{mpk}, \mathsf{msk} &= ([\mathbf{w}', \alpha']), (\mathbf{w}', \alpha'); \\ \mathsf{mpk}_+ &= [(\alpha + \alpha')\mathbf{a}_y + \mathbf{w}\mathbf{K}_y, \mathbf{w}, \mathbf{w}', \alpha, \alpha']; \\ \mathsf{ct}_{x,x'} &= [s, s(\alpha + \alpha')\mathbf{a}_y + s\mathbf{w}\mathbf{K}_y, s\mathbf{w}\mathbf{C}_x, s\mathbf{w}'\mathbf{C}'_{x'}], [s\alpha] \cdot \mathsf{m}; \\ \mathsf{sk}_{y'} &= \alpha'\mathbf{a}'_{y'} + \mathbf{w}'\mathbf{K}'_{y'}. \end{aligned} \tag{5}$$

The user keeps $\mathsf{sk}_{y'}$ decrypt $\mathsf{ct}_{x,x'}$ as follows

(i) When $P(x, y) = 1$, with the equation (2) as in one-slot Reg-ABE, one can recover $[s\alpha + s\alpha']$.

(ii) When $P'(x', y') = 1$, with the equation (4) as in one-key ABE, one can recover $[s\alpha']$.

With $[s\alpha']$ and $[s\alpha + s\alpha']$, the user compute as follows to recover m:

$$\frac{[s\alpha'] \cdot \overbrace{[s\alpha] \cdot \mathsf{m}}^{\mathsf{ct}_{x,x'}}}{[s\alpha + s\alpha']} = \mathsf{m}$$

For security, we consider two cases:

- When $P(x, y) = 0$, the security can be reduced to the first case for [ZZGQ23] one-slot scheme, which also requires $P(x, y) = 0$.
- When $P(x, y) = 1$, we require $\mathsf{msk} = (\mathbf{w}', \alpha')$ is secret and $P'(x', y') = 0$. Analogous to the security of [CGW15], with the α-privacy of P', it ensures that α' will not be leaked by $\mathsf{sk}_{y'}$. It implies that the security can be reduced to the second case for [ZZGQ23] one-slot scheme.

2.2 To L-slot & One-key Scheme.

We follow the strategy in [ZZGQ23] to extend the scheme for L-slot, which is allowed to register $(\mathsf{mpk}_1, y_1), \ldots, (\mathsf{mpk}_L, y_L)$. We run L parallel instances (indexed by $i \in [L]$) of scheme (5), and "add" the corresponding mpk_+ and ciphertext. Additionally, we introduce bilinear groups into the scheme, 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 with generator g_T; and the order of all groups is prime p. We place the above parallel instances over $\mathbb{G}_1$ and use $\mathbb{G}_2$ to hold L helper key hsk_i for decryption, with new random coin r_i. For each parallel instance indexed by $i \in [L]$, writing $(\mathbf{w}, \alpha)$ in crs as $(\mathbf{w}_{0,i}, v_i)$, and writing $(\mathbf{w}', \alpha')$ in master key pairs as $(\mathbf{w}_{1,i}, u_i)$. Moreover, we use $\mathbb{G}_T$ to accommodate a new α in order to hide m, and connect this α with v_i for

all $i \in [L]$ in $\mathbb{G}_2$. In more detail, our L-slot & one-key scheme is as follows:

$$\begin{aligned}
\mathsf{crs} &= [\alpha]_T, [v_i, \mathbf{w}_{0,i}]_1, \quad \forall i \in [L];\\
&\quad\ [r_j, r_j v_i, r_j \mathbf{w}_{0,i}, r_j v_j + \alpha]_2, \quad \forall i, j \in [L] \text{ s.t. } i \neq j;\\
\mathsf{mpk}_i, \mathsf{msk}_i &= ([\mathbf{w}_{1,i}, u_i]_1, \{[r_j \mathbf{w}_{1,i}, r_j u_i]_2\}_{j\neq i}), (\mathbf{w}_{1,i}, u_i);\\
\mathsf{mpk}_+ &= [\textstyle\sum_i((v_i+u_i)\mathbf{a}_{y_i} + \mathbf{w}_{0,i}\mathbf{K}_{y_i}), \sum_i \mathbf{w}_{0,i}, \sum_i \mathbf{w}_{1,i}]_1, [\alpha]_T;\\
\mathsf{hsk}_i &= [r_i, r_i \textstyle\sum_{j\neq i}((v_j+u_j)\mathbf{a}_{y_j} + \mathbf{w}_{0,j}\mathbf{K}_{y_j}), r_i \sum_{j\neq i} \mathbf{w}_{0,j}, r_i \sum_{j\neq i} \mathbf{w}_{1,j}, r_i v_i + \alpha]_2;\\
\mathsf{ct}_{x,x'} &= [s, s\textstyle\sum_i(v_i+u_i)\mathbf{a}_{y_i} + s\mathbf{w}_{0,i}\mathbf{K}_{y_i}, s\sum_i \mathbf{w}_{0,i}\mathbf{C}_x, s\sum_i \mathbf{w}_{1,i}\mathbf{C}'_{x'}]_1, [s\alpha]_T \cdot \mathsf{m};\\
\mathsf{sk}_{i,y'} &= u_i \mathbf{a}'_{y'} + \mathbf{w}_{1,i}\mathbf{K}'_{y'}
\end{aligned} \tag{6}$$

For each $i \in [L]$, hsk_i helps to recover a ciphertext of the same message over $\mathbb{G}_T$ in the i-th *one-slot & one-key* instance, with random coin sr_i instead of s:

$$\begin{aligned}
&\overbrace{r_i}^{\mathsf{hsk}_i} \cdot \overbrace{s\sum_i (v_i+u_i)\mathbf{a}_{y_i} + s\mathbf{w}_{0,i}\mathbf{K}_{y_i}}^{\mathsf{ct}_{x,x'}} - \overbrace{s}^{\mathsf{ct}_{x,x'}} \cdot \overbrace{r_i \sum_{j\neq i}((v_j+u_j)\mathbf{a}_{y_j} + \mathbf{w}_{0,j}\mathbf{K}_{y_j})}^{\mathsf{hsk}_i} &&= sr_i(v_i+u_i)\mathbf{a}_{y_i} + sr_i\mathbf{w}_{0,i}\mathbf{K}_{y_i}\\
&r_i \cdot s\textstyle\sum_i \mathbf{w}_{0,i}\mathbf{C}_x - s \cdot r_i \sum_{j\neq i}\mathbf{w}_{0,j} && \mathbf{C}_x &= sr_i\mathbf{w}_{0,i}\mathbf{C}_x\\
&r_i \cdot s\textstyle\sum_i \mathbf{w}_{1,i}\mathbf{C}'_{x'} - s \cdot r_i \sum_{j\neq i}\mathbf{w}_{1,j} && \mathbf{C}'_{x'} &= sr_i\mathbf{w}_{1,i}\mathbf{C}'_{x'}
\end{aligned} \tag{7}$$

When $P(x, y_i) = 1 \wedge P'(x', y') = 1$, use the decryption operation in the scheme (5), user with $\mathsf{sk}_{i,y'}$ can recover $[sr_i \cdot (v_i+u_i)]_T$ and $[sr_i \cdot u_i]_T$. Then, one can compute as follows and recover m:

$$\frac{[sr_i \cdot (v_i+u_i)]_T \cdot \overbrace{[s\alpha]_T \cdot \mathsf{m}}^{\mathsf{ct}_{x,x'}}}{e(\underbrace{[s]_1}_{\mathsf{ct}_{x,x'}}, \underbrace{[r_i v_i + \alpha]_2}_{\mathsf{hsk}_i}) \cdot [sr_i \cdot u_i]_T} = \mathsf{m}. \tag{8}$$

For security, we need to embed the scheme into the composite-order group, and use the dual-system method to change $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ conceptually as in [ZZGQ23][3], but with the case-study for scheme (5) instead. We omit the detail here.

2.3 To L-slot & Many-key Scheme

To achieve many-key, a naive solution is to follow the approach in [CGW15]: for y', let the authority in i-th slot freshly sample $r \leftarrow \mathbb{Z}_p$ and generate secret key as follows

$$\mathsf{sk}_{i,y'} = [r, u_i \mathbf{a}'_{y'} + r\mathbf{w}_{1,i}\mathbf{K}'_{y'}]_2$$

However, using above secret key, along with $[s]_1$, $[r_i]_2$ and $[sr_i\mathbf{w}_{1,i}\mathbf{C}'_{x'}]_T$, that respectively obtained from $\mathsf{ct}_{x,x'}$, hsk_i and R.H.S of equalities (7), the user cannot reveal $[sr_i \cdot u_i]_T$ via predicate encoding of P' to proceed with the decryption stage (8). To solve this problem, we observe that when the authority in i-th slot generates a secret key, $[r_i]_2$ is fully determined in crs and is encoded over $\mathbb{G}_2$, while r, u_i and $\mathbf{w}_{1,i}$ are fully determined by the authority and known over $\mathbb{Z}_p$. This allows the authority to embed $[r_i]_2$ into the above secret key and the fresh r into the corresponding term of hsk'. Instead of an independent random coin r, we choose the fresh random coin as $r_i r$. This random coin is related to r_i, and serves to ensure that $\mathsf{sk}_{i,y'}$ is issued by i-th authority. In more details, with msk_i and hsk_i as in scheme (6), the i-authority generates the secret key for y' with a freshly sampled $r \leftarrow \mathbb{Z}_p$ as follow:

$$\mathsf{sk}_{i,y'} = [r_i u_i \mathbf{a}'_{y'} + r_i r\mathbf{w}_{1,i}\mathbf{K}'_{y'}]_2, [r_i r, r_i r \textstyle\sum_{j\neq i}\mathbf{w}_{1,j}]_2.$$

[3] Notice that the actual proof makes changes in crs instead of $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ since aggregation is public and deterministic.

For correctness, the third equality in (7) can be modified as follow:

$$\overbrace{\lceil r_i \bar{r} \rceil}^{\mathsf{sk}_{i,y'}} \cdot \overbrace{s \sum_i \mathbf{w}_{1,i} \mathbf{C}'_{x'}}^{\mathsf{ct}_{x,x'}} - \overbrace{s}^{\mathsf{ct}_{x,x'}} \cdot \overbrace{\lceil r_i \bar{r} \rceil \sum_{j \neq i} \mathbf{w}_{1,j}}^{\mathsf{sk}_{i,y'}} \mathbf{C}'_{x'} = s \lceil r_i \bar{r} \rceil \mathbf{w}_{1,i} \mathbf{C}'_{x'} \tag{9}$$

When $P'(x', y') = 1$, decryption can recover $[sr_i \cdot u_i]_T$ with $[r_i(u_i \mathbf{a}'_{y'} + r\mathbf{w}_{1,i}\mathbf{K}'_{y'})]_2$ and $[s]_1$ as equality (4), using random coin $sr_i r$ instead of s. And with equality (8), the user can continue the decryption to recover m. To prove the security, we first use the dual-system method to conceptually change $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ one-by-one as in the scheme (6). Moreover, during changing hsk_i, to prove that u_i is not leaked when dealing with the second case of the case study, it needs to hierarchically invoke dual-system method to change all queried $\mathsf{sk}_{i,y'}$.

To Prime-order Slotted Scheme. As for the random coin in sk, we extend the "composite-order-to-prime-order" transformation in [CGW15] to support the hierarchical invocation of dual-system method. We don't substitute $[r_j]_2 \mapsto [\mathbf{B}\mathbf{r}_j^\top]_2$ and $[\alpha]_2 \mapsto [\mathbf{k}^\top]_2$, $[\alpha]_T \mapsto [\mathbf{A}\mathbf{k}^\top]_T$ as [CGW15]. Instead, given $\mathbf{A} \in \mathbb{Z}_p^{k \times (k+1)}$ and $\mathbf{B} \in \mathbb{Z}_p^{(3k+1) \times k}$, we substitute $[r_j]_2$ and $[r_j r]_2$ with:

$$[\mathbf{B}\mathbf{R}_j]_2 \in \mathbb{G}_2^{(3k+1)\times k} \quad \text{and} \quad [\mathbf{B}\mathbf{R}_j\mathbf{R}]_2 \in \mathbb{G}_2^{(3k+1)\times k}$$

to match the matrices' size, substitute $[\alpha]_2$, $[\alpha]_T$ and $[s\alpha]_T$ with:

$$[\mathbf{K}]_2 \in \mathbb{G}_2^{(k+1)\times k}, [\mathbf{A}\mathbf{K}]_T \in \mathbb{G}_T^{k\times k} \quad \text{and} \quad [\mathbf{s}\mathbf{A}\mathbf{K}\mathbf{e}^\top]_T \in \mathbb{G}_T^k$$

In particular, we get the prime-order scheme as follows:

$$\begin{aligned}
\mathsf{crs} &= [\mathbf{A}\mathbf{K}]_T, [\mathbf{A}\mathbf{V}_i, \mathbf{A}\mathbf{W}_{0,i}]_1, \quad \forall i \in [L] \\
&\quad [\mathbf{B}\mathbf{R}_j, \mathbf{V}_j\mathbf{B}\mathbf{R}_j + \mathbf{K}, \mathbf{V}_i\mathbf{B}\mathbf{R}_j, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{R}_j)]_2, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\
\mathsf{mpk}_+ &= [\textstyle\sum_i ((\mathbf{A}\mathbf{V}_i + \mathbf{A}\mathbf{U}_i)(\mathbf{a}_{y_i} \otimes \mathbf{I}) + \mathbf{A}\mathbf{W}_{0,i}(\mathbf{K}_{y_i} \otimes \mathbf{I})), \sum_i \mathbf{A}\mathbf{W}_{0,i}, \sum_i \mathbf{A}\mathbf{W}_{1,i}]_1, [\mathbf{A}\mathbf{K}]_T, \\
\mathsf{hsk}_j &= [\mathbf{B}\mathbf{R}_j, \textstyle\sum_{i\neq j} \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{R}_j), \sum_{i\neq j} \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j), \mathbf{V}_j\mathbf{B}\mathbf{R}_j + \mathbf{K}]_2, \\
&\quad [\textstyle\sum_{i\neq j} (\mathbf{V}_i\mathbf{B}\mathbf{R}_j + \mathbf{U}_i\mathbf{B}\mathbf{R}_j)(\mathbf{a}_{y_i} \otimes \mathbf{I}) + \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{R}_j)(\mathbf{K}_{y_i} \otimes \mathbf{I})]_2 \\
\mathsf{ct}_{x,x'} &= [\mathbf{s}\mathbf{A}, \textstyle\sum_i ((\mathbf{s}\mathbf{A}\mathbf{V}_i + \mathbf{s}\mathbf{A}\mathbf{U}_i)(\mathbf{a}_{y_i} \otimes \mathbf{I}) + \mathbf{s}\mathbf{A}\mathbf{W}_{0,i}(\mathbf{K}_{y_i} \otimes \mathbf{I}))]_1, \\
&\quad [\textstyle\sum_i \mathbf{s}\mathbf{A}\mathbf{W}_{0,i}(\mathbf{C}_x \otimes \mathbf{I}), \sum_i \mathbf{s}\mathbf{A}\mathbf{W}_{1,i}(\mathbf{C}'_{x'} \otimes \mathbf{I})]_1, [\mathbf{s}\mathbf{A}\mathbf{K}\mathbf{e}^\top]_T \cdot \mathsf{m}, \\
\mathsf{sk}_{j,y'} &= [\mathbf{B}\mathbf{R}_j\mathbf{R}, \textstyle\sum_{i\neq j} \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j\mathbf{R})]_2 \\
&\quad [\mathbf{U}_j\mathbf{B}\mathbf{R}_j(\mathbf{a}'_{y'} \otimes \mathbf{I}) + \mathbf{W}_{1,j}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I})]_2.
\end{aligned} \tag{10}$$

where $\mathsf{msk}_i = (\mathbf{U}_i, \mathbf{W}_{1,i}) \in \mathbb{Z}_p^{(k+1)\times(3k+1)} \times \mathbb{Z}_p^{(k+1)\times(3k+1)n'}$ and $\mathsf{mpk}_i = ([\mathbf{A}\mathbf{U}_i, \mathbf{A}\mathbf{W}_{1,i}]_1, \{[\mathbf{U}_i\mathbf{B}\mathbf{R}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j)]_2\}_{j\neq i})$; and we let all matrices $\mathbf{I}$ have proper size.

Security Analysis in Prime-order Groups. Neither the dual-system or nested dual-system method used in Reg-ABE [HLWW23,ZZGQ23] and Reg-IPFE [ZLZ+24] is sufficient to prove above slotted delegated Reg-ABE. In previous proofs, they first replace ciphertext to semi-function ciphertext, and conceptually change $\mathsf{hsk}_1, \ldots, \mathsf{hsk}_L$ to semi-function one-by-one, where security is ensured by the fact that a semi-function hsk is unable to decrypt a semi-function ciphertext. During switching hsk_j, previous proof required arguments in the following two cases: (1) when j is a corrupted slot, it holds $P(x, y_j) = 0$ and the α-privacy of predicate encodings ensures the replacement; (2) when j is an honest slot, the justification for the substitution relies on the hiddenness of the private key. However, in our delegated Reg-ABE, even if the msk_j is hidden, the adversary can obtain some secret keys generated from msk_j. We need a new approach to justify the semi-function switching of hsk_j.

Gm	ct^*	hsk_j	$\mathsf{sk}_{j,y'}$	**Remark**
G_0	$[\mathbf{sA}]_1, [\mathbf{sAKe}^\top]_T \cdot \mathsf{m}_b^*$	$[\mathbf{BR}_j]_2, [\mathbf{V}_j\mathbf{BR}_j + \mathbf{K}]_2$	$[\mathbf{BR}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{BR}_j]_2$	Real Game
G_1	$[\mathbf{c}]_1, [\mathbf{cKe}^\top]_T \cdot \mathsf{m}_b^*$	$[\mathbf{BR}_j]_2, [\mathbf{V}_j\mathbf{BR}_j + \mathbf{K}]_2$	$[\mathbf{BR}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{BR}_j]_2$	MDDH
$\mathsf{G}_{2,j,1}$	$[\mathbf{c}]_1, [\mathbf{cKe}^\top]_T \cdot \mathsf{m}_b^*$	$[\mathbf{D}_j]_2, [\mathbf{V}_j\mathbf{D}_j + \mathbf{K}]_2$	$[\mathbf{D}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{D}_j]_2$	MDDH
$\mathsf{G}_{2,j,2}$	$[\mathbf{c}]_1, [\mathbf{cKe}^\top]_T \cdot \mathsf{m}_b^*$	$[\mathbf{D}_j]_2, [\mathbf{V}_j\mathbf{D}_j + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2$	$[\mathbf{D}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{D}_j]_2$	Case-study
$\mathsf{G}_{2,j,3}$	$[\mathbf{c}]_1, [\mathbf{cKe}^\top]_T \cdot \mathsf{m}_b^*$	$[\mathbf{BR}_j]_2, [\mathbf{V}_j\mathbf{BR}_j + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2$	$[\mathbf{BR}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{BR}_j]_2$	MDDH
G_3	$[\mathbf{c}]_1$, random	$[\mathbf{BR}_j]_2, [\mathbf{V}_j\mathbf{BR}_j + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2$	$[\mathbf{BR}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{BR}_j]_2$	Statistic

Fig. 3: Games for dual-system method with $b \in \{0,1\}$, and games $\{\mathsf{G}_{2,j,k}\}_{k=1,2,3}$ are one-by-one for all slot $j \in [L]$. Here $\widetilde{\mathbf{k}}$ is randomly chosen, $\mathbf{c}^\perp$ such that $\mathbf{cc}^\perp =$ and $\mathbf{Ac}^\perp = \mathbf{0}$.

Dual-system Method. Recall that $\mathsf{m}_0^*, \mathsf{m}_1^*$ are challenge messages. For any slot $j \in [L]$, let y_j be the challenge value with j and assume $\mathsf{msk}_j = \mathbf{U}_j, \mathbf{W}_{1,j}$ is honestly generated (but can be corrupted by the adversary later). And let $\mathsf{sk}_{j,y'}$ be the secret keys from slot j obtained by the adversary, where $\mathbf{R}$ is freshly chosen for each $\mathsf{sk}_{j,y'}$. At a high level, we will follow the dual-system method with $([\mathbf{A}]_1, [\mathbf{B}]_2)$ as the dual-system spaces, see Fig 3. We begin with a challenge ciphertext of m_b^* where b is the secret bit, (see G_0) and continue the process as follows:

- First in G_1, we change ct^* to semi-function. Namely, we replace all $[\mathbf{sA}]_1$ that appear in ct^* with $[\mathbf{c}]_1$; and replace $[\mathbf{sAKe}^\top]_T$ with $[\mathbf{cKe}^\top]_T$. This follows from MDDH assumption $[\mathbf{sA}]_1 \approx_c [\mathbf{c}]_1$ given $[\mathbf{A}]_1$.
- Then, we work in a one-by-one fashion, conceptually changing hsk_j to semi-function as below, which corresponds to $\mathsf{G}_{2,j,1}, \mathsf{G}_{2,j,2}$ and $\mathsf{G}_{2,j,3}$ respectively.
  - In $\mathsf{G}_{2,j,1}$, we change hsk_i to pseudo-normal. Namely, we conceptually replace all $[\mathbf{BR}_j]_2$ that appear in hsk_j with $[\mathbf{D}_j]_2$. Since we actually change crs, $[\mathbf{BR}_j]_2$ appear in all queried $\mathsf{sk}_{j,y'}$ will also be substituted. This follows from MDDH assumption $[\mathbf{BR}_j]_2 \approx_c [\mathbf{D}_j]_2$ given $[\mathbf{B}]_1$.
  - In $\mathsf{G}_{2,j,2}$, we change hsk_j to pseudo-semi-function. Namely, we replace $[\mathbf{V}_j\mathbf{D}_j + \mathbf{K}]_2$ with $[\mathbf{V}_j\mathbf{D}_j + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2$ where $\widetilde{\mathbf{k}}$ is random and $\mathbf{c}^\perp$ satisfies $\mathbf{cc}^\perp = 1, \mathbf{Ac}^\perp = \mathbf{0}$. This follows from the case-study arguments:
    $P(x,y) = 0$ In this case, we make use of the entropy in $\mathbf{W}_{0,j}$ and α-privacy of P's predicate encoding, to hide the entropy in $\mathbf{V}_j$. To argue the "partial" secrecy of $\mathbf{K}$ in $\mathbf{V}_j\mathbf{D}_j + \mathbf{K}$.
    $P(x,y) = 1$ This case implies that $\mathsf{msk}_j = (\mathbf{U}_j, \mathbf{W}_{1,j})$ is not leaked to the adversary. We aim to make use of the entropy in $\mathbf{U}_j$ to hide entropy in $\mathbf{V}_j$. To argue the "partial" secrecy of $\mathbf{K}$ in term $\mathbf{V}_j\mathbf{BR}_j + \mathbf{K}$. In advance, we must argue that all queried $\mathsf{sk}_{j,y'}$ will not leak the entropy of $\mathbf{U}_j$. We *hierarchically invoke a dual-system method* on all $\mathsf{sk}_{j,y'}$ to finish this argument, we explain the sketch in this case later and give a high-level overview in Fig 4.
  - In $\mathsf{G}_{2,j,3}$, we change hsk_j to semi-function. Namely, we replace all $[\mathbf{D}_j]_2$ that appeared in hsk_j and all queried $\mathsf{sk}_{j,y'}$, with $[\mathbf{BR}_j]_2$. This justified by MDDH assumption analogous to $\mathsf{G}_{2,j,1}$.
- Last, we change $[\mathbf{cKe}^\top]_T \cdot \mathsf{m}_b^*$ in ct_b^* to random. This is justified by the fact that $\mathbf{cK}$ is statistically random given $\mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}$ that in all hsk.

Hierarchically Invoked Dual-system Method. The goal is to prove $\mathsf{G}_{2,j,1} \mapsto \mathsf{G}_{2,j,2}$ in the case: $P(x,y) = 1$. Recall that this case implies: (1) $\mathsf{msk}_j = (\mathbf{U}_j, \mathbf{W}_{1,j})$ is hidden from the adversary; (2) for all queried $\mathsf{sk}_{j,y'}$, it holds that $P'(x',y') = 0$. As the overview in Fig 4, we employ the "key-related" part of dual-system approach on all $\mathsf{sk}_{j,y'}$, using $([\mathbf{A}]_1, [(\mathbf{B}\|\mathbf{D}_j)]_2)$ as the dual-system spaces instead. We begin with the game H_0 that identical to $\mathsf{G}_{2,j,1}$, and proceed with the process as follows:

Hm	hsk_j	$\mathsf{sk}_{j,y'}$	**Remark**
H_0	$[\mathbf{V}_j\mathbf{D}_j+\mathbf{K}]_2$	$[\mathbf{D}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{D}_j]_2$	Identical to $\mathsf{G}_{2,j,1}$
$\mathsf{H}_{1,q,1}$	$[\mathbf{V}_j\mathbf{D}_j+\mathbf{K}]_2$	$[\widetilde{\mathbf{R}}]_2, [\mathbf{U}_j\mathbf{D}_j]_2$	MDDH
$\mathsf{H}_{1,q,2}$	$[\mathbf{V}_j\mathbf{D}_j+\mathbf{K}]_2$	$[\widetilde{\mathbf{R}}]_2, [\mathbf{U}_j\mathbf{D}_j+\mathbf{c}^{\perp}\widehat{\mathbf{k}}]_2$	α-privacy of P'
$\mathsf{H}_{1,q,3}$	$[\mathbf{V}_j\mathbf{D}_j+\mathbf{K}]_2$	$[\mathbf{D}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{D}_j+\mathbf{c}^{\perp}\widehat{\mathbf{k}}]_2$	MDDH
H_2	$[\mathbf{V}_j\mathbf{D}_j+\mathbf{K}+\mathbf{c}^{\perp}\widetilde{\mathbf{k}}]_2$	$[\mathbf{D}_j\mathbf{R}]_2, [\mathbf{U}_j\mathbf{D}_j+\mathbf{c}^{\perp}\widehat{\mathbf{k}}]_2$	Statistic

Fig. 4: Games for hierarchically invoked dual-system method, and sequence $\{\mathsf{H}_{1,q,k}\}_{k=1,2,3}$ are one-by-one for all $q \in [Q]$. Here Q refers to the number of queried $\mathsf{sk}_{j',y}$, and q refers to the k-th secret keys. Note that $\widehat{\mathbf{k}}$ is randomly chosen, $\mathbf{c}^{\perp}$ is defined as in Fig 3. For simplicity, we omit a sequence $\{\mathsf{H}_{3,q,k}\}_{k=1,2,3}$ that analogous to $\{\mathsf{H}_{1,q,k}\}_{k=1,2,3}$, except cancel the extra term $\mathbf{c}^{\perp}\widehat{\mathbf{k}}$ in $\mathsf{H}_{3,j,2}$. Observe that $\mathsf{H}_{3,Q,3}$ is identical to $\mathsf{G}_{2,j,2}$ in Fig 3.

- First, since msk_j is honest and secret, we are able to change all $\mathsf{sk}_{j,y'}$ to semi-function gradually as follows, which corresponds to $\mathsf{H}_{1,q,1}$, $\mathsf{H}_{1,q,2}$ and $\mathsf{H}_{1,q,3}$ respectively.
  - In $\mathsf{H}_{1,q,1}$, we change the q-th $\mathsf{sk}_{j,y'}$ to pseudo-normal. By switching all $[\mathbf{D}_j\mathbf{R}]_2$ that appear in the q-th $\mathsf{sk}_{j,y'}$ to $[\widetilde{\mathbf{R}}]_2$. This follows from MDDH assumption $[\mathbf{D}_j\mathbf{R}]_2 \approx_c [\widetilde{\mathbf{R}}]_2$ given $[\mathbf{D}_j\mathbf{R}]_2$.
  - In $\mathsf{H}_{1,q,2}$, we change the q-th $\mathsf{sk}_{j,y'}$ to pseudo-semi-function. Namely, we replace $[\mathbf{U}_j\mathbf{D}_j]_2$ with $[\mathbf{U}_j\mathbf{D}_j+\mathbf{c}^{\perp}\widehat{\mathbf{k}}]_2$ where $\widetilde{\mathbf{k}}$ is random. Since $P'(x', y') = 0$, we can use the entropy in $\mathbf{W}_{1,j}$ and α-privacy to argue the "partial" secrecy of $\mathbf{U}_j$ in q-th $\mathsf{sk}_{j,y'}$.
  - In $\mathsf{H}_{1,q,3}$, we switch the q-th $\mathsf{sk}_{j,y'}$ to semi-function. Namely, we change all $[\widetilde{\mathbf{R}}]_2$ that appear in the q-th $\mathsf{sk}_{j,y'}$ to $[\mathbf{D}_j\mathbf{R}]_2$. This is ensured by MDDH assumption analogous to $\mathsf{H}_{1,q,1}$.
- Then in H_2, we change hsk_j to pseudo-semi-function by switching $[\mathbf{V}_j\mathbf{D}_j+\mathbf{K}]_2$ to $[\mathbf{V}_j\mathbf{D}_j+\mathbf{K}+\mathbf{c}^{\perp}\widetilde{\mathbf{k}}]_2$. This follows from the fact that the entropy in $\mathbf{U}_j$ is statistically hidden, given $\mathbf{U}_j\mathbf{D}_j+\mathbf{c}^{\perp}\widehat{\mathbf{k}}$. So that the entropy in $\mathbf{U}_j$ is sufficient to hide the entropy in $\mathbf{V}_j$. In order to argue the "partial" secrecy of $\mathbf{K}$ in $\mathbf{V}_j\mathbf{D}_j+\mathbf{K}$.
- Last, we change all $\mathsf{sk}_{j,y'}$ back to normal one-by-one. It need a sequence sequence $\{\mathsf{H}_{3,q,k}\}_{k=1,2,3}$ that analogous to $\{\mathsf{H}_{1,q,k}\}_{k=1,2,3}$, we omit the details here.

Observe that after switching back all $\mathsf{sk}_{j,y'}$, the final $\mathsf{H}_{3,Q,2}$ is identical to $\mathsf{G}_{2,j,2}$, that give the desired form of hsk_j and $\mathsf{sk}_{j,y'}$.

2.4 Final Delegated Reg-ABE Scheme

There still exists two gaps between scheme (10) with the final delegated Reg-ABE:

- handling maliciously registered authorities;
- transforming the slotted scheme to the (full-fledged) delegated Reg-ABE scheme.

To address these gaps, we provide a brief explanation of how to handle maliciously registered authorities and construct a full-fledged scheme via the slotted scheme in this section.

Handle Malicious Slots. In the previous overview, we ignored the case the case where some slots are malicious. [ZZGQ23] provides a solution to handle the malicious public keys in sReg-ABE, but in our scheme of slotted delegated Reg-ABE, the malicious slots bring some new obstacles in the proof, we explain how to modify the approach in [ZZGQ23] to handle them:

1. Suppose the i^*-th slot is malicious, the first obstacle is identical to that in [ZZGQ23,ZLZ+24]: When switching $[\mathbf{sA}]_1 \rightarrow [\mathbf{c}]_1$ (in $\mathsf{G}_0 \mapsto \mathsf{G}_1$), the simulator cannot simulate $[\mathbf{cU}_{i^*}, \mathbf{cW}_{1,i^*}]_1$ in challenge ciphertext, since $(\mathbf{U}_{i^*}, \mathbf{W}_{1,i^*})$ over $\mathbb{Z}_p$ is unknown. We can handle this obstacle via quasi-adaptive non-interactive zero-knowledge proof/argument (QA-NIZK) as in [ZZGQ23,ZLZ+24].
2. Suppose i^*-th slot is malicious, the hierarchically invoked dual-system brings another obstacle into the case-study of $P(x, y_j) = 1$, for some $j \neq i^*$. During switching $[\mathbf{D}_j\mathbf{R}]_2 \rightarrow [\widetilde{\mathbf{R}}]_2$ (in $\mathsf{H}_{1,q,1} \mapsto \mathsf{H}_{1,q,2}$), the simulator cannot simulate the term $[\sum_{i\neq j} \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}})]_2$ in $\mathsf{sk}_{j,y'}$. Since $\mathbf{W}_{1,i^*}$ is unknown and appears in that term. We give the following solution, inspired by the idea of handling the first obstacle [ZZGQ23].
   (i) Fix the index j, for all $i \in [L]$ such that $i \neq j$, we introduce the terms $[\mathbf{G}_{i,j}]_2$ where $\mathbf{G}_{i,j} \leftarrow \mathbb{Z}_p^{(3k+1)\times(4k+1)}$ into the crs; and include terms $[\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2$ into the mpk_i. In the proof, the simulator program
   $$\mathbf{G}_{i,j} = (\widetilde{\mathbf{R}} \| \mathbf{I}_{3k+1})\widetilde{\mathbf{G}}_{i,j}, \quad \widetilde{\mathbf{G}}_{i,j} \leftarrow \mathbb{Z}_p^{(4k+1)\times(4k+1)}$$
   where $\widetilde{\mathbf{G}}_{i,j}$ makes sure that $\mathbf{G}_{i,j}$ is random. And after switching $[\mathbf{BR}_j]_2 \rightarrow [\mathbf{D}_j]_2$, for all $i \in [L]\backslash\{j\}$, receiving following term in mpk_i:
   $$[\mathbf{H}_{i,j}, \mathbf{P}_{i,j}]_2 = [\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{D}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2$$
   the simulator can extract $[\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}})]_2$ to simulate $\mathsf{sk}_{j,y'}$ by computing
   $$[\mathbf{P}_{i,j}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{G}}_{i,j}^{-1}\mathbf{E}_1)]_2, \quad \mathbf{E}_1 = \begin{pmatrix}\mathbf{I}_k \\ \mathbf{0}\end{pmatrix}.$$
   (ii) To avoid the malicious mpk_i that include terms $\mathbf{H}_{i,j} = \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{D}_j)$ and $\mathbf{P}_{i,j} = \mathbf{W}'_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})$ such that $\mathbf{W}_{1,i} \neq \mathbf{W}'_{1,i}$. We similarly use the QA-NIZK for linear space to prove that
   $$(\mathbf{H}_{i,j} \| \mathbf{P}_{i,j}) \in \mathsf{span}\big((\mathbf{I}_{n'} \otimes \mathbf{D}_j) \| (\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})\big)$$
   which ensure $\mathbf{W}_{1,i} = \mathbf{W}'_{1,i}$.

Moreover, we optimal the matrices size expansion caused by the solution in previous works. We recall that [ZZGQ23,ZLZ+24] employ the wider $\mathbf{A}$, $\mathbf{G}_i$ and higher $\mathbf{U}_i$ to prevent issue that the entropy of $\mathbf{U}_i$ is leaked by $[\mathbf{Q}_{0,i} = \mathbf{G}_i\mathbf{U}_i]_1$[4]. In this work, we improve this technique and no longer employ wider $\mathbf{A}$, $\mathbf{G}_i$ and higher $\mathbf{U}_i$. For simplicity, this technique allows the entropy of $\mathbf{U}_i$ to be revealed in challenge ciphertext and queried secret keys for security, but hidden in $[\mathbf{Q}_{0,i} = \mathbf{G}_i\mathbf{U}_i]_1$. This technique can also be used to show that the entropy of $\mathbf{W}_{1,i}$ will not be revealed by $[\mathbf{G}_i\mathbf{W}_{1,i}]_1$ and $[\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2$ for all $j \in [L] \setminus \{i\}$. See Section 5.4 for more details.

Transformation from Slotted Scheme to Full-fledged Scheme. For generality, we explain the transformation under the semantic of delegated Reg-FE. To build the delegated Reg-FE via slotted delegated Reg-FE scheme, we modified the "power-of-two" approach [HLWW23] to our new primitive. Besides simply introducing an algorithm to issue secret keys, it's also crucial to consider the secret keys updation after updating the corresponding helper key (See Section 10 for more details). The reduction in [HLWW23] which let the simulator to run aggregation of slotted instances after receiving challenge from its adversary, can only prove the security model that allows queries for secret keys after *all* authorities have been registered. However, to achieve a stronger and more natural security model, we allow the adversary to query for secret keys at any time after the *first* authority has been registered. In our reduction, the simulator is allowed to repeatedly aggregate slotted instances whenever the adversary query for a secret key. This required the security model of slotted delegated Reg-FE to support the repeated aggregation and query for secret keys after each one. We propose the detailed definition in Section 4.2, and prove that is equivalent to the model only supports once (challenge) aggregation, which is more natural for slotted delegated Reg-FE. See more details in Appendix B.

[4] Note that the notations $\mathbf{G}_i$ and $\mathbf{Q}_{0,i}$ are corresponding to $\mathbf{R}_i$ and $\mathbf{Q}_i$ in [ZZGQ23,ZLZ+24].

2.5 Generic Scheme

In this section, we give a technical overview of the generic construction of slotted delegated Reg-FE. Applying the "slotted-to-full" transformation in Section 2.4 yields the final generic scheme.

Start Point: "FE-to-HFE" Generic Transformation [BS15]. As we mentioned in Section 1.2, our delegated Reg-FE shares a hierarchical structure analogous to a 3-tiers HFE. Given two general FE instances $(\mathsf{F.Gen}_0, \mathsf{F.Enc}_0)$ and $(\mathsf{F.Gen}_1, \mathsf{F.Enc}_1)$[5] the 3-tiers HFE [BS15] works as follows:

- The ciphertext of the whole system is in the form of $\mathsf{ct} = \mathsf{F.Enc}_0(x)$.
- For a function g, the top-tier entity generates the (helper) secret key as $\mathsf{hsk}_g = \mathsf{F.Key}_0(\mathsf{ReEnc}_g(\cdot))$. Where $\mathsf{ReEnc}_g(\cdot)$ is the re-encryption function, it takes x as input and outputs the encryption of $g(x)$ using $\mathsf{F.Enc}_1$.
- An entity in middle-tier keeps hsk_g can delegate the secret key for function f as $\mathsf{sk}_f = \mathsf{F.Key}_1(f)$.

The bottom-tier user keeps sk_f and hsk_g can decrypt ct as follows

(1) using $\mathsf{hsk}_g = \mathsf{F.Key}_0(\mathsf{ReEnc}_g(\cdot))$ and $\mathsf{ct} = \mathsf{F.Enc}_0(x)$, one can recover $\mathsf{ct}' = \mathsf{ReEnc}_g(x) = \mathsf{Enc}_1(g(x))$;
(2) further, with ct' and $\mathsf{sk}_f = \mathsf{F.Key}_1(f)$, the value $f \circ g(x)$ will be revealed.

We note that for any class of functions (even the simple identity check), the underlying $(\mathsf{F.Enc}_1, \mathsf{F.Gen})$ must be a general-purpose scheme to support the re-encryption function. The security is restricted in the semi-adaptive model. We omit the proof analysis for brevity, and note that the proof needs the help of puncturable pseudorandom functions and secret key encryptions.

Generic Slotted Delegated Reg-FE. Our generic slotted delegated Reg-FE employs the idea of re-encryption in the "curator-authority-user" type of hierarchical framework. Specifically, given a general-purpose slotted Reg-FE $(\mathsf{R.Setup}, \mathsf{R.Gen}, \mathsf{R.Agg}, \mathsf{R.Enc})$ and FE $(\mathsf{F.Setup}, \mathsf{F.Gen}, \mathsf{F.Enc})$, the slotted delegated Reg-FE works as follows:

- crs is exactly that of Reg-FE.
- To generate master key pair $(\mathsf{mpk}, \mathsf{msk})$ with function g, the authority (1) generates a $(\mathsf{mpk}', \mathsf{msk}')$ of FE; (2) generates the Reg-FE's key pair for re-encryption function $\mathsf{ReEnc}_g(\cdot)$, which outputs $\mathsf{F.Enc}(\mathsf{mpk}', g(x))$ for input x. Then the authority set $\mathsf{mpk} = (\mathsf{pk}, \mathsf{ReEnc}_g)$ and $\mathsf{msk} = (\mathsf{sk}, \mathsf{msk}')$. Here, the key-generations of both slotted delegated Reg-FE and slotted Reg-FE depend on specific functions (g and ReEnc_g, respectively).
- During aggregatiopn, the curator collects all slots' mpk and aggregates their $(\mathsf{pk}, \mathsf{ReEnc}_g)$ in the slotted Reg-FE. Here, each mpk is embedded inside the corresponding function ReEnc_g.
- The ciphertext of x is exactly a slotted Reg-FE's ct of x.
- The delegated function key of f consists of a FE's function key sk'_f under msk' and the sk of slotted Reg-FE. Notice that sk can be made public without hurting the security, the security relies on msk'.

The decryption proceeds in two steps: (1) using sk and the corresponding helper key to decrypt the slotted Reg-FE's ct, the user can recover $\mathsf{ReEnc}_g(x) = \mathsf{F.Enc}(\mathsf{mpk}', g(x))$; (2) using the FE's function key sk'_f under msk', the user can recover $f \circ g(x)$. The generic construction achieves weaker security, compared to our concrete schemes, in two aspects.

- Semi-adaptive Security: Inherited from [BS15], the generic result can only achieve semi-adaptive security.
- No malicious slot: Since the security proof adapted from [BS15] crucially depends on programming key-generation and re-encryption function in most steps, the generic construction cannot handle maliciously generated keys. This is true even when the underlying Reg-FE is able to handle malicious slot.

[5] Here we hardcode the master public key and master secret key inside F.Enc, F.Gen, respectively, for notation simplicity.

We note that re-encryption function ReEnc_g has to be hardwired into key generation, since in the proof, the challenger cannot program ReEnc_g during the deterministic and public aggregation phase. As we have mentioned that both delegated Reg-FE and underlying Reg-FE are required to have "function-dependent generation". [CHW25] recently mentioned it in the context of Reg-ABE and considered it as a minor restriction. Similar to [BS15], it also needs the help of puncturable pseudorandom functions and secret key encryptions. The idea of proof is similar to that for FE's simulation-based security. A bit more concretely, the secret key encryption message space serves as a private slot and allows the challenger to embed $g(x)$ into $\mathsf{ReEnc}_g(\cdot)$ and remove x from ciphertext. And similar to [BS15], our generic construction requires the underlying slotted Reg-FE for general class of function to support the registration of ReEnc_g. Instantiating our construction with unbounded Reg-FE [FFM+23,DPY24] and unbounded FE [GGH+13,Wat15] results a slotted delegated Reg-FE for arbitrary functions, and further yields a delegated Reg-FE supporting unbounded registrations and delegations. Also, we note that, the proof will be much simpler that [BS15] since we only consider 3-tier hierarchy. See Section 9 for more details.

2.6 More Slotted Concrete Schemes

Remaining concrete constructions can be built by following the similar technique roadmap of delegated Reg-ABE. Due to the space limitation, in this section, we directly present their slotted construction in the prime-order groups and neglect the malicious case. Applying the final step in Section 2.4 can move them to the full-fledged version respectively.

Scheme of Slotted Delegated Reg-IPFE. Our slotted delegated Reg-IPFE in the prime-order group for inner-product functionalities

$$G = \{\mathbf{M} : \mathbf{x} \mapsto \mathbf{x}\mathbf{M}\} \quad \text{and} \quad F = \{\mathbf{f} : \mathbf{y} \mapsto \mathbf{y}\mathbf{f}^\top\}$$

is as follows:

$$\begin{aligned}
\mathsf{crs} &= [\mathbf{A}\mathbf{V}]_1, [\mathbf{A}\mathbf{W}_i]_1, \quad \forall i \in [L] \\
&\quad\ [\mathbf{B}\mathbf{r}_j^\top, \mathbf{W}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}\mathbf{r}_j^\top)]_2, \quad (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\
\mathsf{mpk}_+ &= [\textstyle\sum_i (\mathbf{A}\mathbf{U}_i + \mathbf{A}\mathbf{W}_i(\mathbf{M}_i \otimes \mathbf{I})), \sum_i \mathbf{A}\mathbf{W}_i, \mathbf{A}\mathbf{V}]_1, \\
\mathsf{hsk}_j &= [\mathbf{B}\mathbf{r}_j^\top, \textstyle\sum_{i\neq j}(\mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}\mathbf{r}_j^\top) + \mathbf{W}_i(\mathbf{M}_i \otimes \mathbf{B}\mathbf{r}_j^\top)), \sum_{i\neq j} \mathbf{W}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}\mathbf{r}_j^\top)]_2, \\
\mathsf{ct} &= [\mathbf{s}\mathbf{A}, \textstyle\sum_i (\mathbf{s}\mathbf{A}\mathbf{U}_i + \mathbf{s}\mathbf{A}\mathbf{W}_i(\mathbf{M}_i \otimes \mathbf{I})), \mathbf{x} \otimes \mathbf{s}\mathbf{A}\mathbf{V} + \sum_i \mathbf{s}\mathbf{A}\mathbf{W}_i, \mathbf{s}\mathbf{A}\mathbf{V}]_1, \\
\mathsf{sk}_{j,\mathbf{f}} &= \mathbf{U}_j(\mathbf{f}^\top \otimes \mathbf{I}).
\end{aligned}$$

where $\mathsf{mpk}_i = ([\mathbf{A}\mathbf{U}_i]_1, \{[\mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}\mathbf{r}_j^\top)]_2\}_{j\neq i})$ and $\mathsf{msk}_i = \mathbf{U}_i \in \mathbb{Z}_p^{(k+1)\times(2k+1)n_2}$; we let all matrices $\mathbf{I}$ have proper size. Here, for all $\mathbf{M} \in G$ and $\mathbf{f} \in F$, we have $\mathbf{M} \in \mathbb{Z}_p^{n_1 \times n_2}$ and $\mathbf{f} \in \mathbb{Z}_p^{1\times n_2}$. The basis $\mathbf{B}$ corresponding a $(2k+1)$-dimensional space and the security proof need the nested dual-system method as the Reg-IPFE [ZLZ+24], but no longer need hierarchically invoked dual-system to handle the secret keys as scheme (10), since we don't embed any random coin into secret keys. See Section 6 for more details of definitions and construction.

Scheme of Slotted Reg-ABE with Delegated IPFE. Our slotted Reg-ABE with delegated IPFE in the prime-order group for predicate P and inner-product functionality $F = \{\mathbf{f} : \mathbf{x} \mapsto \mathbf{x}\mathbf{f}^\top\}$ is as follows:

$$
\begin{aligned}
\mathsf{crs} &= [\mathbf{AV}]_1, [\mathbf{AV}_i, \mathbf{AW}_i]_1, \quad \forall i \in [L] \\
&\quad [\mathbf{Br}_j^\top, \mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{Br}_j^\top), \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{Br}_j^\top)]_2, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\
\mathsf{mpk}_+ &= [\textstyle\sum_i (\mathbf{AV}_i + \mathbf{AU}_i), \sum_i \mathbf{AW}_i, \sum_{i\in[L]} (\mathbf{AV}_i(\mathbf{a}_{y_i} \otimes \mathbf{I}) + \mathbf{AW}_i(\mathbf{K}_{y_i} \otimes \mathbf{I})), \mathbf{AV}]_1, \\
\mathsf{hsk}_j &= [\mathbf{Br}_j^\top, \textstyle\sum_{i\neq j} \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{Br}_j^\top), \sum_{i\neq j} (\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{Br}_j^\top) + \mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{Br}_j^\top))]_2, \\
&\quad [\textstyle\sum_{i\neq j} (\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)(\mathbf{a}_{y_i} \otimes \mathbf{I}_{n'}) + \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)(\mathbf{K}_{y_i} \otimes \mathbf{I}_{n'}))]_2, \\
\mathsf{ct}_x &= [\mathbf{sA}, \mathbf{x} \otimes \mathbf{sAV} + \textstyle\sum_i (\mathbf{sAV}_i + \mathbf{sAU}_i), \sum_i \mathbf{sAW}_i(\mathbf{C}_x \otimes \mathbf{I})]_1, \\
&\quad [\textstyle\sum_i (\mathbf{sAV}_i(\mathbf{a}_{y_i} \otimes \mathbf{I}) + \mathbf{sAW}_i(\mathbf{K}_{y_i} \otimes \mathbf{I})), \mathbf{sAV}]_1, \\
\mathsf{sk}_{j,\mathbf{f}} &= \mathbf{U}_j(\mathbf{f}^\top \otimes \mathbf{I}).
\end{aligned}
$$

where $\mathsf{mpk}_i = ([\mathbf{AU}_i]_1, \{[\mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{Br}_j^\top)]_2\}_{j\neq i})$ and $\mathsf{msk}_i = \mathbf{U}_i \in \mathbb{Z}_p^{(k+1)\times(2k+1)n'}$; we let all matrices $\mathbf{I}$ have proper size. Here, n is the size corresponding to the PE of P, and for all $\mathbf{f} \in F$, we have $\mathbf{f} \in \mathbb{Z}_p^{1\times n'}$. The basis $\mathbf{B}$ corresponding a $(2k+1)$-dimensional space and the security proof need the nested dual-system method as the Reg-IPFE [ZLZ+24], but no longer need hierarchically invoked dual-system to handle the secret keys as scheme (10), since we don't embed any random coin into secret keys. See Section 7 for more details of definitions and construction.

Scheme of Slotted Reg-IPFE with Delegated ABE. Our slotted Reg-IPFE with delegated ABE in the prime-order group for inner-product functionality $F = \{\mathbf{f} : \mathbf{x} \mapsto \mathbf{x}\mathbf{f}^\top\}$ and predicate P is as follows:

$$
\begin{aligned}
\mathsf{crs} &= [\mathbf{AV}]_1, [\mathbf{AW}_{0,i}]_1, \quad \forall i \in [L] \\
&\quad [\mathbf{BR}_j, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_j)]_2, \quad \forall (i,j) \in [L] \times [L] \text{ s.t. } i \neq j \\
\mathsf{mpk}_+ &= [\mathbf{AV}, \textstyle\sum_i (\mathbf{AU}_i + \mathbf{AW}_{0,i}(\mathbf{y}_i^\top \otimes \mathbf{I})), \sum_i \mathbf{AW}_{0,i}, \sum_i \mathbf{AW}_{1,i}]_1, \\
\mathsf{hsk}_j &= [\mathbf{BR}_j, \textstyle\sum_{i\neq j} \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j), \sum_{i\neq j} \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_j)]_2, \\
&\quad [\textstyle\sum_{i\neq j} (\mathbf{U}_i\mathbf{BR}_j + \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_j)(\mathbf{y}_i^\top \otimes \mathbf{I}))]_2, \\
\mathsf{ct}_x &= [\mathbf{sA}, \mathbf{sAV}, \textstyle\sum_i (\mathbf{sAU}_i + \mathbf{sAW}_{0,i}(\mathbf{y}_i^\top \otimes \mathbf{I}))]_1, \\
&\quad [\mathbf{x} \otimes \mathbf{sAV} + \textstyle\sum_{i\in[L]} \mathbf{sAW}_{0,i}, \sum_i \mathbf{sAW}_{1,i}(\mathbf{C}_x \otimes \mathbf{I})]_1, \\
\mathsf{sk}_{j,y} &= [\mathbf{BR}_j\mathbf{R}, \textstyle\sum_{i\neq j} \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j\mathbf{R})]_2, \\
&\quad [\mathbf{U}_j\mathbf{BR}_j(\mathbf{a}_y \otimes \mathbf{I}) + \mathbf{W}_{1,j}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j\mathbf{R})(\mathbf{K}_y \otimes \mathbf{I})]_2.
\end{aligned}
$$

where $\mathsf{msk}_i = (\mathbf{U}_i, \mathbf{W}_{1,i}) \in \mathbb{Z}_p^{(k+1)\times(5k+2)} \times \mathbb{Z}_p^{(k+1)\times(5k+2)n'}$ and $\mathsf{mpk}_i = ([\mathbf{AU}_i, \mathbf{AW}_{1,i}]_1, \{[\mathbf{U}_i\mathbf{BR}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j)]_2\}_{j\neq i})$; and we let all matrices $\mathbf{I}$ have proper size. Here for all $\mathbf{f} \in F$, we have $\mathbf{f} \in \mathbb{Z}_p^{1\times n}$ and n' is the size corresponding to the PE of P. The basis $\mathbf{B}$ corresponding to a $(5k+2)$-dimensional space for using nested dual-system method to change hsk, and hierarchically invoking dual-system method to change secret keys as in scheme (10). See Section 8 for more details.

3 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. $\mathbf{M}$). $\mathbf{a}[i]$

denote the ith entry of $\mathbf{a}$. We use $\mathsf{span}(\mathbf{M})$ to denote the *row* span of $\mathbf{M}$, use $\mathsf{span}^{\intercal}(\mathbf{M})$ to denote the *column* span of $\mathbf{M}$, and use $\mathsf{basis}(\mathbf{M})$ to denote a basis of the row 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 $n, m \in \mathbb{N}$.

3.1 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[6] in $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

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

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:

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

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 $\mathbf{B}_1^{\parallel} \in \mathbb{Z}_p^{\ell_1 \times \ell}, \mathbf{B}_2^{\parallel} \in \mathbb{Z}_p^{\ell_2 \times \ell}, \mathbf{B}_3^{\parallel} \in \mathbb{Z}_p^{\ell_3 \times \ell}$ as its dual basis, for all $\sigma, \delta \in \{1, 2, 3\}$, it holds that:

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

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

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

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

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

Assumption 2 *($\mathrm{SD}^{\mathbb{G}_s}_{\mathbf{B}_1\mapsto\mathbf{B}_2}$ 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 $\mathrm{SD}^{\mathbb{G}_s}_{\mathbf{B}_1\mapsto\mathbf{B}_2}$ 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: $\mathbf{B}_1^{\parallel}, \mathbf{B}_2^{\parallel}, \mathbf{B}_3^{\parallel}$ such that for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

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

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

3.2 Predicate Encodings

We review the notion of predicate encoding [Wee14,CGW15]; for simplicity, we use the formulation in [ABS17,ACGU20]. A predicate $P : X \times Y \to \{0,1\}$ has a (n, n_c, n_k)-predicate encoding if: For all $x \in X$, $y \in Y$, there exist

$$\mathbf{C}_x \in \mathbb{Z}_p^{n\times n_c},\ \mathbf{K}_y \in \mathbb{Z}_p^{n\times n_k},\ \mathbf{a}_y \in \mathbb{Z}_p^{1\times n_k},\ \mathbf{d}_{x,y} \in \mathbb{Z}_p^{1\times(n_k+n_c)}$$

such that, letting

$$\mathbf{M}_{x,y} = \begin{pmatrix} \mathbf{a}_y & \mathbf{0}_{n_c} \\ \mathbf{K}_y & \mathbf{C}_x \end{pmatrix} \in \mathbb{Z}_p^{(1+n)\times(n_k+n_c)}$$

we have

- **correctness:** for $x \in X$ and $y \in Y$ such that $P(x,y) = 1$:

$$\mathbf{M}_{x,y}\mathbf{d}_{x,y}^\top = \mathbf{e}_1^\top;$$

- **security:** for $x \in X$ and $y \in Y$ such that $P(x,y) = 0$ and for all $\alpha \in \mathbb{Z}_p$:

$$\{x, y, \alpha, (\alpha\|\mathbf{w})\mathbf{M}_{x,y}\} \approx_s \{x, y, \alpha, (0\|\mathbf{w})\mathbf{M}_{x,y}\}, \quad \mathbf{w} \leftarrow \mathbb{Z}_p^n.$$

Also, we require that (1) given P, one can efficiently determine n, n_c, n_k; (2) given x, one can efficiently compute $\mathbf{C}_x$; (3) given y, one can efficiently compute $\mathbf{K}_y$ and $\mathbf{a}_y$; (4) given both x and y, one can efficiently compute $\mathbf{d}_{x,y}$.

3.3 Quasi-Adaptive Non-Interactive Zero-Knowledge Argument

Algorithms. A Quasi-adaptive Non-interactive Zero-knowledge Argument (QA-NIZK) for $\mathbb{G}_1$-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 stateful PPT adversary $\mathcal{A}$, the advantage

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

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 $[\mathbf{M}]_1$. And the definition for $\mathbb{G}_2$-linear space is analogous, except that it's for $[\mathbf{M}]_2 \in \mathbb{G}_2^{m\times n}$ instead of $[\mathbf{M}]_1$ and $[\mathbf{Y}]_2$ with $\mathbf{X} \in \mathbb{Z}_p^{\ell\times m}$ such that $\mathbf{Y} = \mathbf{XM}$ instead of $[\mathbf{Y}]_1$; in unbounded simulation soundness, there is $\mathbf{Y}^* \notin \mathsf{span}(\mathbf{M})$ instead of $\mathbf{Y}^* \notin \mathsf{span}^\top(\mathbf{M})$.

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. [ZZGQ23] shows the more detailed scheme for $\mathbb{G}_1$-linear space, while the scheme for $\mathbb{G}_2$ can obtain from it by simply swapping all terms over $\mathbb{G}_1$ and $\mathbb{G}_2$ and transpose all matrices.

3.4 Slotted Registered Functional Encryption

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

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

We require that R.Agg and R.Dec are deterministic.

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

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

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

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

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

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

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

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

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

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

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

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

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. Compared with the original definition in [FFM+23,ZLZ+24,DPY24], the definition we consider as above is a weaker version in the following aspects.

- The key-generation algorithm is function-dependent. Here, the function is specified in R.Gen time rather than in R.Agg time.
- The security model is weakened to semi-adaptive. Here, $\mathcal{A}$ claims the challenge x_o^*, x_1^*, after obtaining crs and before making any query.
- The malicious pk is not allowed in the security model. Here, all pk^*_{i,f_i^*} issued by $\mathcal{A}$ is generated by $\mathsf{OGen}(i, f_i^*)$.

3.5 Functional Encryption

Algorithms. A functional encryption FE for functionality $F : X \to Z$ consists of four efficient algorithms:

- $\mathsf{F.Setup}(1^\lambda, F) \to (\mathsf{mpk}, \mathsf{msk})$: It takes as input security parameter 1^λ, functionality F, output the master key pair $(\mathsf{mpk}, \mathsf{msk})$.
- $\mathsf{F.Gen}(\mathsf{msk}, f) \to \mathsf{sk}_f$: It takes as input master secret key msk and $f \in F$, output a secret key sk_f.
- $\mathsf{F.Enc}(\mathsf{mpk}, x) \to \mathsf{ct}$: It takes as input master public key mpk and $x \in X$, output a ciphertext ct.
- $\mathsf{F.Dec}(\mathsf{sk}_f, \mathsf{ct}) \to z/\perp$: It takes as input sk_f and ct, outputs $z \in Z$ or a special symbol $\perp$.

Correctness. For all $\lambda \in \mathbb{N}$, all F, all $x \in X$ and $f \in F$ we have

$$\Pr\left[\mathsf{F.Dec}(\mathsf{sk}_f, \mathsf{ct}) = f(x) \;\middle|\; \begin{array}{r} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{F.Setup}(1^\lambda, F) \\ \mathsf{ct} \leftarrow \mathsf{F.Enc}(\mathsf{mpk}, x) \\ \mathsf{sk}_f \leftarrow \mathsf{F.Gen}(\mathsf{msk}, f) \end{array}\right] = 1$$

Selective Indistinguishability-based Security (sel IND-security) . For all stateful PPT adversary $\mathcal{A}$, the semi-adaptive indistinguishability-based security requires the advantage function $\mathsf{Adv}^{\mathrm{FE}}_{\mathcal{A}}$ defined as follows is negligible in λ:

$$\mathsf{Adv}^{\mathrm{FE}}_{\mathcal{A}}(\lambda) = \Pr\left[b = b' \middle| \begin{array}{l} x_0^*, x_1^* \leftarrow \mathcal{A}(1^\lambda),\ (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{F.Setup}(1^\lambda, F) \\ b \leftarrow \{0,1\}, \mathsf{ct}^* \leftarrow \mathsf{F.Enc}(\mathsf{mpk}, x_b^*) \\ b' \leftarrow \mathcal{A}^{\mathsf{F.Gen}(\mathsf{msk},\cdot)}(\mathsf{mpk}, \mathsf{ct}^*) \end{array}\right] - 1/2,$$

where we require $f(x_0^*) = f(x_1^*)$ for all f queried to $\mathsf{F.Gen}(\mathsf{msk}, \cdot)$.

3.6 Secret-Key Encryption with Pseudorandom Ciphertext

Algorithms. A secret-key encryption (SKE) consists of three algorithms

- $\mathsf{S.Gen}(1^\lambda) \to k$: It takes as input a security parameter 1^λ, outputs a secret key k.
- $\mathsf{S.Enc}(k, \mathsf{m}) \to c$: It takes as input a secret key k and a message $\mathsf{m} \in \mathcal{M}$, output a ciphertext c.
- $\mathsf{S.Dec}(k, c) \to \mathsf{m}/\perp$: It takes as input a secret key k and ciphertext c, output a message $\mathsf{m} \in \mathcal{M}$ or a special symbol $\perp$.

Correctness. For all $\lambda \in \mathbb{N}$, all message m, it holds that

$$\Pr\left[\mathsf{S.Dec}(k, c) = \mathsf{m} \middle| \begin{array}{l} k \leftarrow \mathsf{S.Gen}(1^\lambda) \\ c \leftarrow \mathsf{S.Enc}(k, \mathsf{m}) \end{array}\right] = 1$$

We also require that $\Pr[\mathsf{S.Dec}(k, c) = \perp] = (1 - \mathsf{negl}(\lambda))$ if $c \leftarrow \{0,1\}^\ell$ for some length $\ell = \ell(\lambda)$.

Pseudorandom Ciphertext. For all statefull PPT adversary $\mathcal{A}$, the pseudorandom ciphertext requires the advantage function $\mathsf{Adv}^{\mathrm{SKE}}_{\mathcal{A}}$ defined as follows is negligible in λ:

$$\mathsf{Adv}^{\mathrm{SKE}}_{\mathcal{A}}(\lambda) = \Pr\left[b = b' \middle| \begin{array}{l} k \leftarrow \mathsf{S.Gen}(1^\lambda), \mathsf{m}^* \leftarrow \mathcal{A}^{\mathsf{S.Enc}(k,\cdot)}(1^\lambda) \\ c_0^* \leftarrow \mathsf{S.Enc}(k, \mathsf{m}^*), c_1^* \leftarrow \{0,1\}^{|c_0^*|} \\ b \leftarrow \{0,1\}, b' \leftarrow \mathcal{A}^{\mathsf{S.Enc}(k,\cdot)}(c_b^*) \end{array}\right]$$

where $|c_0^*|$ denotes the bit-length of c_0^*.

3.7 Puncturable Pseudorandom Function

Algorithms. Let $\{\mathcal{K}_\lambda, \mathcal{X}_\lambda, \mathcal{Y}_\lambda\}_{\lambda \in \mathbb{N}}$ be a sequence of sets, a puncturable pseudorandom function family consists of three algorithms

- $\mathsf{Prf.Gen}(1^\lambda) \to K$: It takes as input security parameter 1^λ, output a key $K \in \mathcal{K}_\lambda$.
- $\mathsf{Prf.Eval}(K, x) \to y$: It takes as input a key $K \in \mathcal{K}_\lambda$ and a value $x \in \mathcal{X}_\lambda$. Outputs a value $y \in \mathcal{Y}_\lambda$.
- $\mathsf{Prf.Punc}(K, x^*) \to K_{x^*}$: It takes as input a key $K \in \mathcal{K}_\lambda$ and a punctured point $x^* \in \mathcal{X}_\lambda$, outputs a punctured key $K_{x^*} \in \mathcal{K}_\lambda$.

Where $\mathcal{K}_\lambda, \mathcal{X}_\lambda, \mathcal{Y}_\lambda$ refer to the key space, domain, and range of the function family. And notice that we require that Prf.Gen, Prf.Punc are probabilistic and Prf.Eval is deterministic.

Pseudorandomness. For any stateful PPT adversary $\mathcal{A}$, it holds that

$$\begin{bmatrix} K \leftarrow \mathsf{Prf.Gen}(1^\lambda) \\ \alpha \leftarrow \mathcal{A}^{\mathsf{Prf.Eval}(K,\cdot)}(1^\lambda) \end{bmatrix} \approx_c \begin{bmatrix} f \leftarrow \mathcal{F}_\lambda \\ \alpha \leftarrow \mathcal{A}^{f(\cdot)}(1^\lambda) \end{bmatrix}$$

where $\mathcal{F}_\lambda$ is the set of all functions that map $\mathcal{X}_\lambda$ to $\mathcal{Y}_\lambda$.

Functionality. For all $\lambda \in \mathbb{N}$, all $x^* \in \mathcal{X}_\lambda$, all $K \leftarrow \mathsf{Prf.Gen}(1^\lambda)$ and $K_{x^*} \leftarrow \mathsf{Prf.Punc}(K, x^*)$, the following equation holds for any $x \in \mathcal{X}_\lambda \setminus \{x^*\}$:

$$\Pr\left[\mathsf{Prf.Eval}(K, x) = \mathsf{Prf.Eval}(K_{x^*}, x)\right] = 1.$$

According to [BS15], without loss of generality, given a $y^* \in \mathcal{Y}_\lambda$, there exist an *augmented evaluation* $\widehat{\mathsf{Prf.Eval}}_{y^*}(K_{x^*}, \cdot)$ such that $\widehat{\mathsf{Prf.Eval}}_{y^*}(K_{x^*}, x^*) = y^*$ and $\widehat{\mathsf{Prf.Eval}}_{y^*}(K_{x^*}, x) = \mathsf{Prf.Eval}(K_{x^*}, x)$ for all $x \neq x^*$.

Pseudorandomness at Punctured Point. For any stateful PPT adversary $\mathcal{A}$, it holds that

$$\begin{bmatrix} x^* \leftarrow \mathcal{A}(1^\lambda) \\ K \leftarrow \mathsf{Prf.Gen}(1^\lambda), K_{x^*} \leftarrow \mathsf{Prf.Punc}(K, x^*) \\ y = \mathsf{Prf.Eval}(K, x^*), \alpha \leftarrow \mathcal{A}(K_{x^*}, y) \end{bmatrix} \approx_c \begin{bmatrix} x^* \leftarrow \mathcal{A}(1^\lambda) \\ K \leftarrow \mathsf{Prf.Gen}(1^\lambda), K_{x^*} \leftarrow \mathsf{Prf.Punc}(K, S^*) \\ y \leftarrow \mathcal{Y}_\lambda, \alpha \leftarrow \mathcal{A}(K_{x^*}, y) \end{bmatrix}$$

4 Delegated Registered Functional Encryption

In this section, we define the notion of delegated registered functional encryption in both full-fledged and slotted version. Analogous to that in Reg-FE and Reg-ABE, slotted delegated Reg-ABE is the core building block underlying our constructions for concrete functionality in the following context. And we present the generic transformation from slotted delegated Reg-FE to delegated Reg-FE in Section 10.

4.1 Definition of Delegated Reg-FE

Algorithms. A *delegated registered functional encryption* for functionalities $G : X \to Y$ and $F : Y \to Z$ consists of seven algorithms:

- $\mathsf{Setup}(1^\lambda, 1^L, F, G) \to \mathsf{crs}$: It takes as input security parameter 1^λ, maximum number of clients 1^L, functionality F, G, outputs a common reference string crs.
- $\mathsf{Gen}(\mathsf{crs}, \mathsf{aux}) \to (\mathsf{mpk}, \mathsf{msk})$: It takes as input crs and state aux, outputs master key pair $(\mathsf{mpk}, \mathsf{msk})$.
- $\mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}, g) \to (\mathsf{mpk}_+, \mathsf{aux}')$: It takes as input crs, aux, and mpk along with function $g \in G$, outputs a global 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.
- $\mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}) \to \mathsf{hsk}$: It takes as input crs, aux, mpk, outputs a helper key hsk.
- $\mathsf{Key}(\mathsf{msk}, \mathsf{hsk}, \mathsf{aux}, f) \to \mathsf{sk}_f$: It takes as input the delegated client's msk, corresponding hsk, state aux and a function $f \in F$, outputs a secret key sk_f.
- $\mathsf{Dec}(\mathsf{sk}_f, \mathsf{hsk}, \mathsf{ct}) \to z/\perp/\mathtt{getupd}$: It takes as input sk_f, hsk, ct and outputs $z \in Z$ or a special symbol $\perp$ to indicate a decryption failure, or a special flag `getupd` to indicate the need of an updated helper key and secret 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 $L \in \mathbb{N}$, the following advantage function is negligible in λ:

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

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

- $\mathsf{ORegNT}(\mathsf{mpk}, g)$: run $(\mathsf{mpk}_+, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}, g)$, update $\mathsf{aux} = \mathsf{aux}'$, append $(\mathsf{mpk}_+, \mathsf{aux})$ to $\mathcal{R}$ and return $(|\mathcal{R}|, \mathsf{mpk}_+, \mathsf{aux})$;
- $\mathsf{ORegT}(g^*)$: run $(\mathsf{mpk}^*, \mathsf{msk}^*) \leftarrow \mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$, $(\mathsf{mpk}_+, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}^*, g^*)$, update $\mathsf{aux} = \mathsf{aux}'$, compute $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}^*)$, append $(\mathsf{mpk}_+, \mathsf{aux})$ to $\mathcal{R}$, return $(t = |\mathcal{R}|, \mathsf{mpk}_+, \mathsf{aux}, \mathsf{mpk}^*, \mathsf{hsk}^*)$;
- $\mathsf{OKeyT}(f^*)$: run $\mathsf{sk}^* \leftarrow \mathsf{Key}(\mathsf{msk}^*, \mathsf{hsk}^*, f^*)$ and return sk^*;
- $\mathsf{OEnc}(i, x)$: 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 $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}^*)$ and $\mathsf{sk}^* \leftarrow \mathsf{Key}(\mathsf{msk}^*, \mathsf{hsk}^*, f^*)$, recompute $z_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$. Set $b = 1$ when $z_j \neq f^* \circ g^*(x_j)$.

with the following restrictions:

- there are at most $L - 1$ queries to ORegNT and there is exactly one query to ORegT and OKeyT; therefore, we will consider $g^*, f^*, \mathsf{mpk}^*, \mathsf{msk}^*, \mathsf{hsk}^*, \mathsf{sk}^*$ 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 functionalities G, 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 indistinguishability-based security requires the advantage function $\mathsf{Adv}^{\text{Del-Reg-FE}}_{\mathcal{A}}(\lambda)$ defined as follows is negligible in λ:

$$\Pr\left[b = b' \middle| \begin{array}{l} \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F, G); \\ x_0^*, x_1^* \leftarrow \mathcal{A}^{\mathsf{ORegCC}(\cdot,\cdot),\mathsf{ORegHC}(\cdot),\mathsf{OCorHC}(\cdot),\mathsf{OCorK}(\cdot,\cdot)}(\mathsf{crs}); \\ b \leftarrow \{0,1\}, \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}_+, x_b^*), b' \leftarrow \mathcal{A}^{\mathsf{OCorK}(\cdot,\cdot)}(\mathsf{ct}^*) \end{array}\right] - 1/2,$$

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

- $\mathsf{ORegCC}(\mathsf{mpk}, g)$: run $(\mathsf{mpk}'_+, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}, g)$, update $\mathsf{mpk}_+ = \mathsf{mpk}'_+$, $\mathsf{aux} = \mathsf{aux}'$, $\mathcal{D}[\mathsf{mpk}] = \mathcal{D}[\mathsf{mpk}] \cup \{g\}$, append mpk to $\mathcal{C}$ and return $(\mathsf{mpk}_+, \mathsf{aux})$;
- $\mathsf{ORegHC}(g)$: run $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$ and $(\mathsf{mpk}'_+, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}, g)$, update $\mathsf{mpk}_+ = \mathsf{mpk}'_+$, $\mathsf{aux} = \mathsf{aux}'$, $\mathcal{D}[\mathsf{mpk}] = \mathcal{D}[\mathsf{mpk}] \cup \{g\}$, append $(\mathsf{mpk}, \mathsf{msk})$ to $\mathcal{H}$ and return $(|\mathcal{H}|, \mathsf{mpk}_+, \mathsf{aux}, \mathsf{mpk})$;
- $\mathsf{OCorHC}(i)$: let $\mathcal{H}[i] = (\mathsf{mpk}, \mathsf{msk})$, append mpk to $\mathcal{C}$ and return msk;
- $\mathsf{OCorK}(i, f)$: let $\mathcal{H}[i] = (\mathsf{mpk}, \mathsf{msk})$, compute $\mathsf{hsk} \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk})$, $\mathsf{sk} \leftarrow \mathsf{Key}(\mathsf{msk}, \mathsf{hsk}, f)$ and return sk;

with the following restrictions:

- for query i to OCorHC, it holds that $\mathcal{H}[i] \neq \perp$;
- for all $g \in \bigcup_{\mathsf{mpk} \in \mathcal{C}} \mathcal{D}[\mathsf{mpk}]$, it holds that $g(x_0^*) = g(x_1^*)$.
- for query (i, f) to OCorK, it holds that $\mathcal{H}[i] = (\mathsf{mpk}_i, \star) \neq \perp$, and for $g \in \mathcal{D}[\mathsf{mpk}_i]$, it hold that $f \circ g(x_0^*) = f \circ g(x_1^*)$.

Some Weaker Definitions. Compared with the current definition, we can consider the definition is weakened in the following aspects:

- *Function-Dependent Generation:* In the original definition, the Gen algorithm is independent of the function. While in a weaker definition, one can consider the function g is specified at generation time rather than registration time. Namely, the Gen takes g as input and outputs $(\mathsf{mpk}_g, \mathsf{msk}_g)$ that are tied with the function. In addition, Reg takes mpk_g as input rather than mpk, g in the original version. Similar to the discussion of "Policy-Dependent Key Generation" in [CHW25], "Function-Dependent Generation" can also be viewed as a minor restriction.
- *Semi-Adaptive Security:* The definition of semi-adaptive security is analogous to the above definition, except that the $\mathcal{A}$ claims the challenge x_0^*, x_1^* after seeing the crs before making any query.
- *Security without Malicious Registration:* The definition of security without malicious registration is analogous to the current definition, except that the query to oracle ORegCC is not allowed.

4.2 Definition of Slotted Delegated Reg-FE

Algorithms. A *slotted delegated registered functional encryption* for functionalities $G : X \to Y$ and $F : Y \to Z$ consists of seven algorithms:

- $\mathsf{Setup}(1^\lambda, 1^L, F, G) \to \mathsf{crs}$: It takes as input security parameter 1^λ, maximum number of delegated clients 1^L, functionalities F, G, outputs a common reference string crs.
- $\mathsf{Gen}(\mathsf{crs}, i) \to (\mathsf{mpk}_i, \mathsf{msk}_i)$: It takes as input crs and delegated client slot number $i \in [L]$, outputs delegated client master public/secret key pair $(\mathsf{mpk}_i, \mathsf{msk}_i)$.
- $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i) \to 0/1$: It takes as input crs, i, mpk_i and outputs a bit.
- $\mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i, g_i)_{i\in[L]}) \to (\mathsf{mpk}_+, (\mathsf{hsk}_j)_{j\in[L]})$: It takes as input crs, a series of mpk_i with $g_i \in G$ for all $i \in [L]$, output a global 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_+ and $x \in X$, outputs a ciphertext ct.
- $\mathsf{Key}(\mathsf{msk}, \mathsf{hsk}, f) \to \mathsf{sk}_f$: It takes as input msk, hsk and $f \in F$, outputs a secret key sk_f.
- $\mathsf{Dec}(\mathsf{sk}_f, \mathsf{hsk}, \mathsf{ct}) \to z/\perp$: It takes as input sk_f, 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, G, and all $i \in [L]$, we have

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

Correctness. For all $\lambda, L \in \mathbb{N}$, all F, G, all $j^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F, G)$, all $(\mathsf{mpk}_{j^*}, \mathsf{msk}_{j^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, j^*)$, all $\{\mathsf{mpk}_i\}_{i\in[L]\setminus\{j^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i) = 1$, all $x \in X$, $f \in F$ and $g_1, \ldots, g_L \in G$, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{j^*,f}, \mathsf{hsk}_{j^*}, \mathsf{ct}) = f \circ g_{j^*}(x) \,\middle|\, \begin{array}{r} (\mathsf{mpk}_+, (\mathsf{hsk}_j)_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i, g_i)_{i\in[L]}) \\ \mathsf{sk}_{j^*,f} \leftarrow \mathsf{Key}(\mathsf{msk}_{j^*}, \mathsf{hsk}_{j^*}, f) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}_+, x) \end{array}\right] = 1.$$

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

$$|\mathsf{mpk}_+| = \mathsf{poly}(\lambda, F, G, \log L) \quad \text{and} \quad |\mathsf{hsk}_i| = \mathsf{poly}(\lambda, F, G, \log L).$$

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

$$\Pr\left[b = b' \;\middle|\; \begin{array}{l} L \leftarrow \mathcal{A}(1^\lambda);\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F, G) \\ (\mathsf{mpk}_i^*, g_i^*)_{i\in[L]} \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot),\mathsf{OCor}(\cdot)}(\mathsf{crs}) \\ (\mathsf{mpk}_+^*, (\mathsf{hsk}_j^*)_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i^*, g_i^*)_{i\in[L]}) \\ x_0^*, x_1^* \leftarrow \mathcal{A}^{\mathsf{OKey}(\cdot,\cdot)}(\mathsf{mpk}_+^*, (\mathsf{hsk}_j^*)_{j\in[L]}) \\ b \leftarrow \{0,1\}, \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}_+^*, x_b^*), b' \leftarrow \mathcal{A}^{\mathsf{OKey}(\cdot,\cdot)}(\mathsf{ct}^*) \end{array}\right] - 1/2,$$

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

- $\mathsf{OGen}(i)$: run $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)$, set $\mathcal{D}_i[\mathsf{mpk}] = \mathsf{msk}$ and return mpk.
- $\mathsf{OCor}(i, \mathsf{mpk})$: return $\mathcal{D}_i[\mathsf{mpk}]$ and update $C = C \cup \{(i, \mathsf{mpk})\}$.
- $\mathsf{OKey}(i, f)$: return $\mathsf{sk}_{i,f} \leftarrow \mathsf{Key}(\mathcal{D}_i[\mathsf{mpk}_i^*], \mathsf{hsk}_i, f)$ and append f to $\mathcal{K}_i$.

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

$$\begin{aligned} \mathcal{D}_i[\mathsf{mpk}_i^*] = \perp &\implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i^*) = 1 \wedge \mathcal{K}_i = \emptyset \\ (i, \mathsf{mpk}_i^*) \in C \vee \mathcal{D}_i[\mathsf{mpk}_i^*] = \perp &\implies g_i^*(x_0^*) = g_i^*(x_1^*) \\ f \in \mathcal{K}_i &\implies f \circ g_i^*(x_0^*) = f \circ g_i^*(x_1^*) \end{aligned}$$

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 corruption-queries.

Remark 1. (IND-security with Repeated Aggregations) We also introduce a version of security model which allow $\mathcal{A}$ to repeat the procedures of submitting a set $(\mathsf{mpk}_i, g_i)_{i\in[L]}$ for aggregating and query for some sk_f. The security model is equivalent to above standard one and is beneficial for constructing the full-fledged delegated Reg-FE. In particular, the security model is defined as follows:

$$\mathsf{Adv}^{\mathsf{sDel\text{-}Reg\text{-}FE\text{-}ReAgg}}_{\mathcal{A}}(\lambda) = \Pr\left[b = b' \;\middle|\; \begin{array}{l} L \leftarrow \mathcal{A}(1^\lambda);\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, P, P') \\ \left\{\begin{array}{l} (\mathsf{mpk}_i, g_i)_{i\in[L]} \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot),\mathsf{OCor}(\cdot)}(\mathsf{crs}) \\ (\mathsf{mpk}_+, (\mathsf{hsk}_j)_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i, g_i)_{i\in[L]}) \\ \mathcal{A}^{\mathsf{OKey}(\cdot,\cdot)}(\mathsf{mpk}_+, (\mathsf{hsk}_j)_{j\in[L]}) \end{array}\right\} \\ (\mathsf{mpk}_i^*, y_i^*)_{i\in[L]} \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot),\mathsf{OCor}(\cdot)}(\mathsf{crs}) \\ (\mathsf{mpk}_+^*, (\mathsf{hsk}_j^*)_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i^*, g_i^*)_{i\in[L]}) \\ x_0^*, x_1^* \leftarrow \mathcal{A}^{\mathsf{OKey}(\cdot,\cdot)}(\mathsf{mpk}_+^*, (\mathsf{hsk}_j^*)_{j\in[L]}) \\ b \leftarrow \{0,1\}, \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}_+^*, x_b^*), b' \leftarrow \mathcal{A}^{\mathsf{OKey}(\cdot,\cdot)}(\mathsf{ct}^*) \end{array}\right] - 1/2,$$

the oracles and auxiliary states are identical to the above security model, except that the third restriction is only required for the f that queried to OKey after issue the final challenge aggregation tuples $(\mathsf{mpk}_i^*, g_i^*)_{i\in[L]}$ or after challenge. In addition, for each aggregation tuples set $S = \{(\mathsf{mpk}_i, g_i)\}_{i\in[L]}$ we require $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i) = 1$; and for the final challenge aggregation tuples set $S^* = \{(\mathsf{mpk}_i, y_i)\}_{i\in[L]}$, we require: $S \cap S^* = \emptyset$. We have the security model is equivalent to the that only allows challenge aggregation, since all additional aggregation tuples will not be aggregated into the final mpk_+^* and ct^*, we defer the detailed proof in Lemma 11. In this work, for simplicity, we will only show the slotted scheme in the security without repeated aggregation, but assume they are secure with repeated aggregation when moving to the full-fledged delegated Reg-FE.

Some Weaker Definitions. Compared with the current definition, we can consider the definition is weakened in the following aspects:

- *Function-Dependent Generation:* It's analogous to the minor restriction "Policy-Dependent Key Generation" in [CHW25]. We consider the function g is specified at generation time rather than aggregation time. Namely, the Gen algorithm (and OGen oracle) takes g_i as input, and master key pair $(\mathsf{mpk}_{i,g_i}, \mathsf{msk}_{i,g_i})$ are associated with the function. In addition Agg takes mpk_{i,g_i} for all $i \in [L]$ as input, rather than mpk_i, g_i in the original version. Slightly stronger than [CHW25], it has one more restriction here. We also require $g_i(x_0^*) = g_i(x_1^*)$ for all $(i, \mathsf{mpk}_{i,g_i}) \in C$, not only for challenged mpk^*_{i,g_i^*}
- *Semi-Adaptive Security:* The definition of semi-adaptive security is analogous to the above definition, except that the $\mathcal{A}$ claims the challenge x_0^*, x_1^* after seeing the crs before making any query.
- *Security without Malicious Slot:* The definition of security without malicious slot is analogous to the current definition, except that all mpk_i^* issued by $\mathcal{A}$ is generated by $\mathsf{OGen}(i)$. Namely, we require $\mathcal{D}_i[\mathsf{mpk}_i^*] \neq \bot$ for all $i \in [L]$. (We have the same restriction on mpk_i in the security model in Remark 1.)

5 Slotted Delegated Reg-ABE from Pairings

In this section, we present the construction of slotted delegated Reg-ABE for predicates, which is covered by the notion of slotted delegated Reg-FE. In particular, a (slotted) delegated Reg-ABE for predicates $P : X \times Y \to \{0,1\}$, $P' : X' \times Y' \to \{0,1\}$ and message space $\mathcal{M}$, can be seen as a (slotted) delegated Reg-FE for the following induced functionalities:

$$G_P : X \times X' \times \mathcal{M} \to X' \times (\mathcal{M} \cup \{\bot\}) \quad \text{and} \quad F_{P'} : X' \times (\mathcal{M} \cup \{\bot\}) \to (\mathcal{M} \cup \{\bot\})$$

where for all $g_y \in G_p$ and $f_{y'} \in F_{P'}$, we have

$$g_y(x, x', \mathsf{m}) = \begin{cases} (x', \mathsf{m}) & \text{if } P(x,y) = 1 \\ (x', \bot) & \text{if } P(x,y) = 0 \end{cases} \quad \text{and} \quad f_{y'}(x', \mathsf{m}) = \begin{cases} \mathsf{m} & \text{if } P'(x', y') = 1 \\ \bot & \text{if } P'(x', y') = 0 \end{cases}$$

And we recall in this section:

- for correctness, we consider

$$f_{y'} \circ g_y(x, x', \mathsf{m}) = \mathsf{m} \quad \text{when} \quad P(x,y) = 1 \wedge P'(x', y') = 1;$$

- for security, we consider the challenge as $(x^*, x'^*, \mathsf{m}_b^*)$ for $b \in \{0,1\}$, and consider the requirements as

$$g_y(x^*, x'^*, \mathsf{m}_0^*) = g_y(x^*, x'^*, \mathsf{m}_1^*) \implies P(x^*, y) = 0$$
$$f_{y'} \circ g_y(x^*, x'^*, \mathsf{m}_0^*) = f_{y'} \circ g_y(x^*, x'^*, \mathsf{m}_1^*) \implies P(x^*, y) = 0 \vee P'(x'^*, y') = 0$$

Our construction is based on predicate encodings (c.f. Section 3.2) and achieves the IND-security under MDDH assumption. By the Remark 1 and generic transformation in Section 10, this yields a full-fledged Reg-ABE (Reg-FE for above induced functionalities) via predicate encodings under MDDH assumption.

5.1 Scheme

Assuming QA-NIZKs $\Pi_1 = (\mathsf{LGen}_1, \mathsf{LPrv}_1, \mathsf{LVer}_1, \mathsf{LSim}_1)$ for $\mathbb{G}_1$-linear space and $\Pi_2 = (\mathsf{LGen}_2, \mathsf{LPrv}_2, \mathsf{LVer}_2, \mathsf{LSim}_2)$ for $\mathbb{G}_2$-linear space over bilinear groups(c.f. Section 3.3), our slotted delegated Reg-ABE scheme in prime-order bilinear groups works as follows:

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

$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(3k+1)\times k},\ \mathbf{K} \leftarrow \mathbb{Z}_p^{(k+1)\times k}.$$

Compute parameter (n, n_c, n_k) from P and parameter (n', n'_c, n'_k) from P', see Section 3.2. For all $i \in [L]$, sample

$$\mathbf{V}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(3k+1)},\ \mathbf{W}_{0,i} \leftarrow \mathbb{Z}_p^{(k+1)\times(3k+1)n},\ \mathbf{G}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)},\ \mathbf{R}_i \leftarrow \mathbb{Z}_p^{k\times k}.$$

For all $i \in [L]$, write $\mathbf{A}_i = \begin{pmatrix}\mathbf{A}\\ \mathbf{G}_i\end{pmatrix} \in \mathbb{Z}_p^{(2k+2)\times(k+1)}$ and run

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

For all $j \in [L]$ and $i \in [L] \setminus \{j\}$, sample

$$\mathbf{G}_{i,j} \leftarrow \mathbb{Z}_p^{(3k+1)\times(4k+1)}$$

write $\mathbf{B}_{i,j} = (\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,j}) \in \mathbb{Z}_p^{(3k+1)n'\times(5k+1)n'}$ and run

$$(\mathsf{crs}_{i,j}, \mathsf{td}_{i,j}) \leftarrow \mathsf{LGen}_2(1^\lambda, \mathbb{G}_2, [\mathbf{B}_{i,j}]_2)$$

Output

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}]_1,\ [\mathbf{A}\mathbf{K}]_T,\ \{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{A}\mathbf{V}_i, \mathbf{A}\mathbf{W}_{0,i}]_1\}_{i\in[L]} \\ \{[\mathbf{B}\mathbf{R}_j, \mathbf{V}_j\mathbf{B}\mathbf{R}_j + \mathbf{K}]_2\}_{j\in[L]} \\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{V}_i\mathbf{B}\mathbf{R}_j, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{R}_j)]_2\}_{j\in[L],i\in[L]\setminus\{j\}} \end{pmatrix}.$$

Notice that we do not use $\{\mathsf{td}_i\}_{i\in[L]}$ and $\{\mathsf{td}_{i,j}\}_{j\in[L],i\in[L]\setminus\{j\}}$ in the actual scheme.

– $\mathsf{Gen}(\mathsf{crs}, i)$: Sample $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(3k+1)}$ and $\mathbf{W}_{1,i} \leftarrow \mathbb{Z}_p^{(k+1)\times(3k+1)n'}$. Define

$$\mathbf{F}_i = \begin{pmatrix}(\mathbf{T}_{0,i}\|\mathbf{T}_{1,i})\\ (\mathbf{Q}_{0,i}\|\mathbf{Q}_{1,i})\end{pmatrix} = \begin{pmatrix}\mathbf{A}(\mathbf{U}_i\|\mathbf{W}_{1,i})\\ \mathbf{G}_i(\mathbf{U}_i\|\mathbf{W}_{1,i})\end{pmatrix} = \mathbf{A}_i(\mathbf{U}_i\|\mathbf{W}_{1,i}) \in \mathbb{Z}_p^{(2k+2)\times(3k+1)(n'+1)}$$

and run

$$\pi_i \leftarrow \mathsf{LPrv}_1(\mathsf{crs}_i, [\mathbf{F}_i]_1, (\mathbf{U}_i\|\mathbf{W}_{1,i})).$$

For all $j \in [L] \setminus \{i\}$, define

$$\mathbf{F}_{i,j} = (\mathbf{H}_{1,i,j}\|\mathbf{P}_{i,j}) = \big(\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j)\|\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})\big) = \mathbf{W}_{1,i}\mathbf{B}_{i,j} \in \mathbb{Z}_p^{(k+1)\times(5k+1)n'}$$

and run

$$\pi_{i,j} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,j}, [\mathbf{F}_{i,j}]_2, \mathbf{W}_{1,i}).$$

Output

$$\mathsf{mpk}_i = \begin{pmatrix} [\overbrace{\mathbf{A}\mathbf{U}_i}^{\mathbf{T}_{0,i}}, \overbrace{\mathbf{A}\mathbf{W}_{1,i}}^{\mathbf{T}_{1,i}}, \overbrace{\mathbf{G}_i\mathbf{U}_i}^{\mathbf{Q}_{0,i}}, \overbrace{\mathbf{G}_i\mathbf{W}_{1,i}}^{\mathbf{Q}_{1,i}}]_1, \pi_i \\ \{[\underbrace{\mathbf{U}_i\mathbf{B}\mathbf{R}_j}_{\mathbf{H}_{0,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j)}_{\mathbf{H}_{1,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})}_{\mathbf{P}_{i,j}}]_2, \pi_{i,j}\}_{j\in[L]\setminus\{i\}} \end{pmatrix} \quad \text{and} \quad \mathsf{msk}_i = (\mathbf{U}_i, \mathbf{W}_{1,i}).$$

– $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i)$: Parse $\mathsf{mpk}_i = \begin{pmatrix} [\mathbf{T}_{0,i}, \mathbf{T}_{1,i}, \mathbf{Q}_{0,i}, \mathbf{Q}_{1,i}]_1, \pi_i, \\ \{[\mathbf{H}_{0,i,j}, \mathbf{H}_{1,i,j}, \mathbf{P}_{i,j}]_2, \pi_{i,j}\}_{j\in[L]\setminus\{i\}} \end{pmatrix}$. Write $\mathbf{F}_i = \begin{pmatrix}(\mathbf{T}_{0,i}\|\mathbf{T}_{1,i})\\ (\mathbf{Q}_{0,i}\|\mathbf{Q}_{1,i})\end{pmatrix}$ and check

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

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

$$e([\mathbf{A}]_1, [\mathbf{H}_{0,i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_{0,i}]_1, [\mathbf{BR}_j]_2)$$
$$e([\mathbf{A}]_1, [\mathbf{H}_{1,i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_{1,i}]_1, [\mathbf{I}_{n'} \otimes \mathbf{BR}_j]_2),$$

write $\mathbf{F}_{i,j} = (\mathbf{H}_{1,i,j} \| \mathbf{P}_{i,j})$ and check

$$\mathsf{LVer}_2(\mathsf{crs}_{i,j}, [\mathbf{F}_{i,j}]_2, \pi_{i,j}) \stackrel{?}{=} 1$$

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

– $\mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i, y_i)_{i\in[L]})$: For all $i \in [L]$, compute $\mathbf{a}_{y_i}, \mathbf{K}_{y_i}$ from y_i, and fetch $[\mathbf{T}_{0,i}, \mathbf{T}_{1,i}]_1, \{[\mathbf{H}_{0,i,j}, \mathbf{H}_{1,i,j}]_2\}_{j\in[L]\setminus\{i\}}$ from mpk_i. Output:

$$\mathsf{mpk}_+ = \left(\left[\mathbf{A}, \sum_{i\in[L]} ((\mathbf{AV}_i + \mathbf{T}_{0,i})(\mathbf{a}_{y_i} \otimes \mathbf{I}_{3k+1}) + \mathbf{AW}_{0,i}(\mathbf{K}_{y_i} \otimes \mathbf{I}_{3k+1})), \sum_{i\in[L]} \mathbf{AW}_{0,i}, \sum_{i\in[L]} \mathbf{T}_{1,i}\right]_1, [\mathbf{AK}]_T\right)$$

and for all $j \in [L]$

$$\mathsf{hsk}_j = \left(\begin{bmatrix} \overbrace{\mathbf{BR}_j}^{\mathbf{K}_{j,0}}, \overbrace{\sum_{i\in[L]\setminus\{j\}} \mathbf{H}_{1,i,j}}^{\mathbf{K}_{j,1}}, \overbrace{\sum_{i\in[L]\setminus\{j\}} \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_j)}^{\mathbf{K}_{j,2}}, \overbrace{\mathbf{V}_j\mathbf{BR}_j + \mathbf{K}}^{\mathbf{K}_{j,3}} \end{bmatrix}_2, \underbrace{\left[\sum_{i\in[L]\setminus\{j\}} ((\mathbf{V}_i\mathbf{BR}_j + \mathbf{H}_{0,i,j})(\mathbf{a}_{y_i} \otimes \mathbf{I}_k) + \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_j)(\mathbf{K}_{y_i} \otimes \mathbf{I}_k))\right]_2}_{\mathbf{K}_{j,4}}\right).$$

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

$$\mathsf{ct}_{x,x'} = \left(\begin{bmatrix} \overbrace{\mathbf{sA}}^{\mathbf{c}_0}, \overbrace{\sum_{i\in[L]} ((\mathbf{sAV}_i + \mathbf{sT}_{0,i})(\mathbf{a}_{y_i} \otimes \mathbf{I}_{3k+1}) + \mathbf{sAW}_{0,i}(\mathbf{K}_{y_i} \otimes \mathbf{I}_{3k+1}))}^{\mathbf{c}_1} \end{bmatrix}_1, \begin{bmatrix} \underbrace{\sum_{i\in[L]} \mathbf{sAW}_{0,i}(\mathbf{C}_x \otimes \mathbf{I}_{3k+1})}_{\mathbf{c}_2}, \underbrace{\sum_{i\in[L]} \mathbf{sT}_{1,i}(\mathbf{C}'_{x'} \otimes \mathbf{I}_{3k+1})}_{\mathbf{c}_3} \end{bmatrix}_1, \underbrace{[\mathbf{sAKe}_1^\top]_T \cdot \mathsf{m}}_{C}\right).$$

– $\mathsf{Key}(\mathsf{msk}_{j^*}, \mathsf{hsk}_{j^*}, y')$: Compute $\mathbf{a}'_{y'}, \mathbf{K}'_{y'}$ from y' and parse $\mathsf{msk}_{j^*} = (\mathbf{U}_{j^*}, \mathbf{W}_{1,j^*})$. Sample $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times k}$ and output:

$$\mathsf{sk}_{j^*,y'} = \left(\left[\underbrace{\mathbf{BR}_{j^*}\mathbf{R}}_{\mathbf{K}_0}, \underbrace{\sum_{i\in[L]\setminus\{j^*\}} \mathbf{H}_{1,i,j}(\mathbf{I}_{n'} \otimes \mathbf{R})}_{\mathbf{K}_1}, \underbrace{\mathbf{U}_{j^*}\mathbf{BR}_{j^*}(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}_{1,j^*}(\mathbf{I}_{n'} \otimes \mathbf{BR}_{j^*}\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)}_{\mathbf{K}_2}\right]_2\right).$$

– $\mathsf{Dec}(\mathsf{sk}_{j^*,y'}, \mathsf{hsk}_{j^*}, \mathsf{ct}_{x,x'})$: Parse

$$\mathsf{sk}_{j^*,y'} = ([\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2]_2), \quad \mathsf{hsk}_{j^*} = ([\mathbf{K}_{j^*,0}, \mathbf{K}_{j^*,1}, \mathbf{K}_{j^*,2}, \mathbf{K}_{j^*,3}, \mathbf{K}_{j^*,4}]_2), \quad \mathsf{ct} = ([\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3]_1, C).$$

Recover

$$[\mathbf{z}_1]_T = e([\mathbf{c}_1 \| \mathbf{c}_2]_1, [\mathbf{I}_{n_k+n_c} \otimes \mathbf{K}_{j^*,0}]_2), \quad [\mathbf{z}_2]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_{j^*,4} \| \mathbf{K}_{j^*,2}(\mathbf{C}_x \otimes \mathbf{I}_k)]_2);$$
$$[\mathbf{z}_3]_T = e([\mathbf{c}_3]_1, [\mathbf{I}_{n'_c} \otimes \mathbf{K}_0]_2), \quad [\mathbf{z}_4]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_1(\mathbf{C}'_{x'} \otimes \mathbf{I}_k)]_2);$$
$$[\mathbf{z}_5]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_2]_2), \quad [\mathbf{z}_6]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_{j^*,3}]_2).$$

Compute $\mathbf{d}_{x,y_{j^*}}$ from x and y_{j^*}, $\mathbf{d}_{x',y'}$ from x' and y', recover

$$[\mathbf{z}]_T = [(\mathbf{z}_1 - \mathbf{z}_2)(\mathbf{d}_{x,y_{j^*}}^\top \otimes \mathbf{I}_k) - (\mathbf{z}_5 \| (\mathbf{z}_3 - \mathbf{z}_4))(\mathbf{d}'^{\top}_{x',y'} \otimes \mathbf{I}_k) - \mathbf{z}_6]_T$$

Output

$$z = [\mathbf{ze}_1^\top]_T \cdot C$$

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

$$\mathsf{mpk}_i = \left(\begin{array}{l} [\overbrace{\mathbf{AU}_i}^{\mathbf{T}_{0,i}}, \overbrace{\mathbf{AW}_{1,i}}^{\mathbf{T}_{1,i}}, \overbrace{\mathbf{G}_i\mathbf{U}_i}^{\mathbf{Q}_{0,i}}, \overbrace{\mathbf{G}_i\mathbf{W}_{1,i}}^{\mathbf{Q}_{1,i}}]_1, \pi_i \\ \{[\underbrace{\mathbf{U}_i\mathbf{BR}_j}_{\mathbf{H}_{0,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j)}_{\mathbf{H}_{1,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})}_{\mathbf{P}_{i,j}}]_2, \pi_{i,j}\}_{j \in [L] \setminus \{i\}} \end{array} \right)$$

for some $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(3k+1)}$, $\mathbf{W}_{1,i} \leftarrow \mathbb{Z}_p^{(k+1)\times(3k+1)n'}$, and

- $\pi_i \leftarrow \mathsf{LPrv}_1(\mathsf{crs}_i, [\mathbf{A}_i(\mathbf{U}_i \| \mathbf{W}_{1,i})]_1, (\mathbf{U}_i \| \mathbf{W}_{1,i}))$, where $(\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$ and $\mathbf{A}_i = \begin{pmatrix} \mathbf{A} \\ \mathbf{G}_i \end{pmatrix}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{G}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$;
- for all $j \in [L] \setminus \{i\}$, $\pi_{i,j} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,j}, [\mathbf{W}_{1,i}\mathbf{B}_{i,j}]_2, \mathbf{W}_{1,i})$, where $(\mathsf{crs}_{i,j}, \mathsf{td}_{i,j}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_2, [\mathbf{B}_{i,j}]_2)$ and $\mathbf{B}_{i,j} = (\mathbf{I}_{n'} \otimes \mathbf{BR}_j \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})$ with $\mathbf{B} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$, $\mathbf{R}_j \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{G}_{i,j} \leftarrow \mathbb{Z}_p^{(3k+1)\times(4k+1)}$.

Then:

- Write $\mathbf{F}_i = \begin{pmatrix} (\mathbf{T}_{0,i} \| \mathbf{T}_{1,i}) \\ (\mathbf{Q}_{0,i} \| \mathbf{Q}_{1,i}) \end{pmatrix} = \begin{pmatrix} \mathbf{A}(\mathbf{U}_i \| \mathbf{W}_{1,i}) \\ \mathbf{G}_i(\mathbf{U}_i \| \mathbf{W}_{1,i}) \end{pmatrix}$, we have $\mathsf{LVer}_1(\mathsf{crs}_i, [\mathbf{F}_i]_1, \pi_i) = 1$ by the perfect completeness of Π_1 (see Section 3.3) and the fact that $\mathbf{F}_i = \mathbf{A}_i(\mathbf{U}_i \| \mathbf{W}_{1,i})$;
- For each $j \in [L] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_i\mathbf{BR}_j]_2) = e([\mathbf{AU}_i]_1, [\mathbf{BR}_j]_2)$ by the definition of bilinear map e (see Section 3.1) and the fact that $\mathbf{A} \cdot \mathbf{U}_i\mathbf{BR}_j = \mathbf{AU}_i \cdot \mathbf{BR}_j$.
- For each $j \in [L] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j)]_2) = e([\mathbf{AW}_{1,i}]_1, [\mathbf{I}_{n'} \otimes \mathbf{BR}_j]_2)$ by the definition of bilinear map e (see Section 3.1) and the fact that $\mathbf{A} \cdot \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j) = \mathbf{AW}_{1,i} \cdot (\mathbf{I}_{n'} \otimes \mathbf{BR}_j)$.
- For each $j \in [L] \setminus \{i\}$, write $\mathbf{F}_{i,j} = (\mathbf{H}_{1,i,j} \| \mathbf{P}_{i,j}) = \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})$, we have $\mathsf{LPrv}_2(\mathsf{crs}_{i,j}, [\mathbf{F}_{i,j}]_2, \pi_{i,j}) = 1$ by the perfect completeness of Π_2 (see Section 3.3) and the fact that $\mathbf{F}_{i,j} = \mathbf{W}_{1,i}\mathbf{B}_{i,j}$.

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

Correctness. For all $\lambda, L \in \mathbb{N}$, all P and P', all $j^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, P, P', 1^L)$, all $(\mathsf{mpk}_{j^*}, \mathsf{msk}_{j^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, j^*)$, all $\{\mathsf{mpk}_i\}_{i \in [L] \setminus \{j^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i) = 1$, for all $y_1, \ldots, y_L \in Y$, $x \in X$ such that $P(x, y_{j^*}) = 1$, all $y' \in Y'$, $x' \in X'$ such that $P'(x', y') = 1$ and all m, we have:

$$\mathsf{sk}_{j^*,y'} = \left(\left[\underbrace{\mathbf{BR}_{j^*}\mathbf{R}}_{\mathbf{K}_0}, \underbrace{\sum_{i \in [L] \setminus \{j^*\}} \mathbf{H}_{1,i,j^*}(\mathbf{I}_{n'} \otimes \mathbf{R})}_{\mathbf{K}_1}, \underbrace{\mathbf{U}_{j^*}\mathbf{BR}_{j^*}(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}_{1,j^*}(\mathbf{I}_{n'} \otimes \mathbf{BR}_{j^*}\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)}_{\mathbf{K}_2} \right]_2 \right),$$

$$\mathsf{hsk}_{j^*} = \left(\begin{array}{l} \left[\overbrace{\mathbf{BR}_j}^{\mathbf{K}_{j^*,0}}, \overbrace{\sum_{i \in [L] \setminus \{j^*\}} \mathbf{H}_{1,i,j^*}}^{\mathbf{K}_{j^*,1}}, \overbrace{\sum_{i \in [L] \setminus \{j^*\}} \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_{j^*})}^{\mathbf{K}_{j^*,2}}, \overbrace{\mathbf{V}_{j^*}\mathbf{BR}_{j^*} + \mathbf{K}}^{\mathbf{K}_{j^*,3}} \right]_2, \\ \underbrace{\left[\sum_{i \in [L] \setminus \{j^*\}} ((\mathbf{V}_i\mathbf{BR}_{j^*} + \mathbf{H}_{0,i,j^*})(\mathbf{a}_{y_i} \otimes \mathbf{I}_k) + \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_{j^*})(\mathbf{K}_{y_i} \otimes \mathbf{I}_k)) \right]_2}_{\mathbf{K}_{j^*,4}} \end{array} \right),$$

$$\mathsf{ct}_{x,x'} = \left(\begin{array}{l} \left[\overbrace{\mathbf{sA}}^{\mathbf{c}_0}, \overbrace{\sum_{i \in [L]} ((\mathbf{sAV}_i + \mathbf{sT}_{0,i})(\mathbf{a}_{y_i} \otimes \mathbf{I}_{3k+1}) + \mathbf{sAW}_{0,i}(\mathbf{K}_{y_i} \otimes \mathbf{I}_{3k+1}))}^{\mathbf{c}_1} \right]_1, \\ \left[\underbrace{\sum_{i \in [L]} \mathbf{sAW}_{0,i}(\mathbf{C}_x \otimes \mathbf{I}_{3k+1})}_{\mathbf{c}_2}, \underbrace{\sum_{i \in [L]} \mathbf{sT}_{1,i}(\mathbf{C}'_{x'} \otimes \mathbf{I}_{3k+1})}_{\mathbf{c}_3} \right]_1, \underbrace{[\mathbf{sAKe}_1^\top]_T \cdot \mathsf{m}}_{c} \end{array} \right).$$

where

$$\mathbf{AH}_{0,i,j^*} = \mathbf{T}_{0,i}\mathbf{BR}_{j^*}, \quad \mathbf{AH}_{1,i,j^*} = \mathbf{T}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j) \quad \forall i \in [L] \setminus \{j^*\};$$
$$\mathbf{T}_{0,j^*} = \mathbf{AU}_{j^*}, \qquad \mathbf{T}_{1,j^*} = \mathbf{AW}_{1,j^*}.$$

Note that in Key and Dec, we actually consider hsk_j for $j = j^*$ and msk_i for $i = j^*$; and all above equalities are ensured by Ver, Gen and Key. Then, as in Section 3.2, let

$$\mathbf{M}_{x,y_i} = \begin{pmatrix} \mathbf{a}_{y_i} & \mathbf{0}_{n_c} \\ \mathbf{K}_{y_i} & \mathbf{C}_x \end{pmatrix}, \quad \forall i \in [L] \quad \text{and} \quad \mathbf{M}'_{x',y'} = \begin{pmatrix} \mathbf{a}'_{y'} & \mathbf{0}_{n'_c} \\ \mathbf{K}'_{y'} & \mathbf{C}'_{x'} \end{pmatrix}$$

we have

$$\begin{aligned}
\mathbf{z}_1 &= \sum_{i\in[L]} (\mathbf{sAV}_i + \mathbf{sT}_{0,i} \| \mathbf{sAW}_{0,i})(\mathbf{M}_{x,y_i} \otimes \mathbf{I}_{3k+1})(\mathbf{I}_{n_k+n_c} \otimes \mathbf{BR}_{j^*}) \\
&= \sum_{i\in[L]} (\mathbf{sAV}_i + \mathbf{sT}_{0,i} \| \mathbf{sAW}_{0,i})(\mathbf{I}_{1+n} \otimes \mathbf{BR}_{j^*})(\mathbf{M}_{x,y_i} \otimes \mathbf{I}_k) \qquad (11) \\
&= \sum_{i\in[L]} (\mathbf{sAV}_i\mathbf{BR}_{j^*} + \mathbf{sT}_{0,i}\mathbf{BR}_{j^*} \| \mathbf{sAW}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_{j^*}))(\mathbf{M}_{x,y_i} \otimes \mathbf{I}_k) \\
\mathbf{z}_2 &= \sum_{i\in[L]\setminus\{j^*\}} (\mathbf{sAV}_i\mathbf{BR}_{j^*} + \mathbf{sAH}_{0,i,j^*} \| \mathbf{sAW}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_{j^*}))(\mathbf{M}_{x,y_i} \otimes \mathbf{I}_k) \\
\mathbf{z}_3 &= \sum_{i\in[L]} \mathbf{sT}_{1,i}(\mathbf{C}'_{x'} \otimes \mathbf{I}_{3k+1})(\mathbf{I}_{n'_c} \otimes \mathbf{BR}_{j^*}\mathbf{R}) \\
&= \sum_{i\in[L]} \mathbf{sT}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_{j^*}\mathbf{R})(\mathbf{C}'_{x'} \otimes \mathbf{I}_k) \qquad (12) \\
\mathbf{z}_4 &= \sum_{i\in[L]\setminus\{j^*\}} \mathbf{sAH}_{1,i,j^*}(\mathbf{I}_{n'} \otimes \mathbf{R})(\mathbf{C}'_{x'} \otimes \mathbf{I}_k) \\
\mathbf{z}_5 &= \mathbf{sAU}_{j^*}\mathbf{BR}_{j^*}(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{sAW}_{1,j^*}(\mathbf{I}_{n'} \otimes \mathbf{BR}_{j^*}\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k) \\
\mathbf{z}_6 &= \mathbf{sAV}_{j^*}\mathbf{BR}_{j^*} + \mathbf{sAK}
\end{aligned}$$

and then

$$\begin{aligned}
[\mathbf{z}]_T &= [(\mathbf{z}_1 - \mathbf{z}_2)(\mathbf{d}^\top_{x,y_{j^*}} \otimes \mathbf{I}_k) - (\mathbf{z}_5 \| (\mathbf{z}_3 - \mathbf{z}_4))(\mathbf{d}'^{\top}_{x',y'} \otimes \mathbf{I}_k) - \mathbf{z}_6]_T \\
&= [(\mathbf{sAV}_{j^*}\mathbf{BR}_{j^*} + \mathbf{sAU}_{j^*}\mathbf{BR}_{j^*} \| \mathbf{sAW}_{0,i^*}(\mathbf{I}_n \otimes \mathbf{BR}_{j^*}))(\mathbf{M}_{x,y_{j^*}} \otimes \mathbf{I}_k)(\mathbf{d}^\top_{x,y_{j^*}} \otimes \mathbf{I}_k) \\
&\quad -(\mathbf{sAU}_{j^*}\mathbf{BR}_{j^*} \| \mathbf{sAW}_{1,j^*}(\mathbf{I}_{n'} \otimes \mathbf{BR}_{j^*}\mathbf{R}))(\mathbf{M}'_{x',y'} \otimes \mathbf{I}_k)(\mathbf{d}'^{\top}_{x',y'} \otimes \mathbf{I}_k) \\
&\quad -(\mathbf{sAV}_{j^*}\mathbf{BR}_{j^*} + \mathbf{sAK})]_T \qquad (13) \\
&= [\mathbf{sAV}_{j^*}\mathbf{BR}_{j^*} + \mathbf{sAU}_{j^*}\mathbf{BR}_{j^*} - \mathbf{sAU}_{j^*}\mathbf{BR}_{j^*} - (\mathbf{sAV}_{j^*}\mathbf{BR}_{j^*} + \mathbf{sAK})]_T \qquad (14) \\
&= [-\mathbf{sAK}]_T
\end{aligned}$$

Here, equalities (11) and (12) follows from the property of tensor product: $(\mathbf{M}_1 \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{M}_2) = \mathbf{M}_1 \otimes \mathbf{M}_2 = (\mathbf{I} \otimes \mathbf{M}_2)(\mathbf{M}_1 \otimes \mathbf{I})$ for matrices of proper size; equality (13) follows from the fact that $\mathbf{AH}_{0,i,j} = \mathbf{T}_{0,i}\mathbf{BR}_{j^*}$, $\mathbf{AH}_{1,i,j} = \mathbf{T}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_{j^*})$ for all $i \in [L] \setminus \{j^*\}$ and fact that $\mathbf{T}_{0,j^*} = \mathbf{AU}_{j^*}$, $\mathbf{T}_{1,j^*} = \mathbf{AW}_{1,j^*}$; equality (14) follows from the correctness of predicate encodings. Then, we have

$$\begin{aligned}
z &= [\mathbf{z}\mathbf{e}_1^\top]_T \cdot C \\
&= [-\mathbf{sAK}\mathbf{e}_1^\top]_T \cdot [\mathbf{sAK}\mathbf{e}_1^\top]_T \cdot \mathsf{m} \\
&= \mathsf{m}
\end{aligned}$$

This readily proves the correctness.

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

$$|\mathsf{crs}| = n \cdot L^2 \cdot \mathsf{poly}(\lambda); \quad |\mathsf{mpk}_+| = (n_k + n + n') \cdot \mathsf{poly}(\lambda); \quad |\mathsf{hsk}_j| = n_k \cdot \mathsf{poly}(\lambda);$$
$$|\mathsf{ct}| = (n_k + n_c + n'_c) \cdot \mathsf{poly}(\lambda); \quad |\mathsf{sk}| = n'_k \cdot \mathsf{poly}(\lambda).$$

Note that the total size of $\{\mathsf{crs}_i\}_{i\in[L]}$ and $\{\mathsf{crs}_{i,j}\}_{j\in[L],i\in[L]\setminus\{j\}}$ is $L^2 \cdot \mathsf{poly}(\lambda)$ 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], our slotted delegated Reg-ABE scheme uses prime-order bilinear group and the security can be reduced to MDDH assumption.

Theorem 1. *Assume $\Pi_1 = (\mathsf{LGen}_1, \mathsf{LPrv}_1, \mathsf{LVer}_1, \mathsf{LSim}_1)$, $\Pi_2 = (\mathsf{LGen}_2, \mathsf{LPrv}_2, \mathsf{LVer}_2, \mathsf{LSim}_2)$ are QA-NIZKs with perfect completeness, perfect zero-knowledge and unbounded simulation soundness respectively for $\mathbb{G}_1$-linear space and $\mathbb{G}_2$-linear space defined in Section 3.3, our slotted delegated Reg-ABE scheme achieves the adaptive IND-security defined in Section 4.1 (with the consideration we have mentioned in the beginning of this section) under MDDH assumption.*

5.2 Proof

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

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

$$\mathsf{Adv}^{\mathit{sDel\text{-}Reg\text{-}ABE}}_{\mathcal{A}}(\lambda) \le (L + 2QL^2) \cdot \mathsf{Adv}^{\mathit{USS}}_{\mathcal{B}_1}(\lambda) + (1 + 6L + 20QL) \cdot \mathsf{Adv}^{\mathit{MDDH}}_{\mathcal{B}_2}(\lambda) + \mathsf{negl}(\lambda)$$

where L is the number of slots, Q is the maximum number of queries on $\mathsf{OKey}(i,\cdot)$ for some slot i; and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2) \approx \mathsf{Time}(\mathcal{A})$.

Game Sequence. Suppose that crs is the common reference string, x^*, x'^* are the challenge "attribute", $(\mathsf{m}^*_0, \mathsf{m}^*_1)$ is the challenge pair, $\{\mathsf{mpk}^*_i, y^*_i\}_{i\in[L]}$ are challenge mater public keys along with challenge "policy" to be registered. For all $i \in [L]$, define $D_i = \{\mathsf{mpk}_i : \mathcal{D}_i[\mathsf{mpk}_i] = \mathsf{msk}_i \neq \perp\}$ as responses to $\mathsf{OGen}(i)$, $C_i = \{\mathsf{mpk}_i : (i, \mathsf{mpk}_i) \in C\}$ records master public keys in D_i that have been sent to $\mathsf{OCor}(i,\cdot)$; recall that $\mathcal{K}_i$ is the list that records the queries to $\mathsf{OKey}(i,\cdot)$. For each $i \in [L]$, we have the restrictions as follow

$$\begin{aligned} \mathsf{mpk}^*_i \notin D_i &\implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}^*_i) = 1 \wedge \mathcal{K}_i = \emptyset, \\ \mathsf{mpk}^*_i \in C_i \vee \mathsf{mpk}^*_i \notin D_i &\implies P(x^*, y^*_i) = 0, \\ y' \in \mathcal{K}_i &\implies P(x^*, y^*_i) = 0 \vee P'(x'^*, y') = 0. \end{aligned} \tag{15}$$

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

- G_0 : This is the real game, recall that we have
  - crs is in the form:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}]_1,\ [\mathbf{AK}]_T,\ \left\{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{AV}_i, \mathbf{AW}_{0,i}]_1\right\}_{i\in[L]} \\ \left\{[\mathbf{BR}_j, \mathbf{V}_j\mathbf{BR}_j + \mathbf{K}]_2\right\}_{j\in[L]} \\ \left\{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{V}_i\mathbf{BR}_j, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_j)]_2\right\}_{j\in[L],i\in[L]\setminus\{j\}} \end{pmatrix}.$$

    where $\mathsf{crs}_i \in \mathsf{LGen}_1(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$ with $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{G}_i}$, $\mathsf{crs}_{i,j} \in \mathsf{LGen}_2(1^\lambda, \mathbb{G}_2, [\mathbf{B}_{i,j}]_2)$ with $\mathbf{B}_{i,j} = \left(\mathbf{I}_{n'} \otimes \mathbf{BR}_j \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,j}\right)$.

- For each $i \in [L]$, each $\mathsf{mpk}_i \in D_i$ is in the form:

$$\mathsf{mpk}_i = \left(\begin{array}{l} [\overbrace{\mathbf{AU}_i}^{\mathbf{T}_{0,i}}, \overbrace{\mathbf{AW}_{1,i}}^{\mathbf{T}_{1,i}}, \overbrace{\mathbf{G}_i\mathbf{U}_i}^{\mathbf{Q}_{0,i}}, \overbrace{\mathbf{G}_i\mathbf{W}_{1,i}}^{\mathbf{Q}_{1,i}}]_1, \pi_i \\ \{[\underbrace{\mathbf{U}_i\mathbf{BR}_j}_{\mathbf{H}_{0,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j)}_{\mathbf{H}_{1,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})}_{\mathbf{P}_{i,j}}]_2, \pi_{i,j}\}_{j \in [L] \setminus \{i\}} \end{array} \right)$$

  where $\pi_i \leftarrow \mathsf{LPrv}_1(\mathsf{crs}_i, [\mathbf{F}_i]_1, (\mathbf{U}_i \| \mathbf{W}_{1,i}))$ with $\mathbf{F}_i = \begin{pmatrix} \mathbf{A}(\mathbf{U}_i \| \mathbf{W}_{1,i}) \\ \mathbf{G}_i(\mathbf{U}_i \| \mathbf{W}_{1,i}) \end{pmatrix}$, $\pi_{i,j} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,j}, [\mathbf{F}_{i,j}]_2, \mathbf{W}_{1,i})$ with $\mathbf{F}_{i,j} = \big(\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j) \| \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})\big)$. And $(\mathbf{U}_i, \mathbf{W}_{1,i})$ is the corresponding msk_i.
- For all $i \in [L]$, mpk_i^* is in the form:

$$\mathsf{mpk}_i^* = ([\mathbf{T}_{0,i}^*, \mathbf{T}_{1,i}^*, \mathbf{Q}_{0,i}^*, \mathbf{Q}_{1,i}^*]_1, \pi_i^*; \{[\mathbf{H}_{0,i,j}^*, \mathbf{H}_{1,i,j}^*, \mathbf{P}_{i,j}^*]_2, \pi_{i,j}^*\}_{j \in [L] \setminus \{i\}})$$

  such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i^*) = 1$ which means $\mathsf{LVer}_1\left(\mathsf{crs}_i, \begin{bmatrix} (\mathbf{T}_{0,i}^*, \mathbf{T}_{1,i}^*) \\ (\mathbf{Q}_{0,i}^*, \mathbf{Q}_{1,i}^*) \end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{AH}_{0,i,j}^* = \mathbf{T}_{0,i}^*\mathbf{BR}_j$, $\mathbf{AH}_{1,i,j}^* = \mathbf{T}_{1,i}^*(\mathbf{I}_{n'} \otimes \mathbf{BR}_j)$, $\mathsf{LVer}_2(\mathsf{crs}_{i,j}, [\mathbf{H}_{1,i,j} \| \mathbf{P}_{i,j}]_2, \pi_{i,j}^*) = 1$ for each $j \in [L] \setminus \{i\}$.
- For each $j \in [L]$ such that $\mathsf{mpk}_j^* \in D_j$, and each $y' \in \mathcal{K}_j$, secret key returned from $\mathsf{OKey}(j, y')$ is in the form:

$$\mathsf{sk}_{j,y'} = \left(\left[\underbrace{\mathbf{BR}_j\mathbf{R}}_{\mathbf{K}_0}, \underbrace{\sum_{i \in [L] \setminus \{j\}} \mathbf{H}_{1,i,j}^*(\mathbf{I}_{n'} \otimes \mathbf{R})}_{\mathbf{K}_1}, \underbrace{\mathbf{U}_j^*\mathbf{BR}_j(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}_{1,j}^*(\mathbf{I}_{n'} \otimes \mathbf{BR}_j\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)}_{\mathbf{K}_2} \right]_2 \right)$$

  where $\mathbf{R} \leftarrow \mathbb{Z}_p^{k \times k}$ is freshly sampled for each query and $(\mathbf{U}_j^*, \mathbf{W}_{1,j}^*) = \mathsf{msk}_j^* = \mathcal{D}_j[\mathsf{mpk}_j^*]$.
- ct^* for x^*, x'^* and $(\mathsf{m}_0^*, \mathsf{m}_1^*)$ is in the form:

$$\mathsf{ct}^* = \left(\begin{array}{l} \left[\overbrace{\mathbf{sA}}^{\mathbf{c}_0^*}, \overbrace{\sum_{i \in [L]} ((\mathbf{sAV}_i + \mathbf{sT}_{0,i}^*)(\mathbf{a}_{y_i^*} \otimes \mathbf{I}_{3k+1}) + \mathbf{sAW}_{0,i}(\mathbf{K}_{y_i^*} \otimes \mathbf{I}_{3k+1}))}^{\mathbf{c}_1^*} \right]_1, \\ \left[\underbrace{\sum_{i \in [L]} \mathbf{sAW}_{0,i}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1})}_{\mathbf{c}_2^*}, \underbrace{\sum_{i \in [L]} \mathbf{sT}_{1,i}^*(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1})}_{\mathbf{c}_3^*} \right]_1, \underbrace{[\mathbf{sAKe}_1^\top]_T \cdot \mathsf{m}_b^*}_{C^*} \end{array} \right).$$

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

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

$$\widetilde{\pi}_i \leftarrow \boxed{\mathsf{LSim}_1}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{F}_i]_1) \quad \text{where} \quad \mathbf{F}_i = \begin{pmatrix} \mathbf{A}(\mathbf{U}_i \| \mathbf{W}_{1,i}) \\ \mathbf{G}_i(\mathbf{U}_i \| \mathbf{W}_{1,i}) \end{pmatrix}.$$

  We have $\mathsf{G}_1 \equiv \mathsf{G}_0$. This follows from the perfect zero-knowledge of Π_1.

– 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 $\mathbf{G}_i$ in crs with

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

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

– G_3: Identical to G_2 except that we replace $\mathbf{sT}^*_{0,i}$ with $\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i}$ in $\mathbf{c}^*_1$, and replace $\mathbf{sT}^*_{1,i}$ with $\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{1,i}$ in $\mathbf{c}^*_3$; namely, we have

$$\mathbf{c}^*_1 = \textstyle\sum_{i\in[L]}((\mathbf{sAV}_i + \boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i}})(\mathbf{a}_{y^*_i}\otimes\mathbf{I}_{3k+1}) + \mathbf{sAW}_{0,i}(\mathbf{K}_{y^*_i}\otimes\mathbf{I}_{3k+1})),$$
$$\mathbf{c}^*_3 = \textstyle\sum_{i\in[L]}\boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{1,i}}(\mathbf{C}'_{x'^*}\otimes\mathbf{I}_{3k+1}).$$

We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from stronger unbounded simulation soundness of Π_1 along with the fact that $\mathsf{LVer}_1(\mathsf{crs}_i, [\mathbf{F}^*_i]_1, \pi^*_i) = 1$ for all $i \in [L]$ where $\mathbf{F}^*_i = \begin{pmatrix}(\mathbf{T}^*_{0,i}, \mathbf{T}^*_{1,i})\\(\mathbf{Q}^*_{0,i}, \mathbf{Q}^*_{1,i})\end{pmatrix}$. Assume $\mathsf{mpk}^*_{i^*} \notin D_{i^*}$, i.e., $\mathsf{mpk}^*_{i^*}$ is malicious. In the reduction, we guess $i^* \leftarrow [L]$ and obtain $\mathbf{A}, \widehat{\mathbf{G}}_{i^*}, \mathsf{crs}_{i^*}$ as input; we simulate honestly as in G_3 except that for all $\mathsf{mpk}_{i^*} \in D_{i^*}$, 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 $\mathsf{mpk}^*_{i^*} \notin D_{i^*}$. Observe that once it happens that $\mathbf{e}_1\widetilde{\mathbf{G}}_{i^*}^{-1}(\mathbf{Q}^*_{0,i^*}\|\mathbf{Q}^*_{1,i^*}) \neq \mathbf{s}(\mathbf{T}^*_{0,i^*}\|\mathbf{T}^*_{1,i^*})$, we must have $\mathbf{F}^*_{i^*} \notin \mathsf{span}^\top(\mathbf{A}_{i^*})$. When $\mathsf{mpk}^*_{i^*} \in D_{i^*}$, we always have $\mathsf{G}_3 \equiv \mathsf{G}_2$.

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

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

and generate the challenge ciphertext as follows:

$$\mathsf{ct}^* = \left(\left[\overbrace{\boxed{\mathbf{c}}}^{\mathbf{c}^*_0}, \overbrace{\textstyle\sum_{i\in[L]}((\boxed{\mathbf{c}}\mathbf{V}_i + \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i})(\mathbf{a}_{y^*_i}\otimes\mathbf{I}_{3k+1}) + \boxed{\mathbf{c}}\mathbf{W}_{0,i}(\mathbf{K}_{y^*_i}\otimes\mathbf{I}_{3k+1}))}^{\mathbf{c}^*_1}\right]_1,\right.$$
$$\left.\left[\underbrace{\textstyle\sum_{i\in[L]}\boxed{\mathbf{c}}\mathbf{W}_{0,i}(\mathbf{C}_{x^*}\otimes\mathbf{I}_{3k+1})}_{\mathbf{c}^*_2}, \underbrace{\textstyle\sum_{i\in[L]}\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{1,i}(\mathbf{C}'_{x'^*}\otimes\mathbf{I}_{3k+1})}_{\mathbf{c}^*_3}\right]_1, \underbrace{[\boxed{\mathbf{c}}\mathbf{K}\mathbf{e}_1^\top]_T\cdot\mathsf{m}^*_b}_{C^*}\right).$$

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 $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}, \mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ and $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$.

– $\mathsf{G}_{5,\ell}$, $(\ell \in [0, L])$: Identical to G_4 except we change $[\mathbf{V}_j\mathbf{BR}_j + \mathbf{K}]_2$ for all $j \in [\ell]$ as follows:

$$[\mathbf{V}_j\mathbf{BR}_j + \mathbf{K} + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{k}}}]_2$$

where $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ such that $\mathbf{cc}^\perp = 1$ and $\mathbf{Ac}^\perp = \mathbf{0}$ and $\widetilde{\mathbf{k}} \leftarrow \mathbb{Z}_p^{1\times k}$. We have that

- $\mathsf{G}_{5,0} = \mathsf{G}_4$; the two games are exactly identical, since $[0] = \emptyset$;
- $\mathsf{G}_{5,\ell} \approx_c \mathsf{G}_{5,\ell-1}$ for all $\ell \in [L]$, we will employ a sub-sequence of games for the proof described later.

– G_6: Identical to $\mathsf{G}_{5,L}$ except that we replace term C^* in ct^* as $\boxed{C^* \leftarrow \mathbb{G}_T}$. We have $\mathsf{G}_6 \equiv \mathsf{G}_{5,L}$. This follows from the following statistical argument:

$$(\overbrace{\mathbf{AK}, \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}}^{\mathsf{crs}}, \overbrace{\mathbf{cKe}^\top}^{C^*\text{ in }\mathsf{ct}^*}) \equiv (\mathbf{AK}, \mathbf{K}, \mathbf{cKe}^\top - \widetilde{\mathbf{k}}\mathbf{e}^\top)$$

when $\mathbf{K} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$ and the fact that $[\widetilde{\mathbf{k}}]_T$ only appears in C^* in right hand-side. We can prove the statement via change of variable $\mathbf{K} \mapsto \mathbf{K} - \mathbf{c}^\perp\widetilde{\mathbf{k}}$.

Observe that, in G_6, the challenge ciphertext ct^* is independent of b and the adversary's advantage is exactly 0.

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

– $\mathsf{G}_{5,\ell-1,0}$: Identical to $\mathsf{G}_{5,\ell-1}$. We recall crs, $\mathsf{mpk}_i \in D_i$ in the following form, where we highlight $\mathbf{R}_\ell$-related terms using dashed boxes which will be changed in this sub-sequence.

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}]_1, [\mathbf{AK}]_T, \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{AV}_i, \mathbf{AW}_{0,i}]_1\}_{i\in[L]} \\ \left\{[\mathbf{BR}_j, \mathbf{V}_j\mathbf{BR}_j + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2\right\}_{j\in[\ell-1]}, \boxed{[\mathbf{BR}_\ell, \mathbf{V}_\ell\mathbf{BR}_\ell + \mathbf{K}]_2}, \left\{[\mathbf{BR}_j, \mathbf{V}_j\mathbf{BR}_j + \mathbf{K}]_2\right\}_{j\in[\ell+1,L]} \\ \left\{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{V}_i\mathbf{BR}_j, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_j)]_2\right\}_{j\in[L]\setminus\{\ell\}, i\in[L]\setminus\{j\}}, \\ \left\{\boxed{\mathsf{crs}_{i,\ell}}, [\mathbf{G}_{i,\ell}]_2, \boxed{[\mathbf{V}_i\mathbf{BR}_\ell, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_\ell)]_2}\right\}_{i\in[L]\setminus\{\ell\}} \end{pmatrix}$$

$$\mathsf{mpk}_i = \begin{cases} \begin{pmatrix} [\mathbf{AU}_i, \mathbf{AW}_{1,i}, \widehat{\mathbf{G}}_i\mathbf{U}_i, \widehat{\mathbf{G}}_i\mathbf{W}_{1,i}]_1, \widetilde{\pi}_i \\ \{[\mathbf{U}_i\mathbf{BR}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[L]\setminus\{i,\ell\}}, \\ \boxed{[\mathbf{U}_i\mathbf{BR}_\ell, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_\ell)]_2}, [\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})]_2, \boxed{\pi_{i,\ell}} \end{pmatrix} & \text{if } i \neq \ell \\ \begin{pmatrix} [\mathbf{AU}_\ell, \mathbf{AW}_{1,\ell}, \widehat{\mathbf{G}}_\ell\mathbf{U}_\ell, \widehat{\mathbf{G}}_\ell\mathbf{W}_{1,\ell}]_1, \widetilde{\pi}_\ell \\ \{[\mathbf{U}_\ell\mathbf{BR}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{BR}_j), \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2, \pi_{\ell,j}\}_{j\in[L]\setminus\{\ell\}} \end{pmatrix} & \text{if } i = \ell \end{cases}$$

and when $\mathsf{mpk}^*_\ell \in D_\ell$, for each $y' \in \mathcal{K}_\ell$ we recall secret key returned from $\mathsf{OKey}(\ell, y')$ in the following form

$$\mathsf{sk}_{\ell,y'} = \begin{pmatrix} \boxed{[\mathbf{BR}_\ell\mathbf{R}]_2}, \left[\sum_{i\in[L]\setminus\{\ell\}} \mathbf{H}^*_{1,i,\ell}(\mathbf{I}_{n'} \otimes \mathbf{R})\right]_2, \\ \boxed{\left[\mathbf{U}^*_\ell\mathbf{BR}_\ell(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{BR}_\ell\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)\right]_2} \end{pmatrix}$$

where $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times k}$ is freshly sampled for each $y' \in \mathcal{K}_\ell$. Clearly, we have $\mathsf{G}_{5,\ell-1,0} = \mathsf{G}_{5,\ell-1}$; all changes are conceptual.

– $\mathsf{G}_{5,\ell-1,1}$: Identical to $\mathsf{G}_{5,\ell-1,0}$ except that we replace all $\mathbf{BR}_\ell$ with $\boxed{\mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}}$ in crs; in particular, we change the dash-boxed terms in crs as follows:

$$[\boxed{\mathbf{D}_\ell}, \mathbf{V}_\ell\boxed{\mathbf{D}_\ell} + \mathbf{K}]_2, \left\{[\mathbf{V}_i\boxed{\mathbf{D}_\ell}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \boxed{\mathbf{D}_\ell})]_2\right\}_{i\in[L]\setminus\{\ell\}},$$

and for all $i \in [L] \setminus \{\ell\}$

$$\mathsf{crs}_{i,\ell} \in \mathsf{LGen}_2(1^\lambda, \mathbb{G}_2, [\boxed{\mathbf{B}_{i,\ell}}]_2) \quad \text{with} \quad \mathbf{B}_{i,\ell} = (\mathbf{I}_{n'} \otimes \boxed{\mathbf{D}_\ell} \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell});$$

for all $i \in [L] \setminus \{\ell\}$, change the dash-boxed terms in each $\mathsf{mpk}_i \in D_i$ as follow:

$$[\mathbf{U}_i\boxed{\mathbf{D}_\ell}, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{D}_\ell})]_2,$$

and

$$\pi_{i,\ell} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,\ell}, [\boxed{\mathbf{F}_{i,\ell}}]_2, \mathbf{W}_{1,i}) \quad \text{where} \quad \mathbf{F}_{i,\ell} = (\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{D}_\ell}) \| \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell}));$$

when $\mathsf{mpk}^*_\ell \in D_\ell$, for each query $y' \in \mathcal{K}_\ell$, change the dash-boxed terms in returned $\mathsf{sk}_{\ell,y'}$ as follow:

$$[\boxed{\mathbf{D}_\ell}\mathbf{R}]_2, [\mathbf{U}^*_\ell\boxed{\mathbf{D}_\ell}(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{D}_\ell}\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)]_2.$$

We have $\mathsf{G}_{5,\ell-1,1} \approx_c \mathsf{G}_{5,\ell-1,0}$. This follows from MDDH assumption w.r.t. $[\mathbf{B}]_2$ which ensures that $([\mathbf{B}]_2, [\mathbf{BR}_\ell]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{D}_\ell]_2)$ when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$, $\mathbf{R}_\ell \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$.

– $\mathsf{G}_{5,\ell-1,2}$: Identical to $\mathsf{G}_{5,\ell-1,2}$ except that we replace $[\mathbf{V}_\ell\mathbf{D}_\ell + \mathbf{K}]_2$ in crs with

$$[\mathbf{V}_\ell\mathbf{D}_\ell + \mathbf{K} + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{k}}}]_2$$

We have $\mathsf{G}_{5,\ell-1,2} \approx_c \mathsf{G}_{5,\ell-1,1}$. We will prove this by considering two cases: (1) $P(x^*, y^*_\ell) = 0$; (2) $P(x^*, y^*_\ell) = 1$. We provide the detailed proof of these two cases in Section 5.3 and Section 5.4 respectively.

– $\mathsf{G}_{5,\ell-1,3}$: Identical to $\mathsf{G}_{5,\ell-1,2}$ except that we replace all $\mathbf{D}_\ell$ with $\boxed{\mathbf{BR}_\ell}$ where $\mathbf{R}_\ell \leftarrow \mathbb{Z}_p^{k\times k}$; in particular, we change the dash-boxed terms in crs as follows:

$$[\boxed{\mathbf{BR}_\ell}, \mathbf{V}_\ell\boxed{\mathbf{BR}_\ell} + \mathbf{K}]_2, \left\{[\mathbf{V}_i\boxed{\mathbf{BR}_\ell}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \boxed{\mathbf{BR}_\ell})]_2\right\}_{i\in[L]\setminus\{\ell\}},$$

and for all $i \in [L] \setminus \{\ell\}$

$$\mathsf{crs}_{i,\ell} \in \mathsf{LGen}_2(1^\lambda, \mathbb{G}_2, [\boxed{\mathbf{B}_{i,\ell}}]_2) \quad \text{with} \quad \mathbf{B}_{i,\ell} = (\mathbf{I}_{n'} \otimes \boxed{\mathbf{BR}_\ell} \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})$$

and for all $i \in [L] \setminus \{\ell\}$, change the dash-boxed terms in each $\mathsf{mpk}_i \in D_i$ as follow:

$$[\mathbf{U}_i\boxed{\mathbf{BR}_\ell}, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{BR}_\ell})]_2,$$

and

$$\pi_{i,\ell} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,\ell}, [\boxed{\mathbf{F}_{i,\ell}}]_2, \mathbf{W}_{1,i}) \quad \text{where} \quad \mathbf{F}_{i,\ell} = (\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{BR}_\ell}) \| \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell}))$$

when $\mathsf{mpk}^*_\ell \in D_\ell$, for each query $y' \in \mathcal{K}_\ell$, change the dash-boxed terms in returned $\mathsf{sk}_{\ell,y'}$ as follow:

$$[\boxed{\mathbf{BR}_\ell}\mathbf{R}]_2, [\mathbf{U}^*_\ell\boxed{\mathbf{BR}_\ell}(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{BR}_\ell}\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)]_2.$$

We have $\mathsf{G}_{5,\ell-1,3} \approx_c \mathsf{G}_{5,\ell-1,2}$. Analogous to $\mathsf{G}_{5,\ell-1,1} \approx_c \mathsf{G}_{5,\ell-1,0}$, it follows from MDDH assumption w.r.t. $[\mathbf{B}]_2$ which ensures that $([\mathbf{B}]_2, [\mathbf{D}_\ell]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{BR}_\ell]_2)$ when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$, $\mathbf{R}_\ell \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$.

Observe that, we have $\mathsf{G}_{5,\ell-1,3} = \mathsf{G}_{5,\ell}$ and this proves $\mathsf{G}_{5,\ell-1} \approx_c \mathsf{G}_{5,\ell}$.

5.3 From $\mathsf{G}_{5,\ell-1,1}$ to $\mathsf{G}_{5,\ell-1,2}$: If $P(x^*, y^*_\ell) = 0$

We review $\mathsf{G}_{5,\ell-1,1}$ and $\mathsf{G}_{5,\ell-1,2}$ in the following form. Here we use gray boxes to indicate the difference between two games and use dashed boxes to highlight those terms that are relevant to our proof in this case.

$$\begin{aligned}
\mathsf{crs} = &\left(\begin{array}{l}
[\mathbf{A}]_1, [\mathbf{AK}]_T, \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{AV}_i, \mathbf{AW}_{0,i}]_1\}_{i\in[L]} \\
\left\{[\mathbf{BR}_j, \mathbf{V}_j\mathbf{BR}_j + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2\right\}_{j\in[\ell-1]}, \boxed{[\mathbf{D}_\ell, \mathbf{V}_\ell\mathbf{D}_\ell + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2}, \left\{[\mathbf{BR}_j, \mathbf{V}_j\mathbf{BR}_j + \mathbf{K}]_2\right\}_{j\in[\ell+1,L]} \\
\left\{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{V}_i\mathbf{BR}_j, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{BR}_j)]_2\right\}_{j\in[L]\setminus\{\ell\}, i\in[L]\setminus\{j\}}, \\
\left\{\mathsf{crs}_{i,\ell}, [\mathbf{G}_{i,\ell}]_2, \boxed{[\mathbf{V}_i\mathbf{D}_\ell, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{D}_\ell)]_2}\right\}_{i\in[L]\setminus\{\ell\}}
\end{array}\right) \\
\mathbf{c}^*_1 = &\boxed{(\mathbf{cV}_\ell + \mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}^*_{0,\ell})(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \mathbf{cW}_{0,\ell}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1})} \\
&+ \textstyle\sum_{i\in[L]\setminus\{\ell\}}((\mathbf{cV}_i + \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i})(\mathbf{a}_{y^*_i} \otimes \mathbf{I}_{3k+1}) + \mathbf{cW}_{0,i}(\mathbf{K}_{y^*_i} \otimes \mathbf{I}_{3k+1})), \\
\mathbf{c}^*_2 = &\boxed{\mathbf{cW}_{0,\ell}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1})} + \textstyle\sum_{i\in[L]\setminus\{\ell\}} \mathbf{cW}_{0,i}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1}).
\end{aligned}$$

We define $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ and $\mathbf{D}^\perp \in \mathbb{Z}_p^{k\times(3k+1)}$ such that $\mathbf{Ac}^\perp = \mathbf{0}$, $\mathbf{cc}^\perp = 1$, $\mathbf{D}^\perp\mathbf{B} = \mathbf{0}$ and $\mathbf{D}^\perp\mathbf{D}_\ell = \mathbf{I}$; these use the facts that $\binom{\mathbf{A}}{\mathbf{c}}$ is (row) full-rank w.h.p and $(\mathbf{B}\|\mathbf{D}_\ell)$ is (column) full-rank w.h.p.

Notice that with our restrictions (15), if mpk^*_ℓ is corrupted or maliciously generated, it must be in this case; and if mpk^*_ℓ is honest, it has possibility to be in this case. And we prove $\mathsf{G}_{5,\ell-1,2} \approx_s \mathsf{G}_{5,\ell-1,1}$ in this case using the

following argument for all $b' \in \{0,1\}$:

$$
\begin{aligned}
& \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{D}_\ell, \mathbf{AV}_\ell, \mathbf{V}_\ell\mathbf{B}, \mathbf{AW}_\ell, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{V}_\ell\mathbf{D}_\ell + b'\mathbf{c}^\perp\widetilde{\mathbf{k}} && \text{//crs} \\
& \mathbf{c}, \mathbf{cV}_\ell(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \mathbf{cW}_{0,\ell}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) && \text{//}\mathbf{c}^*_0, \mathbf{c}^*_1 \\
& \mathbf{cW}_{0,\ell}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1}) && \text{//}\mathbf{c}^*_2 \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{D}_\ell, \mathbf{AV}_\ell, \mathbf{V}_\ell\mathbf{B}, \mathbf{AW}_\ell, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{V}_\ell\mathbf{D}_\ell + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{v}}} + b'\mathbf{c}^\perp\widetilde{\mathbf{k}} \\
& \mathbf{c}, \mathbf{cV}_\ell(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \mathbf{cW}_{0,\ell}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \boxed{\widetilde{\mathbf{v}}(\mathbf{a}_{y^*_\ell} \otimes \mathbf{D}^\perp) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{D}^\perp)} \\
& \mathbf{cW}_{0,\ell}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1}) + \boxed{\widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{D}^\perp)} \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{D}_\ell, \mathbf{AV}_\ell, \mathbf{V}_\ell\mathbf{B}, \mathbf{AW}_\ell, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{V}_\ell\mathbf{D}_\ell + \mathbf{c}^\perp\widetilde{\mathbf{v}} + b'\mathbf{c}^\perp\widetilde{\mathbf{k}} \\
& \mathbf{c}, \mathbf{cV}_\ell(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \mathbf{cW}_{0,\ell}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \cancel{\widetilde{\mathbf{v}}(\mathbf{a}_{y^*_\ell} \otimes \mathbf{D}^\perp)} + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{D}^\perp) \\
& \mathbf{cW}_{0,\ell}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1}) + \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{D}^\perp) \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}, \mathbf{D}_\ell, \mathbf{AV}_\ell, \mathbf{V}_\ell\mathbf{B}, \mathbf{AW}_\ell, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}), \mathbf{V}_\ell\mathbf{D}_\ell + \mathbf{c}^\perp\widetilde{\mathbf{v}} + \cancel{b'\mathbf{c}^\perp\widetilde{\mathbf{k}}} \\
& \mathbf{c}, \mathbf{cV}_\ell(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \mathbf{cW}_{0,\ell}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{D}^\perp) \\
& \mathbf{cW}_{0,\ell}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1}) + \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{D}^\perp)
\end{aligned}
$$

where $\widetilde{\mathbf{v}} \leftarrow \mathbb{Z}_p^{1\times k}$ and $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{1\times kn}$. We justify each step as follows: The first "$\approx_s$" uses the change of variables:

$$\mathbf{V}_\ell \mapsto \mathbf{V}_\ell + \mathbf{c}^\perp\widetilde{\mathbf{v}}\mathbf{D}^\perp \quad \text{and} \quad \mathbf{W}_{0,\ell} \mapsto \mathbf{W}_{0,\ell} + \mathbf{c}^\perp\widetilde{\mathbf{w}}(\mathbf{I}_n \otimes \mathbf{D}^\perp)$$

The second "$\approx_s$" uses the fact that $P(x^*, y^*_\ell) = 0$ in this case and the security of predicate encoding (c.f. Section 3.2), which ensure that

$$
\begin{aligned}
& \left(\widetilde{\mathbf{v}}(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) \| \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1})\right) \\
\approx_s\ & \left(\mathbf{0}(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) \| \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{3k+1})\right)
\end{aligned}
$$

The third "$\approx_s$" is straight-forward with the observation that $\widetilde{\mathbf{v}}$ only appears with $\widetilde{\mathbf{k}}$ and is sufficient to hide $\widetilde{\mathbf{k}}$ in crs.

5.4 From $\mathsf{G}_{5,\ell-1,1}$ to $\mathsf{G}_{5,\ell-1,2}$: If $P(x^*, y^*_\ell) = 1$

Useful Lemma. Before our proceeding, we prepare the following lemmata.

Lemma 2. *For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ such that $\binom{\mathbf{A}}{\mathbf{c}}\mathbf{c}^\perp = \binom{\mathbf{0}}{1}$; any $\mathbf{B} \in \mathbb{Z}_p^{(3k+1)\times k}$, $\mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$ and $\mathbf{D}^\perp \leftarrow \mathbb{Z}_p^{k\times(3k+1)}$ such that $\mathbf{D}^\perp(\mathbf{B}\|\mathbf{D}_\ell) = (\mathbf{0}\|\mathbf{I}_k)$; and for any adversary $\mathcal{A}$, there exist an adversary $\mathcal{B}_2$ such that*

$$
\begin{aligned}
& \left| \Pr\left[\mathcal{A}\begin{pmatrix} [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{AU}^*_\ell]_1, \mathbf{cU}^*_\ell, \mathbf{B}, \mathbf{D}_\ell, \\ \mathbf{U}^*_\ell\mathbf{B}, \mathbf{U}^*_\ell\mathbf{D}_\ell, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{U}^*_\ell]_1 \end{pmatrix} = 1\right] - \right. \\
& \left. \Pr\left[\mathcal{A}\begin{pmatrix} [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{AU}^*_\ell]_1, \mathbf{cU}^*_\ell + \boxed{\widetilde{\mathbf{u}}\mathbf{D}^\perp}, \mathbf{B}, \mathbf{D}_\ell, \\ \mathbf{U}^*_\ell\mathbf{B}, \mathbf{U}^*_\ell\mathbf{D}_\ell + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{u}}}, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{U}^*_\ell]_1 \end{pmatrix} = 1\right] \right| \\
\le\ & 2 \cdot \mathsf{Adv}^{MDDH}_{\mathcal{B}_2} + \mathsf{negl}(\lambda)
\end{aligned}
$$

where $\widetilde{\mathbf{u}} \leftarrow \mathbb{Z}_p^{1\times k}$.

Lemma 3. *For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ such that $\binom{\mathbf{A}}{\mathbf{c}}\mathbf{c}^\perp = \binom{\mathbf{0}}{1}$; any $\mathbf{B}, \mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$, $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$ and $\mathbf{R}^\perp \in \mathbb{Z}_p^{k\times(3k+1)}$ such that $\mathbf{R}^\perp(\mathbf{B}\|\mathbf{D}_\ell\|\widetilde{\mathbf{R}}) = (\mathbf{0}\|\mathbf{0}\|\mathbf{I}_k)$; and for any adversary $\mathcal{A}$, there exist an*

adversary $\mathcal{B}_2$ such that

$$\left|\Pr\left[\mathcal{A}\left(\begin{array}{l}[\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell},\\ \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}),\\ [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\mathbf{G}_\ell, \mathbf{G}_\ell \mathbf{W}^*_{1,\ell}]_1,\\ \{[\mathbf{G}_{\ell,j}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{\forall j \in [L]\setminus\{\ell\}}\end{array}\right) = 1\right] -$$
$$\Pr\left[\mathcal{A}\left(\begin{array}{l}[\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell} + \boxed{\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp)},\\ \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \boxed{\mathbf{c}^\perp \widetilde{\mathbf{w}}},\\ [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\mathbf{G}_\ell, \mathbf{G}_\ell \mathbf{W}^*_{1,\ell}]_1,\\ \{[\mathbf{G}_{\ell,j}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{\forall j \in [L]\setminus\{\ell\}}\end{array}\right) = 1\right]\Bigg|$$
$$\leq \; 4 \cdot \mathsf{Adv}^{MDDH}_{\mathcal{B}_2} + \mathsf{negl}(\lambda)$$

where $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{kn'}$.

We provide the proof of Lemma 2 and Lemma 3 in Appendix A.

Notice that with our restrictions (15), this case implies that $\mathsf{mpk}^*_\ell \in D_\ell \setminus C_\ell$ and $P'(x'^*, y') = 0$ for all $y' \in \mathcal{K}_\ell$. Define $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ and $\mathbf{D}^\perp \in \mathbb{Z}_p^{k\times(3k+1)}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$, $\mathbf{c}\mathbf{c}^\perp = 1$ and $\mathbf{D}^\perp\mathbf{B} = \mathbf{0}$, $\mathbf{D}^\perp\mathbf{D}_\ell = \mathbf{I}$, notice that these use the facts that $\binom{\mathbf{A}}{\mathbf{c}}$ is (row) full-rank w.h.p and $(\mathbf{B}\|\mathbf{D}_\ell)$ is (column) full-rank w.h.p. Assume the adversary makes Q queries to $\mathsf{OKey}(\ell, \cdot)$, we prove $\mathsf{G}_{5,\ell-1,2} \approx_c \mathsf{G}_{5,\ell-1,1}$ in this case via following sequence of hybrid argument:

– H_0 : Identical to $\mathsf{G}_{5,\ell-1,1}$. We review crs, $\mathsf{mpk}_i \in D_i$, $\mathbf{c}^*_1, \mathbf{c}^*_3$ in the following form. Here we (1) use gray boxes to indicate the difference between $\mathsf{G}_{5,\ell-1,1}$ and $\mathsf{G}_{5,\ell-1,2}$, (2) use dashed boxes to highlight the terms relevant to the proof in following hybrid sequence:

$$\mathsf{crs} = \left(\begin{array}{l}[\mathbf{A}]_1, [\mathbf{A}\mathbf{K}]_T, \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{A}\mathbf{V}_i, \mathbf{A}\mathbf{W}_{0,i}]_1\}_{i\in[L]\setminus\{\ell\}}, \mathsf{crs}_\ell, [\boxed{\widehat{\mathbf{G}}_\ell}, \mathbf{A}\mathbf{V}_\ell, \mathbf{A}\mathbf{W}_{0,\ell}]_1\\ \{[\mathbf{B}\mathbf{R}_j, \mathbf{V}_j\mathbf{B}\mathbf{R}_j + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2\}_{j\in[\ell-1]}, \boxed{[\mathbf{D}_\ell, \mathbf{V}_\ell\mathbf{D}_\ell + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2}, \{[\mathbf{B}\mathbf{R}_j, \mathbf{V}_j\mathbf{B}\mathbf{R}_j + \mathbf{K}]_2\}_{j\in[\ell+1,L]}\\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{V}_i\mathbf{B}\mathbf{R}_j, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{R}_j)]_2\}_{i\in[L]\setminus\{j,\ell\}}\}_{j\in[L]\setminus\{\ell\}, i\in[L]\setminus\{j\}},\\ \{\mathsf{crs}_{i,\ell}, [\mathbf{G}_{i,\ell}]_2, \boxed{[\mathbf{V}_i\mathbf{D}_\ell, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{D}_\ell)]_2}\}_{i\in[L]\setminus\{\ell\}}\end{array}\right)$$

$$\mathsf{mpk}_i = \begin{cases}\left(\begin{array}{l}[\mathbf{A}\mathbf{U}_i, \mathbf{A}\mathbf{W}_{1,i}, \widehat{\mathbf{G}}_i\mathbf{U}_i, \widehat{\mathbf{G}}_i\mathbf{W}_{1,i}]_1, \widetilde{\pi}_i\\ \{[\mathbf{U}_i\mathbf{B}\mathbf{R}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[L]\setminus\{i,\ell\}},\\ \boxed{[\mathbf{U}_i\mathbf{D}_\ell, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell)]_2}, [\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})]_2, \pi_{i,\ell}\end{array}\right) & \text{if } i \neq \ell\\ \left(\begin{array}{l}[\mathbf{A}\mathbf{U}_\ell, \mathbf{A}\mathbf{W}_{1,\ell}]_1, [\boxed{\widehat{\mathbf{G}}_\ell\mathbf{U}_\ell, \widehat{\mathbf{G}}_\ell\mathbf{W}_{1,\ell}}]_1, \widetilde{\pi}_\ell\\ \{[\mathbf{U}_\ell\mathbf{B}\mathbf{R}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j), \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2, \pi_{\ell,j}\}_{j\in[L]\setminus\{\ell\}}\end{array}\right) & \text{if } i = \ell\end{cases}$$

$$\begin{aligned}\mathbf{c}^*_1 = {} & \boxed{(\mathbf{c}\mathbf{V}_\ell + \mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}^*_{0,\ell})(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \mathbf{c}\mathbf{W}_{0,\ell}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1})}\\ & + \sum_{i\in[L]\setminus\{\ell\}} ((\mathbf{c}\mathbf{V}_i + \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i})(\mathbf{a}_{y^*_i} \otimes \mathbf{I}_{3k+1}) + \mathbf{c}\mathbf{W}_{0,i}(\mathbf{K}_{y^*_i} \otimes \mathbf{I}_{3k+1})),\\ \mathbf{c}^*_3 = {} & \boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}^*_{1,\ell}(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1})} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{1,i}(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1}).\end{aligned}$$

This case implies that $\mathsf{mpk}^*_\ell \in D_\ell \setminus C_\ell$, namely mpk^*_ℓ is honest and corresponding $\mathsf{msk}^*_\ell = (\mathbf{U}^*_\ell, \mathbf{W}^*_{1,\ell})$ is hidden from the adversary; moreover, for each $y' \in \mathcal{K}_\ell$, it holds that $P'(x'^*, y') = 0$. The adversary can only obtain

secret keys as follows for all $y' \in \mathcal{K}_\ell$:

$$\mathsf{sk}_{\ell,y'} = \begin{pmatrix} [\overbrace{\mathbf{D}_\ell \mathbf{R}}^{\mathbf{K}_0}]_2, & \Big[\overbrace{\sum_{i\in[L]\setminus\{\ell\}} \mathbf{H}^*_{1,i,\ell}(\mathbf{I}_{n'} \otimes \mathbf{R})}^{\mathbf{K}_1}\Big]_2, \\ \underbrace{\big[\boxed{\mathbf{U}^*_\ell \mathbf{D}_\ell(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell \mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)}\big]_2}_{\mathbf{K}_2} \end{pmatrix}$$

where $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times k}$ is freshly sampled for each $y' \in \mathcal{K}_\ell$. Clearly, we have $\mathsf{H}_0 = \mathsf{G}_{5,\ell-1,1}$; all changes are conceptual.

– H_1 : Identical to H_0 we rewrite the dashboxed terms in $\mathbf{c}_1^*$ and $\mathbf{c}_3^*$ as follow:

$$(\mathbf{c}\mathbf{V}_\ell + \boxed{\mathbf{c}\mathbf{U}^*_\ell})(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) + \mathbf{c}\mathbf{W}_{0,\ell}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{3k+1}) \quad \text{and} \quad \boxed{\mathbf{c}\mathbf{W}^*_{1,\ell}}(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1})$$

and replace all $\widehat{\mathbf{G}}_\ell = \widetilde{\mathbf{G}}_\ell \left(\begin{smallmatrix} \mathbf{c} \\ \mathbf{I}_{k+1} \end{smallmatrix}\right)$ with $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have $\mathsf{H}_1 \equiv \mathsf{H}_0$. This follows from the fact that mpk^*_ℓ must be honest in this case. Namely, we know $\mathsf{msk}^*_\ell = (\mathbf{U}^*_\ell, \mathbf{W}^*_{1,\ell})$ such that $(\mathbf{Q}^*_{0,\ell} \| \mathbf{Q}^*_{1,\ell}) = \widehat{\mathbf{G}}_\ell(\mathbf{U}^*_\ell \| \mathbf{W}^*_{1,\ell})$, and can directly simulate $\mathbf{c}(\mathbf{U}^*_\ell \| \mathbf{W}^*_{1,\ell})$ instead of $\mathbf{e}_1 \widetilde{\mathbf{G}}_\ell^{-1}(\mathbf{Q}^*_{0,\ell} \| \mathbf{Q}^*_{1,\ell})$, so that we can also replace $\widehat{\mathbf{G}}_\ell$ with a truly random $\mathbf{G}_\ell$ such as in "$\mathsf{G}_1 \equiv \mathsf{G}_2$".

– $\mathsf{H}_{2,q}$, $(q \in [0, Q])$: Identical to H_1, except that for the first q answers to $\mathsf{OKey}(\ell, \cdot)$, we replace $[\mathbf{K}_2]_2$ in dashboxed with

$$[\mathbf{K}_2]_2 = \big[(\mathbf{U}^*_\ell \mathbf{D}_\ell + \boxed{\mathbf{c}^\perp \widehat{\mathbf{k}}})(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell \mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)\big]_2$$

where $\widehat{\mathbf{k}} \leftarrow \mathbb{Z}_p^{1\times k}$. We have that

- $\mathsf{H}_{2,0} = \mathsf{H}_1$; the two games are exactly identical, since $[0] = \emptyset$;
- $\mathsf{H}_{2,q} \approx_c \mathsf{H}_{2,q-1}$; we will employ a sub-sequence of hybrid arguments for the proof described later.

– H_3 : Identical to $\mathsf{H}_{2,Q}$ except that for we replace $[\mathbf{V}_\ell \mathbf{D}_\ell + \mathbf{K}]_2$ with

$$[\mathbf{V}_\ell \mathbf{D}_\ell + \mathbf{K} + \boxed{\mathbf{c}^\perp \widetilde{\mathbf{k}}}]_2$$

We have $\mathsf{H}_3 \approx_c \mathsf{H}_{2,Q}$. This follows from the following argument for all $b' \in \{0, 1\}$:

$$\begin{aligned}
& [\mathbf{A}]_1, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{G}_\ell]_1, [\mathbf{A}\mathbf{V}_\ell]_1, \mathbf{V}_\ell \mathbf{B}, \mathbf{D}_\ell, \mathbf{V}_\ell \mathbf{D}_\ell + b' \mathbf{c}^\perp \widetilde{\mathbf{k}} && \text{//crs, } \mathsf{mpk}_\ell \\
& \mathbf{c}, \mathbf{c}\mathbf{V}_\ell + \mathbf{c}\mathbf{U}^*_\ell, \ [\mathbf{A}\mathbf{U}^*_\ell]_1, [\mathbf{G}_\ell \mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell \mathbf{B}, \mathbf{U}^*_\ell \mathbf{D}_\ell + \mathbf{c}^\perp \widehat{\mathbf{k}} && \text{//ct}^*, \mathsf{mpk}^*_\ell, \{\mathsf{sk}_{y'}\}_{y' \in \mathcal{K}_\ell} \\
\approx_c \ & [\mathbf{A}]_1, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{G}_\ell]_1, \mathbf{A}\mathbf{V}_{\ell 1}, \mathbf{V}_\ell \mathbf{B}, \mathbf{D}_\ell, \mathbf{V}_\ell \mathbf{D}_\ell + b' \mathbf{c}^\perp \widetilde{\mathbf{k}} \\
& \mathbf{c}, \mathbf{c}\mathbf{V}_\ell + \mathbf{c}\mathbf{U}^*_\ell + \boxed{\widetilde{\mathbf{u}}\mathbf{D}^\perp}, \ [\mathbf{A}\mathbf{U}^*_\ell]_1, [\mathbf{G}_\ell \mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell \mathbf{B}, \mathbf{U}^*_\ell \mathbf{D}_\ell + \boxed{\mathbf{c}^\perp \widetilde{\mathbf{u}}} + \mathbf{c}^\perp \widehat{\mathbf{k}} \\
\approx_s \ & [\mathbf{A}]_1, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{G}_\ell]_1, [\mathbf{A}\mathbf{V}_\ell]_1, \mathbf{V}_\ell \mathbf{B}, \mathbf{D}_\ell, \mathbf{V}_\ell \mathbf{D}_\ell + \boxed{\mathbf{c}^\perp \widetilde{\mathbf{v}}} + b' \mathbf{c}^\perp \widetilde{\mathbf{k}} \\
& \mathbf{c}, \mathbf{c}\mathbf{V}_\ell + \mathbf{c}\mathbf{U}^*_\ell + \boxed{\widetilde{\mathbf{v}}\mathbf{D}^\perp} + \widetilde{\mathbf{u}}\mathbf{D}^\perp, \ [\mathbf{A}\mathbf{U}^*_\ell]_1, [\mathbf{G}_\ell \mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell \mathbf{B}, \mathbf{U}^*_\ell \mathbf{D}_\ell + \mathbf{c}^\perp \widetilde{\mathbf{u}} + \mathbf{c}^\perp \widehat{\mathbf{k}} \\
\approx_s \ & [\mathbf{A}]_1, \mathbf{c}^\perp, \mathbf{B}, [\mathbf{G}_\ell]_1, [\mathbf{A}\mathbf{V}_\ell]_1, \mathbf{V}_\ell \mathbf{B}, \mathbf{D}_\ell, \mathbf{V}_\ell \mathbf{D}_\ell + \mathbf{c}^\perp \widetilde{\mathbf{v}} + \cancel{b' \mathbf{c}^\perp \widetilde{\mathbf{k}}} \\
& \mathbf{c}, \mathbf{c}\mathbf{V}_\ell + \mathbf{c}\mathbf{U}^*_\ell + \widetilde{\mathbf{v}}\mathbf{D}^\perp + \widetilde{\mathbf{u}}\mathbf{D}^\perp, \ [\mathbf{A}\mathbf{U}^*_\ell]_1, [\mathbf{G}_\ell \mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell \mathbf{B}, \mathbf{U}^*_\ell \mathbf{D}_\ell + \mathbf{c}^\perp \widetilde{\mathbf{u}} + \mathbf{c}^\perp \widehat{\mathbf{k}}
\end{aligned}$$

where $\widetilde{\mathbf{u}} \leftarrow \mathbb{Z}_p^{1\times k}$ and $\widetilde{\mathbf{v}} \leftarrow \mathbb{Z}_p^{1\times k}$. We justify each step as follows: The first "$\approx_c$" uses Lemma 2, which let $\widetilde{\mathbf{u}}$ to appear in ct^* and all $\mathsf{sk}_{\ell,y'}$. The second "$\approx_s$" uses the change of variables:

$$\mathbf{V}_\ell \mapsto \mathbf{V}_\ell + \mathbf{c}^\perp \widetilde{\mathbf{v}} \mathbf{D}^\perp.$$

The third "$\approx_s$" is straight-forward with the observation that $\widetilde{\mathbf{u}}$ in $\mathsf{sk}_{\ell,y'}$ is hidden by $\widehat{\mathbf{k}}$, so that $\widetilde{\mathbf{u}}$ can hide $\widetilde{\mathbf{v}}$ in ct^*, and further, $\widetilde{\mathbf{v}}$ is sufficient to hide $\widetilde{\mathbf{k}}$ in crs.

– $\mathsf{H}_{4,q}$, $(q \in [0, Q])$: Identical to H_2, except that for the first q answers to $\mathsf{OKey}(\ell, \cdot)$, we replace $[\mathbf{K}_2]_2$ in dashboxed with

$$[\mathbf{K}_2]_2 = \left[(\mathbf{U}_\ell^* \mathbf{D}_\ell + \cancel{\mathbf{c}^\perp \widetilde{\mathbf{k}}})(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell \mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)\right]_2$$

We have that

- $\mathsf{H}_{4,0} = \mathsf{H}_3$; the two games are exactly identical, since $[0] = \emptyset$;
- $\mathsf{H}_{4,q} \approx_c \mathsf{H}_{4,q-1}$; the proof is identical to that for $\mathsf{H}_{2,q} \approx_c \mathsf{H}_{2,q-1}$.

– H_5 : Identical to $\mathsf{H}_{4,Q}$ except that we replace all $\mathbf{G}_\ell$ with $\widehat{\mathbf{G}}_\ell = \widetilde{\mathbf{G}}_\ell \begin{pmatrix} \mathbf{c} \\ \mathbf{I}_{k+1} \end{pmatrix}$ where $\widetilde{\mathbf{G}}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+2)}$; and rewrite the dashboxed terms in $\mathbf{c}_1^*$ and $\mathbf{c}_3^*$ as follow:

$$(\mathbf{c}\mathbf{V}_\ell + \boxed{\mathbf{e}_1 \widetilde{\mathbf{G}}_\ell^{-1} \mathbf{Q}_{0,\ell}^*})(\mathbf{a}_{y_\ell^*} \otimes \mathbf{I}_{3k+1}) + \mathbf{c}\mathbf{W}_{0,\ell}(\mathbf{K}_{y_\ell^*} \otimes \mathbf{I}_{3k+1}) \quad \text{and} \quad \boxed{\mathbf{e}_1 \widetilde{\mathbf{G}}_\ell^{-1} \mathbf{Q}_{1,\ell}^*}$$

We have $\mathsf{H}_5 \equiv \mathsf{H}_{4,Q}$. The reason is identical to that in $\mathsf{H}_1 \equiv \mathsf{H}_0$

Observe that $\mathsf{H}_5 = \mathsf{G}_{5,\ell-1,2}$ and this proves $\mathsf{G}_{5,\ell-1,1} \approx_c \mathsf{G}_{5,\ell-1,2}$ in this case.

From $\mathsf{H}_{2,q-1}$ to $\mathsf{H}_{2,q}$. We are ready to prove $\mathsf{H}_{2,q-1} \approx_c \mathsf{H}_{2,q}$, and this will complete the proof of $\mathsf{G}_{5,\ell-1,2} \approx_c \mathsf{G}_{5,\ell-1,1}$ in the case that $P(x^*, y_\ell^*) = 1$. Combining with Section 5.3 which provides proof in the case that $P(x^*, y_\ell^*) = 0$, the proof of $\mathsf{G}_{5,\ell-1} \approx_c \mathsf{G}_{5,\ell}$ is finished, and this readily complete the proof of Lemma 1. For this, we need the following sub-sequence of hybrid argument for each $q \in [Q]$:

– $\mathsf{H}_{2,q-1,0}$: Identical to $\mathsf{H}_{2,q-1}$. We recall the crs, $\mathsf{mpk}_i \in D_i$, $\mathbf{c}_3^*$ and $\mathsf{sk}_{\ell,y'}$ for all $y' \in \mathcal{K}_\ell$ in the following form

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}]_1, [\mathbf{A}\mathbf{K}]_T, \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{A}\mathbf{V}_i, \mathbf{A}\mathbf{W}_{0,i}]_1\}_{i\in[L]\setminus\{\ell\}}, \mathsf{crs}_\ell, [\mathbf{G}_\ell, \mathbf{A}\mathbf{V}_\ell, \mathbf{A}\mathbf{W}_{0,\ell}]_1 \\ \left\{[\mathbf{B}\mathbf{R}_j, \mathbf{V}_j\mathbf{B}\mathbf{R}_j + \mathbf{K} + \mathbf{c}^\perp\widetilde{\mathbf{k}}]_2\right\}_{j\in[\ell-1]}, \boxed{[\mathbf{D}_\ell, \mathbf{V}_\ell\mathbf{D}_\ell + \mathbf{K}]_2}, \left\{[\mathbf{B}\mathbf{R}_j, \mathbf{V}_j\mathbf{B}\mathbf{R}_j + \mathbf{K}]_2\right\}_{j\in[\ell+1,L]} \\ \left\{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{V}_i\mathbf{B}\mathbf{R}_j, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}\mathbf{R}_j)]_2\right\}_{i\in[L]\setminus\{j,\ell\}}\Big\}_{j\in[L]\setminus\{\ell\}, i\in[L]\setminus\{j\}}, \\ \left\{\boxed{\mathsf{crs}_{i,\ell}, [\mathbf{G}_{i,\ell}]_2}, \boxed{[\mathbf{V}_i\mathbf{D}_\ell, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{D}_\ell)]_2}\right\}_{i\in[L]\setminus\{\ell\}} \end{pmatrix}$$

$$\mathsf{mpk}_i = \begin{cases} \begin{pmatrix} [\mathbf{A}\mathbf{U}_i, \mathbf{A}\mathbf{W}_{1,i}, \widehat{\mathbf{G}}_i\mathbf{U}_i, \widehat{\mathbf{G}}_i\mathbf{W}_{1,i}]_1, \widetilde{\pi}_i \\ \{[\mathbf{U}_i\mathbf{B}\mathbf{R}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[L]\setminus\{i,\ell\}}, \\ \boxed{[\mathbf{U}_i\mathbf{D}_\ell, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})]_2}, \pi_{i,\ell} \end{pmatrix} & \text{if } i \neq \ell \\ \begin{pmatrix} [\mathbf{A}\mathbf{U}_\ell, \mathbf{A}\mathbf{W}_{1,\ell}]_1, [\mathbf{G}_\ell\mathbf{U}_\ell, \mathbf{G}_\ell\mathbf{W}_{1,\ell}]_1, \widetilde{\pi}_\ell \\ \{[\mathbf{U}_\ell\mathbf{B}\mathbf{R}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j)], \boxed{[\mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2}, \pi_{\ell,j}\}_{j\in[L]\setminus\{\ell\}} \end{pmatrix} & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_3^* = \boxed{\mathbf{c}\mathbf{W}_{1,\ell}^*(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1})} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{e}_1 \widetilde{\mathbf{G}}_i^{-1} \mathbf{Q}_{1,i}^*(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1}).$$

and for the q–th secret key answered to $\mathsf{OKey}(\ell, \cdot)$, we rewrite it in the form of

$$\mathsf{sk}_{\ell,y'^*}^* = \begin{pmatrix} \overbrace{[\boxed{\mathbf{D}_\ell\mathbf{R}^*}]_2}^{\mathbf{K}_0}, & \overbrace{\left[\boxed{\sum_{i\in[L]\setminus\{\ell\}} \mathbf{H}_{1,i,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{R}^*)}\right]_2}^{\mathbf{K}_1}, \\ \underbrace{[\boxed{\mathbf{U}_\ell^*\mathbf{D}_\ell(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell\mathbf{R}^*)(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k)}]_2}_{\mathbf{K}_2} \end{pmatrix} \quad \text{where} \quad \mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}$$

here and in the following sub-sequence, we use $\mathsf{sk}_{\ell,y'^*}^*$ to indicate the q–th answer to $\mathsf{OKey}(\ell, \cdot)$, and use $\mathbf{R}^*$ and y'^* to indicate the specific random coin and query of it, they are different from the $\mathbf{R}$ and y' for other $\mathsf{sk}_{\ell,y'}$, which can have more than one assignments. And notice it holds that $P'(x'^*, y'^*) = 0$ in this case. We have $\mathsf{H}_{2,q-1,0} = \mathsf{H}_{2,q-1}$, all the changes are conceptual.

– $\mathsf{H}_{2,q-1,1}$: Identical to $\mathsf{H}_{2,q-1,0}$ except that for all $i \in [L] \setminus \{\ell\}$ and all $\mathsf{mpk}_i \in D_i$, we replace $\pi_{i,\ell}$ with

$$\widetilde{\pi}_{i,\ell} \leftarrow \boxed{\mathsf{LSim}_2}(\mathsf{crs}_{i,\ell}, \mathsf{td}_{i,\ell}, [\mathbf{F}_{i,\ell}]_2) \quad \text{where} \quad \mathbf{F}_{i,\ell} = (\underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell)}_{\mathbf{H}_{1,i,\ell}} \| \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})}_{\mathbf{P}_{i,\ell}})$$

We have $\mathsf{H}_{2,q-1,1} \equiv \mathsf{H}_{2,q-1,0}$. This follows from the perfect zero-knowledge of Π_2.

– $\mathsf{H}_{2,q-1,2}$: Identical to $\mathsf{H}_{2,q-1,1}$ except that we sample $\mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}$ along with $\mathbf{D}_\ell$ and for all $i \in [L] \setminus \{\ell\}$, we replace all $\mathbf{G}_{i,\ell}$ in crs with

$$\widehat{\mathbf{G}}_{i,\ell} = (\mathbf{D}_\ell \mathbf{R}^* \| \mathbf{I}_{3k+1}) \widetilde{\mathbf{G}}_{i,\ell}, \quad \widetilde{\mathbf{G}}_{i,\ell} \leftarrow \mathbb{Z}_p^{(4k+1)\times(4k+1)}$$

In particular, for all $i \in [L] \setminus \{\ell\}$, for the dashboxed term in each $\mathsf{mpk}_i \in D_i$, we have

$$\mathbf{P}_{i,\ell} = \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\widehat{\mathbf{G}}_{i,\ell}})$$

We have $\mathsf{H}_{2,q-1,2} \equiv \mathsf{H}_{2,q-1,1}$. This follows from the fact that both $\mathbf{G}_{i,\ell}$ and $\widehat{\mathbf{G}}_{i,\ell}$ are truly random since $(\mathbf{D}_\ell \mathbf{R}^* \| \mathbf{I}_{3k+1})$ is (row) full-rank.

– $\mathsf{H}_{2,q-1,3}$: Identical to $\mathsf{H}_{2,q-1,2}$ except that we replace $\mathbf{K}_1$ in $\mathsf{sk}^*_{\ell,y'^*}$ with

$$\mathbf{K}_1 = \sum_{i\in[L]\setminus\{\ell\}} \boxed{\mathbf{P}^*_{i,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{G}}^{-1}_{i,\ell}\mathbf{E}_1)} \quad \text{where} \quad \mathbf{E}_1 = \begin{pmatrix}\mathbf{I}_k \\ \mathbf{0}\end{pmatrix} \in \mathbb{Z}_p^{(4k+1)\times k}$$

We have $\mathsf{H}_{2,q-1,3} \approx_c \mathsf{H}_{2,q-1,2}$. This follows from stronger unbounded simulation soundness of Π_2 along with the fact that $\mathsf{LVer}_2(\mathsf{crs}_{i,\ell}, [\mathbf{F}^*_{i,\ell}]_1, \pi^*_{i,\ell}) = 1$ for all $i \in [L]\setminus\{\ell\}$ where $\mathbf{F}^*_{i,\ell} = (\mathbf{H}^*_{1,i,\ell} \| \mathbf{P}^*_{i,\ell})$. Assume $\mathsf{mpk}^*_{i^*} \notin D_{i^*}$, i.e., $\mathsf{mpk}^*_{i^*}$ is malicious. In the reduction, we guess $i^* \leftarrow [L]\setminus\{\ell\}$ and obtain $\mathbf{D}_\ell, \widehat{\mathbf{G}}_{i^*,\ell}, \mathsf{crs}_{i^*,\ell}$ as input; we simulate honestly as in $\mathsf{H}_{2,q-1,3}$ except that for all $\mathsf{mpk}_{i^*} \in D_{i^*}$, we make an oracle query $[\mathbf{F}_{i^*,\ell}]_2$ and get $\widetilde{\pi}_{i^*,\ell}$ in it; we finally output $([\mathbf{F}^*_{i^*,\ell}]_2, \pi^*_{i^*,\ell})$ in $\mathsf{mpk}^*_{i^*} \notin D_{i^*}$. Observe that once it happens that $\mathbf{P}^*_{i^*,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{G}}^{-1}_{i^*,\ell}\mathbf{E}_1) \neq \mathbf{H}^*_{1,i^*,\ell}(\mathbf{I}_{n'} \otimes \mathbf{R}^*)$, we must have $\mathbf{F}^*_{i^*,\ell} \notin \mathsf{span}(\mathbf{B}_{i^*,\ell})$. When $\mathsf{mpk}^*_{i^*} \in D_{i^*}$, we always have $\mathsf{H}_{2,q-1,3} \equiv \mathsf{H}_{2,q-1,2}$.

– $\mathsf{H}_{2,q-1,4}$: Identical to $\mathsf{H}_{2,q-1,3}$ except that we replace all $\mathbf{D}_\ell \mathbf{R}^*$ with $\boxed{\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}}$; in particular, for all $i \in [L] \setminus \{\ell\}$ we generate $\widehat{\mathbf{G}}_{i,\ell}$ as follows:

$$\widehat{\mathbf{G}}_{i,\ell} = (\boxed{\widetilde{\mathbf{R}}} \| \mathbf{I}_{3k+1}) \widetilde{\mathbf{G}}_{i,\ell}, \quad \widetilde{\mathbf{G}}_{i,\ell} \leftarrow \mathbb{Z}_p^{(4k+1)\times(4k+1)}$$

and generate the $[\mathbf{K}_0]_2, [\mathbf{K}_2]_2$ in $\mathsf{sk}^*_{\ell,y'^*}$ as:

$$[\boxed{\widetilde{\mathbf{R}}}]_2 \quad \text{and} \quad [\mathbf{U}^*_\ell \mathbf{D}_\ell(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\widetilde{\mathbf{R}}})(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k)]_2$$

We have $\mathsf{H}_{2,q-1,4} \approx_c \mathsf{H}_{2,q-1,3}$. This follows from MDDH assumption w.r.t. $[\mathbf{D}_\ell]_2$ which ensures that $([\mathbf{D}_\ell]_2, [\mathbf{D}_\ell \mathbf{R}^*]_2) \approx_c ([\mathbf{D}_\ell]_2, [\widetilde{\mathbf{R}}]_2)$ when $\mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}, \mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}, \widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$.

– $\mathsf{H}_{2,q-1,5}$: Identical to $\mathsf{H}_{2,q-1,4}$ except that we replace the $\mathbf{K}_2$ in $\mathsf{sk}^*_{\ell,y'^*}$ with

$$\mathbf{K}_2 = (\mathbf{U}^*_\ell \mathbf{D}_\ell + \boxed{\mathbf{c}^\perp \widehat{\mathbf{k}}})(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}})(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k)$$

We have $\mathsf{H}_{2,q-1,5} \approx_c \mathsf{H}_{2,q-1,4}$. Define $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ and $\mathbf{R}^\perp \in \mathbb{Z}_p^{k\times(3k+1)}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$, $\mathbf{c}\mathbf{c}^\perp = 1$ and $\mathbf{R}^\perp \mathbf{B} = \mathbf{0}$, $\mathbf{R}^\perp \mathbf{D}_\ell = \mathbf{0}$ and $\mathbf{R}^\perp \widetilde{\mathbf{R}} = \mathbf{I}_k$, notice that these use the fact that $\left(\begin{smallmatrix}\mathbf{A}\\ \mathbf{c}\end{smallmatrix}\right)$ is (row) full-rank w.h.p and $(\mathbf{B} \| \mathbf{D}_\ell \| \widetilde{\mathbf{R}})$ is (column)

full-rank w.h.p. The $\mathsf{H}_{2,q-1,5} \approx_c \mathsf{H}_{2,q-1,4}$ follows from the following argument for $b' \in \{0,1\}$:

$$
\begin{aligned}
& [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{B}]_1, \mathbf{D}_\ell, [\mathbf{G}_\ell]_1, \{[\mathbf{G}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}} && \text{// crs, } \mathsf{mpk}_\ell \\
& \mathbf{c}, \mathbf{c}\mathbf{W}^*_{1,\ell}(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1}) && \text{// } \mathsf{ct}^* \\
& \widetilde{\mathbf{R}}, (\mathbf{U}^*_\ell \mathbf{D}_\ell + b'\mathbf{c}^\perp \widehat{\mathbf{k}})(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}})(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k) && \text{// } \mathsf{sk}^*_{\ell,y'^*} \\
& \begin{pmatrix} [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, [\mathbf{G}_\ell \mathbf{W}^*_{1,\ell}]_1, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, \\ \{[\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{j\in[L]\setminus\{\ell\}} \end{pmatrix}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell) && \text{// } \mathsf{mpk}^*_\ell, \text{ other } \mathsf{sk}_{\ell,y'} \\
\approx_c\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{B}]_1, \mathbf{D}_\ell, [\mathbf{G}_\ell]_1, \{[\mathbf{G}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}} \\
& \mathbf{c}, (\mathbf{c}\mathbf{W}^*_{1,\ell} + \boxed{\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp)})(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1}) \\
& \widetilde{\mathbf{R}}, (\mathbf{U}^*_\ell \mathbf{D}_\ell + b'\mathbf{c}^\perp \widehat{\mathbf{k}})(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + (\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \boxed{\mathbf{c}^\perp \widetilde{\mathbf{w}}})(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k) \\
& \begin{pmatrix} [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, [\mathbf{G}_\ell \mathbf{W}^*_{1,\ell}]_1, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, \\ \{[\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{j\in[L]\setminus\{\ell\}} \end{pmatrix}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell) \\
\approx_s\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{B}]_1, \mathbf{D}_\ell, [\mathbf{G}_\ell]_1, \{[\mathbf{G}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}} \\
& \mathbf{c}, (\mathbf{c}\mathbf{W}^*_{1,\ell} + \widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp))(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_{3k+1}) \\
& \widetilde{\mathbf{R}}, (\mathbf{U}^*_\ell \mathbf{D}_\ell + \cancel{b'\mathbf{c}^\perp \widehat{\mathbf{k}}})(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + (\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \mathbf{c}^\perp \widetilde{\mathbf{w}})(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k) \\
& \begin{pmatrix} [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, [\mathbf{G}_\ell \mathbf{W}^*_{1,\ell}]_1, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, \\ \{[\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{j\in[L]\setminus\{\ell\}} \end{pmatrix}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell)
\end{aligned}
$$

where $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{kn'}$. We justify each step as follows: The first "$\approx_c$" uses Lemma 3, which let $\widetilde{\mathbf{w}}$ appears in ct^* and $\mathsf{sk}^*_{\ell,y'^*}$. The second "$\approx_s$" uses the fact that $P'(x'^*, y'^*) = 0$ in this case and security of predicate encoding (c.f. Section 3.2), which ensure that

$$
\begin{aligned}
& \left(\widehat{\mathbf{k}}(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + \widetilde{\mathbf{w}}(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k) \| \widetilde{\mathbf{w}}(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_k)\right) \\
\approx_s\ & \left(\mathbf{0}(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + \widetilde{\mathbf{w}}(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k) \| \widetilde{\mathbf{w}}(\mathbf{C}'_{x'^*} \otimes \mathbf{I}_k)\right)
\end{aligned}
$$

- $\mathsf{H}_{2,q-1,6}$: Identical to $\mathsf{H}_{2,q-1,5}$ except that we replace all $\widetilde{\mathbf{R}}$ with $\boxed{\mathbf{D}_\ell \mathbf{R}^*}$ where $\mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}$; in particular, for all $i \in [L] \setminus \{\ell\}$ we generate $\widehat{\mathbf{G}}_{i,\ell}$ as follows:

$$
\widehat{\mathbf{G}}_{i,\ell} = \left(\boxed{\mathbf{D}_\ell \mathbf{R}^*} \| \mathbf{I}_{3k+1}\right) \widetilde{\mathbf{G}}_{i,\ell}, \quad \widetilde{\mathbf{G}}_{i,\ell} \leftarrow \mathbb{Z}_p^{(4k+1)\times(4k+1)}
$$

and generate the $[\mathbf{K}_0]_2, [\mathbf{K}_2]_2$ in $\mathsf{sk}^*_{\ell,y'^*}$ as:

$$
[\boxed{\mathbf{D}_\ell \mathbf{R}^*}]_2 \quad \text{and} \quad [\mathbf{U}^*_\ell \mathbf{D}_\ell (\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{D}_\ell \mathbf{R}^*})(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k)]_2
$$

We have $\mathsf{H}_{2,q-1,6} \approx_c \mathsf{H}_{2,q-1,5}$. The reason is identical to that for $\mathsf{H}_{2,q-1,3} \approx_c \mathsf{H}_{2,q-1,4}$. This follows from MDDH assumption w.r.t. $[\mathbf{D}_\ell]_2$ which ensures that $([\mathbf{D}_\ell]_2, [\widetilde{\mathbf{R}}]_2) \approx_c ([\mathbf{D}_\ell]_2, [\mathbf{D}_\ell \mathbf{R}^*]_2)$ when $\mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$, $\mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}$, $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$.

- $\mathsf{H}_{2,q-1,7}$: Identical to $\mathsf{H}_{2,q-1,6}$, except that we replace $\mathbf{K}_1$ in $\mathsf{sk}^*_{\ell,y'^*}$ with

$$
\mathbf{K}_1 = \sum_{i\in[L]\setminus\{\ell\}} \boxed{\mathbf{H}^*_{1,i,\ell}(\mathbf{I}_{n'} \otimes \mathbf{R}^*)}
$$

We have $\mathsf{H}_{2,q-1,7} \approx_c \mathsf{H}_{2,q-1,6}$. The reason is identical to that for $\mathsf{H}_{2,q-1,2} \approx_c \mathsf{H}_{2,q-1,3}$. This follows from stronger unbounded simulation soundness of Π_2 along with the fact that $\mathsf{LVer}_2(\mathsf{crs}_{i,\ell}, [\mathbf{F}^*_{i,\ell}]_1, \pi^*_{i,\ell}) = 1$ for all $i \in [L] \setminus \{\ell\}$ where $\mathbf{F}^*_{i,\ell} = (\mathbf{H}^*_{1,i,\ell} \| \mathbf{P}^*_{i,\ell})$.

– $\mathsf{H}_{2,q-1,8}$: Identical to $\mathsf{H}_{2,q-1,7}$ except that for all $i \in [L] \setminus \{\ell\}$, we replace $\widehat{\mathbf{G}}_{i,\ell}$ with $\mathbf{G}_{i,\ell} \leftarrow \mathbb{Z}_p^{(3k+1)\times(4k+1)}$. In particular, for all $i \in [L] \setminus \{\ell\}$, for the dashboxed term in each $\mathsf{mpk}_i \in D_i$, we have

$$\mathbf{P}_{i,\ell} = \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{G}_{i,\ell}})$$

We have $\mathsf{H}_{2,q-1,8} \equiv \mathsf{H}_{2,q-1,7}$. The reason is identical to that for $\mathsf{H}_{2,q-1,2} \equiv \mathsf{H}_{2,q-1,1}$. This follows from the fact that both $\mathbf{G}_{i,\ell}$ and $\widehat{\mathbf{G}}_{i,\ell}$ are truly random since $(\mathbf{D}_\ell \mathbf{R}^* \| \mathbf{I}_{3k+1})$ is (row) full-rank.

– $\mathsf{H}_{2,q-1,9}$: Identical to $\mathsf{H}_{2,q-1,8}$ except that for all $i \in [L] \setminus \{\ell\}$ and all $\mathsf{mpk}_i \in D_i$, we replace $\widetilde{\pi}_{i,\ell}$ with

$$\pi_{i,\ell} \leftarrow \boxed{\mathsf{LPrv}_2}(\mathsf{crs}_{i,\ell}, [\mathbf{F}_{i,\ell}]_2, \mathbf{W}_{1,i}) \quad \text{where} \quad \mathbf{F}_{i,\ell} = (\underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell)}_{\mathbf{H}_{1,i,\ell}} \| \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})}_{\mathbf{P}_{i,\ell}})$$

We have $\mathsf{H}_{2,q-1,9} \equiv \mathsf{H}_{2,q-1,8}$. The reason is identical to that for $\mathsf{H}_{2,q-1,1} \equiv \mathsf{H}_{2,q-1,0}$. This follows from the perfect zero-knowledge of Π_2.

Observe that we have $\mathsf{H}_{2,q-1,9} = \mathsf{H}_{2,q}$ and this proves $\mathsf{H}_{2,q-1} \approx_c \mathsf{H}_{2,q}$.

6 Slotted Delegated Reg-IPFE from Pairings

In this section, we propose a construction of slotted delegated Reg-IPFE for two inner-product functionalities which are defined by $X = \mathbb{Z}_p^{1\times n_1}$, $Y = \mathbb{Z}_p^{1\times n_2}$, $Z = \mathbb{Z}_p$ and

$$G = \{\mathbf{M} : \mathbf{x} \mapsto \mathbf{x}\mathbf{M}\} \quad \text{and} \quad F = \{\mathbf{f} : \mathbf{y} \mapsto \mathbf{y}\mathbf{f}^\top\}$$

By the Remark 1 and generic transformation in Section 10, this yields a full-fledged Reg-IPFE.

6.1 Scheme

Under k–lin assumption, the scheme achieves the adaptive IND-security (c.f. Section 4.1). Assuming QA-NIZK $\Pi = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ for $\mathbb{G}_1$-linear space over bilinear groups, see Section 3.3, our slotted delegated Reg-IPFE scheme in prime-order bilinear groups works as follows:

– $\mathsf{Setup}(1^\lambda, 1^{n_1}, 1^{n_2}, 1^L)$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

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

Sample

$$\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}, \ \mathbf{B}_2 \leftarrow \mathbb{Z}_p^{(2k+1)\times 1}, \ \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$$

and compute the dual basis $(\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel)$, see section 3.1. For all $i \in [L]$, sample

$$\mathbf{W}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)n_1}, \ \mathbf{G}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}, \ \mathbf{r}_i \leftarrow \mathbb{Z}_p^{1\times k}.$$

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

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

Output

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{A}\mathbf{V}]_1, \{[\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[L]} \\ \{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$

Notice that we do not use $\mathsf{td}_1, \ldots, \mathsf{td}_L$ and $\mathbf{B}_2, \mathbf{B}_3$, $(\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel)$ in the actual scheme.

– $\mathsf{Gen}(\mathsf{crs}, i)$: Sample $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)n_2}$. Define $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i} = \binom{\mathbf{A}\mathbf{U}_i}{\mathbf{G}_i\mathbf{U}_i} = \mathbf{A}_i\mathbf{U}_i \in \mathbb{Z}_p^{(2k+2)\times(2k+1)n_2}$ 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

$$\mathsf{mpk}_i = \Big([\underbrace{\mathbf{A}\mathbf{U}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{G}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{\underbrace{[\mathbf{U}_i(\mathbf{I}_{n_2}\otimes\mathbf{B}_1\mathbf{r}_j^\top)]_2}_{\mathbf{H}_{i,j}}\}_{j\in[L]\setminus\{i\}}, \pi_i\Big) \quad \text{and} \quad \mathsf{msk}_i = \mathbf{U}_i.$$

– $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i)$: Parse $\mathsf{mpk}_i = \big([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{H}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$. 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

$$e([\mathbf{A}]_1, [\mathbf{H}_{i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_i]_1, [\mathbf{I}_{n_2}\otimes\mathbf{B}_1\mathbf{r}_j^\top]_2).$$

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

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

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

and for all $j \in [L]$

$$\mathsf{hsk}_j = \left(\left[\underbrace{\mathbf{B}_1\mathbf{r}_j^\top}_{\mathbf{k}_{j,0}^\top}, \underbrace{\sum_{i\in[L]\setminus\{j\}}(\mathbf{H}_{i,j} + \mathbf{W}_i(\mathbf{I}_{n_1}\otimes\mathbf{B}_1\mathbf{r}_j^\top)\mathbf{M}_i)}_{\mathbf{K}_{j,1}}, \underbrace{\sum_{i\in[L]\setminus\{j\}}\mathbf{W}_i(\mathbf{I}_{n_1}\otimes\mathbf{B}_1\mathbf{r}_j^\top)}_{\mathbf{K}_{j,2}}\right]_2\right).$$

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

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

– $\mathsf{Key}(\mathsf{msk}_{j^*}, \mathsf{hsk}_{j^*}, \mathbf{f})$: Parse $\mathsf{msk}_{j^*} = \mathbf{U}_{j^*}$. Output

$$\mathsf{sk}_{j^*,\mathbf{f}} = \underbrace{\mathbf{U}_{j^*}(\mathbf{f}^\top\otimes\mathbf{I}_{2k+1})}_{\mathbf{K}_0}$$

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

$$\mathsf{sk}_{j^*,\mathbf{f}} = \mathbf{K}_0, \quad \mathsf{hsk}_{j^*} = ([\mathbf{k}_{j^*,0}^\top, \mathbf{K}_{j^*,1}, \mathbf{K}_{j^*,2}]_2), \quad \mathsf{ct} = ([\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3]_1).$$

Recover

$$\begin{aligned}
&[\mathbf{z}_1]_T = e([\mathbf{c}_2]_1, [\mathbf{I}_{n_1}\otimes\mathbf{k}_{j^*,0}^\top]_2), \quad [\mathbf{z}_2]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_{j^*,2}]_2);\\
&[\mathbf{z}_3]_T = e([\mathbf{c}_1]_1, [\mathbf{I}_{n_2}\otimes\mathbf{k}_{j^*,0}^\top]_2), \quad [\mathbf{z}_4]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_{j^*,1}]_2);\\
&[z_5]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_0\mathbf{k}_{j^*,0}^\top]_2),\\
&[z_6]_T = e([\mathbf{c}_3]_1, [\mathbf{k}_{j^*,0}^\top]_2).
\end{aligned}$$

Compute

$$[z']_T = [(\mathbf{z}_1 - \mathbf{z}_2)\mathbf{M}_{j^*}\mathbf{f}^\top - (\mathbf{z}_3 - \mathbf{z}_4)\mathbf{f}^\top + z_5]_T$$

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

Completeness. For all $\lambda, L, n_1, n_2 \in \mathbb{N}$, all $i \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^{n_1}, 1^{n_2}, 1^L)$ and $(\mathsf{mpk}_i, \mathsf{msk}_i) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)$, we have

$$\mathsf{mpk}_i = \left([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{H}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\right) = \left([\mathbf{AU}_i, \mathbf{G}_i\mathbf{U}_i]_1, \{[\mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\right)$$

for some $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)n_2}$ 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 $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{G}_i}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{G}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. Then

- Write $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i} = \binom{\mathbf{AU}_i}{\mathbf{G}_i\mathbf{U}_i}$, we have $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \pi_i) = 1$ by the perfect completeness of Π (see Section 3.3) and the fact that $\mathbf{F}_i = \mathbf{A}_i\mathbf{U}_i$;
- For each $j \in [L] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2) = e([\mathbf{AU}_i]_1, [\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_j^\top]_2)$ by the definition of bilinear map e (see Section 3.1) and the fact that $\mathbf{A} \cdot \mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_j^\top) = \mathbf{AU}_i \cdot (\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_j^\top)$.

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

Correctness. For all $\lambda, L, n_1, n_2 \in \mathbb{N}$, all $j^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^{n_1}, 1^{n_2}, 1^L)$, all $(\mathsf{mpk}_{j^*}, \mathsf{msk}_{j^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, j^*)$, all $\{\mathsf{mpk}_i\}_{i\in[L]\setminus\{j^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i) = 1$, for all $\mathbf{M}_1, \ldots, \mathbf{M}_L \in \mathbb{Z}_p^{n_1\times n_2}$ and $\mathbf{x} \in \mathbb{Z}_p^{1\times n_1}$, $\mathbf{f} \in \mathbb{Z}_p^{1\times n_2}$, we have:

$$\begin{aligned}
\mathsf{sk}_{j^*,\mathbf{f}} &= \underbrace{\mathbf{U}_{j^*}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})}_{\mathbf{K}_0}, \\
\mathsf{hsk}_{j^*} &= \left(\left[\underbrace{\mathbf{B}_1\mathbf{r}_{j^*}^\top}_{\mathbf{k}_{j^*,0}^\top}, \underbrace{\sum_{i\in[L]\setminus\{j^*\}} (\mathbf{H}_{i,j^*} + \mathbf{W}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)\mathbf{M}_i)}_{\mathbf{K}_{j^*,1}}, \underbrace{\sum_{i\in[L]\setminus\{j^*\}} \mathbf{W}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)}_{\mathbf{K}_{j^*,2}}\right]_2\right), \\
\mathsf{ct} &= \left(\left[\underbrace{\mathbf{sA}}_{\mathbf{c}_0}, \underbrace{\sum_{i\in[L]} (\mathbf{sT}_i + \mathbf{sAW}_i(\mathbf{M}_i \otimes \mathbf{I}_{2k+1}))}_{\mathbf{c}_1}, \underbrace{\mathbf{x} \otimes \mathbf{sAV} + \sum_{i\in[L]} \mathbf{sAW}_i}_{\mathbf{c}_2}, \underbrace{\mathbf{sAV}}_{\mathbf{c}_3}\right]_1\right)
\end{aligned}$$

where

$$\mathbf{AH}_{i,j^*} = \mathbf{T}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) \quad \forall i \in [L] \setminus \{j^*\} \quad \text{and} \quad \mathbf{T}_{j^*} = \mathbf{AU}_{j^*}.$$

Note that in Key and Dec, we actually consider hsk_j for $j = j^*$ and msk_i for $i = j^*$; and all above equalities are ensured by Ver, Gen and Key. And we have

$$\begin{aligned}
\mathbf{z}_1 &= (\mathbf{x} \otimes \mathbf{sAV})(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) \\
&= \mathbf{x} \otimes \mathbf{sAVB}_1\mathbf{r}_{j^*}^\top + \sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) \qquad (16)\\
&= \mathbf{sAVB}_1\mathbf{r}_{j^*}^\top \cdot \mathbf{x} + \sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) \\
\mathbf{z}_2 &= \sum_{i\in[L]\setminus\{j^*\}} \mathbf{sAW}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) \\
\mathbf{z}_3 &= \sum_{i\in[L]} (\mathbf{sT}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \mathbf{sAW}_i(\mathbf{M}_i \otimes \mathbf{I}_{2k+1})(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)) \\
&= \sum_{i\in[L]} (\mathbf{sT}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \mathbf{sAW}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)\mathbf{M}_i) \qquad (17)\\
\mathbf{z}_4 &= \sum_{i\in[L]\setminus\{j^*\}} (\mathbf{sAH}_{i,j^*} + \mathbf{sAW}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)\mathbf{M}_i) \\
z_5 &= \mathbf{sAU}_{j^*}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})\mathbf{B}_1\mathbf{r}_{j^*}^\top \\
&= \mathbf{sAU}_{j^*}(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)\mathbf{f}^\top \qquad (18)\\
z_6 &= \mathbf{sAVB}_1\mathbf{r}_{j^*}^\top
\end{aligned}$$

and then

$$\begin{aligned}
[z']_T &= [(\mathbf{z}_1 - \mathbf{z}_2)\mathbf{M}_{j^*}\mathbf{f}^\top - (\mathbf{z}_3 - \mathbf{z}_4)\mathbf{f}^\top + z_5)]_T \\
&= [(\mathbf{sAVB}_1\mathbf{r}_{j^*}^\top \cdot \mathbf{xM}_{j^*}\mathbf{f}^\top + \mathbf{sAW}_{j^*}(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)\mathbf{M}_{j^*}\mathbf{f}^\top) \\
&\quad -(\mathbf{sAU}_{j^*}(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \mathbf{sAW}_{j^*}(\mathbf{I}_{n_1} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)\mathbf{M}_{j^*}\mathbf{f}^\top) + \mathbf{sAU}_{j^*}(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)\mathbf{f}^\top]_T \qquad (19)\\
&= [\mathbf{sAVB}_1\mathbf{r}_{j^*}^\top \cdot \mathbf{xM}_{j^*}\mathbf{f}^\top]_T
\end{aligned}$$

Here, equality (16), equality (17) and equality (18) 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 (19) follows from the fact that $\mathbf{AH}_{i,j^*} = \mathbf{T}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)$ for all $i \in [L] \setminus \{j^*\}$ and the fact that $\mathbf{T}_{j^*} = \mathbf{AU}_{j^*}$. Treat $[z_6]_T = [\mathbf{sAVB}_1\mathbf{r}_{j^*}^\top]_T$ as the basis, and recover z from $[z']_T = [\mathbf{sAVB}_1\mathbf{r}_{j^*}^\top \cdot \mathbf{xM}_{j^*}\mathbf{f}^\top]_T$ via brute-force DLOG, we have

$$z = \mathbf{xM}_{j^*}\mathbf{f}^\top$$

This proves the correctness.

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

$$|\mathsf{crs}| = L^2 \cdot n_1 \cdot \mathsf{poly}(\lambda); \quad |\mathsf{mpk}_+| = n_2 \cdot \mathsf{poly}(\lambda); \quad |\mathsf{hsk}_j| = n_2 \cdot \mathsf{poly}(\lambda); \quad |\mathsf{ct}| = n \cdot \mathsf{poly}(\lambda); \quad |\mathsf{sk}| = \mathsf{poly}(\lambda).$$

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 delegated Reg-IPFE scheme achieves adaptive IND-security from MDDH assumption.

Theorem 2. *Assume* $\Pi = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ *is a QA-NIZK with perfect completeness, perfect zero-knowledge and unbounded simulation soundness for* $\mathbb{G}_1$*-linear space defined in Section 3.3, our slotted delegated Reg-IPFE scheme achieves the adaptive IND-security defined in Section 4.1 under MDDH assumption and subspace decision assumption.*

6.2 Proof

We prove the following technical lemma; this immediately proves Theorem 2.

Lemma 4. *For any adversaries* $\mathcal{A}$*, there exist adversaries* $\mathcal{B}_1$*,* $\mathcal{B}_2$*,* $\mathcal{B}_3$ *and* $\mathcal{B}_4$ *such that:*

$$\mathsf{Adv}^{\mathit{sDel\text{-}Reg\text{-}IPFE}}_{\mathcal{A}}(\lambda) \le L \cdot \mathsf{Adv}^{\mathit{USS}}_{\mathcal{B}_1}(\lambda) + (8L+1)\mathsf{Adv}^{\mathit{MDDH}}_{\mathcal{B}_2}(\lambda) + L \cdot \mathsf{Adv}^{\mathrm{SD}^{\mathbb{G}_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_3}}_{\mathcal{B}_3}(\lambda) + L \cdot \mathsf{Adv}^{\mathrm{SD}^{\mathbb{G}_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_2}}_{\mathcal{B}_4}(\lambda) + \mathsf{negl}(\lambda)$$

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, $\{\mathsf{mpk}_i^*, \mathbf{M}_i^*\}_{i\in[L]}$ are challenge mater public keys along with challenge functions to be registered. For all $i \in [L]$, define $D_i = \{\mathsf{mpk}_i : \mathcal{D}_i[\mathsf{mpk}_i] = \mathsf{msk}_i \neq \bot\}$ be responses to $\mathsf{OGen}(i)$ and $C_i = \{\mathsf{mpk}_i : (i, \mathsf{mpk}_i) \in C\}$ records master public keys in D_i that have been sent to $\mathsf{OCor}(i, \cdot)$; recall that $\mathcal{K}_i$ is the list that record the queries to $\mathsf{OKey}(i, \cdot)$. For each $i \in [L]$, we have the restrictions as follow

$$\begin{aligned} \mathsf{mpk}_i^* \notin D_i &\implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i^*) = 1 \wedge \mathcal{K}_i = \emptyset, \\ \mathsf{mpk}_i^* \in C_i \vee \mathsf{mpk}_i^* \notin D_i &\implies \mathbf{x}_0^*\mathbf{M}_i^* = \mathbf{x}_1^*\mathbf{M}_i^*, \\ \mathbf{f} \in \mathcal{K}_i &\implies \mathbf{x}_0^*\mathbf{M}_i^*\mathbf{f}^\top = \mathbf{x}_1^*\mathbf{M}_i^*\mathbf{f}^\top. \end{aligned}$$

Note that mpk_i serves as a *general* entry in D_i while mpk_i^* is the *specific* challenge public for slot i; for $\mathsf{mpk}_i \in D_i$, there can be more than one assignments, since the adversary can invoke $\mathsf{OGen}(i)$ for many times. We prove the Lemma 4 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:
$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AV}]_1, \{[\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[L]} \\ \{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{AW}_i]_1\}_{i\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L], i\in[L]\setminus\{j\}} \end{pmatrix}.$$
    where $\mathsf{crs}_i \in \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$, $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{G}_i}$.
  - For each $i \in [L]$, each $\mathsf{mpk}_i \in D_i$ is in the form:
$$\mathsf{mpk}_i = (\underbrace{[\mathbf{AU}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{G}_i\mathbf{U}_i]}_{\mathbf{Q}_i}{}_1, \underbrace{\{[\mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L]\setminus\{i\}}}_{\mathbf{H}_{i,j}}, \pi_i)$$
    where $\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i)$, $\mathbf{F}_i = \binom{\mathbf{AU}_i}{\mathbf{G}_i\mathbf{U}_i}$, and $\mathbf{U}_i$ is the corresponding msk_i.
  - For all $i \in [L]$, mpk_i^* is in the form:
$$\mathsf{mpk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{H}_{i,j}^*]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$$
    such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i^*) = 1$ which means $\mathsf{LVer}\left(\mathsf{crs}_i, \begin{bmatrix}\mathbf{T}_i^* \\ \mathbf{Q}_i^*\end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{AH}_{i,j}^* = \mathbf{T}_i^*(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}_j^\top)$ for each $j \in [L] \setminus \{i\}$.

- For each $j \in [L]$ such that $\mathsf{mpk}_j^* \in D_j$, and each $\mathbf{f} \in \mathcal{K}_j$, the secret key returned from $\mathsf{OKey}(j, \mathbf{f})$ are in the form:

$$\mathsf{sk}_{j,\mathbf{f}} = \mathbf{U}_j^*(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})$$

  where $\mathbf{U}_j^* = \mathsf{msk}_j^* = \mathcal{D}_j[\mathsf{mpk}_j^*]$.
- ct^* for $(\mathbf{x}_0^*, \mathbf{x}_1^*)$ is in the form:

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

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

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

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

  We have $\mathsf{G}_1 \equiv \mathsf{G}_0$. This follows from the perfect zero-knowledge of Π.
– 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 $\mathbf{G}_i$ in crs with

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

  We have $\mathsf{G}_2 \equiv \mathsf{G}_1$. This follows from the fact that both $\mathbf{G}_i$ (in G_1) and $\widehat{\mathbf{G}}_i$ (in G_2) are truly random since matrix $\left(\begin{smallmatrix}\mathbf{sA} \\ \mathbf{I}_{k+1}\end{smallmatrix}\right)$ is full-rank.
– G_3: Identical to G_2 except that we generate the $\mathbf{c}_1^*$ as follows:

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

  We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from stronger unbounded simulation soundness of Π along with the fact that $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i^*]_1, \pi_i^*) = 1$ for all $i \in [L]$ where $\mathbf{F}_i^* = \begin{pmatrix}\mathbf{T}_i^* \\ \mathbf{Q}_i^*\end{pmatrix}$. Assume $\mathsf{mpk}_{i^*}^* \notin D_{i^*}$, i.e., $\mathsf{mpk}_{i^*}^*$ is malicious. In the reduction, we guess $i^* \leftarrow [L]$ and obtain $\mathbf{A}, \widehat{\mathbf{G}}_{i^*}, \mathsf{crs}_{i^*}$ as input; we simulate honestly as in G_2 except that for all $\mathsf{mpk}_{i^*} \in D_{i^*}$, 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 $\mathsf{mpk}_{i^*}^* \notin D_{i^*}$. Observe that once it happens that $\mathbf{e}_1\widetilde{\mathbf{G}}_{i^*}^{-1}\mathbf{Q}_{i^*}^* \neq \mathbf{sT}_{i^*}^*$, we must have $\mathbf{F}_{i^*}^* \notin \mathsf{span}^\top(\mathbf{A}_{i^*})$. When $\mathsf{mpk}_{i^*}^* \in D_{i^*}$, we always have $\mathsf{G}_3 \equiv \mathsf{G}_2$.
– G_4: Identical to G_3 except that we replace all $\mathbf{sA}$ with $\boxed{\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}}$; in particular, we generate $\widehat{\mathbf{G}}_i$ as follows:

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

  and generate the challenge ciphertext as follows:

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

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

– 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:

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

and generate the challenge ciphertext as

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

We have $\mathsf{G}_5 \equiv \mathsf{G}_4$. This follows from the fact that when $\mathbf{V}$ is uniformly sampled from $\mathbb{Z}_p^{(k+1)\times(2k+1)}$ 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 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 $\mathbf{B}_2^{\parallel}$ 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

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

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.

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

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

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):

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

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 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 crs, $\mathsf{mpk}_i \in D_i$ and $\mathbf{c}_2^*$, with highlighting relevant terms in the following sub-sequence with dashed boxes as follows:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \{[\mathbf{d}_j^\top]_2\}_{j\in[\ell-1]}, \boxed{[\mathbf{B}_1\mathbf{r}_\ell^\top]_2}, \{[\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[\ell+1,L]} \\ \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_{n_1}\otimes\mathbf{d}_j^\top)]_2\}_{j\in[\ell-1],i\in[L]\setminus\{j\}}, \\ \{\boxed{[\mathbf{W}_i(\mathbf{I}_{n_1}\otimes\mathbf{B}_1\mathbf{r}_\ell^\top)]_2}\}_{i\in[L]\setminus\{\ell\}}, \\ \{[\mathbf{W}_i(\mathbf{I}_{n_1}\otimes\mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L],i\in[L]\setminus\{j\}} \end{pmatrix},$$

$$\mathsf{mpk}_i = \begin{cases} \left([\mathbf{A}\mathbf{U}_i, \widehat{\mathbf{G}}_i\mathbf{U}_i]_1, \{[\mathbf{U}_i(\mathbf{I}_{n_2}\otimes\mathbf{d}_j^\top)]_2\}_{j\in[\ell-1]\setminus\{i\}}, \boxed{[\mathbf{U}_i(\mathbf{I}_{n_2}\otimes\mathbf{B}_1\mathbf{r}_\ell^\top)]_2}, \right. & \text{if } i \neq \ell \\ \left. \{[\mathbf{U}_i(\mathbf{I}_{n_2}\otimes\mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L]\setminus\{i\}}, \widetilde{\pi}_i \right) & \\ \left([\mathbf{A}\mathbf{U}_\ell, \widehat{\mathbf{G}}_i\mathbf{U}_\ell]_1, \{[\mathbf{U}_\ell(\mathbf{I}_{n_2}\otimes\mathbf{d}_j^\top)]_2\}_{j\in[\ell-1]}, \right. & \text{if } i = \ell \\ \left. \{[\mathbf{U}_\ell(\mathbf{I}_{n_2}\otimes\mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L]}, \widetilde{\pi}_\ell \right) & \end{cases}$$

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

  where $\mathbf{d}_j^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_2)$ for all $j \in [\ell-1]$. And when $\mathsf{mpk}_\ell^* \in D_\ell$, for each $\mathbf{f} \in \mathcal{K}_\ell$ we recall secret key returned from $\mathsf{OKey}(\ell, \mathbf{f})$ in the following form

$$\mathsf{sk}_{\ell,\mathbf{f}} = \mathbf{U}_\ell^*(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})$$

  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

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

  In particular, we change the dashed boxed term in crs, mpk_i and $\mathsf{sk}_{\ell,\mathbf{f}}$ as follows:

$$[\boxed{\mathbf{d}_\ell^\top}]_2, \{[\mathbf{W}_i(\mathbf{I}_{n_1}\otimes\boxed{\mathbf{d}_\ell^\top})]_2, [\mathbf{U}_i(\mathbf{I}_{n_2}\otimes\boxed{\mathbf{d}_\ell^\top})]_2\}_{i\in[L]\setminus\{\ell\}}$$

  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

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

  Where $\mathbf{t}_0^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_1)$ corresponding to $\mathsf{G}_{7,\ell-1,0}$, and $\mathbf{t}_1^\top \leftarrow \mathsf{span}(\mathbf{B}_3)$ 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 the detailed proof in Section 6.3.
- $\mathsf{G}_{7,\ell-1,3}$: Identical to $\mathsf{G}_{7,\ell-1,2}$ except that we replace all $\mathbf{d}_\ell^\top$ in crs with

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

  In particular, we change the dashed boxed term in crs, mpk_i and $\mathsf{sk}_{\ell,\mathbf{f}}$ as follows:

$$[\boxed{\mathbf{d}_\ell^\top}]_2, \{[\mathbf{W}_i(\mathbf{I}_{n_1}\otimes\boxed{\mathbf{d}_\ell^\top})]_2, [\mathbf{U}_i(\mathbf{I}_{n_2}\otimes\boxed{\mathbf{d}_\ell^\top})]_2\}_{i\in[L]\setminus\{\ell\}}$$

  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

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

  Where $\mathbf{t}_0^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_3)$ corresponding to $\mathsf{G}_{7,\ell-1,2}$, and $\mathbf{t}_1^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_2)$ 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, we have $\mathsf{G}_{7,\ell-1,4} = \mathsf{G}_{7,\ell}$ and this proves $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$.

6.3 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 $\mathbf{d}_j^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_2)$ with $\mathbf{B}_2 r_j$, for some $r_j \leftarrow \mathbb{Z}_p$.

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \{[\mathbf{B}_2 r_j]_2\}_{j\in[\ell-1]}, \boxed{[\mathbf{d}_\ell^\top]_2}, \{[\mathbf{B}_1 \mathbf{r}_j^\top]_2\}_{j\in[\ell+1,L]} \\ \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\mathbf{W}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_2 r_j)]_2\}_{j\in[\ell-1], i\in[L]\setminus\{j\}}, \\ \{\boxed{[\mathbf{W}_i(\mathbf{I}_{n_1} \otimes \mathbf{d}_\ell^\top)]_2}\}_{i\in[L]\setminus\{\ell\}}, \\ \{[\mathbf{W}_i(\mathbf{I}_{n_1} \otimes \mathbf{B}_1 \mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L], i\in[L]\setminus\{j\}} \end{pmatrix},$$

$$\mathsf{mpk}_i = \begin{cases} \begin{pmatrix} [\mathbf{A}\mathbf{U}_i, \widehat{\mathbf{G}}_i \mathbf{U}_i]_1, \{[\mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_2 r_j)]_2\}_{j\in[\ell-1]\setminus\{i\}}, \boxed{[\mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{d}_\ell^\top)]_2}, \\ \{[\mathbf{U}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1 \mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L]\setminus\{i\}}, \widetilde{\pi}_i \end{pmatrix} & \text{if } i \neq \ell \\ \begin{pmatrix} [\mathbf{A}\mathbf{U}_\ell, \widehat{\mathbf{G}}_i \mathbf{U}_\ell]_1, \{[\mathbf{U}_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_2 r_j^\top)]_2\}_{j\in[\ell-1]}, \\ \{[\mathbf{U}_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_1 \mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L]}, \widetilde{\pi}_\ell \end{pmatrix} & \text{if } i = \ell \end{cases}$$

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

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

where $\mathbf{d}_\ell^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_3)$. We define $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$ and $\mathbf{c}\mathbf{c}^\perp = 1$, this use the facts that $\binom{\mathbf{A}}{\mathbf{c}}$ is (row) full-rank w.h.p. With the orthogonality of dual basis, for all $\mathbf{v}^{(3)} \in \mathsf{span}(\mathbf{B}_3^\parallel)$, 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) mpk_ℓ^* is honest; (2) mpk_ℓ^* is corrupted or maliciously generated by the adversary.

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

Lemma 5. *For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ such that $\binom{\mathbf{A}}{\mathbf{c}}\mathbf{c}^\perp = \binom{\mathbf{0}}{1}$; any basis $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B}_2 \leftarrow \mathbb{Z}_p^{(2k+1)}$, $\mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, with dual basis $\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel$, and any $\mathbf{d}^\perp \in \mathsf{span}(\mathbf{B}_3^\parallel)$ such that $\mathbf{d}^\perp\mathbf{B}_1 = \mathbf{0}$ and $\mathbf{d}^\perp\mathbf{B}_2 = 0$; for any $\widehat{\mathbf{x}} \in \mathbb{Z}_p^{1\times n}$ and $\mathcal{K}_\ell$; and for any adversary $\mathcal{A}$, there exist an adversary $\mathcal{B}_2$ such that*

$$\left| \Pr\left[\mathcal{A}\begin{pmatrix} [\mathbf{A}]_1, \mathbf{c}, [\mathbf{G}]_1, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{d}^\perp, [\mathbf{A}\mathbf{U}]_1, \mathbf{c}\mathbf{U}, \\ [\mathbf{G}\mathbf{U}]_1, \mathbf{U}(\mathbf{I}_n \otimes (\mathbf{B}_1\|\mathbf{B}_2)), \{\mathbf{U}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})\}_{\mathbf{f}\in\mathcal{K}_\ell} \end{pmatrix} = 1\right] - \right.$$

$$\left. \Pr\left[\mathcal{A}\begin{pmatrix} [\mathbf{A}]_1, \mathbf{c}, [\mathbf{G}]_1, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{d}^\perp, [\mathbf{A}\mathbf{U}]_1, \mathbf{c}\mathbf{U} + \boxed{\widehat{\mathbf{x}} \otimes \mathbf{d}^\perp}, \\ [\mathbf{G}\mathbf{U}]_1, \mathbf{U}(\mathbf{I}_n \otimes (\mathbf{B}_1\|\mathbf{B}_2)), \{\mathbf{U}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \boxed{\mathbf{c}^\perp(\widehat{\mathbf{x}}\mathbf{f}^\top \otimes \mathbf{d}^\perp)}\}_{\mathbf{f}\in\mathcal{K}_\ell} \end{pmatrix} = 1\right] \right|$$

$$\leq \quad 2 \cdot \mathsf{Adv}_{\mathcal{B}_2}^{MDDH} + \mathsf{negl}(\lambda)$$

where $\mathbf{G} \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$, $\mathbf{U} \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)}$.

We provide the proof of Lemma 5 in Appendix A.

Honest Case. In this case, we have $\mathsf{mpk}^*_\ell = ([\mathbf{T}^*_\ell, \mathbf{Q}^*_\ell]_1, \{[\mathbf{H}^*_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}}, \pi^*_\ell) \in D_\ell \setminus C_\ell$. Namely we know $\mathbf{U}^*_\ell$ (such that $\mathbf{T}^*_\ell = \mathbf{A}\mathbf{U}^*_\ell$ and $\mathbf{Q}^*_\ell = \widehat{\mathbf{G}}_\ell\mathbf{U}^*_\ell$), we can write the dashboxed terms in $\mathbf{c}^*_1$ as follows:

$$\boxed{\mathbf{c}\mathbf{U}^*_\ell} + \mathbf{c}\mathbf{W}_\ell(\mathbf{M}^*_\ell \otimes \mathbf{I}_{2k+1})$$

and replace $\widehat{\mathbf{R}}_\ell$ in crs with a random $\mathbf{R}_\ell$ as in G_1. And in this case, $\mathbf{U}^*_\ell$ is hidden from the adversary, the adversary can only obtain secret keys as follows:

$$\boxed{\mathbf{U}^*_\ell}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) \quad \forall \mathbf{f} \in \mathcal{K}_\ell$$

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 this case:

$$\begin{aligned}
& [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, [\mathbf{A}\mathbf{W}_\ell]_1, \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_2) && \text{//crs, } \mathsf{mpk}_\ell \\
& \mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\mathbf{M}^*_\ell \otimes \mathbf{I}_{2k+1}), \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell && \text{//ct}^* \\
& [\mathbf{A}\mathbf{U}^*_\ell]_1, [\mathbf{G}_\ell\mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_1), \mathbf{U}^*_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_2) && \text{//mpk}^*_\ell \\
& \{\mathbf{U}^*_\ell(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})\}_{\mathbf{f}\in\mathcal{K}_\ell} && \text{//}\{\mathsf{sk}_{\ell,\mathbf{f}}\}_{\mathbf{f}\in\mathcal{K}_\ell} \\
\approx_c\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, [\mathbf{A}\mathbf{W}_\ell]_1, \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \boxed{(\mathbf{x}^*_{b'} - \mathbf{x}^*_0)\mathbf{M}^*_\ell \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_\ell(\mathbf{M}^*_\ell \otimes \mathbf{I}_{2k+1}), \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell \\
& [\mathbf{A}\mathbf{U}^*_\ell]_1, [\mathbf{G}_\ell\mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_1), \mathbf{U}^*_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_2) \\
& \{\mathbf{U}^*_\ell(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \boxed{\mathbf{c}^\perp((\mathbf{x}^*_{b'} - \mathbf{x}^*_0\mathbf{M}^*_\ell\mathbf{f}^\top) \otimes \mathbf{v}^{(3)})}\}_{\mathbf{f}\in\mathcal{K}_\ell} \\
\approx_s\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, [\mathbf{A}\mathbf{W}_\ell]_1, \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \cancel{(\mathbf{x}^*_{b'} - \mathbf{x}^*_0)\mathbf{M}^*_\ell \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_\ell(\mathbf{M}^*_\ell \otimes \mathbf{I}_{2k+1}), \boxed{\mathbf{x}^*_0} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell \\
& [\mathbf{A}\mathbf{U}^*_\ell]_1, [\mathbf{G}_\ell\mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_1), \mathbf{U}^*_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_2) \\
& \{\mathbf{U}^*_\ell(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \mathbf{c}^\perp((\mathbf{x}^*_{b'} - \mathbf{x}^*_0\mathbf{M}^*_\ell\mathbf{f}^\top) \otimes \mathbf{v}^{(3)})\}_{\mathbf{f}\in\mathcal{K}_\ell} \\
=\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, [\mathbf{A}\mathbf{W}_\ell]_1, \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{c}\mathbf{U}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\mathbf{M}^*_\ell \otimes \mathbf{I}_{2k+1}), \mathbf{x}^*_0 \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell \\
& [\mathbf{A}\mathbf{U}^*_\ell]_1, [\mathbf{G}_\ell\mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_1), \mathbf{U}^*_\ell(\mathbf{I}_{n_2} \otimes \mathbf{B}_2) \\
& \{\mathbf{U}^*_\ell(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \cancel{\mathbf{c}^\perp((\mathbf{x}^*_{b'} - \mathbf{x}^*_0\mathbf{M}^*_\ell\mathbf{f}^\top) \otimes \mathbf{v}^{(3)})}\}_{\mathbf{f}\in\mathcal{K}_\ell}
\end{aligned}$$

We justify each step as below: The first $\approx_c$ uses Lemma 5 with $n = n_2, \mathbf{G} = \mathbf{G}_\ell, \mathbf{U} = \mathbf{U}^*_\ell, \mathbf{d}^\perp = \mathbf{v}^{(3)}$ and $\widehat{\mathbf{x}} = (\mathbf{x}^*_{b'} - \mathbf{x}^*_0)\mathbf{M}^*_\ell$. The second $\approx_s$ uses change of variables

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

The last = follows from the fact that $(\mathbf{x}^*_{b'} - \mathbf{x}^*_0)\mathbf{M}^*_\ell\mathbf{f}^\top = 0$ for all $\mathbf{f} \in \mathcal{K}_\ell$.

Corrupted & Malicious Case. In this case, we have $\mathsf{mpk}^*_\ell = ([\mathbf{T}^*_\ell, \mathbf{Q}^*_\ell]_1, \{[\mathbf{H}^{*\top}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}}, \pi^*_\ell) \in C_\ell \cup \overline{D}_\ell$. It's required that $\mathbf{x}^*_0\mathbf{M}^*_i = \mathbf{x}^*_1\mathbf{M}^*_i$. In this case, the adversary knows the corresponding msk^*_ℓ and can generate $\mathsf{sk}_{\ell,\mathbf{f}}$ for any $\mathbf{f}$. Without losing generality, we don't consider the secret keys returned from $\mathsf{OKey}(\ell, \cdot)$ in this case[7]. Let's use

[7] Notice that, $\mathsf{OKey}(\ell, \cdot)$ will return valid secret keys in the corrupted case; and will return $\perp$ in the malicious case

$\mathbf{x}^*_{b'}$ 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 this case:

$$
\begin{aligned}
& \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_2) && \text{//crs} \\
& \mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{G}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\mathbf{M}^*_\ell \otimes \mathbf{I}_{2k+1}), \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell && \text{//ct}^* \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{G}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\mathbf{M}^*_\ell \otimes \mathbf{I}_{2k+1}) - \boxed{(\mathbf{x}^*_{b'} - \mathbf{x}^*_0)\mathbf{M}^*_\ell \otimes \mathbf{v}^{(3)}}, \boxed{\mathbf{x}^*_0 \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_\ell \\
=\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}^\top_\ell, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{n_1} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{e}_1\widetilde{\mathbf{G}}^{-1}_\ell\mathbf{Q}^*_\ell + \mathbf{c}\mathbf{W}_\ell(\mathbf{M}^*_\ell \otimes \mathbf{I}_{2k+1}) - \cancel{(\mathbf{x}^*_{b'} - \mathbf{x}^*_0)\mathbf{M}^*_\ell \otimes \mathbf{v}^{(3)}}, \mathbf{x}^*_0 \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_\ell
\end{aligned}
$$

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

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

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

7 Slotted Reg-ABE with Delegated IPFE from Pairings

In this section, we propose the construction of slotted Reg-ABE with delegated IPFE, which is covered by the notion of slotted delegated Reg-FE. In particular, a (slotted) Reg-ABE with delegated IPFE for predicate $P : X \times Y \to \{0,1\}$ and inner-product functionality $\mathsf{IP}_{n'} = \{\mathbf{f} : \mathbf{x} \mapsto \mathbf{x}\mathbf{f}^\top\}$ can be seen as a delegated Reg-FE for induced functionalities:

$$G_P : X \times \mathbb{Z}_p^{n'} \to (\mathbb{Z}_p^{n'} \cup \{\perp\}) \quad \text{and} \quad F_{\mathsf{IP}} : (\mathbb{Z}_p^{n'} \cup \{\perp\}) \to (\mathbb{Z}_p \cup \{\perp\})$$

where for all $g_y \in G_P$ and $f_{\mathbf{f}} \in F_{\mathsf{IP}}$, we have

$$g_y(x, \mathbf{x}) = \begin{cases} \mathbf{x} & \text{if } P(x,y) = 1 \\ \perp & \text{if } P(x,y) = 0 \end{cases} \quad \text{and} \quad f_{\mathbf{f}}(\mathbf{x}) = \begin{cases} \mathbf{x}\mathbf{f}^\top & \text{if } \mathbf{x} \in \mathbb{Z}_p^{n'} \\ \perp & \text{if } \mathbf{x} = \perp \end{cases}$$

And we recall in this section:

- for correctness, we consider
$$f_{\mathbf{f}} \circ g_y(x, \mathbf{x}) = \mathbf{x}\mathbf{f}^\top \quad \text{when} \quad P(x,y) = 1;$$
- for security, we consider the challenge as $(x^*, \mathbf{x}^*_b)$ for $b \in \{0,1\}$, and consider the requirements as

$$
\begin{aligned}
g_y(x^*, \mathbf{x}^*_0) = g_y(x^*, \mathbf{x}^*_1) &\implies P(x^*, y) = 0 \\
f_{\mathbf{f}} \circ g_y(x^*, \mathbf{x}^*_0) = f_{\mathbf{f}} \circ g_y(x^*, \mathbf{x}^*_1) &\implies P(x^*, y) = 0 \vee \mathbf{x}^*_0\mathbf{f}^\top = \mathbf{x}^*_1\mathbf{f}^\top
\end{aligned}
$$

Our construction is based on predicate encodings (c.f. Section 3.2) and achieves the IND-security under MDDH assumption. By the Remark 1 and generic transformation in Section 10, this yields a Reg-ABE with delegated IPFE (Reg-FE for above induced functionalities) via predicate encodings under MDDH assumption.

7.1 Scheme

Assuming QA-NIZK $\Pi = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ for $\mathbb{G}_1$-linear space over bilinear groups, see Section 3.3, our slotted Reg-ABE with delegated IPFE in prime-order bilinear groups works as follows:

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

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

Sample

$$\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k},\ \mathbf{B}_2 \leftarrow \mathbb{Z}_p^{(2k+1)\times 1},\ \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$$

and compute the dual basis $(\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel)$ (see section 3.1). And compute parameter (n, n_c, n_k) from P (see section 3.2). For all, sample

$$\mathbf{V}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)n'},\ \mathbf{W}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)nn'},\ \mathbf{G}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)},\ \mathbf{r}_i \leftarrow \mathbb{Z}_p^{1\times k}$$

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

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

Output

$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \mathbf{AV}]_1, \left\{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{AV}_i, \mathbf{AW}_i]_1\right\}_{i\in[L]}, \left\{[\mathbf{B}_1\mathbf{r}_j^\top]_2\right\}_{j\in[L]} \\ \left\{[\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top), \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\right\}_{j\in[L], i\in[L]\setminus\{j\}} \end{array} \right).$$

Notice that we do not use $\mathsf{td}_1, \ldots, \mathsf{td}_L$ and $\mathbf{B}_2, \mathbf{B}_3$, $(\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel)$ in the actual scheme.

– $\mathsf{Gen}(\mathsf{crs}, i)$: Sample $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)n'}$. Define $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i} = \binom{\mathbf{AU}_i}{\mathbf{G}_i\mathbf{U}_i} = \mathbf{A}_i\mathbf{U}_i \in \mathbb{Z}_p^{(2k+2)\times(2k+1)n'}$ and run

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

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

$$\mathsf{mpk}_i = \Big([\underbrace{\mathbf{AU}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{G}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{\underbrace{[\mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2}_{\mathbf{H}_{i,j}}\}_{j\in[L]\setminus\{i\}}, \pi_i\Big) \quad \text{and} \quad \mathsf{msk}_i = \mathbf{U}_i.$$

– $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i)$: Parse $\mathsf{mpk}_i = \big([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{H}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$. 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

$$e([\mathbf{A}]_1, [\mathbf{H}_{i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_i]_1, [\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top]_2).$$

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

– $\mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i, y_i)_{i\in[L]})$: For all $i \in [L]$, compute $\mathbf{a}_{y_i}, \mathbf{K}_{y_i}$ from y_i, and parse $\mathsf{mpk}_i = \big([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{H}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$. Output:

$$\mathsf{mpk}_+ = \left(\left[\mathbf{A}, \sum_{i\in[L]}(\mathbf{AV}_i + \mathbf{T}_i), \sum_{i\in[L]}\mathbf{AW}_i, \sum_{i\in[L]}\big(\mathbf{AV}_i(\mathbf{a}_{y_i} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{AW}_i(\mathbf{K}_{y_i} \otimes \mathbf{I}_{(2k+1)n'})\big), \mathbf{AV}\right]_1\right)$$

and for all $j \in [L]$

$$\mathsf{hsk}_j = \left(\begin{array}{l} \Bigg[\overbrace{\mathbf{B}_1\mathbf{r}_j^\top}^{\mathbf{k}_{j,0}^\top}, \overbrace{\sum_{i\in[L]\setminus\{j\}}\mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)}^{\mathbf{K}_{j,1}}, \overbrace{\sum_{i\in[L]\setminus\{j\}}(\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top) + \mathbf{H}_{i,j})}^{\mathbf{K}_{j,2}}\Bigg]_2, \\ \underbrace{\Bigg[\sum_{i\in[L]\setminus\{j\}}(\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)(\mathbf{a}_{y_i} \otimes \mathbf{I}_{n'}) + \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)(\mathbf{K}_{y_i} \otimes \mathbf{I}_{n'}))\Bigg]_2}_{\mathbf{K}_{j,3}} \end{array} \right).$$

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

$$\mathsf{ct}_x = \left(\begin{bmatrix} \overbrace{\mathbf{sA}}^{\mathbf{c}_0}, \overbrace{\mathbf{x}\otimes\mathbf{sAV} + \sum_{i\in[L]}(\mathbf{sAV}_i + \mathbf{sT}_i)}^{\mathbf{c}_1}, \overbrace{\sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{C}_x \otimes \mathbf{I}_{(2k+1)n'})}^{\mathbf{c}_2} \end{bmatrix}_1, \\ \underbrace{\begin{bmatrix} \sum_{i\in[L]} \left(\mathbf{sAV}_i(\mathbf{a}_{y_i}\otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{sAW}_i(\mathbf{K}_{y_i}\otimes \mathbf{I}_{(2k+1)n'})\right), \underbrace{\mathbf{sAV}}_{\mathbf{c}_4} \end{bmatrix}_1}_{\mathbf{c}_3} \right).$$

– $\mathsf{Key}(\mathsf{msk}_{j^*}, \mathsf{hsk}_{j^*}, \mathbf{f})$: Parse $\mathsf{msk}_{j^*} = \mathbf{U}_{j^*}$. Output

$$\mathsf{sk}_{j^*,\mathbf{f}} = \underbrace{\mathbf{U}_{j^*}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})}_{\mathbf{K}_0}$$

– $\mathsf{Dec}(\mathsf{sk}_{j^*,\mathbf{f}}, \mathsf{hsk}_{j^*}, \mathsf{ct}_x)$: Parse

$$\mathsf{sk}_{j^*,\mathbf{f}} = \mathbf{K}_0, \quad \mathsf{hsk}_{j^*} = ([\mathbf{k}_{j^*,0}, \mathbf{K}_{j^*,1}, \mathbf{K}_{j^*,2}, \mathbf{K}_{j^*,3}]_2), \quad \mathsf{ct}_x = ([\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4]_1)$$

Recover

$$\begin{aligned} [\mathbf{z}_1]_T &= e([\mathbf{c}_1]_1, [\mathbf{I}_{n'} \otimes \mathbf{k}_{j^*,0}^\top]_2), & [\mathbf{z}_2]_T &= e([\mathbf{c}_0]_1, [\mathbf{K}_{j^*,2}]_2); \\ [\mathbf{z}_3]_T &= e([\mathbf{c}_3 \| \mathbf{c}_2]_1, [\mathbf{I}_{n_k+n_c} \otimes (\mathbf{I}_{n'} \otimes \mathbf{k}_{j^*,0}^\top)]_2), & [\mathbf{z}_4]_T &= e([\mathbf{c}_0]_1, [\mathbf{K}_{j^*,3} \| \mathbf{K}_{j^*,1}(\mathbf{C}_x \otimes \mathbf{I}_{n'})]); \\ [z_5]_T &= e([\mathbf{c}_4]_1, [\mathbf{k}_{j^*,0}^\top])2), & [z_6]_T &= e([\mathbf{c}_0]_1, [\mathbf{K}_0 \mathbf{k}_{j^*,0}^\top]_2). \end{aligned}$$

Compute $\mathbf{d}_{x,y_{j^*}}$ from x and y_{j^*}, compute

$$[z']_T = [(\mathbf{z}_1 - \mathbf{z}_2)\mathbf{f}^\top - (\mathbf{z}_3 - \mathbf{z}_4)(\mathbf{d}_{x,y_{j^*}}^\top \otimes \mathbf{I}_{n'})\mathbf{f}^\top - z_6]_T.$$

Recover z from $[z']_T$ over $[z_5]_T$ via brute-force DLOG and output z.

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

$$\mathsf{mpk}_i = \left([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{H}_{i,j}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\right) = \left([\mathbf{AU}_i, \mathbf{G}_i\mathbf{U}_i]_1, \{[\mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[L]\setminus\{i\}}, \pi_i\right)$$

for some $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(2k+1)n'}$ 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 $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{G}_i}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{G}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. Then

– Write $\mathbf{F}_i = \binom{\mathbf{T}_i}{\mathbf{Q}_i} = \binom{\mathbf{AU}_i}{\mathbf{G}_i\mathbf{U}_i}$, we have $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \pi_i) = 1$ by the perfect completeness of Π (see Section 3.3) and the fact that $\mathbf{F}_i = \mathbf{A}_i\mathbf{U}_i$;
– For each $j \in [L] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2) = e([\mathbf{AU}_i]_1, [\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top]_2)$ by the definition of bilinear map e (see Section 3.1) and the fact that $\mathbf{A} \cdot \mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top) = \mathbf{AU}_i \cdot (\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)$.

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

Correctness. For all $\lambda, L, n' \in \mathbb{N}$, all P, all $j^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, P, 1^{n'}, 1^L)$, all $(\mathsf{mpk}_{j^*}, \mathsf{msk}_{j^*}) \leftarrow \mathsf{Gen}(\mathsf{crs}, j^*)$, all $\{\mathsf{mpk}_i\}_{i\in[L]\setminus\{j^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i) = 1$, for all $y_1, \ldots, y_L \in Y$ and $x \in X$ with $P(x, y_{j^*}) = 1$; and for all

$\mathbf{x} \in \mathbb{Z}_p^{n'}$, $\mathbf{f} \in \mathbb{Z}_p^{n'}$, we have:

$$\mathsf{sk}_{j^*,\mathbf{f}} = \underbrace{\mathbf{U}_{j^*}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})}_{\mathbf{K}_0},$$

$$\mathsf{hsk}_{j^*} = \begin{pmatrix} \Big[\overbrace{\mathbf{B}_1\mathbf{r}_{j^*}^\top}^{\mathbf{k}_{j^*,0}^\top}, \overbrace{\sum_{i\in[L]\setminus\{j^*\}} \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)}^{\mathbf{K}_{j^*,1}}, \overbrace{\sum_{i\in[L]\setminus\{j^*\}} (\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \mathbf{H}_{i,j^*})}^{\mathbf{K}_{j,2}} \Big]_2, \\ \underbrace{\Big[\sum_{i\in[L]\setminus\{j^*\}} (\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)(\mathbf{a}_{y_i} \otimes \mathbf{I}_{n'}) + \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)(\mathbf{K}_{y_i} \otimes \mathbf{I}_{n'})) \Big]_2}_{\mathbf{K}_{j^*,3}} \end{pmatrix},$$

$$\mathsf{ct}_x = \begin{pmatrix} \Big[\overbrace{\mathbf{sA}}^{\mathbf{c}_0}, \overbrace{\mathbf{x} \otimes \mathbf{sAV} + \sum_{i\in[L]} (\mathbf{sAV}_i + \mathbf{sT}_i)}^{\mathbf{c}_1}, \overbrace{\sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{C}_x \otimes \mathbf{I}_{(2k+1)n'})}^{\mathbf{c}_2} \Big]_1, \\ \Big[\underbrace{\sum_{i\in[L]} \big(\mathbf{sAV}_i(\mathbf{a}_{y_i} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{sAW}_i(\mathbf{K}_{y_i} \otimes \mathbf{I}_{(2k+1)n'})\big)}_{\mathbf{c}_3}, \underbrace{\mathbf{sAV}}_{\mathbf{c}_4} \Big]_1 \end{pmatrix}$$

where

$$\mathbf{AH}_{i,j^*} = \mathbf{T}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) \quad \forall i \in [L] \setminus \{j^*\} \quad \text{and} \quad \mathbf{T}_{j^*} = \mathbf{AU}_{j^*}.$$

Note that in Key and Dec, we actually consider hsk_j for $j = j^*$ and msk_i for $i = j^*$; and all above equalities are ensured by Ver, Gen and Key. Then, as in Section 3.2, let

$$\mathbf{M}_{x,y_i} = \begin{pmatrix} \mathbf{a}_{y_i} & \mathbf{0}_{n_c} \\ \mathbf{K}_{y_i} & \mathbf{C}_x \end{pmatrix}, \quad \forall i \in [L]$$

we have

$$\begin{aligned}
\mathbf{z}_1 &= (\mathbf{x} \otimes \mathbf{sAV})(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \sum_{i\in[L]} (\mathbf{sAV}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \mathbf{sT}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)) \\
&= \mathbf{x} \otimes \mathbf{sAVB}_1\mathbf{r}_{j^*}^\top + \sum_{i\in[L]} (\mathbf{sAV}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \mathbf{sT}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)) \qquad (20) \\
&= \mathbf{sAVB}_1\mathbf{r}_{j^*}^\top \cdot \mathbf{x} + \sum_{i\in[L]} (\mathbf{sAV}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \mathbf{sT}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)) \\
\mathbf{z}_2 &= \sum_{i\in[L]\setminus\{j^*\}} (\mathbf{sAV}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) + \mathbf{sAH}_{i,j^*}) \\
\mathbf{z}_3 &= \sum_{i\in[L]} (\mathbf{sAV}_i \| \mathbf{sAW}_i)(\mathbf{M}_{x,y_i} \otimes \mathbf{I}_{(2k+1)n'})(\mathbf{I}_{n_k+n_c} \otimes (\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)) \\
&= \sum_{i\in[L]} (\mathbf{sAV}_i \| \mathbf{sAW}_i)(\mathbf{I}_{1+n} \otimes (\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top))(\mathbf{M}_{x,y_i} \otimes \mathbf{I}_{n'}) \qquad (21) \\
&= \sum_{i\in[L]} (\mathbf{sAV}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) \| \mathbf{sAW}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top))(\mathbf{M}_{x,y_i} \otimes \mathbf{I}_{n'}) \\
\mathbf{z}_4 &= \sum_{i\in[L]\setminus\{j^*\}} (\mathbf{sAV}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top) \| \mathbf{sAW}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top))(\mathbf{M}_{x,y_i} \otimes \mathbf{I}_{n'}) \\
z_5 &= \mathbf{sAVB}_1\mathbf{r}_{j^*}^\top \\
z_6 &= \mathbf{sAU}_{j^*}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})\mathbf{B}_1\mathbf{r}_{j^*}^\top \\
&= \mathbf{sAU}_{j^*}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_{j^*}^\top)\mathbf{f}^\top \qquad (22)
\end{aligned}$$

and then

$$
\begin{aligned}
[z']_T &= [(\mathbf{z}_1 - \mathbf{z}_2)\mathbf{f}^\top - (\mathbf{z}_3 - \mathbf{z}_4)(\mathbf{d}^\top_{x,y_{j^*}} \otimes \mathbf{I}_{n'})\mathbf{f}^\top - z_6]_T \\
&= [\mathbf{sAVB}_1\mathbf{r}^\top_{j^*} \cdot \mathbf{xf}^\top + (\mathbf{sAV}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}^\top_{j^*})\mathbf{f}^\top + \mathbf{sAU}_{j^*}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}^\top_{j^*})\mathbf{f}^\top) \\
&\quad -(\mathbf{sAV}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}^\top_{j^*})\|\mathbf{sAW}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}^\top_{j^*}))(\mathbf{M}_{x,y_{j^*}} \otimes \mathbf{I}_{n'})(\mathbf{d}^\top_{x,y_{j^*}} \otimes \mathbf{I}_{n'})\mathbf{f}^\top \\
&\quad -\mathbf{sAU}_{j^*}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}^\top_{j^*})\mathbf{f}^\top]_T && (23) \\
&= [\mathbf{sAVB}_1\mathbf{r}^\top_{j^*} \cdot \mathbf{xf}^\top + \mathbf{sAV}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}^\top_{j^*})\mathbf{f}^\top - \mathbf{sAV}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}^\top_{j^*}]_T && (24) \\
&= [\mathbf{sAVB}_1\mathbf{r}^\top_{j^*} \cdot \mathbf{xf}^\top]_T && (25)
\end{aligned}
$$

Here, equalities (20), (21) and (22) follow 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 (23) follows from the fact that $\mathbf{AH}_{i,j^*} = \mathbf{T}_i(\mathbf{I}_{n_2} \otimes \mathbf{B}_1\mathbf{r}^\top_{j^*})$ for all $i \in [L] \setminus \{j^*\}$ and the fact that $\mathbf{T}_{j^*} = \mathbf{AU}_{j^*}$; equality (24) follows from the correctness of predicate encodings. Treat $[z_5]_T = [\mathbf{sAVB}_1\mathbf{r}^\top_{j^*}]_T$ as the basis, and recover z from $[z']_T = [\mathbf{sAVB}_1\mathbf{r}^\top_{j^*} \cdot \mathbf{xf}^\top]_T$ via brute-force DLOG, we have

$$z = \mathbf{xf}^\top$$

This proves the correctness.

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

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

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] under MDDH assumption and the fact that MDDH assumption implies subspace decision assumption [CGKW18], our scheme of slotted Reg-ABE with delegated IPFE uses prime-order bilinear group and the security can be reduced to MDDH assumption.

Theorem 3. *Assume $\Pi = (\mathsf{LGen}, \mathsf{LPrv}, \mathsf{LVer}, \mathsf{LSim})$ is QA-NIZKs with perfect completeness, perfect zero-knowledge and unbounded simulation soundness for $\mathbb{G}_1$-linear space defined in Section 3.3, our scheme of slotted Reg-ABE with delegated IPFE achieves the adaptive IND-security defined in Section 4.1 (with the consideration we have mentioned in the beginning of this section) under MDDH assumption.*

7.2 Proof

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

Lemma 6. *For all adversaries $\mathcal{A}$, there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$, $\mathcal{B}_4$ such that:*

$$\mathsf{Adv}^{\textit{Ad-sReg-FE+Del-ABE}}_{\mathcal{A}}(\lambda) \le L \cdot \mathsf{Adv}^{\textit{USS}}_{\mathcal{B}_1}(\lambda) + (8L+1)\mathsf{Adv}^{\textit{MDDH}}_{\mathcal{B}_2}(\lambda) + L \cdot \mathsf{Adv}^{\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_1\mapsto\mathbf{B}_3}}_{\mathcal{B}_3}(\lambda) + L \cdot \mathsf{Adv}^{\mathsf{SD}^{\mathbb{G}_2}_{\mathbf{B}_3\mapsto\mathbf{B}_2}}_{\mathcal{B}_4}(\lambda) + \mathsf{negl}(\lambda)$$

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 and x^* is the challenge "attribute", $\{\mathsf{mpk}_i^*, y_i^*\}_{i\in[L]}$ are challenge mater public keys along with challenge "policy" to be registered. For all $i \in [L]$, define $D_i = \{\mathsf{mpk}_i : \mathcal{D}_i[\mathsf{mpk}_i] = \mathsf{msk}_i \neq \perp\}$ be responses to $\mathsf{OGen}(i)$, $C_i = \{\mathsf{mpk}_i : (i, \mathsf{mpk}_i) \in C\}$ records master public keys in D_i that have been sent to $\mathsf{OCor}(i, \cdot)$; recall that $\mathcal{K}_i$ is the list that record the queries to $\mathsf{OKey}(i, \cdot)$. For each $i \in [L]$, we have the restrictions as follow

$$\begin{aligned} \mathsf{mpk}_i^* \notin D_i &\implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i^*) = 1 \wedge \mathcal{K}_i = \emptyset, \\ \mathsf{mpk}_i^* \in C_i \vee \mathsf{mpk}_i^* \notin D_i &\implies P(x^*, y_i^*) = 0, \\ \mathbf{f} \in \mathcal{K}_i &\implies P(x^*, y_i^*) = 0 \vee \left(\mathbf{x}_0^* \mathbf{f}^\top = \mathbf{x}_1^* \mathbf{f}^\top\right). \end{aligned} \tag{26}$$

Note that mpk_i serves as a *general* entry in D_i while mpk_i^* is the *specific* challenge public for slot i; for $\mathsf{mpk}_i \in D_i$, there can be more than one assignments, since the adversary can invoke $\mathsf{OGen}(i)$ for many times. We prove the Lemma 6 via the 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:
$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \mathbf{AV}]_1, \left\{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{AV}_i, \mathbf{AW}_i]_1\right\}_{i\in[L]}, \left\{[\mathbf{B}_1\mathbf{r}_j^\top]_2\right\}_{j\in[L]} \\ \left\{[\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top), \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\right\}_{j\in[L], i\in[L]\setminus\{j\}} \end{array} \right).$$
    where $\mathsf{crs}_i \in \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$, $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{G}_i}$.
  - For each $i \in [L]$, each $\mathsf{mpk}_i \in D_i$ is in the form:
$$\mathsf{mpk}_i = \big([\underbrace{\mathbf{AU}_i}_{\mathbf{T}_i}, \underbrace{\mathbf{G}_i\mathbf{U}_i}_{\mathbf{Q}_i}]_1, \{\underbrace{[\mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2}_{\mathbf{H}_{i,j}}\}_{j\in[L]\setminus\{i\}}, \pi_i\big)$$
    where $\pi_i \leftarrow \mathsf{LPrv}(\mathsf{crs}_i, [\mathbf{F}_i]_1, \mathbf{U}_i)$, $\mathbf{F}_i = \binom{\mathbf{AU}_i}{\mathbf{G}_i\mathbf{U}_i}$, and $\mathbf{U}_i$ is the corresponding msk_i.
  - For all $i \in [L]$, mpk_i^* is in the form:
$$\mathsf{mpk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{H}_{i,j}^*]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$$
    such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i^*) = 1$ which means $\mathsf{LVer}\left(\mathsf{crs}_i, \begin{bmatrix}\mathbf{T}_i^* \\ \mathbf{Q}_i^*\end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{AH}_{i,j}^* = \mathbf{T}_i^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)$ for each $j \in [L] \setminus \{i\}$.
  - For each $j \in [L]$ such that $\mathsf{mpk}_j^* \in D_j$, and each $\mathbf{f} \in \mathcal{K}_j$, the secret key returned from $\mathsf{OKey}(j, \mathbf{f})$ are in the form:
$$\mathsf{sk}_{j,\mathbf{f}} = \mathbf{U}_j^*(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})$$
    where $\mathbf{U}_j^* = \mathsf{msk}_j^* = \mathcal{D}_j[\mathsf{mpk}_j^*]$.
  - ct^* for $(\mathbf{x}_0^*, \mathbf{x}_1^*)$ is in the form:
$$\mathsf{ct}_{x^*}^* = \left(\begin{array}{l} \Big[\overbrace{\mathbf{sA}}^{\mathbf{c}_0^*}, \overbrace{\mathbf{x}_b^* \otimes \mathbf{sAV} + \sum_{i\in[L]}(\mathbf{sAV}_i + \mathbf{sT}_i)}^{\mathbf{c}_1^*}, \overbrace{\sum_{i\in[L]} \mathbf{sAW}_i(\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'})}^{\mathbf{c}_2^*}\Big]_1, \\ \Big[\underbrace{\sum_{i\in[L]} \left(\mathbf{sAV}_i(\mathbf{a}_{y_i^*} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{sAW}_i(\mathbf{K}_{y_i^*} \otimes \mathbf{I}_{(2k+1)n'})\right)}_{\mathbf{c}_3^*}, \underbrace{\mathbf{sAV}}_{\mathbf{c}_4^*}\Big]_1 \end{array} \right).$$
    where $b \leftarrow \{0, 1\}$ is the secret bit.

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

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

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

– 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 $\mathbf{G}_i$ in crs with

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

We have $\mathsf{G}_2 \equiv \mathsf{G}_1$. This follows from the fact that both $\mathbf{G}_i$ (in G_1) and $\widehat{\mathbf{G}}_i$ (in G_2) are truly random since matrix $\left(\begin{smallmatrix} \mathbf{s}\mathbf{A} \\ \mathbf{I}_{k+1} \end{smallmatrix}\right)$ is full-rank.

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

$$\mathbf{c}_1^* = \mathbf{x}_b^* \otimes \mathbf{s}\mathbf{A}\mathbf{V} + \sum_{i\in[L]} (\mathbf{s}\mathbf{A}\mathbf{V}_i + \boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_i^*})$$

We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from stronger unbounded simulation soundness of Π along with the fact that $\mathsf{LVer}(\mathsf{crs}_i, [\mathbf{F}_i^*]_1, \pi_i^*) = 1$ for all $i \in [L]$ where $\mathbf{F}_i^* = \begin{pmatrix} \mathbf{T}_i^* \\ \mathbf{Q}_i^* \end{pmatrix}$. Assume $\mathsf{mpk}_{i^*}^* \notin D_{i^*}$, i.e., $\mathsf{mpk}_{i^*}^*$ is malicious. In the reduction, we guess $i^* \leftarrow [L]$ and obtain $\mathbf{A}, \widehat{\mathbf{G}}_{i^*}, \mathsf{crs}_{i^*}$ as input; we simulate honestly as in G_2 except that for all $\mathsf{mpk}_{i^*} \in D_{i^*}$, 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 $\mathsf{mpk}_{i^*}^* \notin D_{i^*}$. Observe that once it happens that $\mathbf{e}_1\widetilde{\mathbf{G}}_{i^*}^{-1}\mathbf{Q}_{i^*}^* \neq \mathbf{s}\mathbf{T}_{i^*}^*$, we must have $\mathbf{F}_{i^*}^* \notin \mathsf{span}^\top(\mathbf{A}_{i^*})$. When $\mathsf{mpk}_{i^*}^* \in D_{i^*}$, we always have $\mathsf{G}_3 \equiv \mathsf{G}_2$.

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

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

and generate the challenge ciphertext as follows:

$$\mathsf{ct}_{x^*}^* = \left(\left[\overbrace{\boxed{\mathbf{c}}}^{\mathbf{c}_0^*}, \overbrace{\mathbf{x}_b^* \otimes \boxed{\mathbf{c}}\mathbf{V} + \sum_{i\in[L]} (\boxed{\mathbf{c}}\mathbf{V}_i + \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_i^*)}^{\mathbf{c}_1^*}, \overbrace{\sum_{i\in[L]} \boxed{\mathbf{c}}\mathbf{W}_i(\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'})}^{\mathbf{c}_2^*} \right]_1, \right.$$
$$\left. \left[\underbrace{\sum_{i\in[L]} \left(\boxed{\mathbf{c}}\mathbf{V}_i(\mathbf{a}_{y_i^*} \otimes \mathbf{I}_{(2k+1)n'}) + \boxed{\mathbf{c}}\mathbf{W}_i(\mathbf{K}_{y_i^*} \otimes \mathbf{I}_{(2k+1)n'})\right)}_{\mathbf{c}_3^*}, \underbrace{\boxed{\mathbf{c}}\mathbf{V}}_{\mathbf{c}_4^*} \right]_1 \right).$$

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

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

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

we replace $\mathbf{c}\mathbf{V}$ in challenge ciphertext with

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

In particular, we generate crs as below:

$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \boxed{\widetilde{\mathbf{V}}}]_1, \left\{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{A}\mathbf{V}_i, \mathbf{A}\mathbf{W}_i]_1\right\}_{i\in[L]}, \left\{[\mathbf{B}_1\mathbf{r}_j^\top]_2\right\}_{j\in[L]} \\ \left\{[\mathbf{V}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top), \mathbf{W}_i(\mathbf{I}_{nn'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\right\}_{j\in[L], i\in[L]\setminus\{j\}} \end{array} \right).$$

and generate the challenge ciphertext as

$$\mathsf{ct}^*_{x^*} = \left(\underbrace{\left[\overbrace{\mathbf{c}}^{\mathbf{c}^*_0}, \overbrace{\mathbf{x}^*_b \otimes \boxed{\mathbf{v}} + \sum_{i\in[L]} (\mathbf{c}\mathbf{V}_i + \mathbf{e}_1 \widetilde{\mathbf{G}}_i^{-1} \mathbf{Q}^*_i)}^{\mathbf{c}^*_1}, \overbrace{\sum_{i\in[L]} \mathbf{c}\mathbf{W}_i (\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'})}^{\mathbf{c}^*_2} \right]_1}_{\mathbf{c}^*_3}, \underbrace{\left[\sum_{i\in[L]} \left(\mathbf{c}\mathbf{V}_i (\mathbf{a}_{y^*_i} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{c}\mathbf{W}_i (\mathbf{K}_{y^*_i} \otimes \mathbf{I}_{(2k+1)n'}) \right), \boxed{\mathbf{v}} \right]_1}_{\mathbf{c}^*_4} \right).$$

We have $\mathsf{G}_5 \equiv \mathsf{G}_4$. This follows from the fact that when $\mathbf{V}$ is uniformly sampled from $\mathbb{Z}_p^{(k+1)\times(2k+1)}$ 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 change $\mathbf{c}^*_1$ as follows:

$$\mathbf{c}^*_1 = \mathbf{x}^*_b \otimes \mathbf{v}^{(1,3)} + \boxed{\mathbf{x}^*_0} \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]} (\mathbf{c}\mathbf{V}_i + \mathbf{e}_1 \widetilde{\mathbf{G}}_i^{-1} \mathbf{Q}^*_i)$$

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):

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

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 $(\mathbf{cV}_i)^{(2)}$ is hidden, this can imply that $\sum_{i\in[L]} (\mathbf{cV}_i)^{(2)}$ 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

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

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.

– G_8: Identical to $\mathsf{G}_{7,L}$ except that we generate the $\mathbf{c}^*_1$ as follows:

$$\mathbf{c}^*_1 = \boxed{\mathbf{x}^*_0} \otimes \mathbf{v}^{(1,3)} + \mathbf{x}^*_0 \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]} (\mathbf{c}\mathbf{V}_i + \mathbf{e}_1 \widetilde{\mathbf{G}}_i^{-1} \mathbf{Q}^*_i)$$

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):

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

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 6. 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, $\mathsf{mpk}_i \in D_i$ and $\mathbf{c}_1^*$, with highlighting relevant terms in the following sub-sequence with dashed boxes as follows:

$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{AV}_i, \mathbf{AW}_i]_1\}_{i\in[L]} \\ \{[\mathbf{d}_j^\top]_2\}_{j\in[\ell-1]}, \boxed{[\mathbf{B}_1\mathbf{r}_\ell^\top]_2}, \{[\mathbf{B}_1\mathbf{r}_j^\top]_2\}_{j\in[\ell+1,L]} \\ \{[\mathbf{V}_i(\mathbf{I}_{n'}\otimes\mathbf{d}_j^\top), \mathbf{W}_i(\mathbf{I}_{nn'}\otimes\mathbf{d}_j^\top)]_2\}_{j\in[\ell-1],i\in[L]\setminus\{j\}}, \\ \boxed{\{[\mathbf{V}_i(\mathbf{I}_{n'}\otimes\mathbf{B}_1\mathbf{r}_\ell^\top), \mathbf{W}_i(\mathbf{I}_{nn'}\otimes\mathbf{B}_1\mathbf{r}_\ell^\top)]_2\}_{i\in[L]\setminus\{\ell\}}}, \\ \{[\mathbf{V}_i(\mathbf{I}_{n'}\otimes\mathbf{B}_1\mathbf{r}_j^\top), \mathbf{W}_i(\mathbf{I}_{nn'}\otimes\mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L],i\in[L]\setminus\{j\}} \end{array}\right),$$

$$\mathsf{mpk}_i = \begin{cases} \left(\begin{array}{l} [\mathbf{AU}_i, \widehat{\mathbf{G}}_i\mathbf{U}_i]_1, \{[\mathbf{U}_i(\mathbf{I}_{n'}\otimes\mathbf{d}_j^\top)]_2\}_{j\in[\ell-1]\setminus\{i\}}, \boxed{[\mathbf{U}_i(\mathbf{I}_{n'}\otimes\mathbf{B}_1\mathbf{r}_\ell^\top)]_2}, \\ \{[\mathbf{U}_i(\mathbf{I}_{n'}\otimes\mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L]\setminus\{i\}}, \widetilde{\pi}_i \end{array}\right) & \text{if } i \neq \ell \\ \left(\begin{array}{l} [\mathbf{AU}_\ell, \widehat{\mathbf{G}}_i\mathbf{U}_\ell]_1, \{[\mathbf{U}_\ell(\mathbf{I}_{n'}\otimes\mathbf{d}_j^\top)]_2\}_{j\in[\ell-1]}, \\ \{[\mathbf{U}_\ell(\mathbf{I}_{n'}\otimes\mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L]}, \widetilde{\pi}_\ell \end{array}\right) & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_1^* = \mathbf{x}_b^*\otimes\mathbf{v}^{(1)} + \mathbf{x}_0^*\otimes\mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*}\otimes\mathbf{v}^{(3)} + (\mathbf{cV}_\ell + \mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}_\ell^*) + \sum_{i\in[L]}(\mathbf{cV}_i + \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_i^*)$$

where $\mathbf{d}_j^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_2)$ for all $j \in [\ell-1]$. And when $\mathsf{mpk}_\ell^* \in D_\ell$, for each $\mathbf{f} \in \mathcal{K}_\ell$ we recall secret key returned from $\mathsf{OKey}(\ell, \mathbf{f})$ in the following form

$$\mathsf{sk}_{\ell,\mathbf{f}} = \mathbf{U}_\ell^*(\mathbf{f}^\top\otimes\mathbf{I}_{2k+1})$$

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

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

In particular, we change the dashed boxed term in crs, mpk_i and $\mathsf{sk}_{\ell,\mathbf{f}}$ as follows:

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

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

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

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

$$\mathbf{c}_1^* = \mathbf{x}_b^*\otimes\mathbf{v}^{(1)} + \mathbf{x}_0^*\otimes\mathbf{v}^{(2)} + \boxed{\mathbf{x}_0^*}\otimes\mathbf{v}^{(3)} + (\mathbf{cV}_\ell + \mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}_\ell^*) + \sum_{i\in[L]}(\mathbf{cV}_i + \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_i^*)$$

We have $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$. We provide the detailed proof in Section 7.3.

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

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

In particular, we change the dashed boxed term in crs, mpk_i and $\mathsf{sk}_{\ell,\mathbf{f}}$ as follows:

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

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

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

Where $\mathbf{t}_0^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_3)$ corresponding to $\mathsf{G}_{7,\ell-1,2}$, and $\mathbf{t}_1^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_2)$ 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 $\mathbf{c}_1^*$ as follows:

$$\mathbf{c}_1^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*} \otimes \mathbf{v}^{(3)} + (\mathbf{c}\mathbf{V}_\ell + \mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}_\ell^*) + \sum_{i\in[L]} (\mathbf{c}\mathbf{V}_i + \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_i^*)$$

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, we have $\mathsf{G}_{7,\ell-1,4} = \mathsf{G}_{7,\ell}$ and this proves $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$.

7.3 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, for all $j \in [\ell-1]$, we rewrite $\mathbf{d}_j^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_2)$ with $\mathbf{B}_2 r_j$, for some $r_j \leftarrow \mathbb{Z}_p$. And we use solid boxes to indicate the difference between two games; use dashed boxes to highlight those terms that are relevant to our proof in this case.

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

$$\mathsf{mpk}_i = \begin{cases} \left([\mathbf{A}\mathbf{U}_i, \widehat{\mathbf{G}}_i\mathbf{U}_i]_1, \{[\mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_2 r_j)]_2\}_{j\in[\ell-1]\setminus\{i\}}, \boxed{[\mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{d}_\ell^\top)]_2}, \right. \\ \left. \{[\mathbf{U}_i(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L]\setminus\{i\}}, \widetilde{\pi}_i \right) & \text{if } i \neq \ell \\ \left([\mathbf{A}\mathbf{U}_\ell, \widehat{\mathbf{G}}_i\mathbf{U}_\ell]_1, \{[\mathbf{U}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_2 r_j^\top)]_2\}_{j\in[\ell-1]}, \right. \\ \left. \{[\mathbf{U}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{r}_j^\top)]_2\}_{j\in[\ell+1,L]}, \widetilde{\pi}_\ell \right) & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_1^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*} \otimes \mathbf{v}^{(3)} + \boxed{(\mathbf{c}\mathbf{V}_\ell + \mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}_\ell^*)} + \sum_{i\in[L]} (\mathbf{c}\mathbf{V}_i + \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_i^*)$$

$$\mathbf{c}_2^* = \boxed{\mathbf{c}\mathbf{W}_\ell(\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'})} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_i(\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'})$$

$$\mathbf{c}_3^* = \boxed{\mathbf{c}\mathbf{V}_\ell(\mathbf{a}_{y_\ell^*} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{c}\mathbf{W}_\ell(\mathbf{K}_{y_\ell^*} \otimes \mathbf{I}_{(2k+1)n'})} + \sum_{i\in[L]\setminus\{\ell\}} \left(\mathbf{c}\mathbf{V}_i(\mathbf{a}_{y_i^*} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{c}\mathbf{W}_i(\mathbf{K}_{y_i^*} \otimes \mathbf{I}_{(2k+1)n'})\right)$$

where $\mathbf{d}_\ell^\top \leftarrow \mathsf{span}^\top(\mathbf{B}_3)$. We define $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$ and $\mathbf{c}\mathbf{c}^\perp = 1$, this use the facts that $\binom{\mathbf{A}}{\mathbf{c}}$ is (row) full-rank w.h.p. With the orthogonality of dual basis, for all $\mathbf{v}^{(3)} \in \mathsf{span}(\mathbf{B}_3^{\parallel})$, 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) if $P(x^*, y_\ell^*) = 0$; (2) if $P(x^*, y_\ell^*) = 1$.

Case: if $P(x^*, y_\ell^*) = 0$. Notice that with our restriction (26), if mpk_ℓ^* is corrupted or maliciously generated, it must be in this case; and if mpk_ℓ^* is honest, it has possibility to be in this case. 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 this case:

$$
\begin{aligned}
& \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{AV}_\ell, \mathbf{AW}_\ell, \mathbf{V}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_1), \mathbf{V}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \mathbf{W}_\ell(\mathbf{I}_{nn'} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{nn'} \otimes \mathbf{B}_2) && \text{//crs} \\
& \mathbf{c}, \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{cV}_\ell, \mathbf{cW}_\ell(\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'}) && \text{//}\mathbf{c}^*_0, \mathbf{c}^*_1, \mathbf{c}^*_2 \\
& \mathbf{cV}_\ell(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{cW}_\ell(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{(2k+1)n'}) && \text{//}\mathbf{c}^*_3 \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{AV}_\ell, \mathbf{AW}_\ell, \mathbf{V}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_1), \mathbf{V}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \mathbf{W}_\ell(\mathbf{I}_{nn'} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{nn'} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{cV}_\ell + \boxed{\widetilde{\mathbf{v}} \otimes \mathbf{v}^{(3)}}, \mathbf{cW}_\ell(\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'}) + \boxed{\widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{n'}) \otimes \mathbf{v}^{(3)}} \\
& \mathbf{cV}_\ell(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{cW}_\ell(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{(2k+1)n'}) + \boxed{\widetilde{\mathbf{v}}(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{n'}) \otimes \mathbf{v}^{(3)} + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{n'}) \otimes \mathbf{v}^{(3)}} \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{AV}_\ell, \mathbf{AW}_\ell, \mathbf{V}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_1), \mathbf{V}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \mathbf{W}_\ell(\mathbf{I}_{nn'} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{nn'} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{cV}_\ell + \widetilde{\mathbf{v}} \otimes \mathbf{v}^{(3)}, \mathbf{cW}_\ell(\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'}) + \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{n'}) \otimes \mathbf{v}^{(3)} \\
& \mathbf{cV}_\ell(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{cW}_\ell(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{(2k+1)n'}) + \cancel{\widetilde{\mathbf{v}}(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{n'}) \otimes \mathbf{v}^{(3)}} + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{n'}) \otimes \mathbf{v}^{(3)} \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{AV}_\ell, \mathbf{AW}_\ell, \mathbf{V}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_1), \mathbf{V}_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \mathbf{W}_\ell(\mathbf{I}_{nn'} \otimes \mathbf{B}_1), \mathbf{W}_\ell(\mathbf{I}_{nn'} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \cancel{\mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)}} + \mathbf{cV}_\ell + \widetilde{\mathbf{v}} \otimes \mathbf{v}^{(3)}, \mathbf{cW}_\ell(\mathbf{C}_{x^*} \otimes \mathbf{I}_{(2k+1)n'}) + \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{n'}) \otimes \mathbf{v}^{(3)} \\
& \mathbf{cV}_\ell(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{(2k+1)n'}) + \mathbf{cW}_\ell(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{(2k+1)n'}) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{n'}) \otimes \mathbf{v}^{(3)}
\end{aligned}
$$

where $\widetilde{\mathbf{v}} \leftarrow \mathbb{Z}_p^{1\times n'}$, $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{1\times nn'}$. We justify each step as follows: The first "$\approx_s$" uses the change of variables:

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

The second "$\approx_s$" uses the fact that $P(x^*, y^*_\ell) = 0$ and the security of predicate encoding (c.f. Section 3.2), which ensure that

$$
\begin{aligned}
& \big(\widetilde{\mathbf{v}}(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{n'}) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{n'})\big) \| \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{n'}) \\
\approx_s\ & \big(\mathbf{0}(\mathbf{a}_{y^*_\ell} \otimes \mathbf{I}_{n'}) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*_\ell} \otimes \mathbf{I}_{n'})\big) \| \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{n'})
\end{aligned}
$$

The third "$\approx_s$" is straight-forward with the observation that $\widetilde{\mathbf{v}}$ only appears with $\mathbf{x}^*_{b'}$ and is sufficient to hide $\mathbf{x}^*_{b'}$ in $\mathbf{c}^*_1$.

Case: if $P(x^*, y^*_\ell) = 1$. Notice that with our restriction (26), this case implies that $\mathsf{mpk}^*_\ell \in D_\ell \setminus C_\ell$ and $\mathbf{x}^*_0 \mathbf{f}^\top = \mathbf{x}^*_1 \mathbf{f}^\top$ for all $\mathbf{f} \in \mathcal{K}_\ell$. Namely we know $\mathbf{U}^*_\ell$ (such that $\mathbf{T}^*_\ell = \mathbf{AU}^*_\ell$ and $\mathbf{Q}^*_\ell = \widehat{\mathbf{G}}_\ell \mathbf{U}^*_\ell$), we can write the dashboxed terms in $\mathbf{c}^*_1$ as follows:

$$\mathbf{cV}_\ell + \boxed{\mathbf{cU}^*_\ell}$$

and replace $\widehat{\mathbf{R}}_\ell$ in crs with a random $\mathbf{R}_\ell$ as in G_1. And in this case, $\mathbf{U}^*_\ell$ is hidden from the adversary, the adversary can only obtain secret keys as follows:

$$\boxed{\mathbf{U}^*_\ell}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) \quad \forall \mathbf{f} \in \mathcal{K}_\ell$$

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 this case:

$$
\begin{aligned}
& [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, [\mathbf{AU}^*_\ell]_1, [\mathbf{G}_\ell \mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_1), \mathbf{U}^*_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_2) && \text{//crs}, \mathsf{mpk}_\ell, \mathsf{mpk}^*_\ell \\
& \mathbf{c}, \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{cU}^*_\ell, \{\mathbf{U}^*_\ell(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})\}_{\mathbf{f}\in\mathcal{K}_\ell} && \text{//ct}^*_x, \{\mathsf{sk}_{\ell,\mathbf{f}}\}_{\mathbf{f}\in\mathcal{K}_\ell} \\
\approx_c\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, [\mathbf{AU}^*_\ell]_1, [\mathbf{G}_\ell \mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_1), \mathbf{U}^*_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \mathbf{cU}^*_\ell + \boxed{(\mathbf{x}^*_0 - \mathbf{x}^*_{b'}) \otimes \mathbf{v}^{(3)}}, \{\mathbf{U}^*_\ell(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \boxed{\mathbf{c}^\perp((\mathbf{x}^*_0 - \mathbf{x}^*_{b'})\mathbf{f}^\top \otimes \mathbf{v}^{(3)})}\}_{\mathbf{f}\in\mathcal{K}_\ell} \\
=\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, [\mathbf{AU}^*_\ell]_1, [\mathbf{G}_\ell \mathbf{U}^*_\ell]_1, \mathbf{U}^*_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_1), \mathbf{U}^*_\ell(\mathbf{I}_{n'} \otimes \mathbf{B}_2) \\
& \mathbf{c}, \boxed{\mathbf{x}^*_0} \otimes \mathbf{v}^{(3)} + \mathbf{cU}^*_\ell + \cancel{(\mathbf{x}^*_0 - \mathbf{x}^*_{b'}) \otimes \mathbf{v}^{(3)}}, \{\mathbf{U}^*_\ell(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \cancel{\mathbf{c}^\perp((\mathbf{x}^*_0 - \mathbf{x}^*_{b'})\mathbf{f}^\top \otimes \mathbf{v}^{(3)})}\}_{\mathbf{f}\in\mathcal{K}_\ell}
\end{aligned}
$$

We justify each step as below: The first $\approx_c$ uses Lemma 5 with $n = n'$, $\mathbf{G} = \mathbf{G}_\ell$, $\mathbf{U} = \mathbf{U}^*_\ell$, $\mathbf{d}^\perp = \mathbf{v}^{(3)}$ and $\widehat{\mathbf{x}} = \mathbf{x}^*_{b'} - \mathbf{x}^*_0$. The second = follows from the fact that $(\mathbf{x}^*_{b'} - \mathbf{x}^*_0)\mathbf{f}^\top = 0$ for all $\mathbf{f} \in \mathcal{K}_\ell$.

8 Slotted Reg-IPFE with Delegated ABE from Pairings

In this section, we propose a slotted Reg-IPFE with delegated ABE for inner-product functionality, which is covered by the notion of slotted delegated Reg-FE. In particular, a (slotted) Reg-IPFE with delegated ABE inner-product functionality $\mathsf{IP}_n = \{\mathbf{f} : \mathbf{x} \mapsto \mathbf{x}\mathbf{f}^\top\}$ with predicate $P : X \times Y \to \{0,1\}$ can be seen as a delegated Reg-FE for induced functionalities:

$$G_{\mathsf{IP}} : \mathbb{Z}_p^n \times X' \to \mathbb{Z}_p \times X' \quad \text{and} \quad F_P : \mathbb{Z}_p \times X' \to (\mathbb{Z}_p \times \{\perp\})$$

where for all $g_{\mathbf{f}} \in G_{\mathsf{IP}}$ and $f_y \in F_P$, we have

$$g_{\mathbf{f}}(\mathbf{x}, x) = (\mathbf{x}\mathbf{f}^\top, x) \quad \text{and} \quad f_y(z, x') = \begin{cases} z & \text{if } P(x,y) = 1 \\ \perp & \text{if } P(x,y) = 0 \end{cases}$$

And we recall in this section:

- for correctness, we consider
$$f_y \circ g_{\mathbf{f}}(\mathbf{x}, x) = \mathbf{x}\mathbf{f}^\top \quad \text{when} \quad P(x,y) = 1;$$
- for security, we consider the challenge as $(\mathbf{x}_b^*, x^*)$ for $b \in \{0,1\}$, and consider the requirements as
$$g_{\mathbf{f}}(\mathbf{x}_0^*, x^*) = g_{\mathbf{f}}(\mathbf{x}_1^*, x^*) \implies \mathbf{x}_0^*\mathbf{f}^\top = \mathbf{x}_1^*\mathbf{f}^\top$$
$$f_y \circ g_{\mathbf{f}}(\mathbf{x}_0^*, x^*) = f_y \circ g_{\mathbf{f}}(\mathbf{x}_1^*, x^*) \implies \mathbf{x}_0^*\mathbf{f}^\top = \mathbf{x}_1^*\mathbf{f}^\top \vee P(x^*, y) = 0$$

Our construction is based on predicate encodings (c.f. Section 3.2) and achieves the IND-security under MDDH assumption. By the Remark 1 and generic transformation in Section 10, this yields a Reg-IPFE with delegated ABE (Reg-FE for above induced functionalities) via predicate encodings under MDDH assumption.

8.1 Scheme

In this section, we propose a slotted Reg-IPFE with delegated ABE for inner-product functionality which is defined by $X = \mathbb{Z}_p^{1\times n}$, $Z = \mathbb{Z}_p$ and

$$F = \{\mathbf{y} : \mathbf{x} \mapsto \mathbf{x}\mathbf{y}^\top\},$$

with predicate $P : X \times Y \to \{0,1\}$ via predicate encoding from MDDH assumption. The scheme achieves the adaptive IND-security (c.f. Section 4.2). Assuming QA-NIZKs $\Pi_1 = (\mathsf{LGen}_1, \mathsf{LPrv}_1, \mathsf{LVer}_1, \mathsf{LSim}_1)$ for $\mathbb{G}_1$-linear space and $\Pi_2 = (\mathsf{LGen}_2, \mathsf{LPrv}_2, \mathsf{LVer}_2, \mathsf{LSim}_2)$ for $\mathbb{G}_2$-linear space over bilinear groups (c.f. Section 3.3), our slotted Reg-IFPE with delegated ABE scheme in prime-order bilinear groups works as follows:

- $\mathsf{Setup}(1^\lambda, 1^n, P, 1^L)$: Run $\mathbb{G} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample
$$\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}, \ \mathbf{V} \leftarrow \mathbb{Z}_p^{(k+1)\times(5k+2)}.$$
Sample
$$\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(5k+2)\times k}, \ \mathbf{B}_2 \leftarrow \mathbb{Z}_p^{(5k+2)\times(2k+1)} \ \mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(5k+2)\times(2k+1)}$$
and compute the dual basis $(\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel)$, see section 3.1. For all $i \in [L]$, sample
$$\mathbf{W}_{0,i} \leftarrow \mathbb{Z}_p^{(k+1)\times(5k+2)n}, \ \mathbf{G}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}, \ \mathbf{R}_i \leftarrow \mathbb{Z}_p^{k\times k}.$$
For all $i \in [L]$, write $\mathbf{A}_i = \begin{pmatrix} \mathbf{A} \\ \mathbf{G}_i \end{pmatrix} \in \mathbb{Z}_p^{(2k+2)\times(k+1)}$ and run
$$(\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}_1(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1).$$

Compute parameter (n', n_c, n_k) from P, see Section 3.2. For all $j \in [L]$ and $i \in [L] \setminus \{j\}$, sample

$$\mathbf{G}_{i,j} \leftarrow \mathbb{Z}_p^{(5k+2)\times(6k+2)}$$

write $\mathbf{B}_{i,j} = (\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,j}) \in \mathbb{Z}_p^{(5k+2)n'\times(7k+2)n'}$ and run

$$(\mathsf{crs}_{i,j}, \mathsf{td}_{i,j}) \leftarrow \mathsf{LGen}_2(1^\lambda, \mathbb{G}_2, [\mathbf{B}_{i,j}]_2)$$

Output

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AV}]_1, \{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{AW}_{0,i}]_1\}_{i\in[L]}, \{[\mathbf{B}_1\mathbf{R}_j]_2\}_{j\in[L]} \\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_j)]_2\}_{j\in[L],i\in[L]\setminus\{j\}} \end{pmatrix}.$$

Notice that we do not use $\{\mathsf{td}_i\}_{i\in[L]}$ and $\{\mathsf{td}_{i,j}\}_{j\in[L],i\in[L]\setminus\{j\}}$ and $\mathbf{B}_2, \mathbf{B}_3$, $(\mathbf{B}_1^{\parallel}, \mathbf{B}_2^{\parallel}, \mathbf{B}_3^{\parallel})$ in the actual scheme.

– $\mathsf{Gen}(\mathsf{crs}, i)$: Sample $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(5k+2)}$ and $\mathbf{W}_{1,i} \leftarrow \mathbb{Z}_p^{(k+1)\times(5k+2)n'}$. Define

$$\mathbf{F}_i = \begin{pmatrix} (\mathbf{T}_{0,i} \| \mathbf{T}_{1,i}) \\ (\mathbf{Q}_{0,i} \| \mathbf{Q}_{1,i}) \end{pmatrix} = \begin{pmatrix} \mathbf{A}(\mathbf{U}_i \| \mathbf{W}_{1,i}) \\ \mathbf{G}_i(\mathbf{U}_i \| \mathbf{W}_{1,i}) \end{pmatrix} = \mathbf{A}_i(\mathbf{U}_i \| \mathbf{W}_{1,i}) \in \mathbb{Z}_p^{(2k+2)\times(5k+2)(n'+1)}$$

and run

$$\pi_i \leftarrow \mathsf{LPrv}_1(\mathsf{crs}_i, [\mathbf{F}_i]_1, (\mathbf{U}_i \| \mathbf{W}_{1,i})).$$

For all $j \in [L] \setminus \{i\}$, define

$$\mathbf{F}_{i,j} = (\mathbf{H}_{1,i,j} \| \mathbf{P}_{i,j}) = \left(\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j) \| \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})\right) = \mathbf{W}_{1,i}\mathbf{B}_{i,j} \in \mathbb{Z}_p^{(k+1)\times(7k+2)n'}$$

and run

$$\pi_{i,j} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,j}, [\mathbf{F}_{i,j}]_2, \mathbf{W}_{1,i})$$

Output

$$\mathsf{mpk}_i = \begin{pmatrix} [\overbrace{\mathbf{AU}_i}^{\mathbf{T}_{0,i}}, \overbrace{\mathbf{AW}_{1,i}}^{\mathbf{T}_{1,i}}, \overbrace{\mathbf{G}_i\mathbf{U}_i}^{\mathbf{Q}_{0,i}}, \overbrace{\mathbf{G}_i\mathbf{W}_{1,i}}^{\mathbf{Q}_{1,i}}]_1, \pi_i \\ \{[\underbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{R}_j}_{\mathbf{H}_{0,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j)}_{\mathbf{H}_{1,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})}_{\mathbf{P}_{i,j}}]_2, \pi_{i,j}\}_{j\in[L]\setminus\{i\}} \end{pmatrix} \quad \text{and} \quad \mathsf{msk}_i = (\mathbf{U}_i, \mathbf{W}_{1,i}).$$

– $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i)$: Parse $\mathsf{mpk}_i = \begin{pmatrix} [\mathbf{T}_{0,i}, \mathbf{T}_{1,i}, \mathbf{Q}_{0,i}, \mathbf{Q}_{1,i}]_1, \pi_i, \\ \{[\mathbf{H}_{0,i,j}, \mathbf{H}_{1,i,j}, \mathbf{P}_{i,j}]_2, \pi_{i,j}\}_{j\in[L]\setminus\{i\}} \end{pmatrix}$. Write $\mathbf{F}_i = \begin{pmatrix} (\mathbf{T}_{0,i} \| \mathbf{T}_{1,i}) \\ (\mathbf{Q}_{0,i} \| \mathbf{Q}_{1,i}) \end{pmatrix}$ and check

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

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

$$e([\mathbf{A}]_1, [\mathbf{H}_{0,i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_{0,i}]_1, [\mathbf{B}_1\mathbf{R}_j]_2)$$
$$e([\mathbf{A}]_1, [\mathbf{H}_{1,i,j}]_2) \stackrel{?}{=} e([\mathbf{T}_{1,i}]_1, [\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j]_2),$$

write $\mathbf{F}_{i,j} = (\mathbf{H}_{1,i,j} \| \mathbf{P}_{i,j})$ and check

$$\mathsf{LVer}_2(\mathsf{crs}_{i,j}, [\mathbf{F}_{i,j}]_2, \pi_{i,j}) \stackrel{?}{=} 1$$

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

– $\mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i, \mathbf{y}_i)_{i\in[L]})$: For all $i \in [L]$, fetch $[\mathbf{T}_{0,i}, \mathbf{T}_{1,i}]_1$, $\{[\mathbf{H}_{0,i,j}, \mathbf{H}_{1,i,j}]_2\}_{j\in[L]\setminus\{i\}}$ from mpk_i. Output:

$$\mathsf{mpk}_+ = \left(\left[\mathbf{A},\ \mathbf{AV},\ \sum_{i\in[L]}(\mathbf{T}_{0,i} + \mathbf{AW}_{0,i}(\mathbf{y}_i^\top \otimes \mathbf{I}_{5k+2})),\ \sum_{i\in[L]}\mathbf{AW}_{0,i},\ \sum_{i\in[L]}\mathbf{T}_{1,i}\right]_1\right)$$

and for all $j \in [L]$

$$\mathsf{hsk}_j = \left(\begin{array}{c}\left[\overbrace{\mathbf{B}_1\mathbf{R}_j}^{\mathbf{K}_{j,0}},\ \overbrace{\sum_{i\in[L]\setminus\{j\}}\mathbf{H}_{1,i,j}}^{\mathbf{K}_{j,1}},\ \overbrace{\sum_{i\in[L]\setminus\{j\}}\mathbf{W}_{0,i}(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{R}_j)}^{\mathbf{K}_{j,2}}\right]_2,\\ \Bigg[\underbrace{\sum_{i\in[L]\setminus\{j\}}(\mathbf{H}_{0,i,j} + \mathbf{W}_{0,i}(\mathbf{I}_n\otimes\mathbf{B}_1\mathbf{R}_j)(\mathbf{y}_i^\top\otimes\mathbf{I}_k))}_{\mathbf{K}_{j,3}}\Bigg]_2\end{array}\right).$$

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

$$\mathsf{ct}_x = \left(\begin{array}{c}\left[\overbrace{\mathbf{sA}}^{\mathbf{c}_0},\ \overbrace{\mathbf{sAV}}^{\mathbf{c}_1},\ \overbrace{\sum_{i\in[L]}(\mathbf{sT}_{0,i} + \mathbf{sAW}_{0,i}(\mathbf{y}_i^\top\otimes\mathbf{I}_{5k+2}))}^{\mathbf{c}_2}\right]_1,\\ \Bigg[\underbrace{\mathbf{x}\otimes\mathbf{sAV} + \sum_{i\in[L]}\mathbf{sAW}_{0,i}}_{\mathbf{c}_3},\ \underbrace{\sum_{i\in[L]}\mathbf{sT}_{1,i}(\mathbf{C}_x\otimes\mathbf{I}_{5k+2})}_{\mathbf{c}_4}\Bigg]_1\end{array}\right).$$

– $\mathsf{Key}(\mathsf{msk}_{j^*}, \mathsf{hsk}_{j^*}, y)$: Compute $\mathbf{a}_y, \mathbf{K}_y$ from y and parse $\mathsf{msk}_{j^*} = (\mathbf{U}_{j^*}, \mathbf{W}_{1,j^*})$. Sample $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times k}$ and output:

$$\mathsf{sk}_{j^*,y} = \left(\left[\underbrace{\mathbf{B}_1\mathbf{R}_{j^*}\mathbf{R}}_{\mathbf{K}_0},\ \underbrace{\sum_{i\in[L]\setminus\{j^*\}}\mathbf{H}_{1,i,j^*}(\mathbf{I}_{n'}\otimes\mathbf{R})}_{\mathbf{K}_1},\ \underbrace{\mathbf{U}_{j^*}\mathbf{B}_1\mathbf{R}_{j^*}(\mathbf{a}_y\otimes\mathbf{I}_k) + \mathbf{W}_{1,j^*}(\mathbf{I}_{n'}\otimes\mathbf{B}_1\mathbf{R}_{j^*}\mathbf{R})(\mathbf{K}_y\otimes\mathbf{I}_k)}_{\mathbf{K}_2}\right]_2\right).$$

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

$$\mathsf{sk}_{j^*,y'} = ([\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2]_2), \quad \mathsf{hsk}_{j^*} = ([\mathbf{K}_{j^*,0}, \mathbf{K}_{j^*,1}, \mathbf{K}_{j^*,2}, \mathbf{K}_{j^*,3}]_2), \quad \mathsf{ct} = ([\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4]_1).$$

Recover

$$\begin{aligned}
&[\mathbf{z}_1]_T = e([\mathbf{c}_3]_1, [\mathbf{I}_n\otimes\mathbf{K}_{j^*,0}]_2), && [\mathbf{z}_2]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_{j^*,2}]_2);\\
&[\mathbf{z}_3]_T = e([\mathbf{c}_2]_1, [\mathbf{K}_{j^*,0}]_2), && [\mathbf{z}_4]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_{j^*,3}]_2);\\
&[\mathbf{z}_5]_T = e([\mathbf{c}_4]_1, [\mathbf{I}_{n_c}\otimes\mathbf{K}_0]_2), && [\mathbf{z}_6]_T = e([\mathbf{c}_0]_1, [\mathbf{K}_1(\mathbf{C}_x\otimes\mathbf{I}_k)]_2);\\
&[\mathbf{z}_7]_T = e([\mathbf{c}_1]_1, [\mathbf{K}_{j^*,0}]_2), && [\mathbf{z}_8]_T = e([\mathbf{c}_0]_1.[\mathbf{K}_2]_2).
\end{aligned}$$

Compute $\mathbf{d}_{x,y}$ from x and y, recover

$$[\mathbf{z}]_T = [(\mathbf{z}_1 - \mathbf{z}_2)(\mathbf{y}_{j^*}^\top\otimes\mathbf{I}_k) - (\mathbf{z}_3 - \mathbf{z}_4) + (\mathbf{z}_8\|(\mathbf{z}_5 - \mathbf{z}_6))(\mathbf{d}_{x,y}^\top\otimes\mathbf{I}_k)]_T$$

Recover z from $[\mathbf{z}\mathbf{e}_1^\top]_T$ over $[\mathbf{z}_7\mathbf{e}_1^\top]_T$ via brute-force DLOG and output z.

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

$$\mathsf{mpk}_i = \left(\begin{array}{l}[\overbrace{\mathbf{AU}_i}^{\mathbf{T}_{0,i}},\overbrace{\mathbf{AW}_{1,i}}^{\mathbf{T}_{1,i}},\overbrace{\mathbf{G}_i\mathbf{U}_i}^{\mathbf{Q}_{0,i}},\overbrace{\mathbf{G}_i\mathbf{W}_{1,i}}^{\mathbf{Q}_{1,i}}]_1, \pi_i\\ \{[\underbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{R}_j}_{\mathbf{H}_{0,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'}\otimes\mathbf{B}_1\mathbf{R}_j)}_{\mathbf{H}_{1,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'}\otimes\mathbf{G}_{i,j})}_{\mathbf{P}_{i,j}}]_2, \pi_{i,j}\}_{j\in[L]\setminus\{i\}}\end{array}\right)$$

for some $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{(k+1)\times(5k+2)}$, $\mathbf{W}_{1,i} \leftarrow \mathbb{Z}_p^{(k+1)\times(5k+2)n'}$, and

– $\pi_i \leftarrow \mathsf{LPrv}_1(\mathsf{crs}_i, [\mathbf{A}_i(\mathbf{U}_i \| \mathbf{W}_{1,i})]_1, (\mathbf{U}_i \| \mathbf{W}_{1,i}))$, where $(\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$ and $\mathbf{A}_i = \begin{pmatrix} \mathbf{A} \\ \mathbf{G}_i \end{pmatrix}$ with $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{G}_i \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$;
– for all $j \in [L] \setminus \{i\}$, $\pi_{i,j} \leftarrow \mathsf{LPrv}_1(\mathsf{crs}_{i,j}, [\mathbf{W}_{1,i}\mathbf{B}_{i,j}]_2, \mathbf{W}_{1,i})$, where $(\mathsf{crs}_{i,j}, \mathsf{td}_{i,j}) \leftarrow \mathsf{LGen}(1^\lambda, \mathbb{G}_2, [\mathbf{B}_{i,j}]_2)$ and $\mathbf{B}_{i,j} = (\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})$ with $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(5k+2)\times k}$, $\mathbf{R}_j \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{G}_{i,j} \leftarrow \mathbb{Z}_p^{(5k+2)\times(6k+2)}$.

Then:

– Write $\mathbf{F}_i = \begin{pmatrix} (\mathbf{T}_{0,i} \| \mathbf{T}_{1,i}) \\ (\mathbf{Q}_{0,i} \| \mathbf{Q}_{1,i}) \end{pmatrix} = \begin{pmatrix} \mathbf{A}(\mathbf{U}_i \| \mathbf{W}_{1,i}) \\ \mathbf{G}_i(\mathbf{U}_i \| \mathbf{W}_{1,i}) \end{pmatrix}$, we have $\mathsf{LVer}_1(\mathsf{crs}_i, [\mathbf{F}_i]_1, \pi_i) = 1$ by the perfect completeness of Π_1 (see Section 3.3) and the fact that $\mathbf{F}_i = \mathbf{A}_i(\mathbf{U}_i \| \mathbf{W}_{1,i})$;
– For each $j \in [L] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{U}_i\mathbf{B}_1\mathbf{R}_j]_2) = e([\mathbf{A}\mathbf{U}_i]_1, [\mathbf{B}\mathbf{R}_j]_2)$ by the definition of bilinear map e (see Section 3.1) and the fact that $\mathbf{A} \cdot \mathbf{U}_i\mathbf{B}_1\mathbf{R}_j = \mathbf{A}\mathbf{U}_i \cdot \mathbf{B}_1\mathbf{R}_j$.
– For each $j \in [L] \setminus \{i\}$, we have $e([\mathbf{A}]_1, [\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j)]_2) = e([\mathbf{A}\mathbf{W}_{1,i}]_1, [\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j]_2)$ by the definition of bilinear map e (see Section 3.1) and the fact that $\mathbf{A} \cdot \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j) = \mathbf{A}\mathbf{W}_{1,i} \cdot (\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j)$.
– For each $j \in [L] \setminus \{i\}$, write $\mathbf{F}_{i,j} = (\mathbf{H}_{1,i,j} \| \mathbf{P}_{i,j}) = \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})$, we have $\mathsf{LPrv}_2(\mathsf{crs}_{i,j}, [\mathbf{F}_{i,j}]_2, \pi_{i,j}) = 1$ by the perfect completeness of Π_2 (see Section 3.3) and the fact that $\mathbf{F}_{i,j} = \mathbf{W}_{1,i}\mathbf{B}_{i,j}$.

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

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

$$\mathsf{sk}_{j^*,y} = \left(\left[\underbrace{\mathbf{B}_1\mathbf{R}_{j^*}\mathbf{R}}_{\mathbf{K}_0}, \underbrace{\sum_{i\in[L]\setminus\{j^*\}} \mathbf{H}_{1,i,j}(\mathbf{I}_{n'} \otimes \mathbf{R})}_{\mathbf{K}_1}, \underbrace{\mathbf{U}_{j^*}\mathbf{B}_1\mathbf{R}_{j^*}(\mathbf{a}_y \otimes \mathbf{I}_k) + \mathbf{W}_{1,j^*}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_{j^*}\mathbf{R})(\mathbf{K}_y \otimes \mathbf{I}_k)}_{\mathbf{K}_2} \right]_2 \right),$$

$$\mathsf{hsk}_{j^*} = \left(\begin{array}{l} \left[\overbrace{\mathbf{B}_1\mathbf{R}_{j^*}}^{\mathbf{K}_{j^*,0}}, \overbrace{\sum_{i\in[L]\setminus\{j^*\}} \mathbf{H}_{1,i,j^*}}^{\mathbf{K}_{j^*,1}}, \overbrace{\sum_{i\in[L]\setminus\{j^*\}} \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*})}^{\mathbf{K}_{j^*,2}} \right]_2, \\ \underbrace{\left[\sum_{i\in[L]\setminus\{j^*\}} (\mathbf{H}_{0,i,j^*} + \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*})(\mathbf{y}_i^\top \otimes \mathbf{I}_k)) \right]_2}_{\mathbf{K}_{j^*,3}} \end{array} \right),$$

$$\mathsf{ct}_x = \left(\begin{array}{l} \left[\overbrace{\mathbf{sA}}^{\mathbf{c}_0}, \overbrace{\mathbf{sAV}}^{\mathbf{c}_1}, \overbrace{\sum_{i\in[L]} (\mathbf{sT}_{0,i} + \mathbf{sAW}_{0,i}(\mathbf{y}_i^\top \otimes \mathbf{I}_{5k+2}))}^{\mathbf{c}_2} \right]_1, \\ \left[\underbrace{\mathbf{x} \otimes \mathbf{sAV} + \sum_{i\in[L]} \mathbf{sAW}_{0,i}}_{\mathbf{c}_3}, \underbrace{\sum_{i\in[L]} \mathbf{sT}_{1,i}(\mathbf{C}_x \otimes \mathbf{I}_{5k+2})}_{\mathbf{c}_4} \right]_1 \end{array} \right).$$

where

$$\mathbf{AH}_{0,i,j^*} = \mathbf{T}_{0,i}\mathbf{B}\mathbf{R}_{j^*}, \quad \mathbf{AH}_{1,i,j^*} = \mathbf{T}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}\mathbf{R}_j) \quad \forall i \in [L] \setminus \{j^*\};$$
$$\mathbf{T}_{0,j^*} = \mathbf{A}\mathbf{U}_{j^*}, \qquad \mathbf{T}_{1,j^*} = \mathbf{A}\mathbf{W}_{1,j^*}.$$

Note that in Key and Dec, we actually consider hsk_j for $j = j^*$ and msk_i for $i = j^*$; and all above equalities are ensured by Ver, Gen and Key. We have

$$\begin{aligned}
\mathbf{z}_1 &= (\mathbf{x} \otimes \mathbf{sAV})(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*}) + \sum_{i\in[L]} \mathbf{sAW}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*}) \\
&= \mathbf{x} \otimes \mathbf{sAVB}_1\mathbf{R}_{j^*} + \sum_{i\in[L]} \mathbf{sAW}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*}) && (27)\\
\mathbf{z}_2 &= \sum_{i\in[L]\setminus\{j^*\}} \mathbf{sAW}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*}) \\
\mathbf{z}_3 &= \sum_{i\in[L]} (\mathbf{sT}_{0,i}\mathbf{B}_1\mathbf{R}_{j^*} + \mathbf{sAW}_{0,i}(\mathbf{y}_i^\top \otimes \mathbf{I}_{5k+2})\mathbf{B}_1\mathbf{R}_{j^*}) \\
&= \sum_{i\in[L]} (\mathbf{sT}_{0,i}\mathbf{B}_1\mathbf{R}_{j^*} + \mathbf{sAW}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*})(\mathbf{y}_i^\top \otimes \mathbf{I}_k)) && (28)\\
\mathbf{z}_4 &= \sum_{i\in[L]\setminus\{j^*\}} (\mathbf{sAH}_{0,i,j^*} + \mathbf{sAW}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*})(\mathbf{y}_i^\top \otimes \mathbf{I}_k)) \\
\mathbf{z}_5 &= \sum_{i\in[L]} \mathbf{sT}_{1,i}(\mathbf{C}_x \otimes \mathbf{I}_{5k+2})(\mathbf{I}_{n_c} \otimes \mathbf{B}_1\mathbf{R}_{j^*}\mathbf{R}) \\
&= \sum_{i\in[L]} \mathbf{sT}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_{j^*}\mathbf{R})(\mathbf{C}_x \otimes \mathbf{I}_k) && (29)\\
\mathbf{z}_6 &= \sum_{i\in[L]\setminus\{j^*\}} \mathbf{sAH}_{1,i,j^*}(\mathbf{I}_{n'} \otimes \mathbf{R}) \\
\mathbf{z}_7 &= \mathbf{sAVB}_1\mathbf{R}_{j^*} \\
\mathbf{z}_8 &= \mathbf{sAU}_{j^*}\mathbf{B}_1\mathbf{R}_{j^*}(\mathbf{a}_y \otimes \mathbf{I}_k) + \mathbf{sAW}_{1,j^*}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_{j^*}\mathbf{R})(\mathbf{K}_y \otimes \mathbf{I}_k)
\end{aligned}$$

Then, as in Section 3.2, let

$$\mathbf{M}_{x,y} = \begin{pmatrix} \mathbf{a}_y & \mathbf{0}_{n_c} \\ \mathbf{K}_y & \mathbf{C}_x \end{pmatrix}$$

we have

$$\begin{aligned}
[\mathbf{z}]_T &= [(\mathbf{z}_1 - \mathbf{z}_2)(\mathbf{y}_{j^*}^\top \otimes \mathbf{I}_k) - (\mathbf{z}_3 - \mathbf{z}_4) + (\mathbf{z}_8 \| (\mathbf{z}_5 - \mathbf{z}_6))(\mathbf{d}_{x,y}^\top \otimes \mathbf{I}_k)]_T \\
&= [(\mathbf{x} \otimes \mathbf{sAVB}_1\mathbf{R}_{j^*})(\mathbf{y}_{j^*}^\top \otimes \mathbf{I}_k) + \mathbf{sAW}_{0,j^*}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*})(\mathbf{y}_{j^*}^\top \otimes \mathbf{I}_k) \\
&\quad -(\mathbf{sAU}_{j^*}\mathbf{B}_1\mathbf{R}_{j^*} + \mathbf{sAW}_{0,j^*}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_{j^*})(\mathbf{y}_{j^*}^\top \otimes \mathbf{I}_k)) \\
&\quad +(\mathbf{sAU}_{j^*}\mathbf{B}_1\mathbf{R}_{j^*} \| \mathbf{sAW}_{1,j^*}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_{j^*}\mathbf{R}))(\mathbf{M}_{x,y} \otimes \mathbf{I}_k)(\mathbf{d}_{x,y}^\top \otimes \mathbf{I}_k)]_T && (30)\\
&= [(\mathbf{x} \otimes \mathbf{sAVB}_1\mathbf{R}_{j^*})(\mathbf{y}_{j^*}^\top \otimes \mathbf{I}_k) - \mathbf{sAU}_{j^*}\mathbf{B}_1\mathbf{R}_{j^*} + \mathbf{sAU}_{j^*}\mathbf{B}_1\mathbf{R}_{j^*}]_T && (31)\\
&= [\mathbf{x}\mathbf{y}_{j^*}^\top \otimes \mathbf{sAVB}_1\mathbf{R}_{j^*}]_T && (32)\\
&= [\mathbf{x}\mathbf{y}_{j^*}^\top \cdot \mathbf{sAVB}_1\mathbf{R}_{j^*}]_T
\end{aligned}$$

Here equalities (27), (28), (29) and (32) follows from the property of tensor product: $(\mathbf{M}_1 \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{M}_2) = \mathbf{M}_1 \otimes \mathbf{M}_2 = (\mathbf{I} \otimes \mathbf{M}_2)(\mathbf{M}_1 \otimes \mathbf{I})$ for matrices of proper size; equality (30) follows from the fact that $\mathbf{AH}_{0,i,j} = \mathbf{T}_{0,i}\mathbf{BR}_{j^*}$, $\mathbf{AH}_{1,i,j} = \mathbf{T}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{BR}_{j^*})$ for all $i \in [L] \setminus \{j^*\}$ and the fact that $\mathbf{T}_{0,j^*} = \mathbf{AU}_{j^*}$, $\mathbf{T}_{1,j^*} = \mathbf{AW}_{1,j^*}$; equality (31) follows from the correctness of predicate encodings. Treat $[\mathbf{z}_7\mathbf{e}_1^\top]_T = [\mathbf{sAVB}_1\mathbf{R}_{j^*}\mathbf{e}_1^\top]_T$ as the basis, and recover z from $[\mathbf{z}\mathbf{e}_1^\top]_T = [\mathbf{x}\mathbf{y}_{j^*}^\top \cdot \mathbf{sAVB}_1\mathbf{R}_{j^*}\mathbf{e}_1^\top]_T$ via brute-force DLOG, we have

$$z = \mathbf{x}\mathbf{y}_{j^*}^\top$$

This proves the correctness.

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

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

Note that the total size of $\{\mathsf{crs}_i\}_{i\in[L]}$ and $\{\mathsf{crs}_{i,j}\}_{j\in[L],i\in[L]\setminus\{j\}}$ is $L^2 \cdot \mathsf{poly}(\lambda)$ 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] under MDDH assumption and the fact that MDDH assumption implies subspace decision assumption [CGKW18], our scheme of slotted Reg-IPFE with delegated ABE uses prime-order bilinear group and the security can be reduced to MDDH assumption.

Theorem 4. *Assume* $\Pi_1 = (\mathsf{LGen}_1, \mathsf{LPrv}_1, \mathsf{LVer}_1, \mathsf{LSim}_1)$, $\Pi_2 = (\mathsf{LGen}_2, \mathsf{LPrv}_2, \mathsf{LVer}_2, \mathsf{LSim}_2)$ *are QA-NIZKs with perfect completeness, perfect zero-knowledge and unbounded simulation soundness respectively for* $\mathbb{G}_1$*-linear space and* $\mathbb{G}_2$*-linear space defined in Section 3.3, our scheme of slotted Reg-IPFE with delegated ABE achieves the adaptive IND-security defined in Section 4.1 (with the consideration we have mentioned in the beginning of this section) under MDDH assumption.*

8.2 Proof

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

Lemma 7. *For all adversaries* $\mathcal{A}$*, there exist adversaries* $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$, $\mathcal{B}_4$ *such that:*

$$\mathsf{Adv}^{\mathit{sReg\text{-}FE+Del\text{-}ABE}}_{\mathcal{A}}(\lambda) \le (L+4QL^2)\mathsf{Adv}^{\mathit{USS}}_{\mathcal{B}_1}(\lambda)+(1+8L+40QL)\mathsf{Adv}^{\mathit{MDDH}}_{\mathcal{B}_2}(\lambda)+L\cdot\mathsf{Adv}^{\mathrm{SD}^{\mathbb{G}_2}_{\mathbf{B}_1\mapsto\mathbf{B}_3}}_{\mathcal{B}_3}(\lambda)+L\cdot\mathsf{Adv}^{\mathrm{SD}^{\mathbb{G}_2}_{\mathbf{B}_3\mapsto\mathbf{B}_2}}_{\mathcal{B}_4}(\lambda)+\mathsf{negl}(\lambda)$$

where L *is the number of slots,* Q *is the maximum number of queries on* $\mathsf{OKey}(i,\cdot)$ *for some slot* i*; 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 and x^* is the challenge "attribute", $\{\mathsf{mpk}_i^*, \mathbf{y}_i^*\}_{i\in[L]}$ are challenge mater public keys along with challenge functions to be registered. For all $i \in [L]$, define $D_i = \{\mathsf{mpk}_i : \mathcal{D}_i[\mathsf{mpk}_i] = \mathsf{msk}_i \neq \bot\}$ be responses to $\mathsf{OGen}(i)$, $C_i = \{\mathsf{mpk}_i : (i, \mathsf{mpk}_i) \in C\}$ records master public keys in D_i that have been sent to $\mathsf{OCor}(i,\cdot)$; recall that $\mathcal{K}_i$ is the list that record the queries to $\mathsf{OKey}(i,\cdot)$. For each $i \in [L]$, we have the restrictions as follow

$$\begin{aligned} \mathsf{mpk}_i^* \notin D_i &\implies \mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i^*) = 1 \wedge \mathcal{K}_i = \emptyset, \\ \mathsf{mpk}_i^* \in C_i \vee \mathsf{mpk}_i^* \notin D_i &\implies \mathbf{x}_0^*(\mathbf{y}_i^*)^\top = \mathbf{x}_1^*(\mathbf{y}_i^*)^\top, \\ y \in \mathcal{K}_i &\implies \left(\mathbf{x}_0^*(\mathbf{y}_i^*)^\top = \mathbf{x}_1^*(\mathbf{y}_i^*)^\top\right) \vee P(x^*, y) = 0. \end{aligned} \tag{33}$$

Note that mpk_i serves as a *general* entry in D_i while mpk_i^* is the *specific* challenge public for slot i; for $\mathsf{mpk}_i \in D_i$, there can be more than one assignments, since the adversary can invoke $\mathsf{OGen}(i)$ for many times. We prove the Lemma 7 via the 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:
$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \mathbf{AV}]_1, \left\{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{AW}_{0,i}]_1\right\}_{i\in[L]}, \left\{[\mathbf{B}_1\mathbf{R}_j]_2\right\}_{j\in[L]} \\ \left\{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_j)]_2\right\}_{j\in[L],i\in[L]\setminus\{j\}} \end{pmatrix}.$$
    where $\mathsf{crs}_i \in \mathsf{LGen}_1(1^\lambda, \mathbb{G}_1, [\mathbf{A}_i]_1)$ with $\mathbf{A}_i = \binom{\mathbf{A}}{\mathbf{G}_i}$, $\mathsf{crs}_{i,j} \in \mathsf{LGen}_2(1^\lambda, \mathbb{G}_2, [\mathbf{B}_{i,j}]_2)$ with $\mathbf{B}_{i,j} = \left(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,j}\right)$.

- For each $i \in [L]$, each $\mathsf{mpk}_i \in D_i$ is in the form:

$$\mathsf{mpk}_i = \left(\begin{array}{l} [\overbrace{\mathbf{AU}_i}^{\mathbf{T}_{0,i}}, \overbrace{\mathbf{AW}_{1,i}}^{\mathbf{T}_{1,i}}, \overbrace{\mathbf{G}_i\mathbf{U}_i}^{\mathbf{Q}_{0,i}}, \overbrace{\mathbf{G}_i\mathbf{W}_{1,i}}^{\mathbf{Q}_{1,i}}]_1, \pi_i \\ \{[\underbrace{\mathbf{U}_i\mathbf{B}_1\mathbf{R}_j}_{\mathbf{H}_{0,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j)}_{\mathbf{H}_{1,i,j}}, \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})}_{\mathbf{P}_{i,j}}]_2, \pi_{i,j}\}_{j \in [L]\setminus\{i\}} \end{array} \right)$$

  where $\pi_i \leftarrow \mathsf{LPrv}_1(\mathsf{crs}_i, [\mathbf{F}_i]_1, (\mathbf{U}_i \| \mathbf{W}_{1,i}))$ with $\mathbf{F}_i = \begin{pmatrix} \mathbf{A}(\mathbf{U}_i \| \mathbf{W}_{1,i}) \\ \mathbf{G}_i(\mathbf{U}_i \| \mathbf{W}_{1,i}) \end{pmatrix}$, $\pi_{i,j} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,j}, [\mathbf{F}_{i,j}]_2, \mathbf{W}_{1,i})$ with $\mathbf{F}_{i,j} = \big(\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j) \| \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})\big)$. And $(\mathbf{U}_i, \mathbf{W}_{1,i})$ is the corresponding msk_i.
- For all $i \in [L]$, mpk_i^* is in the form:

$$\mathsf{mpk}_i^* = ([\mathbf{T}_{0,i}^*, \mathbf{T}_{1,i}^*, \mathbf{Q}_{0,i}^*, \mathbf{Q}_{1,i}^*]_1, \pi_i^*; \{[\mathbf{H}_{0,i,j}^*, \mathbf{H}_{1,i,j}^*, \mathbf{P}_{i,j}^*]_2, \pi_{i,j}^*\}_{j \in [L]\setminus\{i\}})$$

  such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i^*) = 1$ which means $\mathsf{LVer}_1\left(\mathsf{crs}_i, \begin{bmatrix} (\mathbf{T}_{0,i}^*, \mathbf{T}_{1,i}^*) \\ (\mathbf{Q}_{0,i}^*, \mathbf{Q}_{1,i}^*) \end{bmatrix}_1, \pi_i^*\right) = 1$ and $\mathbf{AH}_{0,i,j}^* = \mathbf{T}_{0,i}^*\mathbf{B}_1\mathbf{R}_j$, $\mathbf{AH}_{1,i,j}^* = \mathbf{T}_{1,i}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j)$, $\mathsf{LVer}_2(\mathsf{crs}_{i,j}, [\mathbf{H}_{1,i,j} \| \mathbf{P}_{i,j}]_2, \pi_{i,j}^*) = 1$ for each $j \in [L] \setminus \{i\}$.
- For each $j \in [L]$ such that $\mathsf{mpk}_j^* \in D_j$, and each $y \in \mathcal{K}_j$, secret key returned from $\mathsf{OKey}(j, y)$ is in the form:

$$\mathsf{sk}_{j,y} = \left(\left[\underbrace{\mathbf{B}_1\mathbf{R}_j\mathbf{R}}_{\mathbf{K}_0}, \underbrace{\sum_{i \in [L]\setminus\{j^*\}} \mathbf{H}_{1,i,j}(\mathbf{I}_{n'} \otimes \mathbf{R})}_{\mathbf{K}_1}, \underbrace{\mathbf{U}_j\mathbf{B}_1\mathbf{R}_j(\mathbf{a}_y \otimes \mathbf{I}_k) + \mathbf{W}_{1,j}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j\mathbf{R})(\mathbf{K}_y \otimes \mathbf{I}_k)}_{\mathbf{K}_2} \right]_2 \right).$$

  where $\mathbf{R} \leftarrow \mathbb{Z}_p^{k \times k}$ is freshly sampled for each query and $(\mathbf{U}_j^*, \mathbf{W}_{1,j}^*) = \mathsf{msk}_j^* = \mathcal{D}_j[\mathsf{mpk}_j^*]$.
- ct^* for $(\mathbf{x}_0^*, \mathbf{x}_1^*)$ and x^* is in the form of

$$\mathsf{ct}^* = \left(\begin{array}{l} \left[\overbrace{\mathbf{sA}}^{\mathbf{c}_0^*}, \overbrace{\mathbf{sAV}}^{\mathbf{c}_1^*}, \overbrace{\sum_{i \in [L]} (\mathbf{sT}_{0,i}^* + \mathbf{sAW}_{0,i}((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{5k+2}))}^{\mathbf{c}_2^*} \right]_1, \\ \left[\underbrace{\mathbf{x}_b^* \otimes \mathbf{sAV} + \sum_{i \in [L]} \mathbf{sAW}_{0,i}}_{\mathbf{c}_3^*}, \underbrace{\sum_{i \in [L]} \mathbf{sT}_{1,i}^*(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2})}_{\mathbf{c}_4^*} \right]_1 \end{array} \right).$$

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

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

$$\widetilde{\pi}_i \leftarrow \boxed{\mathsf{LSim}_1}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{F}_i]_1) \quad \text{where} \quad \mathbf{F}_i = \begin{pmatrix} \mathbf{A}(\mathbf{U}_i \| \mathbf{W}_{1,i}) \\ \mathbf{G}_i(\mathbf{U}_i \| \mathbf{W}_{1,i}) \end{pmatrix}.$$

  We have $\mathsf{G}_1 \equiv \mathsf{G}_0$. This follows from the perfect zero-knowledge of Π_1.

– 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 $\mathbf{G}_i$ in crs with

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

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

– G_3: Identical to G_2 except that we replace $\mathbf{s}\mathbf{T}^*_{0,i}$ with $\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i}$ in $\mathbf{c}^*_2$, and replace $\mathbf{s}\mathbf{T}^*_{1,i}$ with $\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{1,i}$ in $\mathbf{c}^*_4$; namely, we have

$$\mathbf{c}^*_2 = \textstyle\sum_{i\in[L]}(\boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i}} + \mathbf{s}\mathbf{A}\mathbf{W}_i((\mathbf{y}^*_i)^\top \otimes \mathbf{I}_{5k+2})),$$
$$\mathbf{c}^*_4 = \textstyle\sum_{i\in[L]} \boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{1,i}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2}).$$

We have $\mathsf{G}_3 \approx_c \mathsf{G}_2$. This follows from stronger unbounded simulation soundness of Π_1 along with the fact that $\mathsf{LVer}_1(\mathsf{crs}_i, [\mathbf{F}^*_i]_1, \pi^*_i) = 1$ for all $i \in [L]$ where $\mathbf{F}^*_i = \begin{pmatrix}(\mathbf{T}^*_{0,i}, \mathbf{T}^*_{1,i})\\(\mathbf{Q}^*_{0,i}, \mathbf{Q}^*_{1,i})\end{pmatrix}$. Assume $\mathsf{mpk}^*_{i^*} \notin D_{i^*}$, i.e., $\mathsf{mpk}^*_{i^*}$ is malicious. In the reduction, we guess $i^* \leftarrow [L]$ and obtain $\mathbf{A}, \widehat{\mathbf{G}}_{i^*}, \mathsf{crs}_{i^*}$ as input; we simulate honestly as in G_3 except that for all $\mathsf{mpk}_{i^*} \in D_{i^*}$, 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 $\mathsf{mpk}^*_{i^*} \notin D_{i^*}$. Observe that once it happens that $\mathbf{e}_1\widetilde{\mathbf{G}}_{i^*}^{-1}(\mathbf{Q}^*_{0,i^*}\|\mathbf{Q}^*_{1,i^*}) \neq \mathbf{s}(\mathbf{T}^*_{0,i^*}\|\mathbf{T}^*_{1,i^*})$, we must have $\mathbf{F}^*_{i^*} \notin \mathsf{span}^\top(\mathbf{A}_{i^*})$. When $\mathsf{mpk}^*_{i^*} \in D_{i^*}$, we always have $\mathsf{G}_3 \equiv \mathsf{G}_2$.

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

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

and generate the challenge ciphertext as follows:

$$\mathsf{ct}^* = \left(\begin{bmatrix}\overbrace{\boxed{\mathbf{c}}}^{\mathbf{c}^*_0}, \overbrace{\boxed{\mathbf{c}}\mathbf{V}}^{\mathbf{c}^*_1}, \overbrace{\sum_{i\in[L]}(\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i} + \boxed{\mathbf{c}}\mathbf{W}_{0,i}((\mathbf{y}^*_i)^\top \otimes \mathbf{I}_{5k+2}))}^{\mathbf{c}^*_2}\end{bmatrix}_1,\right.$$
$$\left.\begin{bmatrix}\underbrace{\mathbf{x}^*_b \otimes \boxed{\mathbf{c}}\mathbf{V} + \sum_{i\in[L]}\boxed{\mathbf{c}}\mathbf{W}_{0,i}}_{\mathbf{c}^*_3}, \underbrace{\sum_{i\in[L]}\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{1,i}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2})}_{\mathbf{c}^*_4}\end{bmatrix}_1\right).$$

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

$$\widetilde{\mathbf{V}} \leftarrow \mathbb{Z}_p^{k\times(5k+2)}$$

we replace $\mathbf{c}\mathbf{V}$ in challenge ciphertext with

$$\mathbf{v} \leftarrow \mathbb{Z}_p^{1\times(5k+2)}$$

In particular, we generate crs as below:

$$\mathsf{crs} = \begin{pmatrix}[\mathbf{A}, \boxed{\widetilde{\mathbf{V}}}]_1, \{\mathsf{crs}_i, [\mathbf{G}_i, \mathbf{A}\mathbf{W}_{0,i}]_1\}_{i\in[L]}, \{[\mathbf{B}_1\mathbf{R}_j]_2\}_{j\in[L]}\\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_j)]_2\}_{j\in[L],i\in[L]\setminus\{j\}}\end{pmatrix},$$

and generate the challenge ciphertext as

$$\mathsf{ct}^* = \left(\begin{bmatrix}\overbrace{\mathbf{c}}^{\mathbf{c}^*_0}, \overbrace{\boxed{\mathbf{v}}}^{\mathbf{c}^*_1}, \overbrace{\sum_{i\in[L]}(\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i} + \mathbf{c}\mathbf{W}_{0,i}((\mathbf{y}^*_i)^\top \otimes \mathbf{I}_{5k+2}))}^{\mathbf{c}^*_2}\end{bmatrix}_1,\right.$$
$$\left.\begin{bmatrix}\underbrace{\mathbf{x}^*_b \otimes \boxed{\mathbf{v}} + \sum_{i\in[L]}\mathbf{c}\mathbf{W}_{0,i}}_{\mathbf{c}^*_3}, \underbrace{\sum_{i\in[L]}\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{1,i}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2})}_{\mathbf{c}^*_4}\end{bmatrix}_1\right).$$

We have $\mathsf{G}_5 \equiv \mathsf{G}_4$. This follows from the fact that when $\mathbf{V}$ is uniformly sampled from $\mathbb{Z}_p^{(k+1)\times(5k+2)}$ 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 $\widetilde{\mathbf{V}} \leftarrow \mathbb{Z}_p^{k\times(5k+2)}, \mathbf{v} \leftarrow \mathbb{Z}_p^{1\times(5k+2)}$ (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 change $\mathbf{c}_3^*$ as follows:

$$\mathbf{c}_3^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1,3)} + \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]} \mathbf{cW}_{0,i}$$

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):

$$\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]} (\mathbf{cW}_{0,i})^{(2)} \equiv \sum_{i\in[L]} (\mathbf{cW}_{0,i})^{(2)}$$

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 $(\mathbf{cW}_{0,i})^{(2)}$ is hidden, this can imply that $\sum_{i\in[L]} (\mathbf{cW}_{0,i})^{(2)}$ 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 $\mathbf{B}_1\mathbf{R}_j$ in crs with

$$\boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_j} \quad \text{where} \quad \widetilde{\mathbf{R}}_j \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$$

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 $\mathbf{c}_3^*$ as follows:

$$\mathbf{c}_3^* = \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(1,3)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \sum_{i\in[L]} \mathbf{cW}_{0,i}$$

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):

$$\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(1,3)} + \sum_{i\in[L]} (\mathbf{cW}_{0,i})^{(1,3)} \equiv \sum_{i\in[L]} (\mathbf{cW}_{0,i})^{(1,3)}$$

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 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, $\mathsf{mpk}_i \in D_i$ and $\mathbf{c}_3^*$, with highlighting relevant terms in the following sub-sequence with dashed boxes as follows:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{AW}_{0,i}]_1\}_{i\in[L]} \\ \{[\mathbf{B}_2\widetilde{\mathbf{R}}_j]_2\}_{j\in[\ell-1]}, \boxed{[\mathbf{B}_1\mathbf{R}_\ell]_2}, \{[\mathbf{B}_1\mathbf{R}_j]_2\}_{j\in[\ell+1,L]} \\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j)]_2\}_{j\in[\ell-1], i\in[L]\setminus\{j\}}, \\ \{\boxed{\mathsf{crs}_{i,\ell}}, [\mathbf{G}_{i,\ell}]_2, \boxed{[\mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_\ell)]_2}\}_{i\in[L]\setminus\{\ell\}}, \\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_j)]_2\}_{j\in[\ell+1,L], i\in[L]\setminus\{j\}} \end{pmatrix}$$

$$\mathsf{mpk}_i = \begin{cases} \begin{pmatrix} [\mathbf{AU}_i, \mathbf{AW}_{1,i}, \widehat{\mathbf{G}}_i\mathbf{U}_i, \widehat{\mathbf{G}}_i\mathbf{W}_{1,i}]_1, \widetilde{\pi}_i \\ \{[\mathbf{U}_i\mathbf{B}_2\widetilde{\mathbf{R}}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[\ell-1]\setminus\{i\}}, \\ \boxed{[\mathbf{U}_i\mathbf{B}_1\mathbf{R}_\ell, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_\ell)]_2}, [\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})]_2, \boxed{\pi_{i,\ell}}; \\ \{[\mathbf{U}_i\mathbf{B}_1\mathbf{R}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[\ell+1,L]\setminus\{i\}} \end{pmatrix} & \text{if } i \neq \ell \\ \begin{pmatrix} [\mathbf{AU}_\ell, \mathbf{AW}_{1,\ell}, \widehat{\mathbf{G}}_\ell\mathbf{U}_\ell, \widehat{\mathbf{G}}_\ell\mathbf{W}_{1,\ell}]_1, \widetilde{\pi}_\ell \\ \{[\mathbf{U}_\ell\mathbf{B}_2\widetilde{\mathbf{R}}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j), \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2, \pi_{\ell,j}\}_{j\in[\ell-1]}, \\ \{[\mathbf{U}_\ell\mathbf{B}_1\mathbf{R}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j), \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2, \pi_{\ell,j}\}_{j\in[\ell+1,L]} \end{pmatrix} & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_3^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*} \otimes \mathbf{v}^{(3)} + \mathbf{cW}_{0,\ell} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{cW}_{0,i}$$

where $\widetilde{\mathbf{R}}_j \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ for all $j \in [\ell-1]$. And when $\mathsf{mpk}^*_\ell \in D_\ell$, for each $y \in \mathcal{K}_\ell$ we recall secret key returned from $\mathsf{OKey}(\ell, y)$ in the following form

$$\mathsf{sk}_{\ell,y} = \left(\begin{array}{l} \boxed{[\mathbf{B}_1\mathbf{R}_\ell\mathbf{R}]_2}, \ \left[\sum_{i\in[L]\setminus\{\ell\}} \mathbf{H}^*_{1,i,\ell}(\mathbf{I}_{n'}\otimes\mathbf{R})\right]_2, \\ \boxed{\left[\mathbf{U}^*_\ell\mathbf{B}_1\mathbf{R}_\ell(\mathbf{a}_y\otimes\mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'}\otimes\mathbf{B}_1\mathbf{R}_\ell\mathbf{R})(\mathbf{K}_y\otimes\mathbf{I}_k)\right]_2} \end{array}\right)$$

where $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times k}$ is freshly sampled for each $y \in \mathcal{K}_\ell$. Clearly, 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 $\mathbf{B}_1\mathbf{R}_\ell$ in crs with

$$\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell} \quad \text{where} \quad \widehat{\mathbf{R}}_\ell \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$$

In particular, we change the dashed boxed term in crs as follow

$$[\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell}]_2, \{[\mathbf{W}_{0,i}(\mathbf{I}_{n_1}\otimes\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell})]_2\},$$

and for all $i \in [L]\setminus\{\ell\}$

$$\mathsf{crs}_{i,\ell} \in \mathsf{LGen}_2(1^\lambda, \mathbb{G}_2, [\boxed{\mathbf{B}_{i,\ell}}]_2) \quad \text{with} \quad \mathbf{B}_{i,\ell} = (\mathbf{I}_{n'}\otimes\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell} \| \mathbf{I}_{n'}\otimes\mathbf{G}_{i,\ell});$$

for all $i \in [L]\setminus\{\ell\}$, change the dash-boxed terms in each $\mathsf{mpk}_i \in D_i$ as follow:

$$[\mathbf{U}_i\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell}, \mathbf{W}_{1,i}(\mathbf{I}_{n'}\otimes\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell})]_2,$$

and

$$\pi_{i,\ell} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,\ell}, [\boxed{\mathbf{F}_{i,\ell}}]_2, \mathbf{W}_{1,i}) \quad \text{where} \quad \mathbf{F}_{i,\ell} = (\mathbf{W}_{1,i}(\mathbf{I}_{n'}\otimes\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell}) \| \mathbf{W}_{1,i}(\mathbf{I}_{n'}\otimes\mathbf{G}_{i,\ell}));$$

when $\mathsf{mpk}^*_\ell \in \mathcal{K}_\ell$, for each $y \in \mathcal{K}_\ell$, change the dashboxed term in returned $\mathsf{sk}_{\ell,y}$ as follows

$$[\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell}\mathbf{R}]_2, [\mathbf{U}^*_\ell\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell}(\mathbf{a}'_{y'}\otimes\mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'}\otimes\boxed{\mathbf{B}_3\widehat{\mathbf{R}}_\ell}\mathbf{R})(\mathbf{K}'_{y'}\otimes\mathbf{I}_k)]_2.$$

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

$$[\mathbf{t}^\top_{0,\kappa}]_2 \approx_c [\mathbf{t}^\top_{1,\kappa}]_2 \quad \text{given} \quad [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_1^\parallel, \mathbf{B}_3^\parallel), \mathsf{basis}(\mathbf{B}_2^\parallel)$$

for all $\kappa \in [k]$. Where $\mathbf{t}^\top_{0,\kappa} \leftarrow \mathsf{span}^\top(\mathbf{B}_1)$ corresponding to the κ-th column of $\mathbf{B}_1\mathbf{R}_\ell$ in $\mathsf{G}_{7,\ell-1,0}$, and $\mathbf{t}^\top_{1,\kappa} \leftarrow \mathsf{span}^\top(\mathbf{B}_3)$ corresponding to κ-th column of $\mathbf{B}_3\widehat{\mathbf{R}}_\ell$ in $\mathsf{G}_{7,\ell-1,1}$.

– $\mathsf{G}_{7,\ell-1,2}$: 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 will provide the proof by considering two cases: (1) $\mathbf{x}^*_0(\mathbf{y}^*_\ell)^\top = \mathbf{x}^*_1(\mathbf{y}^*_\ell)^\top$; (2) $\mathbf{x}^*_0(\mathbf{y}^*_\ell)^\top \neq \mathbf{x}^*_1(\mathbf{y}^*_\ell)^\top$. We provide the detailed proof of these two cases in Section 8.3 and Section 8.4 respectively.

– $\mathsf{G}_{7,\ell-1,3}$: Identical to $\mathsf{G}_{7,\ell-1,2}$ except that we replace all $\mathbf{B}_3\widehat{\mathbf{R}}_\ell$ in crs with

$$\boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell} \quad \text{where} \quad \widetilde{\mathbf{R}}_\ell \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$$

In particular, we change the dashed boxed term in crs as follow

$$[\boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell}]_2, \{[\mathbf{W}_{0,i}(\mathbf{I}_{n_1}\otimes\boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell})]_2\}$$

and for all $i \in [L] \setminus \{\ell\}$

$$\mathsf{crs}_{i,\ell} \in \mathsf{LGen}_2(1^\lambda, \mathbb{G}_2, [\boxed{\mathbf{B}_{i,\ell}}]_2) \quad \text{with} \quad \mathbf{B}_{i,\ell} = (\mathbf{I}_{n'} \otimes \boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell} \| \mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})$$

for all $i \in [L] \setminus \{\ell\}$, change the dash-boxed terms in each $\mathsf{mpk}_i \in D_i$ as follow:

$$[\mathbf{U}_i \boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell}, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell})]_2,$$

and

$$\pi_{i,\ell} \leftarrow \mathsf{LPrv}_2(\mathsf{crs}_{i,\ell}, [\boxed{\mathbf{F}_{i,\ell}}]_2, \mathbf{W}_{1,i}) \quad \text{where} \quad \mathbf{F}_{i,\ell} = (\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell}) \| \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell}))$$

when $\mathsf{mpk}^*_\ell \in \mathcal{K}_\ell$, for each $y \in \mathcal{K}_\ell$, change the dashboxed term in returned $\mathsf{sk}_{\ell,y}$ as follows

$$[\boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell}\mathbf{R}]_2, [\mathbf{U}^*_\ell \boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell}(\mathbf{a}'_{y'} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{B}_2\widetilde{\mathbf{R}}_\ell}\mathbf{R})(\mathbf{K}'_{y'} \otimes \mathbf{I}_k)]_2.$$

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

$$[\mathbf{t}^\top_{0,\kappa}]_2 \approx_c [\mathbf{t}^\top_{1,\kappa}]_2 \quad \text{given} \quad [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel), \mathsf{basis}(\mathbf{B}_1^\parallel)$$

for all $\kappa \in [k]$. Where $\mathbf{t}^\top_{0,\kappa} \leftarrow \mathsf{span}^\top(\mathbf{B}_3)$ corresponding to the κ-th column of $\mathbf{B}_3\widehat{\mathbf{R}}_\ell$ in $\mathsf{G}_{7,\ell-1,2}$, and $\mathbf{t}^\top_{1,\kappa} \leftarrow \mathsf{span}^\top(\mathbf{B}_2)$ corresponding to the κ-th column of $\mathbf{B}_2\widetilde{\mathbf{R}}_\ell$ in $\mathsf{G}_{7,\ell-1,3}$.

– $\mathsf{G}_{7,\ell-1,4}$: Identical to $\mathsf{G}_{7,\ell-1,3}$ except that we generate the $\mathbf{c}^*_3$ as follows:

$$\mathbf{c}^*_2 = \mathbf{x}^*_b \otimes \mathbf{v}^{(1)} + \mathbf{x}^*_0 \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}^*_b} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell} + \sum_{i \in [L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_{0,i}$$

We have $\mathsf{G}_{7,\ell-1,4} \approx_c \mathsf{G}_{7,\ell-1,3}$. The proof is analogous to that for $\mathsf{G}_{7,\ell-1,2} \approx \mathsf{G}_{7,\ell-1,1}$, by instead $\mathbf{B}_3, \widehat{\mathbf{R}}_\ell$ of $\mathbf{B}_2, \widetilde{\mathbf{R}}_\ell$.

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

8.3 From $\mathsf{G}_{7,\ell-1,1}$ to $\mathsf{G}_{7,\ell-1,2}$: If $\mathbf{x}^*_0(\mathbf{y}^*_\ell)^\top = \mathbf{x}^*_1(\mathbf{y}^*_\ell)^\top$

We review $\mathsf{G}_{7,\ell-1,1}$ and $\mathsf{G}_{7,\ell-1,2}$ in the following form. Here we use gray boxes to indicate the difference between two games, where $b' = b$ in $\mathsf{G}_{7,\ell-1,1}$ and $b' = 0$ in $\mathsf{G}_{7,\ell-1,2}$, and we use dashed boxes to highlight those terms that are relevant to our proof in this case.

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{A}\mathbf{W}_{0,i}]_1\}_{i\in[L]} \\ \{[\mathbf{B}_2\widetilde{\mathbf{R}}_j]_2\}_{j\in[\ell-1]}, \boxed{[\mathbf{B}_3\widehat{\mathbf{R}}_\ell]_2}, \{[\mathbf{B}_1\mathbf{R}_j]_2\}_{j\in[\ell+1,L]} \\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j)]_2\}_{j\in[\ell-1], i\in[L]\setminus\{j\}}, \\ \{\mathsf{crs}_{i,\ell}, [\mathbf{G}_{i,\ell}]_2, \boxed{[\mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell)]_2}\}_{i\in[L]\setminus\{\ell\}}, \\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_j)]_2\}_{j\in[\ell+1,L], i\in[L]\setminus\{j\}} \end{pmatrix}$$

$$\mathbf{c}^*_2 = \boxed{(\mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}^*_{0,\ell} + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}^*_\ell)^\top \otimes \mathbf{I}_{5k+2}))} + \sum_{i\in[L]\setminus\{\ell\}} (\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}^*_{0,i} + \mathbf{c}\mathbf{W}_{0,i}((\mathbf{y}^*_i)^\top \otimes \mathbf{I}_{5k+2}))$$

$$\mathbf{c}^*_3 = \mathbf{x}^*_b \otimes \mathbf{v}^{(1)} + \mathbf{x}^*_0 \otimes \mathbf{v}^{(2)} + \mathbf{x}^*_{b'} \otimes \mathbf{v}^{(3)} + \boxed{\mathbf{c}\mathbf{W}_{0,\ell}} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_{0.i}$$

We define $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$, $\mathbf{c}\mathbf{c}^\perp = 1$, this use the facts that $\binom{\mathbf{A}}{\mathbf{c}}$ is (row) full-rank w.h.p. With the orthogonality of dual basis, for all $\mathbf{v}^{(3)} \in \mathsf{span}(\mathbf{B}_3^\parallel)$, we have:

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

Notice that with our restrictions (33), if mpk_ℓ^* is corrupted or maliciously generated, it must be in this case; and if mpk_ℓ^* is honest, it has possibility to be in this case. 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 this case:

$$
\begin{aligned}
& \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_2) && \text{//crs} \\
& \mathbf{c}, \mathbf{e}_1 \widetilde{\mathbf{G}}_{0,\ell}^{-1} \mathbf{Q}_{0,\ell}^* + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}), \mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell} && \text{//ct}^* \\
\approx_s\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{e}_1 \widetilde{\mathbf{G}}_\ell^{-1} \mathbf{Q}_{0,\ell}^* + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}) - \boxed{(\mathbf{x}_{b'}^* - \mathbf{x}_0^*)(\mathbf{y}_\ell^*)^\top \otimes \mathbf{v}^{(3)}}, \boxed{\mathbf{x}_0^* \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_{0,\ell} \\
=\ & \mathbf{A}, \mathbf{c}^\perp, \mathbf{B}_1, \mathbf{B}_2, \mathbf{d}_\ell^\top, \mathbf{A}\mathbf{W}_\ell, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_2) \\
& \mathbf{c}, \mathbf{e}_1 \widetilde{\mathbf{G}}_\ell^{-1} \mathbf{Q}_{0,\ell}^* + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}) - \cancel{(\mathbf{x}_{b'}^* - \mathbf{x}_0^*)(\mathbf{y}_\ell^*)^\top \otimes \mathbf{v}^{(3)}}, \mathbf{x}_0^* \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell}
\end{aligned}
$$

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

$$\mathbf{W}_{0,\ell} \mapsto \mathbf{W}_{0,\ell} - \mathbf{c}^\perp((\mathbf{x}_{b'}^* - \mathbf{x}_0^*) \otimes \mathbf{v}^{(3)})$$

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

8.4 From $\mathsf{G}_{7,\ell-1,1}$ to $\mathsf{G}_{7,\ell-1,2}$: If $\mathbf{x}_0^*(\mathbf{y}_\ell^*)^\top \neq \mathbf{x}_1^*(\mathbf{y}_\ell^*)^\top$

Useful Lemma. Before our proceeding, we prepare the following lemmata.

Lemma 8. *For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ such that $\binom{\mathbf{A}}{\mathbf{c}}\mathbf{c}^\perp = \binom{\mathbf{0}}{1}$; any $\mathbf{B}_1 \in \mathbb{Z}_p^{(5k+2)\times k}$, $\mathbf{B}_2 \in \mathbb{Z}_p^{(5k+2)\times(2k+1)}$, $\mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(5k+2)\times(2k+1)}$, with dual basis $\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel$, and any $\mathbf{v}^{(3)} \in \mathsf{span}(\mathbf{B}_3^\parallel)$ such that $\mathbf{v}^{(3)}(\mathbf{B}_1\|\mathbf{B}_2) = \mathbf{0}$; and for any adversary $\mathcal{A}$, there exist an adversary $\mathcal{B}_2$ such that*

$$
\begin{aligned}
& \left| \Pr\left[\mathcal{A}\begin{pmatrix} [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^*, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{B}_3, \mathbf{v}^{(3)}, \\ \mathbf{U}_\ell^*(\mathbf{B}_1\|\mathbf{B}_2), \mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{U}_\ell^*]_1 \end{pmatrix} = 1\right] - \right. \\
& \left. \Pr\left[\mathcal{A}\begin{pmatrix} [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^* + \boxed{\widetilde{u}\mathbf{v}^{(3)}}, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{B}_3, \mathbf{v}^{(3)}, \\ \mathbf{U}_\ell^*(\mathbf{B}_1\|\mathbf{B}_2), \mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell + \boxed{\mathbf{c}^\perp\widetilde{u}\mathbf{v}^{(3)}\mathbf{B}_3\widehat{\mathbf{R}}_\ell}, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{U}_\ell^*]_1 \end{pmatrix} = 1\right] \right| \\
\leq\ & 2 \cdot \mathsf{Adv}_{\mathcal{B}_2}^{MDDH} + \mathsf{negl}(\lambda)
\end{aligned}
$$

where $\widetilde{u} \leftarrow \mathbb{Z}_p$.

Lemma 9. *For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ such that $\binom{\mathbf{A}}{\mathbf{c}}\mathbf{c}^\perp = \binom{\mathbf{0}}{1}$; any $\mathbf{B}_1 \in \mathbb{Z}_p^{(5k+2)\times k}$, $\mathbf{B}_2 \in \mathbb{Z}_p^{(5k+2)\times(2k+1)}$, $\mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(5k+2)\times(2k+1)}$, with dual basis $\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel$; any $\widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}} \in \mathbb{Z}_p^{(2k+1)\times k}$ and $\mathbf{R}^\perp \in \mathbb{Z}_p^{k\times(2k+1)}$ such that $\mathbf{R}^\perp(\widehat{\mathbf{R}}_\ell\|\widetilde{\mathbf{R}}) = (\mathbf{0}\|\mathbf{I}_k)$; and for any adversary $\mathcal{A}$, there exist an adversary $\mathcal{B}_2$ such that*

$$
\begin{aligned}
& \left| \Pr\left[\mathcal{A}\begin{pmatrix} [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \mathbf{c}\mathbf{W}_{1,\ell}^*, \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3, \\ \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \\ [\mathbf{B}_1]_2, [\mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{W}_{1,\ell}^*]_1, \{[\mathbf{G}_{\ell,j}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{\forall j\in[L]\setminus\{\ell\}} \end{pmatrix} = 1\right] - \right. \\
& \left. \Pr\left[\mathcal{A}\begin{pmatrix} [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \mathbf{c}\mathbf{W}_{1,\ell}^* + \boxed{\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp(\mathbf{B}_3^\parallel)^\top)}, \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3, \\ \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}) + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{w}}}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \\ [\mathbf{B}_1]_2, [\mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{W}_{1,\ell}^*]_1, \{[\mathbf{G}_{\ell,j}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{\forall j\in[L]\setminus\{\ell\}} \end{pmatrix} = 1\right] \right| \\
\leq\ & 4 \cdot \mathsf{Adv}_{\mathcal{B}_2}^{MDDH} + \mathsf{negl}(\lambda)
\end{aligned}
$$

where $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{kn'}$

We provide the proof of Lemma 8 and Lemma 9 in Appendix A.

Notice that with our restrictions (33), this case implies that $\mathsf{mpk}_\ell^* \in D_\ell \setminus C_\ell$ and $P(x^*, y) = 0$ for all $y \in \mathcal{K}_\ell$. Define $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$, $\mathbf{c}\mathbf{c}^\perp = 1$, this use the facts that $\binom{\mathbf{A}}{\mathbf{c}}$ is (row) full-rank w.h.p. With the orthogonality of dual basis, for all $\mathbf{v}^{(3)} \in \mathsf{span}(\mathbf{B}_3^{\parallel})$, we have:

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

Assume the adversary makes Q queries to $\mathsf{OKey}(\ell, \cdot)$, we prove $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$ in this case via following sequence of hybrid argument:

– H_0 : Identical to $\mathsf{G}_{7,\ell-1,1}$. We review crs, $\mathsf{mpk}_i \in D_i$, $\mathbf{c}_2^*, \mathbf{c}_3^*, \mathbf{c}_4^*$ and $\mathsf{sk}_{\ell,y}$ for all $y \in \mathcal{K}_\ell$ in the following form. Here we (1) use gray boxes to indicate the changed term between $\mathsf{G}_{7,\ell-1,1}$ and $\mathsf{G}_{7,\ell-1,2}$, (2) use dashed boxes to highlight the terms relevant to the proof in following hybrid sequence:

$$\mathsf{crs} = \left(\begin{array}{l} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \left\{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{A}\mathbf{W}_{0,i}]_1\right\}_{i\in[L]\setminus\{\ell\}}, \mathsf{crs}_\ell, [\boxed{\widehat{\mathbf{G}}_\ell}, \mathbf{A}\mathbf{W}_{0,\ell}]_1 \\ \left\{[\mathbf{B}_2\widetilde{\mathbf{R}}_j]_2\right\}_{j\in[\ell-1]}, \boxed{[\mathbf{B}_3\widehat{\mathbf{R}}_\ell]_2}, \left\{[\mathbf{B}_1\mathbf{R}_j]_2\right\}_{j\in[\ell+1,L]} \\ \left\{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j)]_2\right\}_{j\in[\ell-1], i\in[L]\setminus\{j\}}, \\ \left\{\mathsf{crs}_{i,\ell}, [\mathbf{G}_{i,\ell}]_2, \boxed{[\mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell)]_2}\right\}_{i\in[L]\setminus\{\ell\}}, \\ \left\{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_j)]_2\right\}_{j\in[\ell+1,L], i\in[L]\setminus\{j\}} \end{array}\right)$$

$$\mathsf{mpk}_i = \begin{cases} \left(\begin{array}{l} [\mathbf{A}\mathbf{U}_i, \mathbf{A}\mathbf{W}_{1,i}, \widehat{\mathbf{G}}_i\mathbf{U}_i, \widehat{\mathbf{G}}_i\mathbf{W}_{1,i}]_1, \widetilde{\pi}_i \\ \{[\mathbf{U}_i\mathbf{B}_2\widetilde{\mathbf{R}}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[\ell-1]\setminus\{i\}}, \\ \boxed{[\mathbf{U}_i\mathbf{B}_3\widehat{\mathbf{R}}_\ell, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell)]_2}, [\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})]_2, \pi_{i,\ell}; \\ \{[\mathbf{U}_i\mathbf{B}_1\mathbf{R}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[\ell+1,L]\setminus\{i\}} \end{array}\right) & \text{if } i \neq \ell \\ \left(\begin{array}{l} [\mathbf{A}\mathbf{U}_\ell, \mathbf{A}\mathbf{W}_{1,\ell}]_1, \boxed{[\widehat{\mathbf{G}}_\ell\mathbf{U}_\ell, \widehat{\mathbf{G}}_\ell\mathbf{W}_{1,\ell}]_1}, \widetilde{\pi}_\ell \\ \{[\mathbf{U}_\ell\mathbf{B}_2\widetilde{\mathbf{R}}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j), \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2, \pi_{\ell,j}\}_{j\in[\ell-1]}, \\ \{[\mathbf{U}_\ell\mathbf{B}_1\mathbf{R}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j), \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2, \pi_{\ell,j}\}_{j\in[\ell+1,L]} \end{array}\right) & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_2^* = \boxed{(\mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}_{0,\ell}^* + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}))} + \sum_{i\in[L]\setminus\{\ell\}} (\mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_{0,i}^* + \mathbf{c}\mathbf{W}_{0,i}((\mathbf{y}_i^*)^\top \otimes \mathbf{I}_{5k+2}))$$

$$\mathbf{c}_3^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_b^*} \otimes \mathbf{v}^{(3)} + \boxed{\mathbf{c}\widetilde{\mathbf{W}}_{0,\ell}} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{c}\mathbf{W}_{0.i}$$

$$\mathbf{c}_4^* = \boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}_{1,\ell}^*(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2})} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_{1,i}^*(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2}).$$

This case implies that $\mathsf{mpk}_\ell^* \in D_\ell \setminus C_\ell$, namely mpk_ℓ^* is honest and corresponding $\mathsf{msk}_\ell^* = (\mathbf{U}_\ell^*, \mathbf{W}_{1,\ell}^*)$ is hidden from the adversary; moreover, for each $y \in \mathcal{K}_\ell$, it holds that $P(x^*, y) = 0$. The adversary can only obtain secret keys as follows for all $y \in \mathcal{K}_\ell$:

$$\mathsf{sk}_{\ell,y} = \left(\begin{array}{l} \overbrace{[\mathbf{B}_3\widehat{\mathbf{R}}_\ell\mathbf{R}]_2}^{\mathbf{K}_0}, \left[\overbrace{\sum_{i\in[L]\setminus\{\ell\}} \mathbf{H}_{1,i,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{R})}^{\mathbf{K}_1}\right]_2, \\ \underbrace{\left[\boxed{\mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell(\mathbf{a}_y \otimes \mathbf{I}_k) + \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell\mathbf{R})(\mathbf{K}_y \otimes \mathbf{I}_k)}\right]_2}_{\mathbf{K}_2} \end{array}\right)$$

where $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times k}$ is freshly sampled for each $y \in \mathcal{K}_\ell$. Clearly, we have $\mathsf{H}_0 = \mathsf{G}_{7,\ell-1,1}$; all changes are conceptual.

– H_1 : Identical to H_0 we rewrite the dashboxed terms in $\mathbf{c}_2^*$ and $\mathbf{c}_4^*$ as follow:

$$\boxed{\mathbf{c}\mathbf{U}_\ell^*} + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}) \quad \text{and} \quad \boxed{\mathbf{c}\mathbf{W}_{1,\ell}^*}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2})$$

and replace all $\widehat{\mathbf{G}}_\ell = \widetilde{\mathbf{G}}_\ell \left(\begin{smallmatrix} \mathbf{c} \\ \mathbf{I}_{k+1} \end{smallmatrix}\right)$ with $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have $\mathsf{H}_1 \equiv \mathsf{H}_0$. This follows from the fact that mpk_ℓ^* must be honest in this case. Namely, we know $\mathsf{msk}_\ell^* = (\mathbf{U}_\ell^*, \mathbf{W}_{1,\ell}^*)$ such that $(\mathbf{T}_{0,\ell}^* \| \mathbf{T}_{1,\ell}^*) = \mathbf{A}(\mathbf{U}_\ell^* \| \mathbf{W}_{1,\ell}^*)$, $(\mathbf{Q}_{0,\ell}^* \| \mathbf{Q}_{1,\ell}^*) = \widehat{\mathbf{G}}_\ell(\mathbf{U}_\ell^* \| \mathbf{W}_{1,\ell}^*)$, and can directly simulate $\mathbf{c}(\mathbf{U}_\ell^* \| \mathbf{W}_{1,\ell}^*)$ instead of $\mathbf{e}_1^\top \widetilde{\mathbf{G}}_\ell^{-1}(\mathbf{Q}_{0,\ell}^* \| \mathbf{Q}_{1,\ell}^*)$, so that we can also replace $\widehat{\mathbf{G}}_\ell$ with a truly random $\mathbf{G}_\ell$ such as in "$\mathsf{G}_1 \equiv \mathsf{G}_2$".

– $\mathsf{H}_{2,q}$, $(q \in [0, Q])$: Identical to H_1, except that for the first q answers to $\mathsf{OKey}(\ell, \cdot)$, we replace $[\mathbf{K}_2]_2$ in dashboxed with

$$[\mathbf{K}_2]_2 = \left[(\mathbf{U}_\ell^* \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + \boxed{\mathbf{c}^\perp \widehat{\mathbf{k}}})(\mathbf{a}_y \otimes \mathbf{I}_k) + \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3 \widehat{\mathbf{R}}_\ell \mathbf{R})(\mathbf{K}_y \otimes \mathbf{I}_k)\right]_2$$

where $\widehat{\mathbf{k}} \leftarrow \mathbb{Z}_p^{1\times k}$. We have that

- $\mathsf{H}_{2,0} = \mathsf{H}_1$; the two games are exactly identical, since $[0] = \emptyset$;
- $\mathsf{H}_{2,q} \approx_c \mathsf{H}_{2,q-1}$; we will employ a sub-sequence of hybrid arguments for the proof described later.

– H_3 : Identical to $\mathsf{H}_{2,Q}$ except that for we generate $\mathbf{c}_3^*$ as

$$\mathbf{c}_3^* = \mathbf{x}_b^* \otimes \mathbf{v}^{(1)} + \mathbf{x}_0^* \otimes \mathbf{v}^{(2)} + \boxed{\mathbf{x}_0^*} \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell} + \sum_{i \in [L] \setminus \{\ell\}} \mathbf{c}\mathbf{W}_{0.i}$$

We have $\mathsf{H}_3 \approx_c \mathsf{H}_{2,Q}$. Let's use $\mathbf{x}_{b'}^*$ to denote the challenge message, which is $\mathbf{x}_b^*$ in $\mathsf{H}_{2,Q}$ and $\mathbf{x}_0^*$ in H_3 respectively. This follows from the following argument holds for both $b' = b$ (in $\mathsf{H}_{2,Q}$) and $b' = 0$ (in H_3):

$$\begin{aligned}
&[\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, [\mathbf{A}\mathbf{W}_{0,\ell}]_1, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_2) && \text{//crs, } \mathsf{mpk}_\ell \\
&\mathbf{c}, \mathbf{c}\mathbf{U}_\ell^* + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}), \mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell} && \text{//ct}^* \\
&[\mathbf{A}\mathbf{U}_\ell^*]_1, [\mathbf{G}_\ell \mathbf{U}_\ell^*]_1, \mathbf{U}_\ell^* \mathbf{B}_1, \mathbf{U}_\ell^* \mathbf{B}_2, \mathbf{U}_\ell^* \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + \mathbf{c}^\perp \widehat{\mathbf{k}} && \text{//}\mathsf{mpk}_\ell^*, \{\mathsf{sk}_{\ell,y}\}_{y \in \mathcal{K}_\ell} \\
\approx_c\ &[\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, [\mathbf{A}\mathbf{W}_{0,\ell}]_1, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_2) \\
&\mathbf{c}, \mathbf{c}\mathbf{U}_\ell^* + \boxed{\widetilde{u}\mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}), \mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell} \\
&[\mathbf{A}\mathbf{U}_\ell^*]_1, [\mathbf{G}_\ell \mathbf{U}_\ell^*]_1, \mathbf{U}_\ell^* \mathbf{B}_1, \mathbf{U}_\ell^* \mathbf{B}_2, \mathbf{U}_\ell^* \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + \boxed{\mathbf{c}^\perp \widetilde{u}\mathbf{v}^{(3)} \mathbf{B}_3 \widehat{\mathbf{R}}_\ell} + \mathbf{c}^\perp \widehat{\mathbf{k}} \\
\approx_s\ &[\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, [\mathbf{A}\mathbf{W}_{0,\ell}]_1, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_2) \\
&\mathbf{c}, \mathbf{c}\mathbf{U}_\ell^* + \widetilde{u}\mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}) + \boxed{\widetilde{\mathbf{w}}(\mathbf{y}_\ell^*)^\top \mathbf{v}^{(3)}}, \mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell} + \boxed{\widetilde{\mathbf{w}} \otimes \mathbf{v}^{(3)}} \\
&[\mathbf{A}\mathbf{U}_\ell^*]_1, [\mathbf{G}_\ell \mathbf{U}_\ell^*]_1, \mathbf{U}_\ell^* \mathbf{B}_1, \mathbf{U}_\ell^* \mathbf{B}_2, \mathbf{U}_\ell^* \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + \mathbf{c}^\perp \widetilde{u}\mathbf{v}^{(3)} \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + \mathbf{c}^\perp \widehat{\mathbf{k}} \\
\approx_s\ &[\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{G}_\ell]_1, \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, [\mathbf{A}\mathbf{W}_{0,\ell}]_1, \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_1), \mathbf{W}_{0,\ell}(\mathbf{I}_n \otimes \mathbf{B}_2) \\
&\mathbf{c}, \mathbf{c}\mathbf{U}_\ell^* + \widetilde{u}\mathbf{v}^{(3)} + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}) + \widetilde{\mathbf{w}}(\mathbf{y}_\ell^*)^\top \mathbf{v}^{(3)}, \cancel{\mathbf{x}_{b'}^* \otimes \mathbf{v}^{(3)}} + \mathbf{c}\mathbf{W}_{0,\ell} + \widetilde{\mathbf{w}} \otimes \mathbf{v}^{(3)} \\
&[\mathbf{A}\mathbf{U}_\ell^*]_1, [\mathbf{G}_\ell \mathbf{U}_\ell^*]_1, \mathbf{U}_\ell^* \mathbf{B}_1, \mathbf{U}_\ell^* \mathbf{B}_2, \mathbf{U}_\ell^* \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + \mathbf{c}^\perp \widetilde{u}\mathbf{v}^{(3)} \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + \mathbf{c}^\perp \widehat{\mathbf{k}}
\end{aligned}$$

where $\widetilde{u} \leftarrow \mathbb{Z}_p$ and $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{1\times n}$. We justify each step as follows: The first "$\approx_c$" uses Lemma 8, which let $\widetilde{u}$ to appear in ct^* and all $\mathsf{sk}_{\ell,y}$. The second "$\approx_s$" uses the change of variables:

$$\mathbf{W}_{0,\ell} \mapsto \mathbf{W}_{0,\ell} + \mathbf{c}^\perp(\widetilde{\mathbf{w}} \otimes \mathbf{v}^{(3)})$$

The third "$\approx_s$" is straight-forward with the observation that $\widetilde{u}\mathbf{v}^{(3)} \mathbf{B}_3 \widehat{\mathbf{R}}_\ell$ in $\mathsf{sk}_{\ell,y'}$ is hidden by $\widehat{\mathbf{k}}$, this implies that $\widetilde{u}$ is sufficient to hide $\widetilde{\mathbf{w}}(\mathbf{y}_\ell^*)^\top$, and $\widetilde{\mathbf{w}}$ hides $\mathbf{x}_{b'}^*$ in $\mathbf{c}_3^*$.

– $\mathsf{H}_{4,q}$, $(q \in [0, Q])$: Identical to H_3, except that for the first q answers to $\mathsf{OKey}(\ell, \cdot)$, we replace $[\mathbf{K}_2]_2$ in dashboxed with

$$[\mathbf{K}_2]_2 = \left[(\mathbf{U}_\ell^* \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + \cancel{\mathbf{c}^\perp \widehat{\mathbf{k}}})(\mathbf{a}_y \otimes \mathbf{I}_k) + \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3 \widehat{\mathbf{R}}_\ell \mathbf{R})(\mathbf{K}_y \otimes \mathbf{I}_k)\right]_2$$

We have that

- $\mathsf{H}_{4,0} = \mathsf{H}_3$; the two games are exactly identical, since $[0] = \emptyset$;
- $\mathsf{H}_{4,q} \approx_c \mathsf{H}_{4,q-1}$; the proof is identical to that for $\mathsf{H}_{2,q} \approx_c \mathsf{H}_{2,q-1}$.

– H_5 : Identical to $\mathsf{H}_{4,Q}$ except that we replace all $\mathbf{G}_\ell$ with $\widehat{\mathbf{G}}_\ell = \widetilde{\mathbf{G}}_\ell \left(\begin{smallmatrix} \mathbf{c} \\ \mathbf{I}_{k+1} \end{smallmatrix}\right)$ where $\widetilde{\mathbf{G}}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+2)}$; and rewrite the dashboxed terms in $\mathbf{c}_2^*$ and $\mathbf{c}_4^*$ as follow:

$$\boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}_{0,\ell}^*} + \mathbf{c}\mathbf{W}_{0,\ell}((\mathbf{y}_\ell^*)^\top \otimes \mathbf{I}_{5k+2}) \quad \text{and} \quad \boxed{\mathbf{e}_1\widetilde{\mathbf{G}}_\ell^{-1}\mathbf{Q}_{1,\ell}^*}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2})$$

We have $\mathsf{H}_5 \equiv \mathsf{H}_{4,Q}$. The reason is identical to that in $\mathsf{H}_1 \equiv \mathsf{H}_0$

Observe that $\mathsf{H}_5 = \mathsf{G}_{7,\ell-1,2}$ and this proves $\mathsf{G}_{7,\ell-1,1} \approx_c \mathsf{G}_{7,\ell-1,2}$ in this case.

From $\mathsf{H}_{2,q-1}$ to $\mathsf{H}_{2,q}$. We are ready to prove $\mathsf{H}_{2,q-1} \approx_c \mathsf{H}_{2,q}$, and this will complete the proof of $\mathsf{G}_{7,\ell-1,2} \approx_c \mathsf{G}_{7,\ell-1,1}$ in the case that $\mathbf{x}_0^*(\mathbf{y}_\ell^*)^\top \neq \mathbf{x}_1^*(\mathbf{y}_\ell^*)^\top$. Combining with Section 8.3 which provides proof in the case that $\mathbf{x}_0^*(\mathbf{y}_\ell^*)^\top = \mathbf{x}_1^*(\mathbf{y}_\ell^*)^\top$, the proof of $\mathsf{G}_{7,\ell-1} \approx_c \mathsf{G}_{7,\ell}$ is finished, and this readily complete the proof of Lemma 7. For this, we need the following sub-sequence of hybrid argument for each $q \in [Q]$:

– $\mathsf{H}_{2,q-1,0}$: Identical to $\mathsf{H}_{2,q-1}$. We recall the crs, $\mathsf{mpk}_i \in D_i$, $\mathbf{c}_3^*$ and $\mathsf{sk}_{\ell,y'}$ for all $y' \in \mathcal{K}_\ell$ in the following form

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}, \widetilde{\mathbf{V}}]_1, \{\mathsf{crs}_i, [\widehat{\mathbf{G}}_i, \mathbf{A}\mathbf{W}_{0,i}]_1\}_{i\in[L]\setminus\{\ell\}}, \mathsf{crs}_\ell, [\mathbf{G}_\ell, \mathbf{A}\mathbf{W}_{0,\ell}]_1 \\ \{[\mathbf{B}_2\widetilde{\mathbf{R}}_j]_2\}_{j\in[\ell-1]}, \boxed{[\mathbf{B}_3\widehat{\mathbf{R}}_\ell]_2}, \{[\mathbf{B}_1\mathbf{R}_j]_2\}_{j\in[\ell+1,L]} \\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j)]_2\}_{j\in[\ell-1],i\in[L]\setminus\{j\}}, \\ \{\boxed{\mathsf{crs}_{i,\ell}, [\mathbf{G}_{i,\ell}]_2}, \boxed{[\mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell)]_2}\}_{i\in[L]\setminus\{\ell\}}, \\ \{\mathsf{crs}_{i,j}, [\mathbf{G}_{i,j}, \mathbf{W}_{0,i}(\mathbf{I}_n \otimes \mathbf{B}_1\mathbf{R}_j)]_2\}_{j\in[\ell+1,L],i\in[L]\setminus\{j\}} \end{pmatrix}$$

$$\mathsf{mpk}_i = \begin{cases} \begin{pmatrix} [\mathbf{A}\mathbf{U}_i, \mathbf{A}\mathbf{W}_{1,i}, \widehat{\mathbf{G}}_i\mathbf{U}_i, \widehat{\mathbf{G}}_i\mathbf{W}_{1,i}]_1, \widetilde{\pi}_i \\ \{[\mathbf{U}_i\mathbf{B}_2\widetilde{\mathbf{R}}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[\ell-1]\setminus\{i\}}, \\ \boxed{[\mathbf{U}_i\mathbf{B}_3\widehat{\mathbf{R}}_\ell, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), [\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})]_2, \pi_{i,\ell}}; \\ \{[\mathbf{U}_i\mathbf{B}_1\mathbf{R}_j, \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j), \mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,j})]_2, \pi_{i,j}\}_{j\in[\ell+1,L]\setminus\{i\}} \end{pmatrix} & \text{if } i \neq \ell \\ \begin{pmatrix} [\mathbf{A}\mathbf{U}_\ell, \mathbf{A}\mathbf{W}_{1,\ell}]_1, \mathbf{G}_\ell\mathbf{U}_\ell, \mathbf{G}_\ell\mathbf{W}_{1,\ell}]_1, \widetilde{\pi}_\ell \\ \{[\mathbf{U}_\ell\mathbf{B}_2\widetilde{\mathbf{R}}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_2\widetilde{\mathbf{R}}_j), \boxed{\mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})}]_2, \pi_{\ell,j}\}_{j\in[\ell-1]}, \\ \{[\mathbf{U}_\ell\mathbf{B}_1\mathbf{R}_j, \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_1\mathbf{R}_j), \boxed{\mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})}]_2, \pi_{\ell,j}\}_{j\in[\ell+1,L]} \end{pmatrix} & \text{if } i = \ell \end{cases}$$

$$\mathbf{c}_4^* = \boxed{\mathbf{c}\mathbf{W}_{1,\ell}^*(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2})} + \sum_{i\in[L]\setminus\{\ell\}} \mathbf{e}_1\widetilde{\mathbf{G}}_i^{-1}\mathbf{Q}_{1,i}^*(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2}).$$

and for the q–th secret key answered to $\mathsf{OKey}(\ell, \cdot)$, we rewrite it in the form of

$$\mathsf{sk}_{\ell,y^*}^* = \begin{pmatrix} \overbrace{\boxed{[\mathbf{B}_3\widehat{\mathbf{R}}_\ell\mathbf{R}^*]_2}}^{\mathbf{K}_0}, \overbrace{\boxed{\left[\sum_{i\in[L]\setminus\{\ell\}} \mathbf{H}_{1,i,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{R}^*)\right]_2}}^{\mathbf{K}_1}, \\ \underbrace{\boxed{[\mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell(\mathbf{a}_{y^*} \otimes \mathbf{I}_k) + \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell\mathbf{R}^*)(\mathbf{K}_{y^*} \otimes \mathbf{I}_k)]_2}}_{\mathbf{K}_2} \end{pmatrix} \quad \text{where} \quad \mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}$$

here and in the following sub-sequence, we use sk_{ℓ,y^*}^* to indicate the q–th answer to $\mathsf{OKey}(\ell, \cdot)$, and use $\mathbf{R}^*$ and y^* to indicate the specific random coin and query of it, they are different from the $\mathbf{R}$ and y for other $\mathsf{sk}_{\ell,y}$, which can have more than one assignments. And notice it holds that $P(x^*, y^*) = 0$ in this case. We have $\mathsf{H}_{2,q-1,0} = \mathsf{H}_{2,q-1}$, all the changes are conceptual.

– $\mathsf{H}_{2,q-1,1}$: Identical to $\mathsf{H}_{2,q-1,0}$ except that for all $i \in [L] \setminus \{\ell\}$ and all $\mathsf{mpk}_i \in D_i$, we replace $\pi_{i,\ell}$ with

$$\widetilde{\pi}_{i,\ell} \leftarrow \boxed{\mathsf{LSim}_2}(\mathsf{crs}_{i,\ell}, \mathsf{td}_{i,\ell}, [\mathbf{F}_{i,\ell}]_2) \quad \text{where} \quad \mathbf{F}_{i,\ell} = (\underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell)}_{\mathbf{H}_{1,i,\ell}} \| \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})}_{\mathbf{P}_{i,\ell}})$$

We have $\mathsf{H}_{2,q-1,1} \equiv \mathsf{H}_{2,q-1,0}$. This follows from the perfect zero-knowledge of Π_2.

– $\mathsf{H}_{2,q-1,2}$: Identical to $\mathsf{H}_{2,q-1,1}$ except that we sample $\mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}$ along with $\mathbf{D}_\ell$ and for all $i \in [L] \setminus \{\ell\}$, we replace all $\mathbf{G}_{i,\ell}$ with

$$\widehat{\mathbf{G}}_{i,\ell} = (\mathbf{B}_3\widehat{\mathbf{R}}_\ell\mathbf{R}^* \| \mathbf{I}_{5k+2})\widetilde{\mathbf{G}}_{i,\ell}, \quad \widetilde{\mathbf{G}}_{i,\ell} \leftarrow \mathbb{Z}_p^{(6k+2)\times(6k+2)}$$

In particular, for all $i \in [L] \setminus \{\ell\}$, for the dashboxed term in each $\mathsf{mpk}_i \in D_i$, we have

$$\mathbf{P}_{i,\ell} = \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\widehat{\mathbf{G}}_{i,\ell}})$$

We have $\mathsf{H}_{2,q-1,2} \equiv \mathsf{H}_{2,q-1,1}$. This follows from the fact that both $\mathbf{G}_{i,\ell}$ and $\widehat{\mathbf{G}}_{i,\ell}$ are truly random since $(\mathbf{B}_3\widehat{\mathbf{R}}_\ell\mathbf{R}^* \| \mathbf{I}_{5k+2})$ is (row) full-rank.

– $\mathsf{H}_{2,q-1,3}$: Identical to $\mathsf{H}_{2,q-1,2}$ except that we replace $\mathbf{K}_1$ in $\mathsf{sk}^*_{\ell,y'^*}$ with

$$\mathbf{K}_1 = \sum_{i\in[L]\setminus\{\ell\}} \boxed{\mathbf{P}^*_{i,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{G}}^{-1}_{i,\ell}\mathbf{E}_1)} \quad \text{where} \quad \mathbf{E}_1 = \begin{pmatrix}\mathbf{I}_k\\ \mathbf{0}\end{pmatrix} \in \mathbb{Z}_p^{(6k+2)\times k}$$

We have $\mathsf{H}_{2,q-1,3} \approx_c \mathsf{H}_{2,q-1,2}$. This follows from stronger unbounded simulation soundness of Π_2 along with the fact that $\mathsf{LVer}_2(\mathsf{crs}_{i,\ell}, [\mathbf{F}^*_{i,\ell}]_1, \pi^*_{i,\ell}) = 1$ for all $i \in [L]\setminus\{\ell\}$ where $\mathbf{F}^*_{i,\ell} = (\mathbf{H}^*_{1,i,\ell} \| \mathbf{P}^*_{i,\ell})$. Assume $\mathsf{mpk}^*_{i^*} \notin D_{i^*}$, i.e., $\mathsf{mpk}^*_{i^*}$ is malicious. In the reduction, we guess $i^* \leftarrow [L]\setminus\{\ell\}$ and obtain $\mathbf{D}_\ell, \widehat{\mathbf{G}}_{i^*,\ell}, \mathsf{crs}_{i^*,\ell}$ as input; we simulate honestly as in $\mathsf{H}_{2,q-1,3}$ except that for all $\mathsf{mpk}_{i^*} \in D_{i^*}$, we make an oracle query $[\mathbf{F}_{i^*,\ell}]_2$ and get $\widetilde{\pi}_{i^*,\ell}$ in it; we finally output $([\mathbf{F}^*_{i^*,\ell}]_2, \pi^*_{i^*,\ell})$ in $\mathsf{mpk}^*_{i^*} \notin D_{i^*}$. Observe that once it happens that $\mathbf{P}^*_{i^*,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{G}}^{-1}_{i^*,\ell}\mathbf{E}_1) \neq \mathbf{H}^*_{1,i^*,\ell}(\mathbf{I}_{n'} \otimes \mathbf{R}^*)$, we must have $\mathbf{F}^*_{i^*,\ell} \notin \mathsf{span}(\mathbf{B}_{i^*,\ell})$. When $\mathsf{mpk}^*_{i^*} \in D_{i^*}$, we always have $\mathsf{H}_{2,q-1,3} \equiv \mathsf{H}_{2,q-1,2}$.

– $\mathsf{H}_{2,q-1,4}$: Identical to $\mathsf{H}_{2,q-1,3}$ except that we replace all $\widehat{\mathbf{R}}_\ell\mathbf{R}^*$ with $\boxed{\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}}$, in particular, for all $i \in [L] \setminus \{\ell\}$ we generate $\widehat{\mathbf{G}}_{i,\ell}$ as follows:

$$\widehat{\mathbf{G}}_{i,\ell} = \big(\mathbf{B}_3\boxed{\widetilde{\mathbf{R}}} \| \mathbf{I}_{5k+2}\big)\widetilde{\mathbf{G}}_{i,\ell}, \quad \widetilde{\mathbf{G}}_{i,\ell} \leftarrow \mathbb{Z}_p^{(6k+2)\times(6k+2)}$$

and generate the $[\mathbf{K}_0]_2, [\mathbf{K}_2]_2$ in sk^*_{ℓ,y^*} as:

$$[\mathbf{B}_3\boxed{\widetilde{\mathbf{R}}}]_2 \quad \text{and} \quad [\mathbf{U}^*_\ell\mathbf{B}_3\widehat{\mathbf{R}}_\ell(\mathbf{a}_{y^*} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\boxed{\widetilde{\mathbf{R}}})(\mathbf{K}_{y^*} \otimes \mathbf{I}_k)]_2$$

We have $\mathsf{H}_{2,q-1,4} \approx_c \mathsf{H}_{2,q-1,3}$. This follows from MDDH assumption w.r.t. $[\widehat{\mathbf{R}}_\ell]_2$ which ensures that $([\widehat{\mathbf{R}}_\ell]_2, [\widehat{\mathbf{R}}_\ell\mathbf{R}^*]_2) \approx_c ([\widehat{\mathbf{R}}_\ell]_2, [\widetilde{\mathbf{R}}]_2)$ when $\widehat{\mathbf{R}}_\ell \leftarrow \mathbb{Z}_p^{(2k+1)\times k}, \mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}, \widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$.

– $\mathsf{H}_{2,q-1,5}$: Identical to $\mathsf{H}_{2,q-1,4}$ except that we replace the $\mathbf{K}_2$ in sk^*_{ℓ,y^*} with

$$\mathbf{K}_2 = (\mathbf{U}^*_\ell\mathbf{B}_3\widehat{\mathbf{R}}_\ell + \boxed{\mathbf{c}^\perp\widehat{\mathbf{k}}})(\mathbf{a}'_{y'^*} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}})(\mathbf{K}'_{y'^*} \otimes \mathbf{I}_k)$$

We have $\mathsf{H}_{2,q-1,5} \approx_c \mathsf{H}_{2,q-1,4}$. Define $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ and $\mathbf{R}^\perp \in \mathbb{Z}_p^{k\times(2k+1)}$ such that $\mathbf{A}\mathbf{c}^\perp = \mathbf{0}$, $\mathbf{c}\mathbf{c}^\perp = 1$ and $\mathbf{R}^\perp\widehat{\mathbf{R}}_\ell = \mathbf{0}$ and $\mathbf{R}^\perp\widetilde{\mathbf{R}} = \mathbf{I}_k$, notice that these use the fact that $\left(\begin{smallmatrix}\mathbf{A}\\ \mathbf{c}\end{smallmatrix}\right)$ is (row) full-rank w.h.p and $(\widehat{\mathbf{R}}_\ell \| \widetilde{\mathbf{R}})$ is (column) full-rank w.h.p.

The $\mathsf{H}_{2,q-1,5} \approx_c \mathsf{H}_{2,q-1,4}$ follows from the following argument for $b' \in \{0,1\}$:

$$
\begin{aligned}
& [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{B}_1]_1, \mathbf{B}_2, \mathbf{B}_3, \widehat{\mathbf{R}}_\ell, [\mathbf{G}_\ell]_1, \{[\mathbf{G}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}} && \text{// crs, mpk}_\ell \\
& \mathbf{c}, \mathbf{c}\mathbf{W}^*_{1,\ell}(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2}) && \text{// ct}^* \\
& \widetilde{\mathbf{R}}, (\mathbf{U}^*_\ell \mathbf{B}_3 \widehat{\mathbf{R}}_\ell + b'\mathbf{c}^\perp \widehat{\mathbf{k}})(\mathbf{a}_{y^*} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3 \widetilde{\mathbf{R}})(\mathbf{K}_{y^*} \otimes \mathbf{I}_k) && \text{// sk}^*_{\ell,y^*} \\
& \begin{pmatrix} [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, [\mathbf{G}_\ell \mathbf{W}^*_{1,\ell}]_1, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \\ [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2 \{[\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{j\in[L]\setminus\{\ell\}} \end{pmatrix}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3 \widetilde{\mathbf{R}}) && \text{// mpk}^*_\ell, \text{ other sk}_{\ell,y'} \\
\approx_c\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{B}_1]_1, \mathbf{B}_2, \mathbf{B}_3, \widehat{\mathbf{R}}_\ell, [\mathbf{G}_\ell]_1, \{[\mathbf{G}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}} \\
& \mathbf{c}, (\mathbf{c}\mathbf{W}^*_{1,\ell} + \boxed{\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp (\mathbf{B}_3^{\parallel})^\top)})(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2}) \\
& \widetilde{\mathbf{R}}, (\mathbf{U}^*_\ell \mathbf{D}_\ell + b'\mathbf{c}^\perp \widehat{\mathbf{k}})(\mathbf{a}_{y^*} \otimes \mathbf{I}_k) + (\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \boxed{\mathbf{c}^\perp \widetilde{\mathbf{w}}})(\mathbf{K}_{y^*} \otimes \mathbf{I}_k) \\
& \begin{pmatrix} [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, [\mathbf{G}_\ell \mathbf{W}^*_{1,\ell}]_1, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \\ [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2 \{[\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{j\in[L]\setminus\{\ell\}} \end{pmatrix}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3 \widetilde{\mathbf{R}}) \\
\approx_s\ & [\mathbf{A}]_1, \mathbf{c}^\perp, [\mathbf{B}_1]_1, \mathbf{B}_2, \mathbf{B}_3, \widehat{\mathbf{R}}_\ell, [\mathbf{G}_\ell]_1, \{[\mathbf{G}_{\ell,j}]_2\}_{j\in[L]\setminus\{\ell\}} \\
& \mathbf{c}, (\mathbf{c}\mathbf{W}^*_{1,\ell} + \widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp (\mathbf{B}_3^{\parallel})^\top))(\mathbf{C}_{x^*} \otimes \mathbf{I}_{5k+2}) \\
& \widetilde{\mathbf{R}}, (\mathbf{U}^*_\ell \mathbf{D}_\ell + \cancel{b'\mathbf{c}^\perp \widehat{\mathbf{k}}})(\mathbf{a}_{y^*} \otimes \mathbf{I}_k) + (\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \mathbf{c}^\perp \widetilde{\mathbf{w}})(\mathbf{K}_{y^*} \otimes \mathbf{I}_k) \\
& \begin{pmatrix} [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, [\mathbf{G}_\ell \mathbf{W}^*_{1,\ell}]_1, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_2), \\ [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2 \{[\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\}_{j\in[L]\setminus\{\ell\}} \end{pmatrix}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3 \widetilde{\mathbf{R}})
\end{aligned}
$$

where $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{kn'}$. We justify each step as follows: The first "$\approx_c$" uses Lemma 9, which let $\widetilde{\mathbf{w}}$ appears in ct^* and sk^*_{ℓ,y^*}. The second "$\approx_s$" uses the fact that $P(x^*, y^*) = 0$ in this case and security of predicate encoding (c.f. Section 3.2), which ensure that

$$
\begin{aligned}
& \left(\widehat{\mathbf{k}}(\mathbf{a}_{y^*} \otimes \mathbf{I}_k) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*} \otimes \mathbf{I}_k) \| \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_k)\right) \\
\approx_s\ & \left(\mathbf{0}(\mathbf{a}_{y^*} \otimes \mathbf{I}_k) + \widetilde{\mathbf{w}}(\mathbf{K}_{y^*} \otimes \mathbf{I}_k) \| \widetilde{\mathbf{w}}(\mathbf{C}_{x^*} \otimes \mathbf{I}_k)\right)
\end{aligned}
$$

- $\mathsf{H}_{2,q-1,6}$: Identical to $\mathsf{H}_{2,q-1,5}$ except that we replace all $\widetilde{\mathbf{R}}$ with $\boxed{\widehat{\mathbf{R}}_\ell \mathbf{R}^*}$ where $\mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}$, in particular, for all $i \in [L] \setminus \{\ell\}$ we generate $\widehat{\mathbf{G}}_{i,\ell}$ as follows:

$$
\widehat{\mathbf{G}}_{i,\ell} = \left(\mathbf{B}_3 \boxed{\widehat{\mathbf{R}}_\ell \mathbf{R}^*} \| \mathbf{I}_{5k+2}\right) \widetilde{\mathbf{G}}_{i,\ell}, \quad \widetilde{\mathbf{G}}_{i,\ell} \leftarrow \mathbb{Z}_p^{(6k+2)\times(6k+2)}
$$

and generate the $[\mathbf{K}_0]_2, [\mathbf{K}_2]_2$ in sk^*_{ℓ,y^*} as:

$$
[\mathbf{B}_3 \boxed{\widehat{\mathbf{R}}_\ell \mathbf{R}^*}]_2 \quad \text{and} \quad [\mathbf{U}^*_\ell \mathbf{B}_3 \widehat{\mathbf{R}}_\ell (\mathbf{a}_{y^*} \otimes \mathbf{I}_k) + \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3 \boxed{\widehat{\mathbf{R}}_\ell \mathbf{R}^*})(\mathbf{K}_{y^*} \otimes \mathbf{I}_k)]_2
$$

We have $\mathsf{H}_{2,q-1,6} \approx_c \mathsf{H}_{2,q-1,5}$. The reason is identical to that for $\mathsf{H}_{2,q-1,3} \approx_c \mathsf{H}_{2,q-1,4}$. This follows from MDDH assumption w.r.t. $[\widehat{\mathbf{R}}_\ell]_2$ which ensures that $([\widehat{\mathbf{R}}_\ell]_2, [\widetilde{\mathbf{R}}]_2) \approx_c ([\widehat{\mathbf{R}}_\ell]_2, [\widehat{\mathbf{R}}_\ell \mathbf{R}^*]_2)$ when $\widehat{\mathbf{R}}_\ell \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{R}^* \leftarrow \mathbb{Z}_p^{k\times k}$, $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$.

- $\mathsf{H}_{2,q-1,7}$: Identical to $\mathsf{H}_{2,q-1,6}$, except that we replace $\mathbf{K}_1$ in sk^*_{ℓ,y^*} with

$$
\mathbf{K}_1 = \sum_{i\in[L]\setminus\{\ell\}} \boxed{\mathbf{H}^*_{1,i,\ell}(\mathbf{I}_{n'} \otimes \mathbf{R}^*)}
$$

We have $\mathsf{H}_{2,q-1,7} \approx_c \mathsf{H}_{2,q-1,6}$. The reason is identical to that for $\mathsf{H}_{2,q-1,2} \approx_c \mathsf{H}_{2,q-1,3}$. This follows from stronger unbounded simulation soundness of Π_2 along with the fact that $\mathsf{LVer}_2(\mathsf{crs}_{i,\ell}, [\mathbf{F}^*_{i,\ell}]_1, \pi^*_{i,\ell}) = 1$ for all $i \in [L] \setminus \{\ell\}$ where $\mathbf{F}^*_{i,\ell} = (\mathbf{H}^*_{1,i,\ell} \| \mathbf{P}^*_{i,\ell})$.

– $\mathsf{H}_{2,q-1,8}$: Identical to $\mathsf{H}_{2,q-1,7}$ except that for all $i \in [L] \setminus \{\ell\}$, we replace $\widehat{\mathbf{G}}_{i,\ell}$ with $\mathbf{G}_{i,\ell} \leftarrow \mathbb{Z}_p^{(5k+2)\times(6k+2))}$. In particular, for all $i \in [L] \setminus \{\ell\}$, for the dashboxed term in each $\mathsf{mpk}_i \in D_i$, we have

$$\mathbf{P}_{i,\ell} = \mathbf{W}_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{G}_{i,\ell}})$$

We have $\mathsf{H}_{2,q-1,8} \equiv \mathsf{H}_{2,q-1,7}$. The reason is identical to that for $\mathsf{H}_{2,q-1,2} \equiv \mathsf{H}_{2,q-1,1}$. This follows from the fact that both $\mathbf{G}_{i,\ell}$ and $\widehat{\mathbf{G}}_{i,\ell}$ are truly random since $(\mathbf{B}_3\widehat{\mathbf{R}}_\ell\mathbf{R}^* \| \mathbf{I}_{5k+2})$ is (row) full-rank.

– $\mathsf{H}_{2,q-1,9}$: Identical to $\mathsf{H}_{2,q-1,8}$ except that for all $i \in [L] \setminus \{\ell\}$ and all $\mathsf{mpk}_i \in D_i$, we replace $\widetilde{\pi}_{i,\ell}$ with

$$\pi_{i,\ell} \leftarrow \boxed{\mathsf{LPrv}_2}(\mathsf{crs}_{i,\ell}, [\mathbf{F}_{i,\ell}]_2, \mathbf{W}_{1,i}) \quad \text{where} \quad \mathbf{F}_{i,\ell} = (\underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell)}_{\mathbf{H}_{1,i,\ell}} \| \underbrace{\mathbf{W}_{1,i}(\mathbf{I}_{n'} \otimes \mathbf{G}_{i,\ell})}_{\mathbf{P}_{i,\ell}})$$

We have $\mathsf{H}_{2,q-1,9} \equiv \mathsf{H}_{2,q-1,8}$. The reason is identical to that for $\mathsf{H}_{2,q-1,1} \equiv \mathsf{H}_{2,q-1,0}$. This follows from the perfect zero-knowledge of Π_2.

Observe that we have $\mathsf{H}_{2,q-1,9} = \mathsf{H}_{2,q}$ and this proves $\mathsf{H}_{2,q-1} \approx_c \mathsf{H}_{2,q}$.

9 Slotted Delegated Reg-FE for Arbitrary Functionalities

In this section, we build the slotted delegated Reg-FE for arbitrary functionalities. It's a generic construction from the combination of slotted registered functional encryption (slotted Reg-FE) and functional encryption (FE), and requires a secret-key encryption (SKE) and a puncturable pseudorandom function (punc-PRF) as ingredients.

9.1 Construction

Let $G : X \to Y, F : Y \to Z$ be arbitrary function spaces. The slotted delegated Reg-FE for F, G is built with following ingredients:

– a slotted Reg-FE for general class of all function as defined in Section 3.4: $\Pi_1 = \{\mathsf{R.Setup}, \mathsf{R.Gen}, \mathsf{R.Ver}, \mathsf{R.Agg}, \mathsf{R.Enc}, \mathsf{R.Dec}\}$;
– a FE for functionality F as defined in Section 3.5: $\Pi_2 = \{\mathsf{F.Setup}, \mathsf{F.Gen}, \mathsf{F.Enc}, \mathsf{F.Dec}\}$;
– a secret-key encryption with pseudoranndom ciphertext as defined in Section 3.6: $\Pi_3 = \{\mathsf{S.Gen}, \mathsf{S.Enc}, \mathsf{S.Dec}\}$, with message space that is exactly the cipher space of Π_2, and over this message space, the Π_3 has $\ell = \ell(\lambda)$-bit long ciphertexts;
– a puncturable pseudorandom function family as defined in Section 3.7: $\Pi_4 = \{\mathsf{Prf.Gen}, \mathsf{Prf.Eval}, \mathsf{Prf.Punc}\}$, with the domain $\mathcal{X}_\lambda = \{0,1\}^\lambda$ and range that is the random coin space of the encryption of Π_2.

Our generic slotted delegated Reg-FE works as follows:

– $\mathsf{Setup}(1^\lambda, 1^L, F, G)$: Run and output

$$\underbrace{\mathsf{R.crs}}_{\mathsf{crs}} \leftarrow \mathsf{R.Setup}(1^\lambda, 1^L)$$

– $\mathsf{Gen}(\mathsf{crs}, i, g_i)$: Parse $\mathsf{crs} = \mathsf{R.crs}$. Proceed as follows:
  • run $(\mathsf{F.mpk}_i, \mathsf{F.msk}_i) \leftarrow \mathsf{F.Setup}(1^\lambda)$;
  • sample a tag $t_i \leftarrow \{0,1\}^\lambda$, $c_i \leftarrow \{0,1\}^\ell$;
  • run $(\mathsf{R.pk}_{i,\mathsf{ReEnc}_i}, \mathsf{R.sk}_{i,\mathsf{ReEnc}_i}) \leftarrow \mathsf{R.Gen}(\mathsf{R.crs}, i, \mathsf{ReEnc}_i)$, where ReEnc_i is defined as follows.

$\mathsf{ReEnc}_i(x, K, k)$
Compute $\mathsf{F.ct}_i \leftarrow \mathsf{S.Dec}(k, c_i)$, $s_i = \mathsf{Prf.Eval}(K, t_i)$
If $\mathsf{F.ct}_i \neq \perp$, output $\mathsf{F.ct}_i$;
else, output $\mathsf{F.ct}_i = \mathsf{F.Enc}(\mathsf{F.mpk}_i, g_i(x); s_i)$.

Output:

$$\mathsf{mpk}_{i,g_i} = (\mathsf{R.pk}_{i,\mathsf{ReEnc}_i}, \mathsf{ReEnc}_i) \quad \text{and} \quad \mathsf{msk}_{i,g_i} = (\mathsf{R.sk}_{i,\mathsf{ReEnc}_i}, \mathsf{F.msk}_i).$$

- $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_{i,g_i})$: Parse $\mathsf{crs} = \mathsf{R.crs}$ and $\mathsf{mpk}_{i,g_i} = (\mathsf{R.pk}_{i,\mathsf{ReEnc}_i}, \mathsf{ReEnc}_i)$. Run and output

$$b \leftarrow \mathsf{R.Ver}(\mathsf{R.crs}, i, \mathsf{R.pk}_{i,\mathsf{ReEnc}_i}, \mathsf{ReEnc}_i).$$

- $\mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_{i,g_i})_{i\in[L]})$: Parse $\mathsf{crs} = \mathsf{R.crs}$. For all $i \in [L]$, parse $\mathsf{mpk}_{i,g_i} = (\mathsf{R.pk}_{i,\mathsf{ReEnc}_i}, \mathsf{ReEnc}_i)$. Run and output

$$(\underbrace{\mathsf{R.mpk}}_{\mathsf{mpk}_+}, \underbrace{(\mathsf{R.hsk}_j)_{j\in[L]}}_{\mathsf{hsk}_j}) \leftarrow \mathsf{R.Agg}(\mathsf{R.crs}, (\mathsf{R.pk}_{i,\mathsf{ReEnc}_i})_{i\in[L]}).$$

- $\mathsf{Enc}(\mathsf{mpk}_+, x)$: Parse $\mathsf{mpk}_+ = \mathsf{R.mpk}$. Sample $K \leftarrow \mathsf{Prf.Gen}(1^\lambda)$ and output

$$\underbrace{\mathsf{R.ct}}_{\mathsf{ct}} \leftarrow \mathsf{R.Enc}(\mathsf{R.mpk}, (x, K, \bot)).$$

- $\mathsf{Key}(\mathsf{msk}_{j^*,g_{j^*}}, f)$: Parse $\mathsf{msk}_{j^*,g_{j^*}} = (\mathsf{R.sk}_{j^*,\mathsf{ReEnc}_{j^*}}, \mathsf{F.msk}_{j^*})$, run $\mathsf{F.sk}_f \leftarrow \mathsf{F.Gen}(\mathsf{F.msk}_{j^*}, f)$. Output

$$\mathsf{sk}_{j^*,f} = (\mathsf{R.sk}_{j^*,\mathsf{ReEnc}_{j^*}}, \mathsf{F.sk}_f)$$

- $\mathsf{Dec}(\mathsf{sk}_{j^*,f}, \mathsf{hsk}_{j^*}, \mathsf{ct})$: Parse

$$\mathsf{sk}_{j^*,f} = (\mathsf{R.sk}_{j^*,\mathsf{ReEnc}_{j^*}}, \mathsf{F.sk}_f), \quad \mathsf{hsk}_{j^*} = \mathsf{R.hsk}_{j^*} \quad \text{and} \quad \mathsf{ct} = \mathsf{R.ct}$$

And run $\mathsf{F.ct}_{j^*} \leftarrow \mathsf{R.Dec}(\mathsf{R.sk}_{j^*,\mathsf{ReEnc}_{j^*}}, \mathsf{R.hsk}_{j^*}, \mathsf{R.ct})$, output $z \leftarrow \mathsf{F.Dec}(\mathsf{F.sk}_f, \mathsf{F.ct}_{j^*})$.

Completeness. The completeness of our generic construction follows from the completeness of Π_1. In particular, for all $\lambda, L \in \mathbb{N}$, all G and F, all $i \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F, G)$ and $(\mathsf{mpk}_{i,g_i}, \mathsf{msk}_{i,g_i}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i, g_i)$, we have $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_{i,g_i}) = 1$. This is ensured by the specification of Setup, Gen, Ver along with the completeness of Π_1.

Correctness. For all $\lambda, L \in \mathbb{N}$, all G and F, all $j^* \in [L]$, all $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, F, G)$, all $g_1, \ldots, g_L \in G$, all $(\mathsf{mpk}_{j^*,g_{j^*}}, \mathsf{msk}_{j^*,g_{j^*}}) \leftarrow \mathsf{Gen}(\mathsf{crs}, j^*, g_{j^*})$, all $\{\mathsf{mpk}_{i,g_i}\}_{i\in[L]\setminus\{j^*\}}$ such that $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_{i,g_i}) = 1$, for all $x \in X$ and $f \in F$, we have:

- $\mathsf{F.ct}_{j^*} = \mathsf{ReEnc}_{j^*}(x, K, \bot) \in \mathsf{F.Enc}(\mathsf{F.mpk}_{j^*}, g_{j^*}(x))$, which follows from the definition of ReEnc_{j^*}, the specification of Setup, Gen, Ver, Agg, Enc and the correctness of Π_1.
- $z = f(g_{j^*}(x))$, which follows from the specification of Gen, Key and the correctness of Π_2.

This readily proves the correctness.

Compactness and Efficiency. Our slotted delegated Reg-FE for general class of function achieves the compactness and efficiency requirements as defined in Section 4.2, according to the compactness and effiency of Π_1.

Security. We have the following theorem. Given (1) slotted Reg-FE which achieves semi-adaptive IND-security without malicious slot and supports general class of functions; (2) FE which achieves selective IND-security and supports general class of functions; (3) secret-key encryption which has pseudorandom ciphertext; (4) puncturable pseudorandom function which achieves pseudorandomness, functionality and pseudorandomness at punctured point; our slotted Reg-FE for general class of functions achieves the semi-adaptive security without malicious slot.

Theorem 5. *Assume* $\Pi_1 = (\mathsf{R.Setup}, \mathsf{R.Gen}, \mathsf{R.Ver}, \mathsf{R.Agg}, \mathsf{R.Enc}, \mathsf{R.Dec})$ *is slotted Reg-FE with function-dependent generation, semi-adaptive IND-security without malicious slot (c.f. Section 3.4),* $\Pi_2 = (\mathsf{F.Setup}, \mathsf{F.Gen}, \mathsf{F.Enc}, \mathsf{F.Dec})$ *is FE with selective IND-security (c.f. Section 3.5),* Π_3 *is a SKE with pseudorandom ciphertext (c.f. Section 3.6), and* Π_4 *is a PRF family with pseudorandomness, functionality, pseudorandomness at punctured point (c.f. Section 3.7), our slotted delegated Reg-FE scheme in Section 9.1 achieves the semi-adaptive IND-security without malicious slots defined in Section 4.1.*

9.2 Proof of Security

We prove the Theorem 5 via following game sequence.

Game Sequence. Suppose that crs is the common reference string, (x_0^*, x_1^*) is the challenge pair, $\{\mathsf{mpk}^*_{i,g_i^*}\}_{i\in[L]}$ are challenge master public keys to be registered, which respectively associated with challenge function g_i^*. Assume that the maximum number of queries to $\mathsf{OGen}(\cdot,\cdot)$ is Q. On input (i, g_i), we use mpk_{i,g_i} to denote the output of $\mathsf{OGen}(i, g_i)$. The security without malicious slot means that for each mpk^*_{i,g_i^*}, there exists $q \in [Q]$ such that the q-th query to OGen is (i, g_i^*) and mpk^*_{i,g_i^*} is exactly the output. For all $i \in [L]$, it holds that

$$\begin{aligned} \mathcal{D}_i[\mathsf{mpk}^*_{i,g_i^*}] &\neq \bot \\ g_i(x_0^*) \neq g_i(x_1^*) &\Longrightarrow (i, \mathsf{mpk}_{i,g_i}) \notin C \\ f \in \mathcal{K}_i &\Longrightarrow f \circ g_i^*(x_0^*) = f \circ g_i^*(x_1^*) \end{aligned}$$

where $\mathcal{K}_i$ is the list that records the queries to $\mathsf{OKey}(i, \cdot)$. Note that we let mpk_{i,g_i} and g_i have more than one assignments, while mpk^*_{i,g_i^*} is the *specific* challenge master public key for slot i, associated with *specific* challenge function g_i^*.

- G_0 : This is the real game. We recall the form of related terms in the game as follows.
  - $\mathsf{crs} = \mathsf{R.crs}$, where $\mathsf{R.crs} \leftarrow \mathsf{R.Setup}(1^\lambda, 1^L)$.
  - For all $q \in [Q]$, when answering the q-th query to $\mathsf{OGen}(\cdot,\cdot)$ with input (i, g_i) [8], it generates master key pair in form of

    $$\mathsf{mpk}_{i,g_i} = (\mathsf{R.pk}_{i,\mathsf{ReEnc}_i}, \mathsf{ReEnc}_i) \quad \text{and} \quad \mathsf{msk}_{i,g_i} = (\mathsf{R.sk}_{i,\mathsf{ReEnc}_i}, \mathsf{F.msk}_i)$$

    where $(\mathsf{R.pk}_{i,\mathsf{ReEnc}_i}, \mathsf{R.sk}_{i,\mathsf{ReEnc}_i}) \leftarrow \mathsf{R.Gen}(\mathsf{R.crs}, i, \mathsf{ReEnc}_i)$ with ReEnc_i as follows.

$\mathsf{ReEnc}_i(x, K, k)$
Compute $\mathsf{F.ct}_i \leftarrow \mathsf{S.Dec}(k, c_i)$, $s_i = \mathsf{Prf.Eval}(K, t_i)$
If $\mathsf{F.ct}_i \neq \bot$, output $\mathsf{F.ct}_i$;
else, output $\mathsf{F.ct}_i = \mathsf{F.Enc}(\mathsf{F.mpk}_i, g_i(x); s_i)$.

    with $t_i \leftarrow \{0,1\}^\lambda$, $c_i \leftarrow \{0,1\}^\ell$ and $(\mathsf{F.mpk}_i, \mathsf{F.msk}_i) \leftarrow \mathsf{F.Setup}(1^\lambda)$. Notice that all these related terms with subscript i have more than one assignment, since adversary may query (i, g_i) more than once. And if mpk_{i,g_i} is chosen to be the challenge master public key mpk^*_{i,g_i^*}, we also mark above related terms with the asterisk superscript.

[8] The g_i and following terms that generated during answering $\mathsf{OGen}(i, g_i)$ may have different assignment for different q-th query.

- For each $i \in [L]$ and each $f \in \mathcal{K}_i$, secret key return from $\mathsf{OKey}(i, f)$ is in the form of

$$\mathsf{sk}_{i,f} = (\mathsf{R.sk}^*_{i,\mathsf{ReEnc}^*_i}, \mathsf{F.sk}_f)$$

  where $\mathsf{F.sk}_f \leftarrow \mathsf{F.Gen}(\mathsf{F.msk}^*_i, f)$.
- For secret bit $b \leftarrow \{0,1\}$, we have $\mathsf{ct}^* = \mathsf{R.ct}^*$, where $\mathsf{R.ct}^* \leftarrow \mathsf{R.Enc}(\mathsf{R.mpk}, (x^*_b, K^*, \perp))$ and $K^* \leftarrow \mathsf{Prf.Gen}(1^\lambda)$.

– G_1 : Identical to G_0, except that the challenger samples $t^{(q)} \leftarrow \{0,1\}^\lambda$ and $(\mathsf{F.mpk}^{(q)}, \mathsf{F.msk}^{(q)}) \leftarrow \mathsf{F.Setup}(1^\lambda)$ for all $q \in [Q]$ at the beginning of game. And when answering the q-th query to $\mathsf{OGen}(\cdot,\cdot)$, on input (i, g_i), the challenger uses $(\mathsf{F.mpk}_i, \mathsf{F.msk}_i) = \boxed{(\mathsf{F.mpk}^{(q)}, \mathsf{F.msk}^{(q)})}$, and use tag $t_i = t^{(q)}$. We have $\mathsf{G}_1 = \mathsf{G}_0$. The view of the adversary in these two games is distributed identically.

– G_2 : Identical to G_1 except that after generating $t^{(q)}$ for all $q \in [Q]$, check if $t^{(q)} \stackrel{?}{=} t^{(q')}$ for some $q' < q$. Abort if the check doesn't pass. We have the probability of aborting is at most $(Q+1)^2 \cdot 2^{-\lambda}$, which implies $\mathsf{G}_2 \approx_s \mathsf{G}_1$.

– $\mathsf{G}_{3,\xi}, (\xi \in [0, Q])$: Identical to G_2 except that we sample $\boxed{k^* \leftarrow \mathsf{S.Gen}(1^\lambda)}$ and $\boxed{K^* \leftarrow \mathsf{Prf.Gen}(1^\lambda)}$ at beginning. And for all $q \in [\xi]$, when answering the q-th query to OGen with input (i, g_i), we replace c_i with

$$c_i \leftarrow \boxed{\mathsf{S.Enc}(k^*, \mathsf{F.ct}_i)}$$

  where $\mathsf{F.ct}_i \leftarrow \mathsf{F.Enc}(\mathsf{F.mpk}_i, g_i(x^*_b); s_i)$ and $s_i = \mathsf{Prf.Eval}(K^*, t_i)$. We have:
  - $\mathsf{G}_{3,0} = \mathsf{G}_2$. The view of the adversary in these two games are distributed identically.
  - $\mathsf{G}_{3,\xi} \approx_c \mathsf{G}_{3,\xi-1}$ for all $\xi \in [Q]$, this follows from the fact that Π_3 has pseudorandom ciphertext since k^* is not leak to adversary anywhere.

– G_4 : Identical to $\mathsf{G}_{3,Q}$ except that when generating challenge ciphertext, we replace ct^* with

$$\mathsf{ct}^* \leftarrow \mathsf{R.Enc}(\mathsf{R.mpk}, \boxed{(\perp, K^*, k^*)}).$$

  Notice that for all $i \in [L]$, we have $\mathsf{mpk}^*_{i,g^*_i} = (\mathsf{R.pk}^*_{i,\mathsf{ReEnc}^*_i}, \mathsf{ReEnc}^*_i)$, where

$$(\mathsf{R.pk}^*_{i,\mathsf{ReEnc}^*_i}, \mathsf{R.sk}^*_{i,\mathsf{ReEnc}^*_i}) \leftarrow \mathsf{R.Gen}(\mathsf{R.crs}, i, \mathsf{ReEnc}^*_i)$$

  such that

$$\overbrace{\mathsf{ReEnc}^*_i(\perp, K^*, k^*)}^{\text{in } \mathsf{G}_4} = \mathsf{F.Enc}(\mathsf{F.mpk}^*_i, g^*_i(x^*_b); s^*_i) = \overbrace{\mathsf{ReEnc}^*_i(x^*_b, K^*, \perp)}^{\text{in } \mathsf{G}_{3,Q}}$$

  With the security of Π_1, we have $\mathsf{G}_4 \approx_c \mathsf{G}_{3,Q}$. Notice that all $\mathsf{R.sk}^*_{i,\mathsf{ReEnc}^*_i}$ can be leaked during $\mathsf{sk}_{i,f} \leftarrow \mathsf{OKey}(i, f)$, but the reduction can still go through, which is ensured by above equation for all $i \in [L]$.

– $\mathsf{G}_{5,\xi}, (\xi \in [0, Q])$: Identical to G_4, except that for $q \in [\xi]$, when answering the q-th query to OGen, on input (i, g_i), c_i is programmed as $c_i \leftarrow \mathsf{S.Enc}(k^*, \boxed{\mathsf{F.ct}_i})$, where $\boxed{\mathsf{F.ct}_i} \leftarrow \mathsf{F.Enc}(\mathsf{F.mpk}_i, g_i(x^*_b); \boxed{s_i})$, and $\boxed{s_i} \leftarrow \boxed{\mathsf{Coin}}$. We have:
  - $\mathsf{G}_{5,0} = \mathsf{G}_4$, this follows from the fact that $[0] = \emptyset$.
  - $\mathsf{G}_{5,\xi} \approx_c \mathsf{G}_{5,\xi-1}$ for all $\xi \in [Q]$. We defer the detailed proof via a sub-game sequence later.

– $\mathsf{G}_{6,\xi}, (\xi \in [0, Q])$: Identical to $\mathsf{G}_{5,Q}$, except that for $q \in [\xi]$, when answering the q-th query to OGen with input (i, g_i), c_i is programmed as $c_i \leftarrow \mathsf{S.Enc}(k^*, \boxed{\mathsf{F.ct}_i})$, where $\boxed{\mathsf{F.ct}_i} \leftarrow \mathsf{F.Enc}(\mathsf{F.mpk}_i, g_i(\boxed{x^*_0}); \mathsf{Coin})$. We have:
  - $\mathsf{G}_{6,0} = \mathsf{G}_{5,Q}$, this follows from the fact that $[0] = \emptyset$.
  - $\mathsf{G}_{6,\xi} \approx_c \mathsf{G}_{6,\xi-1}$ for all $\xi \in [L]$. This follows from the arguments in following two cases:
    $\underline{g_i(x^*_0) = g_i(x^*_1)}$**:** The equality is trivial in this case.
    $\underline{g_i(x^*_0) \neq g_i(x^*_1)}$**:** This case implies that $(i, \mathsf{mpk}_{i,g_i}) \notin C$. Namely, the corresponding $\mathsf{msk}_{i,g_i} = (\mathsf{R.sk}_{i,\mathsf{ReEnc}^*_i}, \mathsf{F.msk}_i)$ is not corrupted by the adversary. And the equality follows from the security of Π_2. This is ensured by the fact that $\mathsf{F.msk}_i$ is hidden to adversary. And even if mpk_{i,g_i} is chosen as the challenge mpk^*_{i,g^*_i},the adversary can learn no more than $\mathsf{F.sk}_f \leftarrow \mathsf{F.Gen}(\mathsf{F.msk}_i, f)$ for $f \in \mathcal{K}_i$, via quering to $\mathsf{OKey}(i, f)$.

Observe that, in $\mathsf{G}_{6,Q}$, all the terms obtained by the adversary is independent to secret bit b. The advantage of adversary is exactly 0.

From $\mathsf{G}_{5,\xi-1}$ to $\mathsf{G}_{5,\xi}$. We will prove $\mathsf{G}_{5,\xi} \approx_c \mathsf{G}_{5,\xi-1}$ via following sub-sequence for all $\xi \in [Q]$. Notice that in the following sub-sequence, we assume (i, g_i) is the ξ-th query on OGen.

- $\mathsf{G}_{5,\xi-1,0}$: Identical to $\mathsf{G}_{5,\xi-1}$.
- $\mathsf{G}_{5,\xi-1,1}$: Identical to $\mathsf{G}_{5,\xi-1,0}$, except that the challenger computes the punctured key $K^*_{t^{(\xi)}} \leftarrow \mathsf{Prf.Punc}(K^*, t^{(\xi)})$, and a value $y_\xi = \mathsf{Prf.Eval}(K^*, t^{(\xi)})$ at beginning. We define the augmented evaluation as Section 3.7:

$$\widehat{\mathsf{Prf.Eval}}_{y_\xi}(K^*_{t^{(\xi)}}, t) = \begin{cases} y_\xi, & \text{if } t = t^{(\xi)} \\ \mathsf{Prf.Eval}(K^*_{t^{(\xi)}}, t), & \text{if } t \neq t^{(\xi)} \end{cases}$$

  And for all $q \in [Q]$, when answering the q-th query to OGen, we replace all $\mathsf{Prf.Eval}(K^*, \cdot)$ with $\widehat{\mathsf{Prf.Eval}}_{y_\xi}(K^*_{t^{(\xi)}}, \cdot)$. In particular:
  - If $q < \xi$, on input (j, g_j), it sample $s_j \leftarrow \mathsf{Coin}$ as same as in $\mathsf{G}_{5,\xi-1,0}$.
  - If $q = \xi$, on input (i, g_i), when encoding c_i, we sample $s_i = \boxed{\widehat{\mathsf{Prf.Eval}}_{y_\xi}(K^*_{t^{(\xi)}}, t^{(\xi)})} = y_\xi$.
  - If $q > \xi$, on input (j, g_j), when encoding c_j, we use $s_j = \boxed{\widehat{\mathsf{Prf.Eval}}_{y_\xi}(K^*_{t^{(\xi)}}, t^{(q)})}$ instead. Note that $t^{(q)} \neq t^{(\xi)}$.

  We have $\mathsf{G}_{5,\xi-1,1} \equiv \mathsf{G}_{5,\xi-1,0}$. This follows from the fact that $\widehat{\mathsf{Prf.Eval}}_{y_\xi}(K^*_{t^{(\xi)}}, \cdot)$ is functionally identical to $\mathsf{Prf.Eval}(K^*, \cdot)$, which ensured by (1) the specification of pre-determined value y_ξ on the punctured point $t^{(\xi)}$; (2) the functionality of Π_4.
- $\mathsf{G}_{5,\xi-1,2}$: Identical to $\mathsf{G}_{5,\xi-1,1}$, except that we replace challenge ciphertext with

$$\mathsf{ct}^* \leftarrow \mathsf{R.Enc}\left(\mathsf{mpk}, \left(\bot, \boxed{K^*_{t^{(\xi)}}}, k^*\right)\right).$$

  For all $i \in [L]$, we have $\mathsf{mpk}^*_{i,g_i^*} = (\mathsf{R.pk}^*_{i,\mathsf{ReEnc}^*_i}, \mathsf{ReEnc}^*_i)$ where

$$(\mathsf{R.pk}^*_{i,\mathsf{ReEnc}^*_i}, \mathsf{R.sk}^*_{i,\mathsf{ReEnc}^*_i}) \leftarrow \mathsf{R.Gen}(\mathsf{R.crs}, i, \mathsf{ReEnc}^*_i)$$

  such that

$$\overbrace{\mathsf{ReEnc}^*_i(\bot, K^*, k^*)}^{\text{in } \mathsf{G}_{5,\xi,1}} = \mathsf{S.Dec}(k^*, c^*_i) = \overbrace{\mathsf{ReEnc}^*_i(\bot, K^*_{t^{(\xi)}}, k^*)}^{\text{in } \mathsf{G}_{5,\xi,2}}$$

  With the security of Π_1, we have $\mathsf{G}_{5,\xi-1,2} \approx_c \mathsf{G}_{5,\xi-1,1}$. Notice that all $\mathsf{R.sk}^*_{i,\mathsf{ReEnc}^*_i}$ can be leaked during $\mathsf{sk}_{i,f} \leftarrow \mathsf{OKey}(i, f)$, but the reduction can still go through, which is ensured by above equation for all $i \in [L]$.
- $\mathsf{G}_{5,\xi,3}$: Identical to $\mathsf{G}_{5,\xi,2}$, except that we substitute punctured value to random value. Namely, we change y_ξ as $y_\xi \leftarrow \boxed{\mathsf{Coin}}$. We have $\mathsf{G}_{5,\xi,3} \approx_c \mathsf{G}_{5,\xi,2}$, this follows from the pseudorandomness at punctured point $t^{(\xi)}$ of Π_4, which is ensured by the observation that K^* is fully hidden to the adversary, and the $t^{(q)} \neq t^{(\xi)}$ for all $q \neq \xi$.
- $\mathsf{G}_{5,\xi,4}$: Identical to $\mathsf{G}_{5,\xi,3}$, except that when answering the ξ-th query of OGen, on input (i, g_i), it computes $c_i \leftarrow \mathsf{S.Enc}(k^*, \boxed{\mathsf{F.ct}_i})$, where $\boxed{\mathsf{F.ct}_i} \leftarrow \mathsf{F.Enc}(\mathsf{F.mpk}_i, g_i(x^*_b); \boxed{s_i})$, and $\boxed{s_i} \leftarrow \boxed{\mathsf{Coin}}$. We have $\mathsf{G}_{5,\xi,4} \equiv \mathsf{G}_{5,\xi,3}$. This follows from the fact that the distribution of s_i is truly random in both two games.
- $\mathsf{G}_{5,\xi,5}$: Identical to $\mathsf{G}_{5,\xi,4}$ except that we replace ct^* as

$$\mathsf{ct}^* \leftarrow \mathsf{R.Enc}(\mathsf{mpk}, (\bot, \boxed{K^*}, k^*))$$

  For all $i \in [L]$, we have $\mathsf{mpk}^*_{i,g_i^*} = (\mathsf{R.pk}^*_{i,\mathsf{ReEnc}^*_i}, \mathsf{ReEnc}^*_i)$ where

$$(\mathsf{R.pk}^*_{i,\mathsf{ReEnc}^*_i}, \mathsf{R.sk}^*_{i,\mathsf{ReEnc}^*_i}) \leftarrow \mathsf{R.Gen}(\mathsf{R.crs}, i, \mathsf{ReEnc}^*_i)$$

  such that

$$\overbrace{\mathsf{ReEnc}^*_i(\bot, K^*, k^*)}^{\text{in } \mathsf{G}_{5,\xi,5}} = \mathsf{S.Dec}(k^*, c^*_i) = \overbrace{\mathsf{ReEnc}^*_i(\bot, K^*_{t^{(\xi)}}, k^*)}^{\text{in } \mathsf{G}_{5,\xi,4}}$$

  With the security of Π_1, we have $\mathsf{G}_{5,\xi-1,5} \approx_c \mathsf{G}_{5,\xi-1,4}$. Notice that all $\mathsf{R.sk}^*_{i,\mathsf{ReEnc}^*_i}$ can be leaked during $\mathsf{sk}_{i,f} \leftarrow \mathsf{OKey}(i, f)$, but the reduction can still go through, which is ensured by above equation for all $i \in [L]$.

– $\mathsf{G}_{5,\xi-1,6}$: Identical to $\mathsf{G}_{5,\xi-1,5}$, except that the challenger doesn't generate punctured key on $t^{(\xi)}$ and sample pre-determined punctured value y_ξ anymore. And for all $q \in [Q]$, when answering the q-th query to OGen, we replace all $\widehat{\mathsf{Prf.Eval}}_{y_\xi}(K^*_{t_1^{(\xi)}}, \cdot)$ with $\mathsf{Prf.Eval}(K^*, \cdot)$. In particular:
  - If $q < \xi$, on input (j, g_j), it sample $s_j \leftarrow \mathsf{Coin}$ as same as in $\mathsf{G}_{5,\xi-1,0}$.
  - If $q = \xi$, on input (i, g_i), when encoding c_i, we sample $s_i \leftarrow \mathsf{Coin}$.
  - If $q > \xi$, on input (j, g_j), when encoding c_j, we use $s_j = \boxed{\mathsf{Prf.Eval}(K^*, t^{(q)})}$ instead. Note that $t^{(q)} \neq t^{(\xi)}$

  We have $\mathsf{G}_{5,\xi-1,6} \equiv \mathsf{G}_{5,\xi-1,5}$. This follows from the fact that $\widehat{\mathsf{Prf.Eval}}_{y_\xi}(K^*_{t^{(\xi)}}, \cdot)$ and $\mathsf{Prf.Eval}(K^*, \cdot)$ are functionally identical except at punctured point $t^{(\xi)}$, and $t^{(\xi)}$ is never evaluated in both two games.

Observe that we have $\mathsf{G}_{5,\xi,6} = \mathsf{G}_{5,\xi}$. And this proves $\mathsf{G}_{5,\xi-1} \approx_c \mathsf{G}_{5,\xi}$ readily.

Instantiations To instantiate our construction above, we claim some candidate schemes of building blocks can achieve the requirements as follows:

– For supporting the registration of function ReEnc, it needs the underlying Π_1 to support general function class (at least function class larger than quadratic function). Such a slotted Reg-FE only appears in [FFM+23,DPY24] and the security relies on iO (a minor modification for "function-dependent generation" is required).
– The FE for arbitrary function class F and achieves security beyond selective IND-security is provided by the iO-based schemes in [GGH+13,Wat15].
– The SKE with pseudorandom ciphertext is available in [Gol04].
– The punctured PRF in [KPTZ13,BW13,SW14,BGI14] can satisfy our requirements.

10 From Slotted Delegated Reg-FE to Delegated Reg-FE

In this section, we present a generic transformation from slotted delegated Reg-FE (c.f. Section 4.2) to delegated Reg-FE (c.f. Section 4.1). The transformation is adapted from "power-of-two" method [HLWW23] that transforms slotted Reg-ABE to Reg-ABE. Assume a delegated Reg-FE support $L = 2^m$ clients at most, the transformation will invoke $m+1$ instances of slotted delegated Reg-FE with $2^0, \ldots, 2^m$ slots. In the this section, we use two difference indices i and j, respectively referring to the global range from 1 to L and instances' internal ranges from 1 to 2^k (for each $k \in [0, m]$)

Auxiliary Data Structure. We will count clients from 0 and set $\mathsf{aux} = (\mathsf{ctr}_{\mathsf{aux}}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathsf{mpk})$:

– Counter $\mathsf{ctr}_{\mathsf{aux}} \in [0, L]$ is the current number of registered clients in the system, or the index of the next client.
– $\mathcal{D}_1$ is a dictionary that maps $k \in [0, m]$ and $j \in [2^k]$ to master public key $\mathsf{mpk}_{k,j}$ and function $g_{k,j}$.
– $\mathcal{D}_2$ is a dictionary that maps $k \in [0, m]$ and $i \in [L]$ to a helper key hsk.
– $\mathcal{D}_3$ is a dictionary that maps $k \in [0, m]$ and $j \in [2^k]$ to a counter ctr.
– mpk_+ will be in the form $(\mathsf{ctr}_{\mathsf{aux}}, \mathsf{mpk}_{+,0}, \ldots, \mathsf{mpk}_{+,m})$.

Initially, we set $\mathsf{ctr}_{\mathsf{aux}} = 0$, $\mathcal{D}_1 = \emptyset$, $\mathcal{D}_2 = \emptyset$, $\mathcal{D}_3 = \emptyset$, $\mathsf{mpk} = (0, \bot, \ldots, \bot)$; the system is overloaded when $\mathsf{ctr} = L$.

Transformation. With slotted delegated Reg-FE scheme $\Pi_s = (\mathsf{sSetup}, \mathsf{sGen}, \mathsf{sVer}, \mathsf{sAgg}, \mathsf{sEnc}, \mathsf{sKey}, \mathsf{sDec})$, our delegated Reg-FE works as follow:

– $\mathsf{Setup}(1^\lambda, 1^L, F, G)$: Compute $m = \log L$, for all $k \in [0, m]$, run $\mathsf{crs}_k \leftarrow \mathsf{sSetup}(1^\lambda, 1^{2^k}, F, G)$. Output

$$\mathsf{crs} = (\mathsf{crs}_0, \ldots, \mathsf{crs}_m).$$

– $\mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$: Parse $\mathsf{aux} = (\mathsf{ctr}_{\mathsf{aux}}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathsf{mpk}_+)$ where $\mathsf{mpk}_+ = (\mathsf{ctr}_{\mathsf{aux}}, \mathsf{mpk}_{+,0}, \ldots, \mathsf{mpk}_{+,m})$. Set $\mathsf{ctr} = \mathsf{ctr}_{\mathsf{aux}}$ and for all $k \in [0, m]$, run

$$(\mathsf{mpk}_k, \mathsf{msk}_k) \leftarrow \mathsf{sGen}(\mathsf{crs}_k, (\mathsf{ctr} \bmod 2^k) + 1).$$

Output

$$\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_0, \ldots, \mathsf{mpk}_m) \quad \text{and} \quad \mathsf{msk} = (\mathsf{ctr}, \mathsf{msk}_0, \ldots, \mathsf{msk}_m).$$

– $\mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}, g)$: Parse $\mathsf{aux} = (\mathsf{ctr}_{\mathsf{aux}}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathsf{mpk}_+)$ where $\mathsf{mpk}_+ = (\mathsf{ctr}_{\mathsf{aux}}, \mathsf{mpk}_{+,0}, \ldots, \mathsf{mpk}_{+,m})$ and $\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_0, \ldots, \mathsf{mpk}_m)$. Abort if one of the following checks doesn't pass:

$$\mathsf{ctr}_{\mathsf{aux}} \stackrel{?}{=} \mathsf{ctr} \quad \text{and} \quad \mathsf{sVer}(\mathsf{crs}_k, (\mathsf{ctr} \bmod 2^k) + 1, \mathsf{mpk}_k) \stackrel{?}{=} 1 \quad k \in [0, m]$$

For each $k \in [0, m]$, update $\mathcal{D}_1[k, (\mathsf{ctr} \bmod 2^k)+1] = (\mathsf{mpk}_k, g)$ and $\mathcal{D}_3[k, (\mathsf{ctr} \bmod 2^k)+1] = \mathsf{ctr}$; furthermore, if $\mathsf{ctr} + 1 = 0 \bmod 2^k$, run

$$(\mathsf{mpk}'_{+,k}, \mathsf{hsk}'_{k,1}, \ldots, \mathsf{hsk}'_{k,2^k}) \leftarrow \mathsf{sAgg}(\mathsf{crs}_k, \mathcal{D}_1[k, 1], \ldots, \mathcal{D}_1[k, 2^k])$$

and update $\mathcal{D}_2[k, \mathsf{ctr} + 1 - 2^k + j] = \mathsf{hsk}'_{k,j}$ for all $j \in [2^k]$; otherwise, set $\mathsf{mpk}'_{+,k} = \mathsf{mpk}_{+,k}$. Output

$$\mathsf{mpk}_+ = (\mathsf{ctr}_{\mathsf{aux}} + 1, \mathsf{mpk}'_{+,0}, \ldots, \mathsf{mpk}'_{+,m}) \quad \text{and} \quad \mathsf{aux} = (\mathsf{ctr}_{\mathsf{aux}} + 1, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathsf{mpk}_+)$$

– $\mathsf{Enc}(\mathsf{mpk}_+, x)$: Parse $\mathsf{mpk}_+ = (\mathsf{ctr}_{\mathsf{aux}}, \mathsf{mpk}_{+,0}, \ldots, \mathsf{mpk}_{+,m})$. Set $\mathsf{ctr}_{\mathsf{ct}} = \mathsf{ctr}_{\mathsf{aux}}$, for all $k \in [0, m]$, compute

$$\mathsf{ct}_k = \begin{cases} \bot & \text{if } \mathsf{mpk}_{+,k} = \bot \\ \mathsf{sEnc}(\mathsf{mpk}_{+,k}, x) & \text{otherwise} \end{cases}$$

Output

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

– $\mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk})$: Parse $\mathsf{aux} = (\mathsf{ctr}_{\mathsf{aux}}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathsf{mpk}_+)$ and $\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_0, \ldots, \mathsf{mpk}_m)$. Abort if $\mathsf{ctr} \geq \mathsf{ctr}_{\mathsf{aux}}$; otherwise, output

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

– $\mathsf{Key}(\mathsf{msk}, \mathsf{hsk}, \mathsf{aux}, f)$: Parse $\mathsf{aux} = (\mathsf{ctr}_{\mathsf{aux}}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathsf{mpk}_+)$, $\mathsf{msk} = (\mathsf{ctr}, \mathsf{msk}_0, \ldots, \mathsf{msk}_m)$ and $\mathsf{hsk} = (\mathsf{hsk}_0, \ldots, \mathsf{hsk}_m)$. Abort if $\mathsf{ctr} \geq \mathsf{ctr}_{\mathsf{aux}}$; otherwise, for all $k \in [0, m]$, compute

$$\mathsf{sk}_{k,f} = \begin{cases} \bot & \text{if } \mathsf{hsk}_k = \bot \vee \mathcal{D}_3[k, (\mathsf{ctr} \bmod 2^k) + 1] \neq \mathsf{ctr} \\ \mathsf{sKey}(\mathsf{msk}_k, \mathsf{hsk}_k, f) & \text{otherwise} \end{cases}$$

[9] Output

$$\mathsf{sk}_{y'} = (\mathsf{ctr}, \mathsf{sk}_{0,f}, \ldots, \mathsf{sk}_{m,f}).$$

– $\mathsf{Dec}(\mathsf{sk}_f, \mathsf{hsk}, \mathsf{ct})$: Parse $\mathsf{sk}_f = (\mathsf{ctr}, \mathsf{sk}_{0,f}, \ldots, \mathsf{sk}_{m,f})$, $\mathsf{hsk} = (\mathsf{hsk}_0, \ldots, \mathsf{hsk}_m)$ and $\mathsf{ct} = (\mathsf{ctr}_{\mathsf{ct}}, \mathsf{ct}_0, \ldots, \mathsf{ct}_m)$. Abort if $\mathsf{ctr} \geq \mathsf{ctr}_{\mathsf{ct}}$; otherwise, find $k^* = \max\{k \in [0, m] : \text{s.t. } 2^k \leq (\mathsf{ctr} \oplus \mathsf{ctr}_{\mathsf{ct}})\}$. Output

$$z = \begin{cases} \texttt{getupd} & \text{if } \mathsf{hsk}_{k^*} = \bot \vee \mathsf{sk}_{k^*,f} = \bot \\ \mathsf{sDec}(\mathsf{sk}_{k^*,f}, \mathsf{hsk}_{k^*,f}, \mathsf{ct}_{k^*}) & \text{otherwise} \end{cases}$$

[9] Note that $\mathcal{D}_3[k, (\mathsf{ctr} \bmod 2^k) + 1] \neq \mathsf{ctr}$ means this client is no longer aggregated in the k-th slotted instance.

Correctness. Assume $\Pi_s = (\mathsf{sSetup}, \mathsf{sGen}, \mathsf{sVer}, \mathsf{sAgg}, \mathsf{sEnc}, \mathsf{sKey}, \mathsf{sDec})$ is a slotted delegated Reg-FE with completeness and correctness (defined in Section 4.2), the delegated Reg-FE obtained via above transformation achieve the correctness as defined in Section 4.1.

Proof. Firstly, note that ignoring the operation on $\mathcal{D}_3$, our Setup, Reg, Enc, Upd algorithms work identically to that in the original "power-of-two" method from [HLWW23]. For all $\mathsf{crs} = (\mathsf{crs}_0, \ldots, \mathsf{crs}_m)$, where

$$\mathsf{crs}_k \leftarrow \mathsf{sSetup}(1^\lambda, 1^{2^k}, F, G) \quad \forall k \in [0, m]$$

And for any $g^* \in G$, $\mathsf{ORegT}(g^*)$ generated $\mathsf{mpk}^* = (\mathsf{ctr}^*, \mathsf{mpk}^*_0, \ldots, \mathsf{mpk}^*_m)$ and $\mathsf{msk}^* = (\mathsf{ctr}^*, \mathsf{msk}^*_0, \ldots, \mathsf{msk}^*_m)$, where $\mathsf{ctr}^* + 1 = t$ and

$$(\mathsf{mpk}^*_k, \mathsf{msk}^*_k) \leftarrow \mathsf{sGen}(\mathsf{crs}_k, (\mathsf{ctr}^* \bmod 2^k) + 1) \quad \forall k \in [0, m]$$

We continue our proof by considering $\mathsf{ODec}(j)$ for any j. Let $\mathcal{E}[j] = x_j \neq \perp$ which was updated in $\mathsf{OEnc}(i_j, x_j, x'_j, \mathsf{m}_j)$, let $\mathsf{ct}_j = (\mathsf{ctr}_{\mathsf{ct}}, \mathsf{ct}_{j,0}, \ldots, \mathsf{ct}_{j,m})$ and $\mathsf{mpk}_+ = (\mathsf{ctr}_{\mathsf{aux}}, \mathsf{mpk}_{+,0}, \ldots, \mathsf{mpk}_{+,m})$, where we have $\mathsf{ctr}_{\mathsf{ct}} = \mathsf{ctr}_{\mathsf{aux}}$ and

$$\mathsf{ct}_{j,k} \leftarrow \mathsf{sEnc}(\mathsf{mpk}_{+,k}, x_j, x'_j, \mathsf{m}_j) \quad \forall k \in [0, m]$$

With the restriction in the correctness game, we have $\mathsf{ctr}_{\mathsf{ct}} = \mathsf{ctr}_{\mathsf{aux}} = i_j \geq t = \mathsf{ctr}^* + 1$, along with the reason in [HLWW23, Lemma 6.3], for $k^* = \max\{k \in [0, m] : \text{s.t. } 2^k \leq (\mathsf{ctr}^* \oplus \mathsf{ctr}_{\mathsf{ct}})\}$, we have

$$(\mathsf{mpk}_{+,k^*}, \ldots, \mathcal{D}_2[k^*, \mathsf{ctr}^* + 1], \ldots) \leftarrow \mathsf{sAgg}(\mathsf{crs}_{k^*}, \ldots, (\mathsf{mpk}^*_{k^*}, g^*), \ldots)$$

Namely $(\mathsf{mpk}^*_{k^*}, g^*)$ is aggregated into mpk_{+,k^*} and $\mathcal{D}_2[k^*, \mathsf{ctr}^*{+}1]$ records the corresponding $\mathsf{hsk}^*_{k^*}$, this also implies $\mathcal{D}_3[k, (\mathsf{ctr}^* \bmod 2^{k^*}){+}1] = \mathsf{ctr}^*$. With the construction of Reg, it ensures that all other mpk_{k^*} aggregated into mpk_{+,k^*} satisfy $\mathsf{sVer}(\mathsf{crs}_{k^*}, i, \mathsf{mpk}_{k^*}) = 1$ for all $[2^{k^*}] \setminus \{(\mathsf{ctr}^* \bmod 2^{k^*}) + 1\}$. We consider the following two cases:

- **If** $(\mathbf{hsk}^*_{k^*} = \perp \vee \mathbf{sk}^*_{k^*,f^*} = \perp)$**:** In this case, $\mathsf{ODec}(j)$ runs $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}^*)$, $\mathsf{sk}^*_{f^*} \leftarrow \mathsf{Key}(\mathsf{msk}^*, \mathsf{hsk}^*, \mathsf{aux}, f^*)$ and recompute $\mathsf{m}'_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*_{f^*}, \mathsf{hsk}^*, \mathsf{ct}_j)$. It will assign $\mathsf{hsk}^*_{k^*} = \mathcal{D}_2[k^*, \mathsf{ctr}^*{+}1]$ and since it must have $\mathcal{D}_3[k, (\mathsf{ctr}^* \bmod 2^{k^*}) + 1] = \mathsf{ctr}^*$, we have $\mathsf{sk}^*_{k^*,f^*} \leftarrow \mathsf{sKey}(\mathsf{msk}^*_{k^*}, \mathsf{hsk}^*_{k^*}, f^*)$. And we have $\mathsf{m}'_j = \mathsf{sDec}(\mathsf{sk}^*_{k^*,f^*}, \mathsf{hsk}^*_{k^*}, \mathsf{ct}_{j,k^*})$. Along with the correctness of Π_s, we have $\mathsf{m}'_j = \mathsf{m}_j$.
- **Otherwise:** In this case, we have $\mathsf{ODec}(j)$ output $\mathsf{m}'_j = \mathsf{sDec}(\mathsf{sk}^*_{k^*,f^*}, \mathsf{hsk}^*_{k^*}, \mathsf{ct}_{j,k^*})$. As pointed out by [HLWW23], $\mathsf{hsk}^*_{k^*}$ can only be assigned once, which means $\mathsf{hsk}^*_{k^*} \neq \perp$ is exactly $\mathcal{D}_2[k^*, \mathsf{ctr}^* + 1]$, this also implies that $\mathsf{sk}^*_{k^*,f^*} \in \mathsf{sKey}(\mathsf{msk}^*_{k^*}, \mathsf{hsk}^*_{k^*}, f^*)$ for $\mathsf{sk}^*_{k^*,f^*} \neq \perp$. Along with the correctness of Π_s, we have $\mathsf{m}'_j = \mathsf{m}_j$.

□

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

$$|\mathsf{crs}| = L^2 \cdot \log L \cdot \mathsf{poly}(\lambda, \mathsf{par}); \quad |\mathsf{mpk}_+| = \log L \cdot \mathsf{poly}(\lambda, \mathsf{par}); \quad |\mathsf{hsk}| = \log L \cdot \mathsf{poly}(\lambda, \mathsf{par});$$
$$|\mathsf{ct}| = \log L \cdot \mathsf{poly}(\lambda, \mathsf{par}); \quad |\mathsf{sk}| = \log L \cdot \mathsf{poly}(\lambda, \mathsf{par}).$$

And analogous to [HLWW23], 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. Notice that in delegated Reg-FE, $|\mathcal{R}|$ denotes the number of registered clients, and the number of users can be larger than $|\mathcal{R}|$.

Security. We have the following theorem. Given a slotted delegated Reg-FE with IND-security, the delegated Reg-FE generated obtained via above transformation is secure.

Theorem 6. *Assume $\Pi_s = (\mathsf{sSetup}, \mathsf{sGen}, \mathsf{sVer}, \mathsf{sAgg}, \mathsf{sEnc}, \mathsf{sKey}, \mathsf{sDec})$ is a slotted delegated Reg-FE with adaptive IND-security as defined in Section 4.2, our delegated Reg-FE generated via above transformation achieves the adaptive IND-security defined in Section 4.1.*

Proof. We prove the following technical lemma; along with Lemma 11, these can prove Theorem 6

Lemma 10. *For all adversary $\mathcal{A}$, there exist $\mathcal{B}$ such that*

$$\mathsf{Adv}^{\textit{Del-Reg-FE}}_{\mathcal{A}}(\lambda) \leq \log L \cdot \mathsf{Adv}^{\textit{sDel-Reg-FE-ReAgg}}_{\mathcal{B}}(\lambda)$$

where $L = 2^m$ is the maximum number of clients, and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$.

Game Sequence. Suppose that $\mathsf{crs} = (\mathsf{crs}_0, \ldots, \mathsf{crs}_m)$ is the common reference string, $\mathsf{aux} = (\mathsf{ctr}_{\mathsf{aux}}, \mathcal{D}_1, \mathcal{D}_2, \mathsf{mpk}_+)$ is the auxiliary data, where $\mathsf{mpk}_+ = (\mathsf{ctr}_{\mathsf{aux}}, \mathsf{mpk}_{+,0}, \ldots, \mathsf{mpk}_{+,m})$, x^*, x'^* are the challenge "attribute", $(\mathsf{m}^*_0, \mathsf{m}^*_1)$ is the challenge pair. We prove the Lemma 10 via following game sequence:

- $\mathsf{G}_{k^*}, (k^* \in [0, m])$: Identical to the real game except that for challenge ciphertext $\mathsf{ct}^* = (\mathsf{ctr}_{\mathsf{ct}}, \mathsf{ct}^*_0, \ldots, \mathsf{ct}^*_{k-1}, \mathsf{ct}^*_k, \ldots, \mathsf{ct}^*_m)$, we have

$$\mathsf{ct}^*_k \leftarrow \begin{cases} \perp & \text{if } \mathsf{mpk}_{+,k} = \perp \\ \mathsf{sEnc}(\mathsf{mpk}_{+,k}, \boxed{x^*_1}) & \text{otherwise} \end{cases}, \qquad (\forall k \in [0, k^* - 1]);$$

  and

$$\mathsf{ct}^*_k \leftarrow \begin{cases} \perp & \text{if } \mathsf{mpk}_{+,k} = \perp \\ \mathsf{sEnc}(\mathsf{mpk}_{+,k}, \boxed{x^*_0}) & \text{otherwise} \end{cases}, \qquad (\forall k \in [k^*, m]).$$

  We have $\mathsf{G}_{k^*} \approx \mathsf{G}_{k^*-1}$ for all $k^* \in [m]$. See Lemma 12 for more details.

Observe that when $k^* = 0$, G_0 is the real game with secret bit $b = 0$; and when $k^* = m$, G_m is the real game with secret bit $b = 1$. This readily proves Lemma 10.

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, Berlin, Heidelberg, March / April 2015. 4

ABG+13. Prabhanjan Ananth, Dan Boneh, Sanjam Garg, Amit Sahai, and Mark Zhandry. Differing-inputs obfuscation and applications. Cryptology ePrint Archive, Report 2013/689, 2013. 6

ABS17. Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt. Generic transformations of predicate encodings: Constructions and applications. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 36–66. Springer, Cham, August 2017. 8, 19

ACGU20. Michel Abdalla, Dario Catalano, Romain Gay, and Bogdan Ursu. Inner-product functional encryption with fine-grained access control. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 467–497. Springer, Cham, December 2020. 8, 19

AT24. Nuttapong Attrapadung and Junichi Tomida. A modular approach to registered ABE for unbounded predicates. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part III*, volume 14922 of *LNCS*, pages 280–316. Springer, Cham, August 2024. 2

BGG+14. Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 533–556. Springer, 2014. 6

BGI+12. Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *J. ACM*, 59(2):6:1–6:48, 2012. 2, 5

BGI14. Elette Boyle, Shafi Goldwasser, and Ioana Ivan. Functional signatures and pseudorandom functions. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 501–519. Springer, Berlin, Heidelberg, March 2014. 86

BHR12. Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In Ting Yu, George Danezis, and Virgil D. Gligor, editors, *ACM CCS 2012*, pages 784–796. ACM Press, October 2012. 2

BLM+24. Pedro Branco, Russell W. F. Lai, Monosij Maitra, Giulio Malavolta, Ahmadreza Rahimi, and Ivy K. Y. Woo. Traitor tracing without trusted authority from registered functional encryption. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part III*, volume 15486 of *LNCS*, pages 33–66. Springer, Singapore, December 2024. 2, 5

BS15. Zvika Brakerski and Gil Segev. Hierarchical functional encryption. Cryptology ePrint Archive, Paper 2015/1011, 2015. 6, 15, 16, 23

BSW11. Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273. Springer, Berlin, Heidelberg, March 2011. 2

BW13. Dan Boneh and Brent Waters. Constrained pseudorandom functions and their applications. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 280–300. Springer, Berlin, Heidelberg, December 2013. 86

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, Cham, April / May 2018. 46, 57, 69

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, Berlin, Heidelberg, April 2015. 4, 7, 8, 9, 10, 11, 19

CHW25. Jeffrey Champion, Yao-Ching Hsieh, and David J. Wu. Registered ABE and adaptively-secure broadcast encryption from succinct LWE. Cryptology ePrint Archive, Report 2025/044, 2025. 2, 16, 25, 27

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, Cham, April 2023. 2, 6

DMQ25. Jesko Dujmovic, Giulio Malavolta, and Wei Qi. Registration-based encryption in the plain model, 2025. 2

DPY24. Pratish Datta, Tapas Pal, and Shota Yamada. Registered FE beyond predicates: (attribute-based) linear functions and more. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part I*, volume 15484 of *LNCS*, pages 65–104. Springer, Singapore, December 2024. 2, 5, 16, 21, 86

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, Berlin, Heidelberg, August 2013. 18

FFM+23. Danilo Francati, Daniele Friolo, Monosij Maitra, Giulio Malavolta, Ahmadreza Rahimi, and Daniele Venturi. Registered (inner-product) functional encryption. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part V*, volume 14442 of *LNCS*, pages 98–133. Springer, Singapore, December 2023. 2, 4, 5, 16, 21, 86

FKdP23. Dario Fiore, Dimitris Kolonelos, and Paola de Perthuis. Cuckoo commitments: Registration-based encryption and key-value map commitments for large spaces. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part V*, volume 14442 of *LNCS*, pages 166–200. Springer, Singapore, December 2023. 2

FWW23. Cody Freitag, Brent Waters, and David J. Wu. How to use (plain) witness encryption: Registered ABE, flexible broadcast, and more. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part IV*, volume 14084 of *LNCS*, pages 498–531. Springer, Cham, August 2023. 2

GGH+13. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th FOCS*, pages 40–49. IEEE Computer Society Press, October 2013. 2, 5, 16, 86

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, Cham, 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, Cham, November 2018. 2

GKMR23. Noemi Glaeser, Dimitris Kolonelos, Giulio Malavolta, and Ahmadreza Rahimi. Efficient registration-based encryption. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *ACM CCS 2023*, pages 1065–1079. ACM Press, November 2023. 2

GLWW24. Rachit Garg, George Lu, Brent Waters, and David J. Wu. Reducing the CRS size in registered ABE systems. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part III*, volume 14922 of *LNCS*, pages 143–177. Springer, Cham, August 2024. 2

Gol04. Oded Goldreich. Foundations of cryptography. ii: Basic applications. 2, 05 2004. 86

GPSW06. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 2006*, pages 89–98. ACM Press, October / November 2006. Available as Cryptology ePrint Archive Report 2006/309. 2

GS02. Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. In Yuliang Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 548–566. Springer, Berlin, Heidelberg, December 2002. 6

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, Cham, August 2020. 2

GVW13. Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 545–554. ACM Press, June 2013. 6

HL02. Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-based encryption. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 466–481. Springer, Berlin, Heidelberg, April / May 2002. 6

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, Cham, April 2023. 2, 3, 4, 7, 11, 14, 21, 26, 86, 88

HW15. Pavel Hubácek and Daniel Wichs. On the communication complexity of secure function evaluation with long output. In Tim Roughgarden, editor, *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ITCS 2015, Rehovot, Israel, January 11-13, 2015*, pages 163–172. ACM, 2015. 5

JLS22. Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from LPN over $\mathbb{F}_p$, DLIN, and PRGs in NC^0. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part I*, volume 13275 of *LNCS*, pages 670–699. Springer, Cham, May / June 2022. 2, 5

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, Berlin, Heidelberg, December 2013. 19

KPTZ13. Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos, and Thomas Zacharias. Delegatable pseudorandom functions and applications. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM CCS 2013*, pages 669–684. ACM Press, November 2013. 86

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, Berlin, Heidelberg, April 2015. 19, 20, 32, 46, 57, 69

LOS+10. Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91. Springer, Berlin, Heidelberg, May / June 2010. 6

LWW25. George Lu, Brent Waters, and David J. Wu. Multi-authority registered attribute-based encryption. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025*, pages 3–33, Cham, 2025. Springer Nature Switzerland. 6

O'N10. Adam O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Paper 2010/556, 2010. 2

OT09. Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 214–231. Springer, Berlin, Heidelberg, December 2009. 6

Sha84. Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer, Berlin, Heidelberg, August 1984. 2

SW05. Amit Sahai and Brent R. Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Berlin, Heidelberg, May 2005. 2

SW08. Elaine Shi and Brent Waters. Delegating capabilities in predicate encryption systems. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 560–578. Springer, Berlin, Heidelberg, July 2008. 6

SW14. Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In David B. Shmoys, editor, *46th ACM STOC*, pages 475–484. ACM Press, May / June 2014. 86

Wat15. Brent Waters. A punctured programming approach to adaptively secure functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 678–697. Springer, Berlin, Heidelberg, August 2015. 5, 16, 86

Wee14. Hoeteck Wee. Dual system encryption via predicate encodings. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer, Berlin, Heidelberg, February 2014. 4, 7, 19

Yao82. Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*, pages 80–91. IEEE Computer Society, 1982. 2

ZCHZ24. Yijian Zhang, Jie Chen, Debiao He, and Yuqing Zhang. Bounded collusion-resistant registered functional encryption for circuits. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part I*, volume 15484 of *LNCS*, pages 32–64. Springer, Singapore, December 2024. 2, 5

ZLZ+24. Ziqi Zhu, Jiangtao Li, Kai Zhang, Junqing Gong, and Haifeng Qian. Registered functional encryptions from pairings. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part II*, volume 14652 of *LNCS*, pages 373–402. Springer, Cham, May 2024. 2, 4, 11, 14, 16, 17, 21

ZZC+25. Ziqi Zhu, Kai Zhang, Zhili Chen, Junqing Gong, and Haifeng Qian. Black-box registered ABE from lattices. Cryptology ePrint Archive, Report 2025/051, 2025. 2

ZZGQ23. Ziqi Zhu, Kai Zhang, Junqing Gong, and Haifeng Qian. Registered ABE via predicate encodings. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part V*, volume 14442 of *LNCS*, pages 66–97. Springer, Singapore, December 2023. 2, 4, 7, 8, 9, 10, 11, 13, 14, 20

Appendix

A Missing Proof

A.1 Proof of Lemma 2

For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ such that $\binom{\mathbf{A}}{\mathbf{c}}\mathbf{c}^\perp = \binom{\mathbf{0}}{1}$; any $\mathbf{B} \in \mathbb{Z}_p^{(3k+1)\times k}$, $\mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$ and $\mathbf{D}^\perp \leftarrow \mathbb{Z}_p^{k\times(3k+1)}$ such that $\mathbf{D}^\perp(\mathbf{B}\|\mathbf{D}_\ell) = (\mathbf{0}\|\mathbf{I}_k)$. We recall that the L.H.S of our argument is

$$\begin{aligned}\text{L.H.S} = [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^*, \mathbf{B}, \mathbf{D}_\ell,\\ \mathbf{U}_\ell^*\mathbf{B}, \mathbf{U}_\ell^*\mathbf{D}_\ell, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{U}_\ell^*]_1\end{aligned}$$

and the R.H.S of our argument is

$$\begin{aligned}\text{R.H.S} = [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^* + \boxed{\widetilde{\mathbf{u}}\mathbf{D}^\perp}, \mathbf{B}, \mathbf{D}_\ell,\\ \mathbf{U}_\ell^*\mathbf{B}, \mathbf{U}_\ell^*\mathbf{D}_\ell + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{u}}}, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{U}_\ell^*]_1\end{aligned}$$

We prove that L.H.S $\approx_c$ R.H.S as follows:
Step 1. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\mathbf{G}_\ell]_1) \approx_c ([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^*, \mathbf{B}, \mathbf{D}_\ell,\\ \mathbf{U}_\ell^*\mathbf{B}, \mathbf{U}_\ell^*\mathbf{D}_\ell, [\boxed{\widetilde{\mathbf{T}}\mathbf{A}}, \boxed{\widetilde{\mathbf{T}}\mathbf{A}}\mathbf{U}_\ell^*]_1\end{aligned}$$

Step 2. Use the change of variable

$$\mathbf{U}_\ell^* \mapsto \mathbf{U}_\ell^* + \mathbf{c}^\perp\widetilde{\mathbf{u}}\mathbf{D}^\perp$$

where $\widetilde{\mathbf{u}} \leftarrow \mathbb{Z}_p^{1\times k}$. We have

$$\begin{aligned}\text{L.H.S} \approx_s [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^* + \boxed{\widetilde{\mathbf{u}}\mathbf{D}^\perp}, \mathbf{B}, \mathbf{D}_\ell,\\ \mathbf{U}_\ell^*\mathbf{B}, \mathbf{U}_\ell^*\mathbf{D}_\ell + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{u}}}, [\widetilde{\mathbf{T}}\mathbf{A}, \widetilde{\mathbf{T}}\mathbf{A}\mathbf{U}_\ell^*]_1\end{aligned}$$

Step 3. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{G}_\ell]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\begin{aligned}\text{L.H.S} &\approx_c [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^* + \widetilde{\mathbf{u}}\mathbf{D}^\perp, \mathbf{B}, \mathbf{D}_\ell,\\ &\quad \mathbf{U}_\ell^*\mathbf{B}, \mathbf{U}_\ell^*\mathbf{D}_\ell + \mathbf{c}^\perp\widetilde{\mathbf{u}}, [\boxed{\mathbf{G}_\ell}, \boxed{\mathbf{G}_\ell}\mathbf{U}_\ell^*]_1\\ &= \text{R.H.S}\end{aligned}$$

□

A.2 Proof of Lemma 3

For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \in \mathbb{Z}_p^{k+1}$ such that $\left(\begin{smallmatrix}\mathbf{A}\\ \mathbf{c}\end{smallmatrix}\right)\mathbf{c}^\perp = \left(\begin{smallmatrix}\mathbf{0}\\ 1\end{smallmatrix}\right)$; any $\mathbf{B}, \mathbf{D}_\ell \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$, $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$ and $\mathbf{R}^\perp \in \mathbb{Z}_p^{k\times(3k+1)}$ such that $\mathbf{R}^\perp\left(\mathbf{B}\|\mathbf{D}_\ell\|\widetilde{\mathbf{R}}\right) = (\mathbf{0}\|\mathbf{0}\|\mathbf{I}_k)$. We recall the L.H.S of our argument is

$$\begin{aligned}\text{L.H.S} = [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell},\\ \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}),\\ [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{W}^*_{1,\ell}]_1,\\ \left\{[\mathbf{G}_{\ell,j}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

and the R.H.S of our argument is

$$\begin{aligned}\text{R.H.S} = [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell} + \boxed{\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp)},\\ \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{w}}},\\ [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{W}^*_{1,\ell}]_1,\\ \left\{[\mathbf{G}_{\ell,j}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

We prove that L.H.S $\approx_c$ R.H.S as follows:

Step 1. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\mathbf{G}_\ell]_1) \approx_c ([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell},\\ \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}),\\ [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\boxed{\widetilde{\mathbf{T}}\mathbf{A}}, \boxed{\widetilde{\mathbf{T}}\mathbf{A}}\mathbf{W}^*_{1,\ell}]_1,\\ \left\{[\mathbf{G}_{\ell,j}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

Step 2. With MDDH assumption w.r.t on $[\mathbf{B}]_2$ which ensure that

$$([\mathbf{B}]_2, [\mathbf{G}_{\ell,j}]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{B}\widetilde{\mathbf{T}}_j]_2) \quad \forall j \in [L] \setminus \{\ell\}$$

when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$, $\widetilde{\mathbf{T}}_j \leftarrow \mathbb{Z}_p^{k\times(4k+1)}$ and $\mathbf{G}_{\ell,j} \leftarrow \mathbb{Z}_p^{(3k+1)\times(4k+1)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell},\\ \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}),\\ [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\widetilde{\mathbf{T}}\mathbf{A}, \widetilde{\mathbf{T}}\mathbf{A}\mathbf{W}^*_{1,\ell}]_1,\\ \left\{[\boxed{\mathbf{B}\widetilde{\mathbf{T}}_j}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{B}\widetilde{\mathbf{T}}_j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

Step 3. Use the change of variable

$$\mathbf{W}^*_{1,\ell} \mapsto \mathbf{W}^*_{1,\ell} + \mathbf{c}^\perp\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp)$$

where $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{1\times kn'}$. We have

$$\begin{aligned}\text{L.H.S} \approx_s [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell} + \boxed{\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp)},\\ \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{w}}},\\ [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\widetilde{\mathbf{T}}\mathbf{A}, \widetilde{\mathbf{T}}\mathbf{A}\mathbf{W}^*_{1,\ell}]_1,\\ \left\{[\mathbf{B}\widetilde{\mathbf{T}}_j, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}\widetilde{\mathbf{T}}_j)]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

Step 4. With MDDH assumption w.r.t on $[\mathbf{B}]_2$ which ensure that

$$([\mathbf{B}]_2, [\mathbf{B}\widetilde{\mathbf{T}}_j]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{G}_{\ell,j}]_2) \quad \forall j \in [L] \setminus \{\ell\}$$

when $\mathbf{B} \leftarrow \mathbb{Z}_p^{(3k+1)\times k}$, $\widetilde{\mathbf{T}}_j \leftarrow \mathbb{Z}_p^{k\times(4k+1)}$ and $\mathbf{G}_{\ell,j} \leftarrow \mathbb{Z}_p^{(3k+1)\times(4k+1)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c\ & [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell} + \widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp),\\ & \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \mathbf{c}^\perp\widetilde{\mathbf{w}},\\ & [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\widetilde{\mathbf{T}}\mathbf{A}, \widetilde{\mathbf{T}}\mathbf{A}\mathbf{W}^*_{1,\ell}]_1,\\ & \left\{[\boxed{\mathbf{G}_{\ell,j}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{G}_{\ell,j}})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

Step 5. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{G}_\ell]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c\ & [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell} + \widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp),\\ & \mathbf{D}_\ell, \widetilde{\mathbf{R}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{D}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \widetilde{\mathbf{R}}) + \mathbf{c}^\perp\widetilde{\mathbf{w}},\\ & [\mathbf{B}]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B})]_2, [\boxed{\mathbf{G}_\ell}, \boxed{\mathbf{G}_\ell}\mathbf{W}^*_{1,\ell}]_1,\\ & \left\{[\mathbf{G}_{\ell,j}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\\ =\ & \text{R.H.S}\end{aligned}$$

□

A.3 Proof of Lemma 5

For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ such that $\left(\begin{smallmatrix}\mathbf{A}\\ \mathbf{c}\end{smallmatrix}\right)\mathbf{c}^\perp = \left(\begin{smallmatrix}\mathbf{0}\\ 1\end{smallmatrix}\right)$; any basis $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B}_2 \leftarrow \mathbb{Z}_p^{(2k+1)}$, $\mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, with dual basis $\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel$, and any $\mathbf{d}^\perp \in \mathsf{span}((\mathbf{B}_3^\parallel)^\top)$ such that $\mathbf{d}^\perp\mathbf{B}_1 = \mathbf{0}$ and $\mathbf{d}^\perp\mathbf{B}_2 = 0$; for any $\widehat{\mathbf{x}} \in \mathbb{Z}_p^{1\times n}$ and all $\mathcal{K}_\ell$. We recall the L.H.S of our argument is

$$\begin{aligned}\text{L.H.S} = & [\mathbf{A}]_1, \mathbf{c}, [\mathbf{G}]_1, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{d}^\perp, [\mathbf{A}\mathbf{U}]_1, \mathbf{c}\mathbf{U},\\ & [\mathbf{G}\mathbf{U}]_1, \mathbf{U}(\mathbf{I}_n \otimes (\mathbf{B}_1\|\mathbf{B}_2)), \{\mathbf{U}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})\}_{\mathbf{f}\in\mathcal{K}_\ell}\end{aligned}$$

and the R.H.S of our argument is

$$\begin{aligned}\text{R.H.S} = & [\mathbf{A}]_1, \mathbf{c}, [\mathbf{G}]_1, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{d}^\perp, [\mathbf{A}\mathbf{U}]_1, \mathbf{c}\mathbf{U} + \boxed{\widehat{\mathbf{x}} \otimes \mathbf{d}^\perp},\\ & [\mathbf{G}\mathbf{U}]_1, \mathbf{U}(\mathbf{I}_n \otimes (\mathbf{B}_1\|\mathbf{B}_2)), \{\mathbf{U}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \boxed{\mathbf{c}^\perp(\widehat{\mathbf{x}}\mathbf{f}^\top \otimes \mathbf{d}^\perp)}\}_{\mathbf{f}\in\mathcal{K}_\ell}\end{aligned}$$

We prove that L.H.S $\approx_c$ R.H.S as follows:

Step 1. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\mathbf{G}]_1) \approx_c ([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G} \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c\ & [\mathbf{A}]_1, \mathbf{c}, [\boxed{\widetilde{\mathbf{T}}\mathbf{A}}]_1, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{d}^\perp, [\mathbf{A}\mathbf{U}]_1, \mathbf{c}\mathbf{U},\\ & [\boxed{\widetilde{\mathbf{T}}\mathbf{A}}\mathbf{U}]_1, \mathbf{U}(\mathbf{I}_n \otimes (\mathbf{B}_1\|\mathbf{B}_2)), \{\mathbf{U}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1})\}_{\mathbf{f}\in\mathcal{K}_\ell}\end{aligned}$$

Step 2. Use the change of variable

$$\mathbf{U} \mapsto \mathbf{U} + \mathbf{c}^\perp(\widehat{\mathbf{x}} \otimes \mathbf{d}^\perp)$$

We have

$$\text{L.H.S} \approx_s [\mathbf{A}]_1, \mathbf{c}, [\widetilde{\mathbf{T}}\mathbf{A}]_1, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{d}^\perp, [\mathbf{A}\mathbf{U}]_1, \mathbf{c}\mathbf{U} + \boxed{\widehat{\mathbf{x}} \otimes \mathbf{d}^\perp},$$
$$[\widetilde{\mathbf{T}}\mathbf{A}\mathbf{U}]_1, \mathbf{U}(\mathbf{I}_n \otimes (\mathbf{B}_1\|\mathbf{B}_2)), \{\mathbf{U}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \boxed{\mathbf{c}^\perp(\widehat{\mathbf{x}}\mathbf{f}^\top \otimes \mathbf{d}^\perp)}\}_{\mathbf{f}\in\mathcal{K}_\ell}$$

Step 3. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{G}]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G} \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\text{L.H.S} \approx_c [\mathbf{A}]_1, \mathbf{c}, [\boxed{\mathbf{G}}]_1, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{d}^\perp, [\mathbf{A}\mathbf{U}]_1, \mathbf{c}\mathbf{U} + \widehat{\mathbf{x}} \otimes \mathbf{d}^\perp,$$
$$[\boxed{\mathbf{G}}\mathbf{U}]_1, \mathbf{U}(\mathbf{I}_n \otimes (\mathbf{B}_1\|\mathbf{B}_2)), \{\mathbf{U}(\mathbf{f}^\top \otimes \mathbf{I}_{2k+1}) + \mathbf{c}^\perp(\widehat{\mathbf{x}}\mathbf{f}^\top \otimes \mathbf{d}^\perp)\}_{\mathbf{f}\in\mathcal{K}_\ell}$$

□

A.4 Proof of Lemma 9

For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ such that $\binom{\mathbf{A}}{\mathbf{c}}\mathbf{c}^\perp = \binom{\mathbf{0}}{1}$; any $\mathbf{B}_1 \in \mathbb{Z}_p^{(5k+2)\times k}$, $\mathbf{B}_2 \in \mathbb{Z}_p^{(5k+2)\times(2k+1)}$, $\mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(5k+2)\times(2k+1)}$, with dual basis $\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel$, and any $\mathbf{v}^{(3)} \in \mathsf{span}((\mathbf{B}_3^\parallel)^\top)$ such that $\mathbf{v}^{(3)}(\mathbf{B}_1\|\mathbf{B}_2) = \mathbf{0}$. We recall the L.H.S of our argument is

$$\text{L.H.S} = [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^*, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{B}_3, \mathbf{v}^{(3)},$$
$$\mathbf{U}_\ell^*(\mathbf{B}_1\|\mathbf{B}_2), \mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{U}_\ell^*]_1$$

and the R.H.S of our argument is

$$\text{R.H.S} = [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^* + \boxed{\widetilde{u}\mathbf{v}^{(3)}}, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{B}_3, \mathbf{v}^{(3)},$$
$$\mathbf{U}_\ell^*(\mathbf{B}_1\|\mathbf{B}_2), \mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell + \boxed{\mathbf{c}^\perp\widetilde{u}\mathbf{v}^{(3)}\mathbf{B}_3\widehat{\mathbf{R}}_\ell}, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{U}_\ell^*]_1$$

We prove that L.H.S $\approx_c$ R.H.S as follows:

Step 1. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\mathbf{G}_\ell]_1) \approx_c ([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\text{L.H.S} \approx_c [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^*, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{B}_3, \mathbf{v}^{(3)},$$
$$\mathbf{U}_\ell^*(\mathbf{B}_1\|\mathbf{B}_2), \mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell, [\boxed{\widetilde{\mathbf{T}}\mathbf{A}}, \boxed{\widetilde{\mathbf{T}}\mathbf{A}}\mathbf{U}_\ell^*]_1$$

Step 2. Use the change of variable

$$\mathbf{U}_\ell^* \mapsto \mathbf{U}_\ell^* + \mathbf{c}^\perp\widetilde{u}\mathbf{v}^{(3)}$$

where $\widetilde{u} \leftarrow \mathbb{Z}_p$. We have

$$\text{L.H.S} \approx_s [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^* + \boxed{\widetilde{u}\mathbf{v}^{(3)}}, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{B}_3, \mathbf{v}^{(3)},$$
$$\mathbf{U}_\ell^*(\mathbf{B}_1\|\mathbf{B}_2), \mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell + \boxed{\mathbf{c}^\perp\widetilde{u}\mathbf{v}^{(3)}\mathbf{B}_3\widehat{\mathbf{R}}_\ell}, [\widetilde{\mathbf{T}}\mathbf{A}, \widetilde{\mathbf{T}}\mathbf{A}\mathbf{U}_\ell^*]_1$$

Step 3. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{G}_\ell]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\text{L.H.S} \approx_c [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{U}_\ell^*]_1, \mathbf{c}\mathbf{U}_\ell^* + \widetilde{u}\mathbf{v}^{(3)}, (\mathbf{B}_1\|\mathbf{B}_2), \mathbf{B}_3, \mathbf{v}^{(3)},$$
$$\mathbf{U}_\ell^*(\mathbf{B}_1\|\mathbf{B}_2), \mathbf{U}_\ell^*\mathbf{B}_3\widehat{\mathbf{R}}_\ell + \mathbf{c}^\perp\widetilde{u}\mathbf{v}^{(3)}\mathbf{B}_3\widehat{\mathbf{R}}_\ell, [\boxed{\mathbf{G}_\ell}, \boxed{\mathbf{G}_\ell}\mathbf{U}_\ell^*]_1$$
$$= \text{R.H.S}$$

□

A.5 Proof of Lemma 9

For any $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and $\mathbf{c}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ such that $\left(\begin{smallmatrix}\mathbf{A}\\ \mathbf{c}\end{smallmatrix}\right)\mathbf{c}^\perp = \left(\begin{smallmatrix}\mathbf{0}\\ 1\end{smallmatrix}\right)$; any $\mathbf{B}_1 \in \mathbb{Z}_p^{(5k+2)\times k}$, $\mathbf{B}_2 \in \mathbb{Z}_p^{(5k+2)\times(2k+1)}$, $\mathbf{B}_3 \leftarrow \mathbb{Z}_p^{(5k+2)\times(2k+1)}$, with dual basis $\mathbf{B}_1^\parallel, \mathbf{B}_2^\parallel, \mathbf{B}_3^\parallel$; any $\widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}} \in \mathbb{Z}_p^{(2k+1)\times k}$ and $\mathbf{R}^\perp \in \mathbb{Z}_p^{k\times(2k+1)}$ such that $\mathbf{R}^\perp(\widehat{\mathbf{R}}_\ell \| \widetilde{\mathbf{R}}) = (\mathbf{0}\|\mathbf{I}_k)$. We recall the L.H.S of our argument is

$$\begin{aligned}\text{L.H.S} = [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \mathbf{c}\mathbf{W}_{1,\ell}^*, \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3,\\ \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_2),\\ [\mathbf{B}_1]_2, [\mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{W}_{1,\ell}^*]_1, \left\{[\mathbf{G}_{\ell,j}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

and the R.H.S of our argument is

$$\begin{aligned}\text{R.H.S} = [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \mathbf{c}\mathbf{W}_{1,\ell}^* + \boxed{\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp(\mathbf{B}_3^\parallel)^\top)}, \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3,\\ \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}) + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{w}}}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_2),\\ [\mathbf{B}_1]_2, [\mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\mathbf{G}_\ell, \mathbf{G}_\ell\mathbf{W}_{1,\ell}^*]_1, \left\{[\mathbf{G}_{\ell,j}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

We prove that L.H.S $\approx_c$ R.H.S as follows:

Step 1. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\mathbf{G}_\ell]_1) \approx_c ([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \mathbf{c}\mathbf{W}_{1,\ell}^*, \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3,\\ \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_2),\\ [\mathbf{B}_1]_2, [\mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\boxed{\widetilde{\mathbf{T}}\mathbf{A}}, \boxed{\widetilde{\mathbf{T}}\mathbf{A}}\mathbf{W}_{1,\ell}^*]_1, \left\{[\mathbf{G}_{\ell,j}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

Step 2. With MDDH assumption w.r.t on $[\mathbf{B}_1]_2$ which ensure that

$$([\mathbf{B}_1]_2, [\mathbf{G}_{\ell,j}]_2) \approx_c ([\mathbf{B}_1]_2, [\mathbf{B}_1\widetilde{\mathbf{T}}_j]_2) \quad \forall j \in [L]\setminus\{\ell\}$$

when $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(5k+2)\times k}$, $\widetilde{\mathbf{T}}_j \leftarrow \mathbb{Z}_p^{k\times(6k+2)}$ and $\mathbf{G}_{\ell,j} \leftarrow \mathbb{Z}_p^{(5k+2)\times(6k+2)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \mathbf{c}\mathbf{W}_{1,\ell}^*, \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3,\\ \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_2),\\ [\mathbf{B}_1]_2, [\mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\widetilde{\mathbf{T}}\mathbf{A}, \widetilde{\mathbf{T}}\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \left\{[\boxed{\mathbf{B}_1\widetilde{\mathbf{T}}_j}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \boxed{\mathbf{B}_1\widetilde{\mathbf{T}}_j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

Step 3. Use the change of variable

$$\mathbf{W}_{1,\ell}^* \mapsto \mathbf{W}_{1,\ell}^* + \mathbf{c}^\perp\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp(\mathbf{B}_3^\parallel)^\top)$$

where $\widetilde{\mathbf{w}} \leftarrow \mathbb{Z}_p^{1\times kn'}$. We have

$$\begin{aligned}\text{L.H.S} \approx_s [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \mathbf{c}\mathbf{W}_{1,\ell}^* + \boxed{\widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp(\mathbf{B}_3^\parallel)^\top)}, \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3,\\ \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}) + \boxed{\mathbf{c}^\perp\widetilde{\mathbf{w}}}, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_2),\\ [\mathbf{B}_1]_2, [\mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\widetilde{\mathbf{T}}\mathbf{A}, \widetilde{\mathbf{T}}\mathbf{A}\mathbf{W}_{1,\ell}^*]_1, \left\{[\mathbf{B}_1\widetilde{\mathbf{T}}_j, \mathbf{W}_{1,\ell}^*(\mathbf{I}_{n'} \otimes \mathbf{B}_1\widetilde{\mathbf{T}}_j)]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

Step 4. With MDDH assumption w.r.t on $[\mathbf{B}_1]_2$ which ensure that

$$([\mathbf{B}_1]_2, [\mathbf{B}_1\widetilde{\mathbf{T}}_j]_2) \approx_c ([\mathbf{B}_1]_2, [\mathbf{G}_{\ell,j}]_2) \quad \forall j \in [L]\setminus\{\ell\}$$

when $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(5k+2)\times k}$, $\widetilde{\mathbf{T}}_j \leftarrow \mathbb{Z}_p^{k\times(6k+2)}$ and $\mathbf{G}_{\ell,j} \leftarrow \mathbb{Z}_p^{(5k+2)\times(6k+2)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c\ & [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell} + \widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp(\mathbf{B}_3^{\parallel})^\top), \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3,\\ & \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}) + \mathbf{c}^\perp\widetilde{\mathbf{w}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_2),\\ & [\mathbf{B}_1]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\widetilde{\mathbf{T}}\mathbf{A}, \widetilde{\mathbf{T}}\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \left\{[\boxed{\mathbf{G}_{\ell,j}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \boxed{\mathbf{G}_{\ell,j}})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\end{aligned}$$

Step 5. With MDDH assumption w.r.t on $[\mathbf{A}]_1$ which ensured that

$$([\mathbf{A}]_1, [\widetilde{\mathbf{T}}\mathbf{A}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{G}_\ell]_1)$$

when $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$, $\widetilde{\mathbf{T}} \leftarrow \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{G}_\ell \leftarrow \mathbb{Z}_p^{(k+2)\times(k+1)}$. We have

$$\begin{aligned}\text{L.H.S} \approx_c\ & [\mathbf{A}]_1, \mathbf{c}, \mathbf{c}^\perp, [\mathbf{A}\mathbf{W}^*_{1,\ell}]_1, \mathbf{c}\mathbf{W}^*_{1,\ell} + \widetilde{\mathbf{w}}(\mathbf{I}_{n'} \otimes \mathbf{R}^\perp(\mathbf{B}_3^{\parallel})^\top), \widehat{\mathbf{R}}_\ell, \widetilde{\mathbf{R}}, \mathbf{B}_2, \mathbf{B}_3,\\ & \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widehat{\mathbf{R}}_\ell), \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_3\widetilde{\mathbf{R}}) + \mathbf{c}^\perp\widetilde{\mathbf{w}}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_2),\\ & [\mathbf{B}_1]_2, [\mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{B}_1)]_2, [\boxed{\mathbf{G}_\ell}, \boxed{\mathbf{G}_\ell}\mathbf{W}^*_{1,\ell}]_1, \left\{[\mathbf{G}_{\ell,j}, \mathbf{W}^*_{1,\ell}(\mathbf{I}_{n'} \otimes \mathbf{G}_{\ell,j})]_2\right\}_{\forall j\in[L]\setminus\{\ell\}}\\ =\ & \text{R.H.S}\end{aligned}$$

□

B Missing Lemmata

In this section, we provide the missing lemmata in the main body and provide their proof

Lemma 11. *For any adversary $\mathcal{A}$, there exist an algorithm $\mathcal{B}$ such that* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *and*

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

Proof. The $\mathcal{B}$ proceeds as follows:

(Setup) On input 1^L from $\mathcal{A}$, $\mathcal{B}$ sent it to its challenger and obtain crs, return crs to $\mathcal{A}$. And initialize $\mathcal{S} = \emptyset$.

(Repeated Aggregations) In repeated aggregations phase, $\mathcal{B}$ repeat following interaction with its challenger and $\mathcal{A}$:

- When $\mathcal{A}$ makes query $\mathsf{OGen}(i)$ or $\mathsf{OCor}(i, \mathsf{mpk})$, $\mathcal{B}$ forwards the same query to its challenger and returns the response to $\mathcal{A}$.
- Then on input the aggregation tuples $S = \{(\mathsf{mpk}_i, g_i)\}_{i\in[L]}$, $\mathcal{B}$ checks $\mathsf{Ver}(\mathsf{crs}, i, \mathsf{mpk}_i) \stackrel{?}{=} 1$ for all $i \in [L]$ and abort if not. If all checks pass, $\mathcal{B}$ appends $(\mathsf{mpk}_i, g_i)_{i\in[L]}$ to $\mathcal{S}$ and return $(\mathsf{mpk}_+, (\mathsf{hsk}_j)_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, (\mathsf{mpk}_i, g_i)_{i\in[L]})$.
- Then, when $\mathcal{A}$ makes query $\mathsf{OKey}(i, f)$, $\mathcal{B}$ fetches mpk_i from S and gets $\mathsf{msk}_i \leftarrow \mathsf{OCor}(i, \mathsf{mpk}_i)$ from its challenger. And $\mathcal{B}$ output $\mathsf{sk}_{i,f} = \mathsf{Key}(\mathsf{msk}_i, \mathsf{hsk}_i, f)$.

(Challenge Aggregation) In the challenge aggregation phase, $\mathcal{B}$ interact with its challenger and $\mathcal{A}$ as follows:

- When $\mathcal{A}$ makes query $\mathsf{OGen}(i)$ or $\mathsf{OCor}(i, \mathsf{mpk})$, $\mathcal{B}$ forwards the same query to its challenger and returns the response to $\mathcal{A}$.
- On input the challenge aggregation tuples $S^* = \{(\mathsf{mpk}^*_i, g^*_i)\}_{i\in[L]}$, $\mathcal{B}$ checks $(\mathsf{mpk}^*_i, g^*_i) \stackrel{?}{\in} \mathcal{S}$ for all $i \in [L]$, abort if not. And if all checks pass, $\mathcal{B}$ submit the challenge aggregation tuples $S^* = \{(\mathsf{mpk}^*_i, g^*_i)\}_{i\in[L]}$ to its challenger and returns the response $(\mathsf{mpk}^*_+, (\mathsf{hsk}^*_j)_{j\in[L]})$ to $\mathcal{A}$.
- Then, when $\mathcal{A}$ makes query $\mathsf{OKey}(i, f)$, $\mathcal{B}$ forwards the same query to its challenger and returns the response to $\mathcal{A}$.

(Challenge) On input (x_0^*, x_1^*) from $\mathcal{A}$, $\mathcal{B}$ submit the same challenge to its challenger, and return the response ct^* to $\mathcal{A}$.

(Post Challenge Query) When $\mathcal{A}$ makes query $\mathsf{OKey}(i, f)$, $\mathcal{B}$ forwards the same query to its challenger and returns the response to $\mathcal{A}$.

(Output) At the end, on input $b' \in \{0,1\}$ from $\mathcal{A}$, $\mathcal{B}$ outputs b'.

Observe that $\mathcal{B}$ is a slotted delegated Reg-FE adversary that without repeated aggregations and simulates the challenger of $\mathcal{A}$. Since we require $S^* \cap \mathcal{S} = \emptyset$, the OCor queries in the third part of the repeated aggregation phase will not affect the admissibility of $\mathcal{B}$.

Lemma 12. *($\mathsf{G}_{k^*} \approx_c \mathsf{G}_{k^*-1}, \forall k^* \in [m]$). For any adversary $\mathcal{A}$, there exist algorithm $\mathcal{B}$ such that* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *and*

$$|\mathsf{Adv}^{k^*}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{k^*-1}_{\mathcal{A}}| \leq \mathsf{Adv}^{\textit{Ad-sDel-Reg-FE-ReAgg}}_{\mathcal{B}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. This follows from the adaptive IND-security of the k^*-th slotted delegated Reg-FE instance which allow repeated aggregations, on input $L = 2^m$, the algorithm $\mathcal{B}$ works as follow:

(Setup) In setup phase, $\mathcal{B}$ works as follows:

- $\mathcal{B}$ sends 2^{k^*} to its challenger and obtains crs_{k^*}.
- For $\mathsf{aux} = (\mathsf{ctr}_{\mathsf{aux}}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathsf{mpk}_+)$, $\mathcal{B}$ initially sets $\mathsf{ctr} = 0$, $\mathcal{D}_1[k,j] = \perp$, $\mathcal{D}_3[k,j] = \perp$ for all $k \in [0,m]$ and $j \in [2^k]$, $\mathcal{D}_2[k,i] = \perp$ for all $k \in [0,m]$ and $j \in [2^m]$ and $\mathsf{mpk}_+ = (0, \perp, \ldots, \perp)$. And $\mathcal{B}$ initially sets $\mathcal{H} = \emptyset$, $C = \emptyset$ and $\mathcal{D}[\mathsf{mpk}] = \emptyset$ for all possible mpk. In addition, $\mathcal{B}$ initially sets $\mathcal{K} = \emptyset$ to record y' queried to OCorK along with corresponding y, and initially sets three lists with 2^{k^*}-length: $S^{\mathrm{old}} = (\perp, \ldots, \perp)$, $S^{\mathrm{cur}} = (\perp, \ldots, \perp)$, $S^{\mathrm{new}} = (\perp, \ldots, \perp)$ to track the aggregated tuple for k^*-th slotted instance.
- For all $k \in [0,m] \setminus \{k^*\}$, runs $\mathsf{crs}_k \leftarrow \mathsf{sSetup}(1^\lambda, 1^{2^k}, F, G)$.

Returns $\mathsf{crs} = (\mathsf{crs}_0, \ldots, \mathsf{crs}_{k^*}, \ldots, \mathsf{crs}_m)$ to $\mathcal{A}$.

(Pre-challenge Query) For pre-challenge queries, $\mathcal{B}$ works as follows:

- ORegCC: On input (mpk, g), runs $(\mathsf{mpk}'_+, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}, g)$ returns $(\mathsf{mpk}'_+, \mathsf{aux}')$ to $\mathcal{A}$ and updates internal data $\mathsf{mpk}_+ \leftarrow \mathsf{mpk}'_+$, $\mathsf{aux} \leftarrow \mathsf{aux}'$, $\mathcal{D}[\mathsf{mpk}] = \mathcal{D}[\mathsf{mpk}] \cup \{g\}$ and appends mpk to C. Moreover, when $\mathsf{aux}' \neq \mathsf{aux}$, fetches mpk_{k^*} and ctr from mpk and updates $S^{\mathrm{new}}[(\mathsf{ctr} \bmod 2^{k^*}) + 1] \leftarrow (\mathsf{mpk}_{k^*}, g)$; and when $\mathsf{ctr} + 1 = 0 \bmod 2^{k^*}$, updates $S^{\mathrm{cur}} \leftarrow S^{\mathrm{new}}$.
- ORegHC: On input y, $\mathcal{B}$ proceeds as
  - Sets $\mathsf{ctr} = \mathsf{ctr}_{\mathsf{aux}}$, runs $(\mathsf{mpk}_k, \mathsf{msk}_k) \leftarrow \mathsf{sGen}(\mathsf{crs}_k, (\mathsf{ctr} \bmod 2^k) + 1)$ for all $k \in [0,m] \setminus \{k^*\}$.
  - Makes $\mathsf{OGen}((\mathsf{ctr}_{\mathsf{aux}} \bmod 2^{k^*}) + 1)$ query to its challenger and obtains mpk_{k^*}

  Sets $\mathsf{msk}_{k^*} = \perp$ and append $(\mathsf{mpk}, \mathsf{msk})$ to $\mathcal{H}$, where $\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_0, \ldots, \mathsf{mpk}_{k^*}, \ldots, \mathsf{mpk}_m)$ and $\mathsf{msk} = (\mathsf{ctr}, \mathsf{msk}_0, \ldots, \mathsf{msk}_{k^*}, \ldots, \mathsf{msk}_m)$. Runs $(\mathsf{mpk}'_+, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk}, g)$. Returns $(|\mathcal{H}|, \mathsf{mpk}'_+, \mathsf{aux}', \mathsf{mpk})$ to $\mathcal{A}$ and updates internal data $\mathsf{mpk}_+ \leftarrow \mathsf{mpk}'_+$, $\mathsf{aux} \leftarrow \mathsf{aux}'$ and $\mathcal{D}[\mathsf{mpk}] = \mathcal{D}[\mathsf{mpk}] \cup \{y\}$. Moreover, updates $S^{\mathrm{new}}[(\mathsf{ctr} \bmod 2^{k^*}) + 1] \leftarrow (\mathsf{mpk}_{k^*}, y)$; and if $\mathsf{ctr} + 1 = 0 \bmod 2^{k^*}$, updates $S^{\mathrm{cur}} \leftarrow S^{\mathrm{new}}$.
- OCorHC: On input i, abort if $\mathcal{H}[i] = \perp$; else looks up $\mathcal{H}[i] = (\mathsf{mpk}, \mathsf{msk})$ where $\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_0, \ldots, \mathsf{mpk}_{k^*}, \ldots, \mathsf{mpk}_m)$ and $\mathsf{msk} = (\mathsf{ctr}, \mathsf{msk}_0, \ldots, \mathsf{msk}_{k^*}, \ldots, \mathsf{msk}_m)$.
  - When $\mathsf{msk}_{k^*} \neq \perp$, returns msk to $\mathcal{A}$.
  - When $\mathsf{msk}_{k^*} = \perp$, makes $\mathsf{OCor}((\mathsf{ctr} \bmod 2^{k^*}) + 1, \mathsf{mpk}_{k^*})$ query to its challenger and obtains msk'_{k^*} and updates $\mathsf{msk} = (\mathsf{ctr}, \mathsf{msk}_0, \ldots, \mathsf{msk}'_{k^*}, \ldots, \mathsf{msk}_m)$. Returns msk to $\mathcal{A}$ and updates $\mathcal{H}[i] = (\mathsf{mpk}, \mathsf{msk})$.
- OCorK: On input (i, f), abort if $\mathcal{H}[i] = \perp$; else $\mathcal{B}$ appends (i, f) to $\mathcal{K}$ and looks up $\mathcal{H}[i] = (\mathsf{mpk}, \mathsf{msk})$ where $\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_0, \ldots, \mathsf{mpk}_{k^*}, \ldots, \mathsf{mpk}_m)$ and $\mathsf{msk} = (\mathsf{ctr}, \mathsf{msk}_0, \ldots, \mathsf{msk}_{k^*}, \ldots, \mathsf{msk}_m)$. Runs $\mathsf{hsk} \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk})$ and proceeds as

- For all $k \in [0, m] \setminus \{k^*\}$, compute

$$\mathsf{sk}_{k,f} = \begin{cases} \perp & \text{if } \mathsf{hsk}_k = \perp \vee \mathcal{D}_3[k, (\mathsf{ctr} \bmod 2^k) + 1] \neq \mathsf{ctr} \\ \mathsf{sKey}(\mathsf{msk}_k, \mathsf{hsk}_k, f) & \text{otherwise} \end{cases}$$

- For k^*, $\mathcal{B}$ proceeds as:
  * If $\mathsf{hsk}_{k^*} = \perp \vee \mathcal{D}_3[k^*, (\mathsf{ctr} \bmod 2^{k^*}) + 1] \neq \mathsf{ctr}$, set $\mathsf{sk}_{k^*,f} = \perp$.
  * Else if $S^{\mathrm{cur}} \neq S^{\mathrm{old}}$, submits S^{cur} to its challenger for aggregating and updates $S^{\mathrm{old}} \leftarrow S^{\mathrm{cur}}$. Then makes $\mathsf{OKey}((\mathsf{ctr} \bmod 2^{k^*}) + 1, f)$ query to its challenger and obtain $\mathsf{sk}_{k^*,f}$.
  * Else if $S^{\mathrm{cur}} = S^{\mathrm{old}}$, makes $\mathsf{OKey}((\mathsf{ctr} \bmod 2^{k^*}) + 1, f)$ query to its challenger and obtain $\mathsf{sk}_{k^*,f}$.

Returns $\mathsf{sk}_f = (\mathsf{ctr}, \mathsf{sk}_{0,f}, \ldots, \mathsf{sk}_{k^*,f}, \ldots, \mathsf{sk}_{m,y'})$ to $\mathcal{A}$.

(Challenge) On input (x_0^*, x_1^*), $\mathcal{B}$ does the following checks:

- For all $g \in \bigcup_{\mathsf{mpk} \in C} \mathcal{D}[\mathsf{mpk}]$, checks $g(x_0^*) \stackrel{?}{=} g(x_1^*)$, abort if not.
- For all $(i, f) \in \mathcal{K}$, looks up $(\mathsf{mpk}, \star) = \mathcal{H}[i]$, for all $g \in \mathcal{D}[\mathsf{mpk}]$, checks $f \circ g(x_0^*) \stackrel{?}{=} f \circ g(x_1^*)$, abort if not.

Then, $\mathcal{B}$ parse current $\mathsf{mpk}_+ = (\mathsf{ctr}_{\mathsf{aux}}, \mathsf{mpk}_{+,0}, \ldots, \mathsf{mpk}_{+,m})$ and works as follows for all $k \in [0, m] \setminus \{k^*\}$:

- If $\mathsf{mpk}_{+,k} = \perp$, set $\mathsf{ct}_k^* = \perp$.
- Else if $\mathsf{mpk}_{+,k} \neq \perp \wedge k < k^*$, compute $\mathsf{ct}_k^* \leftarrow \mathsf{sEnc}(\mathsf{mpk}_{+,k}, x_1^*)$.
- Else if $\mathsf{mpk}_{+,k} \neq \perp \wedge k > k^*$, compute $\mathsf{ct}_k^* \leftarrow \mathsf{sEnc}(\mathsf{mpk}_{+,k}, x_0^*)$.

And for k^*, $\mathcal{B}$ works as follows:

- If $\mathsf{mpk}_{+,k^*} = \perp$, set $\mathsf{ct}_{k^*}^* = \perp$.
- Else if $\mathsf{mpk}_{+,k^*} \neq \perp \wedge S^{\mathrm{old}} = (\perp, \ldots, \perp)$, using S^{cur} as the final challenge aggregation tuples set; then issue challenge (x_0^*, x_1^*) to its challenger and obtain $\mathsf{ct}_{k^*}^*$.
- Else if $\mathsf{mpk}_{+,k^*} \neq \perp \wedge S^{\mathrm{old}} \neq (\perp, \ldots, \perp)$, issue challenge (x_0^*, x_1^*) to its challenger and obtains $\mathsf{ct}_{k^*}^*$.

Returns $\mathsf{ct}^* = (\mathsf{ctr}_{\mathsf{aux}}, \mathsf{ct}_0^*, \ldots, \mathsf{ct}_{k^*}^*, \ldots, \mathsf{ct}_m^*)$ to $\mathcal{A}$.

(Post-challenge Query) For post-challenge queries, $\mathcal{B}$ works as follows:

- OCorK: On input (i, f), $\mathcal{B}$ looks up $\mathcal{H}[i] = (\mathsf{mpk}, \mathsf{msk})$ and checks

$$f \circ g(x_0^*) \stackrel{?}{=} f \circ g(x_1^*) \quad \forall g \in \mathcal{D}[\mathsf{mpk}].$$

  Abort if not. Then, parse $\mathsf{mpk} = (\mathsf{ctr}, \mathsf{mpk}_0, \ldots, \mathsf{mpk}_{k^*}, \ldots, \mathsf{mpk}_m)$ and $\mathsf{msk} = (\mathsf{ctr}, \mathsf{msk}_0, \ldots, \mathsf{msk}_{k^*}, \ldots, \mathsf{msk}_m)$. Runs $\mathsf{hsk} \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{mpk})$ and proceeds as

  - For all $k \in [0, m] \setminus \{k^*\}$, compute

$$\mathsf{sk}_{k,f} = \begin{cases} \perp & \text{if } \mathsf{hsk}_k = \perp \vee \mathcal{D}_3[k, (\mathsf{ctr} \bmod 2^k) + 1] \neq \mathsf{ctr} \\ \mathsf{sKey}(\mathsf{msk}_k, \mathsf{hsk}_k, f) & \text{otherwise} \end{cases}$$

  - For k^*, $\mathcal{B}$ set:

$$\mathsf{sk}_{k^*,f} = \begin{cases} \perp & \text{if } \mathsf{hsk}_{k^*} = \perp \vee \mathcal{D}_3[k^*, (\mathsf{ctr} \bmod 2^{k^*}) + 1] \neq \mathsf{ctr} \\ \mathsf{OKey}((\mathsf{ctr} \bmod 2^{k^*}) + 1, f) & \text{otherwise} \end{cases}$$

  Returns $\mathsf{sk}_f = (\mathsf{ctr}, \mathsf{sk}_{0,f}, \ldots, \mathsf{sk}_{k^*,f}, \ldots, \mathsf{sk}_{m,f})$ to $\mathcal{A}$.

(Output) On input $b' \in \{0, 1\}$, $\mathcal{B}$ outputs b' to its challenger.

□

Table of Contents

When KGC Meets Curator: New Paradigm of Registered ABE and FE . . . 1
Ziqi Zhu, Jun Zhao, Kai Zhang, Junqing Gong✉, and Haifeng Qian✉
1 Introduction . . . 2
1.1 Results . . . 3
1.2 Discussions . . . 6
2 Technical Overview . . . 7
2.1 One-slot & One-key Scheme . . . 9
2.2 To L-slot & One-key Scheme. . . . 9
2.3 To L-slot & Many-key Scheme . . . 10
2.4 Final Delegated Reg-ABE Scheme . . . 13
2.5 Generic Scheme . . . 15
2.6 More Slotted Concrete Schemes . . . 16
3 Preliminaries . . . 17
3.1 Prime-Order Bilinear Groups . . . 18
3.2 Predicate Encodings . . . 19
3.3 Quasi-Adaptive Non-Interactive Zero-Knowledge Argument . . . 19
3.4 Slotted Registered Functional Encryption . . . 20
3.5 Functional Encryption . . . 21
3.6 Secret-Key Encryption with Pseudorandom Ciphertext . . . 22
3.7 Puncturable Pseudorandom Function . . . 22
4 Delegated Registered Functional Encryption . . . 23
4.1 Definition of Delegated Reg-FE . . . 23
4.2 Definition of Slotted Delegated Reg-FE . . . 25
5 Slotted Delegated Reg-ABE from Pairings . . . 27
5.1 Scheme . . . 27
5.2 Proof . . . 32
5.3 From $\mathsf{G}_{5,\ell-1,1}$ to $\mathsf{G}_{5,\ell-1,2}$: If $P(x^*, y^*_\ell) = 0$ . . . 36
5.4 From $\mathsf{G}_{5,\ell-1,1}$ to $\mathsf{G}_{5,\ell-1,2}$: If $P(x^*, y^*_\ell) = 1$ . . . 37
6 Slotted Delegated Reg-IPFE from Pairings . . . 43
6.1 Scheme . . . 43
6.2 Proof . . . 47
6.3 From $\mathsf{G}_{7,\ell-1,1}$ to $\mathsf{G}_{7,\ell-1,2}$ . . . 51
7 Slotted Reg-ABE with Delegated IPFE from Pairings . . . 53
7.1 Scheme . . . 53
7.2 Proof . . . 57
7.3 From $\mathsf{G}_{7,\ell-1,1}$ to $\mathsf{G}_{7,\ell-1,2}$ . . . 62
8 Slotted Reg-IPFE with Delegated ABE from Pairings . . . 64
8.1 Scheme . . . 64
8.2 Proof . . . 69
8.3 From $\mathsf{G}_{7,\ell-1,1}$ to $\mathsf{G}_{7,\ell-1,2}$: If $\mathbf{x}^*_0(\mathbf{y}^*_\ell)^\top = \mathbf{x}^*_1(\mathbf{y}^*_\ell)^\top$ . . . 74

8.4 From $\mathsf{G}_{7,\ell-1,1}$ to $\mathsf{G}_{7,\ell-1,2}$: If $\mathbf{x}_0^*(\mathbf{y}_\ell^*)^\top \neq \mathbf{x}_1^*(\mathbf{y}_\ell^*)^\top$ 75
9 Slotted Delegated Reg-FE for Arbitrary Functionalities 81
9.1 Construction 81
9.2 Proof of Security 83
10 From Slotted Delegated Reg-FE to Delegated Reg-FE 86
A Missing Proof 93
A.1 Proof of Lemma 2 93
A.2 Proof of Lemma 3 94
A.3 Proof of Lemma 5 95
A.4 Proof of Lemma 9 96
A.5 Proof of Lemma 9 97
B Missing Lemmata 98