A Modular Approach to Registered ABE for Unbounded Predicates

Nuttapong Attrapadung[1] and Junichi Tomida[2]

[1] National Institute of Advanced Industrial Science and Technology (AIST),
Tokyo, Japan. n.attrapadung@aist.go.jp
[2] NTT Social Informatics Laboratories, Tokyo, Japan. tomida.junichi@gmail.com

Abstract. Registered attribute-based encryption (Reg-ABE), introduced by Hohenberger *et al.* (Eurocrypt'23), emerges as a pivotal extension of attribute-based encryption (ABE), aimed at mitigating the key-escrow problem. Although several Reg-ABE schemes with black-box use of cryptography have been proposed so far, there remains a significant gap in the class of achievable predicates between vanilla ABE and Reg-ABE. To narrow this gap, we propose a modular framework for constructing Reg-ABE schemes for a broader class of predicates. Our framework is a Reg-ABE analog of the predicate transformation framework for ABE introduced by Attrapadung (Eurocrypt'19) and later refined by Attrapadung and Tomida (Asiacrypt'20) to function under the standard MDDH assumption. As immediate applications, our framework implies the following new Reg-ABE schemes under the standard MDDH assumption:

- the first Reg-ABE scheme for (non-)monotone span programs with the traditional completely unbounded property.
- the first Reg-ABE scheme for general non-monotone span programs (also with the completely unbounded property) as defined in the case of vanilla ABE by Attrapadung and Tomida (Asiacrypt'20).

Here, the term "completely unbounded" signifies the absence of restrictions on attribute sets for users and policies associated with ciphertexts.

From a technical standpoint, we first substantially modify pair encoding schemes (PES), originally devised for vanilla ABE by Attrapadung (Eurocrypt'14), to make them compatible with Reg-ABE. Subsequently, we present a series of predicate transformations through which we can construct complex predicates, particularly those with an "unbounded" characteristic, starting from simple ones. Finally, we define new properties of PES necessary for constructing Reg-ABE schemes and prove that these properties are preserved through the transformations. This immediately implies that we can obtain Reg-ABE schemes for any predicates derived via predicate transformations.

Keywords: attribute-based encryption, registered attribute-based encryption, registration-based encryption, pair encodings

Table of Contents

1 Introduction

Registered Attribute-base Encryption. Attribute-based encryption (ABE) [GPSW06] stands as a versatile cryptographic primitive enabling fine-grained access control over encrypted data. Registered attribute-based encryption (Reg-ABE) has recently emerged as a pivotal extension of ABE, designed to tackle the notorious key-escrow problem [HLWW23]. More precisely, in traditional ABE systems, a trusted authority needs to maintain a long-term master secret key (msk) to generate secret decryption keys as long as the system is in operation. However, the possession of msk grants adversaries the ability to decrypt all ciphertexts within the system, thereby rendering the authority a single point of failure.

In contrast, Reg-ABE presents a novel paradigm by introducing the “key curator” concept instead of relying on a trusted authority. Each user within a Reg-ABE system generates a pair of public and secret keys and registers the public key, along with its associated attribute y, with the key curator. The key curator then aggregates these pairs into a compact master public key (mpk) in a *completely verifiable and transparent* manner. In a Reg-ABE system, a user encrypts a message with respect to a policy x using mpk to generate a ciphertext. Decryption of the ciphertext is possible only for users possessing the attribute y satisfying the policy x with their secret key. More generally, decryption is feasible if and only if the predicate $\mathsf{P}(x, y) = 1$ holds for some predicate P.

The study of Reg-ABE began with registration-based encryption (RBE) [GHMR18], which can be conceptualized as Reg-ABE for the equality predicate $\mathsf{P}(x, y) = 1 \Leftrightarrow x = y$, to address the key escrow problem of identity-based encryption [BF01]. The first RBE scheme [GHMR18] uses indistinguishability obfuscation (iO) [GGH$^+$13][3], and lately RBE schemes relying on standard assumptions were proposed [GHM$^+$19, GV20, CES21]. However, these schemes heavily rely on non-black-box use of cryptographic primitives, making them impractical (ciphertext size estimated at 4.5 terabytes for 2 billion users [CES21]). The non-black-box approach is also used for constructing Reg-ABE and more generalized registered functional encryption [FWW23, FFM$^+$23, DPY23].

Reg-ABE via Black-box Approach. Motivated by the inefficiency of non-black-box constructions, several Reg-ABE (including RBE) schemes with only black-box use of cryptography have recently been proposed in succession [HLWW23, DKL$^+$23, GKMR23, FFM$^+$23, FKdP23, ZZGQ23]. These schemes exhibit concrete efficiency, with some even rivaling vanilla ABE schemes for the same predicate. Among them, the most general scheme is that proposed by Zhu *et al.* [ZZGQ23], where the term “general” refers to its capability to handle any predicates P that have predicate encodings [Wee14], and the predicates supported by the other schemes can be captured by predicate encodings (predicate encodings will be explained later in the technical overview).

Predicate Encodings vs. Pair Encodings. One of the main focuses in ABE research is exploring which class of predicates can be achieved under certain assumptions. While predicate encodings offer a versatile framework capable of capturing various predicates, there exist ABE constructions beyond its scope, such as unbounded ABE [LW11], non-monotone ABE with large universes [OSW07], ABE supporting multi-use of attributes [KW19], and ABE for DFA [Wat12]. On the other hand, pair encodings [Att14] present a more general framework, encompassing most pairing-based ABE schemes, including the aforementioned examples [AC17, Att19, AT20]. A natural question arises: can pair encodings be applied to Reg-ABE, potentially broadening the class of Reg-ABE schemes? Zhu et al. [ZZGQ23] explicitly stated that their scheme cannot operate with pair encodings, leaving this unresolved.

1.1 Our Results

In this work, we take a significant stride towards addressing the challenge of applying pair encodings to Reg-ABE. Our main contributions are three-fold:

- **New Notion of Pair Encoding Schemes:** Pair encoding schemes (PES) designed for vanilla ABE are incompatible with Reg-ABE (we will discuss this later in the technical overview). To overcome this obstacle, we carefully devise a new notion of PES tailored for Reg-ABE compatibility.

[3] They also constructed a “weakly-efficient” RBE scheme from standard assumptions.

Table 1. Comparison among Reg-ABE schemes for *span program predicates*.

Schemes	Achievable properties for span program predicates					Properties of constructions				
	Comprising completely unbounded property									
	Large universe	Unbounded attributes	Unbounded policy sizes	Multi-use	Non-monotonicity	KP/CP	Unbounded users	Prime-order	Assumption	W/O Non-BB
HLWW [HLWW23, §5] (Pairing-based)	–	–	–	–	–	CP	–	–	GS	✓
HLWW [HLWW23, §7]† (iO-based)	✓	–	✓	✓	✓✓	CP	✓	n/a	iO,SSB,PRG	–
FWW [FWW23]†	✓	–	–	–	✓✓	CP	✓	n/a	WE,FBH,PKE	–
ZZGQ [ZZGQ23, §D1]	–	–	–	–	–	KP, CP	–	✓	MDDH	✓
Ours 1	✓	✓	✓	✓	–	CP	–	✓	MDDH	✓
Ours 2	✓	✓	✓	✓	✓	CP	–	✓	MDDH	✓
Ours 3	✓	✓	✓	✓	✓✓	CP	–	✓	MDDH	✓

Note: Large universe ABE involves attribute universes of super-polynomial size; unbounded attributes imply no prior limit on attributes per user; unbounded policy sizes mean policy sizes (span program matrix sizes) are not bounded in advance; multi-use allows attributes to be used arbitrarily many times in a policy; KP and CP denote key-policy and ciphertext-policy, respectively. Unbounded users mean the setup running time (and the size of common reference string output from the setup) is at most polylogarithmic in the maximum number of users. Prime-order refers to constructions in pairing groups with prime order. GS stands for generalized subgroup assumption. iO is for indistinguishability obfuscation; SSB is for somewhere statistically binding hash function; PRG is for pseudorandom generator; WE is for witness encryption; FBH is for function-bindng hash function; PKE is for public-key encryption. W/O Non-BB means: without relying on non-black-box use of cryptographic primitives. ✓✓ (for non-monotonicity) denotes *general non-monotone span programs* (referred to as OSWOT-type in [AT20]). †: The iO-based scheme of [HLWW23] and the WE-based scheme of [FWW23] support circuit predicates; we envision instantiating a circuit to implement a span program and write the properties that are possibly achieved by their resulting schemes for span programs here to ensure a direct comparison; see a discussion in §7.2.

- **Framework:** We propose a framework that enables us to construct Reg-ABE schemes in a modular manner. Our framework serves as a Reg-ABE counterpart to the predicate transformation framework introduced by Attrapadung [Att19] for vanilla ABE, refined further by Attrapadung and Tomida [AT20], enabling the handling of PES (including predicate encodings) for Reg-ABE. The resulting Reg-ABE is secure under the standard MDDH assumption. Our framework does not rely on non-black box use of cryptography.
- **Concrete Instantiations:** As a usage example of our framework, we present three new instantiations of Reg-ABE that are not known prior to our work:
  1. the first completely unbounded Reg-ABE for monotone span programs;
  2. the first completely unbounded Reg-ABE for non-monotone span programs, as defined by [OSW07] for vanilla ABE;
  3. the first completely unbounded Reg-ABE for general non-monotone span programs that unify the two types of existing non-monotonicity by [OSW07] and [OT10] (see [AT20, §6.5] for the motivation of this predicate).

  We employ the term "completely unbounded Reg-ABE" to signify satisfaction of large universe, unbounded attribute and policy size, and multi-use criteria. We compare our Reg-ABE instantiations for span program predicates to prior works qualitatively in Table 1 and quantitatively in Table 3 in §7.2. Notably, none of these properties were previously realized within the context of *pairing-based* Reg-ABE. However, if one allows iO or witness encryption (WE) with non-black-box usages of cryptographic primitives, the Reg-ABE schemes in [HLWW23, FWW23] already achieve some of these properties, notably including the large-universe property, as shown in Table 1. We also note that the iO/WE based schemes of [HLWW23, FWW23] supports circuit predicates; we adapt them to span programs to ensure a direct comparison of equivalent functionalities here. Definitions of predicates and comparisons to prior works are provided in §7.

Similar to prior pairing-based Reg-ABE schemes [HLWW23, FFM+23, ZZGQ23], our system requires a structured common reference string crs. Its generation necessitates a trusted party or multi-party computation at the system's inception. It is essential to note that once crs is published, no trusted party is required. Additionally, as with prior pairing-based schemes [HLWW23, FFM+23, ZZGQ23], we need to fix a bound L on the number of registered users in the system beforehand, with the size of crs quadratic in L (ignoring a polylogarithmic factor). Therefore, all these pairing-based schemes and ours are *bounded-user* schemes. Contrastingly, the iO/WE-based Reg-ABE schemes of [HLWW23,FWW23] obtain the size of crs being polylogarithmic in L, and hence are *unbounded-user* schemes. We also note these latter two schemes can rely on random crs. On a flip side, the WE-based scheme of [FWW23] is only selectively secure, while all the rest including ours are adaptively secure.

1.2 Technical Overview

Slotted Registered ABE. Hohenberger *et al.* proposed a primitive called slotted registered ABE and showed that full-fledged Reg-ABE can be generically constructed from slotted registered ABE [HLWW23]. Notably, as described in [HLWW23], the conversion preserves the (un)bounded-user property: if the slotted registered ABE is a bounded-user scheme, so is the resulting Reg-ABE. We focus on constructing pairing-based Reg-ABE, for which only bounded-user schemes are currently known. Leveraging the conversion of [HLWW23], our focus shifts to constructing bounded-user slotted registered ABE. Throughout the paper, unless specified otherwise, *we use sReg-ABE to refer to bounded-user slotted registered ABE.*

sReg-ABE and Predicate Encodings. Our starting point is the ZZGQ framework [ZZGQ23], which allows us to construct sReg-ABE schemes from predicate encodings [Wee14]. We briefly recall sReg-ABE and predicate encodings. The sReg-ABE system is started by generating and publishing common reference string crs. Each user generates a pair of its public and secret keys $(\mathsf{pk}, \mathsf{sk})$ from crs. In sReg-ABE for a predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$, the number L of users who can join the system is fixed in advance[4], and all users join the system all at once by registering their pk and key attribute $y \in \mathcal{Y}$. Then, the system generates a *compact* master public key mpk and helper secret keys hsk_i for user i, *i.e.,* $|\mathsf{mpk}|$ and $|\mathsf{hsk}_i|$ are $O(\log L)$, in a deterministic manner. An encryptor takes mpk, a ciphertext attribute $x \in \mathcal{X}$, and a message M to generate ciphertext ct_x. Finally, ct_x can be decrypted with sk_i and hsk_i for user i if and only if $\mathsf{P}(x, y_i) = 1$.

Predicate encodings for $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ is a set of matrices depending on key and ciphertext attributes $(x, y) \in \mathcal{X} \times \mathcal{Y}$, which was originally used for abstracting structure of the ABE scheme for P. Specifically, (ω, n_c, n_k)-predicate encodings for P uniquely specify matrices

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

for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$, which satisfies *decoding* correctness, *i.e.,* $\mathbf{M}_{x,y}\mathbf{d}_{x,y}^\top = (1, \mathbf{0})^\top$ if $\mathsf{P}(x, y) = 1$ and security, *i.e.,* the columns of $\mathbf{M}_{x,y}$ do not span $(1, \mathbf{0})^\top$ if $\mathsf{P}(x, y) = 0$ (the above formulation of predicate encodings follows [ZZGQ23]). For instance, predicate encodings P for identity-based encryption (IBE), *i.e.,* $\mathsf{P}(x, y) = 1 \Leftrightarrow x = y$, are given as $\mathbf{C}_x = (x, 1)^\top, \mathbf{K}_y = (y, 1)^\top, \mathbf{a}_y = 1, \mathbf{d}_{x,y} = (1, -1)$.

sReg-ABE from Predicate Encodings. Next, we recall the simplified ZZGQ sReg-ABE scheme from predicate encodings [ZZGQ23]. Let $e : G_1 \times G_2 \to G_\mathsf{T}$ be bilinear groups, and $[\cdot]_i$ denotes element-wise exponentiation to $g_i \in G_i$. Their scheme is described as follows:

$$\begin{aligned}
\mathsf{crs} &= ([\alpha]_\mathsf{T},\ \{[w_{j,0}, \mathbf{w}_j]_1\}_{j \in [L]},\ \{[r_i, r_i w_{j,0}, r_i \mathbf{w}_j, r_i w_{i,0} + \alpha]_2\}_{i,j \in [L], i \neq j}) \\
\mathsf{pk}_i &= ([v_i]_1, \{[v_i r_j]_2\}_{j \neq i}), \quad \mathsf{sk}_i = v_i \\
\mathsf{mpk} &= ([\textstyle\sum_{j \in [L]}((w_{j,0} + v_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j}), \sum_j \mathbf{w}_j]_1,\ [\alpha]_\mathsf{T}) \\
\mathsf{hsk}_i &= [r_i, \underbrace{r_i \textstyle\sum_{j \neq i}((w_{j,0} + v_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})}_{\mathbf{h}_1}, \underbrace{r_i \textstyle\sum_{j \neq i} \mathbf{w}_j}_{\mathbf{h}_2}, \underbrace{r_i w_{i,0} + \alpha}_{h_3}]_2 \qquad (1) \\
\mathsf{ct}_x &= ([s, \underbrace{s \textstyle\sum_j ((w_{j,0} + v_j)\mathbf{a}_{y_j} + \mathbf{w}_j \mathbf{K}_{y_j})}_{\mathbf{c}_1}, \underbrace{s \textstyle\sum_j \mathbf{w}_j \mathbf{C}_x}_{\mathbf{c}_2}]_1, [s\alpha]_\mathsf{T} M)
\end{aligned}$$

[4] A scheme is called unbounded-user if it achieves the generation time and size of crs as polylogarithmic in L [HLWW23]. Our schemes, however, resort to bounded-user schemes.

where $\alpha, w_{i,0}, r_i, v_i, s \leftarrow \mathbb{Z}_p, \mathbf{w}_j \leftarrow \mathbb{Z}_p^{\omega}$, and the system aggregates $(\mathsf{pk}_1, y_1), \ldots, (\mathsf{pk}_L, y_L)$ into mpk. In decryption for user i with attribute $y = y_i$, we compute

$$\begin{aligned}
&[(r_i\mathbf{c}_1 - s\mathbf{h}_1 \,||\, r_i\mathbf{c}_2 - s\mathbf{h}_2\mathbf{C}_x)\mathbf{d}_{x,y}^{\top} - sh_3 - sr_iv_i]_{\mathsf{T}} \cdot [s\alpha]_{\mathsf{T}}M \\
=&[sr_i((w_{i,0}+v_i)\mathbf{a}_{y_i} + \mathbf{w}_i\mathbf{K}_{y_i} \,||\, \mathbf{w}_i\mathbf{C}_x)\mathbf{d}_{x,y}^{\top} - sr_i(w_{i,0}+v_i) - s\alpha]_{\mathsf{T}} \cdot [s\alpha]_{\mathsf{T}}M \\
=&\left[sr_i(w_{i,0}+v_i \,||\, \mathbf{w}_i)\begin{pmatrix} \mathbf{a}_{y_i} & \mathbf{0} \\ \mathbf{K}_{y_i} & \mathbf{C}_x \end{pmatrix}\mathbf{d}_{x,y}^{\top} - sr_i(w_{i,0}+v_i) - s\alpha\right]_{\mathsf{T}} \cdot [s\alpha]_{\mathsf{T}}M = M,
\end{aligned} \tag{2}$$

where the third equality holds only if $\mathsf{P}(x, y_i) = 1$ from the correctness of predicate encodings. Let $\mathsf{mpk}_j = [(w_{j,0}+v_j)\mathbf{a}_{y_j} + \mathbf{w}_j\mathbf{K}_{y_j}, \mathbf{w}_j]_1$. Then, by stretching the notation a bit, we can view $\mathsf{mpk} = \sum_j \mathsf{mpk}_j$. In essence, ct_x represents a ciphertext relative to $\sum_j \mathsf{mpk}_j$, and during decryption for user i, hsk_i enables us to strip ct_x of its association with $\sum_{j \neq i} \mathsf{mpk}_j$, retaining only the relationship with mpk_i. This adjustment ensures that the correctness and security of the ZZGQ sReg-ABE scheme rely primarily on predicate encodings, akin to vanilla ABE.

Pair Encoding Schemes. As in the case of vanilla ABE, we cannot capture unbounded schemes by predicate encodings and need more generalized framework, namely, pair encoding schemes (PES) [Att14, AC17]. Roughly speaking, PES for predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ define two vectors of polynomials for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$:

$$\mathbf{c}_x(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}) = \hat{\mathbf{s}}\mathbf{F}_x + \mathbf{s}(\mathbf{I}_{n_1} \otimes \mathbf{w})\widehat{\mathbf{F}}_x, \quad \mathbf{k}_y(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w}) = \hat{\mathbf{r}}\mathbf{L}_y + \mathbf{r}(\mathbf{I}_{m_1} \otimes \mathbf{w})\widehat{\mathbf{L}}_y \tag{3}$$

in variables $\mathbf{s} = (s_1, \ldots, s_{n_1}), \mathbf{r} = (r_1, \ldots, r_{m_1})$ (called *non-lone* variables), $\hat{\mathbf{s}} = (\hat{s}_1, \ldots, \hat{s}_{n_3}), \hat{\mathbf{r}} = (\hat{r}_1, \ldots, \hat{r}_{m_3})$ (called *lone* variables), and $\mathbf{w} = (w_1, \ldots, w_\omega)$ (called *common* variables).[5] Matrices $\mathbf{F}_x \in \mathbb{Z}_p^{n_3 \times n_2}, \widehat{\mathbf{F}}_x \in \mathbb{Z}_p^{n_1\omega \times n_2}$ and $\mathbf{L}_y \in \mathbb{Z}_p^{m_3 \times m_2}, \widehat{\mathbf{L}}_y \in \mathbb{Z}_p^{m_1\omega \times m_2}$ are coefficient matrices depending on x and y, respectively.[6] $\mathbf{I}_t$ denotes the identity matrix of size $t \times t$. Note that n_1, n_2, n_3 and m_1, m_2, m_3 depend on x and y, respectively. These polynomials satisfy *decoding* correctness, which says that if $\mathsf{P}(x, y) = 1$, then there exist $\mathbf{E}_{x,y} \in \mathbb{Z}_p^{n_2 \times m_1}, \overline{\mathbf{E}}_{x,y} \in \mathbb{Z}_p^{m_2 \times n_1}$ such that $\mathbf{c}_x\mathbf{E}_{x,y}\mathbf{r}^{\top} + \mathbf{k}_y\overline{\mathbf{E}}_{x,y}\mathbf{s}^{\top} = s_1\hat{r}_1$ holds symbolically. Intuitively, $s_1\hat{r}_1$ is a special term, for which $[s_1\hat{r}_1]_{\mathsf{T}} \cdot M$ is the masked message term in the vanilla ABE from PES. Note that predicate encodings are special case of pair encodings where $n_1 = m_1 = 1, n_2 = n_c, m_2 = n_k, n_3 = 0, m_3 = 1, \widehat{\mathbf{F}}_x = \mathbf{C}_x, \mathbf{L}_y = \mathbf{a}_y, \widehat{\mathbf{L}}_y = \mathbf{K}_y$ for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$ and captured as

$$\mathbf{c}_x(s_1, \mathbf{w}) = s_1\mathbf{w}\mathbf{C}_x, \quad \mathbf{k}_y(r_1, \hat{r}_1, \mathbf{w}) = \hat{r}_1\mathbf{a}_y + r_1\mathbf{w}\mathbf{K}_y.$$

Challenges for sReg-ABE from PES. When trying to apply general PES to the ZZGQ sReg-ABE, two obstacles emerge due to disparities between PES and predicate encodings: (1) Decoding involves non-lone variables. (2) Sizes m_1, m_2, m_3 and the coefficient matrix $\mathbf{L}_y$ (in the polynomial vector $\mathbf{k}_y$) depend on y. Let us explore why these pose obstacles.

Firstly, a crucial difference between sReg-ABE and ABE is that in sReg-ABE, both the key encoding $(\mathbf{K}_y, \mathbf{a}_y)$ and the ciphertext encoding $\mathbf{C}_x$ appear in G_1, while in ABE, they appear in G_1 and G_2 respectively. For predicate encodings, decoding efficiently works even if the entire $\mathbf{M}_{x,y}$ is encoded in G_1, allowing for the computation of $[\mathbf{M}_{x,y}\mathbf{d}_{x,y}^{\top}]_1$ from $[\mathbf{M}_{x,y}]_1$. However, decoding in pair encodings is not confined to G_1 alone: it involves non-lone variables $\mathbf{s}, \mathbf{r}$ multiplying with encodings $\mathbf{c}_x$, $\mathbf{k}_y$. Specifically, $[\mathbf{c}_x\mathbf{E}_{x,y}\mathbf{r}^{\top} + \mathbf{k}_y\overline{\mathbf{E}}_{x,y}\mathbf{s}^{\top}]_1$ cannot be efficiently computed from $[\mathbf{s}, \mathbf{r}, \mathbf{c}_x, \mathbf{k}_y]_1$.

Initially, encoding $\mathbf{r}, \mathbf{k}_y$ in G_2 and computing $\mathbf{c}_x\mathbf{E}_{x,y}\mathbf{r}^{\top} + \mathbf{k}_y\overline{\mathbf{E}}_{x,y}\mathbf{s}^{\top}$ in G_{T} seems intuitive. However, it is evident that this approach falls short, as an additional pairing between the resulting term and the "slot-specific" element, namely, r_i in hsk_i, is needed. This is since hsk_i must be encoded in

[5] The naming terminology follows [AC17]. Intuitively, the *non-lone* ones are multiplied with the *common* ones, while the *lone* ones are not multiplied with other variables. The *common* ones appear in both vectors of polynomials.

[6] In contrast to previous works where pair encodings are denoted by sets of polynomials, we denote them by vectors (or matrices) of polynomials in this paper.

group elements and linked with r_i for each i (to prevent "mix-and-match" attack with other slots). Consequently, in decryption, the term $r_i(\mathbf{c}_x\mathbf{E}_{x,y}\mathbf{r}^\top + \mathbf{k}_y\overline{\mathbf{E}}_{x,y}\mathbf{s}^\top)$ needs to be computed. Intuitively, this term is the canonical PES counterpart of the expression $sr_i(w_{i,0} + v_i \,||\, \mathbf{w}_i)\begin{pmatrix} \mathbf{a}_{y_i} & \mathbf{0} \\ \mathbf{K}_{y_i} & \mathbf{C}_x \end{pmatrix}\mathbf{d}_{x,y}^\top$ in the ZZGQ scheme as per Eq. (2).

New PES Formulation. We resolve the above problem by observing that:

$$\mathbf{c}_x\mathbf{E}_{x,y}\mathbf{r}^\top + \mathbf{k}_y\overline{\mathbf{E}}_{x,y}\mathbf{s}^\top = \mathsf{tr}(\mathbf{E}_{x,y}\underbrace{\mathbf{r}^\top\mathbf{c}_x}_{\mathbf{C}}) + \mathsf{tr}(\overline{\mathbf{E}}_{x,y}\underbrace{\mathbf{s}^\top\mathbf{k}_y}_{\mathbf{K}})$$

where $\mathsf{tr}(\mathbf{M})$ denotes the trace of square matrix $\mathbf{M}$, *i.e.,* the sum of its diagonal entries. In other words, we can efficiently compute $[\mathbf{c}_x\mathbf{E}_{x,y}\mathbf{r}^\top + \mathbf{k}_y\overline{\mathbf{E}}_{x,y}\mathbf{s}^\top]_1$ from $[\mathbf{C}, \mathbf{K}]_1 = [\mathbf{r}^\top\mathbf{c}_x, \mathbf{s}^\top\mathbf{k}_y]_1$. For security reasons, we use the following replacement of variables in $(\mathbf{C}, \mathbf{K})$: $\mathbf{r}^\top\hat{\mathbf{s}} \mapsto \mathbf{T}$, $\mathbf{s}^\top\hat{\mathbf{r}} \mapsto \mathbf{U}$, $\mathbf{r}^\top\mathbf{s} \mapsto \mathbf{S}'$ where $\mathbf{T} = (t_{i,j})_{i,j}, \mathbf{U} = (u_{i,j})_{i,j}, \mathbf{S}' = (s'_{i,j})_{i,j}$ (recall that we have $\mathbf{C} = \mathbf{r}^\top\hat{\mathbf{s}}\mathbf{F}_x + \mathbf{r}^\top\mathbf{s}(\mathbf{I}_{n_1} \otimes \mathbf{w})\widehat{\mathbf{F}}_x$ and $\mathbf{K} = \mathbf{s}^\top\hat{\mathbf{r}}\mathbf{L}_y + \mathbf{s}^\top\mathbf{r}(\mathbf{I}_{m_1} \otimes \mathbf{w})\widehat{\mathbf{L}}_y$ from Eq. (3)). Intuitively, this replacement increases the entropy of $(\mathbf{C}, \mathbf{K})$ when all variables are randomly taken from $\mathbb{Z}_p$ and thus does not harm the security of the original PES. This leads to a new variant of PES for sReg-ABE:

$$\begin{aligned} \mathbf{C}_{x,y}(\mathbf{S}', \mathbf{T}, \mathbf{w}) &= \mathbf{T}\mathbf{F}_x + \mathbf{S}'\underbrace{(\mathbf{I}_{n_1} \otimes \mathbf{w})\widehat{\mathbf{F}}_x}_{\widehat{\mathbf{C}}_x(\mathbf{w})}, \\ \mathbf{K}_{x,y}(\mathbf{S}', \mathbf{U}, \mathbf{w}) &= \mathbf{U}\mathbf{L}_y + \mathbf{S}'^\top\underbrace{(\mathbf{I}_{m_1} \otimes \mathbf{w})\widehat{\mathbf{L}}_y}_{\widehat{\mathbf{K}}_y(\mathbf{w})} \end{aligned} \tag{4}$$

Note that the special term $s_1\hat{r}_1$ is now replaced with $u_{1,1}$, the $(1,1)$-th entry of $\mathbf{U}$. A caveat is that both $\mathbf{C}_{x,y}$ and $\mathbf{K}_{x,y}$ depend on (x, y) since $\mathbf{C}_{x,y}$ and $\mathbf{K}_{x,y}$ depend on m_1 and n_1, which depend on y and x, respectively. Looking ahead, it will be useful to separate a term which depends only on y, namely, $\widehat{\mathbf{K}}_y(\mathbf{w})$ in Eq. (4); we call it a common variable encoding. This is since we use $\widehat{\mathbf{K}}_y(\mathbf{w})$ in generation of mpk where x is not given at this point, as we will see in Eq. (5).

Generalizing the ZZGQ scheme so as to be compatible with our variant of PES above leads to the following candidate scheme (but not yet correct, see below):

$$\begin{aligned} \mathsf{crs} &= ([\alpha]_\mathsf{T},\ \{[w_{j,0}, \mathbf{w}_j]_1\}_{j\in[L]},\ \{[r_i, r_iw_{j,0}, r_i\mathbf{w}_j, r_iw_{i,0} + \alpha]_2\}_{i,j\in[L],i\neq j}) \\ \mathsf{pk}_i &= ([v_i]_1, \{[v_ir_j]_2\}_{j\neq i}), \quad \mathsf{sk}_i = v_i \\ \mathsf{mpk} &= (y_1, [\underbrace{\textstyle\sum_{j\in[L]}(w_{j,0} + v_j)}_{p_1}, \underbrace{\textstyle\sum_j \widehat{\mathbf{K}}_{y_j}(\mathbf{w}_j)}_{\mathbf{P}_2}, \textstyle\sum_j \mathbf{w}_j]_1, [\alpha]_\mathsf{T}) \\ \mathsf{hsk}_i &= [r_i, \underbrace{r_i\textstyle\sum_{j\neq i}(w_{j,0} + v_j)}_{h_1}, \underbrace{r_i\textstyle\sum_{j\neq i}\widehat{\mathbf{K}}_{y_j}(\mathbf{w}_j)}_{\mathbf{H}_2}, \underbrace{r_i\textstyle\sum_{j\neq i}\mathbf{w}_j}_{\mathbf{h}_3}, \underbrace{r_iw_{i,0} + \alpha}_{h_4}]_2 \\ \mathsf{ct}_x &= ([s_0, \mathbf{S}', \underbrace{\textstyle\sum_j \mathbf{K}_{x,y_j}(\mathbf{S}', \mathbf{U}, \mathbf{w}_j)}_{\mathbf{C}_1}, \underbrace{\mathbf{C}_{x,y_1}(\mathbf{S}', \mathbf{T}, \textstyle\sum_j \mathbf{w}_j)}_{\mathbf{C}_2}]_1, [s_0\alpha]_\mathsf{T}M) \end{aligned} \tag{5}$$

where all variables are randomly taken from $\mathbb{Z}_p$ except that we set $u_{1,1} = s_0p_1$, where p_1 is defined as above. As a side note, generalizing ZZGQ with PES is already not trivial in the first place; for example, we have to split the first term in mpk into the terms p_1 and $\mathbf{P}_2$, to accommodate potential multiplications of $\mathbf{P}_2$ by various non-lone variables in $\mathbf{C}_1$ during encryption. (Recall that predicate encoding has only one non-lone variable in each encoding.)

The second obstacle arises here: if the sizes $m_{j,1}, m_{j,2}, m_{j,3}$ depend on an attribute y_j, defining the terms $\mathbf{P}_2, \mathbf{H}_2, \mathbf{C}_1$ becomes problematic due to the potential variation in sizes for matrices in the sums. To address this, for now, we assume the existence of constants $m_1, m_2, m_3 \in \mathbb{N}$ such that $\widehat{\mathbf{K}}_y(\mathbf{w}) \in \mathbb{Z}_p^{m_1\times m_2}$ and $\mathbf{L}_y \in \mathbb{Z}_p^{m_3\times m_2}$ for all $y \in \mathcal{Y}$. With this adjustment, all the "ciphertext encoding" of x remains invariant across different values of y_i, i.e., $\mathbf{C}_{x,y_1} = \cdots = \mathbf{C}_{x,y_L}$. This is since the only factor of $\mathbf{C}_{x,y_i}$ that is affected by y_i is the size $m_{i,1}$. In decryption for user i with $\mathsf{P}(x, y_i) = 1$, we would compute

$$\begin{aligned}[d]_\mathsf{T} =& [\mathsf{tr}(\mathbf{E}(r_i\mathbf{C}_2 - \mathbf{S}'\widehat{\mathbf{C}}_x(\mathbf{h}_3))) + \mathsf{tr}(\overline{\mathbf{E}}(r_i\mathbf{C}_1 - \mathbf{S}'^\top\mathbf{H}_2))]_\mathsf{T}\\ =& [r_i(\mathsf{tr}(\mathbf{E}(\mathbf{C}_{x,y_i}(\mathbf{S}', \mathbf{T}, \mathbf{w}))) + \mathsf{tr}(\overline{\mathbf{E}}(\mathbf{K}_{x,y_i}(\mathbf{S}', \mathbf{U}, \mathbf{w}) + \textstyle\sum_{j\neq i}\mathbf{UL}_{y_j})))]_\mathsf{T}.\end{aligned}$$

This equality relies on the property of invariant ciphertext encoding. Next, suppose we could remove the "cross term" $\sum_{j\neq i}\mathbf{UL}_{y_j}$, then we would have $d = s_0r_ip_1$, which follows the correctness of the PES and be able to compute $[d - s_0h_1 - s_0r_iv_i - s_0h_4]_\mathsf{T} = [-s_0\alpha]_\mathsf{T}$; thus, the decryption would work. Our idea here is then to further assume that there exists $\mathbf{L}$ such that $\mathbf{L}_y = \mathbf{L}$ for all $y \in \mathcal{Y}$ and redefine $\mathbf{C}_1$ in Eq. (5) with $\mathbf{C}'_1$ as follows.

$$\mathbf{C}'_1 = \mathbf{UL} + \textstyle\sum_j \mathbf{S}'^\top\widehat{\mathbf{K}}_{y_j}(\mathbf{w}_j) = \mathbf{C}_1 - \sum_{j\neq i}\mathbf{UL}_{y_j} \tag{6}$$

Here, the second equality holds *for all* $i \in [L]$, if $\mathbf{L}_y = \mathbf{L}$ for all $y \in \mathcal{Y}$ (by the definition in Eq. (4)). Hence, this replacement prevents the appearance of the "cross term" $\sum_{j\neq i}\mathbf{UL}_{y_j}$ for all i and decryption for every user work.

Although the above ideas work, it turns out that assuming $\exists m_1, m_2, \mathbf{L} : \widehat{\mathbf{K}}_y(\mathbf{w}) \in \mathbb{Z}_p^{m_1\times m_2}, \mathbf{L}_y = \mathbf{L}$ for all $y \in \mathcal{Y}$ significantly limits expressiveness of PES. More precisely, if the size of $\mathbf{L}_y$ is a priori fixed, we can replace non-lone variables with common variables, and the expressiveness of key encodings become essentially the same as predicate encodings. Hence, via this PES, we cannot capture unbounded sReg-ABE scheme, where the number of attribute to be associated with the key encoding element $\mathbf{C}_1$ in ct_x is not a priori bounded.

Mitigating to Partial Limitation: Well-formedness w.r.t. Registered Set. The main observation to ease the above limitation is that the scheme in Eq. (5) with the modification in Eq. (6) remains effective even when the constraint on key encodings is relaxed to: $\exists m_1, m_2, \mathbf{L} : \widehat{\mathbf{K}}_{y_j}(\mathbf{w}) \in \mathbb{Z}_p^{m_1\times m_2}, \mathbf{L}_{y_j} = \mathbf{L}$ $\underline{\text{for all } j \in [L]}$. Put simply, this condition need only hold for the attributes $\{y_j\}_{j\in[L]}$ associated with $\underline{\text{users registered}}$ in the system, rather than the entire attribute space $\mathcal{Y}$. Going forward, we employ the term "well-formed" in this context, implying that a PES is well-formed if the condition is met for any given set $\{y_j\}_{j\in[L]}$.

Registered Set Dependency via Short Auxiliary Input. To ensure the significance of the "partial limitation" compared to the "entire limitation", it is crucial for the key encoding $\mathbf{K}_{x,y_i}$ (*cf.* Eq. (4)) to depend on the registered set $\{y_j\}_{j\in[L]}$, since otherwise, both limitations would render to the same thing.

We investigate how to establish this dependency. First, in PES-based sReg-ABE constructions (ZZGQ and our candicate), the "key encoding" is embedded into a ciphertext. In particular, the key encoding $\mathbf{K}_{x,y_i}$ resides in $\mathbf{C}_1$ of the ciphertext ct_x (as in Eq. (5)). Next, considering the definition of sReg-ABE, a ciphertext ct_x is formed from (mpk, x, M), and not from the registered set $\{y_j\}_{j\in[L]}$. However, directly incorporating $\{y_j\}_j$ into mpk would result in $|\mathsf{mpk}| = O(L)$, violating the compactness requirement for registered ABE. To address this, we observe that it suffices to utilize only *auxiliary information*, aux_k, that is efficiently computable from $\{y_j\}_j$ to serve as a "digest" of the information about $\{y_j\}_{j\in[L]}$. Loosely speaking, we can think of y_j as a set of attributes, and aux_k as the maximum number of attributes among $\{y_j\}_{j\in[L]}$ in our constructions. It is crucial that $|\mathsf{aux}_k|$ remains independent of L, allowing its inclusion in mpk.

In summary, we form our final PES for sReg-ABE as:

$$\mathbf{C}_{x,y,\mathsf{aux}_c}(\mathbf{S}', \mathbf{T}, \mathbf{w}) = \mathbf{TF}_{x,\mathsf{aux}_c} + \mathbf{S}'\underbrace{(\mathbf{I}_{n_1} \otimes \mathbf{w})\widehat{\mathbf{F}}_{x,\mathsf{aux}_c}}_{\widehat{\mathbf{C}}_{x,\mathsf{aux}_c}(\mathbf{w})}$$

$$\mathbf{K}_{x,y,\mathsf{aux}_k}(\mathbf{S}', \mathbf{U}, \mathbf{w}) = \mathbf{UL}_{y,\mathsf{aux}_k} + \mathbf{S}'^\top\underbrace{(\mathbf{I}_{m_1} \otimes \mathbf{w})\widehat{\mathbf{L}}_{y,\mathsf{aux}_k}}_{\widehat{\mathbf{K}}_{y,\mathsf{aux}_k}(\mathbf{w})}$$

Note that although aux_c is not essential in the sReg-ABE construction, we use it for security analysis of PES. Our sReg-ABE scheme from well-formed PES is given as follows, where $\mathsf{crs}, \mathsf{pk}_i, \mathsf{sk}_i$ are the same as in Eq. (5), and $u_{1,1} = s_0 p_1$:

$$\begin{aligned}
\mathsf{mpk} &= (y_1, \mathsf{aux}_k, [\underbrace{\textstyle\sum_{j \in [L]} (w_{j,0} + v_j)}_{p_1}, \underbrace{\textstyle\sum_j \widehat{\mathbf{K}}_{y_j, \mathsf{aux}_k}(\mathbf{w}_j)}_{\mathbf{P}_2}, \textstyle\sum_j \mathbf{w}_j]_1, [\alpha]_{\mathsf{T}}) \\
\mathsf{hsk}_i &= [r_i, r_i \textstyle\sum_{j \neq i} (w_{j,0} + v_j), r_i \sum_{j \neq i} \widehat{\mathbf{K}}_{y_j, \mathsf{aux}_k}(\mathbf{w}_j), r_i \sum_{j \neq i} \mathbf{w}_j, r_i w_{i,0} + \alpha]_2 \\
\mathsf{ct}_x &= ([s_0, \mathbf{S}', \mathbf{U}\mathbf{L}_{y_1, \mathsf{aux}_k} + \mathbf{S}'^{\top} \mathbf{P}_2, \mathbf{C}_{x, y_1, \mathsf{aux}_c}(\mathbf{S}', \mathbf{T}, \textstyle\sum_j \mathbf{w}_j)]_1, [s_0 \alpha]_{\mathsf{T}} M).
\end{aligned}$$

sReg-ABE for Unbounded Predicates from Well-formed PES. Next challenge is to devise PES for *sReg-ABE for unbounded predicates* that satisfies well-formedness. What makes things more difficult is that we also need to take security into account for the PES construction. Furthermore, our goal is sReg-ABE scheme based on the static MDDH assumption, and thus we cannot rely on the symbolic property which rely on a dynamic assumption [AC17]. We address this formidable challenge through the PES transformation framework proposed by Attrapadung and Tomida [AT20].

Let us briefly recall their framework. The main idea of their work, which originally observed by Attrapadung [Att19], is that applying three predicate transformations to a simple predicate (such as the predicate for IBE) in an appropriate order results in predicates for unbounded ABE. This approach allows us to construct ABE for a complex predicate in a modular manner. Attrapadung also provides corresponding PES transformations for the three predicate transformations. The three predicate transformations are $\mathsf{DS}, \mathsf{Dual}, \mathsf{KP1}$, which are defined as follows. The direct sum of predicates $\mathcal{P} = (\mathsf{P}_1, \ldots, \mathsf{P}_n)$ where $\mathsf{P}_i : \mathcal{X}_i \times \mathcal{Y}_i \to \{0,1\}$ combines predicates as $\mathsf{DS}[\mathcal{P}]((i,x),(j,y)) = 1 \Leftrightarrow i = j \wedge \mathsf{P}_i(x,y) = 1$. The dual transformation switches the ciphertext with key attribute spaces of P, *i.e.,* $\mathsf{Dual}[\mathsf{P}](x,y) = 1 \Leftrightarrow \mathsf{P}(y,x) = 1$. The key policy (KP) augmentation of P is defined as $\mathsf{KP1}[\mathsf{P}](x,(\mathbf{M},\phi)) = 1 \Leftrightarrow (1,\mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i \in [n] : \mathsf{P}_\kappa(x,\phi(i))=1})$ where $\mathbf{M} \in \mathbb{Z}_p^{n \times m}$ is a span program, $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$, and $\phi : [n] \to \mathcal{Y}$ is a labeling function.[7] For instance, let $\mathsf{P}^{\mathsf{IBE}}(x,y) = 1 \Leftrightarrow x = y$, then we can obtain by $\mathsf{KP1}[\mathsf{Dual}[\mathsf{KP1}[\mathsf{P}^{\mathsf{IBE}}]]]$ a predicate for completely unbounded KP-ABE for monotone span programs (see [AT20, Section 6] for details).

The main technical contribution in [AT20] is to introduce the new security notion for PES called key-encoding indistinguishability ($\mathsf{KE\text{-}ind}$) and prove the three properties on $\mathsf{KE\text{-}ind}$ under the MDDH assumption:

1. PES obtained from predicate encodings satisfies $\mathsf{KE\text{-}ind}$;
2. $\mathsf{KE\text{-}ind}$ is preserved through the three PES transformations;
3. Adaptively secure ABE for P can be constructed from PES for P with $\mathsf{KE\text{-}ind}$.

As a corollary, an adaptively secure ABE scheme for P can be constructed if P can be obtained by applying the three transformations to predicates that have predicate encodings.

Our strategy is to introduce a sReg-ABE analog of $\mathsf{KE\text{-}ind}$. However, our situation is more intricate since we need to ensure that the final PES used for constructing a sReg-ABE scheme satisfies both well-formedness and $\mathsf{KE\text{-}ind}$. To this end, we prove the following properties under the MDDH assumption:

1. PES obtained from predicate encodings satisfies $\mathsf{KE\text{-}ind}$ and well-formedness;
2. $\mathsf{KE\text{-}ind}$ and well-formedness are preserved through certain PES transforms;
3. A secure sReg-ABE scheme for P can be constructed from PES for P with $\mathsf{KE\text{-}ind}$ and well-formedness.

[7] [AT20] consider less expressive policy than span programs, namely, Boolean formulae for KP augmentation, so as to achieve (adaptive) security for ABE under MDDH. For Reg-ABE, the security is inherently less adaptive (as all keys are embedded already in mpk), and we can consider span programs (while relying in MDDH).

While items 1 and 3 are not so hard to prove, item 2 poses a challenge as two PES transforms, DS and $\mathsf{KP1}$, do not preserve well-formedness. Hence, we introduce alternative transformations to obtain sReg-ABE for unbounded predicates.

Alternative Transformations for $\mathsf{KP1}$. First, we elaborate on why $\mathsf{KP1}$ fails to maintain well-formedness and introduce alternative transformations. Let Γ be a PES for $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, $\mathsf{KP1\text{-}Trans}(\Gamma)$ be a PES for $\mathsf{KP1}[\mathsf{P}]$, and $\mathbf{L}_y = \begin{pmatrix} \bar{\mathbf{l}}_y \\ \underline{\mathbf{L}}_y \end{pmatrix}$ be a coefficient matrix in Γ for $y \in \mathcal{Y}$ ($\bar{\mathbf{l}}_y$ is the first row). The PES $\mathsf{KP1\text{-}Trans}(\Gamma)$ by [Att19] sets a coefficient matrix $\mathbf{L}'_{(\mathbf{M},\phi)}$ for key attribute $(\mathbf{M},\phi)$ as:

$$\mathbf{L}'_{(\mathbf{M},\phi)} = \begin{pmatrix} \mathbf{m}_1^\top \bar{\mathbf{l}}_{\phi(1)} & \cdots & \mathbf{m}_n^\top \bar{\mathbf{l}}_{\phi(n)} \\ \underline{\mathbf{L}}_{\phi(1)} & & \\ & \ddots & \\ & & \underline{\mathbf{L}}_{\phi(n)} \end{pmatrix}$$

where $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$. (For notational simplicity, we omit to subscript aux_k here and in what follows.) It is clear that $\mathbf{L}'_{(\mathbf{M},\phi)}$ depends on even the size of $\mathbf{M}$, and thus the coefficient matrices will never be the same for a set of adversarially chosen key attributes $\{(\mathbf{M}_i, \phi_i)\}_{i\in[L]}$.

To solve this issue, we first observe that some applications of $\mathsf{KP1}$ in obtaining unbounded ABE are overkilled. Recall that a predicate $\mathsf{P}^{\mathsf{KP-MSP}}$ for monotone unbounded KP-ABE can be obtained by $\mathsf{KP1}[\mathsf{Dual}[\mathsf{KP1}[\mathsf{P}^{\mathsf{IBE}}]]]$. As observed in [Att19]; however, at the first application of $\mathsf{KP1}$, it suffices to handle OR policies, denoted by $\mathsf{KP1}_{\mathsf{OR}}$. That is, $\mathsf{P}^{\mathsf{KP-MSP}}$ is obtained by $\mathsf{KP1}[\mathsf{Dual}[\mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}^{\mathsf{IBE}}]]]$.

Let us put the second $\mathsf{KP1}$ aside for a moment and focus on $\mathsf{KP1}_{\mathsf{OR}}$. OR policies are captured by span programs of the form $\mathbf{M} = (1,\ldots,1)^\top$, or equivalently $\mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}](x,\phi) = 1 \Leftrightarrow \bigvee_{i\in[n]} \mathsf{P}(x,\phi(i)) = 1$ (we can omit $\mathbf{M}$ from key attribute since it can be specified by only the policy size n). Hence, the coefficient matrices $\{\mathbf{L}'_{\phi_i}\}_{i\in[L]}$ of OR policies become the same if the domains of $\{\phi_i\}_i$ have the same size n, and $\{\mathbf{L}_{\phi_i(j)}\}_{(i,j)\in[L]\times[n]}$ are the same. In fact, the latter condition can be straightforwardly achieved if Γ is well-formed.

To address the former condition, we use the fact that $\bigvee_{i\in[n]} \mathsf{P}(x,\phi(i)) = 1 \Leftrightarrow \bigvee_{i\in[n]} \mathsf{P}(x,\phi(i)) \vee 0 \vee \cdots \vee 0 = 1$. In other words, if $\mathcal{Y}$ contains a null attribute null such that $\mathsf{P}(x,\mathsf{null}) = 0$ for all $x \in \mathcal{X}$, we always have $\mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}](x,\phi) = \mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}](x,\phi')$ where $\delta > n$, $\phi : [n] \to \mathcal{Y}$, and $\phi' : [\delta] \to \mathcal{Y}$ such that $\phi'(i) = \phi(i)$ for $i \in [n]$ and $\phi'(i) = \mathsf{null}$ for $n < i \le \delta$. Hence, for a set of OR policies $\{\phi_i\}_i$, we can obtain a set of equivalent OR policies $\{\phi'_i\}_i$ of the same size by setting $\delta = \max n_i$ where n_i is the domain size of ϕ_i. Armed with this idea, we can achieve the PES transformation for $\mathsf{KP1}_{\mathsf{OR}}$ that preserves $\mathsf{KE\text{-}ind}$ and well-formedness by including δ in aux_k (see §4.3 for details). Additionally, we also present a predicate transformation Null that adds null to $\mathcal{Y}$ to make the above idea work for any predicates (§4.1). We also remark that we need $\mathsf{KP1}$ for AND policies, denoted by $\mathsf{KP1}_{\mathsf{AND}}$, to obtain a predicate for non-monotone unbounded ABE. Similar to $\mathsf{KP1}_{\mathsf{OR}}$, we can obtain the PES transformation for $\mathsf{KP1}_{\mathsf{AND}}$ that preserves $\mathsf{KE\text{-}ind}$ and well-formedness together with a transformation WC that adds a wildcard $*$ to $\mathcal{Y}$ where $\mathsf{P}(x,*) = 1$ for all x (see §4.2 and 4.4 for details).

Finally, we discuss the deferred $\mathsf{KP1}$ transformation, applied second when constructing $\mathsf{P}^{\mathsf{KP-MSP}}$. Due to the need for a fully-fledged $\mathsf{KP1}$ at this stage, we cannot hope that it preserves well-formedness. However, there is a silver lining: $\mathsf{KP1}$ preserves well-formedness *with respect to ciphertext encodings* (note also that other transformations described in this paragraph also do so). Specifically, we can construct a PES for $\mathsf{KP1}[\mathsf{P}]$ where $\exists n_1, n_2, \mathbf{F}, \forall i \in [L] : \widehat{\mathbf{C}}_{x_i}(\mathbf{w}) \in \mathbb{Z}_p^{n_1\times n_2}, \mathbf{F}_{x_i} = \mathbf{F}$ for given $\{x_i\}_{i\in[L]}$ if the underlying PES for P satisfies ciphertext well-formedness. Leveraging the fact that Dual switches the well-formedness in ciphertext and key encodings, and only the key well-formedness is needed to construct a sReg-ABE scheme, we can achieve a predicate $\mathsf{P}^{\mathsf{CP-MSP}}$ for unbounded monotone *CP-ABE* by $\mathsf{Dual}[\mathsf{KP1}[\mathsf{Dual}[\mathsf{KP1}_{\mathsf{OR}}[\mathsf{Null}[\mathsf{P}^{\mathsf{IBE}}]]]]]$ together with a PES satisfying $\mathsf{KE\text{-}ind}$ and key well-formedness. In summary, we introduce four transformations $\mathsf{KP1}_{\mathsf{OR}}, \mathsf{KP1}_{\mathsf{AND}}, \mathsf{Null}, \mathsf{WC}$ for a substitution of some applications of $\mathsf{KP1}$ while we also use $\mathsf{KP1}$ only in the last step of a series of transformations.

Alternative Transformations for DS. Next, let us explore alternative transformations for DS. The problem of PES for $\mathsf{DS}[\mathcal{P}]$ for $\mathcal{P} = (\mathsf{P}_1, \ldots, \mathsf{P}_n)$ comes from the fact that y in a key attribute (j, y) of $\mathsf{DS}[\mathcal{P}]$ belongs to *one* of $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$. More precisely, the coefficient matrix $\mathbf{L}'_{(j,y)}$ of (j, y) in the PES for $\mathsf{DS}[\mathcal{P}]$ would be $\mathbf{L}_{j,y}$, which is the coefficient matrix of y in the PES for P_j. Hence, for an arbitrarily chosen set of key attributes $(j_\ell, y_\ell)_{\ell\in[L]}$, the corresponding coefficient matrices $\{\mathbf{L}_{j_\ell,y_\ell}\}$ will never be the same unless PES for $\mathsf{P}_1, \ldots, \mathsf{P}_n$ have the same coefficient matrix. However, such a strong restriction makes DS transformation almost useless for combining predicates.

Looking back at [AT20], we can observe that DS is mainly used to obtain static predicate compositions [ABS17] and construct two-mode identity-based broadcast encryption (TIBBE). Roughly speaking, static predicate compositions allow us to obtain a predicate like $\mathsf{P} = \mathsf{P}_1 \wedge \mathsf{P}_2$ where $\mathsf{P}((x_1, x_2), (y_1, y_2)) = 1 \Leftrightarrow \mathsf{P}_1(x_1, y_1) = 1 \wedge \mathsf{P}_2(x_2, y_2) = 1$. Furthermore, we find that TIBBE can be constructed from static predicate compositions (SPC) together with the Null transformation which adds the null attribute to a key attribute space. Luckily, SPC preserves well-formedness because the coefficient matrix $\mathbf{L}'_{(y_1,y_2)}$ in the PES for P is specified by coefficients matrices $\mathbf{L}_{y_1}$ in P_1 and $\mathbf{L}_{y_2}$ in P_2 and the form of composition, which is a priori fixed. To summarize, we use SPC and Null to substitute DS.

Malicious pk and Prime-order Scheme. The remaining tasks are handling of maliciously generated public keys and security proofs in prime-order groups. Since this step closely resembles [ZZGQ23], we omit details here. Briefly, we prevent users from registering malicious keys by forcing them to add a proof of quasi-adaptive non-interactive zero-knowledge argument [JR13], and to prove the security of sReg-ABE scheme in prime-order groups via the dual system technique [Wat09] we use the variable-to-matrix substitution framework in [CGW15] as described in §A.

Discussions on Open Problems. Our study primarily focuses on registered ABE for complex predicates, particularly those with unbounded characteristics. An orthogonal objective, not addressed in our work, involves achieving unbounded-user schemes, for which current solutions are limited to relying on iO or WE and non-black-box usage of cryptographic primitives. Additionally, obtaining key-policy registered ABE for unbounded span program predicates poses another unresolved challenge. We leave these issues as open problems.

2 Preliminaries

Notations. For $n, m \in \mathbb{N}$, $[m]$ and $[n, m]$ denotes $\{1, \ldots, m\}$ and $\{n, \ldots, m\}$, respectively. $\mathbf{O}$ and $\mathbf{0}$ denotes a zero matrix and a zero vector (with sizes corresponding to the context). For a square matrix $\mathbf{M}$, $\mathsf{tr}(\mathbf{M})$ denotes the trace of $\mathbf{M}$. For matrices $\mathbf{M}, \mathbf{N}$, $\mathbf{M} \otimes \mathbf{N}$ denotes the Kronecker product. A useful fact is that $(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = \mathbf{AC} \otimes \mathbf{BD}$ if $\mathbf{AC}$ and $\mathbf{BD}$ are defined. For $\mathbf{W} = (w_{i,j})_{i,j}$, $\mathbb{Z}_p[\mathbf{W}]$ denotes a set of all polynomials in $(w_{i,j})_{i,j}$ where coefficients are in $\mathbb{Z}_p$. For set S, $s \leftarrow S$ means that s is uniformly chosen from S. For two families of distributions $A = \{A_\lambda\}, B = \{B_\lambda\}$, $A \approx_c B$ and $A \approx_s B$ mean A and B are computationally and statistically indistinguishable, respectively. For matrix $\mathbf{M} = (\mathbf{m}_{i,j})_{i,j}$, we define $\mathbf{M}^{\mathsf{BT}} = (\mathbf{m}'_{i,j})_{i,j}$ where $\mathbf{m}'_{i,j} = \mathbf{m}_{j,i}$ (BT stands for block transpose). We sometimes abuse the notation: for $\mathbf{S}_{\mathbf{A}} = (\mathbf{s}_{i,j}\mathbf{A})_{i,j}$ denote $(\mathbf{s}'_{i,j}\mathbf{A})_{i,j}$ by $\mathbf{S}^{\mathsf{BT}}_{\mathbf{A}}$ where $\mathbf{s}'_{i,j} = \mathbf{s}_{j,i}$. $\mathsf{span}(\mathbf{M})$ denotes the row span of $\mathbf{M}$.

2.1 Definitions

Definition 2.1 (Bilinear Groups). Let $\{\mathbb{G}_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of bilinear groups. Bilinear groups $\mathbb{G}_\lambda{=}(p, G_1, G_2, G_T, g_1, g_2, e)$ are specified by a prime p, cyclic groups G_1, G_2, G_T of order p, generators g_1 and g_2 of G_1 and G_2 respectively, and a bilinear map $e : G_1 \times G_2 \to G_T$, which has two properties.

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

In what follows, we omit the index λ from $\mathbb{G}_\lambda$ and abuse notation by denoting a family of bilinear groups $\{\mathbb{G}_\lambda\}_{\lambda\in\mathbb{N}}$ also by $\mathbb{G}$ if it is clear in the context.

Definition 2.2 (MDDH Assumption [EHK+13]). Let $\{\mathbb{G}\}$ be a family of bilinear groups. We consider the following distribution, for any $n > k$ and $m \in \mathbb{N}$: $\mathbf{M} \leftarrow \mathbb{Z}_p^{k\times n}, \mathbf{R} \leftarrow \mathbb{Z}_p^{m\times k}, \mathbf{Z}_0 = \mathbf{R}\mathbf{M}, \mathbf{Z}_1 \leftarrow \mathbb{Z}_p^{m\times n}, P_{i,\beta} = (\mathbb{G}, [\mathbf{M}]_i, [\mathbf{Z}_\beta]_i)$. We say that the MDDH_k assumption holds with respect to $\{\mathbb{G}\}$ if $P_{i,0} \approx_c P_{i,1}$ for $i \in \{1,2\}$.

Definition 2.3 (QA-NIZK [JR13]). Quasi-adaptive non-interactive zero knowledge argument (QA-NIZK) for linear space over bilinear groups $\mathbb{G}$ consists of the four algorithms.

$\mathsf{LGen}(1^\lambda, [\mathbf{A}]_1)$**:** It takes a security parameter 1^λ and $[\mathbf{A}]_1 \in G_1^{n\times m}$ as input and outputs a common reference string crs and a trapdoor td.

$\mathsf{LProve}(\mathsf{crs}, [\mathbf{M}]_1, \mathbf{V})$**:** It takes crs, $[\mathbf{M}]_1 \in G_1^{n\times \ell}$ with a witness $\mathbf{V} \in \mathbb{Z}_p^{m\times \ell}$ as input and outputs a proof π.

$\mathsf{LVerify}(\mathsf{crs}, [\mathbf{M}]_1, \pi)$**:** It takes $\mathsf{crs}, [\mathbf{M}]_1, \pi$ as input and outputs $\beta \in \{0,1\}$.

$\mathsf{LSim}(\mathsf{crs}, \mathsf{td}, [\mathbf{M}]_1)$**:** It takes $\mathsf{crs}, \mathsf{td}, [\mathbf{M}]_1$ and outputs a simulated proof $\tilde{\pi}$.

Perfect Completeness. For all $n, m, \ell, \lambda, \mathbf{A}, \mathbf{V}, \mathbf{M}$ such that $\mathbf{M} = \mathbf{A}\mathbf{V}$,

$$\Pr\left[\mathsf{LVerify}(\mathsf{crs}, [\mathbf{M}]_1, \pi) = 1 \ : \ \begin{array}{l} (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{LGen}(1^\lambda, [\mathbf{A}]_1) \\ \pi \leftarrow \mathsf{LProve}(\mathsf{crs}, [\mathbf{M}]_1, \mathbf{V}) \end{array}\right] = 1$$

Perfect Zero-knowledge. For all $n, m, \ell, \lambda, \mathbf{A}, \mathbf{V}, \mathbf{M}$ such that $\mathbf{M} = \mathbf{A}\mathbf{V}$, $\mathsf{LProve}(\mathsf{crs}, [\mathbf{M}]_1, \mathbf{V})$ and $\mathsf{LSim}(\mathsf{crs}, \mathsf{td}, [\mathbf{M}]_1)$ are identically distributed where $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{LGen}(1^\lambda, [\mathbf{A}]_1)$.

Stronger Unbounded Simulation Soundness. For all PPT adversaries $\mathcal{A}$ and $n, m \in \mathbb{N}$, the following advantage of $\mathcal{A}$ is negligible in λ:

$$\Pr\left[\begin{array}{l} \quad ([\mathbf{M}^*]_1, \pi^*) \notin \mathcal{L} \\ \wedge \nexists \mathbf{V}, \mathbf{M}^* = \mathbf{A}\mathbf{V} \\ \wedge \ \mathsf{LVerify}(\mathsf{crs}, [\mathbf{M}^*]_1, \pi^*) = 1 \end{array} : \begin{array}{l} \mathbf{A} \leftarrow \mathbb{Z}_p^{n\times m} \\ (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{LGen}(1^\lambda, [\mathbf{A}]_1) \\ ([\mathbf{M}^*]_1, \pi^*) \leftarrow \mathcal{A}^{\mathsf{LSim}(\mathsf{crs}, \mathsf{td}, \cdot)}(1^\lambda, \mathsf{crs}, \mathbf{A}) \end{array}\right]$$

where $\mathcal{L}$ is a list of pairs of $\mathcal{A}$'s query to LSim and the corresponding response.

A QA-NIZK scheme that satisfies the above properties from MDDH is given in [KW15] (see also [ZZGQ23, Appindix B]).

We now describe the definition of *bounded-user* slotted registered ABE, which we refer to as sReg-ABE throughout the paper. We follow the definition in [ZZGQ23] (which, in turn, follows [HLWW23]).[8] A slight difference from their definition is compactness, that is, since we consider sReg-ABE where the attribute size is not a priori bounded, we allow $|\mathsf{mpk}|$ and $|\mathsf{hsk}|$ to depend on the size of the longest attribute to be registered. The definition for full-fledged registered attribute-based encryption (Reg-ABE) is deferred to §B. It is shown in [HLWW23, ZZGQ23] how to generically convert (bounded-user or unbounded-user) slotted registered ABE to registered ABE while preserving the (un)bounded-user property and compactness. We further note that the above modified compactness is also preserved via the conversion; see §B. We thus focus on constructing sReg-ABE.

Definition 2.4 (Bounded-User Slotted Registered ABE [HLWW23, ZZGQ23]). Let $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa$ be a predicate indexed by κ, where κ specifies some parameters. Let $\mathcal{M}$ be a message space. A bounded-user slotted registered attribute-based encryption (sReg-ABE) scheme for $\mathcal{P}_\kappa$ consists of the following algorithms.

$\mathsf{Setup}(1^\lambda, 1^L, \kappa)$**:** It takes a security parameter 1^λ, the number of slots 1^L, and an index κ as input, and outputs a common reference string crs.[9]

[8] To avoid ambiguity regarding boundedness, we use the term *bounded-user*, as opposed to simply *bounded*, as used in [HLWW23].

[9] In *unbounded-user* schemes, Setup takes L in binary instead of unary and is efficient even if we set $L = O(2^\lambda)$; see [HLWW23].

$\mathsf{Gen}(\mathsf{crs}, i)$**:** It takes crs and an index $i \in [L]$ as input, and outputs a public key pk_i and a secret key sk_i.

$\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i)$**:** It takes $\mathsf{crs}, i, \mathsf{pk}_i$ as input, and outputs 1 if pk_i is valid, and 0 otherwise.

$\mathsf{Agg}(\mathsf{crs}, \{\mathsf{pk}_i, y_i\}_{i\in[L]})$**:** It takes crs, a set of pairs pk_i, and $y_i \in \mathcal{Y}_\kappa$ for $i \in [L]$ as input, and outputs a master public key mpk and a set of helper keys hsk_i for $i \in [L]$. This algorithm is deterministic.

$\mathsf{Enc}(\mathsf{mpk}, x, M)$**:** It takes mpk, $x \in \mathcal{X}_\kappa$, and a message $M \in \mathcal{M}$ as inputs, and outputs a ciphertext ct_x.

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_x)$**:** It takes $\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_x$ as input, and outputs a message M or a symbol $\perp$.

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

$$\Pr[\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i) = 1 : \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, \kappa); (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)] = 1$$

Correctness. For all $\lambda, L \in \mathbb{N}, i \in [L], \kappa, \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, \kappa)$, $\{\mathsf{pk}_j\}_{j\in[L]\setminus\{i\}}$ such that $\mathsf{Ver}(\mathsf{crs}, j, \mathsf{pk}_j) = 1$, $x \in \mathcal{X}_\kappa$, $y_1, \ldots, y_L \in \mathcal{Y}_\kappa$ such that $\mathsf{P}_\kappa(x, y_i) = 1$, and $M \in \mathcal{M}$, we have

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_x) = M \ : \begin{array}{l} (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Gen}(\mathsf{crs}, i) \\ (\mathsf{mpk}, \{\mathsf{hsk}_j\}_{j\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, \{\mathsf{pk}_j, y_j\}_j) \\ \mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, M) \end{array}\right] = 1$$

Compactness. For all $\lambda, L \in \mathbb{N}, \kappa, i \in [L]$, the sizes of mpk and hsk_i obtained from $\mathsf{Agg}(\mathsf{crs}, \{\mathsf{pk}_i, y_i\}_{i\in[L]})$ are $\mathsf{poly}(\lambda, \max_i |y_i|, \log L)$.

Security. For all stateful admissible adversaries $\mathcal{A}$, the following advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sRegABE}}(\lambda)$ is negligible in λ:

$$\Pr\left[\beta = \beta' \ : \begin{array}{l} L \leftarrow \mathcal{A}(1^\lambda);\ \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, 1^L, \kappa) \\ \{\mathsf{pk}_i^*, y_i\}_{i\in[L]}, x, M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{OGen}(\cdot),\mathsf{OCor}(\cdot)}(\mathsf{crs}) \\ (\mathsf{mpk}, \{\mathsf{hsk}_i\}_{i\in[L]}) \leftarrow \mathsf{Agg}(\mathsf{crs}, \{\mathsf{pk}_i^*, y_i\}_{i\in[L]}) \\ \beta \leftarrow \{0,1\};\ \mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, M_\beta);\ \beta' \leftarrow \mathcal{A}(\mathsf{ct}_x) \end{array}\right] - \frac{1}{2}$$

where $\mathcal{D}_i$ and $\mathcal{C}$ are dictionaries that are initially empty, $\mathsf{OGen}(i)$ runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\mathsf{crs}, i)$, set $\mathcal{D}_i = \mathcal{D}_i \cup \{(\mathsf{pk}, \mathsf{sk})\}$ and returns pk, and $\mathsf{OCor}(i, \mathsf{pk})$ returns sk if $(\mathsf{pk}, \mathsf{sk}) \in \mathcal{D}_i$ (returns $\perp$ otherwise) and set $\mathcal{C} = \mathcal{C} \cup \{(i, \mathsf{pk})\}$. $\mathcal{A}$ is admissible if its queries satisfy

$$(\mathsf{pk}_i^*, *) \notin \mathcal{D}_i \Rightarrow \mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}) = 1$$
$$(i, \mathsf{pk}_i^*) \in \mathcal{C} \vee (\mathsf{pk}_i^*, *) \notin \mathcal{D}_i \Rightarrow \mathsf{P}_\kappa(x, y_i) = 0$$

Definition 2.5 (Predicate Encodings [Wee14]). A (ω, n_c, n_k)-predicate encoding for $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ is the matrix system defined as follows. For every $x \in \mathcal{X}, y \in \mathcal{Y}$, there exist

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

which satisfy the following two properties:

Correctness: For all (x, y) such that $\mathsf{P}(x, y) = 1$, we have $\mathbf{M}_{x,y}\mathbf{d}_{x,y}^\top = (1, \mathbf{0})^\top$.

Security: For all (x, y) such that $\mathsf{P}(x, y) = 0$ and $\alpha \in \mathbb{Z}_p$, the following distributions are statistically close over $\mathbf{w} \leftarrow \mathbb{Z}_p^\omega$:

$$\{\alpha, \mathbf{M}_{x,y}, (\alpha, \mathbf{w})\mathbf{M}_{x,y}\} \quad \text{and} \quad \{\alpha, \mathbf{M}_{x,y}, (0, \mathbf{w})\mathbf{M}_{x,y}\}$$

Lemma 2.1. *For any (ω, n_c, n_k)-predicate encoding for $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, we can construct $(\omega + 2, n_c + 1, n_k + 1)$-predicate encoding for also P such that $\mathbf{a}_y = (1, \mathbf{0}) \in \mathbb{Z}_p^{n_k+1}$ for all $y \in \mathcal{Y}$. We can obtain such a predicate encoding by applying the dual conversion [ABS17] to the original predicate encoding twice.*

3 Pair Encoding Schemes for sReg-ABE

We define pair encoding schemes (PES) suitable for sReg-ABE, which is majorly modified from the original PES for vanilla ABE as explained in §1.2

Definition 3.1 (Pair Encoding Schemes). Let $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$ be a predicate family. A PES for P_κ is given by six deterministic polynomial-time algorithms:

- $\mathsf{Param}(\kappa) \to \omega$. When given κ as input, Param outputs $\omega \in \mathbb{N}$ that specifies the number of *common* variables, which we denote by $\mathbf{w} = (w_1, \ldots, w_\omega)$.
- $\mathsf{CVEncC}(x, \mathsf{aux}_c) \to (n_1, n_2, \widehat{\mathbf{F}}, \widehat{\mathbf{C}})$. On input $x \in \mathcal{X}_\kappa$ and auxiliary information $\mathsf{aux}_c \in \{0,1\}^*$, it outputs a symbol $\perp$ or a matrix of polynomials $\widehat{\mathbf{C}} = (\hat{c}_{\nu,\mu})_{(\nu,\mu)\in[n_1]\times[n_2]}$ in common variables $\mathbf{w}$ as follows, where $\widehat{\mathbf{F}} \in \mathbb{Z}_p^{n_1\omega\times n_2}$:
$$\widehat{\mathbf{C}}(\mathbf{w}) = (\mathbf{I}_{n_1} \otimes \mathbf{w})\widehat{\mathbf{F}}$$
- $\mathsf{CVEncK}(y, \mathsf{aux}_k) \to (m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}})$. On input $y \in \mathcal{Y}_{(\kappa)}$ and $\mathsf{aux}_k \in \{0,1\}^*$, it outputs a symbol $\perp$ or a matrix of polynomials $\widehat{\mathbf{K}} = (\hat{k}_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[m_2]}$ in common variables $\mathbf{w}$ as follows, where $\widehat{\mathbf{L}} \in \mathbb{Z}_p^{m_1\omega\times m_2}$:
$$\widehat{\mathbf{K}}(\mathbf{w}) = (\mathbf{I}_{m_1} \otimes \mathbf{w})\widehat{\mathbf{L}}$$
- $\mathsf{EncC}(x, m_1, \mathsf{aux}_c) \to (n_3, \mathbf{F}, \mathbf{C})$. On input $m_1 \in \mathbb{N}$, $x \in \mathcal{X}_\kappa$, and aux_c, EncC outputs a symbol $\perp$ or a ciphertext encoding $\mathbf{C} = (c_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_2]}$ where $\mathbf{C}$ is a matrix of polynomials in *non-lone* variables $\mathbf{S} = (s_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_1]}$, *lone* variables $\mathbf{T} = (t_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_3]}$, and common variables $\mathbf{w}$ as follows, where $\mathbf{F} \in \mathbb{Z}_p^{n_3\times n_2}$ is a matrix independent of m_1, $\widehat{\mathbf{C}}$ is the output of $\mathsf{CVEncC}(x, \mathsf{aux}_c)$:
$$\mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w}) = \mathbf{T}\mathbf{F} + \mathbf{S}\widehat{\mathbf{C}}(\mathbf{w})$$
- $\mathsf{EncK}(y, n_1, \mathsf{aux}_k) \to (m_3, \mathbf{L}, \mathbf{K})$. On input $n_1 \in \mathbb{N}$, $y \in \mathcal{Y}_\kappa$, and aux_k, EncK outputs a symbol $\perp$ or a key encoding $\mathbf{K} = (k_{\nu,\mu})_{(\nu,\mu)\in[n_1]\times[m_2]}$ where $\mathbf{K}$ is a matrix of polynomials in *non-lone* variables $\mathbf{S} = (s_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_1]}$, *lone* variables $\mathbf{U} = (u_{\nu,\mu})_{(\nu,\mu)\in[n_1]\times[m_3]}$ and common variables $\mathbf{w}$ as follows, where $\mathbf{L} \in \mathbb{Z}_p^{m_3\times m_2}$ is a matrix independent of n_1, $\widehat{\mathbf{K}}$ is the output of $\mathsf{CVEncK}(y)$:
$$\mathbf{K}(\mathbf{S}, \mathbf{U}, \mathbf{w}) = \mathbf{U}\mathbf{L} + \mathbf{S}^\top\widehat{\mathbf{K}}(\mathbf{w})$$
- $\mathsf{Pair}(x, y, \mathsf{aux}_c, \mathsf{aux}_k) \to (\mathbf{E}, \overline{\mathbf{E}})$. On input $x, y, \mathsf{aux}_c, \mathsf{aux}_k$, Pair outputs two matrices $\mathbf{E} \in \mathbb{Z}_p^{n_2\times m_1}, \overline{\mathbf{E}} \in \mathbb{Z}_p^{m_2\times n_1}$.

Second Inputs to EncC and EncK. We assume that the second inputs m_1 and n_1 to EncC and EncK, respectively, only affect the sizes of the variable matrices $\mathbf{T}, \mathbf{U}, \mathbf{S}$, and do not affect $\mathbf{L}$ or whether they output $\perp$ or not.

Notations for PES. In the outputs of $\mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{EncC}, \mathsf{EncK}$, we sometimes omit the coefficient matrices $\widehat{\mathbf{F}}, \widehat{\mathbf{L}}, \mathbf{F}, \mathbf{L}$, respectively, (e.g., $(n_1, n_2, \mathbf{C}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$) if they are not necessary in the context. In contrast, when we need only the coefficient matrix $\mathbf{F}, \mathbf{L}$, which is independent of m_1, n_1, we use the notation like $(n_3, \mathbf{F}) \leftarrow \mathsf{EncC}(x, \mathsf{aux}_c)$.

Validity. We say aux_c is valid with respect to x if $\perp \not\leftarrow \mathsf{EncC}(x, \mathsf{aux}_c)$. A PES for $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$ is ciphertext valid if for all $x \in \mathcal{X}_\kappa$, there exists an efficiently computable valid aux_c with respect to x. Similarly, the PES is key valid if for all $y \in \mathcal{Y}_\kappa$, there exists an efficiently computable valid aux_k with respect to y. We say the PES is valid if it is ciphertext valid and key valid.

Correctness. A PES is correct if for every κ, $(x, y) \in \mathcal{X}_\kappa \times \mathcal{Y}_\kappa$ such that $\mathsf{P}_\kappa(x, y) = 1$, and valid $\mathsf{aux}_c, \mathsf{aux}_k$ with respect to x, y, respectively, the following holds symbolically:
$$\mathsf{tr}(\mathbf{E}\mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w})) + \mathsf{tr}(\overline{\mathbf{E}}\mathbf{K}(\mathbf{S}, \mathbf{U}, \mathbf{w})) = u_{1,1}$$
where $(n_1, n_2, \widehat{\mathbf{F}}, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$, $(m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y, \mathsf{aux}_k)$, $(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c)$, $(m_3, \mathbf{L}, \mathbf{K}) \leftarrow \mathsf{EncK}(y, n_1, \mathsf{aux}_k)$.

3.1 Evaluating PES with Vectors/Matrices

We can evaluate ciphertext encoding $\mathbf{C}(\mathbf{S},\mathbf{T},\mathbf{w})$ and key encoding $\mathbf{K}(\mathbf{S},\mathbf{U},\mathbf{w})$ together with matrices $\widehat{\mathbf{C}}(\mathbf{w}),\widehat{\mathbf{K}}(\mathbf{w})$ with the following substitution from scalar variables to vectors/matrices over $\mathbb{Z}_p$: for all $d,d'\in\mathbb{N}$, $s_{\nu,\mu}\mapsto\mathbf{s}_{\nu,\mu}\in\mathbb{Z}_p^d$, $t_{\nu,\mu}\mapsto\mathbf{t}_{\nu,\mu}\in\mathbb{Z}_p^{d'}$, $u_{\nu,\mu}\mapsto\mathbf{u}_{\nu,\mu}\in\mathbb{Z}_p^{d'}$, $w_\ell\mapsto\mathbf{W}_\ell\in\mathbb{Z}_p^{d\times d'}$. Then, for $\overline{\mathbf{S}}=(\mathbf{s}_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_1]}$, $\overline{\mathbf{T}}=(\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_3]}$, $\overline{\mathbf{U}}=(\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n_1]\times[m_3]}$, $\mathbf{W}=(\mathbf{W}_1||\cdots||\mathbf{W}_\omega)$, we define

$$\begin{aligned}
\widehat{\mathbf{C}}(\mathbf{W})&=(\mathbf{I}_{n_1}\otimes\mathbf{W})(\widehat{\mathbf{F}}\otimes\mathbf{I}_{d'})\in\mathbb{Z}_p^{dn_1\times d'n_2}\\
\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}},\mathbf{W})&=\overline{\mathbf{T}}(\mathbf{F}\otimes\mathbf{I}_{d'})+\overline{\mathbf{S}}\widehat{\mathbf{C}}(\mathbf{W})\in\mathbb{Z}_p^{m_1\times d'n_2}\\
\widehat{\mathbf{K}}(\mathbf{W})&=(\mathbf{I}_{m_1}\otimes\mathbf{W})(\widehat{\mathbf{L}}\otimes\mathbf{I}_{d'})\in\mathbb{Z}_p^{dm_1\times d'm_2}\\
\mathbf{K}(\overline{\mathbf{S}},\overline{\mathbf{U}},\mathbf{W})&=\overline{\mathbf{U}}(\mathbf{L}\otimes\mathbf{I}_{d'})+\overline{\mathbf{S}}^{\mathsf{BT}}\widehat{\mathbf{K}}(\mathbf{W})\in\mathbb{Z}_p^{n_1\times d'm_2}
\end{aligned}\tag{7}$$

Note that $\widehat{\mathbf{C}}$ and $\widehat{\mathbf{K}}$ can be efficiently computed over group elements since they are linear in $\mathbf{W}$, *e.g.*, $\widehat{\mathbf{C}}([\mathbf{W}]_1)=[(\mathbf{I}_{n_1}\otimes\mathbf{W})(\widehat{\mathbf{F}}\otimes\mathbf{I}_{d'})]_1$ can be efficiently computed given $[\mathbf{W}]_1$.

Properties. We show several properties of PES over vectors/matrices that we will use in the ABE construction. The following properties hold for all $(x,y)\in\mathcal{X}_\kappa\times\mathcal{Y}_\kappa$, where $\widehat{\mathbf{C}},\mathbf{C}$ and $\widehat{\mathbf{K}},\mathbf{K}$ are obtained from x and y with valid aux_c and aux_k via the PES algorithms, respectively.

Property 3.1. For any fixed $\overline{\mathbf{S}}$, $\widehat{\mathbf{C}}$ is linear in $\mathbf{W}$, and $\mathbf{C}$ is linear in $(\overline{\mathbf{T}},\mathbf{W})$, that is, for any $\overline{\mathbf{T}}_1,\overline{\mathbf{T}}_2,\mathbf{W}_1,\mathbf{W}_2$ we have

$$\begin{aligned}
\widehat{\mathbf{C}}(\mathbf{W}_1)+\widehat{\mathbf{C}}(\mathbf{W}_2)&=\widehat{\mathbf{C}}(\mathbf{W}_1+\mathbf{W}_2)\\
\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}}_1,\mathbf{W}_1)+\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}}_2,\mathbf{W}_2)&=\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}}_1+\overline{\mathbf{T}}_2,\mathbf{W}_1+\mathbf{W}_2)
\end{aligned}$$

Similarly, $\widehat{\mathbf{K}}$ and $\mathbf{K}$ are linear in $\mathbf{W}$ and $(\overline{\mathbf{U}},\mathbf{W})$, respectively. This property is obvious from Eq. (7).

Property 3.2. For all $\ell\in\mathbb{N}$, $\mathbf{M}\in\mathbb{Z}_p^{d'\times\ell}$, we have

$$\begin{aligned}
\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}},\mathbf{W})(\mathbf{I}_{n_2}\otimes\mathbf{M})&=\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}}(\mathbf{I}_{n_3}\otimes\mathbf{M}),\mathbf{W}(\mathbf{I}_\omega\otimes\mathbf{M}))\\
\mathbf{K}(\overline{\mathbf{S}},\overline{\mathbf{U}},\mathbf{W})(\mathbf{I}_{m_2}\otimes\mathbf{M})&=\mathbf{K}(\overline{\mathbf{S}},\overline{\mathbf{U}}(\mathbf{I}_{m_3}\otimes\mathbf{M}),\mathbf{W}(\mathbf{I}_\omega\otimes\mathbf{M}))
\end{aligned}$$

This property can be shown as follows (the case for $\mathbf{K}$ is similar).

$$\begin{aligned}
&\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}},\mathbf{W})(\mathbf{I}_{n_2}\otimes\mathbf{M})\\
=&(\overline{\mathbf{T}}(\mathbf{F}\otimes\mathbf{I}_{d'})+\overline{\mathbf{S}}(\mathbf{I}_{n_1}\otimes\mathbf{W})(\widehat{\mathbf{F}}\otimes\mathbf{I}_{d'}))(\mathbf{I}_{n_2}\otimes\mathbf{M})\\
=&\overline{\mathbf{T}}(\mathbf{I}_{n_3}\otimes\mathbf{M})(\mathbf{F}\otimes\mathbf{I}_\ell)+\overline{\mathbf{S}}(\mathbf{I}_{n_1}\otimes\mathbf{W})(\mathbf{I}_{n_1\omega}\otimes\mathbf{M})(\widehat{\mathbf{F}}\otimes\mathbf{I}_\ell)\\
=&\overline{\mathbf{T}}(\mathbf{I}_{n_3}\otimes\mathbf{M})(\mathbf{F}\otimes\mathbf{I}_\ell)+\overline{\mathbf{S}}(\mathbf{I}_{n_1}\otimes\mathbf{W})(\mathbf{I}_{n_1}\otimes\mathbf{I}_\omega\otimes\mathbf{M})(\widehat{\mathbf{F}}\otimes\mathbf{I}_\ell)\\
=&\overline{\mathbf{T}}(\mathbf{I}_{n_3}\otimes\mathbf{M})(\mathbf{F}\otimes\mathbf{I}_\ell)+\overline{\mathbf{S}}(\mathbf{I}_{n_1}\otimes\mathbf{W}(\mathbf{I}_\omega\otimes\mathbf{M}))(\widehat{\mathbf{F}}\otimes\mathbf{I}_\ell)\\
=&\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}}(\mathbf{I}_{n_3}\otimes\mathbf{M}),\mathbf{W}(\mathbf{I}_\omega\otimes\mathbf{M}))
\end{aligned}$$

Property 3.3. For all $\ell\in\mathbb{N}$, $\mathbf{M}\in\mathbb{Z}_p^{\ell\times d}$, we have

$$\overline{\mathbf{S}}(\mathbf{I}_{n_1}\otimes\mathbf{M})\widehat{\mathbf{C}}(\mathbf{W})=\mathbf{C}(\overline{\mathbf{S}},\mathbf{O},\mathbf{M}\mathbf{W}),\quad \overline{\mathbf{S}}'(\mathbf{I}_{m_1}\otimes\mathbf{M})\widehat{\mathbf{K}}(\mathbf{W})=\mathbf{K}(\overline{\mathbf{S}},\mathbf{O},\mathbf{M}\mathbf{W})$$

This property is obvious from Eq. (7).

Property 3.4. In the case $d'=1$ and $\mathsf{P}_\kappa(x,y)=1$, the following holds:

$$\mathsf{tr}(\mathbf{E}\mathbf{C}(\overline{\mathbf{S}},\overline{\mathbf{T}},\mathbf{W}))+\mathsf{tr}(\overline{\mathbf{E}}\mathbf{K}(\overline{\mathbf{S}},\overline{\mathbf{U}},\mathbf{W}))=u_{1,1}$$

where $\mathbf{E},\overline{\mathbf{E}}\leftarrow\mathsf{Pair}(x,y)$. This property is obvious from the correctness of PES since this is just substitution of variables: $s_{\nu,\mu}w_\ell\mapsto\mathbf{s}_{\nu,\mu}\mathbf{w}_\ell^\top$.

3.2 Properties of PES

We define two properties of PES, namely, well-formedness and key encoding indistinguishability ($\mathsf{KE\text{-}ind}$). When we construct a sReg-ABE scheme from PES, the former is necessary for compactness and correctness while the latter is for security of the resulting scheme.

Definition 3.2 (Key Well-formedness). We say that a PES $\Gamma = (\mathsf{Param}, \mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ for $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$ is key well-formed if it satisfies the following condition: for all polynomial-size $Y \subseteq \mathcal{Y}_\kappa$, there exist a string $\mathsf{aux}_k \in \{0,1\}^*$, positive integers $m_1, m_2, m_3 \in \mathbb{N}$, a matrix $\mathbf{L} \in \mathbb{Z}_p^{m_3 \times m_2}$, which are all efficiently computable, such that

$$|\mathsf{aux}_k|, |m_1|, |m_2| = \mathsf{poly}(\max_{y \in Y} |y|)$$

and that for all $y \in Y$, when we let $(m_1^{(y)}, m_2^{(y)}, \widehat{\mathbf{K}}^{(y)}) \leftarrow \mathsf{CVEncK}(y, \mathsf{aux}_k)$, $(m_3^{(y)}, \mathbf{L}^{(y)}) \leftarrow \mathsf{EncK}(y, \mathsf{aux}_k)$, we have that $m_1^{(y)} = m_1$, $m_2^{(y)} = m_2$, $m_3^{(y)} = m_3$ and $\mathbf{L}^{(y)} = \mathbf{L}$ (*i.e.,* all the respective parameters are the same among $y \in Y$).

This property requires that the size of aux_k, m_1, m_2 depend only on a single element (the one with maximum size) in Y; intuitively, looking ahead, the sizes of $\mathsf{mpk}, \mathsf{hsk}_i$ in sReg-ABE will involve these three parameters and hence need to be small. The property that the size of $\widehat{\mathbf{K}}^{(y)}$ and matrices $\mathbf{L}^{(y)}$ are the same for all $y \in \mathcal{Y}$ is needed for the correctness of sReg-ABE. We also define ciphertext well-formedness similarly; while this is not directly used in sReg-ABE, it will be useful when converting PES to its dual predicate.

Definition 3.3 (Ciphertext Well-formedness). A PES Γ for P_κ is ciphertext well-formed if it satisfies the following condition: for all polynomial-size $X \subseteq \mathcal{X}_\kappa$, there exist a string $\mathsf{aux}_c \in \{0,1\}^*$, positive integers $n_1, n_2, n_3 \in \mathbb{N}$, a matrix $\mathbf{F} \in \mathbb{Z}_p^{n_3 \times n_2}$, which are all efficiently computable, such that

$$|\mathsf{aux}_c|, |n_1|, |n_2| = \mathsf{poly}(\max_{x \in X} |x|)$$

and that for all $x \in X$, when we let $(n_1^{(x)}, n_2^{(x)}, \widehat{\mathbf{C}}^{(x)}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$, $(n_3^{(x)}, \mathbf{F}^{(x)}) \leftarrow \mathsf{EncC}(x, \mathsf{aux}_c)$, we have that $n_1^{(x)} = n_1$, $n_2^{(x)} = n_2$, $n_3^{(x)} = n_3$ and $\mathbf{F}^{(x)} = \mathbf{F}$ (*i.e.,* all the respective parameters are the same among $x \in X$).

It is not hard to see that a PES is ciphertext (resp. key) valid as per Definition 3.1 if it is ciphertext (resp. key) well-formed.

$\mathsf{KE\text{-}ind}$ is a computational security notion of PES, which was originally defined to prove adaptive security of vanilla ABE schemes [AT20]. We adapt it to the sReg-ABE setting as follows.

Definition 3.4 (Key-Encoding indistinguishability). Let $\Gamma = (\mathsf{Param}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{Pair})$ be a PES for a predicate family $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$. We say that Γ satisfies Key-Encoding indistinguishability ($\mathsf{KE\text{-}ind}$) if the following holds. Consider a game $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ defined in Fig 1, in which an adversary $\mathcal{A}$ can query $\mathcal{O}$ at most once on $x \in \mathcal{X}_\kappa$ and $y \in \mathcal{Y}_\kappa$ such that $\mathsf{P}_\kappa(x,y) = 0$ together with varid $\mathsf{aux}_c, \mathsf{aux}_k$. Then, we have $\mathsf{G}_0^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{G}_1^{\mathsf{KE\text{-}ind}}$.

Lemma 3.1. *Predicate encodings (Definition 2.5) can be captured by PES, and PES constructed from predicate encodings satisfy ciphertext well-formedness, key well-formedness, and* $\mathsf{KE\text{-}ind}$.

Proof of Lemme 3.1. Given a (ω, n_c, n_k)-predicate encoding for $\mathsf{P} : \mathcal{X} \times \mathcal{Y}$, we construct a PES for P as follows. Since we do not use $\mathsf{aux}_c, \mathsf{aux}_k$ and $n_1 = m_1 = 1$ in the PES from predicate encodings, we omit them from inputs to the corresponding algorithms.

- $\mathsf{Param}() \to \omega$. It outputs ω, which specifies the common variables $\mathbf{w} = (w_1, \ldots, w_\omega)$.
- $\mathsf{CVEncC}(x) \to (n_1, n_2, \widehat{\mathbf{F}}, \widehat{\mathbf{C}})$. On input $x \in \mathcal{X}$, it outputs $(1, n_c, \mathbf{C}_x, \widehat{\mathbf{C}})$ where $\widehat{\mathbf{C}}(\mathbf{w}) = \mathbf{w}\mathbf{C}_x$.

```
$\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$
$\omega \leftarrow \mathsf{Param}(\kappa),\ \ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{a} \leftarrow \mathbb{Z}_p^{2k+1},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$
$\mathbf{a}^\perp \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{b}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{a}^\perp(\mathbf{A}^\top||\mathbf{a}^\top) = \mathbf{0},\ \mathbf{b}^\perp\mathbf{B} = \mathbf{0}$
$\mathbf{W} = (\mathbf{W}_1||\cdots||\mathbf{W}_\omega) \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)}$
$P = ([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{AW}]_1, [\mathbf{W}(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(P)$

$\mathcal{O}(\cdot)$
Input: $(x, y) \in \mathcal{X}_\kappa \times \mathcal{Y}_\kappa$ and valid $\mathsf{aux}_c, \mathsf{aux}_k$
$(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c),\ (m_1, m_2, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y, \mathsf{aux}_k)$
$(n_3, \mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w})) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c),\ (m_3, \mathbf{K}(\mathbf{S}, \mathbf{U}, \mathbf{w})) \leftarrow \mathsf{EncK}(y, n_1, \mathsf{aux}_k)$
$\mathbf{s}_{1,1}, \ldots, \mathbf{s}_{n_1,m_1} \leftarrow \mathbb{Z}_p^k,\ \mathbf{t}_{1,1}, \ldots, \mathbf{t}_{m_1,n_3}, \mathbf{u}_{\ell,2}, \ldots, \mathbf{u}_{\ell,m_3} \leftarrow \mathbb{Z}_p^{k+1}$ for $\ell \in [n_1]$
$\mathbf{u}_{1,1} = \beta\mathbf{b}^\perp,\ \mathbf{u}_{2,1} = \cdots = \mathbf{u}_{n_1,1} = \mathbf{0} \in \mathbb{Z}_p^{k+1}$
$\overline{\mathbf{S}}_{\mathbf{A}} = (\mathbf{s}_{\nu,\mu}\mathbf{A})_{(\nu,\mu)\in[m_1]\times[n_1]},\ \ \overline{\mathbf{T}} = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_3]},\ \ \overline{\mathbf{U}} = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n_1]\times[m_3]}$
Output: $[\overline{\mathbf{S}}_{\mathbf{A}},\ \mathbf{C}(\overline{\mathbf{S}}_{\mathbf{A}}, \overline{\mathbf{T}}, \mathbf{W}),\ \mathbf{K}(\overline{\mathbf{S}}_{\mathbf{A}}, \overline{\mathbf{U}}, \mathbf{W})]_1$
```

Fig 1. KE-ind game.

- $\mathsf{CVEncK}(y) \to (m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}})$. On input $y \in \mathcal{Y}$, it outputs $(1, n_k, \mathbf{K}_y, \widehat{\mathbf{K}})$ where $\widehat{\mathbf{K}}(\mathbf{w}) = \mathbf{w}\mathbf{K}_y$.
- $\mathsf{EncC}(x) \to (n_3, \mathbf{F}, \mathbf{C})$. On input $x \in \mathcal{X}$, it outputs $(1, \mathbf{0}, \mathbf{C})$ where $\mathbf{C}(s, t, \mathbf{w}) = s\widehat{\mathbf{C}}(\mathbf{w})$.
- $\mathsf{EncK}(y) \to (m_3, \mathbf{L}, \mathbf{K})$. On input $y \in \mathcal{Y}$, it outputs $(1, \mathbf{a}_y, \mathbf{K})$ where $\mathbf{K}(s, u, \mathbf{w}) = u\mathbf{a}_y + s\widehat{\mathbf{K}}(\mathbf{w})$.
- $\mathsf{Pair}(x, y, \mathsf{aux}_c, \mathsf{aux}_k) \to (\mathbf{E}, \overline{\mathbf{E}})$. On input x, y, Pair outputs $(\underline{\mathbf{d}}_{x,y}^\top \in \mathbb{Z}_p^{n_c\times 1}, \overline{\mathbf{d}}_{x,y}^\top \in \mathbb{Z}_p^{n_k\times 1})$ where $\underline{\mathbf{d}}_{x,y}^\top$ and $\overline{\mathbf{d}}_{x,y}^\top$ are vectors consisting of the last n_c elements and the first n_k elements of $\mathbf{d}_{x,y}$, respectively.
- **Correctness:** We have

$$\mathsf{tr}(\underline{\mathbf{d}}_{x,y}^\top s\widehat{\mathbf{C}}(\mathbf{w})) + \mathsf{tr}(\overline{\mathbf{d}}_{x,y}^\top(u\mathbf{a}_y + s\widehat{\mathbf{K}}(\mathbf{w}))) = s\mathbf{w}\mathbf{C}_x\underline{\mathbf{d}}_{x,y}^\top + (u\mathbf{a}_y + s\mathbf{w}\mathbf{K}_y)\overline{\mathbf{d}}_{x,y}^\top = u$$

  where the second equality follows from the correctness of predicate encodings.

In the above construction, we can observe that $n_1 = 1, n_2 = n_c, \mathbf{F} = \mathbf{0}$ for all $x \in \mathcal{X}$, and $m_1 = 1, m_2 = n_k, \mathbf{F} = \mathbf{a}_y$ for all $y \in \mathcal{Y}$. Hence, by apply Lemma 2.1, we can always obtain a PES from a predicate encoding that satisfies key and ciphertext well-formedness.

Next, we show that the above PES satisfies $\mathsf{KE\text{-}ind}$. In the $\mathsf{KE\text{-}ind}$ game for the above PES construction, $\mathcal{A}$ is given P described in Fig 1 and

$$[\mathbf{sA}, \mathbf{sAW}(\mathbf{C}_x \otimes \mathbf{I}_{k+1}), \beta\mathbf{b}^\perp(\mathbf{a}_y \otimes \mathbf{I}_{k+1}) + \mathbf{sAW}(\mathbf{K}_y \otimes \mathbf{I}_{k+1})]_1 \tag{8}$$

as the reply of $\mathcal{O}((x, y))$ such that $\mathsf{P}(x, y) = 0$. What we need to prove is that the elements in Definition 2.5 for $\beta = 0$ and $\beta = 1$ are indistinguishable. To this end, we consider a hybrid H_β where we change the reply of $\mathcal{O}((x, y))$ as

$$[\mathbf{c}, \mathbf{cW}(\mathbf{C}_x \otimes \mathbf{I}_{k+1}), \beta\mathbf{b}^\perp(\mathbf{a}_y \otimes \mathbf{I}_{k+1}) + \mathbf{cW}(\mathbf{K}_y \otimes \mathbf{I}_{k+1})]_1$$

where $\mathbf{c} \leftarrow \mathsf{span}((\begin{smallmatrix}\mathbf{A}\\ \mathbf{a}\end{smallmatrix}))$. We prove $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_\beta$ and $\mathsf{H}_0 \approx_s \mathsf{H}_1$.

$\underline{\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_\beta}$**.** Since all elements that $\mathcal{A}$ obtains (i.e., P and Eq. (8)) in $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ and H_β are affine in $\mathbf{A}, \mathbf{a}, \mathbf{a}^\perp, \mathbf{sA}, \mathbf{c}$, it suffices to show that the following distributions are indistinguishable:

$$\{[\mathbf{A}]_1, \mathbf{a}, \mathbf{a}^\perp, [\mathbf{c}_0]_1\} \approx_c \{[\mathbf{A}]_1, \mathbf{a}, \mathbf{a}^\perp, [\mathbf{c}_1]_1\} \tag{9}$$

where $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{a}, \mathbf{a}^\perp \leftarrow \mathbb{Z}_p^{2k+1}$ conditioned on $\mathbf{a}^\perp(\mathbf{A}^\top||\mathbf{a}^\top) = \mathbf{0}$ and $\mathbf{c}_0 \leftarrow \mathsf{span}(\mathbf{A}), \mathbf{c}_1 \leftarrow \mathsf{span}((\begin{smallmatrix}\mathbf{A}\\ \mathbf{a}\end{smallmatrix}))$. We show that the above indistinguishability under the MDDH assumption. Given an MDDH instance $([\mathbf{M}]_1, [\mathbf{z}_\beta]_1)$ where $\mathbf{M} \leftarrow \mathbb{Z}_p^{k\times(k+1)}, \mathbf{r} \leftarrow \mathbb{Z}_p^k, \mathbf{z}_0 = \mathbf{rM}, \mathbf{z}_1 \leftarrow \mathbb{Z}_p^{k+1}$, the reduction algorithm samples $\mathbf{X} \leftarrow \mathbb{Z}_p^{(2k+1)\times(2k+1)}$ where $\mathbf{X}$ is invertible with overwhelming probability and computes

$$[\mathbf{A}]_1 = [(\mathbf{M}||\mathbf{O})]_1\mathbf{X}, \quad \mathbf{a} = (\underbrace{0,\ldots,0}_{k},1,\underbrace{0,\ldots,0}_{k})\mathbf{X}, \quad \mathbf{a}^\perp = (\underbrace{0,\ldots,0}_{2k},1)(\mathbf{X}^{-1})^\top$$
$$[\mathbf{c}_\beta]_1 = [\mathbf{z}_\beta]_1\mathbf{X}$$

Then, the distribution of these elements is statistically close to that in Eq. (9) since the rows of $\mathbf{M}$ and $(\underbrace{0,\ldots,0}_{k},1)$ forms a basis of $\mathbb{Z}_p^{k+1}$ with overwhelming probability.

$\underline{\mathsf{H}_0 \approx_s \mathsf{H}_1.}$ We redefine $\mathbf{W} = \mathbf{W}' + \tilde{\mathbf{a}}^{\perp\top}(\mathbf{w}\otimes\mathbf{b}^\perp)$ where $\mathbf{W}' \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)}$, $\mathbf{w} \leftarrow \mathbb{Z}_p^\omega$ and $\tilde{\mathbf{a}}^\perp \in \mathbb{Z}_p^{2k+1}$ be a vector satisfying $\tilde{\mathbf{a}}^\perp\mathbf{A}^\top = \mathbf{0}, \tilde{\mathbf{a}}^\perp\mathbf{c}^\top = 1$. It is not hard to see that the distribution of $\mathbf{W}$ is not changed by the new definition. Then related terms can be written as follows: $\mathbf{AW} = \mathbf{AW}'$, $\mathbf{W}(\mathbf{I}_\omega\otimes\mathbf{B}) = \mathbf{W}'(\mathbf{I}_\omega\otimes\mathbf{B})$ in P and

$$\mathbf{cW}(\mathbf{C}_x\otimes\mathbf{I}_{k+1}) = \mathbf{cW}'(\mathbf{C}_x\otimes\mathbf{I}_{k+1}) + \mathbf{wC}_x\otimes\mathbf{b}^\perp$$
$$\beta\mathbf{b}^\perp(\mathbf{a}_y\otimes\mathbf{I}_{k+1}) + \mathbf{cW}(\mathbf{K}_y\otimes\mathbf{I}_{k+1}) = \mathbf{cW}'(\mathbf{K}_y\otimes\mathbf{I}_{k+1}) + (\beta\mathbf{a}_y + \mathbf{wK}_y)\otimes\mathbf{b}^\perp$$

in the reply from $\mathcal{O}((x,y))$ in H_β. The security of predicate encodings asserts that

$$(\mathbf{C}_x, \mathbf{K}_y, \mathbf{wC}_x, \mathbf{wK}_y) \approx_s (\mathbf{C}_x, \mathbf{K}_y, \mathbf{wC}_x, \mathbf{a}_y + \mathbf{wK}_y)$$

which readily implies $\mathsf{H}_0 \approx_s \mathsf{H}_1$. □

4 Predicate Transformations

We present seven transformations for predicates, which enable us to construct PES for more expressive predicates from simple ones. We summarize transformation efficiency in §4.8. We prove that these transformations preserves KE-ind and (partially) well-formedness, which is given in §C. Specifically, we can classify them into three types with respect to how they preserve well-formedness:

1. both key and ciphertext well-formedness are preserved (§4.1 to 4.5);
2. key and ciphertext well-formedness are switched (§4.6);
3. only ciphertext well-formedness is preserved (§4.7).

4.1 Addition of Null Attribute

Definition 4.1 (Addition of Null Attribute). The predicate obtained by adding the null key-attribute to a predicate $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$, denoted by $\mathsf{Null}[\mathsf{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$, where $\bar{\mathcal{X}}_\kappa = \mathcal{X}_\kappa$ and $\bar{\mathcal{Y}}_\kappa = \mathcal{Y}_\kappa \cup \{\mathsf{null}\}$, is defined by

$$\mathsf{Null}[\mathsf{P}_\kappa](x,y) = 1 \Leftrightarrow y \neq \mathsf{null} \wedge \mathsf{P}_\kappa(x,y) = 1, \quad |\mathsf{null}| = \min_{y\in\mathcal{Y}_\kappa} |y|.$$

PES for $\mathsf{Null}[\mathsf{P}_\kappa]$. Let $\mathit{\Gamma} = (\mathsf{Param}, \mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ be a PES for P_κ. We construct a PES for $\mathsf{Null}[\mathsf{P}_\kappa]$, denoted by $\mathsf{Null\text{-}Trans}(\mathit{\Gamma}) = (\mathsf{Param}', \mathsf{CVEncC}', \mathsf{CVEncK}', \mathsf{EncC}', \mathsf{EncK}', \mathsf{Pair}')$ as follows.

- $\mathsf{Param}'(\kappa) \to \omega'$: Run $\omega \leftarrow \mathsf{Param}(\kappa)$ and output $\omega' = \omega + 1$. This specifies common variables $\mathbf{w}' = (w_0, w_1, \ldots, w_\omega)$, where w_0 is a new common variable. In what follows, we denote $(w_1, \ldots, w_\omega)$ by $\mathbf{w}$.

- $\mathsf{CVEncC}'(x, \mathsf{aux}_c) \to (n_1', n_2', \widehat{\mathbf{F}}', \widehat{\mathbf{C}}')$: Run $(n_1, n_2, \widehat{\mathbf{F}}, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$. Output $(n_1', n_2', \widehat{\mathbf{F}}', \widehat{\mathbf{C}}')$ where $n_1' = n_1$, $n_2' = n_2$, and
$$\widehat{\mathbf{C}}'(\mathbf{w}') = \widehat{\mathbf{C}}(\mathbf{w}).$$
It is not hard to see that there exists $\widehat{\mathbf{F}}' \in \mathbb{Z}_p^{n_1'\omega' \times n_2'}$ such that $\widehat{\mathbf{C}}'(\mathbf{w}') = (\mathbf{I}_{n_1'} \otimes \mathbf{w}')\widehat{\mathbf{F}}'$.
- $\mathsf{CVEncK}'(y, \mathsf{aux}_k) \to (m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$: If $y = \mathsf{null}$, retrieve $y' \in \mathcal{Y}_\kappa$ from aux_k (if $y' \in \mathcal{Y}_\kappa$ is not in aux_k, output $\perp$), run $(m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y', \mathsf{aux}_k)$, $(m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(y', \mathsf{aux}_k)$, and let $\bar{\mathbf{l}}$ be the first row of $\mathbf{L}$. Otherwise, run $(m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y, \mathsf{aux}_k)$. Output $(m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$ where $m_1' = m_1$, $m_2' = m_2$, and
$$\widehat{\mathbf{K}}'(\mathbf{w}') = \begin{cases} \widehat{\mathbf{K}}(\mathbf{w}) & (y \in \mathcal{Y}_\kappa) \\ \begin{pmatrix} w_0\bar{\mathbf{l}} \\ \mathbf{O} \end{pmatrix} & (y = \mathsf{null}) \end{cases} \in \mathbb{Z}_p^{m_1' \times m_2'}.$$
It is not hard to see that there exists $\widehat{\mathbf{L}}' \in \mathbb{Z}_p^{m_1'\omega' \times m_2'}$ such that $\widehat{\mathbf{K}}'(\mathbf{w}') = (\mathbf{I}_{m_1'} \otimes \mathbf{w}')\widehat{\mathbf{L}}'$.
- $\mathsf{EncC}'(x, m_1', \mathsf{aux}_c) = \mathsf{EncC}(x, m_1', \mathsf{aux}_c)$, that is, $n_3' = n_3$, $\mathbf{F}' = \mathbf{F}$, $\mathbf{C}'(\mathbf{S}', \mathbf{T}', \mathbf{w}') = \mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w})$.
- $\mathsf{EncK}'(y, n_1', \mathsf{aux}_k) \to (m_3', \mathbf{L}', \mathbf{K}')$: If $y = \mathsf{null}$, retrieve $y' \in \mathcal{Y}_\kappa$ from aux_k ($y' \in \mathcal{Y}_\kappa$ is not in aux_k, output $\perp$), and redefine $y = y'$. Then, run $(m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}') \leftarrow \mathsf{CVEncK}'(y, \mathsf{aux}_k), (m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(y, \mathsf{aux}_k)$ and output $(m_3', \mathbf{L}', \mathbf{K}')$ where $m_3' = m_3$, $\mathbf{L}' = \mathbf{L}$, and
$$\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}') = \mathbf{U}'\mathbf{L}' + \mathbf{S}'^{\top}\widehat{\mathbf{K}}'(\mathbf{w}') \in \mathbb{Z}_p[\mathbf{S}', \mathbf{U}', \mathbf{w}']^{n_1' \times m_2'}.$$
- $\mathsf{Pair}'(x, y, \mathsf{aux}_c, \mathsf{aux}_k) \to (\mathbf{E}', \overline{\mathbf{E}}')$: If $y = \mathsf{null}$, output $\perp$. Otherwise, output $(\mathbf{E}', \overline{\mathbf{E}}') \leftarrow \mathsf{Pair}(x, y, \mathsf{aux}_c, \mathsf{aux}_k)$.
- **Correctness**: Since $\mathsf{P}_\kappa(x, y) = 1 \Rightarrow y \neq \mathsf{null}$, the correctness of Pair' follows from that of Pair.

4.2 Addition of Wild Card

Definition 4.2 (Addition of Wild Card). Let $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0, 1\}$ be a predicate such that for all $y \in \mathcal{Y}_\kappa$, there exists efficiently computable $x \in \mathcal{X}_\kappa$ satisfying $\mathsf{P}_\kappa(x, y) = 1$.[10] The predicate obtained by adding a wild card to $\mathcal{Y}_\kappa$, denoted by $\mathsf{WC}[\mathsf{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0, 1\}$, where $\bar{\mathcal{X}}_\kappa = \mathcal{X}_\kappa$ and $\bar{\mathcal{Y}}_\kappa = \mathcal{Y}_\kappa \cup \{*\}$, is defined by
$$\mathsf{WC}[\mathsf{P}_\kappa](x, y) = 1 \Leftrightarrow y = * \vee \mathsf{P}_\kappa(x, y) = 1, \quad |*| = \min_{y \in \mathcal{Y}_\kappa} |y|.$$

PES for $\mathsf{WC}[\mathsf{P}_\kappa]$. Let $\Gamma = (\mathsf{Param}, \mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ be a PES for P_κ. A PES for $\mathsf{WC}[\mathsf{P}_\kappa]$, denoted by $\mathsf{WC\text{-}Trans}(\Gamma) = (\mathsf{Param}', \mathsf{CVEncC}', \mathsf{CVEncK}', \mathsf{EncC}', \mathsf{EncK}', \mathsf{Pair}')$ is the same as Γ except that $\mathsf{CVEncK}', \mathsf{EncK}', \mathsf{Pair}'$ are defined as follows.

- $\mathsf{CVEncK}'(y, \mathsf{aux}_k) \to (m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$: Run $(m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y, \mathsf{aux}_k)$ if $y \in \mathcal{Y}_\kappa$. Otherwise, retrieve $y' \in \mathcal{Y}_\kappa$ from aux_k (if $y' \in \mathcal{Y}_\kappa$ is not in aux_k, output $\perp$), run $(m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y', \mathsf{aux}_k)$. Output $(m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$ where $m_1' = m_1$, $m_2' = m_2$, and
$$\widehat{\mathbf{K}}'(\mathbf{w}) = \begin{cases} \widehat{\mathbf{K}}(\mathbf{w}) & (y \in \mathcal{Y}_\kappa) \\ \mathbf{O} & (y = *) \end{cases} \in \mathbb{Z}_p^{m_1' \times m_2'}$$
It is not hard to see that there exists $\widehat{\mathbf{L}}' \in \mathbb{Z}_p^{m_1'\omega' \times m_2'}$ such that $\widehat{\mathbf{K}}'(\mathbf{w}) = (\mathbf{I}_{m_1'} \otimes \mathbf{w})\widehat{\mathbf{L}}'$.

[10] If there exist $\{y\} \subseteq \mathcal{Y}_\kappa$ that do not satisfy this condition, just removing these attributes from $\mathcal{Y}_k$ suffices.

- $\mathsf{EncK}'(y, n'_1, \mathsf{aux}_k) \to (m'_3, \mathbf{L}', \mathbf{K}')$: If $y = *$, retrieve $y' \in \mathcal{Y}_\kappa$ from aux_k (if $y' \in \mathcal{Y}_\kappa$ is not in aux_k, output $\perp$), run $(m'_3, \mathbf{L}') = (m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(y', \mathsf{aux}_k)$, and output $(m'_3, \mathbf{L}', \mathbf{K}')$ where

  $$\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}) = \mathbf{U}'\mathbf{L} \in \mathbb{Z}_p[\mathbf{S}', \mathbf{U}', \mathbf{w}']^{n'_1 \times m'_2}$$

  In case of $y \in \mathcal{Y}_\kappa$, output $(m'_3, \mathbf{L}', \mathbf{K}') = (m_3, \mathbf{L}, \mathbf{K}) \leftarrow \mathsf{EncK}(y, n'_1, \mathsf{aux}_k)$.
- $\mathsf{Pair}'(x, y, \mathsf{aux}_c, \mathsf{aux}_k) \to (\mathbf{E}', \overline{\mathbf{E}}')$: If $y = *$, retrieve $y' \in \mathcal{Y}_\kappa$ from aux_k, choose x' such that $\mathsf{P}_\kappa(x', y') = 1$ (if $y' \in \mathcal{Y}_\kappa$ is not in aux_k, output $\perp$), run $(\mathbf{E}, \overline{\mathbf{E}}) \leftarrow \mathsf{Pair}(x', y', \mathsf{aux}_c, \mathsf{aux}_k)$ where the number of columns of $\mathbf{E}$ is m_1, the number of rows of $\overline{\mathbf{E}}$ is m_2 by letting $(m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y', \mathsf{aux}_k)$. Then, run $(n_1, n_2, \widehat{\mathbf{F}}, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$ and output $\mathbf{E}' = \mathbf{O} \in \mathbb{Z}_p^{n_2 \times m_1}$ and $\overline{\mathbf{E}}' = (\bar{\mathbf{e}}^\top || \mathbf{O}) \in \mathbb{Z}_p^{m_2 \times n_1}$, where $\bar{\mathbf{e}}$ is the first column of $\overline{\mathbf{E}}$. If $y \in \mathcal{Y}_\kappa$, output $(\mathbf{E}', \overline{\mathbf{E}}') = (\mathbf{E}, \overline{\mathbf{E}}) \leftarrow \mathsf{Pair}(x, y, \mathsf{aux}_c, \mathsf{aux}_k)$.
- **Correctness**: First, consider the case $y = *$. Let $\mathbf{C}, \mathbf{K}, \widehat{\mathbf{K}}, \mathbf{L}, \mathbf{E}, \overline{\mathbf{E}}$ be the PES matrices with respect to (x', y'). Due to the correctness of $\mathit{\Gamma}$, the following holds symbolically:

  $$\underbrace{\mathsf{tr}(\mathbf{E}\mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w}))}_{A} + \mathsf{tr}(\overline{\mathbf{E}}\mathbf{K}(\mathbf{S}, \mathbf{U}, \mathbf{w})) = A + \mathsf{tr}(\underbrace{\overline{\mathbf{E}}(\mathbf{U}\mathbf{L} + \mathbf{S}^\top \widehat{\mathbf{K}}(\mathbf{w}))}_{\mathbf{M}}) = u_{1,1}$$

  Observe that variable $u_{1,1}$ does not appear in A, and $\mathbf{M} = \bar{\mathbf{e}}^\top \mathbf{u}\mathbf{L} + \mathbf{M}'$ where $\mathbf{u}$ is the first row of $\mathbf{U}$ and $\mathbf{M}'$ is a matrix not including variable $u_{1,1}$. Hence, $\mathsf{tr}(\bar{\mathbf{e}}^\top \mathbf{u}\mathbf{L}) = u_{1,1}$ and $A + \mathsf{tr}(\mathbf{M}') = 0$ hold symbolically. Thus, recalling $\mathbf{E}' = \mathbf{O}$ and $\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}) = \mathbf{U}'\mathbf{L}$, we have

  $$\mathsf{tr}(\mathbf{E}'\mathbf{C}'(\mathbf{S}', \mathbf{T}', \mathbf{w})) + \mathsf{tr}(\overline{\mathbf{E}}'\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w})) = \mathsf{tr}((\bar{\mathbf{e}}^\top || \mathbf{O})\mathbf{U}'\mathbf{L}) = \mathsf{tr}(\bar{\mathbf{e}}^\top \mathbf{u}'\mathbf{L}) = u'_{1,1}$$

  where $\mathbf{u}'$ is the first row and $u'_{1,1}$ is the $(1,1)$-th element of $\mathbf{U}'$. In case of $y \in \mathcal{Y}_\kappa$, the correctness of Pair' directly follows from that of Pair.

Remark 4.1 (Null Attribute versus Wild Card). By applying $\mathsf{Null}, \mathsf{Dual}, \mathsf{WC}$ in an appropriate order, we can obtain a predicate $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0, 1\}$ where $\mathcal{X}_\kappa$ includes null while $\mathcal{Y}_\kappa$ includes $*$. Although we do not consider such a predicate in this paper, it is worth noting that the attribute added later is valid in our transformations. For instance, if null is added later, then $\mathsf{P}_\kappa(*, \mathsf{null}) = 0$.

4.3 Key-Policy Disjunction

Definition 4.3 (Key-Policy Disjunction). Let $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0, 1\}$ be a predicate where $\mathcal{Y}_\kappa$ contains null (if not, we can add null via the transformation in Section 4.1). The predicate for key-policy disjunction over a single predicate P_κ, denoted by $\mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0, 1\}$, where $\bar{\mathcal{X}}_\kappa = \mathcal{X}_\kappa$ and $\bar{\mathcal{Y}}_\kappa = \bigcup_{n \in \mathbb{N}} \mathit{\Phi}_n$, where $\mathit{\Phi}_n$ consists of all functions $\phi : [n] \to \mathcal{Y}_\kappa$, is defined as follows. For $x \in \bar{\mathcal{X}}_\kappa$ and $y = \phi \in \bar{\mathcal{Y}}_\kappa$, we define

$$\mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}_\kappa](x, \phi) = 1 \Leftrightarrow \bigvee_{i \in [n]} \mathsf{P}_\kappa(x, \phi(i)) = 1, \quad |\phi| = \sum_{i \in [n]} |\phi(i)|.$$

PES for $\mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}_\kappa]$. In the following construction, we use the following fact:

$$\mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}_\kappa](x, \phi) = 1 \Leftrightarrow \bigvee_{i \in [n]} \mathsf{P}_\kappa(x, \phi(i)) \vee \mathsf{P}_\kappa(x, \mathsf{null}) \vee \cdots \vee \mathsf{P}_\kappa(x, \mathsf{null}) = 1.$$

Let $\mathit{\Gamma} = (\mathsf{Param}, \mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ be a PES for P_κ. We construct a PES for $\mathsf{KP1}_{\mathsf{OR}}[\mathsf{P}_\kappa]$, denoted by $\mathsf{KP1}_{\mathsf{OR}}\text{-}\mathsf{Trans}(\mathit{\Gamma}) = (\mathsf{Param}', \mathsf{CVEncC}', \mathsf{CVEncK}', \mathsf{EncC}', \mathsf{EncK}', \mathsf{Pair}')$ as follows.

- $\mathsf{Param}'(\kappa) = \mathsf{Param}(\kappa)$, that is, $\omega' = \omega$ and $\mathbf{w}' = \mathbf{w}$.
- $\mathsf{CVEncC}'(x, \mathsf{aux}_c) = \mathsf{CVEncC}(x, \mathsf{aux}_c)$, that is, $n'_1 = n_1$, $n'_2 = n_2$, $\widehat{\mathbf{F}}' = \widehat{\mathbf{F}}$, $\widehat{\mathbf{C}}'(\mathbf{w}') = \widehat{\mathbf{C}}(\mathbf{w})$.

- $\mathsf{CVEncK}'(\phi, \mathsf{aux}_k) \to (m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$: Retrieve δ from aux_k. If $n > \delta$ outputs $\perp$. Run $(m_{i,1}, m_{i,2}, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}(\phi(i), \mathsf{aux}_k)$ for $i \in [n]$ and $(m_{i,1}, m_{i,2}, \widehat{\mathbf{L}}_i, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}(\mathsf{null}, \mathsf{aux}_k)$ for $i \in [n+1, \delta]$. Output $(m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$ where $m_1' = \sum_{i \in [\delta]} m_{i,1}$, $m_2' = \sum_{i \in [\delta]} m_{i,2}$, and

$$\widehat{\mathbf{K}}'(\mathbf{w}) = \begin{pmatrix} \widehat{\mathbf{K}}_1(\mathbf{w}) & & \\ & \ddots & \\ & & \widehat{\mathbf{K}}_\delta(\mathbf{w}) \end{pmatrix} \in \mathbb{Z}_p[\mathbf{w}]^{m_1' \times m_2'}.$$

  It is not hard to see that there exists $\widehat{\mathbf{L}}' \in \mathbb{Z}_p^{m_1'\omega' \times m_2'}$ such that $\widehat{\mathbf{K}}'(\mathbf{w}) = (\mathbf{I}_{m_1'} \otimes \mathbf{w})\widehat{\mathbf{L}}'$.
- $\mathsf{EncC}'(x, m_1', \mathsf{aux}_c) = \mathsf{EncC}(x, m_1', \mathsf{aux}_c)$, that is, $n_3' = n_3$, $\mathbf{F}' = \mathbf{F}$, $\mathbf{C}'(\mathbf{S}', \mathbf{T}', \mathbf{w}') = \mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w})$.
- $\mathsf{EncK}'(\phi, n_1', \mathsf{aux}_k) \to (m_3', \mathbf{L}', \mathbf{K}')$: Retrieve δ from aux_k. If $n > \delta$ outputs $\perp$. Run $(m_{i,3}, \mathbf{L}_i) \leftarrow \mathsf{EncK}(\phi(i), \mathsf{aux}_k)$ for $i \in [n]$ and $(m_{i,3}, \mathbf{L}_i) \leftarrow \mathsf{EncK}(\mathsf{null}, \mathsf{aux}_k)$ for $i \in [n+1, \delta]$. Let $\bar{\mathbf{l}}_i$ be the first row of $\mathbf{L}_i$, and $\underline{\mathbf{L}}_i$ be the submatrix of $\mathbf{L}_i$ obtained by removing the first row. Output $(m_3', \mathbf{L}', \mathbf{K}')$ where $m_3' = 1 + \sum_{i \in [\delta]}(m_{i,3} - 1)$, $\mathbf{L}' = \begin{pmatrix} \bar{\mathbf{l}}_1 & \cdots & \bar{\mathbf{l}}_\delta \\ \underline{\mathbf{L}}_1 & & \\ & \ddots & \\ & & \underline{\mathbf{L}}_\delta \end{pmatrix} \in \mathbb{Z}_p^{m_3' \times m_2'}$ and

$$\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}') = \mathbf{U}'\mathbf{L}' + \mathbf{S}'^{\top}\widehat{\mathbf{K}}'(\mathbf{w}') \in \mathbb{Z}_p[\mathbf{S}', \mathbf{U}', \mathbf{w}']^{n_1' \times m_2'}$$

- $\mathsf{Pair}'(x, \phi, \mathsf{aux}_c, \mathsf{aux}_k) \to (\mathbf{E}', \overline{\mathbf{E}}')$: Retrieve δ from aux_k. Let $i' \in [n]$ be an index such that $\mathsf{P}_\kappa(x, \phi(i')) = 1$. Run $(\mathbf{E}_{i'}, \overline{\mathbf{E}}_{i'}) \leftarrow \mathsf{Pair}(x, \phi(i'), \mathsf{aux}_c, \mathsf{aux}_k)$. Output $\mathbf{E}' = (\mathbf{E}_1 || \cdots || \mathbf{E}_\delta)$ and $\overline{\mathbf{E}}' = \begin{pmatrix} \overline{\mathbf{E}}_1 \\ \vdots \\ \overline{\mathbf{E}}_\delta \end{pmatrix}$ where $\mathbf{E}_i = \mathbf{O} \in \mathbb{Z}_p^{n_{i,2} \times m_{i,1}}$ and $\overline{\mathbf{E}}_i = \mathbf{O} \in \mathbb{Z}_p^{m_{i,2} \times n_{i,1}}$ for $i \in [\delta] \backslash \{i'\}$.
- **Correctness**: Let $\mathbf{T}_i$ and $\mathbf{S}_i$ be the i-th block of $\mathbf{T}'$ and $\mathbf{S}'$ of size $m_{i,1} \times n_3'$ and $m_{i,1} \times n_1'$, that is, $\mathbf{T}' = \begin{pmatrix} \mathbf{T}_1 \\ \vdots \\ \mathbf{T}_\delta \end{pmatrix}$ and $\mathbf{S}' = \begin{pmatrix} \mathbf{S}_1 \\ \vdots \\ \mathbf{S}_\delta \end{pmatrix}$, respectively, $\mathbf{U}' = (\mathbf{u}_0^{\top} || \mathbf{U}_1 || \cdots || \mathbf{U}_\delta)$ where the width of $\mathbf{U}_i$ for $i \in [\delta]$ is $m_{i,3}$. Then, we have

$$\begin{aligned} A &= \mathsf{tr}(\mathbf{E}'\mathbf{C}'(\mathbf{S}', \mathbf{T}', \mathbf{w}')) = \mathsf{tr}\left(\mathbf{E}_{i'}(\mathbf{T}_{i'}\mathbf{F} + \mathbf{S}_{i'}\widehat{\mathbf{C}}(\mathbf{w}))\right) \\ B &= \mathsf{tr}(\overline{\mathbf{E}}'\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}')) \\ &= \mathsf{tr}\left(\overline{\mathbf{E}}'\left((\mathbf{u}_0^{\top} || \mathbf{U}_1)\mathbf{L}_1 + \mathbf{S}_1^{\top}\mathbf{K}(\mathbf{w}) || \cdots || (\mathbf{u}_0^{\top} || \mathbf{U}_\delta)\mathbf{L}_\delta + \mathbf{S}_\delta^{\top}\mathbf{K}(\mathbf{w})\right)\right) \\ &= \mathsf{tr}\left(\overline{\mathbf{E}}_{i'}((\mathbf{u}_0^{\top} || \mathbf{U}_{i'})\mathbf{L}_{i'} + \mathbf{S}_{i'}^{\top}\mathbf{K}(\mathbf{w}))\right). \end{aligned}$$

  Thanks to the correctness of Pair, we have $A + B = u_{1,1}$ where $u_{1,1}$ is the first element of $\mathbf{u}_0^{\top}$ as well as the $(1,1)$-th element of $\mathbf{U}'$.

4.4 Key-Policy Conjunction

Definition 4.4 (Key-Policy Conjunction). Let $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$ be a predicate such that $\mathcal{Y}_\kappa$ contains a wild card attribute $*$ (if not, we can add $*$ via the transformation in Section 4.2). The predicate for key-policy conjunction over a single predicate P_κ, denoted by $\mathsf{KP1}_{\mathsf{AND}}[\mathsf{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$, where $\bar{\mathcal{X}}_\kappa = \mathcal{X}_\kappa$ and $\bar{\mathcal{Y}}_\kappa = \bigcup_{n \in \mathbb{N}} \varPhi_n$, where $\varPhi_n$ consists of all functions $\phi : [n] \to \mathcal{Y}_\kappa$ is defined as follows. For $x \in \bar{\mathcal{X}}_\kappa$ and $y = \phi \in \bar{\mathcal{Y}}_\kappa$, we define

$$\mathsf{KP1}_{\mathsf{AND}}[\mathsf{P}_\kappa](x, \phi) = 1 \Leftrightarrow \bigwedge_{i \in [n]} \mathsf{P}_\kappa(x, \phi(i)) = 1, \quad |\phi| = \sum_{i \in [n]} |\phi(i)|.$$

PES for $\mathsf{KP1}_{\mathsf{AND}}[\mathsf{P}_\kappa]$. We use the following fact in the construction:

$$\mathsf{KP1}_{\mathsf{AND}}[\mathsf{P}_\kappa](x,\phi)=1 \Leftrightarrow \bigwedge_{i\in[n]} \mathsf{P}_\kappa(x,\phi(i)) \wedge \mathsf{P}_\kappa(x,*)\wedge\cdots\wedge \mathsf{P}_\kappa(x,*)=1$$

Let $\mathit{\Gamma}=(\mathsf{Param},\mathsf{CVEncC},\mathsf{CVEncK},\mathsf{EncC},\mathsf{EncK},\mathsf{Pair})$ be a PES for P_κ. We construct a PES for $\mathsf{KP1}_{\mathsf{AND}}[\mathsf{P}_\kappa]$, denoted by $\mathsf{KP1}_{\mathsf{AND}}\text{-}\mathsf{Trans}(\mathit{\Gamma})=(\mathsf{Param}',\mathsf{CVEncC}',\mathsf{CVEncK}',\mathsf{EncC}',\mathsf{EncK}',\mathsf{Pair}')$ as follows.

- $\mathsf{Param}'(\kappa)=\mathsf{Param}(\kappa)$, that is, $\omega'=\omega$ and $\mathbf{w}'=\mathbf{w}$.
- $\mathsf{CVEncC}'(x,\mathsf{aux}_c)=\mathsf{CVEncC}(x,\mathsf{aux}_c)$, that is, $n_1'=n_1$, $n_2'=n_2$, $\widehat{\mathbf{F}}'=\widehat{\mathbf{F}}$, $\widehat{\mathbf{C}}'(\mathbf{w}')=\widehat{\mathbf{C}}(\mathbf{w})$.
- $\mathsf{CVEncK}'(\phi,\mathsf{aux}_k)\to(m_1',m_2',\widehat{\mathbf{L}}',\widehat{\mathbf{K}}')$: Retrieve δ from aux_k. If $n>\delta$ outputs $\perp$. Run $(m_{i,1},m_{i,2},\widehat{\mathbf{K}}_i)\leftarrow\mathsf{CVEncK}(\phi(i),\mathsf{aux}_k)$ for $i\in[n]$ and $(m_{i,1},m_{i,2},\widehat{\mathbf{L}}_i,\widehat{\mathbf{K}}_i)\leftarrow\mathsf{CVEncK}(*,\mathsf{aux}_k)$ for $i\in[n+1,\delta]$. Output $(m_1',m_2',\widehat{\mathbf{L}}',\widehat{\mathbf{K}}')$ where $m_1'=\sum_{i\in[\delta]}m_{i,1}$, $m_2'=\sum_{i\in[\delta]}m_{i,2}$, and

$$\widehat{\mathbf{K}}'(\mathbf{w})=\begin{pmatrix}\widehat{\mathbf{K}}_1(\mathbf{w}) & & \\ & \ddots & \\ & & \widehat{\mathbf{K}}_\delta(\mathbf{w})\end{pmatrix}\in\mathbb{Z}_p[\mathbf{w}]^{m_1'\times m_2'}$$

  It is not hard to see that there exists $\widehat{\mathbf{L}}'\in\mathbb{Z}_p^{m_1'\omega'\times m_2'}$ such that $\widehat{\mathbf{K}}'(\mathbf{w})=(\mathbf{I}_{m_1'}\otimes\mathbf{w})\widehat{\mathbf{L}}'$.
- $\mathsf{EncC}'(x,m_1',\mathsf{aux}_c)=\mathsf{EncC}(x,m_1',\mathsf{aux}_c)$, that is, $n_3'=n_3$, $\mathbf{F}'=\mathbf{F}$, $\mathbf{C}'(\mathbf{S}',\mathbf{T}',\mathbf{w}')=\mathbf{C}(\mathbf{S},\mathbf{T},\mathbf{w})$.
- $\mathsf{EncK}'(\phi,n_1',\mathsf{aux}_k)\to(m_3',\mathbf{L}',\mathbf{K}')$: Retrieve δ from aux_k. If $n>\delta$ outputs $\perp$. Run $(m_{i,3},\mathbf{L}_i)\leftarrow\mathsf{EncK}(\phi(i),\mathsf{aux}_k)$ for $i\in[n]$ and $(m_{i,3},\mathbf{L}_i)\leftarrow\mathsf{EncK}(*,\mathsf{aux}_k)$ for $i\in[n+1,\delta]$. Let $\overline{\mathbf{l}}_i$ be the first row of $\mathbf{L}_i$, $\underline{\mathbf{L}}_i$ be the submatrix of $\mathbf{L}_i$ obtained by removing the first row, $\mathbf{m}_1=(1,\ldots,1)\in\mathbb{Z}_p^\delta$, and $\mathbf{m}_i=(0^{i-1},-1,0^{\delta-i})\in\mathbb{Z}_p^\delta$ for $i\in[2,\delta]$. Output $(m_3',\mathbf{L}',\mathbf{K}')$ where $m_3'=\sum_{i\in[\delta]}m_{i,3}$ and

$$\mathbf{L}'=\begin{pmatrix}\mathbf{m}_1^\top\overline{\mathbf{l}}_1 \cdots \mathbf{m}_\delta^\top\overline{\mathbf{l}}_\delta \\ \underline{\mathbf{L}}_1 \quad\quad\quad \\ \ddots \\ \quad\quad\quad \underline{\mathbf{L}}_\delta\end{pmatrix}\in\mathbb{Z}_p^{m_3'\times m_2'}$$

$$\mathbf{K}'(\mathbf{S}',\mathbf{U}',\mathbf{w}')=\mathbf{U}'\mathbf{L}'+\mathbf{S}'^\top\widehat{\mathbf{K}}'(\mathbf{w}')\in\mathbb{Z}_p[\mathbf{S}',\mathbf{U}',\mathbf{w}']^{n_1'\times m_2'}$$

- $\mathsf{Pair}'(x,\phi,\mathsf{aux}_c,\mathsf{aux}_k)\to(\mathbf{E}',\overline{\mathbf{E}}')$: Retrieve δ from aux_k. Let

$$\phi'(i)=\begin{cases}\phi(i) & (i\in[n])\\ * & (i\in[n+1,\delta])\end{cases}$$

  Run $(\mathbf{E}_i,\overline{\mathbf{E}}_i)\leftarrow\mathsf{Pair}(x,\phi'(i),\mathsf{aux}_c,\mathsf{aux}_k)$ for $i\in[\delta]$. Output $\mathbf{E}'=(\mathbf{E}_1||\cdots||\mathbf{E}_\delta)$ and $\overline{\mathbf{E}}'=\begin{pmatrix}\overline{\mathbf{E}}_1\\ \vdots\\ \overline{\mathbf{E}}_\delta\end{pmatrix}$.
- **Correctness**: Let $\mathbf{T}_i$ and $\mathbf{S}_i$ be the i-th block of $\mathbf{T}'$ and $\mathbf{S}'$ of size $m_{i,1}\times n_3'$ and $m_{i,1}\times n_1'$, that is, $\mathbf{T}'=\begin{pmatrix}\mathbf{T}_1\\ \vdots\\ \mathbf{T}_\delta\end{pmatrix}$ and $\mathbf{S}'=\begin{pmatrix}\mathbf{S}_1\\ \vdots\\ \mathbf{S}_\delta\end{pmatrix}$, respectively, $\mathbf{U}'=(\mathbf{U}_0||\mathbf{U}_1||\cdots||\mathbf{U}_\delta)$ where the width of $\mathbf{U}_0$ is δ and

that of $\mathbf{U}_i$ for $i \in [\delta]$ is $m_{i,3}$. Then, we have

$$\begin{aligned}
\mathsf{tr}(\mathbf{E}'\mathbf{C}'(\mathbf{S}', \mathbf{T}', \mathbf{w}')) &= \mathsf{tr}\left(\sum_{i\in[\delta]} \mathbf{E}_i(\mathbf{T}_i\mathbf{F} + \mathbf{S}_i\widehat{\mathbf{C}}(\mathbf{w}))\right) \\
&= \sum_{i\in[\delta]} \underbrace{\mathsf{tr}(\mathbf{E}_i(\mathbf{T}_i\mathbf{F} + \mathbf{S}_i\widehat{\mathbf{C}}(\mathbf{w})))}_{A_i} \\
\mathsf{tr}(\overline{\mathbf{E}}'\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}')) &= \mathsf{tr}\left(\overline{\mathbf{E}}'\left((\mathbf{U}_0\mathbf{m}_1^\top||\mathbf{U}_1)\mathbf{L}_1 + \mathbf{S}_1^\top\mathbf{K}(\mathbf{w})||\cdots||(\mathbf{U}_0\mathbf{m}_\delta^\top||\mathbf{U}_\delta)\mathbf{L}_\delta + \mathbf{S}_\delta^\top\mathbf{K}(\mathbf{w})\right)\right) \\
&= \sum_{i\in[\delta]} \underbrace{\mathsf{tr}(\overline{\mathbf{E}}_i((\mathbf{U}_0\mathbf{m}_i^\top||\mathbf{U}_i)\mathbf{L}_i + \mathbf{S}_i^\top\mathbf{K}(\mathbf{w})))}_{B_i}
\end{aligned}$$

Thanks to the correctness of Pair, we have $A_i + B_i = \mathbf{u}_{0,1}\mathbf{m}_i^\top$ and $\sum_{i\in[\delta]}(A_i + B_i) = u_{1,1}$, where $\mathbf{u}_{0,1}$ is the first row of $\mathbf{U}_0$ and $u_{1,1}$ is the first element of $\mathbf{u}_{0,1}$ as well as the $(1, 1)$-th element of $\mathbf{U}'$.

4.5 Static Predicate Compositions

Definition 4.5 (Static Predicate Compositions). Let $\mathsf{P}^{(i)}_{\kappa_i} : \mathcal{X}^{(i)}_{\kappa_i} \times \mathcal{Y}^{(i)}_{\kappa_i} \to \{0, 1\}$ be a predicate. Let $\kappa = (\kappa_1, \ldots, \kappa_n)$. The static predicate composition with a span program $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$ over a predicate set $\mathcal{P}_\kappa = (\mathsf{P}^{(1)}_{\kappa_1}, \ldots, \mathsf{P}^{(n)}_{\kappa_n})$, denoted by $\mathsf{SPC}_{\mathbf{M}}[\mathcal{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0, 1\}$, is defined as follows: let $\bar{\mathcal{X}}_\kappa = \mathcal{X}^{(1)}_{\kappa_1} \times \cdots \times \mathcal{X}^{(n)}_{\kappa_n}$, $\bar{\mathcal{Y}}_\kappa = \mathcal{Y}^{(1)}_{\kappa_1} \times \cdots \times \mathcal{Y}^{(n)}_{\kappa_n}$, $\mathbf{m}_i$ be the i-th row of $\mathbf{M}$, and define

$$\mathsf{SPC}_{\mathbf{M}}[\mathcal{P}_\kappa]((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \Leftrightarrow (1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in[n]:\mathsf{P}^{(i)}_{\kappa_i}(x_i,y_i)=1}).$$

Special Cases. We describe two special cases of $\mathsf{SPC}_{\mathbf{M}}$, namely, static disjunctions $\mathsf{SPC}_{\mathsf{OR}}$ and static conjunctions $\mathsf{SPC}_{\mathsf{AND}}$. Specifically, $\mathsf{SPC}_{\mathsf{OR}}$ is $\mathsf{SPC}_{\mathbf{M}}$ where $\mathbf{M} = (1, \ldots, 1)^\top$ and $\mathsf{SPC}_{\mathsf{AND}}$ is $\mathsf{SPC}_{\mathbf{M}}$ where $\mathbf{M} = \begin{pmatrix} 1 & \cdots & 1 \\ \mathbf{0}^\top & -\mathbf{I}_{n-1} \end{pmatrix}$. We sometimes denote $\mathsf{SPC}_{\mathsf{OR}}[(\mathsf{P}_1, \mathsf{P}_2)]$ by $\mathsf{P}_1 \vee \mathsf{P}_2$ and $\mathsf{SPC}_{\mathsf{AND}}[(\mathsf{P}_1, \mathsf{P}_2)]$ by $\mathsf{P}_1 \wedge \mathsf{P}_2$.

PES for $\mathsf{SPC}_{\mathbf{M}}[\mathcal{P}_\kappa]$. Let $\mathit{\Gamma}_i = (\mathsf{Param}_i, \mathsf{CVEncC}_i, \mathsf{CVEncK}_i, \mathsf{EncC}_i, \mathsf{EncK}_i, \mathsf{Pair}_i)$ be a PES for $\mathsf{P}^{(i)}_{\kappa_i}$. We construct a PES for $\mathsf{SPC}_{\mathbf{M}}[\mathcal{P}_\kappa]$, denoted by $\mathsf{SPC}_{\mathbf{M}}\text{-}\mathsf{Trans}(\mathbf{\Gamma}) = (\mathsf{Param}', \mathsf{CVEncC}', \mathsf{CVEncK}', \mathsf{EncC}', \mathsf{EncK}', \mathsf{Pair}')$, where $\mathbf{\Gamma} = (\mathit{\Gamma}_1, \ldots, \mathit{\Gamma}_n)$.

- $\mathsf{Param}'(\kappa) \to \omega'$: Run $\omega_i \leftarrow \mathsf{Param}_i(\kappa)$ and output $\sum_{i\in[n]} \omega_i$. This specifies common variables $\mathbf{w}' = (\mathbf{w}_1, \ldots, \mathbf{w}_n)$, where $\mathbf{w}_i = (w_{i,1}, \ldots, w_{i,\omega_i})$.
- $\mathsf{CVEncC}'((x_1, \ldots, x_n), \mathsf{aux}_c) \to (n'_1, n'_2, \widehat{\mathbf{F}}', \widehat{\mathbf{C}}')$: Run $(n_{i,1}, n_{i,2}, \widehat{\mathbf{C}}_i) \leftarrow \mathsf{CVEncC}_i(x_i, \mathsf{aux}_c)$ for $i \in [n]$. Output $(n'_1, n'_2, \widehat{\mathbf{F}}', \widehat{\mathbf{C}}')$ where $n'_1 = \max_{i\in[n]} n_{i,1}$, $n'_2 = \sum_{i\in[n]} n_{i,2}$, and

$$\widehat{\mathbf{C}}'(\mathbf{w}') = \begin{pmatrix} \widehat{\mathbf{C}}_1(\mathbf{w}_1) \cdots \widehat{\mathbf{C}}_n(\mathbf{w}_n) \\ \mathbf{O} \quad \cdots \quad \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p[\mathbf{w}']^{n'_1\times n'_2}$$

  It is not hard to see that there exists $\widehat{\mathbf{F}}' \in \mathbb{Z}_p^{n'_1\omega'\times n'_2}$ such that $\widehat{\mathbf{F}}'(\mathbf{w}') = (\mathbf{I}_{n'_1} \otimes \mathbf{w}')\widehat{\mathbf{F}}'$.
- $\mathsf{CVEncK}'((y_1, \ldots, y_n), \mathsf{aux}_k) \to (m'_1, m'_2, \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$: Run $(m_{i,1}, m_{i,2}, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}_i(y_i, \mathsf{aux}_k)$ for $i \in [n]$. Output $(m'_1, m'_2, \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$ where $m'_1 = \max_{i\in[n]} m_{i,1}$, $m'_2 = \sum_{i\in[n]} m_{i,2}$, and

$$\widehat{\mathbf{K}}'(\mathbf{w}') = \begin{pmatrix} \widehat{\mathbf{K}}_1(\mathbf{w}_1) \cdots \widehat{\mathbf{K}}_n(\mathbf{w}_n) \\ \mathbf{O} \quad \cdots \quad \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p[\mathbf{w}']^{m'_1\times m'_2}$$

  It is not hard to see that there exists $\widehat{\mathbf{L}}' \in \mathbb{Z}_p^{m'_1\omega'\times m'_2}$ such that $\widehat{\mathbf{L}}'(\mathbf{w}') = (\mathbf{I}_{m'_1} \otimes \mathbf{w}')\widehat{\mathbf{L}}'$.

- $\mathsf{EncC}'((x_1,\ldots,x_n),m_1',\mathsf{aux}_c) \to (n_3',\mathbf{F}',\mathbf{C}')$: Run $(n_{i,3},\mathbf{F}_i) \leftarrow \mathsf{EncK}(x_i,\mathsf{aux}_c)$ for $i \in [n]$. Output $(n_3',\mathbf{F}',\mathbf{C}')$ where $n_3' = \sum_{i\in[n]} n_{i,3}$ and

$$\mathbf{F}' = \begin{pmatrix} \mathbf{F}_1 & & \\ & \ddots & \\ & & \mathbf{F}_n \end{pmatrix} \in \mathbb{Z}_p[\mathbf{w}']^{n_3'\times n_2'}$$
$$\mathbf{C}'(\mathbf{S}',\mathbf{T}',\mathbf{w}') = \mathbf{T}'\mathbf{F}' + \mathbf{S}'\widehat{\mathbf{C}}'(\mathbf{w}') \in \mathbb{Z}_p[\mathbf{S}',\mathbf{T}',\mathbf{w}']^{m_1'\times n_2'}$$

- $\mathsf{EncK}'((y_1,\ldots,y_n),n_1',\mathsf{aux}_k) \to (m_3',\mathbf{L}',\mathbf{K}')$: Run $(m_{i,3},\mathbf{L}_i) \leftarrow \mathsf{EncK}(y_i,\mathsf{aux}_k)$ for $i \in [n]$. Let $\overline{\mathbf{l}}_i$ be the first row of $\mathbf{L}_i$, $\underline{\mathbf{L}}_i$ be the submatrix of $\mathbf{L}_i$ obtained by removing the first row, $\mathbf{m}_i$ be the i-th row of $\mathbf{M}$ for $i \in [n]$. Output $(m_3',\mathbf{L}',\mathbf{K}')$ where $m_3' = m + \sum_{i\in[n]}(m_{i,3}-1)$ and

$$\mathbf{L}' = \begin{pmatrix} \mathbf{m}_1^\top\overline{\mathbf{l}}_1 & \cdots & \mathbf{m}_n^\top\overline{\mathbf{l}}_n \\ \underline{\mathbf{L}}_1 & & \\ & \ddots & \\ & & \underline{\mathbf{L}}_n \end{pmatrix} \in \mathbb{Z}_p^{m_3'\times m_2'}$$
$$\mathbf{K}'(\mathbf{S}',\mathbf{U}',\mathbf{w}') = \mathbf{U}'\mathbf{L}' + \mathbf{S}'^\top\widehat{\mathbf{K}}'(\mathbf{w}') \in \mathbb{Z}_p[\mathbf{S}',\mathbf{U}',\mathbf{w}']^{n_1'\times m_2'}$$

- $\mathsf{Pair}'((x_1,\ldots,x_n),(y_1,\ldots,y_n),\mathsf{aux}_c,\mathsf{aux}_k) \to (\mathbf{E}',\overline{\mathbf{E}}')$: Run $(\mathbf{E}_i,\overline{\mathbf{E}}_i) \leftarrow \mathsf{Pair}_i(x_i,y_i,\mathsf{aux}_c,\mathsf{aux}_k)$ for $i \in [n]$. Let S be a set such that $\mathsf{P}_\kappa^{(i)}(x_i,y_i) = 1$ for $i \in S$ and $(1,\mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in S})$, and $a_1,\ldots,a_n \in \mathbb{Z}_p$ be coefficients such that $a_i = 0$ for $i \notin S$ and $\sum_{i\in[n]} a_i\mathbf{m}_i = (1,\mathbf{0})$. Output

$$\mathbf{E}' = \begin{pmatrix} a_1\mathbf{E}_1 & \mathbf{O} \\ \vdots & \vdots \\ a_n\mathbf{E}_n & \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p^{n_2'\times m_1'}, \quad \overline{\mathbf{E}}' = \begin{pmatrix} a_1\overline{\mathbf{E}}_1 & \mathbf{O} \\ \vdots & \vdots \\ a_n\overline{\mathbf{E}}_n & \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p^{m_2'\times n_1'}$$

- **Correctness**: Let $\mathbf{T}_i$ and $\mathbf{S}_i$ be the i-th block of $\mathbf{T}'$ and $\mathbf{S}'$ of size $m_1' \times n_{i,3}$ and $m_1' \times n_{i,1}$, that is, $\mathbf{T}' = (\mathbf{T}_1||\cdots||\mathbf{T}_n)$ and $\mathbf{S}' = (\mathbf{S}_1||\cdots||\mathbf{S}_n)$, respectively, and $\mathbf{U}' = (\mathbf{U}_0||\mathbf{U}_1||\cdots||\mathbf{U}_n)$ where the width of $\mathbf{U}_0$ is m and that of $\mathbf{U}_i$ for $i \in [n]$ is $m_{i,3}$. Let $\widetilde{\mathbf{T}}_i$ for $i \in [n]$ be the matrix consisting of the first $m_{i,1}$ rows of $\mathbf{T}_i$, $\widetilde{\mathbf{U}}_i$ for $i \in [0,n]$ be the matrix consisting of the first $n_{i,1}$ rows of $\mathbf{U}_i$, and $\widetilde{\mathbf{S}}_i$ for $i \in [n]$ be the upper left submatrix of $\mathbf{S}_i$ of size $m_{i,1} \times n_{i,1}$. Then, we have

$$\begin{aligned}
&\mathsf{tr}(\mathbf{E}'\mathbf{C}'(\mathbf{S}',\mathbf{T}',\mathbf{w}')) \\
=&\mathsf{tr}\left(\mathbf{E}'\left(\mathbf{T}_1\mathbf{F}_1 + \mathbf{S}_1\left(\begin{smallmatrix}\widehat{\mathbf{C}}_1(\mathbf{w}_1)\\ \mathbf{O}\end{smallmatrix}\right)||\cdots||\mathbf{T}_n\mathbf{F}_n + \mathbf{S}_n\left(\begin{smallmatrix}\widehat{\mathbf{C}}_n(\mathbf{w}_n)\\ \mathbf{O}\end{smallmatrix}\right)\right)\right) \\
=&\sum_{i\in[n]} a_i\mathsf{tr}\left((\mathbf{E}_i||\mathbf{O})\left(\mathbf{T}_i\mathbf{F}_i + \mathbf{S}_i\left(\begin{smallmatrix}\widehat{\mathbf{C}}_i(\mathbf{w}_i)\\ \mathbf{O}\end{smallmatrix}\right)\right)\right) \\
=&\sum_{i\in[n]} a_i\underbrace{\mathsf{tr}\left(\mathbf{E}_i\left(\widetilde{\mathbf{T}}_i\mathbf{F}_i + \widetilde{\mathbf{S}}_i\widehat{\mathbf{C}}_i(\mathbf{w}_i)\right)\right)}_{A_i} \\
&\mathsf{tr}(\overline{\mathbf{E}}'\mathbf{K}'(\mathbf{S}',\mathbf{U}',\mathbf{w}')) \\
=&\mathsf{tr}\left(\overline{\mathbf{E}}'\left((\mathbf{U}_0\mathbf{m}_1^\top||\mathbf{U}_1)\mathbf{L}_1 + \mathbf{S}_1^\top\left(\begin{smallmatrix}\widehat{\mathbf{K}}_1(\mathbf{w}_1)\\ \mathbf{O}\end{smallmatrix}\right)||\cdots||(\mathbf{U}_0\mathbf{m}_n^\top||\mathbf{U}_n)\mathbf{L}_n + \mathbf{S}_n^\top\left(\begin{smallmatrix}\widehat{\mathbf{K}}_n(\mathbf{w}_n)\\ \mathbf{O}\end{smallmatrix}\right)\right)\right) \\
=&\sum_{i\in[n]} a_i\mathsf{tr}\left((\overline{\mathbf{E}}_i||\mathbf{O})\left((\mathbf{U}_0\mathbf{m}_i^\top||\mathbf{U}_i)\mathbf{L}_i + \mathbf{S}_i^\top\left(\begin{smallmatrix}\widehat{\mathbf{K}}_i(\mathbf{w}_i)\\ \mathbf{O}\end{smallmatrix}\right)\right)\right) \\
=&\sum_{i\in[n]} a_i\underbrace{\mathsf{tr}(\overline{\mathbf{E}}_i((\widetilde{\mathbf{U}}_0\mathbf{m}_i^\top||\widetilde{\mathbf{U}}_i)\mathbf{L}_i + \widetilde{\mathbf{S}}_i^\top\mathbf{K}_i(\mathbf{w}_i)))}_{B_i}
\end{aligned}$$

Thanks to the correctness of Pair_i, we have $A_i + B_i = \tilde{\mathbf{u}}_{0,1}\mathbf{m}_i^\top$ and $\sum_{i\in[n]} a_i(A_i+B_i) = u_{1,1}$, where $\tilde{\mathbf{u}}_{0,1}$ is the first row of $\widetilde{\mathbf{U}}_0$ and $u_{1,1}$ is the first element of $\mathbf{u}_{0,1}$ as well as the $(1,1)$-th element of $\mathbf{U}'$.

4.6 Dual Predicates

Definition 4.6 (Dual Predicates). The dual predicate of $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$ is $\mathsf{Dual}[\mathsf{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$ where $\bar{\mathcal{X}}_\kappa = \mathcal{Y}_\kappa$ and $\bar{\mathcal{Y}}_\kappa = \mathcal{X}_\kappa$, and defined as $\mathsf{Dual}[\mathsf{P}_\kappa](x,y) = \mathsf{P}_\kappa(y,x)$.

PES for $\mathsf{Dual}[\mathsf{P}_\kappa]$. Let $\Gamma = (\mathsf{Param}, \mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ be a PES for P_κ. We construct a PES for $\mathsf{Dual}[\mathsf{P}_\kappa]$, denoted by $\mathsf{Dual\text{-}Trans}(\Gamma) = (\mathsf{Param}', \mathsf{CVEncC}', \mathsf{CVEncK}', \mathsf{EncC}', \mathsf{EncK}', \mathsf{Pair}')$ as follows.

- $\mathsf{Param}'(\kappa) \to \omega'$: Run $\omega \leftarrow \mathsf{Param}(\kappa)$ and output $\omega' = \omega + 1$. This specifies common variables $\mathbf{w}' = (w_0, w_1, \dots, w_\omega)$, where w_0 is a new common variable. In what follows, we denote $(w_1, \dots, w_\omega)$ by $\mathbf{w}$.
- $\mathsf{CVEncC}'(x, \mathsf{aux}_c) \to (n_1', n_2', \widehat{\mathbf{F}}', \widehat{\mathbf{C}}')$: Run $(m_1, m_2, \widehat{\mathbf{L}}, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(x, \mathsf{aux}_c)$ and $(m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(x, \mathsf{aux}_c)$. Let $\overline{\mathbf{L}}$ be the first row of $\mathbf{L}$. Output $(n_1', n_2', \widehat{\mathbf{F}}', \widehat{\mathbf{C}}')$ where $n_1' = m_1 + 1$, $n_2' = m_2$, and
$$\widehat{\mathbf{C}}'(\mathbf{w}') = \begin{pmatrix} w_0 \overline{\mathbf{L}} \\ \widehat{\mathbf{K}}(\mathbf{w}) \end{pmatrix} \in \mathbb{Z}_p[\mathbf{w}']^{n_1' \times n_2'}.$$
It is not hard to see that there exists $\widehat{\mathbf{F}}' \in \mathbb{Z}_p^{n_1'\omega' \times n_2'}$ such that $\widehat{\mathbf{C}}'(\mathbf{w}') = (\mathbf{I}_{n_1'} \otimes \mathbf{w}')\widehat{\mathbf{F}}'$.
- $\mathsf{CVEncK}'(y, \mathsf{aux}_k) \to (m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$: Run $(n_1, n_2, \widehat{\mathbf{F}}, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(y, \mathsf{aux}_k)$. Output $(m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$ where $m_1' = n_1$, $m_2' = n_2 + 1$, and
$$\widehat{\mathbf{K}}'(\mathbf{w}') = \left(\begin{matrix} -w_0 \\ \mathbf{0}^\top \end{matrix} \;||\; \widehat{\mathbf{C}}(\mathbf{w}) \right) \in \mathbb{Z}_p[\mathbf{w}']^{m_1' \times m_2'}.$$
It is not hard to see that there exists $\widehat{\mathbf{L}}' \in \mathbb{Z}_p^{m_1'\omega' \times m_2'}$ such that $\widehat{\mathbf{K}}'(\mathbf{w}') = (\mathbf{I}_{m_1'} \otimes \mathbf{w}')\widehat{\mathbf{L}}'$.
- $\mathsf{EncC}'(x, m_1', \mathsf{aux}_c) \to (n_3', \mathbf{F}', \mathbf{C}')$: Run $(m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(x, \mathsf{aux}_c)$ and $(n_1', n_2', \widehat{\mathbf{C}}') \leftarrow \mathsf{CVEncC}'(x, \mathsf{aux}_c)$. Output $(n_3', \mathbf{F}', \mathbf{C}')$ where $n_3' = m_3 - 1$, $\mathbf{F}' \in \mathbb{Z}_p^{n_3' \times n_2'}$ be the matrix obtained by removing the first row of $\mathbf{L}$, and
$$\mathbf{C}'(\mathbf{S}', \mathbf{T}', \mathbf{w}') = \mathbf{T}'\mathbf{F}' + \mathbf{S}'\widehat{\mathbf{C}}'(\mathbf{w}') \in \mathbb{Z}_p[\mathbf{S}', \mathbf{T}', \mathbf{w}']^{m_1' \times n_2'}.$$
- $\mathsf{EncK}'(y, n_1', \mathsf{aux}_k) \to (m_3', \mathbf{L}', \mathbf{K}')$: Run $(n_3, \mathbf{F}) \leftarrow \mathsf{EncC}(y, \mathsf{aux}_k)$ and $(m_1', m_2', \widehat{\mathbf{K}}') \leftarrow \mathsf{CVEncK}'(y, \mathsf{aux}_k)$. Output $(m_3', \mathbf{L}', \mathbf{K}')$ where $m_3' = n_3 + 1$ and
$$\mathbf{L}' = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^\top & \mathbf{F} \end{pmatrix} \in \mathbb{Z}_p^{m_3' \times m_2'}$$
$$\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}') = \mathbf{U}'\mathbf{L}' + \mathbf{S}'^\top \widehat{\mathbf{K}}'(\mathbf{w}') \in \mathbb{Z}_p[\mathbf{S}', \mathbf{U}', \mathbf{w}']^{n_1' \times m_2'}$$
- $\mathsf{Pair}'(x, y, \mathsf{aux}_c, \mathsf{aux}_k) \to (\mathbf{E}', \overline{\mathbf{E}}')$: Run $(\mathbf{E}, \overline{\mathbf{E}}) \leftarrow \mathsf{Pair}(y, x, \mathsf{aux}_k, \mathsf{aux}_c)$ and set $\mathbf{E}' = \overline{\mathbf{E}} \in \mathbb{Z}_p^{n_2' \times m_1'}$, $\overline{\mathbf{E}}' = \left(\begin{smallmatrix} 1 & \mathbf{0} \\ \mathbf{0}^\top & \mathbf{E} \end{smallmatrix}\right) \in \mathbb{Z}_p^{m_2' \times n_1'}$.
- **Correctness**: Let $\mathbf{S}$ be the submatrix of $\mathbf{S}'$ obtained by removing the first column, $\mathbf{s}_c$ be the first column of $\mathbf{S}'$, $\mathbf{s}_r^\top$ be the first row of $\mathbf{S}'$, $\mathbf{u}^\top$ be the first column of $\mathbf{U}'$, $\mathbf{U}$ be the submatrix of $\mathbf{U}'$ obtained by removing the first column, $\widehat{\mathbf{U}}$ be the submatrix of $\mathbf{U}$ obtained by removing the first row, and $s_{1,1}$ and $u_{1,1}$ be the $(1,1)$-th element of $\mathbf{S}'$ and $\mathbf{U}'$, respectively. Then, we have
$$\begin{aligned} \mathsf{tr}(\mathbf{E}'\mathbf{C}'(\mathbf{S}', \mathbf{T}', \mathbf{w}')) &= \mathsf{tr}(\overline{\mathbf{E}}(\mathbf{T}'\mathbf{F}' + \mathbf{S}'\widehat{\mathbf{C}}'(\mathbf{w}'))) \\ &= \underbrace{\mathsf{tr}(\overline{\mathbf{E}}((w_0\mathbf{s}_c^\top || \mathbf{T})\mathbf{L} + \mathbf{S}\widehat{\mathbf{K}}(\mathbf{w}))}_{A} \\ \mathsf{tr}(\overline{\mathbf{E}}'\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}')) &= \mathsf{tr}(\overline{\mathbf{E}}'(\mathbf{U}'\mathbf{L}' + \mathbf{S}'^\top \widehat{\mathbf{K}}'(\mathbf{w}'))) \\ &= \mathsf{tr}\left(\left(\begin{smallmatrix} 1 & \mathbf{0} \\ \mathbf{0}^\top & \mathbf{E} \end{smallmatrix}\right) (\mathbf{u}^\top || \mathbf{U}\mathbf{F}) + (-w_0\mathbf{s}_r^\top || \mathbf{S}'^\top \widehat{\mathbf{C}}(\mathbf{w})) \right) \\ &= u_{1,1} - w_0 s_{1,1} + \underbrace{\mathsf{tr}(\mathbf{E}(\widehat{\mathbf{U}}\mathbf{F} + \mathbf{S}^\top \widehat{\mathbf{C}}(\mathbf{w})))}_{B} \end{aligned}$$

Thanks to the correctness of Pair, we have $A + B = w_0 s_{1,1}$, and the correctness of Pair' holds.

4.7 Key-Policy Augmentation

Definition 4.7 (Key-Policy Augmentation). The predicate for key-policy span program augmentation over a single predicate $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$, denoted by $\mathsf{KP1}[\mathsf{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$, where $\bar{\mathcal{X}}_\kappa = \mathcal{X}_\kappa$ and $\bar{\mathcal{Y}}_\kappa = \bigcup_{(n,m)\in\mathbb{N}^2}(\mathbb{Z}_p^{n\times m} \times \varPhi_n)$, where $\varPhi_n$ consists of all functions $\phi : [n] \to \mathcal{Y}_\kappa$ is defined as follows. For $x \in \bar{\mathcal{X}}_\kappa$ and $y = (\mathbf{M}, \phi) \in \bar{\mathcal{Y}}_\kappa$ where $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$ and $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$, let

$$\mathsf{KP1}[\mathsf{P}_\kappa](x, y) = 1 \Leftrightarrow (1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in[n]:\mathsf{P}_\kappa(x,\phi(i))=1}).$$

PES for $\mathsf{KP1}[\mathsf{P}_\kappa]$**.** Let $\varGamma = (\mathsf{Param}, \mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ be a PES for P_κ. We construct a PES for $\mathsf{KP1}[\mathsf{P}_\kappa]$, denoted by $\mathsf{KP1\text{-}Trans}(\varGamma) = (\mathsf{Param}', \mathsf{CVEncC}', \mathsf{CVEncK}', \mathsf{EncC}', \mathsf{EncK}', \mathsf{Pair}')$ as follows.

- $\mathsf{Param}'(\kappa) = \mathsf{Param}(\kappa)$, that is, $\omega' = \omega$ and $\mathbf{w}' = \mathbf{w}$.
- $\mathsf{CVEncC}'(x, \mathsf{aux}_c) = \mathsf{CVEncC}(x, \mathsf{aux}_c)$, that is, $n_1' = n_1$, $n_2' = n_2$, $\widehat{\mathbf{F}}' = \widehat{\mathbf{F}}$, $\widehat{\mathbf{C}}'(\mathbf{w}') = \widehat{\mathbf{C}}(\mathbf{w})$.
- $\mathsf{CVEncK}'((\mathbf{M}, \phi), \mathsf{aux}_k) \to (m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$: Run $(m_{i,1}, m_{i,2}, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}(\phi(i), \mathsf{aux}_k)$ for $i \in [n]$. Output $(m_1', m_2', \widehat{\mathbf{L}}', \widehat{\mathbf{K}}')$ where $m_1' = \sum_{i\in[n]} m_{i,1}$, $m_2' = \sum_{i\in[n]} m_{i,2}$, and

$$\widehat{\mathbf{K}}'(\mathbf{w}) = \begin{pmatrix} \widehat{\mathbf{K}}_1(\mathbf{w}) & & \\ & \ddots & \\ & & \widehat{\mathbf{K}}_n(\mathbf{w}) \end{pmatrix} \in \mathbb{Z}_p[\mathbf{w}]^{m_1' \times m_2'}$$

  It is not hard to see that there exists $\widehat{\mathbf{L}}' \in \mathbb{Z}_p^{m_1'\omega' \times m_2'}$ such that $\widehat{\mathbf{K}}'(\mathbf{w}) = (\mathbf{I}_{m_1'} \otimes \mathbf{w})\widehat{\mathbf{L}}'$.
- $\mathsf{EncC}'(x, m_1', \mathsf{aux}_c) = \mathsf{EncC}(x, m_1', \mathsf{aux}_c)$, that is, $n_3' = n_3$, $\mathbf{F}' = \mathbf{F}$, $\mathbf{C}'(\mathbf{S}', \mathbf{T}', \mathbf{w}') = \mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w})$.
- $\mathsf{EncK}'((\mathbf{M}, \phi), n_1', \mathsf{aux}_k) \to (m_3', \mathbf{L}', \mathbf{K}')$: Run $(m_{i,3}, \mathbf{L}_i) \leftarrow \mathsf{EncK}(\phi(i), \mathsf{aux}_k)$ for $i \in [n]$. Let $\bar{\mathbf{l}}_i$ be the first row of $\mathbf{L}_i$, $\underline{\mathbf{L}}_i$ be the submatrix of $\mathbf{L}_i$ obtained by removing the first row, $\mathbf{m}_i$ be the i-th row of $\mathbf{M}$ for $i \in [n]$. Output $(m_3', \mathbf{L}', \mathbf{K}')$ where $m_3' = m + \sum_{i\in[n]}(m_{i,3} - 1)$, $\mathbf{L}' = \begin{pmatrix} \mathbf{m}_1^\top \bar{\mathbf{l}}_1 & \cdots & \mathbf{m}_n^\top \bar{\mathbf{l}}_n \\ \underline{\mathbf{L}}_1 & & \\ & \ddots & \\ & & \underline{\mathbf{L}}_n \end{pmatrix} \in \mathbb{Z}_p^{m_3' \times m_2'}$ and

$$\mathbf{K}'(\mathbf{S}', \mathbf{U}', \mathbf{w}') = \mathbf{U}'\mathbf{L}' + \mathbf{S}'^\top \widehat{\mathbf{K}}'(\mathbf{w}') \in \mathbb{Z}_p[\mathbf{S}', \mathbf{U}', \mathbf{w}']^{n_1' \times m_2'}$$

- $\mathsf{Pair}'(x, (\mathbf{M}, \phi), \mathsf{aux}_c, \mathsf{aux}_k) \to (\mathbf{E}', \overline{\mathbf{E}}')$: Run $(\mathbf{E}_i, \overline{\mathbf{E}}_i) \leftarrow \mathsf{Pair}(x, \phi(i), \mathsf{aux}_c, \mathsf{aux}_k)$ for $i \in [n]$. Let S be a set such that $\mathsf{P}_\kappa(x, \phi(i)) = 1$ for $i \in S$ and $(1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in S})$, and $a_1, \ldots, a_n \in \mathbb{Z}_p$ be coefficients such that $a_i = 0$ for $i \notin S$ and $\sum_{i\in[n]} a_i \mathbf{m}_i = (1, \mathbf{0})$. Output $\mathbf{E}' = (a_1\mathbf{E}_1 || \cdots || a_n\mathbf{E}_n)$ and $\overline{\mathbf{E}}' = \begin{pmatrix} a_1\overline{\mathbf{E}}_1 \\ \vdots \\ a_n\overline{\mathbf{E}}_n \end{pmatrix}$.
- **Correctness**: Let $\mathbf{T}_i$ and $\mathbf{S}_i$ be the i-th block of $\mathbf{T}'$ and $\mathbf{S}'$ of size $m_{i,1} \times n_3'$ and $m_{i,1} \times n_1'$, that is, $\mathbf{T}' = \begin{pmatrix} \mathbf{T}_1 \\ \vdots \\ \mathbf{T}_n \end{pmatrix}$ and $\mathbf{S}' = \begin{pmatrix} \mathbf{S}_1 \\ \vdots \\ \mathbf{S}_n \end{pmatrix}$, respectively, $\mathbf{U}' = (\mathbf{U}_0 || \mathbf{U}_1 || \cdots || \mathbf{U}_n)$ where the width of $\mathbf{U}_0$ is m

Table 2. Parameters obtained from each PES transformation.

		Ciphertext Encoding			Key Encoding		
Transformation	ω	n'_1	n'_2	n'_3	m'_1	m'_2	m'_3
Null-Trans (§4.1)	$\omega+1$	n_1	n_2	n_3	m_1	m_2	m_3
WC-Trans (§4.2)	ω	n_1	n_2	n_3	m_1	m_2	m_3
$\mathsf{KP1_{OR}}$-Trans (§4.3)	ω	n_1	n_2	n_3	$\sum_{i\in[\delta]} m_{i,1}$	$\sum_{i\in[\delta]} m_{i,2}$	$1+\sum_{i\in[\delta]}(m_{i,3}-1)$
$\mathsf{KP1_{AND}}$-Trans (§4.4)	ω	n_1	n_2	n_3	$\sum_{i\in[\delta]} m_{i,1}$	$\sum_{i\in[\delta]} m_{i,2}$	$\sum_{i\in[\delta]} m_{i,3}$
$\mathsf{SPC_{\mathbf{M}}}$-$\mathsf{Trans}$ (§4.5)	$\sum_{i\in[n]}\omega_i$	$\max_{i\in[n]} n_{i,1}$	$\sum_{i\in[n]} n_{i,2}$	$\sum_{i\in[n]} n_{i,3}$	$\max_{i\in[n]} m_{i,1}$	$\sum_{i\in[n]} m_{i,2}$	$m+\sum_{i\in[n]}(m_{i,3}-1)$
Dual-Trans (§4.6)	$\omega+1$	m_1+1	m_2	m_3-1	n_1	n_2+1	n_3+1
$\mathsf{KP1}$-Trans (§4.7)	ω	n_1	n_2	n_3	$\sum_{i\in[n]} m_{i,1}$	$\sum_{i\in[n]} m_{i,2}$	$m+\sum_{i\in[n]}(m_{i,3}-1)$

Note: This table shows the parameters of the PES $\mathsf{Trans}[\Gamma]$, applied by transformation Trans to the PES Γ. If the transformation involves single-input attribute, the original parameters for PES are $(\omega, n_1, n_2, n_3, m_1, m_2, m_3)$. If the transformation involves multi-input attribute, the original parameters for PES will have *e.g.,* ω_i and $n_{i,j}, m_{i,j}$ for $j = 1, 2, 3$ for their parameters from the i-th input. $n \times m$ is the size of policy matrix for $\mathsf{SPC_{\mathbf{M}}}$ and $\mathsf{KP1}$. $\delta = \mathsf{aux}_k$ is the auxiliary input that defines key well-formedness.

and that of $\mathbf{U}_i$ for $i \in [n]$ is $m_{i,3}$. Then, we have

$$\begin{aligned}\mathsf{tr}(\mathbf{E}'\mathbf{C}'(\mathbf{S}',\mathbf{T}',\mathbf{w}')) &= \mathsf{tr}\left(\sum_{i\in[n]} a_i \mathbf{E}_i(\mathbf{T}_i\mathbf{F} + \mathbf{S}_i\widehat{\mathbf{C}}(\mathbf{w}))\right)\\ &= \sum_{i\in[n]} a_i \underbrace{\mathsf{tr}(\mathbf{E}_i(\mathbf{T}_i\mathbf{F} + \mathbf{S}_i\widehat{\mathbf{C}}(\mathbf{w})))}_{A_i}\end{aligned}$$

$$\begin{aligned}&\mathsf{tr}(\overline{\mathbf{E}}'\mathbf{K}'(\mathbf{S}',\mathbf{U}',\mathbf{w}'))\\ =&\mathsf{tr}\left(\overline{\mathbf{E}}'\left((\mathbf{U}_0\mathbf{m}_1^\top||\mathbf{U}_1)\mathbf{L}_1 + \mathbf{S}_1^\top\mathbf{K}(\mathbf{w})||\cdots||(\mathbf{U}_0\mathbf{m}_n^\top||\mathbf{U}_n)\mathbf{L}_n + \mathbf{S}_n^\top\mathbf{K}(\mathbf{w})\right)\right)\\ =&\sum_{i\in[n]} a_i \underbrace{\mathsf{tr}(\overline{\mathbf{E}}_i((\mathbf{U}_0\mathbf{m}_i^\top||\mathbf{U}_i)\mathbf{L}_i + \mathbf{S}_i^\top\mathbf{K}(\mathbf{w})))}_{B_i}\end{aligned}$$

Thanks to the correctness of Pair, we have $A_i + B_i = \mathbf{u}_{0,1}\mathbf{m}_i^\top$ and $\sum_{i\in[n]} a_i(A_i + B_i) = u_{1,1}$, where $\mathbf{u}_{0,1}$ is the first row of $\mathbf{U}_0$ and $u_{1,1}$ is the first element of $\mathbf{u}_{0,1}$ as well as the $(1,1)$-th element of $\mathbf{U}'$.

4.8 Efficiency of Transformations

In each PES construction, we will often show the corresponding parameters of ciphertext and key encodings. These will in fact define the efficiency of the resulting registered ABE. For ease of visualization, we summarize the parameters achieved by the PES transformations in this paper in Table 2.

5 Conforming PES for sReg-ABE

We can apply our transformations described in §4 to a predicate set $\mathcal{P}_\kappa$ multiple times to obtain a new predicate P_κ. When we apply a PES to construct a sReg-ABE scheme, we need key well-formedness for correctness and KE-ind for security. The theorem below explains how we can apply transformations to construct new predicates that satisfy the above properties.

To state the theorem formally, we define a predicate set $f_c(\mathcal{P}_\kappa)$ for a predicate set $\mathcal{P}_\kappa = (\mathsf{P}^{(1)}_{\kappa_1}, \ldots, \mathsf{P}^{(n)}_{\kappa_n})$. Let $\mathcal{TS} = (\mathsf{Null}, \mathsf{WC}, \mathsf{KP1_{OR}}, \mathsf{KP1_{AND}}, \mathsf{Dual}, \mathsf{KP1})$ be a set of transformations that takes one predicate. Let $\bar{\mathcal{P}}_\kappa$ be a predicate set consisting of all predicates obtained by applying one of the transformations in $\mathcal{TS} \cup \{\mathsf{SPC_{\mathbf{M}}}\}_{\mathbf{M}\in\bigcup_{m\in\mathbb{N}}\mathbb{Z}_p^{n\times m}}$ to $\mathcal{P}_\kappa$. That is, $\bar{\mathcal{P}}_\kappa = (\{\mathsf{SPC_{\mathbf{M}}}[\mathcal{P}_\kappa]\}_{\mathbf{M}\in\bigcup_{m\in\mathbb{N}}\mathbb{Z}_p^{n\times m}}, \{\mathsf{T}[\mathsf{P}^{(i)}_{\kappa_i}]\}_{\mathsf{T}\in\mathcal{TS}, i\in[n]})$. Let f be a deterministic procedure defined as $f(\mathcal{P}_\kappa) = \mathcal{P}_\kappa \cup \bar{\mathcal{P}}_\kappa$. Denote $f \circ \ldots \circ f(\mathcal{P}_\kappa)$ where f appears c times by $f_c(\mathcal{P}_\kappa)$. Then, we have the following theorem.

Theorem 5.1. *For all constants c and predicate sets $\mathcal{P}_\kappa = (\mathsf{P}^{(1)}_{\kappa_1}, \dots, \mathsf{P}^{(n)}_{\kappa_n})$, each of which has predicate encodings, $\mathsf{P}_\kappa \in f_c(\mathcal{P}_\kappa)$ has a valid PES satisfying key well-formedness and* $\mathsf{KE\text{-}ind}$ *under the MDDH assumption as long as P_κ is generated from $\mathcal{P}_\kappa$ without* $\mathsf{KP1}$*, or the last two transformations applied to obtain P_κ are* $\mathsf{KP1}$ *then* Dual *and other than that no* $\mathsf{KP1}$ *is used.*

Proof. Theorem 5.1 is straightforward from Lemmata 3.1 and C.1 to C.14. Specifically, (1) Lemma 3.1 says that each predicate in $\mathcal{P}_\kappa$ has a PES satisfying key and ciphertext well-formedness and $\mathsf{KE\text{-}ind}$; (2) Lemmata C.1 to C.12 say that if underlying PES satisfies key and ciphertext well-formedness and $\mathsf{KE\text{-}ind}$, then all the transformations in §4 except $\mathsf{KP1}$ preserve all of these properties; and (3) Lemmata C.11 to C.14 say that applying $\mathsf{KP1}$ then Dual to a PES satisfying the three properties makes ciphertext well-formedness lost (but still valid) while the other two properties remain. Hence, the theorem holds. □

6 sReg-ABE from PES

In this section, we present our sReg-ABE scheme from PES satisfying key well-formedness (Definition 3.2) and $\mathsf{KE\text{-}ind}$ (Definition 3.4).

6.1 Construction

Let $\mathbb{G} = \{\mathbb{G}_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of bilinear groups where $\mathbb{G}_\lambda{=}(p, G_1, G_2, G_T, g_1, g_2, e)$. Let $\mathit{\Gamma} = (\mathsf{Param}, \mathsf{CVEncC}, \mathsf{CVEncK}, \mathsf{EncC}, \mathsf{EncK}, \mathsf{Pair})$ be a ciphertext valid and key well-formed PES (as per Definitions 3.1 and 3.2) with $\mathsf{KE\text{-}ind}$ for a predicate family $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$. Let $\mathit{\Pi} = (\mathsf{LGen}, \mathsf{LProve}, \mathsf{LVerify}, \mathsf{LSim})$ be a QA-NIZK scheme. Then, we can construct a sReg-ABE scheme for predicate P_κ as follows.

$\mathsf{Setup}(1^\lambda, 1^L, \kappa)$**:** It outputs crs as follows.

$$\omega \leftarrow \mathsf{Param}(\kappa),\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k},\ \mathbf{h} \leftarrow \mathbb{Z}_p^{2k+1}$$

$$\left\{\begin{array}{l} \mathbf{W}_i = (\mathbf{W}_{i,1}||\cdots||\mathbf{W}_{i,\omega}) \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)},\ \mathbf{W}_{i,0} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)} \\ \mathbf{R}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)},\ \mathbf{r}_i \leftarrow \mathbb{Z}_p^k \\ (\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda, [\mathbf{A}_i]_1)\ \text{ where } \mathbf{A}_i = \left(\begin{smallmatrix}\mathbf{A}\\ \mathbf{R}_i\end{smallmatrix}\right) \end{array}\right\}_{i\in[L]}$$

$$\mathsf{crs}{=}\left(\begin{array}{l} [\mathbf{A}]_1, [\mathbf{A}\mathbf{h}^\top]_\mathsf{T}, \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{A}\mathbf{W}_{i,0}, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\mathbf{B}\mathbf{r}_i^\top, \mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top]_2\}_{i\in[L]}, \{[\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_j^\top, \mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_j^\top)]_2\}_{\substack{i,j\in[L]\\ i\neq j}} \end{array}\right)$$

$\mathsf{Gen}(\mathsf{crs}, i)$**:** It outputs pk_i and sk_i as follows:

$$\mathbf{V}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)},\ \mathbf{M}_i = \left(\begin{smallmatrix}\mathbf{A}\mathbf{V}_i\\ \mathbf{R}_i\mathbf{V}_i\end{smallmatrix}\right),\ \pi_i \leftarrow \mathsf{LProve}(\mathsf{crs}_i, [\mathbf{M}_i]_1, \mathbf{V}_i)$$

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

$\mathsf{Ver}(\mathsf{crs}, i, \mathsf{pk}_i)$**:** It parses $\mathsf{pk}_i = ([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{p}_{i,j}^\top]_2\}_{j\in[L]\setminus\{i\}}, \pi_i)$. It outputs 1 if $\mathsf{LVerify}(\mathsf{crs}_i, [\mathbf{M}_i]_1, \pi_i) = 1$ where $\mathbf{M}_i = \left(\begin{smallmatrix}\mathbf{T}_i\\ \mathbf{Q}_i\end{smallmatrix}\right)$ and $\forall i \neq j : [\mathbf{A}\mathbf{p}_{i,j}^\top]_\mathsf{T} = [\mathbf{T}_i\mathbf{B}\mathbf{r}_i^\top]_\mathsf{T}$, and outputs 0 otherwise.

$\mathsf{Agg}(\mathsf{crs}, \{\mathsf{pk}_i, y_i\}_{i\in[L]})$**:** It computes aux_k that satisfies Definition 3.2 with respect to $Y = \{y_i\}_{i\in[L]}$. It parses $\mathsf{pk}_i = ([\mathbf{T}_i, \mathbf{Q}_i]_1, \{[\mathbf{p}_{i,j}^\top]_2\}_{j\in[L]\setminus\{i\}}, \pi_i)$ and computes $(m_1, m_2, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}(y_i, \mathsf{aux}_k)$ for all $i \in [L]$ and $(m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(y_1, \mathsf{aux}_k)$. It outputs mpk and $\mathsf{hsk}_1, \dots, \mathsf{hsk}_L$ as follows:

$$\mathsf{mpk}{=}\left(y_1, \mathsf{aux}_k, [\mathbf{A}\mathbf{h}^\top]_\mathsf{T}, \left[\mathbf{A}, \underbrace{\sum_{i\in[L]}(\mathbf{A}\mathbf{W}_{i,0}+\mathbf{T}_i)}_{\mathbf{P}_1}, \underbrace{\sum_{i\in[L]}\widehat{\mathbf{K}}_i(\mathbf{A}\mathbf{W}_i)}_{\mathbf{P}_2}, \underbrace{\sum_{i\in[L]}\mathbf{A}\mathbf{W}_i}_{\mathbf{P}_3}\right]_1\right)$$

$$\mathsf{hsk}_i = \left(\begin{array}{l} \mathsf{aux}_k, \left[\underbrace{\mathbf{B}\mathbf{r}_i^\top}_{\mathbf{h}_1^\top}, \underbrace{\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top}_{\mathbf{h}_2^\top}, \underbrace{\sum_{j\in[L]\setminus\{i\}}(\mathbf{W}_{j,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{p}_{j,i}^\top)}_{\mathbf{h}_3^\top}\right]_2 \\ \left[\underbrace{\sum_{j\in[L]\setminus\{i\}}\widehat{\mathbf{K}}_j(\mathbf{W}_j(\mathbf{I}_\omega\otimes\mathbf{B}\mathbf{r}_i^\top))}_{\mathbf{H}_4}, \underbrace{\sum_{j\in[L]\setminus\{i\}}\mathbf{W}_j(\mathbf{I}_\omega\otimes\mathbf{B}\mathbf{r}_i^\top)}_{\mathbf{H}_5}\right]_2 \end{array}\right)$$

$\mathsf{Enc}(\mathsf{mpk}, x, M)$**:** It takes mpk, $x \in \mathcal{X}_\kappa$, and $M \in G_\mathsf{T}$ as inputs, and outputs ct_x by computing as follows. It computes aux_c that is valid with respect to x as per Definition 3.1. It runs $(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$, $(m_1, m_2, \widehat{\mathbf{K}}_1) \leftarrow \mathsf{CVEncK}(y_1, \mathsf{aux}_k)$, $(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c)$, and $(m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(y_1, \mathsf{aux}_k)$. It samples $\mathbf{s}_0, \mathbf{s}_{1,1}, \ldots, \mathbf{s}_{m_1,n_1} \leftarrow \mathbb{Z}_p^k$, $\mathbf{t}_{1,1}, \ldots, \mathbf{t}_{m_1,n_3} \leftarrow \mathbb{Z}_p^{k+1}$, $\mathbf{u}_{\ell,2}, \ldots, \mathbf{u}_{\ell,m_3} \leftarrow \mathbb{Z}_p^{k+1}$ for $\ell \in [n_1]$, and computes

$$\mathbf{u}_{1,1} = \mathbf{s}_0\mathbf{P}_1,\ \mathbf{u}_{2,1} = \cdots = \mathbf{u}_{n_1,1} = \mathbf{0} \in \mathbb{Z}_p^{k+1},\ \overline{\mathbf{S}} = (\mathbf{s}_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_1]}$$
$$\overline{\mathbf{T}} = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_3]},\ \overline{\mathbf{U}} = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n_1]\times[m_3]}$$
$$\mathsf{ct}_x = \left(\begin{array}{l} \mathsf{aux}_c, [\underbrace{\mathbf{s}_0\mathbf{A}}_{\mathbf{c}_1}, \underbrace{\overline{\mathbf{S}}(\mathbf{I}_{n_1}\otimes\mathbf{A})}_{\mathbf{C}_2}, \underbrace{\mathbf{C}(\overline{\mathbf{S}}, \overline{\mathbf{T}}, \mathbf{P}_3)}_{\mathbf{C}_3}]_1 \\ \underbrace{[\overline{\mathbf{U}}(\mathbf{L}\otimes\mathbf{I}_{k+1}) + \overline{\mathbf{S}}^{\mathsf{BT}}\mathbf{P}_2]_1}_{\mathbf{C}_4}, \underbrace{[\mathbf{s}_0\mathbf{A}\mathbf{h}^\top]_\mathsf{T}M}_{C} \end{array}\right)$$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_x)$**:** It parses $\mathsf{sk}_i = \mathbf{V}_i$, $\mathsf{hsk}_i = ([\mathbf{h}_1^\top, \mathbf{h}_2^\top, \mathbf{h}_3^\top, \mathbf{H}_4, \mathbf{H}_5]_2)$, $\mathsf{ct}_x = ([\mathbf{c}_1, \mathbf{C}_2, \mathbf{C}_3, \mathbf{C}_4]_1, C)$ and runs $(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$ and $(\mathbf{E}, \overline{\mathbf{E}}) \leftarrow \mathsf{Pair}(x, y_i)$. It outputs $M' = C/[z_3 - z_1 - z_2]_\mathsf{T}$ where

$$[z_1]_\mathsf{T} = [\mathsf{tr}(\mathbf{E}(\underbrace{\mathbf{C}_3(\mathbf{I}_{n_2}\otimes\mathbf{h}_1^\top) - \mathbf{C}_2\widehat{\mathbf{C}}(\mathbf{H}_5)}_{\mathbf{Z}_1}))]_\mathsf{T}$$
$$[z_2]_\mathsf{T} = [\mathsf{tr}(\overline{\mathbf{E}}(\underbrace{\mathbf{C}_4(\mathbf{I}_{m_2}\otimes\mathbf{h}_1^\top) - \mathbf{C}_2^{\mathsf{BT}}\mathbf{H}_4}_{\mathbf{Z}_2}))]_\mathsf{T},\quad [z_3]_\mathsf{T} = [\mathbf{c}_1(\mathbf{h}_2^\top + \mathbf{h}_3^\top) + \mathbf{c}_1\mathbf{V}_i\mathbf{h}_1^\top]_\mathsf{T}$$

Completeness. It is obvious that the completeness of the above scheme holds from the perfect completeness of the QA-NIZK scheme.

Correctness. In decryption, we have

$$\begin{aligned} \mathbf{Z}_1 &= \mathbf{C}(\overline{\mathbf{S}}, \overline{\mathbf{T}}, \mathbf{P}_3)(\mathbf{I}_{n_2}\otimes\mathbf{h}_1^\top) - \overline{\mathbf{S}}(\mathbf{I}_{n_1}\otimes\mathbf{A})\widehat{\mathbf{C}}(\mathbf{H}_5) \\ &= \mathbf{C}(\overline{\mathbf{S}}, \overline{\mathbf{T}}(\mathbf{I}_{n_3}\otimes\mathbf{h}_1^\top), \mathbf{P}_3(\mathbf{I}_\omega\otimes\mathbf{h}_1^\top)) - \mathbf{C}(\overline{\mathbf{S}}, \mathbf{O}, \mathbf{A}\mathbf{H}_5) \\ &= \mathbf{C}(\overline{\mathbf{S}}, \overline{\mathbf{T}}(\mathbf{I}_{n_3}\otimes\mathbf{h}_1^\top), \mathbf{P}_3(\mathbf{I}_\omega\otimes\mathbf{h}_1^\top) - \mathbf{A}\mathbf{H}_5) \\ &= \mathbf{C}(\overline{\mathbf{S}}, \overline{\mathbf{T}}(\mathbf{I}_{n_3}\otimes\mathbf{B}\mathbf{r}_1^\top), \mathbf{A}\mathbf{W}_i(\mathbf{I}_\omega\otimes\mathbf{B}\mathbf{r}_i^\top)) \end{aligned}$$

where the second equality follows from Properties 3.2 and 3.3, and the third equality follows from Property 3.1,

$$\begin{aligned}\mathbf{Z}_2 = &\left(\mathbf{K}_i(\overline{\mathbf{S}}, \overline{\mathbf{U}}, \mathbf{A}\mathbf{W}_i) + \sum_{j\in[L]\setminus\{i\}} \mathbf{K}_j(\overline{\mathbf{S}}, \mathbf{O}, \mathbf{A}\mathbf{W}_j)\right)(\mathbf{I}_{n_2} \otimes \mathbf{h}_1^\top) - \overline{\mathbf{S}}^{\mathsf{BT}}(\mathbf{I}_{m_1} \otimes \mathbf{A})\mathbf{H}_4 \\ = &\left(\mathbf{K}_i(\overline{\mathbf{S}}, \overline{\mathbf{U}}, \mathbf{A}\mathbf{W}_i) + \sum_{j\in[L]\setminus\{i\}} \mathbf{K}_j(\overline{\mathbf{S}}, \mathbf{O}, \mathbf{A}\mathbf{W}_j)\right)(\mathbf{I}_{n_2} \otimes \mathbf{h}_1^\top) \\ &- \sum_{j\in[L]\setminus\{i\}} \mathbf{K}_j(\overline{\mathbf{S}}, \mathbf{O}, \mathbf{A}\mathbf{W}_j(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_i^\top)) \\ = &\mathbf{K}_i(\overline{\mathbf{S}}, \overline{\mathbf{U}}(\mathbf{I}_{m_3} \otimes \mathbf{B}\mathbf{r}_1^\top), \mathbf{A}\mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_i^\top))\end{aligned}$$

where $\mathbf{K}_i$ is the output of $\mathsf{EncK}(y_i, n_1, \mathsf{aux}_k)$, the first equality follows from the key well-formedness of the PES, the second equality follows from Property 3.3, and the third equality follows from Property 3.2, and

$$z_3 = \sum_{j\in[L]} \mathbf{s}_0\mathbf{A}\mathbf{W}_{j,0}\mathbf{B}\mathbf{r}_j^\top + \sum_{j\in[L]\setminus\{i\}} \mathbf{s}_0\mathbf{A}\mathbf{p}_{i,j}^\top + \mathbf{s}_0\mathbf{A}\mathbf{h}^\top + \mathbf{s}_0\mathbf{A}\mathbf{V}_i\mathbf{B}\mathbf{r}_i^\top$$

Observe that $z_1+z_2 = \mathsf{tr}(\mathbf{E}\mathbf{Z}_1)+\mathsf{tr}(\overline{\mathbf{E}}\mathbf{Z}_2) = \mathbf{s}_0\mathbf{P}_1\mathbf{B}\mathbf{r}_i^\top = \sum_{j\in[L]} \mathbf{s}_0(\mathbf{A}\mathbf{W}_{j,0}+\mathbf{T}_j)\mathbf{B}\mathbf{r}_i^\top$, which follows from Property 3.4. Hence, we have $z_3 - z_1 - z_2 = \mathbf{s}_0\mathbf{A}\mathbf{h}^\top$ and $M = M'$, which follows from $\mathbf{A}\mathbf{p}_{i,j}^\top = \mathbf{T}_i\mathbf{B}\mathbf{r}_j^\top$ for $i \neq j$ and $\mathbf{T}_i = \mathbf{A}\mathbf{V}_i$.

Compactness. Since Γ satisfies key well-formedness, for any $Y \in \mathcal{Y}_\kappa$, we have $|\mathsf{aux}_k|, |m_1|, |m_2| = \mathsf{poly}\left(\max_{y\in Y} |y|\right)$. For mpk, it is obvious that

$$\begin{aligned}&|\mathbf{A}\mathbf{h}^\top|, |\mathbf{A}|, |\mathbf{P}_1|, |\mathbf{P}_3| = \mathsf{poly}(\log p) = \mathsf{poly}(\lambda) \\ &|y_1|, |\mathsf{aux}_k|, |\mathbf{P}_2| = \mathsf{poly}(\max_{y\in Y} |y|, \log p) = \mathsf{poly}(\max_{y\in Y} |y|, \lambda)\end{aligned}$$

and thus $|\mathsf{mpk}| = \mathsf{poly}(\max_{y\in Y} |y|, \lambda)$. Similarly, we have

$$|\mathbf{h}_1|, |\mathbf{h}_2|, |\mathbf{h}_3|, |\mathbf{H}_5| = \mathsf{poly}(\lambda), \quad |\mathsf{aux}_k|, |\mathbf{H}_4| = \mathsf{poly}(\max_{y\in Y} |y|, \lambda)$$

and $|\mathsf{hsk}_i| = \mathsf{poly}(\max_{y\in Y} |y|, \lambda)$ for $i \in [L]$.

Efficiency in Terms of PES Parameters. If we instantiate PES with the parameters $(\omega, n_1, n_2, n_3, m_1, m_2, m_3)$ as defined in Definition 3.1, the resulting sReg-ABE scheme achieves the following sizes, measured in terms of the number of group elements (in G_1, G_2, G_T, except all sk_i elements are in $\mathbb{Z}_p$). Note that mpk also contains aux_k, y_1 besides group elements (similarly, hsk_i has aux_k).

$$\begin{aligned}&|\mathsf{crs}| = O(\omega L^2), \qquad &&|\mathsf{pk}_i| = O(L), \qquad &&|\mathsf{hsk}_i| = O(m_1m_2 + \omega), \\ &|\mathsf{mpk}| = O(m_1m_2 + \omega), &&|\mathsf{sk}_i| = O(1), &&|\mathsf{ct}| = O(m_1n_1 + m_1n_2 + n_1m_2).\end{aligned}$$

Note that we treat k from MDDH_k as a constant (*e.g.,* MDDH_1 is implied by the SXDH assumption); if we explicitly include k, at most $O(k^2)$ appears multiplicatively in each term.

6.2 Security

Theorem 6.1. *If Π satisfies perfect zero-knowledge and stronger unbounded simulation soundness for linear space, and the MDDH assumption holds, then our sReg-ABE scheme satisfies the security defined in Definition 2.4.*

Proof. Following the proof strategy outlined in the ZZGQ scheme [ZZGQ23, Section 3], we establish a series of hybrids. A key distinction from ZZGQ lies in our reliance on the KE-ind property of PES to demonstrate the indistinguishability of hybrids within $\mathsf{H}_{5,v}$, as defined below, contrasting with their use of the security property of predicate encodings. It is important to note that while the security of predicate encodings is an information-theoretic notion, KE-ind is a computational one. Consequently, constructing a reduction is necessary, rendering this part somewhat more intricate compared to ZZGQ.

G_0**:** This is the original game. In this game, the adversary is given the following elements from the challenger:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}]_1, [\mathbf{A}\mathbf{h}^\top]_\mathsf{T}, \{\mathsf{crs}_i, [\boxed{\mathbf{R}_i}_{\mathsf{H}_2,\mathsf{H}_4}, \mathbf{A}\mathbf{W}_{i,0}, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\underbrace{\mathbf{B}\mathbf{r}_i^\top}_{\mathbf{f}_i^\top}, \underbrace{\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top}_{\boxed{\mathbf{g}_i^\top}_{\mathsf{H}_{5,i}}}]_2\}_{i\in[L]}, \{[\underbrace{\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_j^\top}_{\mathbf{n}_{i,j}^\top}, \underbrace{\mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_j^\top)}_{\mathbf{N}_{i,j}}]_2\}_{\substack{i,j\in[L]\\ i\neq j}} \end{pmatrix}$$

where each element is computed as described in Setup in Section 6.1,

$$\mathsf{pk}_i^\ell = \Big([\underbrace{\mathbf{A}\mathbf{V}_i^\ell}_{\mathbf{T}_i^\ell}, \underbrace{\mathbf{R}_i\mathbf{V}_i^\ell}_{\mathbf{Q}_i^\ell}]_1, \{[\underbrace{\mathbf{V}_i^\ell\mathbf{B}\mathbf{r}_j^\top}_{\mathbf{p}_{i,j}^{\ell\top}}]_2\}_{j\in[L]\setminus\{i\}}, \boxed{\pi_i^\ell}_{\mathsf{H}_1}\Big), \quad \mathsf{sk}_i^\ell = \mathbf{V}_i^\ell$$

from the ℓ-th query $\mathsf{OGen}(i)$ and $\mathsf{OCor}(i, \mathsf{pk}_i^\ell)$, respectively, where each element is computed as described in Gen in Section 6.1, and the challenge ciphertext ct_x:

$$\Big(\mathsf{aux}_c, [\underbrace{\mathbf{s}_0\mathbf{A}}_{\boxed{\mathbf{c}_1}_{\mathsf{H}_4}}, \underbrace{\overline{\mathbf{S}}(\mathbf{I}_{n_1} \otimes \mathbf{A})}_{\mathbf{C}_2}, \underbrace{\mathbf{C}(\overline{\mathbf{S}}, \overline{\mathbf{T}}, \mathbf{P}_3)}_{\mathbf{C}_3}]_1, [\underbrace{\overline{\mathbf{U}}(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}^{\mathsf{BT}}\mathbf{P}_2}_{\mathbf{C}_4}]_1, \underbrace{[\mathbf{s}_0\mathbf{A}\mathbf{h}^\top]_\mathsf{T} M_\beta}_{\boxed{C}_{\mathsf{H}_4,\mathsf{H}_6}}\Big)$$

with respect to the attributes $x, \{y_i\}_{i\in[L]}$ and the challenge public keys $\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{p}_{i,j}^{*\top}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$, where $\beta \leftarrow \{0,1\}$, $\boxed{\mathbf{u}_{1,1}}_{\mathsf{H}_3,\mathsf{H}_4} = \mathbf{s}_0\mathbf{P}_1$ (the $(1,1)$-th element of $\overline{\mathbf{U}}$), $\mathbf{P}_1 = \sum_{i\in[L]} \mathbf{A}\mathbf{W}_{i,0} + \mathbf{T}_i^*$, $\mathbf{P}_2 = \sum_{i\in[L]} \widehat{\mathbf{K}}_i(\mathbf{A}\mathbf{W}_i)$, $\mathbf{P}_3 = \sum_{i\in[L]} \mathbf{A}\mathbf{W}_i$ and other elements are computed as described in Enc in Section 6.1. The boxed elements $\boxed{\text{element}}_{\mathsf{H}_j}$ will be changed in hybrid H_j.

H_1**:** It is the same as G_0 except that the reply from $\mathsf{OGen}(i)$ is changed. Specifically, π_i^ℓ for all (i, ℓ) is generated as $\pi_i^\ell \leftarrow \mathsf{LSim}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{M}_i^\ell]_1)$ instead of $\mathsf{LProve}(\mathsf{crs}_i, [\mathbf{M}_i^\ell]_1, \mathbf{V}_i^\ell)$ where $\mathbf{M}_i^\ell = \begin{pmatrix} \mathbf{T}_i^\ell \\ \mathbf{Q}_i^\ell \end{pmatrix}$.

H_2**:** It is the same as H_1 except that $[\mathbf{R}_i]_1$ in crs is defined as $\mathbf{R}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix} \mathbf{s}_0\mathbf{A} \\ \mathbf{I}_{2k+1} \end{pmatrix}$ where $\widetilde{\mathbf{R}}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}, \mathbf{s}_0 \leftarrow \mathbb{Z}_p^k$, instead of $\mathbf{R}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}$. Note that $\mathbf{s}_0$ is also used for generating the challenge ciphertext ct_x.

H_3**:** It is the same as H_2 except that we change the way $[\mathbf{C}_4]_1$ in ct_x is generated. Recall that $\mathbf{u}_{1,1} = \mathbf{s}_0\mathbf{P}_1$ (the $(1,1)$-th element of $\overline{\mathbf{U}}$), where $\mathbf{P}_1 = \sum_{i\in[L]}(\mathbf{A}\mathbf{W}_{i,0} + \mathbf{T}_i^*)$. In H_3, $\mathbf{u}_{1,1}$ is generated as $\sum_{i\in[L]}(\mathbf{s}_0\mathbf{A}\mathbf{W}_{i,0} + \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*)$ where $\mathbf{e}_1 = (1, 0, \ldots, 0)$.

H_4**:** It is the same as H_2 except that we replace the term $\mathbf{s}_0\mathbf{A}$ with $\mathbf{c} \leftarrow \mathbb{Z}_p^{2k+1}$. Specifically, we defined $\mathbf{R}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix} \mathbf{c} \\ \mathbf{I}_{2k+1} \end{pmatrix}$ in crs and $\mathbf{c}_1 = \mathbf{c}, \mathbf{u}_{1,1} = \sum_{i\in[L]}(\mathbf{c}\mathbf{W}_{i,0} + \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*), C = [\mathbf{c}\mathbf{h}^\top]_\mathsf{T} M_\beta$ in ct_x.

$\mathsf{H}_{5,v}(v \in [L])$**:** It is the same as H_4 except that $\mathbf{g}_i$ in crs is defined as $\mathbf{g}_i = \mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top + \boxed{\alpha_i\mathbf{a}^{\perp\top}}$ for $i \in [v]$ instead of $\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top$ where $\alpha_i \leftarrow \mathbb{Z}_p, \mathbf{a} \leftarrow \mathbb{Z}_p^{2k+1}$ conditioned on $\mathbf{a}^\perp\mathbf{A} = \mathbf{0}$.

H_6**:** It is the same as $\mathsf{H}_{5,L}$ except that C in ct_x is generated as $C \leftarrow G_\mathsf{T}$ instead of $[\mathbf{c}\mathbf{h}^\top]_\mathsf{T} M_\beta$.

Observe that the adversary does not obtain the information of β in H_6. Theorem 6.1 follows from Lemmata D.1 to D.6 in §D. □

7 Applications and Comparisons

7.1 sReg-ABE for Unbounded Span Programs

We describe applications of our framework, namely, ciphertext-policy sReg-ABE for completely-unbounded monotone, non-monotone, general non-monotone span programs (MSP, NMSP, GNMSP). Thanks to our generic sReg-ABE construction from PES, it suffices to state our results on respective PESs here. We emphasize that the term "completely unbounded" refers to the property of span program predicates. Outside the predicate, sReg-ABE also specifies the parameter L on the number of slots (or also called users). We recall that our sReg-ABE schemes are bounded-user schemes, similarly to prior pairing-based schemes [HLWW23, ZZGQ23].

Definition 7.1. The predicate of completely unbounded ciphertext-policy monotone span programs (MSP) $\mathsf{P}^{\mathsf{CP-MSP}} : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$ for large attribute universe $\mathcal{X}_\kappa = \mathbb{Z}_p$ is defined as follows. Let $\bar{\mathcal{Y}}_\kappa = 2^{\mathcal{X}_\kappa}$ and $\bar{\mathcal{X}}_\kappa = \bigcup_{(n,m)\in\mathbb{N}^2}(\mathbb{Z}_p^{n\times m} \times \varPhi_n)$, where $\varPhi_n$ consists of all functions $\phi : [n] \to \mathcal{X}_\kappa$. For $S \subseteq \mathcal{X}_\kappa$ (*i.e.*, $S \in \bar{\mathcal{Y}}_\kappa$) and $(\mathbf{M}, \phi) \in \bar{\mathcal{X}}_\kappa$ where $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$ and $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$, we define

$$\mathsf{P}_\kappa^{\mathsf{CP-MSP}}((\mathbf{M},\phi), S) = 1 \Leftrightarrow (1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in[n]:\phi(i)\in S}).$$

We can see that the completely unbounded property of the predicate is enforced by the predicate definition: it has a large universe and has no bound on policy size $n \times m$ (or any multi-use restriction on ϕ) or attribute set size for S.

Theorem 7.1. *There exists a PES for sReg-ABE for the completely unbounded ciphertext-policy monotone span programs with large universe $\mathcal{U} = \mathbb{Z}_p$ which satisfies key well-formedness and* KE-ind*, while achieving parameters $\omega = 5$, $(n_1, n_2, n_3) = (n+1, 2n, m-1)$, and $(m_1, m_2, m_3) = (\delta+1, \delta+1, 1)$, where $n \times m$ is the size of the ciphertext policy $(\mathbf{M}, \phi)$ and $\delta = \mathsf{aux}_k$ is the auxiliary input that defines key well-formedness, which is $\delta = \max_{i\in[L]} |S_i|$ for a set of registered key attribute sets $Y = \{S_1, \dots, S_L\} \subset \mathcal{U}$, where L is the number of slots for sReg-ABE.*

Proof sketch. Let $\mathsf{P}^{\mathsf{IBE}}$ be the equality predicate (IBE), $\mathsf{P}^{\mathsf{IBE}} : \mathbb{Z}_p \times \mathbb{Z}_p \to \{0,1\}$ with $\mathsf{P}^{\mathsf{IBE}}(x,y) = 1 \Leftrightarrow x = y$. We can show the following predicate implication:

$$\mathsf{Dual}[\mathsf{KP1}[\mathsf{Dual}[\mathsf{KP1}_{\mathsf{OR}}[\mathsf{Null}[\mathsf{P}^{\mathsf{IBE}}]]]]] \Rightarrow \mathsf{P}^{\mathsf{CP-MSP}}.$$

This implication sequence follows the approach from [Att19, AT20], with differences in using Null (§4.1) and key-policy disjunction (§4.3), instead of the OR key-policy augmentation as in [Att19, AT20]. While we also have OR key-policy augmentation (§4.7), it preserves well-formedness for only ciphertext side; contrastingly, the key-policy disjunction preserves both. Details of this sequence are provided in §E.2, including explicit PES descriptions for self-containment and parameter sizes. Beginning with predicate encoding for IBE [CGW15, Att19], we derive a PES for $\mathsf{P}^{\mathsf{CP-MSP}}$ via successive transformations. As discussed in Theorem 5.1, this sequence ends with "KP1 then Dual", thus the resulting PES achieves key well-formedness and KE-ind. □

Definition 7.2. The predicate of completely unbounded ciphertext-policy *non-monotone* span programs $\mathsf{P}^{\mathsf{CP-NMSP}} : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$ for large attribute universe $\mathcal{X}_\kappa = \mathbb{Z}_p$ is defined as follows. Let $\bar{\mathcal{Y}}_\kappa = 2^{\mathcal{X}_\kappa}$ and $\bar{\mathcal{X}}_\kappa = \bigcup_{(n,m)\in\mathbb{N}^2}(\mathbb{Z}_p^{n\times m} \times \varPhi_n)$, where $\varPhi_n$ consists of all functions $\phi : [n] \to (\{\mathsf{pos}, \mathsf{neg}\} \times \mathcal{X}_\kappa)$. For $S \subseteq \mathcal{X}_\kappa$ (*i.e.*, $S \in \bar{\mathcal{Y}}_\kappa$) and $(\mathbf{M}, \phi) \in \bar{\mathcal{X}}_\kappa$ where $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$ and $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$, we define

$$\mathsf{P}_\kappa^{\mathsf{CP-MSP}}((\mathbf{M},\phi), S) = 1 \Leftrightarrow (1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in[n] \text{ s.t. } \mathsf{P}'(\phi,S)=1}),$$

$$\mathsf{P}'(\phi, S) = 1 \Leftrightarrow \Big(\phi_1(i) = \mathsf{pos} \wedge \phi_2(i) \in S\Big) \vee \Big(\phi_1(i) = \mathsf{neg} \wedge \phi_2(i) \notin S\Big).$$

Table 3. Efficiency comparison among ciphertext-policy slotted registered ABE schemes for *span program predicates.*

Schemes	$\lvert\mathsf{crs}\rvert$	$\lvert\mathsf{pk}_i\rvert$	$\lvert\mathsf{sk}_i\rvert$	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{hsk}_i\rvert$	$\lvert\mathsf{ct}\rvert$
HLWW-1 [HLWW23, §5] (Pairing-based)	$O(\mathsf{B}_{\mathcal{U}}L^2\mathsf{c}(\lambda))$	$O(L\mathsf{c}(\lambda))$	$O(\mathsf{c}(\lambda))$	$O(\mathsf{B}_{\mathcal{U}}\mathsf{c}(\lambda))$	$O(\mathsf{B}_{\mathcal{U}}\mathsf{c}(\lambda))$	$O(n\mathsf{c}(\lambda))$
HLWW-2 [HLWW23, §7]† (iO-based)	$\mathsf{poly}(\lambda, \mathsf{B}_{\lvert S\rvert}, \log \mathsf{B}_{\mathcal{U}}, \log L)$	$O(\lambda)$	$O(\lambda)$	$\mathsf{poly}(\lambda, \mathsf{B}_{\lvert S\rvert}, \log \mathsf{B}_{\mathcal{U}}, \log L)$	$\mathsf{poly}(\lambda, \mathsf{B}_{\lvert S\rvert}, \log \mathsf{B}_{\mathcal{U}}, \log L)$	$\lvert iO(C^\star)\rvert$
FWW [FWW23]† (WE-based)	$\mathsf{poly}(\lambda, \mathsf{B}_{\lvert S\rvert}, \mathsf{B}_n, \mathsf{B}_m, \log \mathsf{B}_{\mathcal{U}}, \log L)$	$\mathsf{poly}(\lambda)$	$O(\lambda)$	$\mathsf{poly}(\lambda, \log L)$	$\mathsf{poly}(\lambda, \mathsf{B}_{\lvert S\rvert}, \log \mathsf{B}_{\mathcal{U}}, \log L)$	$\lvert\text{WE}.\mathsf{ct}\rvert$
ZZGQ [ZZGQ23, §D1]	$O((\mathsf{B}_{\mathcal{U}} + \mathsf{B}_m)L^2\mathsf{p}(\lambda))$	$O(L\mathsf{p}(\lambda))$	$O(\mathsf{p}(\lambda))$	$O((\mathsf{B}_{\mathcal{U}} + \mathsf{B}_m)\mathsf{p}(\lambda))$	$O((\mathsf{B}_{\mathcal{U}} + \mathsf{B}_m)\mathsf{p}(\lambda))$	$O(\mathsf{B}_{\mathcal{U}}\mathsf{p}(\lambda))$
Ours 1,2,3	$O(L^2\mathsf{p}(\lambda))$	$O(L\mathsf{p}(\lambda))$	$O(\mathsf{p}(\lambda))$	$O(\delta^2\mathsf{p}(\lambda))$	$O(\delta^2\mathsf{p}(\lambda))$	$O(\delta n\mathsf{p}(\lambda))$

Note: λ is the security parameter. L is the number of users (slots) in slotted registered ABE. As a convection, we use B_x to refer to the maximum bound for an amount x that is required to be fixed at setup for that scheme. $\mathsf{B}_{\mathcal{U}} = \lvert\mathcal{U}\rvert$ denotes the attribute universe size. $n \times m$ denotes the size of a span program policy; $\mathsf{B}_n, \mathsf{B}_m$ are their bounds, resp. $\lvert S\rvert$ denotes the size of an attribute set; $\mathsf{B}_{\lvert S\rvert}$ is its bound. Let $\mathsf{p}(\lambda) = \mathsf{poly}(\lambda), \mathsf{c}(\lambda) = \mathsf{poly}(\lambda)$ specify the sizes of one group element in prime-order and composite-order pairing groups, resp. For our schemes, $\delta = \max_{i\in[L]} \lvert S_i\rvert$ for a set of registered key attribute sets $Y = \{S_1, \ldots, S_L\}$ where $S_i \subset \mathcal{U} = \mathbb{Z}_p$. In the pairing-based scheme of [HLWW23], denoted as HLWW-1, and the ZZGQ scheme, there exist also implicit bounds $\mathsf{B}_{\lvert S\rvert}, \mathsf{B}_n$ where $\mathsf{B}_{\lvert S\rvert} = \mathsf{B}_n = \mathsf{B}_{\mathcal{U}}$. For these two schemes, we consider their (default) one-use schemes. †: The iO/WE-based schemes of [HLWW23, FWW23], denoted as HLWW-2/FWW, respectively, are originally for circuit predicates; we envision instantiating a circuit to implement a span program and write the efficiency of its resulting scheme for span programs here. Their $\lvert iO(C^\star)\rvert$ and $\lvert\text{WE}.\mathsf{ct}\rvert$ are described in the text below.

Theorem 7.2. *There exists a PES for sReg-ABE for completely unbounded ciphertext-policy non-monotone span programs with large universe $\mathcal{U} = \mathbb{Z}_p$ which satisfies key well-formedness and* KE-ind, *while achieving parameters $\omega = 10$, $(n_1, n_2, n_3) = (n + 1, 4n, m - 1)$, $(m_1, m_2, m_3) = (\delta + 1, 3\delta + 1, \delta)$, where n, m, δ are as in Theorem 7.1.*

Proof sketch. Let $\mathsf{P}^{\mathsf{NIBE}}$ be the negated IBE ($\mathsf{P}^{\mathsf{NIBE}}(x, y){=}1 \leftrightarrow x \neq y$). We show:

$$\mathsf{SPC}_{\mathsf{OR}}[\ \mathsf{Null}[\mathsf{KP1}_{\mathsf{OR}}[\mathsf{Null}[\mathsf{P}^{\mathsf{IBE}}]]],\quad \mathsf{Null}[\mathsf{KP1}_{\mathsf{AND}}[\mathsf{WC}[\mathsf{P}^{\mathsf{NIBE}}]]]\ ] \Rightarrow \mathsf{P}^{\mathsf{TIBBE}},$$
$$\mathsf{Dual}[\mathsf{KP1}[\mathsf{Dual}[\mathsf{P}^{\mathsf{TIBBE}}]]] \Rightarrow \mathsf{P}^{\mathsf{CP-NMSP}}.$$

This sequence roughly follows [Att19, AT20], using an intermediate predicate called two-mode IBBE (TIBBE), which operates in two modes, combining IBBE and its negation. Our approach to obtaining PES for $\mathsf{P}^{\mathsf{TIBBE}}$ differs from [Att19, AT20]. We use static OR composition with Null to split the modes, and non-membership is handled with WC and key-policy conjunction instead of AND key-policy augmentation as in [Att19, AT20]. Note that while we have AND key-policy augmentation, its PES transformation preserves well-formedness for only ciphertext side, while the key-policy conjunction preserves both. The rest can be argued similarly to the previous lemma. See Appendix E.3 for details and parameter sizes. □

PES for General Non-monotone Span Programs (GNMSP). The above non-monotone predicate is a simple type, originally defined in [OSW07], and is thus called the OSW type. There is another type from [OT10], called the OT type, where an element in an attribute set also takes input a *label* with it, but the "atomic" policy check is merely an equality check. A more complex type that unifies both types was suggested in [AT20], which we call GNMSP here, can deal with labels and set membership at the same time. We recap the definition and provide how to obtain PES for sReg-ABE for this in Appendix E.4.

7.2 Efficiency and Comparison to Previous Works

In Table 3, we describe asymptotic efficiency of our sReg-ABE schemes specified by the above three PESs for span programs, and compare to prior works [HLWW23, FWW23, ZZGQ23]. Details regarding the parameters are provided in the table notes. Via the conversion of [HLWW23], one can obtain full-fledged registered ABE with size expansion by at most polylogarithmic in L for all the six parameters in the table. It is thus sufficient to compare among (un)bounded slotted registered ABE schemes.

Comparing to Pairing-based Schemes. The table explicitly displays relevant bounds in each scheme, facilitating the discussion of boundedness as presented in Table 1. Notably, our schemes do not impose any bounds on the properties of the span program predicates. On the other hand, it places a bound on L, the number of users (slots). The previous two pairing-based schemes, HLWW-1 and ZZGQ, also impose the user bound. Additionally, and perhaps more prominently in our context, both schemes require linear bounds $\mathsf{B}_{\mathcal{U}}$ on the universe size, hence they are considered as small-universe schemes. They also implicitly have linear bounds, denoted as $\mathsf{B}_{|S|}$ and B_n, respectively, on attribute set sizes and span program policy row sizes (both equal to the universe size). The ZZGQ scheme additionally imposes a bound B_m on span program policy column sizes. Furthermore, the HLWW-1 and ZZGQ schemes are restricted to "one-use" of attributes in a policy, necessitating the map ϕ of span program to be injective. Generalizing them to bounded multi-use schemes would incur some size expansion due to this bound. Contrastingly, our schemes achieve the unbounded multi-use property.

Comparing to iO/WE-based Schemes. Comparing our scheme to the iO-based and WE-based schemes of [HLWW23, FWW23], denoted as HLWW-2 and FWW, respectively, is more challenging as they target different predicates, specifically bounded-input-length Boolean circuits. We envision instantiating a Boolean circuit to implement a span program to compare slotted registered ABE with similar functionalities as ours.

For the HLWW-2 scheme, due to the various possibilities of circuit instantiations together with the choices of building block constructions (iO, somewhere-statistically-binding hash (SSB) hash, and PRG), we have left $|\mathsf{ct}|$ simply as the size of the obfuscated program for an embedded circuit defined in [HLWW23], denoted as $C^\star$. This circuit embeds a ciphertext policy (a circuit implementing a span program policy) and some non-black-box descriptions of its underlying cryptographic primitives, such as SSB hash and PRG. As $C^\star$ embeds mpk, the complexity of $|iO(C^\star)|$ is at least that of $|\mathsf{mpk}|$, but could be much larger due to the non-black-box usage of primitives and the potentially large overhead from iO constructions. Similarly, for the FWW scheme, its $|\mathsf{ct}|$ corresponds to the ciphertext size of WE for a relation involving a ciphertext policy and some non-black-box descriptions of its underlying cryptographic primitives, such as function-binding hash (FBH) and public-key encryption.

Regardless of circuit instantiations and building block choices, the bounded-input-length restriction of circuits in both the HLWW-2 and FWW schemes will yield a slotted registered ABE scheme for bounded attribute set sizes. Specifically, we require a bound on the attribute set size $\mathsf{B}_{|S|}$, and the input length to circuits needs to be $\mathsf{B}_{|S|} \log \mathsf{B}_{\mathcal{U}}$ to accommodate an arbitrary attribute set of this size. Additionally, the FWW scheme requires fixing the maximum policy size in advance, which is reflected in the policy-size bounds $\mathsf{B}_n, \mathsf{B}_m$ in crs. Following the size inspection as in [HLWW23, FWW23], we obtain $|\mathsf{crs}|$, $|\mathsf{mpk}|$, and $|\mathsf{hsk}_i|$ at least as detailed in the table. These sizes depend on the choices of their respective building block constructions.

In summary, the HLWW-2 and FWW schemes depend only polylogarithmically on $\mathsf{B}_{|\mathcal{U}|}$ and L, making them large-universe and unbounded-user schemes. The HLWW-2 scheme depends linearly on $\mathsf{B}_{|S|}$, and thus imposes a bound on attribute set sizes. Non-monotone polynomial-size Boolean circuits can simulate polynomial-size non-monotone span programs. As iO schemes do not restrict circuit sizes by definition [GGH$^+$13, JLS21], the HLWW-2 scheme can achieve unbounded policy sizes, multi-use, and non-monotonicity. Contrastingly, the FWW scheme does not seem to achieve unbounded policy sizes and multi-use, as it requires fixing the maximum policy size in advance.

Acknowledgement. The authors would like to thank anonymous reviewers for their insightful comments and constructive suggestions. Nuttapong Attrapadung was supported by JSPS KAKENHI Grant Number JP19H01109 and JST CREST Grant Number JPMJCR22M1, Japan.

References

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, Heidelberg, August 2017.

AC17. Shashank Agrawal and Melissa Chase. Simplifying design and analysis of complex predicate encryption schemes. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 627–656. Springer, Heidelberg, April / May 2017.

AHY15. Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada. Conversions among several classes of predicate encryption and applications to ABE with various compactness tradeoffs. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 575–601. Springer, Heidelberg, November / December 2015.

AT20. Nuttapong Attrapadung and Junichi Tomida. Unbounded dynamic predicate compositions in ABE from standard assumptions. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 405–436. Springer, Heidelberg, December 2020.

Att14. Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 557–577. Springer, Heidelberg, May 2014.

Att19. Nuttapong Attrapadung. Unbounded dynamic predicate compositions in attribute-based encryption. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part I*, volume 11476 of *LNCS*, pages 34–67. Springer, Heidelberg, May 2019.

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

BH08. Dan Boneh and Michael Hamburg. Generalized identity based and broadcast encryption schemes. In Josef Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 455–470. Springer, Heidelberg, December 2008.

CES21. Kelong Cong, Karim Eldefrawy, and Nigel P. Smart. Optimizing registration based encryption. In Maura B. Paterson, editor, *18th IMA International Conference on Cryptography and Coding*, volume 13129 of *LNCS*, pages 129–157. Springer, Heidelberg, December 2021.

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

DKL$^+$23. Nico Döttling, Dimitris Kolonelos, Russell W. F. Lai, Chuanwei Lin, Giulio Malavolta, and Ahmadreza Rahimi. Efficient laconic cryptography from learning with errors. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 417–446. Springer, Heidelberg, April 2023.

DPY23. Pratish Datta, Tapas Pal, and Shota Yamada. Registered fe beyond predicates: (attribute-based) linear functions and more. Cryptology ePrint Archive, Paper 2023/457, 2023. https://eprint.iacr.org/2023/457.

EHK$^+$13. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013.

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*, volume 14442, pages 98–133. Springer, 2023.

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*, volume 14442, pages 166–200. Springer, 2023.

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, Heidelberg, August 2023.

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.

GHM$^+$19. Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, Ahmadreza Rahimi, and Sruthi Sekar. Registration-based encryption from standard assumptions. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 63–93. Springer, Heidelberg, April 2019.

GHMR18. Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, and Ahmadreza Rahimi. Registration-based encryption: Removing private-key generator from IBE. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018, Part I*, volume 11239 of *LNCS*, pages 689–718. Springer, Heidelberg, November 2018.

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, 2023.

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.

GV20. Rishab Goyal and Satyanarayana Vusirikala. Verifiable registration-based encryption. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 621–651. Springer, Heidelberg, August 2020.

HLWW23. Susan Hohenberger, George Lu, Brent Waters, and David J. Wu. Registered attribute-based encryption. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 511–542. Springer, Heidelberg, April 2023.

JLS21. Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from well-founded assumptions. In Samir Khuller and Virginia Vassilevska Williams, editors, *53rd ACM STOC*, pages 60–73. ACM Press, June 2021.

JR13. Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, Heidelberg, December 2013.

KW15. Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, April 2015.

KW19. Lucas Kowalczyk and Hoeteck Wee. Compact adaptively secure ABE for NC^1 from k-Lin. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part I*, volume 11476 of *LNCS*, pages 3–33. Springer, Heidelberg, May 2019.

LW11. Allison B. Lewko and Brent Waters. Unbounded HIBE and attribute-based encryption. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 547–567. Springer, Heidelberg, May 2011.

OSW07. Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *ACM CCS 2007*, pages 195–203. ACM Press, October 2007.

OT10. Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, Heidelberg, August 2010.

Wat09. Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, Heidelberg, August 2009.

Wat12. Brent Waters. Functional encryption for regular languages. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 218–235. Springer, Heidelberg, August 2012.

Wee14. Hoeteck Wee. Dual system encryption via predicate encodings. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer, Heidelberg, February 2014.

ZZGQ23. Ziqi Zhu, Kai Zhang, Junqing Gong, and Haifeng Qian. Registered ABE via predicate encodings. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023*, volume 14442, pages 66–97. Springer, 2023.

A Matrix Substitution from Simplified to Full-fledged Schemes

From the simplified scheme in the technical overview (§1.2) to our full-fledged scheme, we use the following substitution of variables to vectors/matrices:

$$\begin{aligned}
&\alpha \mapsto \mathbf{h}^\top,\ \ w_{j,0} \mapsto \mathbf{W}_{j,0},\ \ \mathbf{w}_j \mapsto \mathbf{W}_j \\
&r_i \mapsto \mathbf{B}\mathbf{r}_i^\top,\ \ r_i w_{j,0} \mapsto \mathbf{W}_{j,0}\mathbf{B}\mathbf{r}_i^\top,\ \ r_i\mathbf{w}_j \mapsto \mathbf{W}_{j,0}(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_i^\top),\ \ \mathbf{v}_i \mapsto \mathbf{V}_i, \\
&s_0 \mapsto \mathbf{s}_0\mathbf{A},\ \ \mathbf{S}' \mapsto \overline{\mathbf{S}}(\mathbf{I}_{n_1} \otimes \mathbf{A}),\ \ \mathbf{T} \mapsto \overline{\mathbf{T}},\ \ \mathbf{U} \mapsto \overline{\mathbf{U}},\ \ \mathbf{S}'(\mathbf{I}_{n_1} \otimes \mathbf{w}_j) \mapsto \overline{\mathbf{S}}(\mathbf{I}_{n_1} \otimes \mathbf{A}\mathbf{W}_j)
\end{aligned}$$

where $\mathbf{h} \leftarrow \mathbb{Z}_p^{2k+1}$, $\mathbf{W}_{j,0} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$, $\mathbf{W}_j \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{r} \leftarrow \mathbb{Z}_p^k$, $\mathbf{V}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$, $\mathbf{s}_0 \leftarrow \mathbb{Z}_p^k$, $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$, $\overline{\mathbf{S}} \leftarrow \mathbb{Z}_p^{m_1\times kn_1}$, $\overline{\mathbf{T}} \leftarrow \mathbb{Z}_p^{m_1\times(k+1)n_3}$, $\overline{\mathbf{U}} \leftarrow \mathbb{Z}_p^{n_1\times(k+1)m_3}$:

B Registered ABE

We follow the definition of bounded-user registered ABE in [HLWW23,ZZGQ23]. The definition below is taken mostly verbatim from [ZZGQ23, Appendix A].

Our definition is slightly different from the previous definition in compactness. More precisely, since we now consider Reg-ABE with unbounded properties of predicates, attribute sizes are therefore not a priori bounded. We modify the compactness definition so as to allow $|\mathsf{mpk}|$ and $|\mathsf{hsk}|$ to depend on the size of the longest attribute registered so far.

Definition B.1 (Bounded-user Registered ABE [HLWW23,ZZGQ23]). Let $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa$ be a predicate indexed by κ, where κ specifies some parameters. Let $\mathcal{M}$ be a message space. A bounded-user registered ABE scheme for $\mathcal{P}_\kappa$ consists of the following algorithms.

$\mathsf{Setup}(1^\lambda, 1^L, \kappa)$**:** It takes a security parameter 1^λ, the number of users in unary 1^L, and an index κ as input, and outputs a common reference string crs.[11]

$\mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$**:** It takes crs and a public state aux as input, and outputs a public key pk and a secret key sk.

$\mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, y)$**:** It takes $\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, y \in \mathcal{Y}$ as input, and outputs a master public key mpk and updated state aux.

$\mathsf{Enc}(\mathsf{mpk}, x, M)$**:** It takes mpk, $x \in \mathcal{X}_\kappa$, and a message $M \in \mathcal{M}$ as inputs, and outputs a ciphertext ct_x.

$\mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk})$**:** It takes $(\mathsf{crs}, \mathsf{aux}, \mathsf{pk})$ as input and outputs a helper secret key hsk.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{hsk}, \mathsf{ct}_x)$**:** It takes $(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_x)$ as input, and outputs a message M or a symbol $\perp$ or a special flag `getupd` to indicate the need of an updated helper key.

Correctness. For all stateful adversary $\mathcal{A}$, the following advantage function is negligible in λ:

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

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

- $\mathsf{ORegNT}(\mathsf{pk}, y)$: run $(\mathsf{mpk}, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}, y)$, update $\mathsf{aux} = \mathsf{aux}'$, append $(\mathsf{mpk}, \mathsf{aux})$ to $\mathcal{R}$ and return $(|\mathcal{R}|, \mathsf{mpk}, \mathsf{aux})$;
- $\mathsf{ORegT}(y^*)$: run $(\mathsf{pk}^*, \mathsf{sk}^*) \leftarrow \mathsf{Gen}(\mathsf{crs}, \mathsf{aux})$, $(\mathsf{mpk}, \mathsf{aux}') \leftarrow \mathsf{Reg}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*, y^*)$, update $\mathsf{aux} = \mathsf{aux}'$, compute $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*)$, append $(\mathsf{mpk}, y^*, \mathsf{aux})$ to $\mathcal{R}$, return $(t = |\mathcal{R}|, \mathsf{mpk}, \mathsf{aux}, \mathsf{pk}^*, \mathsf{sk}^*, \mathsf{hsk}^*)$;
- $\mathsf{OEnc}(i, x, M)$: let $\mathcal{R}[i] = (\mathsf{mpk}, *, *)$, run $\mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, M)$, append (x, M, ct_x) to $\mathcal{E}$ and return $(|\mathcal{E}|, \mathsf{ct})$;

[11] When considering bounded-user schemes, it is mandatory to input 1^L in unary. This is already discussed and defined in [HLWW23, Def 4.4]. Note that the definition in [ZZGQ23], which also consider bounded-user schemes, does not contain 1^L; we correct it here.

- $\mathsf{ODec}(j)$: let $\mathcal{E}[j] = (x_j, M_j, \mathsf{ct}_{x_j})$, compute $M'_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$, if $M'_j = \mathtt{getupd}$, run $\mathsf{hsk}^* \leftarrow \mathsf{Upd}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}^*)$ and recompute $M'_j \leftarrow \mathsf{Dec}(\mathsf{sk}^*, \mathsf{hsk}^*, \mathsf{ct}_j)$. Set $b = 1$ when $M'_j \neq M_j$;

with the following restrictions:

- there exists one query to ORegT (we can consider $y^*, \mathsf{pk}^*, \mathsf{sk}^*, \mathsf{hsk}^*$ to be global);
- for query $(i, x, *)$ to OEnc, it holds that $i \geq t, \mathcal{R}[i] \neq \bot$ and $\mathsf{P}_\kappa(x, y^*) = 1$;
- for query j to ODec, it holds that $\mathcal{E}[j] \neq \bot$.

Compactness and Efficiency. Let $\mathcal{R}$ be defined as before. Compactness refers to the property that

$$|\mathsf{mpk}_i| = \mathsf{poly}(\lambda, \max_{j\in[i]} |y_j|, \log i), \quad |\mathsf{hsk}^*| = \mathsf{poly}(\lambda, \max_{j\in[|\mathcal{R}|]} |y_j|, \log |\mathcal{R}|)$$

where we let $\mathcal{R}[i] = (\mathsf{mpk}_i, y_i, *)$ for all $i \in [|\mathcal{R}|]$. Furthermore, update efficiency means that the number of invocations of Upd in ODec is at most $O(\log |\mathcal{R}|)$ and each invocation costs $\mathsf{poly}(\log |\mathcal{R}|)$ time (in RAM model).

Security. For all stateful admissible adversaries $\mathcal{A}$, the advantage

$$\Pr\left[\beta = \beta' \; : \; \begin{array}{l} \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, \kappa) \\ x, M_0, M_1 \leftarrow \mathcal{A}^{\mathsf{ORegCK}(\cdot),\mathsf{ORegHK}(\cdot),\mathsf{OCor}(\cdot)}(\mathsf{crs}) \\ \beta \leftarrow \{0,1\};\ \mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, M_\beta);\ \beta' \leftarrow \mathcal{A}(\mathsf{ct}_x) \end{array}\right] - \frac{1}{2}$$

is negligible in λ, where the oracles as follows with initial setting $\mathsf{aux}, \mathsf{mpk} = \bot, \mathcal{R} = \emptyset, \mathcal{C} = \emptyset$ and $\mathcal{D}$ being a dictionary with $\mathcal{D}[\mathsf{pk}] = \emptyset$ for all possible pk:

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

with the following restrictions

- for query i to OCor, it holds that $\mathcal{R}[i] \neq \bot$;
- for all $y \in \bigcup_{\mathsf{pk}\in\mathcal{C}} \mathcal{D}[\mathsf{pk}]$, it holds that $\mathsf{P}(x, y) = 0$.

Conversion from Slotted Registered ABE to Registered ABE. Hohenberger *et al.* shows a generic conversion that converts slotted registered ABE to registered ABE and also shows that the conversion preserves the (un)bounded-user property and compactness [HLWW23]. By inspection of the conversion of [HLWW23], the size expansions of $|\mathsf{mpk}|$ and $|\mathsf{hsk}_i|$ are at most polylogarithmic in the number of registered users. Particularly, the modified definition of compactness for Reg-ABE will also hold if the underlying sReg-ABE has compactness as per Definition 2.4.

Starting from our bounded-user slotted registered ABE in §6.1, we obtain bounded-user registered ABE for the same predicate. As the (modified) compactness are preserved, when instantiating with PESs from §7.1, we obtain bounded-user registered ABE for completely unbounded ciphertext-policy (monotone, non-monotone, generalized non-monotone) span programs.

C Lemmata for Predicate Transformations

C.1 Lemmata for Null-Trans

Lemma C.1. *If PES Γ is ciphertext well-formed (resp. key well-formed), then* $\mathsf{Null\text{-}Trans}(\Gamma)$ *is ciphertext well-formed (resp. key well-formed).*

```
$\mathsf{G} \in \left\{\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}, \boxed{\mathsf{H}_\beta}\right\}$
$\underline{\mathsf{G}}$
$\omega \leftarrow \mathsf{Param}(\kappa),\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{a} \leftarrow \mathbb{Z}_p^{2k+1},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$
$\mathbf{a}^\perp \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{b}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{a}^\perp(\mathbf{A}^\top||\mathbf{a}^\top) = \mathbf{0},\ \mathbf{b}^\perp\mathbf{B} = \mathbf{0}$
$\mathbf{W}' = (\mathbf{W}_0||\mathbf{W}_1||\cdots||\mathbf{W}_\omega) \leftarrow \mathbb{Z}_p^{(2k+1)\times(\omega+1)(k+1)},\ \mathbf{W} = (\mathbf{W}_1||\cdots||\mathbf{W}_\omega)$
$P = ([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{A}\mathbf{W}']_1, [\mathbf{W}'(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(P)$
$\underline{\mathcal{O}(\cdot)}$
Input: $(x, \mathsf{null}) \in \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa$ and valid $\mathsf{aux}_c, \mathsf{aux}_k$, where $\mathsf{aux}_k$ contains $y'$
$(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c),\ (m_1, m_2, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y', \mathsf{aux}_k)$
$(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c),\ (m_3, \mathbf{L}, \mathbf{K}) \leftarrow \mathsf{EncK}(y', n_1, \mathsf{aux}_k)$
$\widehat{\mathbf{K}}'(\mathbf{W}') = \begin{pmatrix} \mathbf{W}_0(\bar{\mathbf{l}} \otimes \mathbf{I}_{k+1}) \\ \mathbf{O} \end{pmatrix}$
$\mathbf{s}_{1,1}, \ldots, \mathbf{s}_{n'_1,m'_1} \leftarrow \mathbb{Z}_p^k,\ \mathbf{t}_{1,1}, \ldots, \mathbf{t}_{m'_1,n'_3}, \mathbf{u}_{\ell,2}, \ldots, \mathbf{u}_{\ell,m'_3} \leftarrow \mathbb{Z}_p^{k+1}$ for $\ell \in [n'_1]$
$\mathbf{u}_{1,1} = \beta\mathbf{b}^\perp,\ \mathbf{u}_{2,1} = \cdots = \mathbf{u}_{n'_1,1} = \mathbf{0} \in \mathbb{Z}_p^{k+1}$
$\overline{\mathbf{S}}_{\mathbf{A}} = (\mathbf{s}_{\nu,\mu}\mathbf{A})_{(\nu,\mu)\in[m'_1]\times[n'_1]},\ \ \overline{\mathbf{T}} = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m'_1]\times[n'_3]},\ \ \overline{\mathbf{U}} = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n'_1]\times[m'_3]}$
$\boxed{\mathbf{c} \leftarrow \mathsf{span}((\begin{smallmatrix}\mathbf{A}\\ \mathbf{a}\end{smallmatrix})), \text{ replace } \mathbf{s}_{1,1}\mathbf{A} \text{ in } \overline{\mathbf{S}}_{\mathbf{A}} \text{ with } \mathbf{c}}$
$\mathbf{R}'_1 = \overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}\widehat{\mathbf{C}}(\mathbf{W}),\ \mathbf{R}'_2 = \overline{\mathbf{U}}(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}}\widehat{\mathbf{K}}'(\mathbf{W}')$
Output: $[\overline{\mathbf{S}}'_{\mathbf{A}},\ \mathbf{R}'_1,\ \mathbf{R}'_2]_1$
```

Fig 2. KE-ind game for Null-Trans(Γ).

Proof. Ciphertext well-formedness is trivial. For any $Y' \subseteq \bar{\mathcal{Y}}_\kappa$, let y' be the first non-null element of Y' and $Y = Y' \backslash \{\mathsf{null}\}$ (if $Y' = \{\mathsf{null}\}$, let y' be the shortest element of $\mathcal{Y}_\kappa$ and $Y = \{y'\}$). Since Γ is key well-formed, there exists $\mathsf{aux}_k, m_1, m_2, m_3, \mathbf{L}$ such that the key well-formedness condition in Definition 3.2 holds with respect to Y. Then, it is not hard to see that Null-Trans(Γ) is key well-formed since $\mathsf{aux}'_k = (\mathsf{aux}_k, y')$ where aux'_k is efficiently computable and $|\mathsf{aux}'_k| \le 2\max(|\mathsf{aux}_k|, |y'|)$, and $m'_1 = m_1, m'_2 = m_2, m'_3 = m_3, \mathbf{L}' = \mathbf{L}$ satisfy the key well-formedness condition in Definition 3.2 with respect to Y'. □

Lemma C.2. *If Γ satisfies* KE-ind *and the MDDH assumption holds in $\mathbb{G}$, then* Null-Trans(Γ) *also satisfies* KE-ind*.*

Proof. We consider two cases, namely, one is that $\mathcal{A}$ queries $\mathcal{O}$ on (x, y) such that $y \in \mathcal{Y}_\kappa$ and the other is that it queries on (x, null) in the KE-ind game for Null-Trans(Γ). Since we have $\mathsf{EncC}' = \mathsf{EncC}, \mathsf{EncK}' = \mathsf{EncK}$ in the former case, KE-ind for Γ immediately implies KE-ind for Null-Trans(Γ). Hence, we consider the latter case. For $\beta \in \{0, 1\}$, we can describe the KE-ind game $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ for Null-Trans(Γ) in the latter case as shown in Fig 2. To prove the lemma, we consider a hybrid H_β, which is also described in Fig 2. H_β is the same as $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ except that the $(1, 1)$-th element $\mathbf{s}_{1,1}\mathbf{A}$ of $\overline{\mathbf{S}}_{\mathbf{A}}$ is replaced with a random element in $\mathsf{span}((\begin{smallmatrix}\mathbf{A}\\ \mathbf{a}\end{smallmatrix}))$. We prove that $\mathsf{G}_0^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_0 \approx_s \mathsf{H}_1 \approx_c \mathsf{G}_1^{\mathsf{KE\text{-}ind}}$.

$\underline{\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_\beta}$**.** Since all elements that $\mathcal{A}$ obtains are affine in $\mathbf{A}, \mathbf{a}, \mathbf{a}^\perp, \mathbf{s}_{1,1}\mathbf{A}, \mathbf{c}$, it suffices to show that the following distributions are indistinguishable:

$$\{[\mathbf{A}]_1, \mathbf{a}, \mathbf{a}^\perp, [\mathbf{c}_0]_1\} \approx_c \{[\mathbf{A}]_1, \mathbf{a}, \mathbf{a}^\perp, [\mathbf{c}_1]_1\}$$

where $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{a}, \mathbf{a}^\perp \leftarrow \mathbb{Z}_p^{2k+1}$ conditioned on $\mathbf{a}^\perp(\mathbf{A}^\top||\mathbf{a}^\top) = \mathbf{0}$ and $\mathbf{c}_0 \leftarrow \mathsf{span}(\mathbf{A}), \mathbf{c}_1 \leftarrow \mathsf{span}((\begin{smallmatrix}\mathbf{A}\\ \mathbf{a}\end{smallmatrix}))$. The above indistinguishability was proven in the proof of Lemma 3.1 (see Eq. (9)).

$\underline{\mathsf{H}_0 \approx_s \mathsf{H}_1}$**.** We redefine $\mathbf{W}_0 = \mathbf{W}'_0 + \tilde{\mathbf{a}}^{\perp\top}\mathbf{b}^\perp$ where $\mathbf{W}'_0 \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)}$ and $\tilde{\mathbf{a}}^\perp \in \mathbb{Z}_p^{2k+1}$ be a vector satisfying $\tilde{\mathbf{a}}^\perp\mathbf{A}^\top = \mathbf{0}, \tilde{\mathbf{a}}^\perp\mathbf{c}^\top = 1$. Such a vector exists with overwhelming probability. It is not hard to see that the distribution of $\mathbf{W}_0$ is not changed by the new definition. Then related terms can be written as follows: $\mathbf{A}\mathbf{W}_0 = \mathbf{A}\mathbf{W}'_0, \mathbf{W}_0\mathbf{B} = \mathbf{W}'_0\mathbf{B}$ in P and

$$
\begin{aligned}
\mathbf{R}'_2 &= \overline{\mathbf{U}}(\mathbf{L}\otimes\mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}}\widehat{\mathbf{K}}'(\mathbf{W}') \\
&= \begin{pmatrix}\mathbf{u}_{1,1}\\ \mathbf{O}\end{pmatrix}(\bar{\mathbf{l}}\otimes\mathbf{I}_{k+1}) + \underbrace{\mathbf{U}_R(\underline{\mathbf{L}}\otimes\mathbf{I}_{k+1})}_{\mathbf{M}} + \begin{pmatrix}\mathbf{c}\mathbf{W}_0\\ \mathbf{s}_{1,2}\mathbf{A}\mathbf{W}_0\\ \vdots\\ \mathbf{s}\mathbf{A}_{1,n_1}\mathbf{W}_0\end{pmatrix}(\bar{\mathbf{l}}\otimes\mathbf{I}_{k+1}) \\
&= \mathbf{M} + \begin{pmatrix}\mathbf{c}\mathbf{W}_0{+}\mathbf{u}_{1,1}\\ \mathbf{s}_{1,2}\mathbf{A}\mathbf{W}_0\\ \vdots\\ \mathbf{s}\mathbf{A}_{1,n_1}\mathbf{W}_0\end{pmatrix}(\bar{\mathbf{l}}\otimes\mathbf{I}_{k+1}) = \mathbf{M} + \begin{pmatrix}\mathbf{c}\mathbf{W}'_0{+}\mathbf{u}_{1,1}{+}\mathbf{b}^{\perp}\\ \mathbf{s}_{1,2}\mathbf{A}\mathbf{W}'_0\\ \vdots\\ \mathbf{s}\mathbf{A}_{1,n_1}\mathbf{W}'_0\end{pmatrix}(\bar{\mathbf{l}}\otimes\mathbf{I}_{k+1})
\end{aligned}
$$

where $\mathbf{U}_R$ consists of the last $(k+1)(m_3-1)$ columns of $\overline{\mathbf{U}}$ in the reply from $\mathcal{O}((x,\mathsf{null}))$. Hence, setting $\mathbf{u}_{1,1}=\mathbf{0}$ and $\mathbf{u}_{1,1}=\mathbf{b}^{\perp}$ in the reply from $\mathcal{O}((x,\mathsf{null}))$ are identically distributed with overwhelming probability. □

C.2 Lemmata for WC-Trans

Lemma C.3. *If PES Γ is ciphertext well-formed (resp. key well-formed), then* $\mathsf{WC\text{-}Trans}(\Gamma)$ *is ciphertext well-formed (resp. key well-formed).*

Proof. Ciphertext well-formedness is trivial. For any $Y'\subseteq\bar{\mathcal{Y}}_\kappa$, let y' be the first non-$*$ element of Y', and $Y = Y'\backslash\{*\}$ (if $Y'=\{*\}$, let y' be the shortest element of $\mathcal{Y}_\kappa$ and $Y=\{y'\}$). Since Γ is key well-formed, there exists $\mathsf{aux}_k, m_1, m_2, m_3, \mathbf{L}$ such that the key well-formedness condition in Definition 3.2 holds with respect to Y. Then, it is not hard to see that $\mathsf{WC\text{-}Trans}(\Gamma)$ is key well-formed since $\mathsf{aux}'_k = (\mathsf{aux}_k, y')$ where aux'_k is efficiently computable and $|\mathsf{aux}'_k|\le 2\max(|\mathsf{aux}_k|,|y'|)$, and $m'_1=m_1, m'_2=m_2, m'_3=m_3, \mathbf{L}'=\mathbf{L}$ satisfy the key well-formedness condition in Definition 3.2 with respect to Y'.

□

Lemma C.4. *If Γ satisfies* KE-ind*, then* $\mathsf{WC\text{-}Trans}(\Gamma)$ *also satisfies* KE-ind*.*

Proof. In the KE-ind game for $\mathsf{WC\text{-}Trans}(\Gamma)$, $\mathcal{A}$ cannot query $\mathcal{O}$ on $(x,*)$ for all $x\in\mathcal{X}_\kappa$ since this immediately breaks the query condition. Thus, $\mathcal{A}$ is allowed to make queries only of the form $(x,y)\in\mathcal{X}_\kappa\times\mathcal{Y}_\kappa$. Since we have $\mathsf{EncC}'=\mathsf{EncC}, \mathsf{EncK}'=\mathsf{EncK}$ in this condition, which immediately implies Lemma C.4. □

C.3 Lemmata for KP1$_{\mathsf{OR}}$-Trans

Lemma C.5. *If PES Γ is ciphertext well-formed (resp. key well-formed), then* $\mathsf{KP1_{OR}\text{-}Trans}(\Gamma)$ *is ciphertext well-formed (resp. key well-formed).*

Proof. Ciphertext well-formedness is trivial. For any $Y'=(\phi_1,\ldots,\phi_L)\subseteq\bar{\mathcal{Y}}_\kappa$, where $\phi_i:[n^{(1)}]\to\mathcal{Y}_\kappa$, let $\delta=\max_{i\in[L]}n^{(i)}$ and $Y=\bigcup_{i\in[L]}\mathsf{Image}(\phi_i)\subseteq\mathcal{Y}_\kappa$. If Γ is key well-formed, there exists $\mathsf{aux}_k, m_1, m_2, m_3, \mathbf{L}$ such that the key well-formedness condition in Definition 3.2 holds with respect to Y. Then, it is not hard to see that $\mathsf{KP1_{OR}\text{-}Trans}(\Gamma)$ is key well-formed since $\mathsf{aux}'_k=(\mathsf{aux}_k,\delta)$, which is efficiently computable, and $m'_1=\delta m_1, m'_2=\delta m_2, m'_3=\delta m_3-\delta+\ 1$, and $\mathbf{L}'=\begin{pmatrix}\bar{\mathbf{l}} & \cdots & \bar{\mathbf{l}}\\ \underline{\mathbf{L}} & & \\ & \ddots & \\ & & \underline{\mathbf{L}}\end{pmatrix}$ satisfy the key well-formedness condition in Definition 3.2 with respect to Y', where

$$
\begin{aligned}
|\mathsf{aux}'_k| &\le 2\max(|\mathsf{aux}_k|,|\delta|) = \mathsf{poly}(\max_i|\phi(i)|)\\
m'_1 &= \delta m_1 = \mathsf{poly}(\max_i|\phi(i)|)\\
m'_2 &= \delta m_2 = \mathsf{poly}(\max_i|\phi(i)|)
\end{aligned}
$$

□

```
$\mathsf{G} \in \left\{\mathsf{G}_\beta^{\text{KE-ind}}, \boxed{\mathsf{H}_\beta^v}\right\}$
$\underline{\mathsf{G}}$
$\omega \leftarrow \mathsf{Param}(\kappa),\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{a} \leftarrow \mathbb{Z}_p^{2k+1},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$
$\mathbf{a}^\perp \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{b}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{a}^\perp(\mathbf{A}^\top||\mathbf{a}^\top) = \mathbf{0},\ \mathbf{b}^\perp\mathbf{B} = \mathbf{0}$
$\mathbf{W} = (\mathbf{W}_1||\cdots||\mathbf{W}_\omega) \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)}$
$P = ([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{AW}]_1, [\mathbf{W}(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(P)$

$\underline{\mathcal{O}(\cdot)}$
Input: $(x,\phi) \in \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa$ and valid $\mathsf{aux}_c, \mathsf{aux}_k$, where $\mathsf{aux}_k$ contains $\delta$
Define $\phi' : [\delta] \to \mathcal{Y}_\kappa$ as $\phi'(i) = \phi(i)$ for $\phi \in [n]$ and $\phi'(i) = \mathsf{null}$ for $\phi \in [n+1, \delta]$
$(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c),\ (m_1, m_2, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}(\phi'(i), \mathsf{aux}_k)$
$(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c),\ (m_3, \mathbf{L}, \mathbf{K}_i) \leftarrow \mathsf{EncK}(\phi'(i), n_1, \mathsf{aux}_k)$
$\widehat{\mathbf{K}}'(\mathbf{W}) = \begin{pmatrix} \widehat{\mathbf{K}}_1(\mathbf{W}) & & \\ & \ddots & \\ & & \widehat{\mathbf{K}}_\delta(\mathbf{W}) \end{pmatrix},\ \mathbf{L}' = \begin{pmatrix} \bar{\mathbf{l}}_1 & \cdots & \bar{\mathbf{l}}_\delta \\ \underline{\mathbf{L}}_1 & & \\ & \ddots & \\ & & \underline{\mathbf{L}}_\delta \end{pmatrix}$
$\mathbf{s}_{1,1}, \ldots, \mathbf{s}_{n_1',m_1'} \leftarrow \mathbb{Z}_p^k,\ \mathbf{t}_{1,1}, \ldots, \mathbf{t}_{m_1',n_3'}, \mathbf{u}_{\ell,2}, \ldots, \mathbf{u}_{\ell,m_3'} \leftarrow \mathbb{Z}_p^{k+1}$ for $\ell \in [n_1']$
$\mathbf{u}_{1,1} = \beta\mathbf{b}^\perp,\ \mathbf{u}_{2,1} = \cdots = \mathbf{u}_{n_1',1} = \mathbf{0} \in \mathbb{Z}_p^{k+1}$
$\overline{\mathbf{S}}_{\mathbf{A}}' = (\mathbf{s}_{\nu,\mu}\mathbf{A})_{(\nu,\mu)\in[m_1']\times[n_1']},\ \ \overline{\mathbf{T}} = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m_1']\times[n_3']},\ \ \overline{\mathbf{U}}' = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n_1']\times[m_3']}$
$\mathbf{R}_1' = \overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'\widehat{\mathbf{C}}(\mathbf{W}),\ \mathbf{R}_2' = \overline{\mathbf{U}}'(\mathbf{L}' \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'^{\mathsf{BT}}\widehat{\mathbf{K}}'(\mathbf{W}) + \boxed{\widetilde{\mathbf{L}}_v}$
Output: $[\overline{\mathbf{S}}_{\mathbf{A}}',\ \mathbf{R}_1',\ \mathbf{R}_2']_1$
```

Fig 3. KE-ind game for $\mathsf{KP1}_{\mathsf{OR}}$-Trans$(\Gamma)$.

Lemma C.6. *If Γ satisfies* KE-ind*, then* $\mathsf{KP1}_{\mathsf{OR}}$-Trans$(\Gamma)$ *also satisfies* KE-ind*.*

Proof. For $\beta \in \{0,1\}$, we can describe the KE-ind game $\mathsf{G}_\beta^{\text{KE-ind}}$ for $\mathsf{KP1}_{\mathsf{OR}}$-Trans$(\Gamma)$ as shown in Fig 3. Let Δ be the upper-bound of δ in aux_k on which $\mathcal{A}$ queries $\mathcal{O}$. To prove the lemma, we consider hybrids H_β^v for $v \in [\Delta]$, which is also described in Fig 3. H_β^v is the same as $\mathsf{G}_\beta^{\text{KE-ind}}$ except that $\widetilde{\mathbf{L}}_v$ is added to $\mathbf{R}_2'$ where $\beta_i \leftarrow \mathbb{Z}_p$ and $i \le v$, $\beta_i = 0$ otherwise, and

$$\widetilde{\mathbf{L}}_v = \begin{pmatrix} (\bar{\mathbf{l}}_1 \otimes \beta_1\mathbf{b}^\perp) & \cdots & (\bar{\mathbf{l}}_n \otimes \beta_n\mathbf{b}^\perp) \\ \mathbf{O} & \cdots & \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p^{n_1' \times m_2'(k+1)}$$

We prove that $\mathsf{G}_0^{\text{KE-ind}} \approx_c \mathsf{H}_0^1 \approx_c \cdots \approx_c \mathsf{H}_0^\Delta \approx_s \mathsf{H}_1^\Delta \approx_c \cdots \approx_c \mathsf{H}_1^1 \approx_c \mathsf{G}_1^{\text{KE-ind}}$.

$\underline{\mathsf{H}_\beta^{v-1} \approx_c \mathsf{H}_\beta^v}$**.** Let $\mathsf{H}_\beta^0 = \mathsf{G}_\beta^{\text{KE-ind}}$, and we prove $\mathsf{H}_\beta^{v-1} \approx_c \mathsf{H}_\beta^v$ for $v \in [\Delta]$ if Γ satisfies KE-ind. Specifically, we construct an adversary $\mathcal{B}$ against the KE-ind game for Γ internally using an adversary $\mathcal{A}$ that distinguishes H_β^{v-1} and H_β^v. For $\phi : [n] \to \mathcal{Y}_\kappa$ on which $\mathcal{A}$ queries $\mathcal{O}$ in the security games, let $\phi' : [\delta] \to \mathcal{Y}_\kappa$ be the function defined in Fig 3. Note that aux_k is valid due to the query condition, and thus $\delta > n$. Furthermore, it can query $\mathcal{O}$ only on (x,ϕ) such that $\mathsf{P}_\kappa(x, \phi'(i)) = 0$ for all $i \in [\delta]$.

1. $\mathcal{B}$ is given an input of KE-ind game $\mathsf{G}_{\beta'}^{\text{KE-ind}}$ for Γ, namely, $([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{AW}]_1, [\mathbf{W}(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$ and gives it to $\mathcal{A}$ as it is except that $\mathbf{b}^\perp$ is replaced with $\tilde{\mathbf{b}}^\perp = z\mathbf{b}^\perp$ where $z \leftarrow \mathbb{Z}_p$.
2. For $\mathcal{A}$'s query to $\mathcal{O}$ on $(x, \phi, \mathsf{aux}_c, \mathsf{aux}_k)$ such that $\phi : [n] \to \mathcal{Y}_\kappa$, $\mathcal{B}$ queries its oracle $\mathcal{O}'$ in KE-ind game on $(x, \phi'(v), \mathsf{aux}_c, \mathsf{aux}_k)$ and receives

$$[\overline{\mathbf{S}}_{\mathbf{A}}, \underbrace{\overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}\widehat{\mathbf{C}}(\mathbf{W})}_{\mathbf{R}_1}, \underbrace{\overline{\mathbf{U}}(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}}\widehat{\mathbf{K}}(\mathbf{W})}_{\mathbf{R}_2}]_1$$

   where it parses $\overline{\mathbf{S}}_{\mathbf{A}} = \mathbf{S}_v(\mathbf{I}_{n_1} \otimes \mathbf{A}),\ \overline{\mathbf{U}} = \begin{pmatrix} \beta'\mathbf{b}^\perp \\ \mathbf{O} \end{pmatrix} ||\mathbf{U}_v \end{pmatrix}$.

3. $\mathcal{B}$ samples $\mathbf{S}_i \leftarrow \mathbb{Z}_p^{m_{i,1} \times n_1 k}$, $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{n_1 \times (m_{i,3}-1)(k+1)}$ for $i \in [\delta] \backslash \{v\}$, and sets

$$\mathbf{U}_0 = \begin{pmatrix} \beta \tilde{\mathbf{b}}^{\perp} \\ \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p^{n_1 \times (k+1)},\ \overline{\mathbf{S}}'_{\mathbf{A}} = \begin{pmatrix} \mathbf{S}_1 \\ \vdots \\ \mathbf{S}_\delta \end{pmatrix} (\mathbf{I}_{n_1} \otimes \mathbf{A})$$
$$\mathbf{R}_{2,i} = \mathbf{U}_i(\underline{\mathbf{L}_i} \otimes \mathbf{I}_{k+1}) + \mathbf{S}_i^{\mathsf{BT}}(\mathbf{I}_{m_{i,1}} \otimes \mathbf{A})\widehat{\mathbf{K}}_i(\mathbf{W})$$
$$\mathbf{R}'_2 = \mathbf{U}_0((\bar{\mathbf{l}}_1 || \cdots || \bar{\mathbf{l}}_\delta) \otimes \mathbf{I}_{k+1}) + (\mathbf{R}_{2,1} || \cdots || \mathbf{R}_{2,v-1} || \mathbf{R}_2 || \mathbf{R}_{2,v+1} || \cdots || \mathbf{R}_{2,\delta})$$

   and returns $[\overline{\mathbf{S}}'_{\mathbf{A}}, \mathbf{R}_1, \mathbf{R}'_2]_1$ to $\mathcal{A}$. Here, $\mathcal{B}$ implicitly define $\overline{\mathbf{U}}' = (\mathbf{U}_0 || \mathbf{U}_1 || \cdots || \mathbf{U}_\delta)$.
4. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

Observe that $\mathcal{A}$'s view corresponds to H_β^{v-1} if $\beta' = 0$, and H_β^{v} otherwise.

$\mathsf{H}_0^{\Delta} = \mathsf{H}_1^{\Delta}$. Let $\mathbf{u}_0, \mathbf{r}'_2$ the first rows of $\mathbf{U}_0, \mathbf{R}'_2$, respectively, where $\mathbf{U}_0$ is the first $k+1$ columns of $\overline{\mathbf{U}}'$. Then, $\mathbf{r}'_2$ in H_0^{Δ} can be written as

$$\begin{aligned} \mathbf{r}'_2 &= \mathbf{u}_0((\bar{\mathbf{l}}_1 || \cdots || \bar{\mathbf{l}}_\delta) \otimes \mathbf{I}_{k+1}) + (\bar{\mathbf{l}}_1 \otimes \beta_1 \mathbf{b}^{\perp} || \cdots || \bar{\mathbf{l}}_\delta \otimes \beta_\delta \mathbf{b}^{\perp}) + \mathbf{m} \\ &= (\bar{\mathbf{l}}_1 \otimes (\mathbf{u}_0 + \beta_1 \mathbf{b}^{\perp}) || \cdots || \bar{\mathbf{l}}_\delta \otimes (\mathbf{u}_0 + \beta_\delta \mathbf{b}^{\perp})) + \mathbf{m} \\ &= (\bar{\mathbf{l}}_1 \otimes (\mathbf{u}_0 + \mathbf{b}^{\perp} + (\beta_1 - 1)\mathbf{b}^{\perp}) || \cdots || \bar{\mathbf{l}}_\delta \otimes (\mathbf{u}_0 + \mathbf{b}^{\perp} + (\beta_\delta - 1)\mathbf{b}^{\perp})) + \mathbf{m} \end{aligned}$$

where $\mathbf{u}_0 = \mathbf{0}$, $\mathbf{m}$ is a vector independent of $\mathbf{u}_0$, and the second equality follows from $\mathbf{u}_0(\bar{\mathbf{l}}_i \otimes \mathbf{I}_{k+1}) = \bar{\mathbf{l}}_i \otimes \mathbf{u}_0$. Recall that β_i for $i \in [\delta]$ is randomly distributed, and so is $\beta_i - 1$. Hence, $\mathbf{r}'_2$ with $\mathbf{u}_0 = \mathbf{0}$ and that with $\mathbf{u}_0 = \mathbf{b}^{\perp}$ are identically distributed where the former and the latter distributions correspond to H_0^{Δ} and H_1^{Δ}, respectively. □

C.4 Lemmata for $\mathsf{KP1}_{\mathsf{AND}}$-Trans

Lemma C.7. *If PES Γ is ciphertext well-formed (resp. key well-formed), then* $\mathsf{KP1}_{\mathsf{AND}}\text{-}\mathsf{Trans}(\Gamma)$ *is ciphertext well-formed (resp. key well-formed).*

Proof. Ciphertext well-formedness is trivial. For any $Y' = (\phi_1, \ldots, \phi_L) \subseteq \bar{\mathcal{Y}}_\kappa$, where $\phi_i : [n^{(i)}] \to \mathcal{Y}_\kappa$, let $\delta = \max_{i \in [L]} n^{(i)}$ and $Y = \bigcup_{i \in [L]} \mathsf{Image}(\phi_i) \subseteq \mathcal{Y}_\kappa$. If Γ is key well-formed, there exists $\mathsf{aux}_k, m_1, m_2, m_3, \mathbf{L}$ such that the key well-formedness condition in Definition 3.2 holds with respect to Y. Then, it is not hard to see that $\mathsf{KP1}_{\mathsf{AND}}\text{-}\mathsf{Trans}(\Gamma)$ is key well-formed since $\mathsf{aux}'_k = (\mathsf{aux}_k, \delta)$, which is efficiently computable, and $m'_1 = \delta m_1, m'_2 = \delta m_2, m'_3 = \delta m_3$, and $\mathbf{L}' = \begin{pmatrix} \mathbf{m}_1^{\top} \bar{\mathbf{l}} & \cdots & \mathbf{m}_\delta^{\top} \bar{\mathbf{l}} \\ \underline{\mathbf{L}} & & \\ & \ddots & \\ & & \underline{\mathbf{L}} \end{pmatrix}$ satisfy the key well-formedness condition in Definition 3.2 with respect to Y', where

$$\begin{aligned} |\mathsf{aux}'_k| &\leq 2\max(|\mathsf{aux}_k|, |\delta|) = \mathsf{poly}(\max_i |\phi(i)|) \\ m'_1 &= \delta m_1 = \mathsf{poly}(\max_i |\phi(i)|) \\ m'_2 &= \delta m_2 = \mathsf{poly}(\max_i |\phi(i)|) \end{aligned}$$

□

Lemma C.8. *If Γ satisfies* $\mathsf{KE\text{-}ind}$*, then* $\mathsf{KP1}_{\mathsf{AND}}\text{-}\mathsf{Trans}(\Gamma)$ *also satisfies* $\mathsf{KE\text{-}ind}$.

Proof. For $\beta \in \{0,1\}$, we can describe the $\mathsf{KE\text{-}ind}$ game $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ for $\mathsf{KP1}_{\mathsf{AND}}\text{-}\mathsf{Trans}(\Gamma)$ as shown in Fig 4. To prove the lemma, we consider a hybrid H_β, which is also described in Fig 4. Due to the query condition, for (x, ϕ) on which $\mathcal{A}$ queries $\mathcal{O}$, there exists at least one index j such that $\mathsf{P}_\kappa(x, y_j) = 0$.

```
$\mathsf{G} \in \left\{\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}, \boxed{\mathsf{H}_\beta}\right\}$
$\underline{\mathsf{G}}$
$\omega \leftarrow \mathsf{Param}(\kappa),\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{a} \leftarrow \mathbb{Z}_p^{2k+1},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$
$\mathbf{a}^\perp \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{b}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{a}^\perp(\mathbf{A}^\top||\mathbf{a}^\top) = \mathbf{0},\ \mathbf{b}^\perp\mathbf{B} = \mathbf{0}$
$\mathbf{W} = (\mathbf{W}_1||\cdots||\mathbf{W}_\omega) \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)}$
$P = ([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{AW}]_1, [\mathbf{W}(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(P)$

$\underline{\mathcal{O}(\cdot)}$
Input: $(x, \phi) \in \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa$ and valid $\mathsf{aux}_c, \mathsf{aux}_k$, where $\mathsf{aux}_k$ contains $\delta$
Define $\phi' : [\delta] \to \mathcal{Y}_\kappa$ as $\phi'(i) = \phi(i)$ for $\phi \in [n]$ and $\phi'(i) = *$ for $\phi \in [n+1, \delta]$
$(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c),\ (m_1, m_2, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}(\phi'(i), \mathsf{aux}_k)$
$(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c),\ (m_3, \mathbf{L}, \mathbf{K}_i) \leftarrow \mathsf{EncK}(\phi'(i), n_1, \mathsf{aux}_k)$
$\widehat{\mathbf{K}}'(\mathbf{W}) = \begin{pmatrix} \widehat{\mathbf{K}}_1(\mathbf{W}) & & \\ & \ddots & \\ & & \widehat{\mathbf{K}}_\delta(\mathbf{W}) \end{pmatrix},\ \mathbf{L}' = \begin{pmatrix} \mathbf{m}_1^\top\bar{\mathbf{l}}_1 & \cdots & \mathbf{m}_\delta^\top\bar{\mathbf{l}}_\delta \\ \underline{\mathbf{L}}_1 & & \\ & \ddots & \\ & & \underline{\mathbf{L}}_\delta \end{pmatrix}$
$\mathbf{s}_{1,1}, \ldots, \mathbf{s}_{n'_1,m'_1} \leftarrow \mathbb{Z}_p^k,\ \mathbf{t}_{1,1}, \ldots, \mathbf{t}_{m'_1,n'_3}, \mathbf{u}_{\ell,2}, \ldots, \mathbf{u}_{\ell,m'_3} \leftarrow \mathbb{Z}_p^{k+1}$ for $\ell \in [n'_1]$
$\mathbf{u}_{1,1} = \beta\mathbf{b}^\perp,\ \mathbf{u}_{2,1} = \cdots = \mathbf{u}_{n'_1,1} = \mathbf{0} \in \mathbb{Z}_p^{k+1}$
$\overline{\mathbf{S}}'_\mathbf{A} = (\mathbf{s}_{\nu,\mu}\mathbf{A})_{(\nu,\mu)\in[m'_1]\times[n'_1]},\ \ \overline{\mathbf{T}} = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m'_1]\times[n'_3]},\ \ \overline{\mathbf{U}}' = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n'_1]\times[m'_3]}$
$\mathbf{R}'_1 = \overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}'_\mathbf{A}\widehat{\mathbf{C}}(\mathbf{W}),\ \mathbf{R}'_2 = \overline{\mathbf{U}}'(\mathbf{L}' \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}'^{\mathsf{BT}}_\mathbf{A}\widehat{\mathbf{K}}'(\mathbf{W}) + \boxed{\widetilde{\mathbf{L}}}$
Output: $[\overline{\mathbf{S}}'_\mathbf{A},\ \mathbf{R}'_1,\ \mathbf{R}'_2]_1$
```

Fig 4. KE-ind game for $\mathsf{KP1}_{\mathsf{AND}}$-$\mathsf{Trans}(\Gamma)$.

For (x, ϕ), let $j \in [n]$ be the first index such that $\mathsf{P}_\kappa(x, y_j) = 0$. H_β is the same as $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ except that $\widetilde{\mathbf{L}}$ is added to $\mathbf{R}'_2$ where $\beta_i \leftarrow \mathbb{Z}_p$ if $i = j$, $\beta_i = 0$ otherwise, and

$$\widetilde{\mathbf{L}} = \begin{pmatrix} (\bar{\mathbf{l}}_1 \otimes \beta_1\mathbf{b}^\perp) & \cdots & (\bar{\mathbf{l}}_n \otimes \beta_n\mathbf{b}^\perp) \\ \mathbf{O} & \cdots & \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p^{n'_1\times m'_2(k+1)}$$

We prove that $\mathsf{G}_0^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_0 \approx_c \mathsf{H}_1 \approx_c \mathsf{G}_1^{\mathsf{KE\text{-}ind}}$.

$\underline{\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_\beta}$**.** We prove $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_\beta$ if Γ satisfies KE-ind. Specifically, we construct an adversary $\mathcal{B}$ against the KE-ind game for Γ internally using an adversary $\mathcal{A}$ that distinguishes $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ and H_β. For $\phi : [n] \to \mathcal{Y}_\kappa$ on which $\mathcal{A}$ queries $\mathcal{O}$ in the security games, let $\phi' : [\delta] \to \mathcal{Y}_\kappa$ be the function defined in Fig 4. Note that aux_k is valid due to the query condition, and thus $\delta > n$.

1. $\mathcal{B}$ is given an input of KE-ind game $\mathsf{G}_{\beta'}^{\mathsf{KE\text{-}ind}}$ for Γ, namely, $([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{AW}]_1, [\mathbf{W}(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$ and gives it to $\mathcal{A}$ as it is except that $\mathbf{b}^\perp$ is replaced with $\tilde{\mathbf{b}}^\perp = z\mathbf{b}^\perp$ where $z \leftarrow \mathbb{Z}_p$.
2. For $\mathcal{A}$'s query to $\mathcal{O}$ on $(x, \phi, \mathsf{aux}_c, \mathsf{aux}_k)$ such that $\phi : [n] \to \mathcal{Y}_\kappa$, $\mathcal{B}$ queries its oracle $\mathcal{O}'$ in KE-ind game on $(x, \phi'(j), \mathsf{aux}_c, \mathsf{aux}_k)$ and receives

$$[\overline{\mathbf{S}}_\mathbf{A}, \underbrace{\overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_\mathbf{A}\widehat{\mathbf{C}}(\mathbf{W})}_{\mathbf{R}_1}, \underbrace{\overline{\mathbf{U}}(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_\mathbf{A}^{\mathsf{BT}}\widehat{\mathbf{K}}(\mathbf{W})}_{\mathbf{R}_2}]_1$$

   where it parses $\overline{\mathbf{S}}_\mathbf{A} = \mathbf{S}_j(\mathbf{I}_{n_1} \otimes \mathbf{A}),\ \overline{\mathbf{U}} = \begin{pmatrix} \beta'\mathbf{b}^\perp & ||\mathbf{U}_j \\ \mathbf{O} & \end{pmatrix}$.
3. $\mathcal{B}$ samples $\mathbf{S}_i \leftarrow \mathbb{Z}_p^{m_{i,1}\times n_1k}$, $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{n_1\times(m_{i,3}-1)(k+1)}$ for $i \in [\delta]\backslash\{j\}$, $\widetilde{\mathbf{U}}_0 \leftarrow \mathbb{Z}_p^{n_1\times(m-1)(k+1)}$, and sets $\mathbf{U}_0 = \begin{pmatrix} \beta\tilde{\mathbf{b}}^\perp & ||\widetilde{\mathbf{U}}_0 \\ \mathbf{O} & \end{pmatrix}$, $\overline{\mathbf{S}}'_\mathbf{A} = \begin{pmatrix} \mathbf{S}_1 \\ \vdots \\ \mathbf{S}_\delta \end{pmatrix}(\mathbf{I}_{n_1} \otimes \mathbf{A})$,

$$\mathbf{R}_{2,i} = \mathbf{U}_i(\underline{\mathbf{L}_i} \otimes \mathbf{I}_{k+1}) + \mathbf{S}_i^{\mathsf{BT}}(\mathbf{I}_{m_{i,1}} \otimes \mathbf{A})\widehat{\mathbf{K}}_i(\mathbf{W})$$
$$\mathbf{R}'_2 = \mathbf{U}_0((\mathbf{m}_1^\top\bar{\mathbf{l}}_1||\cdots||\mathbf{m}_\delta^\top\bar{\mathbf{l}}_\delta) \otimes \mathbf{I}_{k+1}) + (\mathbf{R}_{2,1}||\cdots||\mathbf{R}_{2,j-1}||\mathbf{R}_2||\mathbf{R}_{2,j+1}||\cdots||\mathbf{R}_{2,\delta})$$

and returns $[\overline{\mathbf{S}}'_{\mathbf{A}}, \mathbf{R}_1, \mathbf{R}'_2]_1$ to $\mathcal{A}$. Here, $\mathcal{B}$ implicitly define $\overline{\mathbf{U}}' = (\mathbf{U}_0||\mathbf{U}_1||\cdots||\mathbf{U}_\delta)$.

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

Observe that $\mathcal{A}$'s view corresponds to H_β^{v-1} if $\beta' = 0$, and H_β^{v} otherwise.

$\underline{\mathsf{H}_0 = \mathsf{H}_1}$**.** Let $\mathbf{u}_0, \mathbf{r}'_2$ the first rows of $\mathbf{U}_0, \mathbf{R}'_2$, respectively, where $\mathbf{U}_0$ is the first $m(k+1)$ columns of $\overline{\mathbf{U}}'$. Then, $\mathbf{r}'_2$ in H_0 can be written as

$$\begin{aligned}\mathbf{r}'_2 &= \mathbf{u}_0((\mathbf{m}_1^\top \bar{\mathbf{l}}_1||\cdots||\mathbf{m}_\delta^\top \bar{\mathbf{l}}_\delta) \otimes \mathbf{I}_{k+1}) + (\bar{\mathbf{l}}_1 \otimes \beta_1 \mathbf{b}^\perp||\cdots||\bar{\mathbf{l}}_\delta \otimes \beta_\delta \mathbf{b}^\perp) + \mathbf{m} \\ &= (\bar{\mathbf{l}}_1 \otimes (\mathbf{u}_0(\mathbf{m}_1^\top \otimes \mathbf{I}_{k+1}) + \beta_1 \mathbf{b}^\perp)||\cdots||\bar{\mathbf{l}}_\delta \otimes (\mathbf{u}_0(\mathbf{m}_\delta^\top \otimes \mathbf{I}_{k+1}) + \beta_\delta \mathbf{b}^\perp)) + \mathbf{m} \qquad (10)\end{aligned}$$

where $\mathbf{u}_0 = (\mathbf{0}, \mathbf{u}_{1,2}, \ldots, \mathbf{u}_{1,m})$, $\mathbf{m}$ is a vector independent of $\mathbf{u}_0$, and the second equality follows from

$$\begin{aligned}\mathbf{u}_0(\mathbf{m}_i^\top \bar{\mathbf{l}}_i \otimes \mathbf{I}_{k+1}) =& \mathbf{u}_0(\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1})(\bar{\mathbf{l}}_i \otimes \mathbf{I}_{k+1}) = \mathbf{u}_0(\bar{\mathbf{l}}_i \otimes (\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1})) \\ =& \bar{\mathbf{l}}_i \otimes (\mathbf{u}_0(\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1}))\end{aligned}$$

Let $\mathbf{z}_j \in \mathbb{Z}_p^\delta$ be $\mathbf{z}_j = \mathbf{e}_1$ if $j = 1$, and $\mathbf{z}_j = \mathbf{e}_1 - \mathbf{e}_j$ if $j \in [2, \delta]$ where $\mathbf{e}_i$ is the one-hot vector with the i-th element being 1. Then, it is easy to see that $\mathbf{z}_j \mathbf{m}_i^\top = 0$ for $i, j \in [\delta], i \neq j$. Hence, the following distributions are identical:

$$(\beta_1, \ldots, \beta_\delta) \otimes \mathbf{b}^\perp \quad \text{and} \quad (\beta_1 + \mathbf{z}_j \mathbf{m}_1^\top, \ldots, \beta_\delta + \mathbf{z}_j \mathbf{m}_\delta^\top) \otimes \mathbf{b}^\perp \qquad (11)$$

This is because β_i is a random element in $\mathbb{Z}_p$ if $i = j$ and $\beta_i = 0$ otherwise. We also have

$$(\mathbf{z}\mathbf{m}_1^\top, \ldots, \mathbf{z}\mathbf{m}_\delta^\top) \otimes \mathbf{b}^\perp = ((\mathbf{z} \otimes \mathbf{b}^\perp)(\mathbf{m}_1^\top \otimes \mathbf{I}_{k+1})||\cdots||(\mathbf{z} \otimes \mathbf{b}^\perp)(\mathbf{m}_\delta^\top \otimes \mathbf{I}_{k+1})) \qquad (12)$$

From Eq. (10) to (12), the distribution of $\mathbf{r}'_2$ is not changed if we replace $\mathbf{u}_0$ in Eq. (10) with $\mathbf{u}_0 + \mathbf{z}_j \otimes \mathbf{b}^\perp = (\mathbf{b}^\perp, \mathbf{u}'_{1,2}, \ldots, \mathbf{u}'_{1,m})$ where $\mathbf{u}'_{1,i} = \mathbf{u}_{1,i} + z_{j,i}\mathbf{b}^\perp$, $z_{j,i}$ is the i-th element of $\mathbf{z}_j$. Since $\mathbf{u}'_{1,i}$ is also randomly distributed, this corresponds to the view in H_1. Hence, H_0 and H_1 are identically distributed. □

C.5 Lemmata for $\mathsf{SPC}_{\mathbf{M}}$-Trans

Lemma C.9. *If PES* $\mathbf{\Gamma}$ *are ciphertext well-formed (resp. key well-formed), then* $\mathsf{SPC}_{\mathbf{M}}\text{-}\mathsf{Trans}(\mathbf{\Gamma})$ *is ciphertext well-formed (resp. key well-formed).*

Proof. If $\mathbf{\Gamma}$ are ciphertext well-formed, for any $X' = (\mathbf{x}_1, \ldots, \mathbf{x}_L) \subseteq \bar{\mathcal{X}}_\kappa$, where $\mathbf{x}_i = (x_{i,1}, \ldots, x_{i,n}) \in \bar{\mathcal{X}}_\kappa$, there exists $\mathsf{aux}_{c,i}, n_{i,1}, n_{i,2}, n_{i,3}, \mathbf{F}_i$ such that the ciphertext well-formedness condition in Definition 3.3 holds with respect to $(x_{1,i}, \ldots, x_{L,i})$ for all $i \in [n]$. Then, it is not hard to see that $\mathsf{SPC}_{\mathbf{M}}\text{-}\mathsf{Trans}(\mathbf{\Gamma})$ is ciphertext well-formed since $\mathsf{aux}'_c = (\mathsf{aux}_{c,1}, \ldots, \mathsf{aux}_{c,n})$, which is efficiently computable, and $n'_1 = \max_{i\in[n]} n_{i,1}, n'_2 = \sum n_{i,2}, n'_3 = \sum n_{i,3}, \mathbf{F}' = \begin{pmatrix} \mathbf{F}_1 & & \\ & \ddots & \\ & & \mathbf{F}_n \end{pmatrix}$ satisfy the ciphertext well-formedness condition in Definition 3.3 with respect to X', where

$$\begin{aligned}|\mathsf{aux}'_c| &\leq n \max(|\mathsf{aux}_{c,1}|, \ldots, |\mathsf{aux}_{c,n}|) = \mathsf{poly}(\max_{j\in[L]} |\mathbf{x}_j|) \\ n'_1 &= \max_{i\in[n]} n_{i,1} = \mathsf{poly}(\max_{j\in[L]} |\mathbf{x}_j|) \\ n'_2 &\leq n \max_{i\in[n]} n_{i,2} = \mathsf{poly}(\max_{j\in[L]} |\mathbf{x}_j|)\end{aligned}$$

The key well-formedness of $\mathsf{SPC}_{\mathbf{M}}\text{-}\mathsf{Trans}(\mathbf{\Gamma})$ is similar. □

Lemma C.10. *If* $\mathbf{\Gamma}$ *satisfy* $\mathsf{KE}\text{-}\mathsf{ind}$*, then* $\mathsf{SPC}_{\mathbf{M}}\text{-}\mathsf{Trans}(\mathbf{\Gamma})$ *also satisfies* $\mathsf{KE}\text{-}\mathsf{ind}$*.*

```
$\mathsf{G} \in \left\{\mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}}, \boxed{\mathsf{H}_{\beta}^{v}}\right\}$
$\underline{\mathsf{G}}$
$\mathbf{A} \leftarrow \mathbb{Z}_p^{k \times (2k+1)},\ \mathbf{a} \leftarrow \mathbb{Z}_p^{2k+1},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1) \times k}$
$\mathbf{a}^{\perp} \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{b}^{\perp} \leftarrow \mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{a}^{\perp}(\mathbf{A}^{\top} || \mathbf{a}^{\top}) = \mathbf{0},\ \mathbf{b}^{\perp}\mathbf{B} = \mathbf{0}$
$\omega_i \leftarrow \mathsf{Param}_i(\kappa_i),\ \mathbf{W}_i = (\mathbf{W}_{i,1} || \cdots || \mathbf{W}_{i,\omega_i}) \leftarrow \mathbb{Z}_p^{(2k+1) \times \omega_i(k+1)}$ for $i \in [n]$
$\omega = \sum_i \omega_i,\ \mathbf{W} = (\mathbf{W}_1 || \cdots || \mathbf{W}_n),\ P = ([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^{\perp}, \mathbf{b}^{\perp}, [\mathbf{A}\mathbf{W}]_1, [\mathbf{W}(\mathbf{I}_{\omega} \otimes \mathbf{B})]_2)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(P)$
$\underline{\mathcal{O}(\cdot)}$
Input: $(\mathbf{x}, \mathbf{y}) = ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \in \bar{\mathcal{X}}_{\kappa} \times \bar{\mathcal{Y}}_{\kappa}$ and valid $\mathsf{aux}_c, \mathsf{aux}_k$
$(n_{i,1}, n_{i,2}, \widehat{\mathbf{C}}_i) \leftarrow \mathsf{CVEncC}_i(x_i, \mathsf{aux}_c),\ (m_{i,1}, m_{i,2}, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}_i(y_i, \mathsf{aux}_k)$
$(n_{i,3}, \mathbf{F}_i, \mathbf{C}_i) \leftarrow \mathsf{EncC}_i(x_i, m_{i,1}, \mathsf{aux}_c),\ (m_{i,3}, \mathbf{L}_i, \mathbf{K}_i) \leftarrow \mathsf{EncK}(y_i, n_{i,1}, \mathsf{aux}_k)$
$\widehat{\mathbf{C}}'(\mathbf{W}) = \begin{pmatrix} \widehat{\mathbf{K}}_1(\mathbf{W}_1) & \cdots & \widehat{\mathbf{K}}_n(\mathbf{W}_n) \\ \mathbf{O} & \cdots & \mathbf{O} \end{pmatrix},\ \mathbf{F}' = \begin{pmatrix} \mathbf{F}_1 & & \\ & \ddots & \\ & & \mathbf{F}_n \end{pmatrix}$
$\widehat{\mathbf{K}}'(\mathbf{W}) = \begin{pmatrix} \widehat{\mathbf{K}}_1(\mathbf{w}_1) & \cdots & \widehat{\mathbf{K}}_n(\mathbf{w}_n) \\ \mathbf{O} & \cdots & \mathbf{O} \end{pmatrix},\ \mathbf{L}' = \begin{pmatrix} \mathbf{m}_1^{\top}\bar{\mathbf{l}}_1 & \cdots & \mathbf{m}_n^{\top}\bar{\mathbf{l}}_n \\ \underline{\mathbf{L}}_1 & & \\ & \ddots & \\ & & \underline{\mathbf{L}}_n \end{pmatrix}$
$\mathbf{s}_{1,1}, \ldots, \mathbf{s}_{n'_1, m'_1} \leftarrow \mathbb{Z}_p^k,\ \mathbf{t}_{1,1}, \ldots, \mathbf{t}_{m'_1, n'_3}, \mathbf{u}_{\ell,2}, \ldots, \mathbf{u}_{\ell, m'_3} \leftarrow \mathbb{Z}_p^{k+1}$ for $\ell \in [n'_1]$
$\mathbf{u}_{1,1} = \beta\mathbf{b}^{\perp},\ \mathbf{u}_{2,1} = \cdots = \mathbf{u}_{n'_1,1} = \mathbf{0} \in \mathbb{Z}_p^{k+1}$
$\overline{\mathbf{S}}'_{\mathbf{A}} = (\mathbf{s}_{\nu,\mu}\mathbf{A})_{(\nu,\mu) \in [m'_1] \times [n'_1]},\ \ \overline{\mathbf{T}} = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu) \in [m'_1] \times [n'_3]},\ \ \overline{\mathbf{U}}' = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu) \in [n'_1] \times [m'_3]}$
$\mathbf{R}'_1 = \overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}'_{\mathbf{A}}\widehat{\mathbf{C}}(\mathbf{W}),\ \mathbf{R}'_2 = \overline{\mathbf{U}}'(\mathbf{L}' \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}'^{\mathsf{BT}}_{\mathbf{A}}\widehat{\mathbf{K}}'(\mathbf{W}) + \boxed{\widetilde{\mathbf{L}}_v}$
Output: $[\overline{\mathbf{S}}'_{\mathbf{A}},\ \mathbf{R}'_1,\ \mathbf{R}'_2]_1$
```

Fig 5. KE-ind game for $\mathsf{SPC}_{\mathbf{M}}\text{-}\mathsf{Trans}(\mathit{\Gamma})$.

Proof. For $\beta \in \{0,1\}$, we can describe the KE-ind game $\mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}}$ for $\mathsf{SPC}_{\mathbf{M}}\text{-}\mathsf{Trans}(\mathbf{\Gamma})$ as shown in Fig 5. To prove the lemma, we consider two hybrids H_{β}^{v} for $v \in [n]$, which is also described in Fig 5. H_{β}^{v} is the same as $\mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}}$ except that $\widetilde{\mathbf{L}}_v$ is added to $\mathbf{R}'_2$ where $\beta_i \leftarrow \mathbb{Z}_p$ if $\mathsf{P}_{\kappa_i}^{(i)}(x_i, y_i) = 0$ and $i \leq v$, $\beta_i = 0$ otherwise, and

$$\widetilde{\mathbf{L}}_v = \begin{pmatrix} (\bar{\mathbf{l}}_1 \otimes \beta_1\mathbf{b}^{\perp}) & \cdots & (\bar{\mathbf{l}}_n \otimes \beta_n\mathbf{b}^{\perp}) \\ \mathbf{O} & \cdots & \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p^{n'_1 \times m'_2(k+1)}$$

We prove that $\mathsf{G}_0^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_0^1 \approx_c \cdots \approx_c \mathsf{H}_0^n \approx_s \mathsf{H}_1^n \approx_c \cdots \approx_c \mathsf{H}_1^1 \approx_c \mathsf{G}_1^{\mathsf{KE\text{-}ind}}$.

$\underline{\mathsf{H}_{\beta}^{v-1} \approx_c \mathsf{H}_{\beta}^{v}}$**.** Let $\mathsf{H}_{\beta}^{0} = \mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}}$, and we prove $\mathsf{H}_{\beta}^{v-1} \approx_c \mathsf{H}_{\beta}^{v}$ for $v \in [n]$ if $\mathit{\Gamma}_v$ satisfies KE-ind. Specifically, we construct an adversary $\mathcal{B}$ against the KE-ind game for $\mathit{\Gamma}_v$ internally using an adversary $\mathcal{A}$ that distinguishes H_{β}^{v-1} and H_{β}^{v}. By definition of $\widetilde{\mathbf{L}}_v$, if $\mathcal{A}$ queries $\mathcal{O}$ on $(\mathbf{x}, \mathbf{y}) = ((x_1, \ldots, x_n), (y_1, \ldots, y_n))$ such that $\mathsf{P}_{\kappa_v}^{(v)}(x_v, y_v) = 1$, then $\mathsf{H}_{\beta}^{v-1} = \mathsf{H}_{\beta}^{v}$. Hence, we only consider the case where $\mathcal{A}$ queries $\mathcal{O}$ on $(\mathbf{x}, \mathbf{y})$ such that $\mathsf{P}_{\kappa_v}^{(v)}(x_v, y_v) = 0$.

1. $\mathcal{B}$ is given an input of KE-ind game $\mathsf{G}_{\beta'}^{\mathsf{KE\text{-}ind}}$ for $\mathit{\Gamma}_v$, namely, $([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^{\perp}, \mathbf{b}^{\perp}, [\mathbf{A}\mathbf{W}_v]_1, [\mathbf{W}_v(\mathbf{I}_{\omega} \otimes \mathbf{B})]_2)$. $\mathcal{B}$ samples $\mathbf{W}_i \leftarrow \mathbb{Z}_p^{(2k+1) \times \omega_i(k+1)}$ for $i \in [n] \backslash \{v\}$, $z \leftarrow \mathbb{Z}_p$ and sets $\mathbf{W} = (\mathbf{W}_1 || \cdots || \mathbf{W}_n)$ and $\tilde{\mathbf{b}}^{\perp} = z\mathbf{b}^{\perp}$. $\mathcal{B}$ gives $([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^{\perp}, \tilde{\mathbf{b}}^{\perp}, [\mathbf{A}\mathbf{W}]_1, [\mathbf{W}(\mathbf{I}_{\omega} \otimes \mathbf{B})]_2)$ to $\mathcal{A}$.
2. For $\mathcal{A}$'s query to $\mathcal{O}$ on $(\mathbf{x}, \mathbf{y}, \mathsf{aux}_c, \mathsf{aux}_k)$ such that $\mathbf{M} \in \mathbb{Z}_p^{n \times m}$, $\mathcal{B}$ queries its oracle $\mathcal{O}'$ in KE-ind game on $(x_v, y_v, \mathsf{aux}_c, \mathsf{aux}_k)$ and receives

$$[\overline{\mathbf{S}}_{\mathbf{A}}, \underbrace{\overline{\mathbf{T}}_v(\mathbf{F}_v \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}\widehat{\mathbf{C}}_v(\mathbf{W}_v)}_{\widetilde{\mathbf{R}}_{1,v}}, \underbrace{\overline{\mathbf{U}}_v(\mathbf{L}_v \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}}\widehat{\mathbf{K}}_v(\mathbf{W}_v)}_{\widetilde{\mathbf{R}}_{2,v}}]_1$$

where it parses $\overline{\mathbf{S}}_{\mathbf{A}} = \mathbf{S}(\mathbf{I}_{n_1} \otimes \mathbf{A}), \mathbf{S} = (\mathbf{s}_{\nu,\mu})_{(\nu,\mu) \in [m_{v,1}] \times [n_{v,1}]}, \overline{\mathbf{U}}_v = \begin{pmatrix} \beta'\mathbf{b}^{\perp} & \\ \mathbf{O} & \end{pmatrix} || \mathbf{U}_v \Big)$.

3. $\mathcal{B}$ samples $\mathbf{s}_{\nu,\mu} \leftarrow \mathbb{Z}_p^k$ for $\nu \in [m_{v,1}+1, m'_1] \vee \mu \in [n_{v,1}+1, n'_1]$, $\underline{\mathbf{T}}_v \leftarrow \mathbb{Z}_p^{(m'_1-m_{v,1})\times n_{v,3}(k+1)}$, $\underline{\mathbf{U}}_v \leftarrow \mathbb{Z}_p^{(n'_1-n_{v,1})\times(m_{v,3}-1)(k+1)}$, $\mathbf{T}_i \leftarrow \mathbb{Z}_p^{m'_1\times n_{i,3}(k+1)}$, $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{n'_1\times(m_{i,3}-1)(k+1)}$ for $i \in [n]\backslash\{v\}$, $\widetilde{\mathbf{U}}_0 \leftarrow \mathbb{Z}_p^{n'_1\times(m-1)(k+1)}$, and sets

$$\overline{\mathbf{S}}'_{\mathbf{A}} = (\mathbf{s}_{\nu,\mu})_{(\nu,\mu)\in[m'_1]\times[n'_1]}(\mathbf{I}_{n'_1} \otimes \mathbf{A}),\ \mathbf{S}_{\mathbf{A},1} = (\mathbf{s}_{\nu,\mu})_{(\nu,\mu)\in[m_{v,1}+1,m'_1]\times[n_{v,1}]}(\mathbf{I}_{n_{v,1}} \otimes \mathbf{A})$$
$$\mathbf{S}_{\mathbf{A},2} = (\mathbf{s}_{\nu,\mu})^{\mathsf{BT}}_{(\nu,\mu)\in[m_{v,1}]\times[n_{v,1}+1,n'_1]}(\mathbf{I}_{m_{v,1}} \otimes \mathbf{A}),\ \mathbf{U}_0 = \begin{pmatrix} \beta\tilde{\mathbf{b}}^{\perp} \\ \mathbf{O} \end{pmatrix} || \widetilde{\mathbf{U}}_0 \Bigg)$$
$$\mathbf{R}_1 = \begin{pmatrix} \widetilde{\mathbf{R}}_1 \\ \underline{\mathbf{T}}_v(\mathbf{F}_v \otimes \mathbf{I}_{k+1}) + \mathbf{S}_{\mathbf{A},1}\widehat{\mathbf{C}}_v(\mathbf{W}_v) \end{pmatrix},\ \mathbf{R}_2 = \begin{pmatrix} \widetilde{\mathbf{R}}_2 \\ \underline{\mathbf{U}}_v(\underline{\mathbf{L}}_v \otimes \mathbf{I}_{k+1}) + \mathbf{S}_{\mathbf{A},2}\widehat{\mathbf{K}}_v(\mathbf{W}_v) \end{pmatrix}$$
$$\mathbf{R}_{1,i} = \mathbf{T}_i(\mathbf{F}_i \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}'_{\mathbf{A}} \begin{pmatrix} \widehat{\mathbf{C}}_i(\mathbf{W}_i) \\ \mathbf{O} \end{pmatrix},\ \mathbf{R}_{2,i} = \mathbf{U}_i(\underline{\mathbf{L}}_i \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}'^{\mathsf{BT}}_{\mathbf{A}} \begin{pmatrix} \widehat{\mathbf{K}}_i(\mathbf{W}_i) \\ \mathbf{O} \end{pmatrix}$$
$$\mathbf{R}'_1 = (\mathbf{R}_{1,1}||\cdots||\mathbf{R}_{1,v-1}||\mathbf{R}_1||\mathbf{R}_{1,v+1}||\cdots||\mathbf{R}_{1,n})$$
$$\mathbf{R}'_2 = \mathbf{U}_0((\mathbf{m}_1^\top\bar{\mathbf{l}}_1||\cdots||\mathbf{m}_n^\top\bar{\mathbf{l}}_n) \otimes \mathbf{I}_{k+1}) + (\mathbf{R}_{2,1}||\cdots||\mathbf{R}_{2,v-1}||\mathbf{R}_2||\mathbf{R}_{2,v+1}||\cdots||\mathbf{R}_{2,n})$$

and returns $[\overline{\mathbf{S}}'_{\mathbf{A}}, \mathbf{R}_1, \mathbf{R}'_2]_1$ to $\mathcal{A}$. Here, $\mathcal{B}$ implicitly define $\mathbf{T}_v = \begin{pmatrix} \overline{\mathbf{T}}_v \\ \underline{\mathbf{T}}_v \end{pmatrix}$, $\mathbf{U}_v = \begin{pmatrix} \overline{\mathbf{U}}_v \\ \underline{\mathbf{U}}_v \end{pmatrix}$, $\overline{\mathbf{T}}' = (\mathbf{T}_1||\cdots||\mathbf{T}_n)$, and $\overline{\mathbf{U}}' = (\mathbf{U}_0||\mathbf{U}_1||\cdots||\mathbf{U}_n)$.

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

Observe that $\mathcal{A}$'s view corresponds to H_β^{v-1} if $\beta' = 0$, and H_β^v otherwise.

$\mathsf{H}_0^n = \mathsf{H}_1^n$. Let $\mathbf{u}_0, \mathbf{r}'_2$ the first rows of $\mathbf{U}_0, \mathbf{R}'_2$, respectively, where $\mathbf{U}_0$ is the first m columns of $\overline{\mathbf{U}}'$. Then, $\mathbf{r}'_2$ in H_0^n can be written as

$$\begin{aligned} \mathbf{r}'_2 &= \mathbf{u}_0((\mathbf{m}_1^\top\bar{\mathbf{l}}_1||\cdots||\mathbf{m}_n^\top\bar{\mathbf{l}}_n) \otimes \mathbf{I}_{k+1}) + (\bar{\mathbf{l}}_1 \otimes \beta_1\mathbf{b}^\perp||\cdots||\bar{\mathbf{l}}_n \otimes \beta_n\mathbf{b}^\perp)+\mathbf{m} \\ &= (\bar{\mathbf{l}}_1 \otimes (\mathbf{u}_0(\mathbf{m}_1^\top \otimes \mathbf{I}_{k+1}) + \beta_1\mathbf{b}^\perp)||\cdots||\bar{\mathbf{l}}_n \otimes (\mathbf{u}_0(\mathbf{m}_n^\top \otimes \mathbf{I}_{k+1}) + \beta_n\mathbf{b}^\perp))+\mathbf{m} \end{aligned} \tag{13}$$

where $\mathbf{u}_0 = (\mathbf{0}, \mathbf{u}_{1,2}, \ldots, \mathbf{u}_{1,m})$, $\mathbf{m}$ is a vector independent of $\mathbf{u}_0$, and the second equality follows from

$$\begin{aligned} \mathbf{u}_0(\mathbf{m}_i^\top\bar{\mathbf{l}}_i \otimes \mathbf{I}_{k+1}) =& \mathbf{u}_0(\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1})(\bar{\mathbf{l}}_i \otimes \mathbf{I}_{k+1}) = \mathbf{u}_0(\bar{\mathbf{l}}_i \otimes (\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1})) \\ =& \bar{\mathbf{l}}_i \otimes (\mathbf{u}_0(\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1})) \end{aligned}$$

Let $S \subseteq [n]$ be the set such that $\mathsf{P}_{\kappa_i}^{(i)}(x_i, y_i) = 1 \Leftrightarrow i \in S$. Then, since $(1, \mathbf{0}) \notin \mathsf{span}(\{\mathbf{m}_i\}_{i\in S})$ due to the query condition of the $\mathsf{KE\text{-}ind}$ game, there exists $\mathbf{z}$ such that $\mathbf{z} = (1, z_2, \ldots, z_m)$, and $\mathbf{z}\mathbf{m}_i^\top = 0$ for all $i \in S$. Hence, the following distributions are identical:

$$(\beta_1, \ldots, \beta_n) \otimes \mathbf{b}^\perp \quad \text{and} \quad (\beta_1 + \mathbf{z}\mathbf{m}_1^\top, \ldots, \beta_n + \mathbf{z}\mathbf{m}_n^\top) \otimes \mathbf{b}^\perp \tag{14}$$

This is because β_i is a random element in $\mathbb{Z}_p$ if $i \notin S$ and $\beta_i = 0$ if $i \in S$. We also have

$$(\mathbf{z}\mathbf{m}_1^\top, \ldots, \mathbf{z}\mathbf{m}_n^\top) \otimes \mathbf{b}^\perp = ((\mathbf{z} \otimes \mathbf{b}^\perp)(\mathbf{m}_1^\top \otimes \mathbf{I}_{k+1})||\cdots||(\mathbf{z} \otimes \mathbf{b}^\perp)(\mathbf{m}_n^\top \otimes \mathbf{I}_{k+1})) \tag{15}$$

From Eq. (13) to (15), the distribution of $\mathbf{r}'_2$ is not changed if we replace $\mathbf{u}_0$ in Eq. (13) with $\mathbf{u}_0+\mathbf{z}\otimes\mathbf{b}^\perp = (\mathbf{b}^\perp, \mathbf{u}'_{1,2}, \ldots, \mathbf{u}'_{1,m})$ where $\mathbf{u}'_{1,i} = \mathbf{u}_{1,i} + z_i\mathbf{b}^\perp$. Since $\mathbf{u}'_{1,i}$ is also randomly distributed, this corresponds to the view in H_1^n. Hence, H_0^n and H_1^n are identically distributed. □

C.6 Lemmata for Dual-Trans

Lemma C.11. *If PES Γ is ciphertext well-formed (resp. key well-formed), then* Dual-Trans(Γ) *is key well-formed (resp. ciphertext well-formed).*

```
$\mathsf{G} \in \left\{ \mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}}, \boxed{\mathsf{H}_{\beta}^{1}, \boxed{\mathsf{H}_{\beta}^{2}}} \right\}$
$\underline{\mathsf{G}}$
$\omega \leftarrow \mathsf{Param}(\kappa),\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{a} \leftarrow \mathbb{Z}_p^{2k+1},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$
$\mathbf{a}^{\perp} \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{b}^{\perp} \leftarrow \mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{a}^{\perp}(\mathbf{A}^{\top}||\mathbf{a}^{\top}) = \mathbf{0},\ \mathbf{b}^{\perp}\mathbf{B} = \mathbf{0}$
$\mathbf{W}' = (\mathbf{W}_0||\mathbf{W}_1||\cdots||\mathbf{W}_{\omega}) \leftarrow \mathbb{Z}_p^{(2k+1)\times(\omega+1)(k+1)},\ \mathbf{W} = (\mathbf{W}_1||\cdots||\mathbf{W}_{\omega})$
$P = ([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^{\perp}, \mathbf{b}^{\perp}, [\mathbf{A}\mathbf{W}']_1, [\mathbf{W}'(\mathbf{I}_{\omega} \otimes \mathbf{B})]_2)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(P)$
$\underline{\mathcal{O}(\cdot)}$
Input: $(x, y) \in \bar{\mathcal{X}}_{\kappa} \times \bar{\mathcal{Y}}_{\kappa}$ and valid $\mathsf{aux}_c, \mathsf{aux}_k$
$(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c),\ (m_1, m_2, \widehat{\mathbf{K}}) \leftarrow \mathsf{CVEncK}(y, \mathsf{aux}_k)$
$(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c),\ (m_3, \mathbf{L}, \mathbf{K}) \leftarrow \mathsf{EncK}(y, n_1, \mathsf{aux}_k)$
$\widehat{\mathbf{C}}'(\mathbf{W}') = \begin{pmatrix} \overline{\mathbf{L}}\otimes\mathbf{W}_0 \\ \widehat{\mathbf{K}}(\mathbf{W}) \end{pmatrix},\ \widehat{\mathbf{K}}'(\mathbf{W}') = \left( \begin{smallmatrix} -\mathbf{W}_0 \\ \mathbf{O} \end{smallmatrix} \ ||\ \widehat{\mathbf{C}}(\mathbf{W}) \right),\ \mathbf{F}' = \underline{\mathbf{L}},\ \mathbf{L}' = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\top} & \mathbf{F} \end{pmatrix}$
$\mathbf{s}_{1,1}, \ldots, \mathbf{s}_{n_1',m_1'} \leftarrow \mathbb{Z}_p^{k},\ \mathbf{t}_{1,1}, \ldots, \mathbf{t}_{m_1',n_3'}, \mathbf{u}_{\ell,2}, \ldots, \mathbf{u}_{\ell,m_3'} \leftarrow \mathbb{Z}_p^{k+1}$ for $\ell \in [n_1']$
$\mathbf{u}_{1,1} = \beta\mathbf{b}^{\perp},\ \mathbf{u}_{2,1} = \cdots = \mathbf{u}_{n_1',1} = \mathbf{0} \in \mathbb{Z}_p^{k+1}$
$\overline{\mathbf{S}}_{\mathbf{A}}' = (\mathbf{s}_{\nu,\mu}\mathbf{A})_{(\nu,\mu)\in[m_1']\times[n_1']},\quad \overline{\mathbf{T}}' = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m_1']\times[n_3']},\quad \overline{\mathbf{U}}' = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n_1']\times[m_3']}$
$\mathbf{R}_1' = \overline{\mathbf{T}}'(\mathbf{F}' \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'\widehat{\mathbf{C}}'(\mathbf{W}'),\ \mathbf{R}_2' = \overline{\mathbf{U}}'(\mathbf{L}' \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'^{\mathsf{BT}}\widehat{\mathbf{K}}'(\mathbf{W}')$
$\boxed{\mathbf{R}_1' = \begin{pmatrix} (1-\beta)\mathbf{b}^{\perp} & \\ \mathbf{O} & ||\overline{\mathbf{T}}' \end{pmatrix} (\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'\widehat{\mathbf{C}}'(\mathbf{W}')}$
$\boxed{\mathbf{c} \leftarrow \mathsf{span}(\left( \begin{smallmatrix} \mathbf{A} \\ \mathbf{a} \end{smallmatrix} \right)), \text{ replace } \mathbf{s}_{1,1}\mathbf{A} \text{ in } \overline{\mathbf{S}}_{\mathbf{A}}' \text{ with } \mathbf{c}}$
Output: $[\overline{\mathbf{S}}_{\mathbf{A}}',\ \mathbf{R}_1',\ \mathbf{R}_2']_1$
```

Fig 6. KE-ind game for Dual-Trans(Γ).

Proof. Suppose Γ is ciphertext well-formed, that is, for all $X \subseteq \mathcal{X}_{\kappa} = \bar{\mathcal{Y}}_{\kappa}$, there exists $\mathsf{aux}_c, n_1, n_2, n_3, \mathbf{F}$ such that the ciphertext well-formedness condition in Definition 3.3 holds. Then, it is not hard to see that Dual-Trans(Γ) is key well-formed since $\mathsf{aux}_k' = \mathsf{aux}_c, m_1' = n_1, m_2' = n_2 + 1, m_3' = n_3 + 1, \mathbf{L}' = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\top} & \mathbf{F} \end{pmatrix}$ satisfy the key well-formedness condition in Definition 3.2 with respect to X. The ciphertext well-formedness of Dual-Trans(Γ) is similar. □

Lemma C.12. *If Γ satisfies* KE-ind *and the MDDH assumption holds in $\mathbb{G}$, then* Dual-Trans(Γ) *also satisfies* KE-ind.

Proof. For $\beta \in \{0, 1\}$, we can describe the KE-ind game $\mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}}$ for Dual-Trans(Γ) as shown in Fig 6. To prove the lemma, we consider two hybrids $\mathsf{H}_{\beta}^1, \mathsf{H}_{\beta}^2$, which is also described in Fig 6. H_{β}^1 is the same as $\mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}}$ except that we change the way $[\mathbf{R}_1]_1$ is generated as described in Fig 6. H_{β}^2 is the same as H_{β}^1 except that the $(1, 1)$-th element $\mathbf{s}_{1,1}\mathbf{A}$ of $\overline{\mathbf{S}}_{\mathbf{A}}'$ is replaced with a random element in $\mathsf{span}(\left(\begin{smallmatrix} \mathbf{A} \\ \mathbf{a} \end{smallmatrix} \right))$. We prove that $\mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_{\beta}^1 \approx_c \mathsf{H}_{\beta}^2$ and $\mathsf{H}_0^2 \approx_s \mathsf{H}_1^2$, which immediately implies $\mathsf{G}_0^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{G}_1^{\mathsf{KE\text{-}ind}}$.

$\underline{\mathsf{G}_{\beta}^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_{\beta}^1}$. First, observe that $\mathbf{R}_1' = \overline{\mathbf{T}}'(\mathbf{F}' \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'\widehat{\mathbf{C}}'(\mathbf{W}') = (\mathbf{O}||\overline{\mathbf{T}}')(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'\widehat{\mathbf{C}}'(\mathbf{W}')$, and thus $\mathsf{G}_1^{\mathsf{KE\text{-}ind}} = \mathsf{H}_1^1$. Hence, proving $\mathsf{G}_0^{\mathsf{KE\text{-}ind}} = \mathsf{H}_0^1$ suffices. We show that $\mathsf{G}_0^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_0^1$ if Γ satisfies KE-ind, that is, we construct an adversary $\mathcal{B}$ against the KE-ind game for Γ internally using an adversary $\mathcal{A}$ that distinguishes $\mathsf{G}_0^{\mathsf{KE\text{-}ind}}$ and H_0^1 as follows:

1. $\mathcal{B}$ is given an input of KE-ind game $\mathsf{G}_{\beta'}^{\mathsf{KE\text{-}ind}}$ for Γ, namely, $([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^{\perp}, \mathbf{b}^{\perp}, [\mathbf{A}\mathbf{W}]_1, [\mathbf{W}(\mathbf{I}_{\omega}\otimes\mathbf{B})]_2)$ where $\mathbf{W} = (\mathbf{W}_1||\cdots||\mathbf{W}_{\omega})$.
2. $\mathcal{B}$ samples $\mathbf{W}_0 \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$ and gives $P = ([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^{\perp}, \mathbf{b}^{\perp}, [\mathbf{A}\mathbf{W}']_1, [\mathbf{W}'(\mathbf{I}_{\omega} \otimes \mathbf{B})]_2)$ where $\mathbf{W} = (\mathbf{W}_0||\mathbf{W}_1||\cdots||\mathbf{W}_{\omega})$.

3. For $\mathcal{A}$'s query to $\mathcal{O}$ on $(x, y, \mathsf{aux}_c, \mathsf{aux}_k)$, $\mathcal{B}$ queries its oracle $\mathcal{O}'$ in $\mathsf{KE\text{-}ind}$ game on $(y, x, \mathsf{aux}_k, \mathsf{aux}_c)$ and receives

$$[\overline{\mathbf{S}}_{\mathbf{A}}, \underbrace{\overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}\widehat{\mathbf{C}}(\mathbf{W})}_{\mathbf{R}_1}, \underbrace{\overline{\mathbf{U}}(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}}\widehat{\mathbf{K}}(\mathbf{W})}_{\mathbf{R}_2}]_1$$

   where it parses $\overline{\mathbf{S}}_{\mathbf{A}} = \begin{pmatrix} \mathbf{s}_{1,2}\mathbf{A} & \cdots & \mathbf{s}_{m_1',2}\mathbf{A} \\ \vdots & & \vdots \\ \mathbf{s}_{1,n_1'}\mathbf{A} & \cdots & \mathbf{s}_{m_1',n_1'}\mathbf{A} \end{pmatrix}$ and $\overline{\mathbf{U}} = \left(\begin{matrix} \beta'\mathbf{b}^{\perp} \\ \mathbf{O} \end{matrix} \; || \mathbf{U}_L \right)$.
4. $\mathcal{B}$ samples $\mathbf{s}_{1,1}, \ldots, \mathbf{s}_{m_1',1} \leftarrow \mathbb{Z}_p^k$, sets

$$\mathbf{S}_c = \begin{pmatrix} \mathbf{s}_{1,1}\mathbf{A} \\ \vdots \\ \mathbf{s}_{m_1',1}\mathbf{A} \end{pmatrix}, \; \mathbf{S}_r = \begin{pmatrix} \mathbf{s}_{1,2}\mathbf{A} \\ \vdots \\ \mathbf{s}_{1,n_1'}\mathbf{A} \end{pmatrix}, \; \overline{\mathbf{S}}'_{\mathbf{A}} = (\mathbf{S}_c || \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}})$$

$$\mathbf{R}_1' = \mathbf{R}_2 + \mathbf{S}_c(\overline{\mathbf{L}} \otimes \mathbf{W}_0), \qquad \mathbf{R}_2' = \begin{pmatrix} -\mathbf{s}_{1,1}\mathbf{A}\mathbf{W}_0 + \mathbf{b}^{\perp} & \mathbf{S}_c^{\mathsf{BT}}\widehat{\mathbf{C}}(\mathbf{W}) \\ \mathbf{S}_r\mathbf{A}\mathbf{W}_0 & \mathbf{R}_1 \end{pmatrix}$$

   and returns $[\overline{\mathbf{S}}'_{\mathbf{A}}, \mathbf{R}_1', \mathbf{R}_2']_1$ to $\mathcal{A}$. Note that $[\mathbf{S}_c^{\mathsf{BT}}\widehat{\mathbf{C}}(\mathbf{W})]_1$ can be computed as $(\mathbf{s}_{1,1}|| \cdots ||\mathbf{s}_{m_1',1})\widehat{\mathbf{C}}([\mathbf{A}\mathbf{W}]_1)$.
5. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

In the above reduction, $\mathcal{B}$ implicitly defines $\overline{\mathbf{T}}' = \mathbf{U}_L$ and $\overline{\mathbf{U}}' = \left(\begin{matrix} \mathbf{b}^{\perp} \\ \mathbf{O} \end{matrix} \; ||\overline{\mathbf{T}}\right)$. Then, we can observe that

$$\begin{aligned}
\mathbf{R}_1' &= \overline{\mathbf{U}}(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}}\widehat{\mathbf{K}}(\mathbf{W}) + \mathbf{S}_c(\overline{\mathbf{L}} \otimes \mathbf{W}_0) \\
&= \left(\begin{matrix} \beta'\mathbf{b}^{\perp} \\ \mathbf{O} \end{matrix} \; ||\overline{\mathbf{T}}'\right)(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}'_{\mathbf{A}}\widehat{\mathbf{C}}'(\mathbf{W}') \\
\mathbf{R}_2' &= \begin{pmatrix} \mathbf{b}^{\perp} & \\ & \overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) \end{pmatrix} + \begin{pmatrix} -\mathbf{s}_{1,1}\mathbf{A}\mathbf{W}_0 & \mathbf{S}_c^{\mathsf{BT}}\widehat{\mathbf{C}}(\mathbf{W}) \\ \mathbf{S}_r\mathbf{W}_0 & \overline{\mathbf{S}}_{\mathbf{A}}\widehat{\mathbf{C}}(\mathbf{W}) \end{pmatrix} \\
&= \left(\begin{matrix} \mathbf{b}^{\perp} \\ \mathbf{O} \end{matrix} \; ||\overline{\mathbf{T}}\right)\left(\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\top} & \mathbf{F} \end{pmatrix} \otimes \mathbf{I}_{k+1}\right) + \begin{pmatrix} \mathbf{S}_c^{\mathsf{BT}} \\ \overline{\mathbf{S}}_{\mathbf{A}} \end{pmatrix}\left(\begin{matrix} -\mathbf{W}_0 \\ \mathbf{O} \end{matrix} \; || \; \widehat{\mathbf{C}}(\mathbf{W})\right) \\
&= \overline{\mathbf{U}}'(\mathbf{L}' \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'^{\mathsf{BT}}\widehat{\mathbf{K}}'(\mathbf{W}')
\end{aligned}$$

and the view of $\mathcal{A}$ corresponds to $\mathsf{G}_0^{\mathsf{KE\text{-}ind}}$ if $\beta' = 0$ and H_0^1 if $\beta' = 1$.

$\underline{\mathsf{H}_\beta^1 \approx_c \mathsf{H}_\beta^2}$**.** Since all elements that $\mathcal{A}$ obtains are affine in $\mathbf{A}, \mathbf{a}, \mathbf{a}^{\perp}, \mathbf{s}_{1,1}\mathbf{A}, \mathbf{c}$, it suffices to show that the following distributions are indistinguishable:

$$\{[\mathbf{A}]_1, \mathbf{a}, \mathbf{a}^{\perp}, [\mathbf{c}_0]_1\} \approx_c \{[\mathbf{A}]_1, \mathbf{a}, \mathbf{a}^{\perp}, [\mathbf{c}_1]_1\}$$

where $\mathbf{A} \leftarrow \mathbb{Z}_p^{k \times (2k+1)}, \mathbf{a}, \mathbf{a}^{\perp} \leftarrow \mathbb{Z}_p^{2k+1}$ conditioned on $\mathbf{a}^{\perp}(\mathbf{A}^{\top}||\mathbf{a}^{\top}) = \mathbf{0}$ and $\mathbf{c}_0 \leftarrow \mathsf{span}(\mathbf{A}), \mathbf{c}_1 \leftarrow \mathsf{span}(\left(\begin{smallmatrix} \mathbf{A} \\ \mathbf{a} \end{smallmatrix}\right))$. The above indistinguishability was proven in the proof of Lemma 3.1 (see Eq. (9)).

$\underline{\mathsf{H}_0^2 \approx_s \mathsf{H}_1^2}$**.** In H_0^2, we can write

$$P = ([\mathbf{A}\mathbf{W}_0]_1, [\mathbf{W}_0\mathbf{B}]_2, P')$$

$$\mathbf{R}_1' = \begin{pmatrix} \overline{\mathbf{L}} \otimes (\mathbf{c}\mathbf{W}_0 + \mathbf{b}^{\perp}) + \mathbf{M}_1 \\ \mathbf{M}_2 \end{pmatrix}, \quad \mathbf{R}_2' = \begin{pmatrix} -\mathbf{c}\mathbf{W}_0 & \mathbf{M}_3 \\ \mathbf{S}_r\mathbf{A}\mathbf{W}_0 & \mathbf{M}_4 \end{pmatrix}$$

```
$\mathsf{G} \in \left\{\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}, \boxed{\mathsf{H}_\beta^v}\right\}$
$\underline{\mathsf{G}}$
$\omega \leftarrow \mathsf{Param}(\kappa),\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{a} \leftarrow \mathbb{Z}_p^{2k+1},\ \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$
$\mathbf{a}^\perp \leftarrow \mathbb{Z}_p^{2k+1}, \mathbf{b}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{a}^\perp(\mathbf{A}^\top||\mathbf{a}^\top) = \mathbf{0},\ \mathbf{b}^\perp\mathbf{B} = \mathbf{0}$
$\mathbf{W} = (\mathbf{W}_1||\cdots||\mathbf{W}_\omega) \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)}$
$P = ([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{AW}]_1, [\mathbf{W}(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(P)$
$\underline{\mathcal{O}(\cdot)}$
Input: $(x, (\mathbf{M}, \phi)) \in \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa$ and valid $\mathsf{aux}_c, \mathsf{aux}_k$
$(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c),\ (m_1, m_2, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}(\phi(i), \mathsf{aux}_k)$
$(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c),\ (m_3, \mathbf{L}, \mathbf{K}_i) \leftarrow \mathsf{EncK}(\phi(i), n_1, \mathsf{aux}_k)$
$\widehat{\mathbf{K}}'(\mathbf{W}) = \begin{pmatrix} \widehat{\mathbf{K}}_1(\mathbf{W}) & & \\ & \ddots & \\ & & \widehat{\mathbf{K}}_n(\mathbf{W}) \end{pmatrix},\ \mathbf{L}' = \begin{pmatrix} \mathbf{m}_1^\top\bar{\mathbf{l}}_1 & \cdots & \mathbf{m}_n^\top\bar{\mathbf{l}}_n \\ \underline{\mathbf{L}}_1 & & \\ & \ddots & \\ & & \underline{\mathbf{L}}_n \end{pmatrix}$
$\mathbf{s}_{1,1}, \ldots, \mathbf{s}_{n_1',m_1'} \leftarrow \mathbb{Z}_p^k,\ \mathbf{t}_{1,1}, \ldots, \mathbf{t}_{m_1',n_3'}, \mathbf{u}_{\ell,2}, \ldots, \mathbf{u}_{\ell,m_3'} \leftarrow \mathbb{Z}_p^{k+1}$ for $\ell \in [n_1']$
$\mathbf{u}_{1,1} = \beta\mathbf{b}^\perp,\ \mathbf{u}_{2,1} = \cdots = \mathbf{u}_{n_1',1} = \mathbf{0} \in \mathbb{Z}_p^{k+1}$
$\overline{\mathbf{S}}_{\mathbf{A}}' = (\mathbf{s}_{\nu,\mu}\mathbf{A})_{(\nu,\mu)\in[m_1']\times[n_1']},\ \ \overline{\mathbf{T}} = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m_1']\times[n_3']},\ \ \overline{\mathbf{U}}' = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n_1']\times[m_3']}$
$\mathbf{R}_1' = \overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'\widehat{\mathbf{C}}(\mathbf{W}),\ \mathbf{R}_2' = \overline{\mathbf{U}}'(\mathbf{L}' \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}'^{\mathsf{T}}\widehat{\mathbf{K}}'(\mathbf{W}) + \boxed{\widetilde{\mathbf{L}}_v}$
Output: $[\overline{\mathbf{S}}_{\mathbf{A}}',\ \mathbf{R}_1',\ \mathbf{R}_2']_1$
```

Fig 7. KE-ind game for KP1-Trans(Γ).

where $P', \mathbf{M}_1, \ldots, \mathbf{M}_4$ are independent of $\mathbf{W}_0$. By setting $\mathbf{W}_0 = \mathbf{W}_0' - \tilde{\mathbf{a}}^{\perp\top}\mathbf{b}^\perp$ where $\mathbf{W}_0' \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$ and $\tilde{\mathbf{a}}^\perp \in \mathbb{Z}_p^{2k+1}$ is a vector satisfying $\tilde{\mathbf{a}}^\perp\mathbf{A} = \mathbf{0}$ and $\tilde{\mathbf{a}}^\perp\mathbf{c}^\top = 1$, we have

$$P = ([\mathbf{AW}_0']_1, [\mathbf{W}_0'\mathbf{B}]_2, P')$$
$$\mathbf{R}_1' = \begin{pmatrix} \overline{\mathbf{L}} \otimes \mathbf{cW}_0' + \mathbf{M}_1 \\ \mathbf{M}_2 \end{pmatrix}, \quad \mathbf{R}_2' = \begin{pmatrix} -\mathbf{cW}_0' + \mathbf{b}^\perp & \mathbf{M}_3 \\ \mathbf{S}_r\mathbf{AW}_0' & \mathbf{M}_4 \end{pmatrix}$$

which corresponds to the distribution in H_1^2. It is obvious that both $\mathbf{W}_0, \mathbf{W}_0'$ are random elements in $\mathbb{Z}_p^{(2k+1)\times(k+1)}$. Hence, H_0^2 and H_1^2 are identically distributed as long as $\tilde{\mathbf{a}}^\perp$ exists, and it is the case if $\mathbf{c} \notin \mathsf{span}(\mathbf{A})$ which occurs with overwhelming probability. □

C.7 Lemmata for KP1-Trans

Lemma C.13. *If PES Γ is ciphertext well-formed (resp. key valid), then* KP1-Trans(Γ) *is ciphertext well-formed (resp. key valid).*

This lemma is trivial by the above construction.

Lemma C.14. *If Γ satisfies* KE-ind*, then* KP1-Trans(Γ) *also satisfies* KE-ind.

Proof. For $\beta \in \{0, 1\}$, we can describe the KE-ind game $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ for KP1-Trans(Γ) as shown in Fig 7. Let N be the maximum number of rows of $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$ on which $\mathcal{A}$ queries $\mathcal{O}$ (i.e., N is the upper bound of n). To prove the lemma, we consider hybrids H_β^v for $v \in [N]$, which is also described in Fig 7. H_β^v is the same as $\mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$ except that $\widetilde{\mathbf{L}}_v$ is added to $\mathbf{R}_2'$ where $\beta_i \leftarrow \mathbb{Z}_p$ if $\mathsf{P}_\kappa(x, \phi(i)) = 0$ and $i \le v$, $\beta_i = 0$ otherwise, and

$$\widetilde{\mathbf{L}}_v = \begin{pmatrix} (\bar{\mathbf{l}}_1 \otimes \beta_1\mathbf{b}^\perp) & \cdots & (\bar{\mathbf{l}}_n \otimes \beta_n\mathbf{b}^\perp) \\ \mathbf{O} & \cdots & \mathbf{O} \end{pmatrix} \in \mathbb{Z}_p^{n_1'\times m_2'(k+1)}$$

We prove that $\mathsf{G}_0^{\mathsf{KE\text{-}ind}} \approx_c \mathsf{H}_0^1 \approx_c \cdots \approx_c \mathsf{H}_0^N \approx_s \mathsf{H}_1^N \approx_c \cdots \approx_c \mathsf{H}_1^1 \approx_c \mathsf{G}_1^{\mathsf{KE\text{-}ind}}$.

$\underline{\mathsf{H}_\beta^{v-1} \approx_c \mathsf{H}_\beta^v}$**.** Let $\mathsf{H}_\beta^0 = \mathsf{G}_\beta^{\mathsf{KE\text{-}ind}}$, and we prove $\mathsf{H}_\beta^{v-1} \approx_c \mathsf{H}_\beta^v$ for $v \in [N]$ if $\varGamma$ satisfies $\mathsf{KE\text{-}ind}$. Specifically, we construct an adversary $\mathcal{B}$ against the $\mathsf{KE\text{-}ind}$ game for $\varGamma$ internally using an adversary $\mathcal{A}$ that distinguishes H_β^{v-1} and H_β^v. By definition of $\widetilde{\mathbf{L}}_v$, if $\mathcal{A}$ queries $\mathcal{O}$ on $(x, (\mathbf{M}, \phi))$ such that $\mathsf{P}_\kappa(x, \phi(v)) = 1$, then $\mathsf{H}_\beta^{v-1} = \mathsf{H}_\beta^v$. Hence, we only consider the case where $\mathcal{A}$ queries $\mathcal{O}$ on $(x, (\mathbf{M}, \phi))$ such that $\mathsf{P}_\kappa(x, \phi(v)) = 0$.

1. $\mathcal{B}$ is given an input of $\mathsf{KE\text{-}ind}$ game $\mathsf{G}_{\beta'}^{\mathsf{KE\text{-}ind}}$ for $\varGamma$, namely, $([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{AW}]_1, [\mathbf{W}(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$ and gives it to $\mathcal{A}$ as it is except that $\mathbf{b}^\perp$ is replaced with $\tilde{\mathbf{b}}^\perp = z\mathbf{b}^\perp$ where $z \leftarrow \mathbb{Z}_p$.
2. For $\mathcal{A}$'s query to $\mathcal{O}$ on $(x, (\mathbf{M}, \phi), \mathsf{aux}_c, \mathsf{aux}_k)$ such that $\mathbf{M} \in \mathbb{Z}_p^{n \times m}$, $\mathcal{B}$ queries its oracle $\mathcal{O}'$ in $\mathsf{KE\text{-}ind}$ game on $(x, \phi(v), \mathsf{aux}_c, \mathsf{aux}_k)$ and receives
$$[\overline{\mathbf{S}}_{\mathbf{A}}, \underbrace{\overline{\mathbf{T}}(\mathbf{F} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}} \widehat{\mathbf{C}}(\mathbf{W})}_{\mathbf{R}_1}, \underbrace{\overline{\mathbf{U}}(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}} \widehat{\mathbf{K}}(\mathbf{W})}_{\mathbf{R}_2}]_1$$
where it parses $\overline{\mathbf{S}}_{\mathbf{A}} = \mathbf{S}_v(\mathbf{I}_{n_1} \otimes \mathbf{A})$, $\overline{\mathbf{U}} = \begin{pmatrix} \beta' \mathbf{b}^\perp & \\ \mathbf{O} & \end{pmatrix} ||\mathbf{U}_v \Big)$.
3. $\mathcal{B}$ samples $\mathbf{S}_i \leftarrow \mathbb{Z}_p^{m_{i,1} \times n_1 k}$, $\mathbf{U}_i \leftarrow \mathbb{Z}_p^{n_1 \times (m_{i,3}-1)(k+1)}$ for $i \in [n] \backslash \{v\}$, $\widetilde{\mathbf{U}}_0 \leftarrow \mathbb{Z}_p^{n_1 \times (m-1)(k+1)}$, and sets $\mathbf{U}_0 = \begin{pmatrix} \beta \tilde{\mathbf{b}}^\perp & ||\widetilde{\mathbf{U}}_0 \\ \mathbf{O} & \end{pmatrix}$, $\overline{\mathbf{S}}'_{\mathbf{A}} = \begin{pmatrix} \mathbf{S}_1 \\ \vdots \\ \mathbf{S}_n \end{pmatrix} (\mathbf{I}_{n_1} \otimes \mathbf{A})$,
$$\begin{aligned} \mathbf{R}_{2,i} &= \mathbf{U}_i(\underline{\mathbf{L}_i} \otimes \mathbf{I}_{k+1}) + \mathbf{S}_i^{\mathsf{BT}}(\mathbf{I}_{m_{i,1}} \otimes \mathbf{A})\widehat{\mathbf{K}}_i(\mathbf{W}) \\ \mathbf{R}'_2 &= \mathbf{U}_0((\mathbf{m}_1^\top \bar{\mathbf{l}}_1 || \cdots || \mathbf{m}_n^\top \bar{\mathbf{l}}_n) \otimes \mathbf{I}_{k+1}) + (\mathbf{R}_{2,1} || \cdots || \mathbf{R}_{2,v-1} || \mathbf{R}_2 || \mathbf{R}_{2,v+1} || \cdots || \mathbf{R}_{2,n}) \end{aligned}$$
and returns $[\overline{\mathbf{S}}'_{\mathbf{A}}, \mathbf{R}_1, \mathbf{R}'_2]_1$ to $\mathcal{A}$. Here, $\mathcal{B}$ implicitly define $\overline{\mathbf{U}}' = (\mathbf{U}_0 || \mathbf{U}_1 || \cdots || \mathbf{U}_n)$.
4. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

Observe that $\mathcal{A}$'s view corresponds to H_β^{v-1} if $\beta' = 0$, and H_β^v otherwise.

$\underline{\mathsf{H}_0^N = \mathsf{H}_1^N}$**.** Let $\mathbf{u}_0, \mathbf{r}'_2$ the first rows of $\mathbf{U}_0, \mathbf{R}'_2$, respectively, where $\mathbf{U}_0$ is the first $m(k+1)$ columns of $\overline{\mathbf{U}}'$. Then, $\mathbf{r}'_2$ in H_0^N can be written as
$$\begin{aligned} \mathbf{r}'_2 &= \mathbf{u}_0((\mathbf{m}_1^\top \bar{\mathbf{l}}_1 || \cdots || \mathbf{m}_n^\top \bar{\mathbf{l}}_n) \otimes \mathbf{I}_{k+1}) + (\bar{\mathbf{l}}_1 \otimes \beta_1 \mathbf{b}^\perp || \cdots || \bar{\mathbf{l}}_n \otimes \beta_n \mathbf{b}^\perp) + \mathbf{m} \\ &= (\bar{\mathbf{l}}_1 \otimes (\mathbf{u}_0(\mathbf{m}_1^\top \otimes \mathbf{I}_{k+1}) + \beta_1 \mathbf{b}^\perp) || \cdots || \bar{\mathbf{l}}_n \otimes (\mathbf{u}_0(\mathbf{m}_n^\top \otimes \mathbf{I}_{k+1}) + \beta_n \mathbf{b}^\perp)) + \mathbf{m} \end{aligned} \tag{16}$$
where $\mathbf{u}_0 = (\mathbf{0}, \mathbf{u}_{1,2}, \ldots, \mathbf{u}_{1,m})$, $\mathbf{m}$ is a vector independent of $\mathbf{u}_0$, and the second equality follows from
$$\begin{aligned} \mathbf{u}_0(\mathbf{m}_i^\top \bar{\mathbf{l}}_i \otimes \mathbf{I}_{k+1}) =& \mathbf{u}_0(\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1})(\bar{\mathbf{l}}_i \otimes \mathbf{I}_{k+1}) = \mathbf{u}_0(\bar{\mathbf{l}}_i \otimes (\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1})) \\ =& \bar{\mathbf{l}}_i \otimes (\mathbf{u}_0(\mathbf{m}_i^\top \otimes \mathbf{I}_{k+1})) \end{aligned}$$
Let $S \subseteq [n]$ be the set such that $\mathsf{P}_\kappa(x, y_i) = 1 \Leftrightarrow i \in S$. Then, since $(1, \mathbf{0}) \notin \mathsf{span}(\{\mathbf{m}_i\}_{i \in S})$ due to the query condition of the $\mathsf{KE\text{-}ind}$ game, there exists $\mathbf{z}$ such that $\mathbf{z} = (1, z_2, \ldots, z_m)$, and $\mathbf{z}\mathbf{m}_i^\top = 0$ for all $i \in S$. Hence, the following distributions are identical:
$$(\beta_1, \ldots, \beta_n) \otimes \mathbf{b}^\perp \quad \text{and} \quad (\beta_1 + \mathbf{z}\mathbf{m}_1^\top, \ldots, \beta_n + \mathbf{z}\mathbf{m}_n^\top) \otimes \mathbf{b}^\perp \tag{17}$$
This is because β_i is a random element in $\mathbb{Z}_p$ if $i \notin S$ and $\beta_i = 0$ if $i \in S$. We also have
$$(\mathbf{z}\mathbf{m}_1^\top, \ldots, \mathbf{z}\mathbf{m}_n^\top) \otimes \mathbf{b}^\perp = ((\mathbf{z} \otimes \mathbf{b}^\perp)(\mathbf{m}_1^\top \otimes \mathbf{I}_{k+1}) || \cdots || (\mathbf{z} \otimes \mathbf{b}^\perp)(\mathbf{m}_n^\top \otimes \mathbf{I}_{k+1})) \tag{18}$$
From Eq. (16) to (18), the distribution of $\mathbf{r}'_2$ is not changed if we replace $\mathbf{u}_0$ in Eq. (16) with $\mathbf{u}_0 + \mathbf{z} \otimes \mathbf{b}^\perp = (\mathbf{b}^\perp, \mathbf{u}'_{1,2}, \ldots, \mathbf{u}'_{1,m})$ where $\mathbf{u}'_{1,i} = \mathbf{u}_{1,i} + z_i \mathbf{b}^\perp$. Since $\mathbf{u}'_{1,i}$ is also randomly distributed, this corresponds to the view in H_1^N. Hence, H_0^N and H_1^N are identically distributed. □

D Lemmata for Security Proof of sReg-ABE

Lemma D.1. *If Π satisfies perfect zero-knowledge, then* $\mathsf{H}_0 = \mathsf{H}_1$.

Proof. Lemma D.1 is obvious from perfect zero-knowledge of Π since $\mathbf{M}_i^\ell = \mathbf{A}_i\mathbf{V}_i^\ell$ for all (i, ℓ) in pk_i^ℓ from the ℓ-query to $\mathsf{OGen}(i)$. □

Lemma D.2. $\mathsf{H}_1 \approx_s \mathsf{H}_2$.

Proof. Since $\begin{pmatrix} \mathbf{s}_0\mathbf{A} \\ \mathbf{I}_{2k+1} \end{pmatrix}$ is full-rank, it suffices to prove that $\mathbf{R} \approx_s \widetilde{\mathbf{R}}\mathbf{M}$ where $\mathbf{R} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}$, $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}$, and $\mathbf{M}$ is a full-rank matrix in $\mathbb{Z}_p^{(2k+2)\times(2k+1)}$ independent of $\mathbf{R}, \widetilde{\mathbf{R}}$. As long as $\mathbf{R}$ and $\widetilde{\mathbf{R}}$ are full-rank, which occurs with overwhelming probability, $\mathbf{R}$ and $\widetilde{\mathbf{R}}\mathbf{M}$ are uniformly distributed in a set of full-rank matrices over $\mathbb{Z}_p^{(2k+2)\times(2k+1)}$. Hence, these distributions are statistically close. □

Lemma D.3. *If Π satisfies unbounded simulation soundness,* $\mathsf{H}_2 \approx_c \mathsf{H}_3$.

Proof. If for all challenge public keys $\{\mathsf{pk}_i^*\}_{i\in[L]}$ that $\mathcal{A}$ outputs, there exists $\mathbf{V}_i^* \in \mathbb{Z}_p^{(2k+1)\times(k+1)}$ such that $\begin{pmatrix} \mathbf{T}_i^* \\ \mathbf{Q}_i^* \end{pmatrix} = \mathbf{A}_i\mathbf{V}_i^*$ where $\mathbf{A}_i = \begin{pmatrix} \mathbf{A} \\ \widetilde{\mathbf{R}}_i \begin{pmatrix} \mathbf{s}_0\mathbf{A} \\ \mathbf{I}_{2k+1} \end{pmatrix} \end{pmatrix}$, then we have

$$\mathbf{s}_0\mathbf{T}_i^* = \mathbf{s}_0\mathbf{A}\mathbf{V}_i^* = \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\widetilde{\mathbf{R}}_i \begin{pmatrix} \mathbf{s}_0\mathbf{A} \\ \mathbf{I}_{2k+1} \end{pmatrix} \mathbf{V}_i^* = \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*$$

Thus, as long as the above condition holds, the views of $\mathcal{A}$ in H_2 and H_3 are identical. Furthermore, the condition always holds if pk^* is obtained from $\mathsf{OGen}(i)$. Hence, H_2 and H_3 are identical unless the following Bad event happens: let Bad be the event such that there exist $\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{p}_{i,j}^{*\top}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$ such that for all $\mathbf{V}_i^* \in \mathbb{Z}_p^{(2k+1)\times(k+1)}$, $\mathbf{M}_i^* = \begin{pmatrix} \mathbf{T}_i^* \\ \mathbf{Q}_i^* \end{pmatrix} \neq \mathbf{A}_i\mathbf{V}_i^*$ and $\mathsf{LVerify}(\mathsf{crs}_i, [\mathbf{M}_i^*]_1, \pi_i^*) = 1$. Hence, to prove the lemma it suffices to show $\Pr[\mathsf{Bad}]$ is negligible.

We show that if $\mathcal{A}$ makes Bad happen with non-negligible probability, we can construct $\mathcal{B}$ that breaks strong unbounded simulation soundness of Π as follows.

1. $\mathcal{B}$ randomly chooses $i^* \leftarrow [L]$ as a guess of the slot for which Bad occurs.
2. $\mathcal{B}$ is given an input for the unbounded simulation soundness game $(1^\lambda, \mathsf{crs}_{i^*}, \mathbf{A}_{i^*})$, samples $\mathbf{s}_0 \leftarrow \mathbb{Z}_p^k$, and parses $\mathbf{A}_{i^*} = \begin{pmatrix} \mathbf{A} \\ \mathbf{R}_{i^*} \end{pmatrix} = \begin{pmatrix} \mathbf{A} \\ \widetilde{\mathbf{R}}_{i^*} \begin{pmatrix} \mathbf{s}_0\mathbf{A} \\ \mathbf{I}_{2k+1} \end{pmatrix} \end{pmatrix}$, i.e, randomly samples $\widetilde{\mathbf{R}}_{i^*} \in \mathbb{Z}_p^{(2k+2)\times(2k+2)}$ satisfying the equality.
3. $\mathcal{B}$ samples $\widetilde{\mathbf{R}}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)}$ and sets $\mathbf{R}_i = \widetilde{\mathbf{R}}_i \begin{pmatrix} \mathbf{s}_0\mathbf{A} \\ \mathbf{I}_{2k+1} \end{pmatrix}$ for $i \in [L]\setminus\{i^*\}$, samples all variable other than $\mathbf{A}, \mathsf{crs}_{i^*}, \{\mathbf{R}_i\}_{i\in[L]}$ in the same manner as $\mathsf{Setup}(1^\lambda, 1^L, \kappa)$, and gives crs to $\mathcal{A}$ as follows:
$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}]_1, [\mathbf{A}\mathbf{h}^\top]_\mathsf{T}, \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{A}\mathbf{W}_{i,0}, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\mathbf{B}\mathbf{r}_i^\top, \mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top]_2\}_{i\in[L]}, \{[\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_{i^*}^\top, \mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_j^\top)]_2\}_{\substack{i,j\in[L] \\ i\neq j}} \end{pmatrix}$$
4. When $\mathcal{A}$ queries $\mathsf{OGen}(i)$, $\mathcal{B}$ computes
$$\mathbf{V}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)},\ \mathbf{M}_i = \begin{pmatrix} \mathbf{A}\mathbf{V}_i \\ \mathbf{R}_i\mathbf{V}_i \end{pmatrix},\ \pi_i \leftarrow \mathsf{LSim}(\mathsf{crs}_i, \mathsf{td}_i, [\mathbf{M}_i]_1)$$
$$\mathsf{pk}_i = ([\mathbf{A}\mathbf{V}_i, \mathbf{R}_i\mathbf{V}_i]_1, \{[\mathbf{V}_i\mathbf{B}\mathbf{r}_j^\top]_2\}_{j\in[L]\setminus\{i\}}, \pi_i),\ \ \mathsf{sk}_i = \mathbf{V}_i$$
where $\mathcal{B}$ uses the simulation oracle in the unbounded simulation soundness game of Π when generating π_{i^*}. Then, $\mathcal{B}$ stores a pair $(\mathsf{pk}_i, \mathsf{sk}_i)$ in dictionary $\mathcal{D}_i$ and gives pk_i to $\mathcal{A}$.
5. When $\mathcal{A}$ queries $\mathsf{OCor}(i, \mathsf{pk})$, $\mathcal{B}$ replies sk if and only if $(\mathsf{pk}, \mathsf{sk}) \in \mathcal{D}_i$.
6. When $\mathcal{A}$ outputs a set of challenge public keys $\{\mathsf{pk}_i^*\}_i$ where $\mathsf{pk}_{i^*}^* = ([\mathbf{T}_{i^*}^*, \mathbf{Q}_{i^*}^*]_1, \{[\mathbf{p}_{i^*,j}^{*\top}]_2\}_{j\in[L]\setminus\{i^*\}}, \pi_{i^*}^*)$, $\mathcal{B}$ outputs $\left(\left[\begin{pmatrix} \mathbf{T}_{i^*}^* \\ \mathbf{Q}_{i^*}^* \end{pmatrix}\right]_1, \pi_{i^*}^*\right)$ and halts.

If Bad occurs, then $\begin{pmatrix}\mathbf{T}^*_{i^*}\\ \mathbf{Q}^*_{i^*}\end{pmatrix}$ is not in the space spanned by the columns of $\mathbf{A}_{i^*}$ with probability at least $1/L$ since i^* is uniformly chosen from $[L]$. Hence, $\mathcal{B}$ breaks strong unbounded simulation soundness of Π with $\Pr[\mathsf{Bad}]/L$, which is non-negligible if $\Pr[\mathsf{Bad}]$ is non-negligible. □

Lemma D.4. *If the MDDH assumption holds in $\mathbb{G}$, $\mathsf{H}_3 \approx_c \mathsf{H}_4$.*

Proof. Thanks to the MDDH assumption, we have $([\mathbf{A}]_1, [\mathbf{s}_0\mathbf{A}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{c}]_1)$ where $\mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$, $\mathbf{s}_0 \leftarrow \mathbb{Z}_p^k$, $\mathbf{c} \leftarrow \mathbb{Z}_p^{sk+1}$. Observe that all elements that $\mathcal{A}$ obtains in H_3 and H_4 are affine in $\mathbf{A}, \mathbf{sA}, \mathbf{c}$. Hence, we can easily construct a reduction $\mathcal{B}$ from the MDDH problem to distinguishing H_3 and H_4. □

Lemma D.5. $\mathsf{H}_{5,L} \approx_s \mathsf{H}_6$.

Proof. Recall that the terms that involve $\mathbf{h}$ in $\mathsf{H}_{5,L}$ are $[\mathbf{A}\mathbf{h}^\top]_\mathsf{T}$ and $\{[\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top + \alpha_i {\mathbf{a}^\perp}^\top]_2\}_{i\in[L]}$ in crs and $[\mathbf{c}\mathbf{h}^\top]_\mathsf{T} M_\beta$ in ct_x. Let $\mathbf{h}^\top = \mathbf{h}'^\top + \alpha' {\mathbf{a}^\perp}^\top$ where $\mathbf{h}' \leftarrow \mathbb{Z}_p^{2k+1}, \alpha' \leftarrow \mathbb{Z}_p$. This does not change the distribution of $\mathbf{h}$. Then, the above terms can be written as $[\mathbf{A}\mathbf{h}'^\top]_\mathsf{T}$, $\{[\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}'^\top + (\alpha_i + \alpha')\mathbf{a}^{\perp\top}]_2\}$, $[\mathbf{c}(\mathbf{h}^\top + \alpha' {\mathbf{a}^\perp}^\top)]_\mathsf{T} M_\beta$. Since $\alpha_i + \alpha'$ is randomly distributed in $\mathbb{Z}_p$, $\alpha' \mathbf{c}{\mathbf{a}^\perp}^\top$ is randomly distributed in $\mathbb{Z}_p$ unless $\mathbf{c}{\mathbf{a}^\perp}^\top = 0$, which occurs with negligible probability. The latter distribution corresponds to H_6. Thus, both hybrids are identical with overwhelming probability. □

Lemma D.6. *Let $\mathsf{H}_{5,0} = \mathsf{H}_4$. If Γ satisfies* KE-ind *and the MDDH assumption holds in $\mathbb{G}$, then $\mathsf{H}_{5,v-1} \approx_c \mathsf{H}_{5,v}$ for $v \in [L]$.*

Proof. We define intermediate hybrids $\widehat{\mathsf{H}}^1_{5,v-1}, \widehat{\mathsf{H}}^2_{5,v-1}, \widehat{\mathsf{H}}^{(3)}_{5,v-1}$ between $\mathsf{H}_{5,v-1}$ and $\mathsf{H}_{5,v}$ and show that $\mathsf{H}_{5,v-1} \approx_c \widehat{\mathsf{H}}^1_{5,v-1} \approx_c \widehat{\mathsf{H}}^2_{5,v-1} \approx_c \widehat{\mathsf{H}}^3_{5,v-1} \approx_c \mathsf{H}_{5,v}$. These hybrids are defined as follows.

$\widehat{\mathsf{H}}^1_{5,v-1}$**:** It is the same as $\mathsf{H}_{5,v-1}$ except that $\mathbf{B}\mathbf{r}_v^\top$ is replaced with $\mathbf{d}^\top$ where $\mathbf{d} \leftarrow \mathbb{Z}_p^{k+1}$. Recall that crs in $\mathsf{H}_{5,v-1}$ is described as

$$\begin{pmatrix} [\mathbf{A}]_1, [\mathbf{A}\mathbf{h}^\top]_\mathsf{T}, \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{A}\mathbf{W}_{i,0}, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\underbrace{\mathbf{B}\mathbf{r}_i^\top}_{\mathbf{f}_i^\top}, \underbrace{\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top + \alpha_i {\mathbf{a}^\perp}^\top}_{\mathbf{g}_i^\top}]_2\}_{i\in[L]}, \{[\underbrace{\mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_j^\top}_{\mathbf{n}_{i,j}^\top}, \underbrace{\mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_j^\top)}_{\mathbf{N}_{i,j}}]_2\}_{\substack{i,j\in[L]\\ i\neq j}} \end{pmatrix}$$

where $\alpha_i \leftarrow \mathbb{Z}_p$ if $i \leq v-1$ and otherwise $\alpha_i = 0$, and pk_i^ℓ obtained from the ℓ-th query to $\mathsf{OGen}(i)$ in $\mathsf{H}_{5,v-1}$ is described as

$$\left([\underbrace{\mathbf{A}\mathbf{V}_i^\ell}_{\mathbf{T}_i^\ell}, \underbrace{\mathbf{R}_i\mathbf{V}_i^\ell}_{\mathbf{Q}_i^\ell}]_1, \{[\underbrace{\mathbf{V}_i^\ell\mathbf{B}\mathbf{r}_j^\top}_{\mathbf{p}_{i,j}^{\ell\top}}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^\ell\right)$$

In $\widehat{\mathsf{H}}^1_{5,v-1}$, the following terms are changed as

$$\mathbf{f}_v^\top = \mathbf{d}^\top,\ \ \mathbf{g}_v^\top = \mathbf{W}_{v,0}\mathbf{d}^\top + \mathbf{h}^\top,\ \ \mathbf{n}_{i,v}^\top = \mathbf{W}_{i,0}\mathbf{d}^\top,\ \ \mathbf{N}_{i,v} = \mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{d}^\top)$$
$$\mathbf{p}_{i,v}^{\ell\top} = \mathbf{V}_i^\ell\mathbf{d}^\top$$

$\widehat{\mathsf{H}}^2_{5,v-1}$**:** It is the same as $\widehat{\mathsf{H}}^1_{5,v-1}$ except that $\mathbf{u}_{1,1} = \sum_{i\in[L]}(\mathbf{c}\mathbf{W}_{i,0} + \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*) + \boxed{\mathbf{b}^\perp}$ where $\mathbf{b}^\perp \leftarrow \mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{b}^\perp\mathbf{B} = \mathbf{0}$, instead of $\mathbf{u}_{1,1} = \sum_{i\in[L]}(\mathbf{c}\mathbf{W}_{i,0} + \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*)$.

$\widehat{\mathsf{H}}^3_{5,v-1}$**:** It is the same as $\widehat{\mathsf{H}}^1_{5,v-2}$ except that $\mathbf{g}_v^\top = \mathbf{W}_{v,0}\mathbf{d}^\top + \mathbf{h}^\top + \boxed{\alpha_v {\mathbf{a}^\perp}^\top}$ where $\alpha_v \leftarrow \mathbb{Z}_p$.

Thanks to Lemmata D.7 to D.10, Lemma D.6 holds. □

Lemma D.7. *If the MDDH assumption holds in $\mathbb{G}$, then $\mathsf{H}_{5,v-1} \approx_c \widehat{\mathsf{H}}^1_{5,v-1}$ for $v \in [L]$.*

Proof. This lemma is straightforward from the MDDH assumption, which asserts that $[\mathbf{B}, \mathbf{z}_0]_2 \approx_c [\mathbf{B}, \mathbf{z}_1]_2$ where $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}, \mathbf{r}_v \leftarrow \mathbb{Z}_p^k, \mathbf{z}_0 = \mathbf{B}\mathbf{r}_v^\top, \mathbf{z}_1 = \mathbf{d} \leftarrow \mathbb{Z}_p$. Since all the terms that the adversary is given are affine in $\mathbf{B}$ or $\mathbf{z}_0$ (resp. $\mathbf{z}_1$) in $\mathsf{H}_{5,v-1}$ (resp. $\widehat{\mathsf{H}}^1_{5,v-1}$), they are simulatable given the MDDH instance. □

Lemma D.8. *If the MDDH assumption holds in $\mathbb{G}$, and Γ satisfies $\mathsf{KE\text{-}ind}$, then $\widehat{\mathsf{H}}^1_{5,v-1} \approx_c \widehat{\mathsf{H}}^2_{5,v-1}$ for $v \in [L]$.*

Proof. We consider two cases of the adversary's behavior, namely, the honest case and the dishonest case. The honest cases refer to one in which the adversary outputs the challenge public key pk^*_v for the v-th slot such that $(\mathsf{pk}^*_v, *) \in \mathcal{D}_v$ and $(v, \mathsf{pk}^*_v) \notin \mathcal{C}$. On the other hand, the dishonest case refers to one that is not the honest case, that is, $(\mathsf{pk}^*_v, *) \notin \mathcal{D}_v$ or $(v, \mathsf{pk}^*_v) \in \mathcal{C}$. Thus, it suffices to prove $\widehat{\mathsf{H}}^1_{5,v-1} \approx_c \widehat{\mathsf{H}}^2_{5,v-1}$ under both cases.

Honest Case. We prove that $\widehat{\mathsf{H}}^1_{5,v-1} \approx_c \widehat{\mathsf{H}}^2_{5,v-1}$ in the honest case if the MDDH assumption holds in $\mathbb{G}$. First, we show the following indistinguishability holds under the MDDH assumption, which we will use later in the proof:

$$\begin{aligned}&\{[\mathbf{R}, \mathbf{R}\mathbf{V}]_1, \mathbf{A}, \mathbf{A}\mathbf{V}, \mathbf{b}^\perp, \mathbf{c}, \mathbf{c}\mathbf{V}\}\\ \approx_c&\{[\mathbf{R}, \mathbf{R}\mathbf{V}]_1, \mathbf{A}, \mathbf{A}\mathbf{V}, \mathbf{b}^\perp, \mathbf{c}, \mathbf{c}\mathbf{V} + \mathbf{b}^\perp\}\end{aligned} \tag{19}$$

where $\mathbf{R} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+1)}, \mathbf{V} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}, \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{b}^\perp \leftarrow \mathbb{Z}_p^{k+1}, \mathbf{c} \leftarrow \mathbb{Z}_p^{2k+1}$. We can prove this similarly to [ZZGQ23, Lemma2] as follows:

$$\begin{aligned}&\{[\mathbf{R}, \mathbf{R}\mathbf{V}]_1, \mathbf{A}, \mathbf{A}\mathbf{V}, \mathbf{b}^\perp, \mathbf{c}, \mathbf{c}\mathbf{V}\}\\ \approx_c&\{[\mathbf{S}\widetilde{\mathbf{A}}\mathbf{V}, \mathbf{S}\widetilde{\mathbf{A}}\mathbf{V}]_1, \mathbf{A}, \mathbf{A}\mathbf{V}, \mathbf{b}^\perp, \mathbf{c}, \mathbf{c}\mathbf{V}\}\\ \approx_s&\{[\mathbf{S}\widetilde{\mathbf{A}}\mathbf{V}, \mathbf{S}\widetilde{\mathbf{A}}\mathbf{V}]_1, \mathbf{A}, \mathbf{A}\mathbf{V}, \mathbf{b}^\perp, \mathbf{c}, \mathbf{c}\mathbf{V} + \mathbf{b}^\perp\}\\ \approx_c&\{[\mathbf{R}, \mathbf{R}\mathbf{V}]_1, \mathbf{A}, \mathbf{A}\mathbf{V}, \mathbf{b}^\perp, \mathbf{c}, \mathbf{c}\mathbf{V} + \mathbf{b}^\perp\}\end{aligned}$$

where $\mathbf{S} \leftarrow \mathbb{Z}_p^{(2k+2)\times k}, \widetilde{\mathbf{A}} \leftarrow \mathbb{Z}_p^{k\times(2k+1)}$. The first and third indistinguishability follows from $[\mathbf{R}]_1 \approx_c [\mathbf{S}\widetilde{\mathbf{A}}]_1$, which is exactly what the $(2k+2)$-fold MDDH assumption asserts. The second indistinguishability can be shown by setting $\mathbf{V} = \mathbf{V}' + \tilde{\mathbf{a}}^{\perp^\top}\mathbf{b}^\perp$ where $\mathbf{V}' \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$ and $\tilde{\mathbf{a}}^\perp \in \mathbb{Z}_p^{2k+1}$ is a vector satisfying $\widetilde{\mathbf{A}}\tilde{\mathbf{a}}^{\perp^\top} = \mathbf{0}^\top, \mathbf{A}\tilde{\mathbf{a}}^{\perp^\top} = \mathbf{0}^\top, \mathbf{c}\tilde{\mathbf{a}}^{\perp^\top} = 1$.

We construct a distinguisher $\mathcal{B}$ between the LHS and RHS in Eq. (19) that internally uses a distinguisher $\mathcal{A}$ between $\widehat{\mathsf{H}}^1_{5,v-1}$ and $\widehat{\mathsf{H}}^2_{5,v-1}$ in the honest case as follows. Let Q be the maximum number of $\mathcal{A}$'s queries of the form $\mathsf{OGen}(i)$ for all $i \in [L]$.

1. $\mathcal{B}$ is given an instance $([\mathbf{R}_v, \mathbf{R}_v\mathbf{V}]_1, \mathbf{A}, \mathbf{A}\mathbf{V}, \mathbf{b}^\perp, \mathbf{c}, \mathbf{z}_{\beta'})$ of Eq. (19) where $\mathbf{z}_{\beta'} = \mathbf{c}\mathbf{V} + \beta'\mathbf{b}^\perp$ for $\beta' \in \{0,1\}$. $\mathcal{B}$ computes crs as follows and gives it to $\mathcal{A}$:

$$\mathsf{crs} = \begin{pmatrix}[\mathbf{A}]_1, [\mathbf{A}\mathbf{h}^\top]_{\mathsf{T}}, \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{A}\mathbf{W}_{i,0}, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]}\\ \{[\mathbf{f}_i^\top, \mathbf{g}_i^\top]_2\}_{i\in[L]}, \{[\mathbf{n}_{i,j}^\top, \mathbf{N}_{i,j}]_2\}_{\substack{i,j\in[L]\\ i\neq j}}\end{pmatrix}$$

where

$$\begin{aligned}
&\mathbf{h} \leftarrow \mathbb{Z}_p^{2k+1},\ (\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda),\ \mathbf{W}_{i,0} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)},\ \mathbf{W}_i \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)}\\
&\widetilde{\mathbf{R}}_{i\neq v} \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)},\ \mathbf{R}_{i\neq v} = \widetilde{\mathbf{R}}_i \left({}^{\mathbf{c}}_{\mathbf{I}_{2k+1}} \right),\ \mathbf{r}_{i\neq v} \leftarrow \mathbb{Z}_p^k,\ \mathbf{d} \leftarrow \mathbb{Z}_p^{k+1}\\
&\alpha_{i<v} \leftarrow \mathbb{Z}_p,\ \alpha_{i>v} = 0,\ \mathbf{a}^\perp \leftarrow \mathbb{Z}_p^{2k+1} \text{ conditioned on } \mathbf{a}^\perp\mathbf{A}^\top = \mathbf{0}\\
&\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k} \text{ conditioned on } \mathbf{b}^\perp\mathbf{B} = \mathbf{0}\\
&\mathbf{f}_i^\top = \begin{cases} \mathbf{B}\mathbf{r}_i^\top & (i\neq v)\\ \mathbf{d}^\top & (i = v)\end{cases},\quad \mathbf{g}_i^\top = \begin{cases} \mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top + \alpha_i{\mathbf{a}^\perp}^\top & (i\neq v)\\ \mathbf{W}_{i,0}\mathbf{d}^\top + \mathbf{h}^\top & (i = v)\end{cases}\\
&\mathbf{n}_{i,j}^\top = \begin{cases} \mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_j^\top & (j\neq v)\\ \mathbf{W}_{i,0}\mathbf{d}^\top & (j = v)\end{cases},\quad \mathbf{N}_{i,j} = \begin{cases} \mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_j^\top) & (j\neq v)\\ \mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{d}^\top) & (j = v)\end{cases}
\end{aligned}$$

2. $\mathcal{B}$ randomly samples $q \leftarrow [Q]$ as a guess of the challenge public key for slot v. When $\mathcal{A}$ makes the ℓ-th query $\mathsf{OGen}(i)$, $\mathcal{B}$ gives pk_i^ℓ to $\mathcal{A}$ as follows:

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

where $\mathbf{V}_i^\ell \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$ and

$$\mathbf{T}_i^\ell = \begin{cases} \mathbf{A}\mathbf{V}_i^\ell & ((i,\ell)\neq(v,q))\\ \mathbf{A}\mathbf{V} & ((i,\ell) = (v,q))\end{cases},\quad \mathbf{Q}_i^\ell = \begin{cases} \mathbf{R}_i\mathbf{V}_i^\ell & ((i,\ell)\neq(v,q))\\ \mathbf{R}_i\mathbf{V} & ((i,\ell) = (v,q))\end{cases}$$

$$\mathbf{p}_{i,j}^{\ell^\top} = \begin{cases} \mathbf{V}_i^\ell\mathbf{B}\mathbf{r}_j^\top & (j\neq v, (i,\ell)\neq(v,q))\\ \mathbf{V}\mathbf{B}\mathbf{r}_j^\top & ((i,\ell) = (v,q))\\ \mathbf{V}_i^\ell\mathbf{d}^\top & (j = v)\end{cases},\quad \pi_i^\ell \leftarrow \mathsf{LSim}\left(\mathsf{crs}_i, \mathsf{td}_i, \left[\begin{pmatrix}\mathbf{T}_i^\ell\\ \mathbf{Q}_i^\ell\end{pmatrix}\right]_1\right)$$

Then, $\mathcal{B}$ sets $\mathcal{D}_i = (\mathsf{pk}_i^\ell, \mathbf{V}_i^\ell) \cup \mathcal{D}_i$ if $(i,\ell) \neq (v,q)$.

3. When $\mathcal{A}$ makes a query $\mathsf{OCor}(i, \mathsf{pk})$, $\mathcal{B}$ checks $i = v$ and $\mathsf{pk} = \mathsf{pk}_v^q$, and if so, $\mathcal{B}$ returns a random bit and halts. Otherwise, $\mathcal{B}$ gives sk to $\mathcal{A}$ if $(\mathsf{pk}, \mathsf{sk}) \in \mathcal{D}_i$.
4. When $\mathcal{A}$ outputs the challenge $(\{\mathsf{pk}_i^*, y_i\}_{i\in[L]}, x, M_0, M_1)$, $\mathcal{B}$ checks $\mathsf{pk}_v^* = \mathsf{pk}_i^q$. If it is not the case, $\mathcal{B}$ returns a random bit and halts. Otherwise, it parses $\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[\mathbf{p}_{i,j}^{*^\top}]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$ and gives $\mathsf{ct}_x = ([\mathbf{c}_1, \mathbf{C}_2, \ldots, \mathbf{C}_4]_1, C)$ to $\mathcal{A}$, where $(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$, $(m_1, m_2, \widehat{\mathbf{K}}_i) \leftarrow \mathsf{CVEncK}(y_i, \mathsf{aux}_k)$, $(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c)$, $(m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(y_1, \mathsf{aux}_k)$ and

$$\begin{aligned}
&\mathbf{s}_{\nu,\mu} \leftarrow \mathbb{Z}_p^k,\ \overline{\mathbf{S}} = (\mathbf{s}_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_1]},\ \mathbf{t}_{\nu,\mu} \leftarrow \mathbb{Z}_p^{k+1},\ \overline{\mathbf{T}} = (\mathbf{t}_{\nu,\mu})_{(\nu,\mu)\in[m_1]\times[n_3]}\\
&\mathbf{u}_{1,1} = \sum_{i\in[L]\setminus\{v\}} (\mathbf{c}\mathbf{W}_{i,0} + \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*) + \mathbf{c}\mathbf{W}_{v,0} + \mathbf{z}_{\beta'}\\
&\mathbf{u}_{\nu,\mu>1} \leftarrow \mathbb{Z}_p^{k+1},\ \mathbf{u}_{\nu>1,1} = \mathbf{0},\ \overline{\mathbf{U}} = (\mathbf{u}_{\nu,\mu})_{(\nu,\mu)\in[n_1]\times[m_3]},\ \beta \leftarrow \{0,1\}\\
&\mathbf{c}_1 = \mathbf{c},\ \mathbf{C}_2 = \overline{\mathbf{S}}(\mathbf{I}_{n_1} \otimes \mathbf{A}),\ \mathbf{C}_3 = \mathbf{C}\left(\overline{\mathbf{S}}, \overline{\mathbf{T}}, \sum_{i\in[L]} \mathbf{A}\mathbf{W}_i\right)\\
&\mathbf{C}_4 = \overline{\mathbf{U}}(\mathbf{L} \otimes \mathbf{I}_{k+1}) + \overline{\mathbf{S}}^{\mathsf{BT}} \sum_{i\in[L]} \widehat{\mathbf{K}}_i(\mathbf{A}\mathbf{W}_i),\ C = [\mathbf{c}\mathbf{h}^\top]_{\mathsf{T}} M_\beta
\end{aligned}$$

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

Observe that $\mathcal{A}$'s view corresponds to $\widehat{\mathsf{H}}_{5,v-1}^1$ if $\beta' = 0$ and $\widehat{\mathsf{H}}_{5,v-1}^2$ otherwise. This follows from the fact that $\mathsf{pk}_v^* = \mathsf{pk}_v^q$ implies $\mathbf{Q}_v^* = \mathbf{R}_v\mathbf{V}$, $\mathbf{R}_v = \widetilde{\mathbf{R}}_v \left({}^{\mathbf{c}}_{\mathbf{I}_{2k+1}} \right)$, and thus $\mathbf{e}_1\widetilde{\mathbf{R}}_v^{-1}\mathbf{Q}_v^* = \mathbf{c}\mathbf{V}$. Finally, since we are considering the honest case, i.e., $\mathcal{A}$ outputs pk_v^* such that $(\mathsf{pk}_v^*, *) \in \mathcal{D}_v$ and $(v, \mathsf{pk}_v^*) \notin \mathcal{C}$, $\mathcal{B}$ does not halt in step 3 or 4 with the probability not less than $1/Q$. Thus, if $\mathcal{A}$ distinguishes $\widehat{\mathsf{H}}^1_{5,v-1}$ and $\widehat{\mathsf{H}}^2_{5,v-1}$ with non-negligible advantage, then $\mathcal{B}$ distinguishes the two cases of Eq. (19) with non-negligible advantage, which breaks the MDDH assumption.

Dishonest Case. We prove that $\widehat{\mathsf{H}}^1_{5,v-1} \approx_c \widehat{\mathsf{H}}^2_{5,v-1}$ in the dishonest case if $\mathit{\Gamma}$ satisfies $\mathsf{KE\text{-}ind}$. Specifically, we construct a distinguisher $\mathcal{B}$ between the $\mathsf{KE\text{-}ind}$ games $\mathsf{G}_0^{\mathsf{KE\text{-}ind}}$ and $\mathsf{G}_1^{\mathsf{KE\text{-}ind}}$ for $\mathit{\Gamma}$ that internally uses a distinguisher $\mathcal{A}$ between $\widehat{\mathsf{H}}^1_{5,v-1}$ and $\widehat{\mathsf{H}}^2_{5,v-1}$ in the dishonest case as follows.

1. $\mathcal{B}$ is a $\mathsf{KE\text{-}ind}$ instance $([\mathbf{A}]_1, [\mathbf{B}]_2, \mathbf{a}, \mathbf{a}^\perp, \mathbf{b}^\perp, [\mathbf{A}\mathbf{W}_v]_1, [\mathbf{W}_v(\mathbf{I}_\omega \otimes \mathbf{B})]_2)$ for $\mathit{\Gamma}$. $\mathcal{B}$ computes crs as follows and gives it to $\mathcal{A}$:

$$\mathsf{crs} = \begin{pmatrix} [\mathbf{A}]_1, [\mathbf{A}\mathbf{h}^\top]_\mathsf{T}, \{\mathsf{crs}_i, [\mathbf{R}_i, \mathbf{A}\mathbf{W}_{i,0}, \mathbf{A}\mathbf{W}_i]_1\}_{i\in[L]} \\ \{[\mathbf{f}_i^\top, \mathbf{g}_i^\top]_2\}_{i\in[L]}, \{[\mathbf{n}_{i,j}^\top, \mathbf{N}_{i,j}]_2\}_{\substack{i,j\in[L] \\ i\neq j}} \end{pmatrix}$$

   where

$$\begin{aligned}
&\mathbf{h} \leftarrow \mathbb{Z}_p^{2k+1},\ (\mathsf{crs}_i, \mathsf{td}_i) \leftarrow \mathsf{LGen}(1^\lambda),\ \mathbf{W}_{i,0} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)},\ \mathbf{W}_{i\neq v} \leftarrow \mathbb{Z}_p^{(2k+1)\times\omega(k+1)} \\
&\mathbf{c} \leftarrow \mathbb{Z}_p^{2k+1},\ \widetilde{\mathbf{R}}_i \leftarrow \mathbb{Z}_p^{(2k+2)\times(2k+2)},\ \mathbf{R}_i = \widetilde{\mathbf{R}}_i \left(\begin{smallmatrix} \mathbf{c} \\ \mathbf{I}_{2k+1} \end{smallmatrix}\right),\ \mathbf{r}_{i\neq v} \leftarrow \mathbb{Z}_p^k,\ \mathbf{d} \leftarrow \mathbb{Z}_p^{k+1} \\
&\alpha_{i<v} \leftarrow \mathbb{Z}_p,\ \alpha_{i>v} = 0 \\
&\mathbf{f}_i^\top = \begin{cases} \mathbf{B}\mathbf{r}_i^\top & (i \neq v) \\ \mathbf{d}^\top & (i = v) \end{cases},\quad \mathbf{g}_i^\top = \begin{cases} \mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top + \alpha_i {\mathbf{a}^\perp}^\top & (i \neq v) \\ \mathbf{W}_{i,0}\mathbf{d}^\top + \mathbf{h}^\top & (i = v) \end{cases} \\
&\mathbf{n}_{i,j}^\top = \begin{cases} \mathbf{W}_{i,0}\mathbf{B}\mathbf{r}_j^\top & (j \neq v) \\ \mathbf{W}_{i,0}\mathbf{d}^\top & (j = v) \end{cases},\quad \mathbf{N}_{i,j} = \begin{cases} \mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{B}\mathbf{r}_j^\top) & (j \neq v) \\ \mathbf{W}_i(\mathbf{I}_\omega \otimes \mathbf{d}^\top) & (j = v) \end{cases}
\end{aligned}$$

2. When $\mathcal{A}$ makes the ℓ-th query $\mathsf{OGen}(i)$, $\mathcal{B}$ gives pk_i^ℓ to $\mathcal{A}$ as follows:

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

   where $\mathbf{V}_i^\ell \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}$, $\mathbf{T}_i^\ell = \mathbf{A}\mathbf{V}_i^\ell$, $\mathbf{Q}_i^\ell = \mathbf{R}_i\mathbf{V}_i^\ell$ and

$${\mathbf{p}_{i,j}^\ell}^\top = \begin{cases} \mathbf{V}_i^\ell\mathbf{B}\mathbf{r}_j^\top & (j \neq v) \\ \mathbf{V}_i^\ell\mathbf{d}^\top & (j = v) \end{cases},\quad \pi_i^\ell \leftarrow \mathsf{LSim}\left(\mathsf{crs}_i, \mathsf{td}_i, \left[\left(\begin{smallmatrix} \mathbf{T}_i^\ell \\ \mathbf{Q}_i^\ell \end{smallmatrix}\right)\right]_1\right)$$

   Then, $\mathcal{B}$ sets $\mathcal{D}_i = (\mathsf{pk}_i^\ell, \mathbf{V}_i^\ell) \cup \mathcal{D}_i$ if $(i, \ell) \neq (v, q)$.
3. When $\mathcal{A}$ makes a query $\mathsf{OCor}(i, \mathsf{pk})$, $\mathcal{B}$ gives sk to $\mathcal{A}$ if $(\mathsf{pk}, \mathsf{sk}) \in \mathcal{D}_i$.
4. When $\mathcal{A}$ outputs the challenge $(\{\mathsf{pk}_i^*, y_i\}_{i\in[L]}, x, M_0, M_1)$, $\mathcal{B}$ computes valid aux_c with respect to x and aux_k satisfying the well-formedness with respect to $\{y_i\}_{i\in[L]}$ in the same manner as Enc and Agg, respectively. Then, $\mathcal{B}$ queries the oracle $\mathcal{O}$ in the $\mathsf{KE\text{-}ind}$ game on $(x, y_v, \mathsf{aux}_c, \mathsf{aux}_k)$ and receives $([\overline{\mathbf{S}}_\mathbf{A},\ \mathbf{C}(\overline{\mathbf{S}}_\mathbf{A}, \overline{\mathbf{T}}, \mathbf{W}_v),\ \mathbf{K}_v(\overline{\mathbf{S}}_\mathbf{A}, \overline{\mathbf{U}}, \mathbf{W}_v)]_1)$, where $\mathbf{u}_{1,1} = \beta'\mathbf{b}^\perp$ (the $(1,1)$-th block of $\overline{\mathbf{U}}$) and β' is the challenge bit of the $\mathsf{KE\text{-}ind}$ game. $\mathcal{B}$ parses $\mathsf{pk}_i^* = ([\mathbf{T}_i^*, \mathbf{Q}_i^*]_1, \{[{\mathbf{p}_{i,j}^*}^\top]_2\}_{j\in[L]\setminus\{i\}}, \pi_i^*)$ and gives $\mathsf{ct}_x = ([\mathbf{c}_1, \mathbf{C}_2, \ldots, \mathbf{C}_4]_1, C)$ to $\mathcal{A}$, where $(n_1, n_2, \widehat{\mathbf{C}}) \leftarrow \mathsf{CVEncC}(x, \mathsf{aux}_c)$, $(m_1, m_2, \widehat{\mathbf{K}}_i) \leftarrow$

$\mathsf{CVEncK}(y_i, \mathsf{aux}_k)$, $(n_3, \mathbf{F}, \mathbf{C}) \leftarrow \mathsf{EncC}(x, m_1, \mathsf{aux}_c)$, $(m_3, \mathbf{L}) \leftarrow \mathsf{EncK}(y_1, \mathsf{aux}_k)$, $\beta \leftarrow \{0,1\}$ and

$$\overline{\mathbf{U}}' = \begin{pmatrix} \sum_{i\in[L]}(\mathbf{c}\mathbf{W}_{i,0} + \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^*) & \mathbf{0} \cdots \mathbf{0} \\ \mathbf{0} & \mathbf{0} \cdots \mathbf{0} \\ \vdots & \vdots \quad \vdots \\ \mathbf{0} & \mathbf{0} \cdots \mathbf{0} \end{pmatrix} \in \mathbb{Z}_p^{n_1 \times (k+1)m_3}$$

$$\mathbf{c}_1 = \mathbf{c},\ \mathbf{C}_2 = \overline{\mathbf{S}}_{\mathbf{A}},\ \mathbf{C}_3 = \mathbf{C}(\overline{\mathbf{S}}_{\mathbf{A}}, \overline{\mathbf{T}}, \mathbf{W}_v) + \sum_{j\in[L]\setminus\{v\}} \overline{\mathbf{S}}_{\mathbf{A}}\widehat{\mathbf{C}}(\mathbf{W}_j)$$

$$\mathbf{C}_4 = \mathbf{K}_v(\overline{\mathbf{S}}_{\mathbf{A}}, \overline{\mathbf{U}}, \mathbf{W}_v) + \overline{\mathbf{U}}'(\mathbf{L}\otimes\mathbf{I}_{k+1}) + \sum_{j\in[L]\setminus\{v\}} \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}}\widehat{\mathbf{K}}_j(\mathbf{W}_j)$$

$$C = [\mathbf{c}\mathbf{h}^\top]_{\mathsf{T}} M_\beta$$

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

$\mathcal{A}$'s view corresponds to $\widehat{\mathsf{H}}^1_{5,v-1}$ if $\beta' = 0$ and $\widehat{\mathsf{H}}^2_{5,v-1}$ otherwise, which follows from the following observation.

- Since $\mathbf{a}$ is not given to $\mathcal{A}$, $\mathbf{A}$ and $\mathbf{a}^\perp$ are distributed correctly.
- For $\mathbf{C}_3, \mathbf{C}_4$ in ct_x, we have

$$\mathbf{C}_3 = \overline{\mathbf{T}}(\mathbf{F}\otimes\mathbf{I}_{k+1}) + \sum_{j\in[L]} \overline{\mathbf{S}}_{\mathbf{A}}\widehat{\mathbf{C}}(\mathbf{W}_j) = \overline{\mathbf{T}}(\mathbf{F}\otimes\mathbf{I}_{k+1}) + \sum_{j\in[L]} \overline{\mathbf{S}}\widehat{\mathbf{C}}(\mathbf{A}\mathbf{W}_j)$$
$$= \mathbf{C}\left(\overline{\mathbf{S}}, \overline{\mathbf{T}}, \sum_{j\in[L]} \mathbf{A}\mathbf{W}_j\right)$$

where $\overline{\mathbf{S}}_{\mathbf{A}} = (\mathbf{s}_{\nu,\mu}\mathbf{A})_{\nu,\mu}$ and $\overline{\mathbf{S}} = (\mathbf{s}_{\nu,\mu})_{\nu,\mu}$, and

$$\mathbf{C}_4 = (\overline{\mathbf{U}} + \overline{\mathbf{U}}')(\mathbf{L}\otimes\mathbf{I}_{k+1}) + \sum_{j\in[L]} \overline{\mathbf{S}}_{\mathbf{A}}^{\mathsf{BT}}\widehat{\mathbf{K}}_j(\mathbf{W}_j)$$
$$= (\overline{\mathbf{U}} + \overline{\mathbf{U}}')(\mathbf{L}\otimes\mathbf{I}_{k+1}) + \overline{\mathbf{S}}^{\mathsf{BT}} \sum_{j\in[L]} \widehat{\mathbf{K}}_j(\mathbf{A}\mathbf{W}_j)$$

Hence, $\mathbf{C}_3, \mathbf{C}_4$ are distributed correctly.

This concludes the proof. □

Lemma D.9. $\widehat{\mathsf{H}}^2_{5,v-1} \approx_s \widehat{\mathsf{H}}^3_{5,v-1}$ *for* $v \in [L]$.

Proof. Let $\mathbf{W}_{v,0} = \mathbf{W}'_{v,0} + \alpha'\mathbf{a}^{\perp^\top}\mathbf{b}^\perp$ where $\mathbf{W}'_{v,0} \leftarrow \mathbb{Z}_p^{(2k+1)\times(k+1)}, \alpha' \leftarrow \mathbb{Z}_p$. Then, $\mathbf{W}_{v,0}$ and $\mathbf{W}'_{v,0}$ are equivalently distributed. The terms involving $\mathbf{W}_{v,0}$ are changed as follows:

$$\mathbf{A}\mathbf{W}_{v,0} = \mathbf{A}\mathbf{W}'_{v,0}, \quad \mathbf{g}_i^\top = \begin{cases} \mathbf{W}'_{i,0}\mathbf{B}\mathbf{r}_i^\top + \mathbf{h}^\top + \alpha_i\mathbf{a}^{\perp^\top} & (i \neq v) \\ \mathbf{W}'_{i,0}\mathbf{d}^\top + \mathbf{h}^\top + \underbrace{(\alpha'\mathbf{b}^\perp\mathbf{d}^\top)}_{\alpha_i}\mathbf{a}^{\perp^\top} & (i = v) \end{cases}$$

in crs, and

$$\mathbf{u}_{1,1} = \sum_{i\in[L]\setminus\{v\}} \mathbf{c}\mathbf{W}_{i,0} + \mathbf{c}\mathbf{W}'_{v,0} + \mathbf{e}_1\widetilde{\mathbf{R}}_i^{-1}\mathbf{Q}_i^* + \underbrace{(1 + \alpha'\mathbf{c}\mathbf{a}^{\perp^\top})\mathbf{b}^\perp}_{\mathbf{b}'^\perp}$$

in ct_x. It is not hard to see that α_v and $\mathbf{b}'^\perp$ are random elements in $\mathbb{Z}_p$ and $\mathbb{Z}_p^{k+1}$ conditioned on $\mathbf{b}'^\perp\mathbf{B} = \mathbf{0}$ unless $\mathbf{b}^\perp\mathbf{d}^\top = 0$ and $1 + \alpha'\mathbf{c}\mathbf{a}^{\perp^\top} = 0$, respectively, which occur with negligible probability. This corresponds to the distribution in $\widehat{\mathsf{H}}^3_{5,v-1}$, and thus $\widehat{\mathsf{H}}^2_{5,v-1} = \widehat{\mathsf{H}}^3_{5,v-1}$ with overwhelming probability. □

Lemma D.10. $\widehat{\mathsf{H}}^3_{5,v-1} \approx_c \mathsf{H}_{5,v}$ *for* $v \in [L]$.

This lemma can be proven similarly to $\mathsf{H}_{5,v-1} \approx_c \widehat{\mathsf{H}}^2_{5,v-1}$.

E PES Instantiations

In this section, we describe various PES constructions for sReg-ABE. The main purpose is to explicitly describe PES constructions that are in the tranformation sequence when constructing PES for sReg-ABE for completely unbounded ciphertext-policy monotone span programs and non-monotone span programs, which we show the results in Section 7.

Various PES constructions in this section are for sReg-ABE for their respective predicates. In particular, they differ from the original PES definition for vanilla ABEs. We do not relate original PES for ABE to PES for sReg-ABE for the same predicate. Instead, we start from predicate encoding for basic predicates and consequently apply transformations in Section 4 to obtain PES for sReg-ABE for more complex predicates until we obtain the ones for unbounded monotone span programs and non-monotone span programs.

E.1 Embedding Lemma

For arguing implications among PESs, we use the embedding lemma. Such a lemma is already known and applied for arguing implications among ABE schemes [BH08,AHY15] and PES for vanilla ABEs [Att19, AT20] . Here we capture that the embedding also preserves properties of our new variant for PES for sReg-ABE as well, in the lemma below.

Definition E.1 (Embedding [Att19]). Let $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$, and $\mathsf{P}'_{\kappa'} : \mathcal{X}'_{\kappa'} \times \mathcal{Y}'_{\kappa'} \to \{0,1\}$ be two predicate families, indexed by $\kappa \in \mathcal{K}$ and $\kappa' \in \mathcal{K}'$, respectively. We say that P' *can be embedded into* P if there exists three efficient mappings $f_\mathsf{p}, f_\mathsf{c}, f_\mathsf{k}$ where $f_\mathsf{p} : \mathcal{K}' \to \mathcal{K}$ maps $\kappa' \mapsto \kappa$ and $f_\mathsf{c} : \mathcal{X}'_{\kappa'} \to \mathcal{X}_\kappa$, $f_\mathsf{k} : \mathcal{Y}'_{\kappa'} \to \mathcal{Y}_\kappa$ such that for all $x' \in \mathcal{X}'_{\kappa'}, y' \in \mathcal{Y}'_{\kappa'}$, we have:

$$\mathsf{P}'_{\kappa'}(x', y') = 1 \quad \Longleftrightarrow \quad \mathsf{P}_\kappa(f_\mathsf{c}(x'), f_\mathsf{k}(y')) = 1. \tag{20}$$

Lemma E.1. *If* P' *can be embedded into* P*, then we can construct a PES* Γ' *for* P' *from a PES* Γ *for* P *in such a way that it preserves the correctness, the well-formedness, and the key-encoding indistinguishability of the PES* Γ *for* P.

Proof sketch. Let Γ be a PES for P. We construct a PES Γ' for P' by simply defining

$$\begin{aligned}
\mathsf{Param}'(\kappa') &= \mathsf{Param}(f_\mathsf{p}(\kappa')),\\
\mathsf{CVEncC}'(x', \mathsf{aux}_c) &= \mathsf{CVEncC}(f_\mathsf{c}(x'), \mathsf{aux}_c),\\
\mathsf{CVEncK}'(y', \mathsf{aux}_k) &= \mathsf{CVEncK}(f_\mathsf{k}(y'), \mathsf{aux}_k),\\
\mathsf{EncC}'(x', m_1, \mathsf{aux}_c) &= \mathsf{EncC}(f_\mathsf{c}(x'), m_1, \mathsf{aux}_c),\\
\mathsf{EncK}'(y', n_1, \mathsf{aux}_k) &= \mathsf{EncK}(f_\mathsf{k}(y'), n_1, \mathsf{aux}_k),\\
\mathsf{Pair}'(x', y', \mathsf{aux}_c, \mathsf{aux}_k) &= \mathsf{Pair}(f_\mathsf{c}(x'), f_\mathsf{k}(y'), \mathsf{aux}_c, \mathsf{aux}_k).
\end{aligned}$$

The correctness and security is guaranteed by the forward and backward direction of Eq. (20), respectively. The well-formedness also preserves due to the existence of respective aux_k, m_1, m_2 in the case of key well-formedness and aux_c, n_1, n_2 in the case of ciphertext well-formedness, as we use these values as is in the inputs of the respective algorithms above. □

E.2 PES for Completely Unbounded MSP Predicates

In this section, we explicitly describe a PES construction for sReg-ABE for completely unbounded ciphertext-policy monotone span program predicates, which we stated the result in Section 7.

PES for IBE. We start with the predicate encoding Γ^{IBE} for equality or also called IBE predicate, $\mathsf{P}^{\mathsf{IBE}}$. The PES Γ^{IBE} is specified by $\mathsf{aux}_c = \mathsf{aux}_k = \varepsilon$ (the empty string) and

- $\mathsf{Param}(\kappa) \to 2$. Let $\mathbf{w} = (w_1, w_2)$.
- $\mathsf{CVEncC}(x) \to n_1 = 1, n_2 = 1,\ \widehat{\mathbf{F}} = (x, 1)^\top,\ \widehat{\mathbf{C}} = w_1 x + w_2$.
- $\mathsf{CVEncK}(y) \to m_1 = 1, m_2 = 1,\ \widehat{\mathbf{L}} = (y, 1)^\top,\ \widehat{\mathbf{K}} = w_1 y + w_2$.
- $\mathsf{EncC}(x, m_1) \to n_3 = 0,\ \mathbf{F} = 0,\ \mathbf{C} = s(w_1 x + w_2)$.
- $\mathsf{EncK}(y, n_1) \to m_3 = 1,\ \mathbf{L} = 1,\ \mathbf{K} = u + s(w_1 y + w_2)$.
- $\mathsf{Pair}(x, y) \to \mathbf{E} = -1,\ \overline{\mathbf{E}} = 1$.

The correctness holds as $\mathsf{tr}(\mathbf{E}\mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w})) + \mathsf{tr}(\overline{\mathbf{E}}\mathbf{K}(\mathbf{S}, \mathbf{U}, \mathbf{w})) = (-1)s(w_1 x + w_2) + (1)(u + s(w_1 y + w_2)) = u$, for $x = y$.

Lemma E.2. *The PES Γ^{IBE} for $\mathsf{P}^{\mathsf{IBE}}$ satisfies ciphertext and key well-formedness, and* KE-ind.

Proof. The above PES is a secure predicate encoding in *e.g.,* [Wee14,CGW15] for $\mathsf{P}^{\mathsf{IBE}}$. Via Lemma 3.1, we obtain the corresponding PES for sReg-ABE which satisfies ciphertext and key well-formedness, and KE-ind for this predicate. □

In what follows, we subsequently apply transformations to the above PES Γ^{IBE}. The correctness of these PESs then immediately follow from the correctness of respective transformation, and we will not explicitly show here. Moreover, via Theorem 5.1, we can argue that all the resulting PESs except the last two satisfy all ciphertext and key well-formedness, and KE-ind. The last one, for unbounded CP-MSP, satisfies key well-formedness and KE-ind; hence it can be used for sReg-ABE construction of Section 6.1.

PES for IBE with Null Attribute. We now obtain a PES, denoted as $\Gamma^{\mathsf{IBE+n}}$. for the predicate $\mathsf{Null}[\mathsf{P}^{\mathsf{IBE}}]$ via the Null-Trans transformation to the PES for IBE above. We have that $\mathsf{aux}_c = \mathsf{aux}_k = \varepsilon$ (the empty string)[12] and

- $\mathsf{Param}(\kappa) \to 3$. Let $\mathbf{w} = (w_0, w_1, w_2)$.
- $\mathsf{CVEncC}(x) \to n_1 = 1, n_2 = 1,\ \widehat{\mathbf{F}} = (0, x, 1)^\top,\ \widehat{\mathbf{C}} = w_1 x + w_2$.
- $\mathsf{CVEncK}(y) \to m_1 = 1, m_2 = 1,\ \widehat{\mathbf{L}} = (0, y, 1)^\top,\ \widehat{\mathbf{K}} = \begin{cases} w_1 y + w_2 & \text{if } y \in \mathcal{Y}_\kappa \\ w_0 & \text{if } y = \mathsf{null} \end{cases}$.
- $\mathsf{EncC}(x, m_1 = 1) \to n_3 = 0,\ \mathbf{F} = 0,\ \mathbf{C} = s(w_1 x + w_2)$.
- $\mathsf{EncK}(y, n_1 = 1) \to m_3 = 1,\ \mathbf{L} = 1,\ \mathbf{K} = \begin{cases} u + s(w_1 y + w_2) & \text{if } y \in \mathcal{Y}_\kappa \\ u + s w_0 & \text{if } y = \mathsf{null} \end{cases}$.
- $\mathsf{Pair}(x, y) \to \begin{cases} \mathbf{E} = -1,\ \overline{\mathbf{E}} = 1 & \text{if } y \in \mathcal{Y}_\kappa \\ \mathbf{E} = \perp,\ \overline{\mathbf{E}} = \perp & \text{if } y = \mathsf{null} \end{cases}$.

PES for Key-Set Membership. We next obtain a PES Γ^{KSM} for the key-set membership predicate $\mathsf{P}^{\mathsf{KSM}}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0, 1\}$, where $\mathcal{Y}_\kappa = 2^{\mathcal{X}_\kappa}$, defined as $\mathsf{P}^{\mathsf{KSM}}_\kappa(x, S) = 1 \Leftrightarrow x \in S$. It is straightforward

[12] In the Null-Trans transformation, it is indeed the case that we define aux_k as follows (see the proof of Lemma C.1). For $Y' \subseteq \mathcal{Y}_\kappa \cup \{\mathsf{null}\}$, set $\mathsf{aux}_k = y' \in \mathcal{Y}_\kappa$, where y' is a non-null element (say, the first) in Y'. However, this y' element is only used to compute $\mathbf{L}$ in the case of a generic predicate. However, for the IBE (with Null) predicate here, we simply have $\mathbf{L} = 1$, and we can neglect aux_k completely.

to see that $\mathsf{P}^{\mathsf{KSM}}$ can be embedded into the predicate $\mathsf{KP1}_{\mathsf{OR}}[\mathsf{Null}[\mathsf{P}^{\mathsf{IBE}}]]$. Note that $\mathsf{KP1}_{\mathsf{OR}}$ is the key policy disjunction as per Definition 4.3. Here the embedding works as:

$$x \mapsto x \qquad\qquad S \mapsto \phi_S \text{ where } \phi_S : \begin{array}{c} [z] \to \mathcal{X}_\kappa \\ j \mapsto a_j \end{array}$$

where $z := |S|$ and write $S = \{a_1, \ldots, a_z\}$ (in a lexicographical order). Hence we apply the $\mathsf{KP1}_{\mathsf{OR}}$-$\mathsf{Trans}$ to the PES above and obtain a new PES as follows. For $Y = \{S_1, \ldots, S_L\} \subseteq \mathcal{Y}_\kappa$, we set $\mathsf{aux}_k = \delta := \max_{i\in[L]} |S_i|$. [13] [14] Note that $\mathsf{aux}_c = \varepsilon$.

- $\mathsf{Param}(\kappa) \to 3$. Let $\mathbf{w} = (w_0, w_1, w_2)$.
- $\mathsf{CVEncC}(x) \to n_1 = 1, n_2 = 1,\ \widehat{\mathbf{F}} = (0, x, 1)^\top,\ \widehat{\mathbf{C}} = w_1 x + w_2$.
- $\mathsf{CVEncK}(S = \{a_1, \ldots, a_z\}, \mathsf{aux}_k = \delta) \to m_1 = \delta, m_2 = \delta,\ \widehat{\mathbf{L}},\ \widehat{\mathbf{K}}$ where

$$\widehat{\mathbf{L}} = \begin{pmatrix} \begin{smallmatrix}0\\a_1\\1\end{smallmatrix} & & & & & \\ & \vdots & & & & \\ & & \begin{smallmatrix}0\\a_z\\1\end{smallmatrix} & & & \\ & & & \begin{smallmatrix}1\\0\\0\end{smallmatrix} & & \\ & & & & \vdots & \\ & & & & & \begin{smallmatrix}1\\0\\0\end{smallmatrix} \end{pmatrix} \in \mathbb{Z}_p^{3\delta\times\delta}$$

$$\widehat{\mathbf{K}} = \begin{pmatrix} w_1 a_1 + w_2 & & & & & \\ & \ddots & & & & \\ & & w_1 a_z + w_2 & & & \\ & & & w_0 & & \\ & & & & \ddots & \\ & & & & & w_0 \end{pmatrix} = (\mathbf{I}_\delta \otimes \mathbf{w})\widehat{\mathbf{L}}\ \in \mathbb{Z}_p[\mathbf{w}]^{\delta\times\delta}$$

- $\mathsf{EncC}(x, m_1 = \delta) \to n_3 = 0,\ \mathbf{F} = 0,\ \mathbf{C} = \mathbf{S}\widehat{\mathbf{C}} = \mathbf{S}(w_1 x + w_2)$ with $\mathbf{S} = (s_1, \ldots, s_\delta)^\top$, *i.e.*,

$$\mathbf{C} = \big(s_1(w_1 x + w_2), \ldots, s_\delta(w_1 x + w_2)\big)^\top.$$

- $\mathsf{EncK}(S = \{a_1, \ldots, a_z\}, n_1 = 1, \mathsf{aux}_k = \delta) \to m_3 = 1,\ \mathbf{L}, \mathbf{K}$ where

$$\begin{aligned} \mathbf{L} &= (1, \ldots 1) \quad \in \mathbb{Z}_p^{1\times\delta} \\ \mathbf{K} &= u\mathbf{L} + \mathbf{S}^\top \widehat{\mathbf{K}} \quad \in \mathbb{Z}_p[\mathbf{S}, u, \mathbf{w}]^{1\times\delta} \\ &= \big(u + s_1(w_1 a_1 + w_2), \ldots, u + s_z(w_1 a_z + w_2), u + s_{z+1} w_0, \ldots, u + s_\delta w_0\big) \end{aligned}$$

  where $\mathbf{S} = (s_1, \ldots, s_\delta)^\top$.
- $\mathsf{Pair}(x, y, \mathsf{aux}_k) \to \mathbf{E} = (0, \ldots, 0, -1, 0, \ldots, 0),\ \overline{\mathbf{E}} = (0, \ldots, 0, 1, 0, \ldots, 0)^\top$ where both are of length δ and -1, 1 is at the i-th position where $a_i = y$.

PES for Ciphertext-Set Membership (IBBE). This predicate is defined as $\mathsf{P}^{\mathsf{CSM}}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$, where $\mathcal{X}_\kappa = 2^{\mathcal{Y}_\kappa}$, defined as $\mathsf{P}^{\mathsf{CSM}}_\kappa(S, y) = 1 \Leftrightarrow y \in S$. It exactly defines the predicate for IBBE (ID-based broadcast encryption). It is the dual of the key-set membership predicate; therefore, we obtain its PES Γ^{CSM} by the Dual-Trans transformation. For $X = \{S_1, \ldots, S_L\} \subseteq \mathcal{X}_\kappa$, we set $\mathsf{aux}_c = \delta := \max_{i\in[L]} |S_i|$. Note that $\mathsf{aux}_k = \varepsilon$.

[13] Recall that we will use this PES to construct sReg-ABE and the $\mathsf{pk}_1, \ldots, \mathsf{pk}_L$ corresponding to $S_1, \ldots, S_L$, respectively, are to be aggregated into mpk.

[14] This follows from the proof of Lemma C.5.

- $\mathsf{Param}(\kappa) \to 4$. Let $\mathbf{w} = (\bar{w}_0, w_0, w_1, w_2)$.
- $\mathsf{CVEncC}(S = \{a_1, \ldots, a_z\}, \mathsf{aux}_c = \delta) \to n_1 = \delta + 1, n_2 = \delta,\ \widehat{\mathbf{F}},\ \widehat{\mathbf{C}}$ where

$$\widehat{\mathbf{F}} = \left(\begin{array}{ccccccc}
1 & 1 & \cdots & & & & 1 \\
0 & 0 & \cdots & & & & 0 \\
0 & 0 & \cdots & & & & 0 \\
0 & 0 & \cdots & & & & 0 \\
0 & & & & & & \\
0 & & & & & & \\
a_1 & & & & & & \\
1 & & & & & & \\
 & \vdots & & & & & \\
 & & & 0 & & & \\
 & & & 0 & & & \\
 & & & a_z & & & \\
 & & & 1 & & & \\
 & & & & 0 & & \\
 & & & & 1 & & \\
 & & & & 0 & & \\
 & & & & 0 & & \\
 & & & & & \vdots & \\
 & & & & & & 0 \\
 & & & & & & 1 \\
 & & & & & & 0 \\
 & & & & & & 0
\end{array}\right) \in \mathbb{Z}_p^{4(\delta+1)\times\delta} \tag{21}$$

$$\widehat{\mathbf{C}} = \left(\begin{array}{cccccc}
\bar{w}_0 & & \cdots & & & \bar{w}_0 \\
w_1 a_1 + w_2 & & & & & \\
 & \ddots & & & & \\
 & & w_1 a_z + w_2 & & & \\
 & & & w_0 & & \\
 & & & & \ddots & \\
 & & & & & w_0
\end{array}\right) = (\mathbf{I}_{\delta+1} \otimes \mathbf{w})\widehat{\mathbf{F}} \ \in \mathbb{Z}_p[\mathbf{w}]^{(\delta+1)\times\delta}$$

- $\mathsf{CVEncK}(y) \to m_1 = 1, m_2 = 2,\ \widehat{\mathbf{L}} = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 0 \\ 0 & y \\ 0 & 1 \end{smallmatrix}\right), \widehat{\mathbf{K}} = \mathbf{w}\widehat{\mathbf{L}} = (-\bar{w}_0, w_1 y + w_2)$.
- $\mathsf{EncC}(S = \{a_1, \ldots, a_z\}, m_1 = 1, \mathsf{aux}_c = \delta) \to n_3 = 0,\ \mathbf{F} = 0,\ \mathbf{C}$ where

$$\begin{aligned}
\mathbf{C} = \Big(&\bar{s}_0\bar{w}_0 + s_1(w_1 a_1 + w_2),\ \ldots,\ \bar{s}_0\bar{w}_0 + s_z(w_1 a_z + w_2), \\
&\qquad\qquad \bar{s}_0\bar{w}_0 + s_{z+1}w_0,\ \ldots,\ \bar{s}_0\bar{w}_0 + s_\delta w_0)\Big) \\
= \mathbf{S}&\widehat{\mathbf{C}} \quad \in \mathbb{Z}_p[\mathbf{S}, \mathbf{w}]^{1\times\delta} \qquad \text{where } \mathbf{S} = (\bar{s}_0, s_1, \ldots, s_\delta).
\end{aligned}$$

- $\mathsf{EncK}(y, n_1 = \delta + 1) \to m_3 = 1,\ \mathbf{L} = (1, 0),\ \mathbf{K}$ where

$$\begin{aligned}
\mathbf{K} &= \mathbf{U}\mathbf{L} + \mathbf{S}^\top\widehat{\mathbf{K}} \in \mathbb{Z}_p[\mathbf{S}, \mathbf{U}, \mathbf{w}]^{(\delta+1)\times 2} \\
&= \begin{pmatrix}
u_{1,1} - \bar{s}_0\bar{w}_0, & \bar{s}_0(w_1 y + w_2) \\
u_{2,1} - s_1\bar{w}_0, & s_1(w_1 y + w_2) \\
\vdots & \vdots \\
u_{\delta+1,1} - s_\delta\bar{w}_0, & s_\delta(w_1 y + w_2)
\end{pmatrix}
\end{aligned}$$

  where $\mathbf{U} = \{u_{i,j}\}_{i\in[\delta+1], j\in[1]}$ and $\mathbf{S} = (\bar{s}_0, s_1, \ldots, s_\delta)$.
- $\mathsf{Pair}(x, y, \mathsf{aux}_k) \to \mathbf{E} = (0, \ldots, 0, 1, 0, \ldots, 0)^\top \in \mathbb{Z}_p^{\delta\times 1}$, s.t. 1 is at i-th row, $\overline{\mathbf{E}} = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & -1 & 0 & \cdots & 0 \end{smallmatrix}\right) \in \mathbb{Z}_p^{2\times(\delta+1)}$, where -1 is at the $(i+1)$-th column, where i is such that $a_i = y$.

PES for Key-Policy Monotone Span Programs over Large Universe. This predicate is defined as $\mathsf{P}^{\mathsf{KP-MSP}} := \mathsf{KP1}[\mathsf{P}^{\mathsf{CSM}}]$. Let $\mathcal{Y}_\kappa$ be the attribute universe. From Definition 4.7, we obtain the concrete definition of $\mathsf{P}^{\mathsf{KP-MSP}_\kappa} = \mathsf{KP1}[\mathsf{P}^{\mathsf{CSM}}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0, 1\}$ as follows. We have $\bar{\mathcal{X}}_\kappa = 2^{\mathcal{Y}_\kappa}$

and $\bar{\mathcal{Y}}_\kappa = \bigcup_{(n,m)\in\mathbb{N}^2}(\mathbb{Z}_p^{n\times m}\times \varPhi_n)$, where $\varPhi_n$ consists of all functions $\phi : [n] \to \mathcal{Y}_\kappa$. For $S \subseteq \mathcal{Y}_\kappa$ (*i.e.*, $S \in \bar{\mathcal{X}}_\kappa$) and $(\mathbf{M}, \phi) \in \bar{\mathcal{Y}}_\kappa$ where $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$ and $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$, we have

$$\mathsf{P}_\kappa^{\mathsf{KP-MSP}}(S, (\mathbf{M}, \phi)) = 1 \Leftrightarrow (1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in[n]:\phi(i)\in S}).$$

We obtain a PES $\Gamma^{\mathsf{KP-MSP}}$ using the $\mathsf{KP1\text{-}Trans}$ transformation over the above PES for $\mathsf{P}^{\mathsf{CSM}}$ as follows. We set $\mathsf{aux}_c, \mathsf{aux}_k$ as in the PES for $\mathsf{P}^{\mathsf{CSM}}$. That is, for $X = \{S_1, \ldots, S_L\} \subseteq \mathcal{X}_\kappa$, we set $\mathsf{aux}_c = \delta := \max_{i\in[L]} |S_i|$. Note that $\mathsf{aux}_k = \varepsilon$.

- $\mathsf{Param}(\kappa) \to 4$. Let $\mathbf{w} = (\bar{w}_0, w_0, w_1, w_2)$.
- $\mathsf{CVEncC}(S = \{a_1, \ldots, a_z\}, \mathsf{aux}_c = \delta) \to n_1 = \delta + 1, n_2 = \delta,\ \widehat{\mathbf{F}},\ \widehat{\mathbf{C}}$ where $\widehat{\mathbf{F}},\ \widehat{\mathbf{C}}$ are exactly as in Eq. (21).
- $\mathsf{CVEncK}((\mathbf{M}, \phi)) \to m_1 = n, m_2 = 2n,\ \widehat{\mathbf{L}},\ \widehat{\mathbf{K}}$ where

$$\widehat{\mathbf{L}} = \begin{pmatrix} \begin{smallmatrix} -1 & 0 \\ 0 & 0 \\ 0 & \phi(1) \\ 0 & 1 \end{smallmatrix} & & \\ & \ddots & \\ & & \begin{smallmatrix} -1 & 0 \\ 0 & 0 \\ 0 & \phi(n) \\ 0 & 1 \end{smallmatrix} \end{pmatrix} \in \mathbb{Z}_p^{4n\times 2n}.$$

$$\widehat{\mathbf{K}} = \begin{pmatrix} -\bar{w}_0,\ w_1\phi(1) + w_2 & & \\ & \ddots & \\ & & -\bar{w}_0,\ w_1\phi(n) + w_2 \end{pmatrix} = (\mathbf{I}_n \otimes \mathbf{w})\widehat{\mathbf{L}}\ \in \mathbb{Z}_p[\mathbf{S}, \mathbf{U}, \mathbf{w}]^{n\times 2n}.$$

- $\mathsf{EncC}(S = \{a_1, \ldots, a_z\}, m_1 = n, \mathsf{aux}_c = \delta) \to n_3 = 0,\ \mathbf{F} = 0,\ \mathbf{C}$ where

$$\mathbf{C} = \mathbf{S}\widehat{\mathbf{C}} \quad \in \mathbb{Z}_p[\mathbf{S}, \mathbf{w}]^{n\times\delta}$$

where $\mathbf{S}$ is of size $n \times (\delta + 1)$. To write $\mathbf{C}$ explicitly, and to relate terms with the base previous PES for $\mathsf{P}_\kappa^{\mathsf{CSM}}$, we set

$$\mathbf{S} = \begin{pmatrix} \bar{s}_{0,1},\ s_{1,1},\ \ldots,\ s_{\delta,1} \\ \vdots \\ \bar{s}_{0,n},\ s_{1,n},\ \ldots,\ s_{\delta,n} \end{pmatrix}.$$

Then, we have $\mathbf{C} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix}$ where

$$\begin{aligned} \mathbf{b}_i := \Big(& \bar{s}_{0,i}\bar{w}_0 + s_{1,i}(w_1 a_1 + w_2),\ \ldots,\ \bar{s}_{0,i}\bar{w}_0 + s_{z,i}(w_1 a_z + w_2), \\ & \qquad \bar{s}_{0,i}\bar{w}_0 + s_{z+1,i}w_0,\ \ldots,\ \bar{s}_{0,i}\bar{w}_0 + s_{\delta,i}w_0)\Big). \end{aligned}$$

- $\mathsf{EncK}((\mathbf{M}, \phi), n_1 = \delta + 1) \to m_3 = m,\ \mathbf{L}, \mathbf{K}$ where

$$\begin{aligned} \mathbf{L} &= (\mathbf{m}_1^\top, \mathbf{0}, \cdots, \mathbf{m}_n^\top, \mathbf{0}) \\ \mathbf{K} &= \mathbf{U}\mathbf{L} + \mathbf{S}^\top\widehat{\mathbf{K}} && \in \mathbb{Z}_p[\mathbf{S}, \mathbf{U}, \mathbf{w}]^{(\delta+1)\times 2n} \end{aligned}$$

where $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$, $\mathbf{U} = \{u_{i,j}\}_{i\in[\delta+1],j\in[m]}$, and $\mathbf{S}$ is as above. In explicit terms, we have $\mathbf{K} = (\mathbf{B}_1, \ldots, \mathbf{B}_n)$ where

$$\mathbf{B}_i := \begin{pmatrix} \mathbf{u}_1\mathbf{m}_i^\top - \bar{s}_{0,i}\bar{w}_0, & \bar{s}_{0,i}(w_1\phi(i) + w_2) \\ \mathbf{u}_2\mathbf{m}_i^\top - s_{1,i}\bar{w}_0, & s_{1,i}(w_1\phi(i) + w_2) \\ \vdots & \vdots \\ \mathbf{u}_{\delta+1}\mathbf{m}_i^\top - s_{\delta,i}\bar{w}_0, & s_{\delta,i}(w_1\phi(i) + w_2) \end{pmatrix} \in \mathbb{Z}_p[\mathbf{S}, \mathbf{U}, \mathbf{w}]^{(\delta+1)\times 2}$$

where $\mathbf{u}_j := (u_{i,1}, \ldots u_{i,m})$.

- $\mathsf{Pair}(x, y, \mathsf{aux}_c) \to \mathbf{E}, \overline{\mathbf{E}}$ described as follows. Let $\mathit{\Omega}$ be a set such that $\phi(i) = a_{j_i} \in S$ for $i \in \mathit{\Omega}$ and $(1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in\mathit{\Omega}})$, and $\tau_1, \ldots, \tau_n \in \mathbb{Z}_p$ be coefficients such that $\tau_i = 0$ for $i \notin \mathit{\Omega}$ and $\sum_{i\in[n]} \tau_i\mathbf{m}_i = (1, \mathbf{0})$. We set $\mathbf{E}' = (\tau_1\mathbf{E}_1|| \cdots ||\tau_n\mathbf{E}_n)$ and $\overline{\mathbf{E}}' = \begin{pmatrix} \tau_1\overline{\mathbf{E}}_1 \\ \vdots \\ \tau_n\overline{\mathbf{E}}_n \end{pmatrix}$ where $\mathbf{E}_i = (0, \ldots, 0, 1, 0, \ldots, 0)^\top \in \mathbb{Z}_p^{\delta\times 1}$ where 1 is at j_i-th row, and $\overline{\mathbf{E}}_i = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & -1 & 0 & \cdots & 0 \end{smallmatrix}\right) \in \mathbb{Z}_p^{2\times(\delta+1)}$, where -1 is at the $(j_i + 1)$-th column.

PES for Ciphertext-Policy Monotone Span Programs over Large Universe. This predicate is defined as $\mathsf{P}^{\mathsf{CP-MSP}} := \mathsf{Dual}[\mathsf{KP1}[\mathsf{P}^{\mathsf{CSM}}]]$. Let $\mathcal{X}_\kappa$ be the attribute universe. We obtain the concrete definition of $\mathsf{P}^{\mathsf{CP-MSP}_\kappa} : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0, 1\}$ as follows. We have $\bar{\mathcal{Y}}_\kappa = 2^{\mathcal{X}_\kappa}$ and $\bar{\mathcal{X}}_\kappa = \bigcup_{(n,m)\in\mathbb{N}^2}(\mathbb{Z}_p^{n\times m} \times \mathit{\Phi}_n)$, where $\mathit{\Phi}_n$ consists of all functions $\phi : [n] \to \mathcal{X}_\kappa$. For $S \subseteq \mathcal{X}_\kappa$ (*i.e.*, $S \in \bar{\mathcal{Y}}_\kappa$) and $(\mathbf{M}, \phi) \in \bar{\mathcal{X}}_\kappa$ where $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$ and $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$, we have

$$\mathsf{P}_\kappa^{\mathsf{CP-MSP}}((\mathbf{M}, \phi), S) = 1 \Leftrightarrow (1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in[n]:\phi(i)\in S}).$$

We obtain a PES $\mathit{\Gamma}^{\mathsf{CP-MSP}}$ using the $\mathsf{Dual\text{-}Trans}$ transformation over the above PES for $\mathsf{P}^{\mathsf{KP-MSP}}$ as follows. For $Y = \{S_1, \ldots, S_L\} \subseteq \mathcal{Y}_\kappa$, we set $\mathsf{aux}_k = \delta := \max_{i\in[L]} |S_i|$. Note that $\mathsf{aux}_c = \varepsilon$.

- $\mathsf{Param}(\kappa) \to 5$. Let $\mathbf{w} = (\bar{\bar{w}}_0, \bar{w}_0, w_0, w_1, w_2)$.
- $\mathsf{CVEncC}((\mathbf{M}, \phi)) \to n_1 = n + 1, n_2 = 2n,\ \widehat{\mathbf{F}},\ \widehat{\mathbf{C}}$ where

$$\widehat{\mathbf{F}} = \begin{pmatrix} 1 & & \cdots & & 1 \\ 0 & & \cdots & & 0 \\ 0 & & \cdots & & 0 \\ 0 & & \cdots & & 0 \\ 0 & & \cdots & & 0 \\ 0 & 0 & & & \\ -1 & 0 & & & \\ 0 & 0 & & & \\ 0 & \phi(1) & & & \\ 0 & 1 & & & \\ & & \ddots & & \\ & & & 0 & 0 \\ & & & -1 & 0 \\ & & & 0 & 0 \\ & & & 0 & \phi(n) \\ & & & 0 & 1 \end{pmatrix} \in \mathbb{Z}_p^{5(n+1)\times 2n}.$$

$$\widehat{\mathbf{C}} = \begin{pmatrix} \bar{\bar{w}}_0 m_{1,1} & 0 & \cdots \bar{\bar{w}}_0 m_{n,1} & 0 \\ -\bar{w}_0, & w_1\phi(1) + w_2 & & \\ & & \ddots & \\ & & -\bar{w}_0, & w_1\phi(n) + w_2 \end{pmatrix} = (\mathbf{I}_{n+1} \otimes \mathbf{w})\widehat{\mathbf{F}}\ \in \mathbb{Z}_p[\mathbf{w}]^{(n+1)\times 2n}.$$

- $\mathsf{CVEncK}(S = \{a_1, \dots, a_z\}, \mathsf{aux}_k = \delta) \to m_1 = \delta + 1, m_2 = \delta + 1,\ \widehat{\mathbf{L}},\ \widehat{\mathbf{K}}$ where

$$\widehat{\mathbf{L}} = \begin{pmatrix} 1 & 1 & \cdots & & & 1 \\ 0 & 0 & \cdots & & & 0 \\ 0 & 0 & \cdots & & & 0 \\ 0 & 0 & \cdots & & & 0 \\ 0 & 0 & \cdots & & & 0 \\ 0 & & & & & \\ 0 & & & & & \\ 0 & & & & & \\ a_1 & & & & & \\ 1 & & & & & \\ & \vdots & & & & \\ & & 0 & & & \\ & & 0 & & & \\ & & 0 & & & \\ & & a_z & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & 0 & & \\ & & & 1 & & \\ & & & 0 & & \\ & & & 0 & & \\ & & & & \vdots & \\ & & & & & 0 \\ & & & & & 0 \\ & & & & & 1 \\ & & & & & 0 \\ & & & & & 0 \end{pmatrix} \in \mathbb{Z}_p^{5(\delta+1)\times(\delta+1)}$$

$$\widehat{\mathbf{K}} = \begin{pmatrix} -\bar{\bar{w}}_0 & \bar{w}_0 & & \cdots & & & \bar{w}_0 \\ 0 & w_1 a_1 + w_2 & & & & & \\ & & \ddots & & & & \\ & & & w_1 a_z + w_2 & & & \\ & & & & w_0 & & \\ & & & & & \ddots & \\ & & & & & & w_0 \end{pmatrix} = (\mathbf{I}_{\delta+1} \otimes \mathbf{w})\widehat{\mathbf{L}} \ \in \mathbb{Z}_p[\mathbf{w}]^{(\delta+1)\times(\delta+1)}$$

- $\mathsf{EncC}((\mathbf{M}, \phi), m_1 = \delta + 1) \to n_3 = m - 1,\ \mathbf{F},\ \mathbf{C}$ where

$$\begin{aligned} \mathbf{F} &= \big(\underline{\mathbf{m}}_1^\top, \mathbf{0}, \cdots, \underline{\mathbf{m}}_n^\top, \mathbf{0}\big) && \in \mathbb{Z}_p^{(m-1)\times 2n} \\ \mathbf{C} &= \mathbf{T}\mathbf{F} + \mathbf{S}\widehat{\mathbf{C}} && \in \mathbb{Z}_p[\mathbf{S}, \mathbf{T}, \mathbf{w}]^{(\delta+1)\times 2n} \end{aligned}$$

where here $\underline{\mathbf{m}}_i = (m_{i,2}, \dots, m_{i,m})$, which is the i-th row of $\mathbf{M}$ but without the first element (*i.e.,* $m_{i,1}$) and $\mathbf{T} = \{t_{i,j}\}_{i\in[\delta+1], j\in[m-1]}$ and

$$\mathbf{S} = \begin{pmatrix} \bar{\bar{s}}_0 & \bar{s}_{0,1} & \cdots & \bar{s}_{0,n} \\ \bar{\bar{s}}_1 & s_{1,1} & \cdots & s_{1,n} \\ \vdots & & & \\ \bar{\bar{s}}_\delta & s_{\delta,1} & \cdots & s_{\delta,n} \end{pmatrix}.$$

In explicit terms, we have $\mathbf{C} = \big(\mathbf{B}_1, \cdots, \mathbf{B}_n\big)$ where

$$\mathbf{B}_i := \begin{pmatrix} \mathbf{t}_1 \underline{\mathbf{m}}_i^\top - \bar{s}_{0,i}\bar{w}_0 + \bar{\bar{s}}_0 \bar{\bar{w}}_0 m_{i,1}, & \bar{s}_{0,i}(w_1\phi(i) + w_2) \\ \mathbf{t}_2 \underline{\mathbf{m}}_i^\top - s_{1,i}\bar{w}_0 + \bar{\bar{s}}_1 \bar{\bar{w}}_0 m_{i,1}, & s_{1,i}(w_1\phi(i) + w_2) \\ \vdots & \vdots \\ \mathbf{t}_{\delta+1} \underline{\mathbf{m}}_i^\top - s_{\delta,i}\bar{w}_0 + \bar{\bar{s}}_\delta \bar{\bar{w}}_0 m_{i,1}, & s_{\delta,i}(w_1\phi(i) + w_2) \end{pmatrix} \in \mathbb{Z}_p^{(\delta+1)\times 2}$$

where $\mathbf{t}_j := (t_{i,1}, \dots t_{i,m-1})$.

- $\mathsf{EncK}(S = \{a_1, \dots, a_z\}, n_1 = n + 1, \mathsf{aux}_k = \delta) \to m_3 = 1,\ \mathbf{L}, \mathbf{K}$ where

$$\begin{aligned} \mathbf{L} &= (1, \mathbf{0}) && \in \mathbb{Z}_p^{1\times(\delta+1)} \\ \mathbf{K} &= \mathbf{U}\mathbf{L} + \mathbf{S}^\top \widehat{\mathbf{K}} && \in \mathbb{Z}_p[\mathbf{S}, \mathbf{U}, \mathbf{w}]^{(n+1)\times(\delta+1)} \end{aligned}$$

where $\mathbf{U} = (u_1, \dots, u_{n+1})^\top$. In explicit terms, we have $\mathbf{K} = \begin{pmatrix} \mathbf{k}_0 \\ \mathbf{k}_1 \\ \vdots \\ \mathbf{k}_n \end{pmatrix}$ where

$$\begin{aligned} \mathbf{k}_0 := \Big(& u_1 - \bar{\bar{s}}_0 \bar{\bar{w}}_0, \bar{\bar{s}}_0 \bar{w}_0 + \bar{\bar{s}}_1(w_1 a_1 + w_2),\ \dots,\ \bar{\bar{s}}_0 \bar{w}_0 + \bar{\bar{s}}_z(w_1 a_z + w_2), \\ & \bar{\bar{s}}_0 \bar{w}_0 + \bar{\bar{s}}_{z+1} w_0,\ \dots,\ \bar{\bar{s}}_0 \bar{w}_0 + \bar{\bar{s}}_\delta w_0)\Big), \\ \mathbf{k}_i := \Big(& u_{i+1} - \bar{s}_{0,i} \bar{\bar{w}}_0,\ \bar{s}_{0,i} \bar{w}_0 + s_{1,i}(w_1 a_1 + w_2),\ \dots,\ \bar{s}_{0,i} \bar{w}_0 + s_{z,i}(w_1 a_z + w_2), \\ & \bar{s}_{0,i} \bar{w}_0 + s_{z+1,i} w_0,\ \dots,\ \bar{s}_{0,i} \bar{w}_0 + s_{\delta,i} w_0)\Big), \end{aligned}$$

for $i \in [n]$.

- $\mathsf{Pair}(x, y, \mathsf{aux}_k) \to \mathbf{E}', \overline{\mathbf{E}}' = \left(\begin{smallmatrix} 1 & \mathbf{0} \\ \mathbf{0}^\top & \mathbf{B} \end{smallmatrix}\right)$ described as follows. Let $\mathit{\Omega}$ be a set such that $\phi(i) = a_{j_i} \in S$ for $i \in \mathit{\Omega}$ and $(1, \mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i \in \mathit{\Omega}})$, and $\tau_1, \dots, \tau_n \in \mathbb{Z}_p$ be coefficients such that $\tau_i = 0$ for $i \notin \mathit{\Omega}$ and $\sum_{i \in [n]} \tau_i \mathbf{m}_i = (1, \mathbf{0})$. We set $\mathbf{E}' = \begin{pmatrix} \tau_1 \mathbf{E}_1 \\ \vdots \\ \tau_n \mathbf{E}_n \end{pmatrix}$ and $\mathbf{B} = (\tau_1 \overline{\mathbf{E}}_1 || \cdots || \tau_n \overline{\mathbf{E}}_n)$ where $\overline{\mathbf{E}}_i = (0, \dots, 0, 1, 0, \dots, 0)^\top \in \mathbb{Z}_p^{\delta \times 1}$ where 1 is at j_i-th row, and $\mathbf{E}_i = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & -1 & 0 & \cdots & 0 \end{smallmatrix}\right) \in \mathbb{Z}_p^{2 \times (\delta+1)}$, where -1 is at the $(j_i + 1)$-th column.

E.3 PES for Completely Unbounded NMSP Predicates

In this section, we describe a PES construction for sReg-ABE for completely unbounded ciphertext-policy non-monotone span programs, which we stated the result in Section 7.

PES for NIBE. We start with the predicate encoding $\mathit{\Gamma}^{\mathsf{NIBE}}$ for inequality or also called negated IBE predicate, $\mathsf{P}^{\mathsf{NIBE}}$. We have that $\mathsf{aux}_c = \mathsf{aux}_k = \varepsilon$ (the empty string) and

- $\mathsf{Param}(\kappa) \to 2$. Let $\mathbf{w} = (w_1, w_2)$.
- $\mathsf{CVEncC}(x) \to n_1 = 1, n_2 = 1,\ \widehat{\mathbf{F}} = (x, 1)^\top,\ \widehat{\mathbf{C}} = w_1 x + w_2$.
- $\mathsf{CVEncK}(y) \to m_1 = 1, m_2 = 2,\ \widehat{\mathbf{L}} = (y, 1)^\top,\ \widehat{\mathbf{K}} = (w_1, w_1 y + w_2)$.
- $\mathsf{EncC}(x, m_1) \to n_3 = 0,\ \mathbf{F} = 0,\ \mathbf{C} = s(w_1 x + w_2)$.
- $\mathsf{EncK}(y, n_1) \to m_3 = 1,\ \mathbf{L} = (1, 0),\ \mathbf{K} = (u + s w_1, s(w_1 y + w_2))$.
- $\mathsf{Pair}(x, y) \to \mathbf{E} = -\frac{1}{x-y},\ \overline{\mathbf{E}} = (1, \frac{1}{x-y})^\top$.

The correctness holds as $\mathsf{tr}(\mathbf{E}\mathbf{C}(\mathbf{S}, \mathbf{T}, \mathbf{w})) + \mathsf{tr}(\overline{\mathbf{E}}\mathbf{K}(\mathbf{S}, \mathbf{U}, \mathbf{w})) = (-\frac{1}{x-y}) s(w_1 x + w_2) + (1, \frac{1}{x-y})^\top (u + s w_1, s(w_1 y + w_2)) = u$, for $x \neq y$.

Lemma E.3. *The PES $\mathit{\Gamma}^{\mathsf{NIBE}}$ for $\mathsf{P}^{\mathsf{NIBE}}$ satisfies ciphertext and key well-formedness, and* $\mathsf{KE\text{-}ind}$.

Proof. The above PES is a secure predicate encoding in [Att19, Construction 9] for $\mathsf{P}^{\mathsf{NIBE}}$. Via Lemma 3.1, we obtain the corresponding PES for sReg-ABE which satisfies ciphertext and key well-formedness, and $\mathsf{KE\text{-}ind}$ for this predicate. □

PES for NIBE with Wild Card. We next obtain a PES $\mathit{\Gamma}^{\mathsf{NIBE+w}}$ for the predicate $\mathsf{WC}[\mathsf{P}^{\mathsf{NIBE}}]$ via the $\mathsf{WC\text{-}Trans}$ transformation to the PES for NIBE above. We have that $\mathsf{aux}_c = \mathsf{aux}_k = \varepsilon$ (the empty string)[15] and

[15] In the $\mathsf{WC\text{-}Trans}$ transformation, it is indeed the case that we define aux_k as follows (see the proof of Lemma C.3). For $Y' \subseteq \mathcal{Y}_\kappa \cup \{*\}$, set $\mathsf{aux}_k = y' \in \mathcal{Y}_\kappa$, where y' is a non-$*$ element (say, the first) in Y'. However, this y' element is only used to compute $\mathbf{L}$ in the case of a generic predicate. However, for the NIBE (with wild card) predicate here, we simply have $\mathbf{L} = (1, 0)$, and we can neglect aux_k completely.

- $\mathsf{Param}(\kappa) \to 2$. Let $\mathbf{w} = (w_1, w_2)$.
- $\mathsf{CVEncC}(x) \to n_1 = 1, n_2 = 1,\ \widehat{\mathbf{F}} = (x, 1)^\top,\ \widehat{\mathbf{C}} = w_1 x + w_2$.
- $\mathsf{CVEncK}(y) \to m_1 = 1, m_2 = 2,\ \widehat{\mathbf{L}} = (y, 1)^\top,\ \widehat{\mathbf{K}} = \begin{cases} (w_1, w_1 y + w_2) & \text{if } y \in \mathcal{Y}_\kappa \\ 0 & \text{if } y = * \end{cases}.$
- $\mathsf{EncC}(x, m_1) \to n_3 = 0,\ \mathbf{F} = 0,\ \mathbf{C} = s(w_1 x + w_2)$.
- $\mathsf{EncK}(y, n_1) \to m_3 = 1,\ \mathbf{L} = (1, 0),\ \mathbf{K} = \begin{cases} (u + s w_1, s(w_1 y + w_2)) & \text{if } y \in \mathcal{Y}_\kappa \\ u & \text{if } y = * \end{cases}.$
- $\mathsf{Pair}(x, y) \to \mathbf{E} = \begin{cases} -\frac{1}{x-y} & \text{if } y \in \mathcal{Y}_\kappa \\ 0 & \text{if } y = * \end{cases},\ \overline{\mathbf{E}} = \begin{cases} (1, \frac{1}{x-y})^\top & \text{if } y \in \mathcal{Y}_\kappa \\ (1, 0) & \text{if } y = * \end{cases}.$

PES for Key-Set Non-membership. We next obtain a PES Γ^{KSNM} for the key-set *non*-membership predicate $\mathsf{P}^{\mathsf{KSNM}}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0, 1\}$, where $\mathcal{Y}_\kappa = 2^{\mathcal{X}_\kappa}$, defined as $\mathsf{P}^{\mathsf{KSNM}}_\kappa(x, S) = 1 \Leftrightarrow x \notin S$. Note that this is exactly the negated predicate of the key-set membership predicate. It is straightforward to see that $\mathsf{P}^{\mathsf{KSNM}}$ can be embedded into the predicate $\mathsf{KP1}_{\mathsf{AND}}[\mathsf{WC}[\mathsf{P}^{\mathsf{NIBE}}]]$, with the same embedding as in the case of the key-set membership predicate. Note that $\mathsf{KP1}_{\mathsf{AND}}$ is the key policy conjunction as per Definition 4.4. Hence we can apply the $\mathsf{KP1}_{\mathsf{AND}}$-$\mathsf{Trans}$ to the PES $\Gamma^{\mathsf{NIBE+w}}$ above and obtain a new PES Γ^{KSM}. We will not write the PES explicitly here, as it is somewhat analogous to the key-set membership predicate. From Table 2, the obtained PES Γ^{KSNM} has parameters $\omega = 2$, $(n_1, n_2, n_3) = (1, 1, 0)$, $(m_1, m_2, m_3) = (\delta, 2\delta, \delta)$.

PES for Ciphertext-Set Non-membership (IBR). This predicate is defined as $\mathsf{P}^{\mathsf{CSNM}}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0, 1\}$, where $\mathcal{X}_\kappa = 2^{\mathcal{Y}_\kappa}$, defined as $\mathsf{P}^{\mathsf{CSNM}}_\kappa(S, y) = 1 \Leftrightarrow y \notin S$. It exactly defines the predicate for IBR (ID-based revocation). It is the dual of the key-set non-membership predicate; therefore, we obtain its PES Γ^{CSNM} by the Dual-Trans transformation to the PES Γ^{KSNM}. From Table 2, the obtained PES Γ^{CSNM} has parameters $\omega = 3$, $(n_1, n_2, n_3) = (\delta + 1, 2\delta, \delta - 1)$, $(m_1, m_2, m_3) = (1, 2, 1)$.

PES for Ciphertext-Set Two-mode-membership (TIBBE). Let $\mathcal{Y} = \mathbb{Z}_p$ be the base attribute domain. This predicate is defined as $\mathsf{P}^{\mathsf{CSTM}}_\kappa : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0, 1\}$, where $\bar{\mathcal{X}}_\kappa = 2^{\mathcal{Y}_\kappa}$ and $\bar{\mathcal{Y}}_\kappa = \{1, 2\} \times \mathcal{Y}_\kappa$, defined as

$$\mathsf{P}^{\mathsf{CSTM}}_\kappa(S, (i, y)) = 1 \qquad \Longleftrightarrow \qquad (i = 1 \wedge y \in S) \vee (i = 2 \wedge y \notin S).$$

This is also called two-mode IBBE (TIBBE) in [Att19, AT20]. In [Att19, AT20], a PES for vanilla ABE for this predicate is obtained by the *direct sum* composition of PES for IBBE and IBR. However, here, we do not have the direct sum composition in the case of PESs intended for sReg-ABE. We instead use the static predicate OR composition, namely, $\mathsf{SPC}_{\mathsf{OR}}$ (*cf.* Section 4.5) over IBBE (CSM) and IBR (CSNM), together with Null attributes in both key attribute domains. More precisely, we observe the following lemma. Via this lemma, we have a PES, denoted as Γ^{CSTM} for predicate $\mathsf{P}^{\mathsf{CSTM}}$.

Lemma E.4. $\mathsf{P}^{\mathsf{CSTM}}$ *can be embedded into* $\widetilde{\mathsf{P}} := \mathsf{Null}[\mathsf{P}^{\mathsf{CSM}}] \vee \mathsf{Null}[\mathsf{P}^{\mathsf{CSNM}}]$*, where the latter is the static predicate OR composition defined in Section 4.5.*

Proof. The considered predicate $\widetilde{\mathsf{P}} : \tilde{\mathcal{X}}_\kappa \times \tilde{\mathcal{Y}}_\kappa \to \{0, 1\}$ can be described explicitly as follows. We have $\tilde{\mathcal{X}}_\kappa = 2^{\mathcal{Y}_\kappa} \times 2^{\mathcal{Y}_\kappa}$ and $\tilde{\mathcal{Y}}_\kappa = \mathcal{Y}_\kappa \cup \{\mathsf{null}'\} \times \mathcal{Y}_\kappa \cup \{\mathsf{null}'\}$.[16]

$$\widetilde{\mathsf{P}}((S', S''), (y', y'')) = 1 \qquad \Leftrightarrow \qquad ((y' \in S') \wedge (y' \neq \mathsf{null}')) \vee ((y'' \notin S'') \wedge (y'' \neq \mathsf{null}'')).$$

We map $f_{\mathsf{c}} : \tilde{\mathcal{X}}_\kappa \to \bar{\mathcal{X}}_\kappa$ and $f_{\mathsf{k}} : \tilde{\mathcal{Y}}_\kappa \to \bar{\mathcal{Y}}_\kappa$ as:

$$f_{\mathsf{c}} : S \mapsto (S, S) \qquad\qquad \begin{aligned} f_{\mathsf{k}} : &(1, y) \mapsto (y, \mathsf{null}'') \\ &(2, y) \mapsto (\mathsf{null}', y) \end{aligned}$$

[16] Note that $\mathsf{P}^{\mathsf{CSM}}$ already contains the null attribute but in the ciphertext attribute domain[17]. In contrast, we add a new null attribute to the key attribute domain here. For unambiguity, we use two new different symbol $\mathsf{null}', \mathsf{null}''$.

It is then straightforward to see that $\mathsf{P}^{\mathsf{CSTM}}_{\kappa}(S,(i,y)) = 1 \Leftrightarrow \widetilde{\mathsf{P}}(f_{\mathsf{c}}(S), f_{\mathsf{k}}((i,y))) = 1$, and hence the lemma holds. □

From Table 2, the obtained PES Γ^{CSTM} has parameters $\omega = 9$, $(n_1,n_2,n_3) = (\delta+1, 3\delta, \delta-1)$, $(m_1,m_2,m_3) = (1,4,1)$.

PES for Key-Policy Non-monotone Span Programs. This predicate can be defined exactly as $\mathsf{P}^{\mathsf{KP-NMSP}} := \mathsf{KP1}[\mathsf{P}^{\mathsf{CSTM}}]$, where $\mathsf{KP1}$ is the KP augmentation defined as in Definition 4.7. Therefore, we can obtain a PES, denoted $\Gamma^{\mathsf{KP-NMSP}}$, for $\mathsf{P}^{\mathsf{KP-NMSP}}$ by applying the $\mathsf{KP1\text{-}Trans}$ to the PES Γ^{CSTM} for the $\mathsf{P}^{\mathsf{CSTM}}$ predicate. From Table 2, the obtained PES $\Gamma^{\mathsf{KP-NMSP}}$ has parameters $\omega = 9$, $(n_1,n_2,n_3) = (\delta+1, 3\delta, \delta-1)$, $(m_1,m_2,m_3) = (n, 4n, m)$, where $n \times m$ is the size of policy matrix.

PES for Ciphertext-Policy Non-monotone Span Programs. This predicate is defined exactly as $\mathsf{P}^{\mathsf{CP-NMSP}} := \mathsf{Dual}[\mathsf{P}^{\mathsf{KP-NMSP}}]$. Therefore, we can obtain a PES, denoted $\Gamma^{\mathsf{CP-NMSP}}$ for $\mathsf{P}^{\mathsf{CP-NMSP}}$ by applying the $\mathsf{Dual\text{-}Trans}$ to the PES $\Gamma^{\mathsf{KP-NMSP}}$ for the $\mathsf{P}^{\mathsf{KP-NMSP}}$ predicate. From Table 2, the obtained PES $\Gamma^{\mathsf{KP-NMSP}}$ has parameters $\omega = 10$, $(n_1,n_2,n_3) = (n+1, 4n, m-1)$, $(m_1,m_2,m_3) = (\delta+1, 3\delta+1, \delta)$, where $n \times m$ is the size of policy matrix.

E.4 PES for More Complex Non-monotone Span Programs

The non-monotone predicate in the previous subsection is a simple type called the OSW-type (for Ostrovsky-Sahai-Waters [OSW07]) as per [AT20]. There is also another type called Okamoto-Takashima (OT) [OT10]. A more general type that unifies these two types is called the OSWOT-type as per [AT20]. The definition is as follows. The intuition is that a single attribute set associated to a key as in CP-NMSP now becomes a set of pairs of id and attribute set. The id serves as label and the atomic policy returns 1 only if there is an attribute with the same label.

Definition E.2. The predicate of completely unbounded ciphertext-policy *general OSWOT-type non-monotone* span programs $\mathsf{P}^{\mathsf{CP-GNMSP}} : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$ for large attribute universe $\mathcal{X}_\kappa = \mathbb{Z}_p$ is defined as follows. Let

$$\bar{\mathcal{Y}}_\kappa = \{\, \{(id_1, S_1), \ldots, (id_t, S_t)\} \mid id_i \in \mathbb{Z}_p, S_i \subseteq \mathbb{Z}_p, t \in \mathbb{N}, \text{if } i \neq j \text{ then } \mathsf{id}_i \neq \mathsf{id}_j \,\}.$$

and $\bar{\mathcal{X}}_\kappa = \bigcup_{(n,m)\in\mathbb{N}^2} (\mathbb{Z}_p^{n\times m} \times \Phi_n)$, where Φ_n consists of all functions $\phi : [n] \to (\{\mathsf{pos}, \mathsf{neg}\} \times \mathbb{Z}_p \times \mathbb{Z}_p)$. For $\mathcal{S} = \{(id_1, S_1), \ldots, (id_t, S_t)\} \in \bar{\mathcal{Y}}_\kappa$ and $(\mathbf{M}, \phi) \in \bar{\mathcal{X}}_\kappa$ where $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$ and $\mathbf{m}_i$ is the i-th row of $\mathbf{M}$, we define

$$\begin{aligned}
\mathsf{P}^{\mathsf{CP-GNMSP}}_{\kappa}((\mathbf{M},\phi),\mathcal{S}) = 1 \Leftrightarrow & (1,\mathbf{0}) \in \mathsf{span}(\{\mathbf{m}_i\}_{i\in[n] \text{ s.t. } \mathsf{P}''(\phi,\mathcal{S})=1}),\\
\mathsf{P}''(\phi,\mathcal{S}) = 1 \Leftrightarrow & \Big(\phi_1(i) = \mathsf{pos} \wedge (\exists j : \phi_2(i) = id_j \wedge \phi_3(i) \in S_j)\Big) \vee \\
& \Big(\phi_1(i) = \mathsf{neg} \wedge (\exists j : \phi_2(i) = id_j \wedge \phi_3(i) \notin S_j)\Big),
\end{aligned}$$

where $\phi(i) = (\phi_1(i), \phi_2(i), \phi_3(i))$.

Lemma E.5. *There exists a PES for sReg-ABE for completely unbounded ciphertext-policy general OSWOT-type non-monotone span programs with large universe $\mathcal{U} = \mathbb{Z}_p$ which satisfies key well-formedness and* $\mathsf{KE\text{-}ind}$, *while achieving parameters $\omega = 15$, $(n_1,n_2,n_3) = (2n+1, 6n, m-1)$, and $(m_1,m_2,m_3) = (\delta_2(\delta_1+1)+1, \delta_2(3\delta_1+2)+1, \delta_2\delta_1+1)$, where $n \times m$ is the size of the policy matrix $\mathbf{M}$ of the ciphertext policy $(\mathbf{M},\phi)$ and if we let $\{\mathcal{S}_1, \ldots, \mathcal{S}_L\} \subseteq \bar{\mathcal{Y}}_\kappa$ be a set of registered key attributes, we denote δ_1 as the maximum size of set S_i's within any $\mathcal{S}_j$, and δ_2 as the maximum size of $|\mathcal{S}_j|$.*

Proof Sketch. A PES for this predicate can be constructed by our PES transformations by again following the idea of [AT20]. A main difference is that we do not have the direct sum transformation for PESs for sReg-ABE. However, this can be circumvented by using static AND and OR composition and appropriate uses of Null attributes similarly to our construction of Γ^{CSTM} for predicate $\mathsf{P}^{\mathsf{CSTM}}$. In fact, it is not difficult to see the following implications:

$$\begin{aligned}\mathsf{KP1}_{\mathsf{OR}}[\mathsf{Null}[\mathsf{SPC}_{\mathsf{AND}}[\,\mathsf{P}^{\mathsf{IBE}},\ \mathsf{P}^{\mathsf{KSTM}}\,]]] &\Rightarrow \mathsf{P}''',\\ \mathsf{Dual}[\mathsf{KP1}[\mathsf{Dual}[\mathsf{P}''']]] &\Rightarrow \mathsf{P}^{\mathsf{CP-GNMSP}}.\end{aligned}$$

where the intermediate $\mathsf{P}''' : (\{\mathsf{pos}, \mathsf{neg}\} \times \mathbb{Z}_p \times \mathbb{Z}_p) \times \bar{\mathcal{Y}}_\kappa$ is defined by:

$$\begin{aligned}\mathsf{P}'''((x_1, x_2, x_3), \mathcal{S}) = 1 \Leftrightarrow &\Big(x_1 = \mathsf{pos} \wedge (\exists j : x_2 = id_j \wedge x_3 \in S_j)\Big) \vee \\ &\Big(x_1 = \mathsf{neg} \wedge (\exists j : x_2 = id_j \wedge x_3 \notin S_j)\Big).\end{aligned}$$

The intuition is that we use static AND composition to combine the IBE and the key-set two-mode-membership predicate (KSTM) to use as the check for the equality of id and that the (two-mode) set membership holds. Note that $\mathsf{P}^{\mathsf{KSTM}}$ can be constructed as the dual of $\mathsf{P}^{\mathsf{CSTM}}$. To enable the $\exists j$ quantifier (in the definition of $\mathsf{P}^{\mathsf{CP-GNMSP}}$), we then use key-policy disjunction together with null attributes analogously to *e.g.,* when constructing PES for $\mathsf{P}^{\mathsf{KSM}}$. The second line of the implication holds by definition of $\mathsf{P}^{\mathsf{CP-GNMSP}}$. The parameter sizes can be deduced by following the implication sequence and referring to Table 2. This concludes the proof. □