Unbounded Dynamic Predicate Compositions in ABE from Standard Assumptions

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

Abstract. At Eurocrypt'19, Attrapadung presented several transformations that dynamically compose a set of attribute-based encryption (ABE) schemes for simpler predicates into a new ABE scheme for more expressive predicates. Due to the powerful unbounded and modular nature of his compositions, many new ABE schemes can be obtained in a systematic manner. However, his approach heavily relies on q-type assumptions, which are not standard. Devising such powerful compositions from standard assumptions was left as an important open problem. In this paper, we present a new framework for constructing ABE schemes that allow unbounded and dynamic predicate compositions among them, and show that the adaptive security of these composed ABE will be preserved by relying only on the standard matrix Diffie-Hellman (MDDH) assumption. This thus resolves the open problem posed by Attrapadung. As for applications, we obtain various ABEs that are the first such instantiations of their kinds from standard assumptions. These include the following adaptively secure *large-universe* ABEs for Boolean formulae under MDDH:

- The first completely unbounded monotone key-policy (KP)/ ciphertext-policy (CP) ABE. Such ABE was recently proposed, but only for the KP and *small-universe* flavor (Kowalczyk and Wee, Eurocrypt'19).
- The first completely unbounded non-monotone KP/CP-ABE. Especially, our ABEs support a new type of non-monotonicity that subsumes previous two types of non-monotonicity, namely, by Ostrovsky *et al.* (CCS'07) and by Okamoto and Takashima (CRYPTO'10).
- The first (non-monotone) KP and CP-ABE with constant-size ciphertexts and secret keys, respectively.
- The first KP and CP-ABE with constant-size secret keys and ciphertexts, respectively.

At the core of our framework lies a new *partially symmetric* design of the core 1-key 1-ciphertext oracle component called Key Encoding Indistinguishability, which exploits the symmetry so as to obtain compositions.

S. Moriai and H. Wang (Eds.): ASIACRYPT 2020, LNCS 12493, pp. 405–436, 2020.
https://doi.org/10.1007/978-3-030-64840-4_14

Keywords: Attribute-based encryption · Predicate compositions · k-Lin · Completely unbounded ABE · Non-monotone ABE · Succinct ABE · Boolean formula

1 Introduction

Attribute-based encryption (ABE) is a generalized form of public-key encryption that allows fine-grained access control over encrypted data [24,33]. In a broader sense of ABE, each scheme specifies a predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, where $\mathcal{X}$ and $\mathcal{Y}$ are ciphertext and secret-key attribute universes, respectively. All users can encrypt a message with an arbitrary attribute $x \in \mathcal{X}$. An owner of a master secret key can generate a secret key for an arbitrary attribute $y \in \mathcal{Y}$. A ciphertext for attribute x is decryptable with a secret key for attribute y if and only if x and y satisfy the predicate P, i.e., $\mathsf{P}(x,y) = 1$. This is in contrast to the traditional public-key encryption, in which only one legitimate user can decrypt a ciphertext.

One of central research topics in ABE is to explore what kind of predicates for which ABE can be realized. This is important in practice since if one attempts to realize an access control system based on ABE, the underlying predicate must be able to express all decryption conditions that appear in the system. A line of works has shown that we can realize ABE for various predicates: ABE for span programs, (non-)deterministic finite automata, polynomial-sized circuits, and so on [4,14,23–25,31,33,37]. These works directly construct ABE schemes for targeting predicates. In contrast, there is also another approach to construct ABE schemes for more expressive new predicates by transformations and combinations of known predicates [6,7,9,13]. The state of the art on this approach is the work by Attrapadung [9], who proposed a framework for dynamic predicate compositions and introduced new ABE schemes such as ABE for key-policy (KP)/ciphertext-policy (CP) augmentation over predicate sets, nested-policy ABE, and mixed-policy ABE. The salient feature of these ABE schemes is that they allow *unbounded* and *dynamic* predicate compositions, that is, they do not impose any restriction on the size and structure of composition policy. This is in contrast to previous works [6,7,13], which allow only *static* (*i.e.,* a-priori fixed) compositions. He also showed that his framework captures predicates that are known but whose adaptively secure ABE instance was still open such as the predicate for completely unbounded non-monotone ABE.

The framework of [9] modularly constructs new predicates with corresponding pair encoding schemes (PES), which are encoding systems that yield concise expressions of ABE schemes [7]. It is shown in [9] that a nested application of three transformations of predicates, namely, direct sum, dual transformation, and KP augmentation over a single predicate (we call it just KP augmentation in what follows), is sufficiently powerful to obtain expressive predicates, such as the predicates for KP/CP augmentation over predicate sets, nested-policy ABE, and completely unbounded non-monotone ABE. He also demonstrates the transformations of PESs that correspond to the three transformations of the predicates. Hence, starting from known predicates and corresponding PESs, one can obtain

Table 1. Comparison among frameworks that compose multiple predicates over ABE.

Framework	Composition type	Comp. class	Input primitive	Assumption
ABS17 [6]	Static	Boolean formulae	Predicate encodings (info.-theoretic)	MDDH
Att19 [9]	Unbounded, Dynamic	SP, BP, DFA	Pair encodings with symbolic security	q-ratio
This work	Unbounded, Dynamic	Boolean formulae	Pair encodings with info.-theoretic security or with Key-Encoding Indistinguishability	MDDH

Note: SP, BP, DFA stand for span programs, branching programs, deterministic, finite automata, respectively.

a new transformed predicate along with its PES. Additionally, all PESs obtained in his framework can be used to instantiate a secure ABE scheme.

A crucial fact that his framework relies on is that the transformations of PESs preserve the symbolic property, introduced by Agrawal and Chase [3]. That is, he proved that all transformed PESs in his framework satisfy the symbolic property if the starting PESs satisfy the symbolic property. Agrawal and Chase showed that an ABE scheme induced by a PES with the symbolic property is adaptively secure under the q-ratio assumption [3]. Thus, we can use known predicates that have a PES with the symbolic property to construct a new expressive predicate and the corresponding PES, which results in a secure ABE scheme.

One drawback of his framework is the necessity of the q-ratio assumption, which is one of so-called q-type assumptions. The q-ratio assumption is parametrized with two parameters d_1 and d_2 and becomes stronger as they grow. We require that the q-ratio assumption holds with respect to sufficiently large d_1 and d_2 to assure the security of most ABE schemes because these parameters depend on adversary's behavior. However, the q-ratio assumption is a new complex assumption and thus not well-understood. Hence, it is desirable if we can transform PESs and instantiate an ABE scheme from a transformed PES under well-understood standard assumptions like the matrix Diffie-Hellman assumption (which includes k-Lin as a special case), instead of q-type assumptions. The realization of such a framework yields many important new ABEs from standard assumptions but has been left as an open problem by Attrapadung [9].

1.1 Our Contributions

New Framework. We give an affirmative answer to the problem and present a new framework for transforming predicates and constructing ABE schemes on prime-order bilinear groups, which relies on only the standard matrix Diffie-Hellman (MDDH) assumption. Following [9], our framework also composes a new predicate by combining three essential transformations, namely, the direct sum, dual transformation, and KP augmentation. Nested applications of these transformations yield various expressive predicates and ABE schemes. Our framework introduces a new property on PESs that satisfies the two requirements under the

Table 2. Comparison among *unbounded* ABE schemes.

References	Large universe	Adaptive security	Multi-use	Static assumption	Without RO	Non-monotonicity	Prime-order	KP/CP
LW11 [27]	✓		✓	✓	✓			KP
OT12 [30]	✓	✓		✓	✓	✓(OT)	✓	KP, CP
RW13 [32]	✓		✓		✓		✓	KP, CP
YAHK14 [39]	✓		✓		✓	✓(OSW)	✓	KP, CP
Att14 [7]	✓	✓	✓		✓			KP
AY15 [13]	✓	✓	✓		✓			CP
Att16 [8]	✓	✓	✓		✓		✓	KP, CP
AC17a [3]	✓	✓	✓		✓		✓	KP, CP
AC17b [2]	✓	✓		✓			✓	KP, CP
CGKW18 [16]		✓		✓	✓		✓	KP, CP
KW19 [26]		✓	✓	✓	✓		✓	KP
Att19 [9]	✓	✓	✓		✓	✓(OSW)	✓	KP, CP
TKN19 [35]	✓	✓	✓	✓		✓(OT)	✓	KP, CP
Ours 1	✓	✓	✓	✓	✓		✓	KP, CP
Ours 2	✓	✓	✓	✓	✓	✓(OSWOT)	✓	KP, CP

Note: KP, CP is for key-policy, ciphertext-policy. RO is for random oracles. We consider three types of non-monotone ABE: OT-type (Okamoto-Takashima [30]), OSW-type (Ostrovsky-Sahai-Waters [31]), and a new unified type (OSWOT) (see Sect. 6).

MDDH assumption: the preservation of the property in the transformations and the induction of the adaptive security of the resulting ABE scheme.

Note that there are two differences between our framework and that by Attrapadung [9] (we provide a comparison among composition frameworks in Table 1). First, our KP augmentation is done with Boolean formulae, whereas that by Attrapadung is augmentation with span programs, branching programs, and deterministic finite automata (realizing them from standard assumptions is an interesting open problem). Second, starting predicates need to have a PES with a certain information-theoretic property, whereas those in his framework only require a PES with the symbolic property. Note that the latter may be attainable by larger classes of predicates (but the symbolic property would require q-type assumptions). Nevertheless, our framework is still sufficiently powerful to realize many ABE schemes of which instantiations under the standard assumptions have remained open before our work.

New Instantiations. Via our new framework, we obtain the following ABE instantiations for important specific predicates. We emphasize that all the instantiations are *large-universe* constructions, which have a super-poly size attribute domain. Their comparisons to previous schemes are given in Tables 2, 3, 4 and 5.

1. The first adaptively secure completely unbounded KP/CP-ABE for monotone Boolean formulae under MDDH.[1] Previously, such an adaptively secure

[1] To be more precise, we describe some terms. *Unbounded ABE* [27] refers to schemes that have no bounds on the sizes of attribute sets (inputs to a Boolean formula) and policies (Boolean formulae). *Multi-use* refers to the property that any attribute can be used arbitrarily many times in one policy. *Completely unbounded ABE* refers to unbounded *large-universe* ABE with multi-use (see *e.g.,* [9]).

Table 3. Closer comparison among *adaptively secure unbounded* ABE with *multi-use* in the standard model.

References	KP/CP	Large univ.	Static assump.	Non-monoton.	$\|\mathsf{pk}\|$	$\|\mathsf{ct}\|$	$\|\mathsf{sk}\|$
Att14 [7], Att16 [8], AC17a [3]	KP	✓			$O(1)$	$O(t)$	$O(n)$
KW19 [26]	KP		✓		$O(1)$	$O(t)$	$O(n)$
Att19 [9]	KP	✓		✓(OSW)	$O(1)$	$O(t)$	$O(n)$
Ours 1	KP	✓	✓		$O(1)$	$O(t)$	$O(n)$
Ours 2	KP	✓	✓	✓(OSWOT)	$O(1)$	$O(t)$	$O(n)$
AY15 [13], Att16 [8], AC17a [3]	CP	✓			$O(1)$	$O(n)$	$O(t)$
Att19 [9]	CP	✓		✓(OSW)	$O(1)$	$O(n)$	$O(t)$
Ours 1	CP	✓	✓		$O(1)$	$O(n)$	$O(t)$
Ours 2	CP	✓	✓	✓(OSWOT)	$O(1)$	$O(n)$	$O(t)$

Table 4. Comparison among ABE with *constant-size ciphertexts* ($|\mathsf{ct}| = O(1)$).

References	KP/CP	Large univ.	Adapt. security	Static assumptn.	Non-monoton.	Prime-order	$\|\mathsf{pk}\|$	$\|\mathsf{sk}\|$
ALP11 [11]	KP	✓			✓(OSW)	✓	$O(T)$	$O(Tn)$
Att14 [7]	KP	✓	✓				$O(T)$	$O(Tn)$
CW14 [17]	KP			✓			$O(T)$	$O(Tn)$
Tak14 [34]	KP	✓		✓	✓(OSW)	✓	$O(T)$	$O(Tn)$
Att16 [8]	KP	✓	✓			✓	$O(T)$	$O(Tn)$
AC17a [3]	KP	✓	✓			✓	$O(T)$	$O(Tn)$
Att19 [9]	KP	✓	✓		✓(OSW)	✓	$O(T^2)$	$O(T^3n)$
Ours 3	KP	✓	✓	✓	✓(OSW)	✓	$O(T)$	$O(Tn)$
AHY15 [10]	CP	✓	✓		✓(OSW)	✓	$O((TN)^2\lambda)$	$O((TN)^4\lambda^2)$
AC16 [1]	CP			✓		✓	$O(N(T+M))$	$O(N^2T+NM)$
Att19 [9]	CP	✓	✓		✓(OSW)	✓	$O(N^2+NM)$	$O(t(N^3+N^2M))$
Ours 5	CP	✓	✓	✓		✓	$\tilde{O}((M+T\lambda)^2)$	$\tilde{O}((M+T\lambda)^4)$

Table 5. Comparison among ABE with *constant-size keys* ($|\mathsf{sk}| = O(1)$).

References	KP/CP	Large univ.	Adapt. security	Static assumptn.	Non-monoton.	Prime-order	$\|\mathsf{pk}\|$	$\|\mathsf{ct}\|$
AY15 [13]	CP	✓	✓				$O(T)$	$O(Tn)$
Att16 [8]	CP	✓	✓			✓	$O(T)$	$O(Tn)$
AC17a [3]	CP	✓	✓			✓	$O(T)$	$O(Tn)$
Att19 [9]	CP	✓	✓		✓(OSW)	✓	$O(T^2)$	$O(T^3n)$
Ours 4	CP	✓	✓	✓	✓(OSW)	✓	$O(T)$	$O(Tn)$
AHY15 [10]	KP	✓	✓		✓(OSW)	✓	$O((TN)^2\lambda)$	$O((TN)^4\lambda^2)$
Att19 [9]	KP	✓	✓		✓(OSW)	✓	$O(N^2+NM)$	$O(t(N^3+N^2M))$
Ours 6	KP	✓	✓	✓		✓	$\tilde{O}((M+T\lambda)^2)$	$\tilde{O}((M+T\lambda)^4)$

Notes for Table 3, 4 and 5: we denote $t = |\text{attribute set}|$, n is the input length of a Boolean formula, while T, N are the maximum bound for t, n, respectively (if required). M is the maximum bound for the size of Boolean formulae (if required). λ is the security parameter, *i.e.,* $\lambda = \lceil \log p \rceil$.

KP/CP-ABE relies on either q-type assumptions [3,8,9] or the one-use restriction (each attribute is usable at most once in a policy) [16,30]. Note that the recent unbounded KP-ABE with multi-use by Kowalczyk and Wee [26, Sect. A] is a *small-universe* construction, i.e., the attribute domain size is (a priori unbounded) polynomial.

2. The first adaptively secure completely unbounded KP/CP-ABE for *non-monotone* Boolean formulae under MDDH. Furthermore, our ABE schemes support a new type of non-monotonicity that conflates the two types of existing non-monotonicity by Ostrovsky, Sahai, and Waters (OSW) [31] and by Okamoto and Takashima (OT) [29]. In other words, both OSW-non-monotone ABE and OT-non-monotone ABE can be captured as a special case of our non-monotone ABE. Previously, an adaptively secure unbounded ABE for non-monotone formulae is either the OSW-type and based on q-type assumption [9] or the OT-type with the one-use restriction [30].
3. The first adaptively secure KP/CP-ABE with constant-size ciphertexts/secret keys under MDDH for (OSW-non-)monotone Boolean formulae, respectively.
4. The first (adaptively secure) KP/CP-ABE with constant-size secret keys/ciphertexts under MDDH for monotone Boolean formulae, respectively.

Note that almost all previous ABE with constant-size ciphertexts or keys rely on q-type assumptions [1,3,7–10,13], even when considering only selective security. There are only two exceptions: KP-ABE with constant-size ciphertexts of [17,34], but these only achieves semi-adaptive security.

Discussions. We clarify that our framework allows us to construct ABEs that are hard to obtain even if given the recent groundbreaking work by Kowalczyk and Wee (KW), who solved the multi-use problem in the adaptive setting and also presented an unbounded KP-ABE scheme with multi-use [26]. Most notably, we can construct completely unbounded OSW-non-monotone KP/CP-ABEs via our framework in a systematic manner (our newly defined non-monotone ABE subsumes OSW-non-monotone ABE). Prior to our work, there are no unbounded OSW-non-monotone ABE schemes based on static assumptions *even with the one-use restriction* (Table 2). This means that the KW technique, which is useful for the multi-use problem, does not directly help to realize unbounded OSW-non-monotone ABE.

We next highlight that our ABE for the newly defined non-monotonicity is practically meaningful, besides providing a theoretical interest. Intuitively, it allows a ciphertext to be assigned with multiple attribute sets each with a "tag". This, in turns, allows flexible blacklisting access controls in dynamic systems where new attributes can be added on into the system *after deployment*. We will describe it in Sect. 6 (with more details and formal definitions in the full version). We remark that, in small universe ABE, we can use monotone ABE as non-monotone ABE by preparing both positive and negative attributes [31]. However, this is not the case in large-universe ABE since we cannot attach an exponentially large number of negative attributes to ciphertexts or secret keys. Hence, for large-universe ABE, non-monotone variant is essentially more difficult to obtain.

From these, we believe that it is challenging and important to devise a modular framework that allows us to construct such ABEs from standard assumptions.

1.2 Technical Overview of Our Framework

We first recall the three main basic predicate transformations/compositions similarly to [9], namely, the *Dual*, the *KP augmentation*, and the *Direct sum*. For a predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, we define the first two, $\mathsf{Dual}[\mathsf{P}]$, $\mathsf{KP1}[\mathsf{P}]$, as[2]

$$\mathsf{Dual}[\mathsf{P}]\,(y,x) = \mathsf{P}(x,y)$$
$$\mathsf{KP1}[\mathsf{P}]\,\Big(x,\ Y = \big((y_1,\ldots,y_n),f\big)\Big) = f\big(\mathsf{P}(x,y_1),\ldots,\mathsf{P}(x,y_n)\big).$$

We remark two things: a composition policy $f : \{0,1\}^n \to \{0,1\}$ is a part of the key attribute Y; the "1" in $\mathsf{KP1}$ refers to the *single* predicate P and a *single* ciphertext attribute x. Next, for a set of predicates $\mathcal{P} = \{\mathsf{P}_1,\ldots,\mathsf{P}_k\}$, we define its direct sum $\mathsf{DS}[\mathcal{P}]$ as follows. Here i,j specifies predicate $\mathsf{P}_i,\mathsf{P}_j$, respectively.

$$\mathsf{DS}[\mathcal{P}]\,\big((i,x),\ (j,y)\big) = 1 \quad \text{iff} \quad i = j \wedge \mathsf{P}_i(x,y) = 1.$$

It is shown in [9] that the three transforms imply the "full" KP augmentation over *predicate sets*, denoted $\mathsf{KP}[\mathcal{P}]$ (notice the absent of "1"), defined as follows. For a set $X = \{(i_1,x_1),\ldots,(i_t,x_t)\}$ and vector $Y = ((j_1,y_1),\ldots,(j_n,y_n),f)$, let

$$\mathsf{KP}[\mathcal{P}]\,\big(X,\,Y\big) = f(b_1,\ldots,b_n) \quad \text{where} \quad b_v = 1 \text{ iff } \exists_{i_u=j_v} : \mathsf{P}_{j_v}(x_u,y_v) = 1$$

It is this full composition that we quantify the static vs dynamic, bounded vs unbounded features: it is *static* if f is fixed (and hence so does n), otherwise it is *dynamic* over the class of f; it is *unbounded* when n is unbounded.

We briefly explain its direct applications. Setting $\mathcal{P}' = \{\mathsf{E}\}$, where E is the equality predicate (IBE), we obtain the completely unbounded KP-ABE for monotone policies, that is, ABE for $\mathsf{KP}[\mathcal{P}']$ implies Ours 1 in Table 2. Similarly, setting $\mathcal{P}'' = \{\mathsf{E},\bar{\mathsf{E}}\}$, where $\bar{\mathsf{E}}$ is the negation of E, basically yields that for non-monotone policies (see other precise ways to define its variants in the full version).

As motivated in [9], the seemingly unrelated Dual indeed plays a crucial role in bootstrapping $\mathsf{KP1}$ to KP (*i.e.,* even when considering bootstrapping over *sole* key-policy flavors, and not considering *across* dual flavors, namely ciphertext-policy). Intuitively, this is since the full KP "intrinsically" contains a *ciphertext-policy* predicate as given by $\mathsf{Dual}[\mathsf{KP1}[\mathsf{P}]]\,\big(X' = \big((x_1,\ldots,x_t),f_{\mathsf{OR}}\big),\ y\big)$, where X' with the OR policy here is another way to express the set X in KP. "Nesting" $\mathsf{KP1}$ and $\mathsf{Dual} \circ \mathsf{KP1}$ together then yields KP (*cf.* [9]). Note also that the direct sum is used to "glue" predicates in $\mathcal{P}$ to single predicate; it is not needed for the case of a singleton $\mathcal{P}$ (such as $\mathcal{P}'$ above). Now that KP is reduced to the much simpler $\mathsf{KP1}$, Dual (and DS), we will deal with these basic transforms.

Background on PES. We now briefly recall PES [7], as refined in [3]. Informally, a PES for $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ is represented by a variable α, five vectors of variables $(\mathbf{w},\mathbf{s},\hat{\mathbf{s}},\mathbf{r},\hat{\mathbf{r}})$, and two sets of polynomials (called ciphertext and key

[2] For simplicity, we omit writing their domains here. See formal treatments in Sect. 4.

encodings, resp.) on these variables $(\mathbf{c}_x(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}), \mathbf{k}_y(\alpha, \mathbf{r}, \hat{\mathbf{r}}, \mathbf{w}))$ that depend on $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively. We require that $\mathbf{s}$ contains a variable s_0. Let $N = p_1 p_2$ for primes p_1, p_2, and $e : G \times H \to G_{\mathsf{T}}$ be bilinear groups of order N. Let g_i, h_i be generators of the subgroups G_i, H_i of order p_i for $i \in \{1, 2\}$, respectively, and $g = g_1 g_2, h = h_1 h_2$. Then, an ABE scheme in composite-order groups based on PES can be described as follows: $\mathsf{pk} = (g_1^{\mathbf{w}}, e(g_1, h)^{\alpha})$ and

$$\mathsf{ct}_x = (g_1^{\mathbf{s}}, g_1^{\mathbf{c}_x(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})}, e(g_1, h)^{s_0 \alpha} m), \qquad \mathsf{sk}_y = (h_1^{\mathbf{r}}, h_1^{\mathbf{k}_y(\alpha, \mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})} h_2^{\mathbf{k}_y(\alpha, \mathbf{0}, \hat{\mathbf{r}}, \mathbf{0})}),$$

where $(\alpha, \mathbf{w}, \mathbf{s}, \hat{\mathbf{s}}, \mathbf{r}, \hat{\mathbf{r}}) \leftarrow \mathbb{Z}_N^t$ (t is the total number of the variables). We require that each polynomial of $\mathbf{c}_x$ is a linear combination of monomials $s_i w_j$ and $\hat{s}_k$ (where $s_i \in \mathbf{s}$, $\hat{s}_k \in \hat{\mathbf{s}}$, $w_j \in \mathbf{w}$). This yields the linearity of $\mathbf{c}_x$ over $\mathbf{s}, \hat{\mathbf{s}}$, when fixing $\mathbf{w}$. Analogous properties go for key encodings. As an example, a PES for IBE [7] has the form $\mathbf{c}_x = s_0(w_1 x + w_2)$, $\mathbf{k}_y = \alpha + r_1(w_1 y + w_2)$, where $\mathbf{w} = (w_1, w_2)$, $\mathbf{s} = s_0$, $\mathbf{r} = r_1$ (and no $\hat{\mathbf{s}}, \hat{\mathbf{r}}$). In what follows in this section, we write $\mathbf{c}_x(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})$ and $\mathbf{k}_y(\alpha, \mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})$ to implicitly include $\mathbf{s}$ and $\mathbf{r}$, respectively.

Our Goal: Three Main Implications. Since the symbolic property works only with the q-ratio assumption, we need a completely different new notion on PES that is preserved via the transformations, and that, at the same time, implies the adaptive security of the induced ABE scheme under standard assumptions. To this end, in this work, we introduce a new central notion called Key-Encoding Indistinguishability for PES, denoted KE-ind. Our goal is to design KE-ind in such a way that the following theorems (stated informally below) hold. The first states the preservation of KE-ind under the transformation. The second states that KE-ind implies adaptively secure ABE under MDDH.

Informal Theorem 1. *For a composition* $\mathsf{C} \in \{\mathsf{Dual}, \mathsf{DS}, \mathsf{KP1}\}$*, if there exists a PES for* P *that satisfies* KE-ind*, then there exists a PES for* $\mathsf{C}[\mathsf{P}]$ *that satisfies* KE-ind *under MDDH. (Note that for* DS*, its input is a predicate set* $\mathcal{P}$*.)*

Informal Theorem 2. *If there exists a PES for* P *that satisfies* KE-ind*, then there exists an adaptively secure ABE scheme for* P *under MDDH.*

The third theorem finally tells us how to achieve KE-ind via the existing information-theoretic notion of PES called perfect master-key hiding (PMH) of PES as defined in [7]. PMH requires that the following two distributions are identical with respect to $(\alpha, \mathbf{w}, \mathbf{s}, \hat{\mathbf{s}}, \mathbf{r}, \hat{\mathbf{r}}) \leftarrow \mathbb{Z}_N^t$:

$$\{\mathbf{c}_x(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}), \mathbf{k}_y(\alpha, \mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})\} \text{ and } \{\mathbf{c}_x(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}), \mathbf{k}_y(0, \mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})\}. \tag{1}$$

Informal Theorem 3. *If a PES satisfies the PMH property, then the same PES also satisfies* KE-ind *under MDDH.*

From these theorems, we have the following corollary.

Informal Corollary 1. *If there exists a PES for* P *satisfying the PMH, then there exists an adaptively secure ABE for the composed predicate* $\mathsf{C}_1 \circ \cdots \circ \mathsf{C}_n[\mathsf{P}]$ *under MDDH, where* $\mathsf{C}_i \in \{\mathsf{Dual}, \mathsf{DS}, \mathsf{KP1}\}$*. (For* DS *inputs are sets.)*

We can start from such information-theoretic PESs for basic predicates in [6,7], such as IBE, and obtain adaptively secure ABE for composed predicates.

To obtain these theorems, it remains to properly design $\mathsf{KE\text{-}ind}$.

Designing Key-Encoding Indistinguishability. For simplicity, we explain our framework in composite-order bilinear groups in this overview since we can basically convert ABE constructions in composite-order groups into those in prime-order groups via the framework by Chen *et al.* [15,16,20]. Note that the MDDH assumption in prime-order groups corresponds to the subgroup (SG) assumptions in composite-order groups (see e.g., [16]).

Our starting point is to define $\mathsf{KE\text{-}ind}$ to be exactly the *computationally master-key hiding* (CMH) property [7], which is a relaxed notion of PMH (and we would obtain Theorem 3 above). We say that a PES Γ specified by $(\alpha, \mathbf{w}, \mathbf{s}, \hat{\mathbf{s}}, \mathbf{r}, \hat{\mathbf{r}}, \mathbf{c}_x, \mathbf{k}_y)$ for P satisfies CMH if the following advantage of $\mathcal{A}$ is negligible:

$$\mathsf{Adv}^{\mathsf{CMH}}_{\mathcal{A},\Gamma}(\lambda) = \left| \Pr\left[\beta = \beta' \middle| \begin{array}{l} \beta \leftarrow \{0,1\} \\ \beta' \leftarrow \mathcal{A}^{\mathsf{cO}(\cdot),\mathsf{kO}_\beta(\cdot)}(g_1, g_2, h_1, h_2) \end{array} \right] - \frac{1}{2} \right|,$$

where the ciphertext encoding oracle cO takes $x \in \mathcal{X}$ and outputs $g_2^{\mathbf{c}_x(\mathbf{s},\hat{\mathbf{s}},\mathbf{w})}$, while the key encoding oracle kO_β takes $y \in \mathcal{Y}$ and outputs $h_2^{\mathbf{k}_y(\beta\alpha,\mathbf{r},\hat{\mathbf{r}},\mathbf{w})}$, where $\alpha, \mathbf{w}, \mathbf{s}, \hat{\mathbf{s}}, \mathbf{r}, \hat{\mathbf{r}}$ are random. Here $\mathcal{A}$ can query each oracle once with $R(x,y) = 0$. Attrapadung showed that if we have a PES for P with CMH, then we can obtain an adaptively secure ABE scheme for P assuming the SG assumption [7] (this implies Theorem 2). Thus, if we could show that CMH is preserved via the transformations black(this would imply Theorem 1), we would achieve the goal.

Unfortunately, we quickly found out that this approach fails; in particular, we do not know how to preserve CMH via the $\mathsf{KP1}$ transformation. Assume that we use the same $\mathsf{KP1}$ transformation as in [9], which transforms a PES Γ for P to a PES Γ' for $\mathsf{KP1}[\mathsf{P}]$ to be exactly the same as Γ except that

$$\mathbf{k}'_Y(\alpha, \mathbf{r}', \hat{\mathbf{r}}', \mathbf{w}) = \{\mathbf{k}_{y_i}(\sigma_i, \mathbf{r}_i, \hat{\mathbf{r}}_i, \mathbf{w})\}_{i\in[n]}$$

and $\mathbf{r}' = \{\mathbf{r}_i\}_{i\in[n]}$, $\hat{\mathbf{r}}' = \{\hat{\mathbf{r}}_i\}_{i\in[n]}$, where $\{\sigma_i\}_{i\in[n]}$ are secret shares of α with respect to f. (Here, primed variables are for Γ'.) Our goal here is to construct a reduction that breaks CMH of Γ internally using an adversary that breaks CMH of Γ'. One hopeful strategy is to limit f to Boolean formulae and consider a series of hybrids as the KW framework [26]. However, this idea does not work as the reduction cannot simulate $\{h_2^{\mathbf{k}_{y_i}(\sigma_i,\mathbf{r}_i,\hat{\mathbf{r}}_i,\mathbf{w})}\}_{i\neq j}$ when randomizing $h_2^{\mathbf{k}_{y_j}(\sigma_j,\mathbf{r}_j,\hat{\mathbf{r}}_j,\mathbf{w})}$ due to the absence of $h_2^{\mathbf{w}}$. Including $h_2^{\mathbf{w}}$ in the input of the CMH adversary does not solve the problem since this makes PMH not imply CMH, and Theorem 3 does not hold in such a definition (observe that in Eq. (1), $\mathbf{w}$ is not given out). Our next observation here is that we will need a property on indistinguishability of H_2 elements where the output of kO_β is simulatable *without* $h_2^{\mathbf{w}}$.

First Step: Subgroups vs Entire Groups. Our first idea is to make the outputs of cO and kO_β use *entire* groups G, H instead of only *subgroups* G_2, H_2,

which can be seen as an extension of the technique by Tomida *et al.* [35]. A new candidate property (say, Cand1) for Γ is then defined as follows:

$$\mathsf{Adv}^{\mathsf{Cand1}}_{\mathcal{A},\Gamma}(\lambda) = \left| \Pr\left[\beta = \beta' \middle| \begin{array}{l} \beta \leftarrow \{0,1\},\ \mathbf{w} \leftarrow \mathbb{Z}_N^{\omega} \\ \beta' \leftarrow \mathcal{A}^{\mathsf{cO}(\cdot),\mathsf{kO}_\beta(\cdot)}(g_1, h_1, h_2, g_1^{\mathbf{w}}, h_1^{\mathbf{w}}) \end{array} \right] - \frac{1}{2} \right|,$$

where $g^{\mathbf{c}_x(\mathbf{s},\hat{\mathbf{s}},\mathbf{w})} \leftarrow \mathsf{cO}(x)$ and $h_1^{\mathbf{k}_y(0,\mathbf{r},\hat{\mathbf{r}},\mathbf{w})} h_2^{\mathbf{k}_y(\beta\alpha,\mathbf{0},\hat{\mathbf{r}},\mathbf{0})} \leftarrow \mathsf{kO}_\beta(y)$ where $\alpha, \mathbf{s}, \hat{\mathbf{s}}, \mathbf{r}, \hat{\mathbf{r}}$ are random. Crucially, now, g_2 is not given out to $\mathcal{A}$.

Cand1 implies an adaptive security of the ABE scheme from Γ (and we obtain Theorem 2). Intuitively, the indistinguishability of the H_2 elements in the output of kO_β implies the indistinguishability between normal and semi-functional keys, which then implies the adaptive security of the ABE scheme via the dual system technique [36]. Next, Cand1 can be shown to be implied by PMH and the SG assumption (and we obtain Theorem 3) as follows (also recall linearity of $\mathbf{k}_y$):

$$h_1^{\mathbf{k}_y(0,\mathbf{r},\hat{\mathbf{r}},\mathbf{w})} h_2^{\mathbf{k}_y(0,\mathbf{0},\hat{\mathbf{r}},\mathbf{0})} \underset{\text{SG}}{\approx_c} - \cdot h_2^{\mathbf{k}_y(0,\underline{\mathbf{r}},\hat{\mathbf{r}},\underline{\mathbf{w}})} \underset{\text{PMH}}{\approx_s} - \cdot h_2^{\mathbf{k}_y(\underline{\alpha},\mathbf{r},\hat{\mathbf{r}},\mathbf{w})} \underset{\text{SG}}{\approx_c} - \cdot h_2^{\mathbf{k}_y(\alpha,\underline{\mathbf{0}},\hat{\mathbf{r}},\underline{\mathbf{0}})}.$$

Note that "$-$" is the same element in H_1, and $\approx_c, \approx_s$ are computational and statistical indistinguishability, respectively. The purpose for making g_2 absent in $\mathcal{A}$'s input is to use the SG assumption that claims $h_1^{\mathbf{r}} \approx_c h^{\mathbf{r}}$. In this way, we can prove that Cand1 is preserved in KP1 for Boolean formulae by extending the KW framework. Intuitively, the reduction goes through as it can simulate $K_i = h_1^{\mathbf{k}_{y_i}(0,\mathbf{r}_i,\hat{\mathbf{r}}_i,\mathbf{w})} h_2^{\mathbf{k}_{y_i}(\sigma_i,\mathbf{0},\hat{\mathbf{r}}_i,\mathbf{0})}$ without $h_2^{\mathbf{w}}$ (observe that there is no $\mathbf{w}$ in the exponent to h_2 in K_i).

However, it turns out that Cand1 is not preserved in Dual. Assume that we use the same Dual transformation as in [3], which transforms a PES Γ for P to a PES $\overline{\Gamma}$ for Dual[P] as follows: first let the variables for $\overline{\Gamma}$ be $\mathbf{w}' = (w_0, \mathbf{w})$, $\mathbf{s}' = (s_{\mathsf{new}}, \mathbf{r})$, $\hat{\mathbf{s}}' = \hat{\mathbf{r}}$, $\mathbf{r}' = \mathbf{s}$, $\hat{\mathbf{r}}' = \hat{\mathbf{s}}$ and define the two encodings for $\overline{\Gamma}$ as

$$\mathbf{c}'_y(\mathbf{s}', \hat{\mathbf{s}}', \mathbf{w}') = \mathbf{k}_y(s_{\mathsf{new}} w_0, \mathbf{r}, \hat{\mathbf{r}}, \mathbf{w}), \quad \mathbf{k}'_x(\alpha, \mathbf{r}', \hat{\mathbf{r}}', \mathbf{w}') = (\mathbf{c}_x(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}), \alpha - s_0 w_0),$$

where w_0, s_{new} are new variables, and s_{new} takes a role of s_0 in $\overline{\Gamma}$. To prove the preservation of Cand1 in Dual, we need to construct a reduction $\mathcal{R}$ that breaks Cand1 of Γ internally using an adversary $\mathcal{A}$ against (Cand1 of) $\overline{\Gamma}$. A crucial fact here is that the roles of G and H are "switched", that is, $\mathcal{R}$ uses its input G and H as H and G for the input of $\mathcal{A}$, respectively. This is since $\mathcal{R}$ needs the reply of $\mathsf{cO}^{\mathcal{R}}$ to answer $\mathcal{A}$'s query to $\mathsf{kO}^{\mathcal{A}}$ (and analogously for $\mathsf{kO}^{\mathcal{R}}$ to $\mathsf{cO}^{\mathcal{A}}$). Now the problem arises as $\mathcal{R}$ does not possess g_2, but this very term will be needed to supply to $\mathcal{A}$'s input as h_2 (recall the "switching" of G and H). Also recall that h_2 was necessary to prove Theorem 2 (to simulate semi-functional keys).

Second Step: Parametrized vs Same-at-once. To solve the above problem, instead of preserving the *same* property from Γ to $\overline{\Gamma}$, we will establish an implication over *slightly different* properties on Γ and $\overline{\Gamma}$. Namely, we use more subgroups by letting $N = p_1 \cdots p_z$ and parametrize the candidate property as (z, ℓ)-Cand2, where $z, \ell \in \mathbb{N}$ s.t. $z \geq \ell$. Defining bilinear groups $e : G \times H \to G_{\mathsf{T}}$

of order N and its subgroups naturally, we then define $\mathsf{Adv}^{(\mathsf{z},\ell)\text{-}\mathsf{Cand2}}_{\mathcal{A},\Gamma}(\lambda)$ as

$$\left|\mathsf{Pr}\left[\beta{=}\beta' \;\middle|\; \begin{array}{l}\beta \leftarrow \{0,1\},\ \ \mathbf{w} \leftarrow \mathbb{Z}_N^{\omega} \\ \beta' \leftarrow \mathcal{A}^{\mathsf{cO}(\cdot),\mathsf{kO}_\beta(\cdot)}(g_1, h_1, g_{\ell+1}, \ldots, g_z, h_\ell, \ldots, h_z, g_1^{\mathbf{w}}, h_1^{\mathbf{w}})\end{array}\right] - \frac{1}{2}\right| \quad (2)$$

where $g^{\mathbf{c}_x(\mathbf{s},\hat{\mathbf{s}},\mathbf{w})} \leftarrow \mathsf{cO}(x)$ and $h_1^{\mathbf{k}_y(0,\mathbf{r},\hat{\mathbf{r}},\mathbf{w})} h_\ell^{\mathbf{k}_y(\beta\alpha,\mathbf{0},\hat{\mathbf{r}},\mathbf{0})} \leftarrow \mathsf{kO}_\beta(y)$. In this way, we have that g_ℓ is absent (generalizing the absence of g_2, so as to establish Theorem 3 as in the first step), but now, at the same time, we can also potentially establish the implication over Dual that $(z,\ell-1)$-$\mathsf{Cand2}$ of Γ implies (z,ℓ)-$\mathsf{Cand2}$ of $\overline{\Gamma}$ for $\ell \geq 2$ in the sense that the reduction $\mathcal{R}$ possesses $g_\ell, \ldots, g_z$ (as per the former notion) which can be used to exactly simulate $h_\ell, \ldots, h_z$ (giving to the adversary $\mathcal{A}$ against the latter notion), where we recall the switching of G and H.

Final Step: Wrapping up (Partial) Symmetries in Two Oracles. In the above, we generalize the functionality of the subgroups G_2, H_2 directly to G_ℓ, H_ℓ and hence obtain the above design of the oracle kO. However, this design fails when we try to use the reply of $\mathsf{cO}^{\mathcal{R}}$ to answer $\mathcal{A}$'s query to $\mathsf{kO}^{\mathcal{A}}$ (as presumably required in the reduction). This is since the former is an element of the entire group, while the latter is in the subgroup with generators h_1, h_ℓ; however, $\mathcal{A}$ possesses $g_{\ell+1}$ and thus can simply distinguish the two. A similar failure occurs analogously when relating $\mathsf{kO}^{\mathcal{R}}$ to $\mathsf{cO}^{\mathcal{A}}$. To solve this, we need to re-design also the two oracles carefully (satisfying not only this particular preservation of Dual that we are discussing but also all the required 3 theorems). To this end, our solution is to define them in partially (and not fully) *symmetrical* manner:

$$\begin{aligned} g_1^{\mathbf{c}_x(\mathbf{s},\mathbf{0},\mathbf{w})} g_{[2,\ell]}^{\mathbf{c}_x((s_0,\mathbf{0}),\mathbf{0},\mathbf{w})} g^{\mathbf{c}_x(\mathbf{0},\hat{\mathbf{s}},\mathbf{0})} \quad &\leftarrow \mathsf{cO}(x), \\ h_1^{\mathbf{k}_y(0,\mathbf{r},\mathbf{0},\mathbf{w})} h_\ell^{\mathbf{k}_y(\beta\alpha,\mathbf{0},\mathbf{0},\mathbf{0})} h^{\mathbf{k}_y(0,\mathbf{0},\hat{\mathbf{r}},\mathbf{0})} \quad &\leftarrow \mathsf{kO}_\beta(y), \end{aligned}$$

and also additionally give out $T = (g_{[1,\ell]}, \ldots, g_{[1,z]}, h_{[1,\ell+1]}, \ldots, h_{[1,z]})$ (as inputs to $\mathcal{A}$ in Eq. (2)), where we denote $g_{[a,b]} = g_a \cdots g_b$ for $a \leq b$. Intuitively, the forms of $\mathsf{cO}^{\mathcal{R}}$ and $\mathsf{kO}^{\mathcal{A}}$ are now *somewhat symmetric*, except the difference lying in the subgroups with indexes $2, \ldots, \ell-1$, and we observe that the adversary does not possess an element from these subgroups so as to distinguish the two; therefore, we can use the former to simulate the latter, under the SG assumption. The additional input T is essential for the other oracle simulation (from $\mathsf{kO}^{\mathcal{R}}$ to $\mathsf{cO}^{\mathcal{A}}$). Crucially, giving out individual generators such as $g_2, \ldots, g_\ell$ would destroy the "absence" requirement (essential for Theorem 3); while, on the other hand, giving out the elements like $g_{[1,i]}$ do work.

This completes our design rational of (z,ℓ)-KE-ind (in the composite-order-groups flavor). Note that ℓ is incremented by 1 after applying one Dual conversion. Starting from $(z,1)$-KE-ind, we have that $z-1$ is the maximum number of Dual applications. Thus, by choosing z depending on the number of dual applications to obtain a target predicate P, we can instantiate a secure ABE scheme for P. Also note that (z,ℓ)-KE-ind will require $\mathbf{s}$ to consist of only s_0 so that it is implied by PMH. We call it single-variable PMH. Note that PESs with

single-variable PMH are still more general encodings than predicate encodings [6,38].

All in all, our conceptually new insight is the *partially symmetric* design of the core 1-key 1-ciphertext component (our KE-ind) so as to incorporate Dual (crucial in bootstrapping KP1 to KP). This differs to other similar core components in the literature, notably, the "1-ABE" in [26]. We discuss more in the next subsection.

1.3 Technical Comparisons to Previous Unbounded ABE and More

Our framework allows us to modularly construct unbounded ABE schemes. Thus, one may wonder how our framework compares to previous unbounded ABE schemes from static assumptions [16,26,27,30]. Basically, these ABE schemes rely on so-called "nested dual system technique", in which entropy in secret keys is increased via entropy propagation between a secret key and ciphertext. All these works uses the IBE predicate as a source of entropy.

Intuitively, when instantiating our framework to completely unbounded monotone ABE, such an entropy propagation can be viewed as being decomposed into modular parts, namely, the PMH (of a PES for IBE), the KP1 transform, and the Dual transform (recall that we apply KP1 and Dual$\circ$KP1 to IBE in a nested manner to achieve such an ABE instance [9]). This predicate transformations implicitly trace a similar hybrid sequence to that by Lewko and Waters (LW) [27], borrowing the power of the KW framework (the piecewise guessing framework) to do it in the adaptive setting. An important fact here is that our framework uses the KW framework in a "nested" manner. Intuitively, this is the reason why our ABE schemes can be constructed as large-universe constructions similarly to the LW unbounded scheme. On the other hand, the KW unbounded scheme [26] is obtained by directly applying the KW framework (not in a nested manner) to the unbounded *small-universe* ABE scheme in [16]. This, in turn, *inherently* poses a linear cost of the universe size U in the security loss (and hence U cannot be super-polynomially large) for the KW scheme (see Table 6).

Another advantage of our framework over the KW scheme is that we do not use the subgroup DDH assumption [16], which requires a k-dimensional semi-functional space for the k-Lin assumption. In contrast, 1-dimensional semi-functional spaces suffice for our framework. This yields asymptotically smaller ciphertexts and keys than the KW scheme (asymptotic in k, see Table 6).

Table 6. Comparison with unbounded KP-ABE from $\mathcal{D}_k$-MDDH by KW19 [26].

References	Security loss	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{ct}\rvert$	$\lvert\mathsf{sk}\rvert$
KW19 [26]	$O(Uq_{\mathsf{sk}})2^{O(B)}$	$(5k^2+k)\lvert G_1\rvert$ $+k\lvert G_{\mathsf{T}}\rvert$	$((3k+1)t+2k+1)\lvert G_1\rvert$ $+\lvert G_{\mathsf{T}}\rvert$	$((5k+2)n+(2k+1)m)\lvert G_2\rvert$
Ours 1	$O(q_{\mathsf{sk}})2^{O(B)}$	$(4k^2+8k)\lvert G_1\rvert$ $+k\lvert G_{\mathsf{T}}\rvert$	$((2k+4)t+k+2)\lvert G_1\rvert$ $+\lvert G_{\mathsf{T}}\rvert$	$(3k+6)n\lvert G_2\rvert$

Note: U is the attribute domain size, q_{sk} is the maximum number of secret key queries, B is the maximum depth of formulae, $t = |\text{attribute set}|$, m and n are the number of gates and the input length of a formula, respectively.

Full Version of This paper. Due to limited spaces, we defer details such as omitted proofs, details on instantiations, and discussions regarding more recent related works (such as [4,5,21,22,28]) to the full version of this paper [12].

2 Preliminaries

Notation. For a natural number $m, n \in \mathbb{N}$, $[m]$ denotes a set $\{1, \ldots, m\}$, $[m]^+$ denotes a set $\{0, \ldots, m\}$, and $[m, n]$ denotes a set $\{m, \ldots, n\}$. For a set S, $s \leftarrow S$ denotes that s is uniformly chosen from S. We treat vectors as column vectors unless specified otherwise. For a generator g_i of a cyclic group G_i of order p and $a \in \mathbb{Z}_p$, $[a]_i$ denotes g_i^a. Furthermore, for a matrix $\mathbf{A} = (a_{j,\ell})_{j,\ell}$ over $\mathbb{Z}_p$, $[\mathbf{A}]_i$ denotes a matrix over G_i whose (j, ℓ)-th entry is $g_i^{a_{j,\ell}}$. For vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$, let $e([\mathbf{x}]_1, [\mathbf{y}]_2) = e(g_1, g_2)^{\langle \mathbf{x}, \mathbf{y} \rangle}$ be a function that computes the inner product on the exponent by $\prod_{i \in [n]} e([x_i]_1, [y_i]_2)$. A function $f : \mathbb{N} \to \mathbb{R}$ is called negligible if $f(\lambda) = \lambda^{-\omega(1)}$ and denotes $f(\lambda) \leq \mathsf{negl}(\lambda)$. For families of distributions $X = \{X_\lambda\}_{\lambda \in \mathbb{N}}$ and $Y = \{Y_\lambda\}_{\lambda \in \mathbb{N}}$, we denote $X \approx_c Y$ (resp. $X \approx_s Y$) as computational indistinguishability (resp. statistical indistinguishability). For an interactive game G, $\langle \mathcal{A}, \mathsf{G} \rangle$ denotes the output of $\mathcal{A}$ in G.

Matrix Notation. Throughout the paper, we use the following matrix notation. For a regular matrix $\overline{\mathbf{M}} \in \mathsf{GL}_{k+\zeta}(\mathbb{Z}_p)$, we define $\mathbf{M}$, $\mathbf{m}_i$, $\mathbf{M}^*$, and $\mathbf{m}_i^*$ as follows. $\mathbf{M}$ and $\mathbf{m}_i$ denote a matrix and a vector consist of the first k columns and the $(k+i)$-th column of $\overline{\mathbf{M}}$, respectively. Similarly, $\mathbf{M}^*$ and $\mathbf{m}_i^*$ denote a matrix and vector consist of the first k columns and the $(k+i)$-th column of $(\overline{\mathbf{M}}^\top)^{-1}$, respectively. We have the relations, $\mathbf{M}^\top \mathbf{m}_i^* = \mathbf{0}$ and $\mathbf{m}_i^\top \mathbf{m}_i^* = 1$ for $i \in [\zeta]$. We also uses the following notations:

$$\mathsf{span}(\mathbf{M}, \mathbf{m}_1, \ldots, \mathbf{m}_n) = \{\mathbf{v} \mid \exists \mathbf{u} \in \mathbb{Z}_p^{k+n}, \mathbf{v} = (\mathbf{M} || \mathbf{m}_1 || \ldots || \mathbf{m}_n)\mathbf{u}\},$$
$$\mathsf{Ker}(\mathbf{M}, \mathbf{m}_1, \ldots, \mathbf{m}_n) = \{\mathbf{v} \mid (\mathbf{M} || \mathbf{m}_1 || \ldots || \mathbf{m}_n)^\top \mathbf{v} = \mathbf{0}\}.$$

2.1 Basic Definitions and Tools

Boolean Formula and NC^1. A monotone Boolean formula can be represented by a Boolean circuit of which all gates have fan-in 2 and fan-out 1. More precisely, we specify a monotone Boolean formula by a tuple $f = (n, w, m, G)$ where $n, w, m \in \mathbb{N}$ represents the number of input wires, the number of all wires (including the input wires), and the number of gates, respectively, while $G : [m] \to \{\text{AND, OR}\} \times [w]^3$ is a function that specifies the gate type, the two incoming wires, and the outgoing wire of each gate. To specify G, we first let all the wires and gates to be numbered. The wire numbers range from 1 to w; while those of gates range from 1 to m. For each gate $i \in [m]$, the information $G(i) = (T, a, b, c)$ tells us that T is the type of the gate i, while a and b specify its incoming wires, and c specifies its outgoing wire. By convention, we always number the wires so that $a < b < c$. The computation of Boolean formula f on

an input in $\{0,1\}^n$ is defined naturally; we often abuse the notation and treat f as a function $f : \{0,1\}^n \to \{0,1\}$.

A non-monotone Boolean formula additionally contains NOT gates, which have fan-in 1 and fan-out 1. It is well-known that, via De Morgan's law, we can express any non-monotone Boolean formula by one in which all the NOT gates are placed on the input wires (and the number of gates of the latter formula is two times of that of the former). Hence, we can specify a non-monotone Boolean formula as a tuple $f = (n, w, m, G, \Sigma)$, where $\Sigma : [n] \to \{\text{Positive}, \text{Negative}\}$ naturally specifies if the input wire $i \in [n]$ is a negative one or not.

Standard complexity theory tells us that circuit complexity class NC^1 and Boolean formulae are equivalent. It is known also that NC^1 is equivalent to the class captured by log-depth Boolean formulae (see *e.g.,* [26]). Thus, the circuit complexity class captured by Boolean formulae is equivalent to the class captured by log-depth Boolean formulae.

Definition 1 (Linear Secret Sharing Scheme). A linear secret sharing scheme (LSSS) for a function class $\mathcal{F}$ consists of two algorithms Share and Rec.

$\mathsf{Share}(f, \mathbf{h})$: It takes a function $f \in \mathcal{F}$ where $f : \{0,1\}^n \to \{0,1\}$ and a vector $\mathbf{h} \in \mathbb{Z}_p^\gamma$. Then, outputs shares $\mathbf{h}_1, \ldots, \mathbf{h}_n \in \mathbb{Z}_p^\gamma$.

$\mathsf{Rec}(f, x, \{\mathbf{h}_i\}_{x_i=1})$: It takes $f : \{0,1\}^n \to \{0,1\}$, a bit string $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ and shares $\{\mathbf{h}_i\}_{x_i=1}$. Then, outputs a vector $\mathbf{h}'$ or $\perp$.

In particular, Rec computes a linear function on shares to reconstruct a secret; $\mathbf{h} = \sum_{x_i=1} a_i \mathbf{h}_i$ where each a_i is determined by f. A LSSS has two properties.

Correctness: For any $f \in F$, $x \in \{0,1\}^n$ such that $f(x) = 1$,

$$\Pr[\mathsf{Rec}(f, x, \{\mathbf{h}_i\}_{x_i=1}) = \mathbf{h} \mid \mathbf{h}_1, \ldots, \mathbf{h}_n \leftarrow \mathsf{Share}(f, \mathbf{h})] = 1.$$

Security: For any $f \in F$, $x \in \{0,1\}^n$ such that $f(x) = 0$, and $\mathbf{h}_1, \ldots, \mathbf{h}_n \leftarrow \mathsf{Share}(f, \mathbf{h})$, shares $\{\mathbf{h}_i\}_{x_i=1}$ have no information about $\mathbf{h}$.

Definition 2 (Bilinear Groups). A description of bilinear groups $\mathbb{G} = (p, G_1, G_2, G_\mathsf{T}, g_1, g_2, e)$ consist of a prime p, cyclic groups G_1, G_2, G_T of order p, generators g_1 and g_2 of G_1 and G_2 respectively, and a bilinear map $e : G_1 \times G_2 \to G_\mathsf{T}$, which has two properties.

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

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

Definition 3 ($\mathcal{D}_{j,k}$-MDDH Assumption [19]). For $j > k$, let $\mathcal{D}_{j,k}$ be a matrix distribution over matrices in $\mathbb{Z}_p^{j \times k}$, which outputs a full-rank matrix with overwhelming probability. Denote $\mathcal{D}_{k+1,k} = \mathcal{D}_k$. We can assume that, wlog, the first k rows of a matrix chosen from $\mathcal{D}_{j,k}$ form an invertible matrix. We consider the following distribution: $\mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{j,k}$, $\mathbf{v} \leftarrow \mathbb{Z}_p^k$, $\mathbf{t}_0 = \mathbf{A}\mathbf{v}$, $\mathbf{t}_1 \leftarrow$

$\mathbb{Z}_p^j$, $P_{i,\beta} = (\mathbb{G}, [\mathbf{A}]_i, [\mathbf{t}_\beta]_i)$. We say that the $\mathcal{D}_{j,k}$-MDDH assumption holds with respect to $\mathcal{G}_{\mathsf{BG}}$ if, for any PPT adversary $\mathcal{A}$,

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

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

Random Self-reducibility. We can obtain arbitrarily many instances of the $\mathcal{D}_k$-MDDH problem without additional security loss. For any $n \in \mathbb{N}$, we define the following distribution: $\mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_k$, $\mathbf{V} \leftarrow \mathbb{Z}_p^{k\times n}$, $\mathbf{T}_0 = \mathbf{AV}$, $\mathbf{T}_1 \leftarrow \mathbb{Z}_p^{(k+1)\times n}$, $P_{i,\beta} = (\mathbb{G}, [\mathbf{A}]_i, [\mathbf{T}_\beta]_i)$. The n-fold $\mathcal{D}_k$-MDDH assumption is similarly defined to the $\mathcal{D}_k$-MDDH assumption. Then, n-fold $\mathcal{D}_k$-MDDH is tightly reduced to $\mathcal{D}_k$-MDDH. That is, $\mathcal{D}_k$-MDDH $\Rightarrow$ n-$\mathcal{D}_k$-MDDH.

2.2 Attribute-Based Encryption

Predicate Family. Let $\mathsf{P} = \{\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\} \mid \kappa \in \mathcal{K}\}$ be a predicate family where $\mathcal{X}_\kappa$ and $\mathcal{Y}_\kappa$ denote "ciphertext attribute" and "key attribute" spaces. The index κ denotes a list of some parameters such as bounds on some quantities (hence $\mathcal{K}$ depends on that predicate). We often omit κ if the context is clear.

Definition 4 (Attribute-Based Encryption). An attribute-based encryption (ABE) scheme for a predicate family P consists of four algorithms:

$\mathsf{Setup}(1^\lambda, \kappa)$]: It takes a security parameter 1^λ, and an index κ as inputs, and outputs a public key pk and a master secret key msk.

$\mathsf{Enc}(\mathsf{pk}, x, M)$]: It takes pk, an attribute $x \in \mathcal{X}$ and a message $M \in \mathcal{M}$ as inputs, and outputs a ciphertext ct_x. (Note that we let $\mathcal{M}$ be specified in pk.)

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{msk}, y)$]: It takes $\mathsf{pk}, \mathsf{msk}$, and an attribute $y \in \mathcal{Y}$ as inputs, and outputs a secret key sk_y.

$\mathsf{Dec}(\mathsf{pk}, \mathsf{ct}_x, \mathsf{sk}_y)$]: It takes $\mathsf{pk}, \mathsf{ct}_x$ and sk_y as inputs, and outputs a message M' or a symbol $\perp$.

Correctness/Security. The standard correctness is specified by the property if $\mathsf{P}(x, y) = 1$ then ct_x can be decrypted by sk_y. The standard security notion is called adaptive security. We refer these to the full version.

3 Pair Encoding Schemes

A pair encoding scheme (PES), introduced by Attrapadung [7], is an encoding system used in a general framework to construct ABE. Structures of a ciphertext and secret keys of an ABE scheme can be concisely captured by polynomials, and its decryption procedure can be represented by matrices. A PES is defined as a set of algorithms that output these polynomials or matrices. Intuitively, the polynomials specify the structures of exponent of group elements in a ciphertext and secret key, and the matrices specify coefficients used in the decryption.

3.1 Pair Encoding Scheme Definition

Definition 5 (Pair Encoding Schemes). Let $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$ be a predicate family, indexed by $\kappa = (N, \mathsf{par})$, where par specifies some parameters. A PES for P_κ is given by four deterministic polynomial-time algorithms:

- $\mathsf{Param}(\mathsf{par}) \to \omega$. When given par as input, Param outputs $\omega \in \mathbb{N}$ that specifies the number of *common* variables, which we denote by $\mathbf{w} = (w_1, \ldots, w_\omega)$.
- $\mathsf{EncCt}(x, N) \to (n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}))$. On input $N \in \mathbb{N}$, $x \in \mathcal{X}_{(N,\mathsf{par})}$, EncCt outputs a vector of polynomial $\mathbf{c} = (c_1, \ldots, c_{n_3})$ in *non-lone* variables $\mathbf{s} = (s_0, s_1, \ldots, s_{n_1})$ and *lone* variables $\hat{\mathbf{s}} = (\hat{s}_1, \ldots, \hat{s}_{n_2})$ as follows, where $\theta_{i,z}, \theta_{i,t,j} \in \mathbb{Z}_N$:

$$\mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}) = \{ \sum_{z \in [n_2]} \theta_{i,z} \hat{s}_z + \sum_{t \in [n_1]^+, j \in [\omega]} \theta_{i,t,j} w_j s_t \}_{i \in [n_3]}.$$

- $\mathsf{EncKey}(y, N) \to (m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w}))$. On input $N \in \mathbb{N}$ and $y \in \mathcal{Y}_{(N,\mathsf{par})}$, EncKey outputs a vector of polynomial $\mathbf{k} = (k_1, \ldots, k_{m_3})$ in *non-lone* variables $\mathbf{r} = (r_1, \ldots, r_{m_1})$ and *lone* variables $\hat{\mathbf{r}} = (\alpha, \hat{r}_1, \ldots, \hat{r}_{m_2})$ as follows, where $\phi_i, \phi_{i,u}, \phi_{i,v,j} \in \mathbb{Z}_N$:

$$\mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w}) = \{\phi_i \alpha + \sum_{u \in [m_2]} \phi_{i,u} \hat{r}_u + \sum_{v \in [m_1], j \in [\omega]} \phi_{i,v,j} w_j r_v \}_{i \in [m_3]}.$$

- $\mathsf{Pair}(x, y, N) \to (\mathbf{E}, \overline{\mathbf{E}})$. On input N, and both x, and y, Pair outputs two matrices $\mathbf{E}, \overline{\mathbf{E}}$ of sizes $(n_1 + 1) \times m_3$ and $n_3 \times m_1$, respectively.

Correctness. A PES is said to be correct if for every $\kappa = (N, \mathsf{par})$, $x \in \mathcal{X}_\kappa$ and $y \in \mathcal{Y}_\kappa$ such that $\mathsf{P}_\kappa(x, y) = 1$, then $\mathbf{s}\mathbf{E}\mathbf{k}^\top + \mathbf{c}\overline{\mathbf{E}}\mathbf{r}^\top = \alpha s_0$ holds symbolically. The left-hand side is indeed a linear combination of $s_t k_p$ and $c_q r_v$, for $t \in [n_1]^+, p \in [m_3], q \in [n_3], v \in [m_1]$. Hence, an equivalent way to describe Pair and correctness together at once is to show such a linear combination that evaluates to αs_0.

Terminology. We denote $(\hat{r}_1, \ldots, \hat{r}_{m_2})$ by $\hat{\mathbf{r}}_{-\alpha}$. Following [3], a variable is called *lone* as it is not multiplied with any w_j (otherwise called *non-lone*). Furthermore, since α, s_0 are treated distinguishably in defining correctness, we also often call them the *special* lone and non-lone variable, respectively. Throughout the paper, we fix N in index κ as prime p, which is an order of bilinear groups used to construct an ABE scheme. For notational conciseness, we consider that κ only specifies par, and p is hard-coded in EncCt, EncKey, and Pair.

Evaluating PES with Vectors/Matrices. We can evaluate ciphertext encoding $\mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})$ with the following substitution from scalar variables to vectors/matrices as follows. Let $d \in \mathbb{N}$. Each s_t is substituted by a vector $\mathbf{s}_t \in \mathbb{Z}_N^d$. Each $\hat{s}_z$ is substituted by a vector $\hat{\mathbf{s}}_z \in \mathbb{Z}_N^d$. Each w_j is substituted by a matrix

$\mathbf{W}_j \in \mathbb{Z}_N^{d\times d}$. Let $\mathbf{S} = (\mathbf{s}_0, \ldots, \mathbf{s}_{n_1}) \in \mathbb{Z}_N^{d\times(n_1+1)}$, $\hat{\mathbf{S}} = (\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2}) \in \mathbb{Z}_N^{d\times n_2}$, and $\mathbb{W} = (\mathbf{W}_1, \ldots, \mathbf{W}_\omega)$, we then define

$$\mathbf{c}(\mathbf{S}, \hat{\mathbf{S}}, \mathbb{W}) = \{ \sum_{z\in[n_2]} \theta_{i,z}\hat{\mathbf{s}}_z + \sum_{t\in[n_1]^+, j\in[\omega]} \theta_{i,t,j}\mathbf{W}_j^\top \mathbf{s}_t\}_{i\in[n_3]},$$
$$\mathbf{k}(\mathbf{R}, \hat{\mathbf{R}}, \mathbb{W}) = \{\phi_i\mathbf{h} + \sum_{u\in[m_2]} \phi_{i,u}\hat{\mathbf{r}}_u + \sum_{v\in[m_1], j\in[\omega]} \phi_{i,v,j}\mathbf{W}_j\mathbf{r}_v\}_{i\in[m_3]}.$$

3.2 Security Properties of PESs

Definition 6 (Perfect Master-Key Hiding (PMH) [7]). Let $\Gamma = (\mathsf{Param}, \mathsf{EncCt}, \mathsf{EncKey}, \mathsf{Pair})$ be a PES for a predicate faimily $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$. We say that Γ satisfies perfect master-key hiding (PMH) if the following holds. Let $\omega \leftarrow \mathsf{Param}(\mathsf{par})$, $(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})) \leftarrow \mathsf{EncCt}(x)$, and $(m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})) \leftarrow \mathsf{EncKey}(y)$. Then, for all κ and $(x, y) \in \mathcal{X}_\kappa \times \mathcal{Y}_\kappa$ such that $\mathsf{P}_\kappa(x, y) = 0$, the two distributions are identical, where the probability is taken over $\mathbf{s} \leftarrow \mathbb{Z}_p^{n_1+1}$, $\hat{\mathbf{s}} \leftarrow \mathbb{Z}_p^{n_2}$, $\mathbf{r} \leftarrow \mathbb{Z}_p^{m_1}$, $\alpha \leftarrow \mathbb{Z}_p$, $\hat{\mathbf{r}}_{-\alpha} \leftarrow \mathbb{Z}_p^{m_2}$, and $\mathbf{w} \leftarrow \mathbb{Z}_p^\omega$.

$$\{\mathbf{s}, \mathbf{r}, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}), \mathbf{k}(\mathbf{r}, (0, \hat{\mathbf{r}}_{-\alpha}), \mathbf{w})\} \quad \text{and} \quad \{\mathbf{s}, \mathbf{r}, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}), \mathbf{k}(\mathbf{r}, (\alpha, \hat{\mathbf{r}}_{-\alpha}), \mathbf{w})\}.$$

Definition 7 (Single-Variable PMH). We say that Γ satisfies single-variable PMH if Γ is PMH and $n_1 = 0$ for all $x \in \mathcal{X}_\kappa$, where $(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})) \leftarrow \mathsf{EncCt}(x)$. In other words, EncCt uses only s_0 for non-lone variable.

Note that Ambrona *et al.* showed that all predicate encodings [38] can be seen as a PES with single-variable PMH [6].

We next introduce the (ζ, ℓ)-key-encoding indistinguishability ((ζ, ℓ)-$\mathsf{KE\text{-}ind}$), which is a central security property in our framework, where we consider several transformations of PESs. The crucial feature on (ζ, ℓ)-$\mathsf{KE\text{-}ind}$ is two-fold: it is preserved after transformations, and it leads to the adaptive security of the resulting ABE scheme.

Definition 8 ((ζ, ℓ)-KE-ind). Let $\Gamma = (\mathsf{Param}, \mathsf{EncCt}, \mathsf{EncKey}, \mathsf{Pair})$ be a PES for a predicate family $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$. Let $\zeta, \ell \in \mathbb{N}$ such that $\ell \le \zeta$. We say that Γ satisfies (ζ, ℓ)-$\mathsf{KE\text{-}ind}$ if the following holds. Consider a game $\mathsf{G}_\beta^{(\zeta,\ell)\text{-}\mathsf{KE\text{-}ind}}$ defined in Fig. 1, in which an adversary $\mathcal{A}$ can adaptively query $\mathcal{O}_\mathcal{X}$ and $\mathcal{O}_\mathcal{Y}$ with $x \in \mathcal{X}_\kappa$ and $y \in \mathcal{Y}_\kappa$ such that $\mathsf{P}_\kappa(x, y) = 0$, respectively. $\mathcal{A}$ is allowed to query each oracle at most once. Then, for all $\eta \in \{1, 2\}$, we have $\mathsf{G}_0^{(\zeta,\ell)\text{-}\mathsf{KE\text{-}ind}} \approx_c \mathsf{G}_1^{(\zeta,\ell)\text{-}\mathsf{KE\text{-}ind}}$.

Note that we can omit the terms that correspond to $g_{[1,i]}, h_{[1,i]}$ of the composite-order variant in the introduction by giving $\mathbf{a}_i^*, \mathbf{b}_i^*$ as $\mathbb{Z}_p$ elements to $\mathcal{A}$.

The following theorem says that all PESs with single-variable PMH satisfy (ζ, ℓ)-$\mathsf{KE\text{-}ind}$ for all $\zeta, \ell \in \mathbb{N}$. We defer its proof to the full version.

$\underline{\mathsf{G}_{\beta}^{(\zeta,\ell)\text{-KE-ind}}}$
$\omega \leftarrow \mathsf{Param}(\mathsf{par}),\ \ \mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^{\lambda})$
$\overline{\mathbf{A}}, \overline{\mathbf{B}} \leftarrow \mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)},\ \ \mathbb{W} = (\mathbf{W}_1, \ldots, \mathbf{W}_\omega) \leftarrow (\mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)})^{\omega}$
$P = (\mathbb{G}, [\mathbf{A}]_\eta, [\mathbf{B}]_{3-\eta}, \{\mathbf{a}_i^*\}_{i\in[\ell,\zeta]}, \{\mathbf{b}_i^*\}_{i\in[\ell+1,\zeta]}, \{[\mathbf{W}_i^\top \mathbf{A}]_\eta, [\mathbf{W}_i \mathbf{B}]_{3-\eta}\}_{i\in[\omega]})$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathcal{X}}(\cdot),\mathcal{O}_{\mathcal{Y}}(\cdot,\cdot)}(P)$

$\underline{\mathcal{O}_{\mathcal{X}}(\cdot)}$
Input: $x \in \mathcal{X}_\kappa$
$(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})) \leftarrow \mathsf{EncCt}(x)$
$\mathbf{c}_0 \leftarrow \mathsf{span}(\mathbf{A}, \mathbf{a}_1, \ldots, \mathbf{a}_\ell),\ \ \mathbf{s}_1, \ldots, \mathbf{s}_{n_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$
$\mathbf{S} = (\mathbf{c}_0, \mathbf{A}\mathbf{s}_1, \ldots, \mathbf{A}\mathbf{s}_{n_1}),\ \ \widehat{\mathbf{S}} = (\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2})$
Output: $([\mathbf{S}]_\eta, [\mathbf{c}(\mathbf{S}, \widehat{\mathbf{S}}, \mathbb{W})]_\eta)$

$\underline{\mathcal{O}_{\mathcal{Y}}(\cdot,\cdot)}$
Input: $y \in \mathcal{Y}_\kappa$ and $\mathbf{h} \in \mathbb{Z}_p^{k+\zeta}$
$(m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})) \leftarrow \mathsf{EncKey}(y),\ \mu \leftarrow \mathbb{Z}_p,\ \ \mathbf{r}_1, \ldots, \mathbf{r}_{m_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{m_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$
$\mathbf{R} = (\mathbf{B}\mathbf{r}_1, \ldots, \mathbf{B}\mathbf{r}_{m_1}),\ \ \widehat{\mathbf{R}} = (\mathbf{h} + \boxed{\beta\mu\mathbf{a}_\ell^*}, \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{m_2})$
Output: $([\mathbf{R}]_{3-\eta}, [\mathbf{k}(\mathbf{R}, \widehat{\mathbf{R}}, \mathbb{W})]_{3-\eta})$

Fig. 1. (ζ, ℓ)-KE-ind game.

Theorem 4 ((ζ, ℓ)-KE-ind of PES with Single-Variable PMH). *Let Γ be a PES with single-variable PMH. Then, for all constants $\zeta, \ell \in \mathbb{N}$, Γ satisfies (ζ, ℓ)-KE-ind under the $\mathcal{D}_k$-MDDH assumption. More precisely, for all PPT adversaries $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}_{\mathcal{A},\Gamma}^{(\zeta,\ell)\text{-KE-ind}}(\lambda) \leq 2\mathsf{Adv}_{\mathcal{B}}^{\mathcal{D}_k\text{-MDDH}}(\lambda) + 2^{-\Omega(\lambda)}.$$

4 Predicate Transformations

In this section, we present several transformations for predicates, which enable us to construct a more expressive predicate from simple predicates. As shown later in Sect. 6, these transformations are sufficiently powerful to construct ABE schemes whose constructions from standard assumptions are still unknown. Concretely, we introduce four transformations called the direct sum, dual transformation, KP augmentation, and CP augmentation. Because the CP augmentation is obtained from the dual transformation and KP augmentation, the former three transformations are sufficient for our framework. We also present the corresponding transformations of PESs for each predicate transformation and prove that these PES transformations preserve the (ζ, ℓ)-KE-ind property. Starting from PESs with the single-variable PMH, which already satisfy (ζ, ℓ)-KE-ind, we can obtain a PES for a expressive predicate that satisfies (ζ', ζ')-KE-ind for some constant ζ'. Finally, we show that we can use the PES with (ζ', ζ')-KE-ind to construct an adaptively secure ABE scheme in Sect. 5.

4.1 Direct Sum of Predicate Families

Definition 9 (Direct Sum [9]). Let $\mathsf{P}^{(i)}_{\kappa_i} : \mathcal{X}^{(i)}_{\kappa_i} \times \mathcal{Y}^{(i)}_{\kappa_i} \to \{0,1\}$ be a predicate family. Let $\kappa = (\kappa_1, \ldots, \kappa_d)$. A predicate family for the direct sum of a predicate family set $\mathcal{P}_\kappa = (\mathsf{P}^{(1)}_{\kappa_1}, \ldots, \mathsf{P}^{(d)}_{\kappa_d})$, denoted by $\mathsf{DS}[\mathcal{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$, is defined as follows: let $\bar{\mathcal{X}}_\kappa = \bigcup_{i\in[d]}(\{i\} \times \mathcal{X}^{(i)}_{\kappa_i})$, $\bar{\mathcal{Y}}_\kappa = \bigcup_{i\in[d]}(\{i\} \times \mathcal{Y}^{(i)}_{\kappa_i})$, and define

$$\mathsf{DS}[\mathcal{P}_\kappa]((i_x, x), (i_y, y)) \Leftrightarrow (i_x = i_y) \wedge (\mathsf{P}^{(i_y)}_{\kappa_{i_y}}(x, y) = 1).$$

We sometimes use another notation, $\mathsf{P}^{(1)}_{\kappa_1} \odot \cdots \odot \mathsf{P}^{(d)}_{\kappa_d}$, to denotes $\mathsf{DS}[\mathcal{P}_\kappa]$.

PES for $\mathsf{DS}[\mathcal{P}_\kappa]$. Let $\Gamma_i = (\mathsf{Param}_i, \mathsf{EncCt}_i, \mathsf{EncKey}_i, \mathsf{Pair}_i)$ be a PES for $\mathsf{P}^{(i)}_{\kappa_i}$. We construct a PES for $\mathsf{DS}[\mathcal{P}_\kappa]$, denoted by $\mathsf{DS\text{-}Trans}(\mathbf{\Gamma}) = (\mathsf{Param}', \mathsf{EncCt}', \mathsf{EncKey}', \mathsf{Pair}')$, where $\mathbf{\Gamma} = (\Gamma_1, \ldots, \Gamma_d)$.

- $\mathsf{Param}'(\mathsf{par}) \to \omega'$: Run $\omega_i \leftarrow \mathsf{Param}_i(\mathsf{par})$ and output $\sum_{i\in[d]} \omega_i$. This specifies common variables $\mathbf{w}' = (\mathbf{w}^{(1)}, \ldots, \mathbf{w}^{(d)})$, where $\mathbf{w}^{(i)} = (w^{(i)}_1, \ldots, w^{(i)}_{\omega_i})$.
- $\mathsf{EncCt}'((i_x, x)) \to (n'_1, n'_2, \mathbf{c}'(\mathbf{s}', \hat{\mathbf{s}}', \mathbf{w}'))$:
  - Output $(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}^{(i_x)})) \leftarrow \mathsf{EncCt}_{i_x}(x)$.
  - Define $n'_1 = n_1$, $n'_2 = n_2$, $\mathbf{s}' = \mathbf{s}$, and $\hat{\mathbf{s}}' = \hat{\mathbf{s}}$.
- $\mathsf{EncKey}'((i_y, y)) \to (m'_1, m'_2, \mathbf{k}'(\mathbf{r}', \hat{\mathbf{r}}', \mathbf{w}'))$:
  - Output $(m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w}^{(i_y)})) \leftarrow \mathsf{EncKey}_{i_y}(y)$.
  - Define $m'_1 = m_1$, $m'_2 = m_2$, $\mathbf{r}' = \mathbf{r}$, and $\hat{\mathbf{r}}' = \hat{\mathbf{r}}$.
- $\mathsf{Pair}'((i_x, x), (i_y, y)) \to (\mathbf{E}', \bar{\mathbf{E}}')$ and correctness:
  - Output $(\mathbf{E}, \bar{\mathbf{E}}) \leftarrow \mathsf{Pair}_{i_y}(x, y)$.
  - Correctness of Pair' directly follows from that of Pair_{i_y}.

Theorem 5 ((ζ,ℓ)-KE-ind *of* $\mathsf{DS\text{-}Trans}(\mathbf{\Gamma})$). *If Γ_i satisfies (ζ,ℓ)-KE-ind for all $i \in [d]$, then $\mathsf{DS\text{-}Trans}(\mathbf{\Gamma})$ satisfies (ζ,ℓ)-KE-ind. More precisely, for all PPT adversaries $\mathcal{A}$, there exist PPT adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}^{(\zeta,\ell)\text{-KE-ind}}_{\mathcal{A},\mathsf{DS\text{-}Trans}(\mathbf{\Gamma})}(\lambda) \le d \max_{i\in[d]} \mathsf{Adv}^{(\zeta,\ell)\text{-KE-ind}}_{\mathcal{B},\Gamma_i}(\lambda).$$

Proof. For $\beta \in \{0,1\}$, we can describe the (ζ,ℓ)-KE-ind game $\mathsf{G}^{(\zeta,\ell)\text{-KE-ind}}_\beta$ for $\mathsf{DS\text{-}Trans}(\mathbf{\Gamma})$ as shown in Fig. 2. To prove the theorem, we consider an adversary $\mathcal{B}$, which samples $t \leftarrow [d]$ and interacts with $\mathcal{O}_{\mathcal{X}^{(t)}}$ and $\mathcal{O}_{\mathcal{Y}^{(t)}}$ of the (ζ,ℓ)-KE-ind game for Γ_t. $\mathcal{B}$ internally runs an adversary $\mathcal{A}$ against (ζ,ℓ)-KE-ind of $\mathsf{DS\text{-}Trans}(\mathbf{\Gamma})$ and interacts with it as follows:

1. Let $\omega_i \leftarrow \mathsf{Param}_i(\mathsf{par})$. $\mathcal{B}$ is given $(\mathbb{G}, [\mathbf{A}]_\eta, [\mathbf{B}]_{3-\eta}, \{\mathbf{a}^*_i\}_{i\in[\ell,\zeta]}, \{\mathbf{b}^*_i\}_{i\in[\ell+1,\zeta]}, \{[\mathbf{W}^\top_{t,j}\mathbf{A}]_\eta, [\mathbf{W}_{t,j}\mathbf{B}]_{3-\eta}\}_{j\in[\omega_t]})$. It then samples $\mathbb{W}_i = (\mathbf{W}_{i,1}, \ldots, \mathbf{W}_{i,\omega_i}) \leftarrow (\mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)})^{\omega_i}$ for $i \in [d]\backslash t$.
2. $\mathcal{B}$ gives to $\mathcal{A}$ the following elements: $\mathbb{G}, [\mathbf{A}]_\eta, [\mathbf{B}]_{3-\eta}, \{\mathbf{a}^*_i\}_{i\in[\ell,\zeta]}, \{\mathbf{b}^*_i\}_{i\in[\ell+1,\zeta]}$, together with $\{[\mathbf{W}^\top_{i,j}\mathbf{A}]_\eta, [\mathbf{W}_{i,j}\mathbf{B}]_{3-\eta}\}_{i\in[d],j\in[\omega_i]}$
3. For $\mathcal{A}$'s query to $\mathcal{O}_{\bar{\mathcal{X}}}$ on (i_x, x), $\mathcal{B}$ replies as follows:

$\underline{\mathsf{G}_{\beta}^{(\zeta,\ell)\text{-KE-ind}}}$
$\overline{\omega_i \leftarrow \mathsf{Param}_i(\mathsf{par}),\ \ \mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda)}$
$\overline{\mathbf{A}}, \overline{\mathbf{B}} \leftarrow \mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)},\ \ \mathbb{W}_i = (\mathbf{W}_{i,1}, \ldots, \mathbf{W}_{i,\omega_i}) \leftarrow (\mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)})^{\omega_i}$
$P = (\mathbb{G}, [\mathbf{A}]_\eta, [\mathbf{B}]_{3-\eta}, \{\mathbf{a}_i^*\}_{i\in[\ell,\zeta]}, \{\mathbf{b}_i^*\}_{i\in[\ell+1,\zeta]}, \{[\mathbf{W}_{i,j}^\top \mathbf{A}]_\eta, [\mathbf{W}_{i,j}\mathbf{B}]_{3-\eta}\}_{i\in[d],j\in[\omega_i]})$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\bar{\mathcal{X}}}(\cdot),\mathcal{O}_{\bar{\mathcal{Y}}}(\cdot,\cdot)}(P)$

$\underline{\mathcal{O}_{\bar{\mathcal{X}}}(\cdot)}$
Input: $(i_x, x) \in \bar{\mathcal{X}}_\kappa$
$(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}^{(i_x)})) \leftarrow \mathsf{EncCt}_{i_x}(x)$
$\mathbf{c}_0 \leftarrow \mathsf{span}(\mathbf{A}, \mathbf{a}_1, \ldots, \mathbf{a}_\ell),\ \ \mathbf{s}_1, \ldots, \mathbf{s}_{n_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$
$\mathbf{S} = (\mathbf{c}_0, \mathbf{A}\mathbf{s}_1, \ldots, \mathbf{A}\mathbf{s}_{n_1}),\ \ \widehat{\mathbf{S}} = (\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2})$
Output: $([\mathbf{S}]_\eta, [\mathbf{c}(\mathbf{S}, \widehat{\mathbf{S}}, \mathbb{W}_{i_x})]_\eta)$

$\underline{\mathcal{O}_{\bar{\mathcal{Y}}}(\cdot,\cdot)}$
Input: $(i_y, y) \in \bar{\mathcal{Y}}_\kappa$ and $\mathbf{h} \in \mathbb{Z}_p^{k+\zeta}$
$(m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w}^{(i_y)})) \leftarrow \mathsf{EncKey}_{i_y}(y)$
$\mu \leftarrow \mathbb{Z}_p,\ \ \mathbf{r}_1, \ldots, \mathbf{r}_{m_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{m_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$
$\mathbf{R} = (\mathbf{B}\mathbf{r}_1, \ldots, \mathbf{B}\mathbf{r}_{m_1}),\ \ \widehat{\mathbf{R}} = (\mathbf{h} + \boxed{\beta\mu\mathbf{a}_\ell^*}, \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{m_2})$
Output: $([\mathbf{R}]_{3-\eta}, [\mathbf{k}(\mathbf{R}, \widehat{\mathbf{R}}, \mathbb{W}_{i_y})]_{3-\eta})$

Fig. 2. (ζ, ℓ)-KE-ind game for DS-Trans($\mathbf{\Gamma}$).

- If $i_x = t$, $\mathcal{B}$ queries its own oracle $\mathcal{O}_{\mathcal{X}^{(t)}}$ on x and gives the reply, which is $([\mathbf{S}]_\eta, [\mathbf{c}(\mathbf{S}, \widehat{\mathbf{S}}, \mathbb{W}_t)]_\eta)$, to $\mathcal{A}$.
- If $i_x \neq t$, $\mathcal{B}$ computes $\mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}^{(i_x)}), \mathbf{S}$, and $\widehat{\mathbf{S}}$ as show below, and gives $([\mathbf{S}]_\eta, [\mathbf{c}(\mathbf{S}, \widehat{\mathbf{S}}, \mathbb{W}_{i_x})]_\eta)$ to $\mathcal{A}$:

$$(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w}^{(i_x)})) \leftarrow \mathsf{EncCt}_{i_x}(x),\ \ \mathbf{c}_0 \leftarrow \mathsf{Ker}(\mathbf{a}_{\ell+1}^*, \ldots, \mathbf{a}_\zeta^*),$$
$$\mathbf{s}_1, \ldots, \mathbf{s}_{n_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$$
$$\mathbf{S} = (\mathbf{c}_0, \mathbf{A}\mathbf{s}_1, \ldots, \mathbf{A}\mathbf{s}_{n_1}),\ \ \widehat{\mathbf{S}} = (\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2}).$$

  Note that $\mathsf{span}(\mathbf{A}, \mathbf{a}_1, \ldots, \mathbf{a}_\ell) = \mathsf{Ker}(\mathbf{a}_{\ell+1}^*, \ldots, \mathbf{a}_\zeta^*)$.

4. For $\mathcal{A}$'s query to $\mathcal{O}_{\bar{\mathcal{Y}}}$ on (i_y, y), $\mathcal{B}$ replies as follows:
   - If $i_y = t$, $\mathcal{B}$ queries its own oracle $\mathcal{O}_{\mathcal{Y}^{(t)}}$ on y and gives the reply, which is $([\mathbf{R}]_{3-\eta}, [\mathbf{k}(\mathbf{R}, \widehat{\mathbf{R}}, \mathbb{W}_t)]_{3-\eta})$, to $\mathcal{A}$. Note that the first element of $\widehat{\mathbf{R}}$ is $\mathbf{h}$ (if $\beta = 0$) or $\mathbf{h} + \mu\mathbf{a}_\ell^*$ (if $\beta = 1$).
   - If $i_y \neq t$, $\mathcal{B}$ aborts the interaction with $\mathcal{A}$ and outputs a random bit β'
5. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

In the above experiment, $\mathcal{B}$ correctly simulates $\mathcal{O}_{\bar{\mathcal{X}}}$. Since $\mathcal{B}$ aborts the experiment if $i_y \neq t$, we focus on the case of $i_y = t$, which occurs with probability $1/d$. Note that since $i_x = t \Rightarrow \mathsf{P}^{(t)}(x, y) = 0$ from the game condition for DS-Trans($\mathbf{\Gamma}$), $\mathcal{B}$ follow the game condition for Γ_t. If $\beta = 0$ in the KE-ind game for Γ_t, $\mathcal{A}$'s view corresponds to that in $\mathsf{G}_0^{(\zeta,\ell)\text{-KE-ind}}$, and it corresponds to $\mathsf{G}_1^{(\zeta,\ell)\text{-KE-ind}}$ otherwise. Thus, we have $\Pr[i_y = t] \cdot \mathsf{Adv}^{(\zeta,\ell)\text{-KE-ind}}_{\mathcal{A},\mathsf{DS\text{-}Trans}(\mathbf{\Gamma})}(\lambda) + \Pr[i_y \neq t] \cdot 0 \leq \mathsf{Adv}^{(\zeta,\ell)\text{-KE-ind}}_{\mathcal{B},\Gamma_t}(\lambda) \leq \max_{i\in[d]} \mathsf{Adv}^{(\zeta,\ell)\text{-KE-ind}}_{\mathcal{B},\Gamma_i}(\lambda)$. This concludes the proof. □

4.2 Dual Predicates

Recall that the dual 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 $\mathsf{Dual}[\mathsf{P}_\kappa](x,y) = \mathsf{P}_\kappa(y,x)$.

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

- $\mathsf{Param}'(\mathsf{par}) \to \omega'$: Run $\omega \leftarrow \mathsf{Param}(\mathsf{par})$ and output $\omega + 1$. This specifies common variables $\mathbf{w}' = (w_0, w_1, \ldots, w_\omega)$, where w_0 is a new common variable.
- $\mathsf{EncCt}'(x) \to (n_1', n_2', \mathbf{c}'(\mathbf{s}', \hat{\mathbf{s}}', \mathbf{w}'))$:
  - Run $(m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})) \leftarrow \mathsf{EncKey}(x)$. Let s_{new} be a new special non-lone variable. Polynomials $\mathbf{c}'(\mathbf{s}', \hat{\mathbf{s}}', \mathbf{w}')$ are defined the same as $\mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})$ except that α is replaced with $s_{\mathsf{new}} w_0$.
  - Define $n_1' = m_1$, $n_2' = m_2$, $\mathbf{s}' = (s_{\mathsf{new}}, \mathbf{r})$, and $\hat{\mathbf{s}}' = \hat{\mathbf{r}}_{-\alpha}$.
- $\mathsf{EncKey}'(y) \to (m_1', m_2', \mathbf{k}'(\mathbf{r}', \hat{\mathbf{r}}', \mathbf{w}))$:
  - Run $(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})) \leftarrow \mathsf{EncCt}(y)$. Let α_{new} be a new special lone variable. Polynomials $\mathbf{k}'(\mathbf{r}', \hat{\mathbf{r}}', \mathbf{w}')$ are defined the same as $\mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})$ except that a polynomial $\alpha_{\mathsf{new}} - s_0 w_0$ is added as the first element of $\mathbf{k}'(\mathbf{r}', \hat{\mathbf{r}}', \mathbf{w}')$.
  - Define $m_1' = n_1 + 1$, $m_2' = n_2$, $\mathbf{r}' = \mathbf{s}$, and $\hat{\mathbf{r}}' = (\alpha_{\mathsf{new}}, \hat{\mathbf{s}})$.
- $\mathsf{Pair}'(x,y) \to (\mathbf{E}', \bar{\mathbf{E}}')$ and correctness:
  - Run $(\mathbf{E}, \bar{\mathbf{E}}) \leftarrow \mathsf{Pair}(y,x)$. Define $\mathbf{E}' = \begin{pmatrix} 1 \\ \bar{\mathbf{E}}^\top \end{pmatrix}$ and $\bar{\mathbf{E}}' = \mathbf{E}^\top$.
  - For correctness, we have

$$\begin{aligned}\mathbf{s}'\mathbf{E}'\mathbf{k}'^\top + \mathbf{c}'\bar{\mathbf{E}}'\mathbf{r}'^\top =& (s_{\mathsf{new}}, \mathbf{r}) \begin{pmatrix} 1 \\ \bar{\mathbf{E}}^\top \end{pmatrix} (\alpha_{\mathsf{new}} - s_0 w_0, \mathbf{c})^\top + \mathbf{k}|_{\alpha \mapsto s_{\mathsf{new}} w_0} \mathbf{E}^\top \mathbf{s}^\top \\ =& s_{\mathsf{new}} \alpha_{\mathsf{new}} - s_{\mathsf{new}} s_0 w_0 + s_{\mathsf{new}} s_0 w_0 = s_{\mathsf{new}} \alpha_{\mathsf{new}}.\end{aligned}$$

Theorem 6 (**(ζ,ℓ)-KE-ind *of* $\mathsf{Dual\text{-}Trans}(\Gamma)$**). *Let $2 \le \ell \le \zeta$. If Γ satisfies $(\zeta, \ell-1)$-KE-ind, then $\mathsf{Dual\text{-}Trans}(\Gamma)$ satisfies (ζ,ℓ)-KE-ind under the $\mathcal{D}_k$-MDDH assumption. More precisely, for all PPT adversaries $\mathcal{A}$, there exist PPT adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$ such that*

$$\mathsf{Adv}^{(\zeta,\ell)\text{-KE-ind}}_{\mathcal{A},\mathsf{Dual\text{-}Trans}(\Gamma)}(\lambda) \le \mathsf{Adv}^{(\zeta,\ell-1)\text{-KE-ind}}_{\mathcal{B}_1,\Gamma}(\lambda) + 2\mathsf{Adv}^{\mathcal{D}_k\text{-MDDH}}_{\mathcal{B}_2}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof. For $\beta \in \{0,1\}$, we can describe the (ζ,ℓ)-KE-ind game $\mathsf{G}^{(\zeta,\ell)\text{-KE-ind}}_\beta$ for $\mathsf{Dual\text{-}Trans}(\Gamma)$ as shown in Fig. 3. To show this theorem, we consider two intermediate hybrids H_1 and H_2, which are also described in Fig. 3. That is, H_1 (resp. H_2) is defined the same as $\mathsf{G}^{(\zeta,\ell)\text{-KE-ind}}_0$ (resp. $\mathsf{G}^{(\zeta,\ell)\text{-KE-ind}}_1$) except that $\mathbf{d}_0$, the first elements of $\mathbf{R}$ generated in $\mathcal{O}_{\bar{y}}$, is set as $\mathbf{d}_0 \leftarrow \mathsf{span}(\mathbf{B}, \mathbf{b}_1, \ldots, \mathbf{b}_{\ell-1})$ instead of $\mathbf{B}\mathbf{r}_0$ where $\mathbf{r}_0 \leftarrow \mathbb{Z}_p^k$. From Lemma 1,2,3 below, we have $\mathsf{G}^{(\zeta,\ell)\text{-KE-ind}}_0 \approx_c \mathsf{H}_1 \approx_c \mathsf{H}_2 \approx_c \mathsf{G}^{(\zeta,\ell)\text{-KE-ind}}_1$. This concludes the proof. □

Lemma 1. *For all PPT adversaries $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}$ such that $|\Pr[\langle \mathcal{A}, \mathsf{G}^{(\zeta,\ell)\text{-KE-ind}}_0 \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{H}_1 \rangle = 1]| \le \mathsf{Adv}^{\mathcal{D}_k\text{-MDDH}}_{\mathcal{B}}(\lambda)$.*

$\mathsf{G} \in \left\{ \mathsf{G}_0^{(\zeta,\ell)\text{-KE-ind}}, \boxed{\mathsf{H}_1}, \boxed{\mathsf{H}_2}, \mathsf{G}_1^{(\zeta,\ell)\text{-KE-ind}} \right\}$

$\underline{\mathsf{G}}$

$\omega \leftarrow \mathsf{Param}(\mathsf{par}),\ \ \mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda)$

$\overline{\mathbf{A}}, \overline{\mathbf{B}} \leftarrow \mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)},\ \ \mathbb{W} = (\mathbf{W}_0^\top, \mathbf{W}_1^\top, \ldots, \mathbf{W}_\omega^\top) \leftarrow (\mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)})^{\omega+1}$

$P = (\mathbb{G}, [\mathbf{A}]_\eta, [\mathbf{B}]_{3-\eta}, \{\mathbf{a}_i^*\}_{i\in[\ell,\zeta]}, \{\mathbf{b}_i^*\}_{i\in[\ell+1,\zeta]}, \{[\mathbf{W}_i^\top \mathbf{A}]_\eta, [\mathbf{W}_i \mathbf{B}]_{3-\eta}\}_{i\in[\omega]^+})$

$\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\bar{\mathfrak{X}}}(\cdot), \mathcal{O}_{\bar{\mathfrak{Y}}}(\cdot,\cdot)}(P)$

$\underline{\mathcal{O}_{\bar{\mathfrak{X}}}(\cdot)}$

Input: $x \in \bar{\mathfrak{X}}_\kappa$

$(m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})) \leftarrow \mathsf{EncKey}(x)$

$\mathbf{c}_0 \leftarrow \mathsf{span}(\mathbf{A}, \mathbf{a}_1, \ldots, \mathbf{a}_\ell),\ \ \mathbf{s}_1, \ldots, \mathbf{s}_{m_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{m_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$

$\mathbf{S} = (\mathbf{A}\mathbf{s}_1, \ldots, \mathbf{A}\mathbf{s}_{m_1}),\ \ \widehat{\mathbf{S}} = (\mathbf{W}_0^\top \mathbf{c}_0, \hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{m_2})$

Output: $([\mathbf{c}_0]_\eta, [\mathbf{S}]_\eta, [\mathbf{k}(\mathbf{S}, \widehat{\mathbf{S}}, \mathbb{W})]_\eta)$

$\underline{\mathcal{O}_{\bar{\mathfrak{Y}}}(\cdot,\cdot)}$

Input: $y \in \bar{\mathfrak{Y}}_\kappa$ and $\mathbf{h} \in \mathbb{Z}_p^{k+\zeta}$

$(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})) \leftarrow \mathsf{EncCt}(y),\ \mu \leftarrow \mathbb{Z}_p,\ \ \mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{n_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{n_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$

$\mathbf{d}_0 = \mathbf{B}\mathbf{r}_0,\ \ \boxed{\mathbf{d}_0 \leftarrow \mathsf{span}(\mathbf{B}, \mathbf{b}_1, \ldots, \mathbf{b}_{\ell-1})}$

$\mathbf{R} = (\mathbf{d}_0, \mathbf{B}\mathbf{r}_1, \ldots, \mathbf{B}\mathbf{r}_{n_1}),\ \ \widehat{\mathbf{R}} = (\hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{n_2})$

Output: $([\mathbf{h} + \boxed{\mu \mathbf{a}_\ell^*} - \mathbf{W}_0 \mathbf{d}_0]_{3-\eta}, [\mathbf{R}]_{3-\eta}, [\mathbf{c}(\mathbf{R}, \widehat{\mathbf{R}}, \mathbb{W})]_{3-\eta})$

Fig. 3. (ζ, ℓ)-KE-ind game for Dual-Trans(Γ).

Proof. We describe the reduction algorithm $\mathcal{B}$. $\mathcal{B}$ is given an instance of $\mathcal{U}_{k+\ell-1,k}$ problem, $(\mathbb{G}, [\mathbf{M}]_{3-\eta}, [\mathbf{t}_\beta]_{3-\eta})$ where $\mathbf{t}_0 = \mathbf{M}\mathbf{u}$ and $\mathbf{t}_1 = \mathbf{v}$, where $\mathbf{u} \leftarrow \mathbb{Z}_p^k$ and $\mathbf{v} \leftarrow \mathbb{Z}_p^{k+\ell-1}$. Then, $\mathcal{B}$ chooses $\mathbf{X} \leftarrow \mathsf{GL}_{k+\zeta}(\mathbb{Z}_p)$ and sets

$$\overline{\mathbf{B}} = \mathbf{X} \begin{pmatrix} \widehat{\mathbf{M}} & \\ \underline{\mathbf{M}}\ \mathbf{I}_{\ell-1} & \\ & \mathbf{I}_{\zeta-\ell+1} \end{pmatrix},\ \ (\overline{\mathbf{B}}^\top)^{-1} = (\mathbf{X}^\top)^{-1} \begin{pmatrix} (\widehat{\mathbf{M}}^\top)^{-1} & -(\widehat{\mathbf{M}}^\top)^{-1}\underline{\mathbf{M}}^\top & \\ & \mathbf{I}_{\ell-1} & \\ & & \mathbf{I}_{\zeta-\ell+1} \end{pmatrix},$$

where $\widehat{\mathbf{M}}$ is the matrix consisting of the first k rows of $\mathbf{M}$, and $\underline{\mathbf{M}}$ is that consisting of the last $\ell - 1$ rows of $\mathbf{M}$. Then, $\mathcal{B}$ can compute

$$[\mathbf{B}]_{3-\eta} = \left[\mathbf{X} \begin{pmatrix} \mathbf{M} \\ \mathbf{O} \end{pmatrix}\right]_{3-\eta},\ \ (\mathbf{b}_{\ell+1}^* || \ldots || \mathbf{b}_\zeta^*) = (\mathbf{X}^\top)^{-1} \begin{pmatrix} \mathbf{O} \\ \mathbf{I}_{\zeta-\ell} \end{pmatrix}.$$

$\mathcal{B}$ generates $\overline{\mathbf{A}}$ and $\mathbb{W}$ by itself and computes the input P for $\mathcal{A}$ from them. When $\mathcal{A}$ queries $\mathcal{O}_{\bar{\mathfrak{X}}}$, $\mathcal{B}$ replies honestly as shown in Fig. 3. When $\mathcal{A}$ queries $\mathcal{O}_{\bar{\mathfrak{Y}}}$, $\mathcal{B}$ replies honestly except that it sets

$$[\mathbf{d}_0]_{3-\eta} = \left[\mathbf{X} \begin{pmatrix} \mathbf{t}_\beta \\ \mathbf{0} \end{pmatrix}\right]_{3-\eta},\ \ [\mathbf{R}]_{3-\eta} = [(\mathbf{d}_0, \mathbf{B}\mathbf{r}_1, \ldots, \mathbf{B}\mathbf{r}_{m_1})]_{3-\eta}.$$

Now since we can write $\mathbf{t}_\beta = \begin{pmatrix} \widehat{\mathbf{M}} \\ \underline{\mathbf{M}} \end{pmatrix} \mathbf{u}_1 + \beta \begin{pmatrix} \mathbf{O} \\ \mathbf{I}_{\ell-1} \end{pmatrix} \mathbf{u}_2$, where $\mathbf{u}_1 \leftarrow \mathbb{Z}_p^k$ and $\mathbf{u}_2 \leftarrow \mathbb{Z}_p^{\ell-1}$, we have that $\mathbf{d}_0$ is uniformly distributed in $\mathsf{span}(\mathbf{B})$ if $\beta = 0$, and in $\mathsf{span}(\mathbf{B}, \mathbf{b}_1, \ldots, \mathbf{b}_{\ell-1})$ otherwise. Thus, the view of $\mathcal{A}$ corresponds to $\mathsf{G}_0^{(\zeta,\ell)\text{-KE-ind}}$ if $\beta = 0$, and H_1 otherwise. This concludes the proof. □

Lemma 2. *For all PPT adversaries $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}$ such that* $|\Pr[\langle \mathcal{A}, \mathsf{H}_1\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{H}_2\rangle = 1]| \leq \mathsf{Adv}^{(\zeta,\ell-1)\text{-}\mathsf{KE\text{-}ind}}_{\mathcal{B},\Gamma}(\lambda) + 2^{-\Omega(\lambda)}$.

Proof. We show that the outputs of $\mathcal{O}_{\bar{\mathcal{Y}}}$ in H_1 and H_2 are computationally indistinguishable if the PES Γ for P_κ satisfies $(\zeta, \ell-1)$-KE-ind. We construct a PPT adversary $\mathcal{B}$ against $(\zeta, \ell-1)$-KE-ind of Γ that internally runs a PPT distinguisher $\mathcal{A}$ between H_1 and H_2. $\mathcal{B}$ behaves as follows.

1. $\mathcal{B}$ is given an input of $(\zeta, \ell-1)$-KE-ind game for Γ, $(\mathbb{G}, [\mathbf{M}]_{3-\eta}, [\mathbf{N}]_\eta, \{\mathbf{m}_i^*\}_{i\in[\ell-1,\zeta]}, \{\mathbf{n}_i^*\}_{i\in[\ell,\zeta]}, \{[\mathbf{V}_i^\top \mathbf{M}]_{3-\eta}, [\mathbf{V}_i\mathbf{N}]_\eta\}_{i\in[\omega]})$. $\mathcal{B}$ implicitly defines that $\mathbf{A} = \mathbf{N}$, $\mathbf{B} = \mathbf{M}$, and $\mathbf{W}_i = \mathbf{V}_i^\top$ for $i \in [\omega]$.
2. $\mathcal{B}$ samples $\mathbf{W}_0 \leftarrow \mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)}$ and gives $P = (\mathbb{G}, [\mathbf{A}]_\eta, [\mathbf{B}]_{3-\eta}, \{\mathbf{a}_i^*\}_{i\in[\ell,\zeta]}, \{\mathbf{b}_i^*\}_{i\in[\ell+1,\zeta]}, \{[\mathbf{W}_i^\top \mathbf{A}]_\eta, [\mathbf{W}_i\mathbf{B}]_{3-\eta}\}_{i\in[\omega]^+})$ to $\mathcal{A}$.
3. For $\mathcal{A}$'s query to $\mathcal{O}_{\bar{\mathcal{X}}}$ on x, $\mathcal{B}$ samples $\mathbf{c}_0 \leftarrow \mathsf{Ker}(\mathbf{a}_{\ell+1}^*, \ldots, \mathbf{a}_\zeta^*)$ and queries its own oracle $\mathcal{O}_{\mathcal{Y}}$ on $(x, \mathbf{W}_0^\top \mathbf{c}_0)$ to obtain $([\mathbf{T}]_\eta, [\mathbf{k}(\mathbf{T}, \widehat{\mathbf{T}}, \mathbb{V})]_\eta)$, where

$$\mathbf{T} = (\mathbf{N}\mathbf{t}_0, \mathbf{N}\mathbf{t}_1, \ldots, \mathbf{N}\mathbf{t}_{m_1}) = (\mathbf{A}\mathbf{t}_0, \mathbf{A}\mathbf{t}_1, \ldots, \mathbf{A}\mathbf{t}_{m_1}),$$
$$\widehat{\mathbf{T}} = (\mathbf{W}_0^\top \mathbf{c}_0 + \beta\hat{\mu}\mathbf{m}_{\ell-1}^*, \hat{\mathbf{t}}_1, \ldots, \hat{\mathbf{t}}_{m_2}) = (\mathbf{W}_0^\top \mathbf{c}_0 + \beta\hat{\mu}\mathbf{b}_{\ell-1}^*, \hat{\mathbf{t}}_1, \ldots, \hat{\mathbf{t}}_{m_2}),$$
$$\mathbb{V} = (\mathbf{V}_1, \ldots, \mathbf{V}_\omega) = (\mathbf{W}_1^\top, \ldots, \mathbf{W}_\omega^\top).$$

   Note that $\hat{\mu}$ is a random value in $\mathbb{Z}_p$ chosen by $\mathcal{O}_{\mathcal{Y}}$. $\mathcal{B}$ implicitly defines that $\mathbf{s}_i = \mathbf{t}_i$ for $i \in [m_1]^+$, $\hat{\mathbf{s}}_i = \hat{\mathbf{t}}_i$ for $i \in [m_2]$, $\mathbf{S} = \mathbf{T}$, $\widehat{\mathbf{S}} = \widehat{\mathbf{T}}$, and $\mathbb{W} = \mathbb{V}$. $\mathcal{B}$ replies $([\mathbf{c}_0]_\eta, [\mathbf{S}]_\eta, [\mathbf{k}(\mathbf{S}, \widehat{\mathbf{S}}, \mathbb{W})]_\eta)$ to $\mathcal{A}$. Note that $\mathsf{span}(\mathbf{A}, \mathbf{a}_1, \ldots, \mathbf{a}_\ell) = \mathsf{Ker}(\mathbf{a}_{\ell+1}^*, \ldots, \mathbf{a}_\zeta^*)$.
4. For $\mathcal{A}$'s query to $\mathcal{O}_{\bar{\mathcal{Y}}}$ with y and $\mathbf{h}$, $\mathcal{B}$ queries its own oracle $\mathcal{O}_{\mathcal{X}}$ on y to obtain $([\mathbf{U}]_{3-\eta}, [\mathbf{c}(\mathbf{U}, \widehat{\mathbf{U}}, \mathbb{V})]_{3-\eta})$, where

$$\mathbf{U} = (\mathbf{o}_0, \mathbf{M}\mathbf{u}_1, \ldots, \mathbf{M}\mathbf{u}_{n_1}) = (\mathbf{o}_0, \mathbf{B}\mathbf{u}_1, \ldots, \mathbf{B}\mathbf{u}_{n_1}), \quad \widehat{\mathbf{U}} = (\hat{\mathbf{u}}_1, \ldots, \hat{\mathbf{u}}_{n_2}).$$

   Note that $\mathbf{o}_0$ is randomly distributed in $\mathsf{span}(\mathbf{M}, \mathbf{m}_1, \ldots, \mathbf{m}_{\ell-1})$, which equals to $\mathsf{span}(\mathbf{B}, \mathbf{b}_1, \ldots, \mathbf{b}_{\ell-1})$. $\mathcal{B}$ implicitly defines that $\mathbf{r}_i = \mathbf{u}_i$ for $i \in [n_1]$, $\hat{\mathbf{r}}_i = \hat{\mathbf{u}}_i$ for $i \in [n_2]$, $\mathbf{R} = \mathbf{U}$, $\widehat{\mathbf{R}} = \widehat{\mathbf{U}}$, and $\mathbf{d}_0 = \mathbf{o}_0$. $\mathcal{B}$ replies $([\mathbf{h} - \mathbf{W}_0\mathbf{d}_0]_{3-\eta}, [\mathbf{R}]_{3-\eta}, [\mathbf{c}(\mathbf{R}, \widehat{\mathbf{R}}, \mathbb{W})]_{3-\eta})$ to $\mathcal{A}$.
5. $\mathcal{B}$ outputs $\mathcal{A}$'s output as it is.

At a glance, this simulation seems that the distribution of the reply from $\mathcal{O}_{\bar{\mathcal{X}}}$ is changed. However, entire views of $\mathcal{A}$ correspond to H_1 and H_2. To see this, we redefine $\mathbf{W}_0$ as $\mathbf{W}_0 = \widetilde{\mathbf{W}}_0 - \frac{\beta\hat{\mu}}{\mathbf{a}_\ell^{*\top}\mathbf{c}_0}\mathbf{a}_\ell^*\mathbf{b}_{\ell-1}^{*\top}$ where $\widetilde{\mathbf{W}}_0 \leftarrow \mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)}$. Clearly, this does not change the distribution of $\mathbf{W}_0$. This affects $\mathcal{A}$'s view as follows:

$$P: \ \mathbf{W}_0^\top \mathbf{A} = \widetilde{\mathbf{W}}_0^\top \mathbf{A}, \ \ \mathbf{W}_0\mathbf{B} = \widetilde{\mathbf{W}}_0\mathbf{B}.$$
$$\mathcal{O}_{\bar{\mathcal{X}}}: \ \mathbf{W}_0^\top \mathbf{c}_0 + \beta\hat{\mu}\mathbf{b}_{\ell-1}^* = \widetilde{\mathbf{W}}_0^\top \mathbf{c}_0.$$
$$\mathcal{O}_{\bar{\mathcal{Y}}}: \ \mathbf{h} - \mathbf{W}_0\mathbf{d}_0 = \mathbf{h} - \widetilde{\mathbf{W}}_0\mathbf{d}_0 + \frac{\beta\hat{\mu}\mathbf{b}_{\ell-1}^{*\top}\mathbf{d}_0}{\mathbf{a}_\ell^{*\top}\mathbf{c}_0}\mathbf{a}_\ell^* = \mathbf{h} - \widetilde{\mathbf{W}}_0\mathbf{d}_0 + \beta\mu\mathbf{a}_\ell^*.$$

Because $\hat{\mu}$ is randomly distributed in $\mathbb{Z}_p$, we can set $\mu = \frac{\hat{\mu}\mathbf{b}_{\ell-1}^{*\top}\mathbf{d}_0}{\mathbf{a}_\ell^{*\top}\mathbf{c}_0}$ if $\mathbf{b}_{\ell-1}^{*\top}\mathbf{d}_0 \neq 0$ and $\mathbf{a}_\ell^{*\top}\mathbf{c}_0 \neq 0$. Since $\mathbf{c}_0$ and $\mathbf{d}_0$ are randomly distributed in $\mathsf{span}(\mathbf{A}, \mathbf{a}_1, \ldots, \mathbf{a}_\ell)$ and $\mathsf{span}(\mathbf{B}, \mathbf{b}_1, \ldots, \mathbf{b}_{\ell-1})$, respectively, this is the case with an overwhelming probability. Thus, $\mathcal{A}$'s view corresponds to H_1 if $\beta = 0$ in the (ζ, ℓ)-KE-ind game of Γ, and it corresponds to H_2 otherwise. This concludes the proof. □

Lemma 3. *For all PPT adversaries $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}$ such that* $|\Pr[\langle \mathcal{A}, \mathsf{H}_2\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_1^{(\zeta,\ell)\text{-KE-ind}}\rangle = 1]| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathcal{D}_k\text{-MDDH}}(\lambda)$.

The proof of Lemma 3 is similar to Lemma 1, and hence we omit it here.

4.3 Key-Policy Augmentation

Definition 10 (Key-Policy Augmentation). A predicate family for key-policy Boolean formula augmentation over a single predicate family $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0,1\}$, denoted by $\mathsf{KBF1}[\mathsf{P}_\kappa] : \bar{\mathcal{X}}_\kappa \times \bar{\mathcal{Y}}_\kappa \to \{0,1\}$, where $\bar{\mathcal{X}}_\kappa = \mathcal{X}_\kappa$ and $\bar{\mathcal{Y}}_\kappa = \bigcup_{i\in\mathbb{N}}(\mathcal{Y}_\kappa^i \times \mathcal{F}_i)$, where $\mathcal{F}_i$ consists of all monotone Boolean formulae with input length i, is defined as follows. For $x \in \bar{\mathcal{X}}_\kappa$ and $y = ((y_1, \ldots, y_n), f) \in \bar{\mathcal{Y}}_\kappa$ where $f : \{0,1\}^n \to \{0,1\}$, we define

$$\mathsf{KBF1}[\mathsf{P}_\kappa](x, y) = f\big(\mathsf{P}_\kappa(x, y_1), \ldots, \mathsf{P}_\kappa(x, y_n)\big).$$

We use $\mathsf{KBF1}_{\mathsf{OR}}[\mathsf{P}_\kappa]$ (resp. $\mathsf{KBF1}_{\mathsf{AND}}[\mathsf{P}_\kappa]$) to denote a predicate family that is the same as $\mathsf{KBF1}[\mathsf{P}_\kappa]$ except that $\mathcal{F}_i$ in $\bar{\mathcal{Y}}_\kappa$ consists of monotone Boolean formulae whose all gates are OR (resp. AND) gates. The "1" in KBF1 refers to the property that the augmentation is over *one* predicate family. An augmentation over a *set* of predicate families follows analogously to [9], and we defer to Sect. 6 (and more details in the full version). In *dynamic* compositions, f can be chosen freely (as opposed to static ones, where f is fixed). *Unbounded* compositions mean n is unbounded.

PES for $\mathsf{KBF1}[\mathsf{P}_\kappa]$. Let $\Gamma = (\mathsf{Param}, \mathsf{EncCt}, \mathsf{EncKey}, \mathsf{Pair})$ be a PES for P_κ. We construct a PES for $\mathsf{KBF1}[\mathsf{P}_\kappa]$, denoted by $\mathsf{KBF1\text{-}Trans}(\Gamma)$ as follows. Let $\mathsf{Share}_{\mathsf{p}}$ be the linear secret sharing algorithm on polynomials defined in Fig. 4.

- $\mathsf{Param}'(\mathsf{par}) = \mathsf{Param}(\mathsf{par})$ and $\mathsf{EncCt}'(x) = \mathsf{EncCt}(x)$
- $\mathsf{EncKey}'((y_1, \ldots, y_n), f) \to (m_1', m_2', \mathbf{k}'(\mathbf{r}', \hat{\mathbf{r}}', \mathbf{w}))$:
  - For $i \in [n]$, run $\mathsf{EncKey}(y_i)$ to obtain n sets of polynomials $\mathbf{k}^{(1)}, \ldots, \mathbf{k}^{(n)}$, where $\mathbf{k}^{(i)} = \mathbf{k}(\mathbf{r}^{(i)}, \hat{\mathbf{r}}^{(i)}, \mathbf{w})$.
  - Let τ be a number of AND gates in f. Let α_{new} be a new special lone variable and $\mathbf{u} = (u_1, \ldots, u_\tau)$ be new lone variables. Let $\sigma_1, \ldots, \sigma_n$ be polynomials that are an output of $\mathsf{Share}_{\mathsf{p}}(f, \alpha_{\mathsf{new}}, \mathbf{u})$. A new set of polynomials $\mathbf{k}'^{(i)}$ is defined the same as $\mathbf{k}^{(i)}$ except that the variable $\alpha^{(i)}$ in each polynomial is replaced with σ_i.
  - Define $m_1' = nm_1$, $m_2' = \tau + nm_2$, and $\mathbf{k}'(\mathbf{r}', \hat{\mathbf{r}}', \mathbf{w}) = (\mathbf{k}'^{(1)}, \ldots, \mathbf{k}'^{(n)})$. Note that $\mathbf{r}' = (\mathbf{r}^{(1)}, \ldots, \mathbf{r}^{(n)})$ and $\hat{\mathbf{r}}' = (\alpha_{\mathsf{new}}, \mathbf{u}, \hat{\mathbf{r}}^{(1)}_{-\alpha^{(1)}}, \ldots, \hat{\mathbf{r}}^{(n)}_{-\alpha^{(n)}})$.

$\mathsf{Share}_{\mathsf{p}}(f, \alpha, \mathbf{u})$

Input: A monotone Boolean formula $f = (n, w, m, G)$ with τ AND gates, a variable α, and τ variables $\mathbf{u} = (u_1, \ldots, u_\tau)$.

1. Set a variable $\sigma_{\mathsf{out}} = \alpha$ on the output wire.
2. Let $\phi : [m] \to [\tau]$ be a function such that $\phi(i) = |\{j \mid j \leq i \wedge G_1(j) = \text{AND}\}|$, where $G_1(j)$ denotes the first element of $G(j)$. For each AND gate g with incoming wires a, b and an outgoing wire c where a polynomial σ_c is set on c, set new polynomials $\sigma_a = \sigma_c - u_{\phi(g)}$ and $\sigma_b = u_{\phi(g)}$ on a and b, respectively.
3. For each OR gate g with incoming wires a, b and an outgoing wire c where a vector σ_c is set on c, set new polynomials $\sigma_a = \sigma_c$, $\sigma_b = \sigma_c$ on a, b, respectively.
4. Output polynomials $\sigma_1, \ldots, \sigma_n$, which are set on the input wires $1, \ldots, n$.

Fig. 4. Linear secret sharing scheme for Boolean formulae on polynomials.

– $\mathsf{Pair}'(x, y) \to (\mathbf{E}', \bar{\mathbf{E}}')$ and correctness:
  - Let polynomials $\sigma_1, \ldots, \sigma_n$ be an output of $\mathsf{Share}_{\mathsf{p}}(f, \alpha_{\mathsf{new}}, \mathbf{u})$. It is not hard to see that, for all $b = (b_1, \ldots, b_n) \in \{0,1\}^n$ such that $f(b) = 1$, there exists a set $S \subseteq \{i \mid b_i = 1\}$ such that $\sum_{i \in S} \sigma_i = \alpha_{\mathsf{new}}$. Thus, if x and $y = ((y_1, \ldots, y_n), f)$ satisfy $\mathsf{KBF1}[\mathsf{P}_\kappa](x, y) = 1$, there exists $S \subseteq \{i \mid \mathsf{P}_\kappa(x, y_i) = 1\}$ such that $\sum_{i \in S} \sigma_i = \alpha_{\mathsf{new}}$.
  - For $i \in S$, run $\mathsf{Pair}(x, y_i) \to (\mathbf{E}^{(i)}, \bar{\mathbf{E}}^{(i)})$, satisfying $\mathbf{s}\mathbf{E}^{(i)}\mathbf{k}^{(i)\top} + \mathbf{c}\bar{\mathbf{E}}^{(i)}\mathbf{r}^{(i)\top} = \sigma_i s_0$. Then, we can obtain $\sum_{i \in S} \sigma_i s_0 = \alpha_{\mathsf{new}} s_0$ by the linear combination.

Theorem 7 ((ζ, ℓ)-$\mathsf{KE\text{-}ind}$ *of* $\mathsf{KBF1\text{-}Trans}(\Gamma)$)**.** *Let B be the maximum depth of f chosen by $\mathcal{A}$ in the (ζ, ℓ)-$\mathsf{KE\text{-}ind}$ game for $\mathsf{KBF1\text{-}Trans}(\Gamma)$. If Γ satisfies (ζ, ℓ)-$\mathsf{KE\text{-}ind}$, then $\mathsf{KBF1\text{-}Trans}(\Gamma)$ satisfies (ζ, ℓ)-$\mathsf{KE\text{-}ind}$ as long as $B = O(\log \lambda)$. That is, for all PPT adversaries $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}^{(\zeta,\ell)\text{-}\mathsf{KE\text{-}ind}}_{\mathcal{A},\mathsf{KBF1\text{-}Trans}(\Gamma)}(\lambda) \leq 2^{9B+1}\mathsf{Adv}^{(\zeta,\ell)\text{-}\mathsf{KE\text{-}ind}}_{\mathcal{B},\Gamma}(\lambda).$$

We prove Lemma 7 by extending the techniques regarding pebbling arguments that Kowalczyk-Wee [26] have introduced in proving adaptive security of their ABE schemes for formulae with multi-use. We defer the proof to the full version.

Ciphertext-Policy Augmentation. Analogously to [9], for a predicate family P, we define its CP augmentation predicate—denoted as $\mathsf{CBF1}[\mathsf{P}]$—as the dual of $\mathsf{KBF1}[\mathsf{P}']$ where P' is the dual of P. Therefore, we can use the dual conversion—applying two times–sandwiching $\mathsf{KBF1\text{-}Trans}$, to obtain a PES conversion for $\mathsf{CBF1}[\mathsf{P}]$. See the full version for more details.

4.4 Conforming PES for ABE

We can apply our transformations, namely, direct sum, dual, and key-policy augmentation, to a predicate family set $\mathcal{P}_\kappa$ multiple times to obtain a new predicate family P_κ. When we apply a PES to construct an ABE scheme, (ζ', ζ')-$\mathsf{KE\text{-}ind}$ for

some constant ζ' implies the adaptive security of the resulting ABE scheme. The following theorem says that if we have predicate families $\mathcal{P}_\kappa = (\mathsf{P}^{(1)}_{\kappa_1}, \ldots, \mathsf{P}^{(d)}_{\kappa_d})$ that satisfy (ζ, ℓ)-KE-ind for all constants $\ell, \zeta \in \mathbb{N}$, we can construct an ABE scheme for a predicate family P_κ obtained by applying the above transformations to $\mathcal{P}_\kappa$ arbitrarily many times.

To state the theorem formally, we define a composed predicate set $f_c(\mathcal{P}_\kappa)$ for a predicate family set $\mathcal{P}_\kappa = (\mathsf{P}^{(1)}_{\kappa_1}, \ldots, \mathsf{P}^{(d)}_{\kappa_d})$. Let $\bar{\mathcal{P}}_\kappa$ be a predicate family set that consists of all predicate families obtained by applying one of transformations, $(\mathsf{DS}, \mathsf{Dual}, \mathsf{KBF1})$, to $\mathcal{P}_\kappa$. That is, $\bar{\mathcal{P}}_\kappa = (\mathsf{DS}[\mathcal{P}_\kappa], \{\mathsf{Dual}[\mathsf{P}^{(i)}_{\kappa_i}]\}_{i\in[d]}, \{\mathsf{KBF1}[\mathsf{P}^{(i)}_{\kappa_i}]\}_{i\in[d]})$ (we do not consider DS for a subset of $\mathcal{P}_\kappa$, because it can be embedded into $\mathsf{DS}[\mathcal{P}_\kappa]$). 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 8. *For all constant c and predicate family sets $\mathcal{P}_\kappa = (\mathsf{P}^{(1)}_{\kappa_1}, \ldots, \mathsf{P}^{(d)}_{\kappa_d})$, each of whose elements has a corresponding PES with (ζ, ℓ)-KE-ind for all constants $\zeta, \ell \in \mathbb{N}$, there exists a constant ζ' such that $\mathsf{P}_\kappa \in f_c(\mathcal{P}_\kappa)$ has a PES that satisfies (ζ', ζ')-KE-ind under the $\mathcal{D}_k$-MDDH assumption.*

Proof. Let $\mathbf{\Gamma} = (\Gamma_1, \ldots, \Gamma_d)$ be PESs for $(\mathsf{P}^{(1)}_{\kappa_1}, \ldots, \mathsf{P}^{(d)}_{\kappa_d})$, respectively. We can construct a PES Γ for P by applying PES transformations in Sects. 4.1, 4.2 and 4.3 to $\mathbf{\Gamma}$ multiple times. Let δ be the maximum number of Dual-Trans that is applied to each single PES Γ_i to obtain Γ. For instance, δ in the following PES is 2 because the first Γ_2 is transformed by Dual-Trans twice, and the others are transformed by Dual-Trans less that twice.

$$\mathsf{KBF1\text{-}Trans}\left(\mathsf{DS\text{-}Trans}\left(\mathsf{Dual\text{-}Trans}\left(\mathsf{DS\text{-}Trans}\left(\Gamma_1, \mathsf{Dual\text{-}Trans}\left(\Gamma_2\right)\right)\right), \Gamma_2, \Gamma_3\right)\right).$$

Then, it is not hard to see that we can construct Γ with (ζ', ζ')-KE-ind for $\zeta' = \delta + 1$. This directly follows from Theorems 5 to 7. □

Corollary 2. *Let $\mathcal{P}_\kappa = (\mathsf{P}^{(1)}_{\kappa_1}, \ldots, \mathsf{P}^{(d)}_{\kappa_d})$ be predicate families that have a PES with single-variable PMH. Then, we have a PES for $\mathsf{P}_\kappa \in f_c(\mathcal{P}_\kappa)$ with (ζ', ζ')-KE-ind for a constant ζ' under the $\mathcal{D}_k$-MDDH assumption, where $\zeta' - 1$ is the maximum number of Dual applied to each single predicate $\mathsf{P}^{(i)}_{\kappa_i}$ to obtain P_κ.*

This corollary directly follows from Theorems 4 and 8.

5 ABE from PES

In this section, we present our ABE scheme. We can construct an ABE scheme for any predicate family P_κ and a corresponding PES obtained in our framework if the PES satisfies (ζ, ζ)-KE-ind for some constant $\zeta \in \mathbb{N}$.

Construction. Let $\Gamma = (\mathsf{Param}, \mathsf{EncCt}, \mathsf{EncKey}, \mathsf{Pair})$ be a PES with (ζ, ζ)-KE-ind for a predicate family $\mathsf{P}_\kappa : \mathcal{X}_\kappa \times \mathcal{Y}_\kappa \to \{0, 1\}$. Then, we can construct an ABE scheme for predicate P_κ as follows.

$\mathsf{Setup}(1^\lambda, \kappa)$: Parse par from κ. It outputs pk and msk as follows.

$$\omega \leftarrow \mathsf{Param}(\mathsf{par}),\ \ \mathbb{G} \leftarrow \mathcal{G}_{\mathsf{BG}}(1^\lambda),\ \ \overline{\mathbf{A}}, \overline{\mathbf{B}} \leftarrow \mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)},\ \ \mathbf{h} \leftarrow \mathbb{Z}_p^{k+\zeta},$$
$$\mathbb{W} = (\mathbf{W}_1, \ldots, \mathbf{W}_\omega) \leftarrow (\mathbb{Z}_p^{(k+\zeta)\times(k+\zeta)})^\omega,$$
$$\mathsf{pk}{=}(\mathbb{G}, [\mathbf{A}]_1, [\mathbf{W}_1^\top \mathbf{A}]_1, \ldots, [\mathbf{W}_\omega^\top \mathbf{A}]_1, [\mathbf{A}^\top \mathbf{h}]_\mathsf{T}),\ \mathsf{msk}{=}(\mathbf{B}, \mathbf{h}, \mathbf{W}_1, \ldots, \mathbf{W}_\omega).$$

$\mathsf{Enc}(\mathsf{pk}, x, M)$: It takes pk, $x \in \mathcal{X}_\kappa$, and $M \in G_\mathsf{T}$ as inputs, and outputs ct_x by computing as follows.

$$(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})) \leftarrow \mathsf{EncCt}(x),\ \ \mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{n_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$$
$$\mathbf{S} = (\mathbf{A}\mathbf{s}_0, \mathbf{A}\mathbf{s}_1, \ldots, \mathbf{A}\mathbf{s}_{n_1}),\ \ \widehat{\mathbf{S}} = (\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2})$$
$$\mathsf{ct}_x = (\mathsf{ct}_1, \mathsf{ct}_2, \mathsf{ct}_3) = ([\mathbf{S}]_1, [\mathbf{c}(\mathbf{S}, \widehat{\mathbf{S}}, \mathbb{W})]_1, [\mathbf{s}_0^\top \mathbf{A}^\top \mathbf{h}]_\mathsf{T} M).$$

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{msk}, y)$: It takes pk, msk, and $y \in \mathcal{Y}_\kappa$ as inputs, and outputs sk_y by computing as follows.

$$(m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})) \leftarrow \mathsf{EncKey}(y),\ \ \mathbf{r}_1, \ldots, \mathbf{r}_{m_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{m_2} \leftarrow \mathbb{Z}_p^{k+\zeta}$$
$$\mathbf{R} = (\mathbf{B}\mathbf{r}_1, \ldots, \mathbf{B}\mathbf{r}_{m_1}),\ \ \widehat{\mathbf{R}} = (\mathbf{h}, \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{m_2})$$
$$\mathsf{sk}_y = (\mathsf{sk}_1, \mathsf{sk}_2) = ([\mathbf{R}]_2, [\mathbf{k}(\mathbf{R}, \widehat{\mathbf{R}}, \mathbb{W})]_2).$$

$\mathsf{Dec}(\mathsf{pk}, \mathsf{ct}_x, \mathsf{sk}_y)$: It takes pk, $\mathsf{ct}_x = (\mathsf{ct}_1, \mathsf{ct}_2, \mathsf{ct}_3)$, and $\mathsf{sk}_y = (\mathsf{sk}_1, \mathsf{sk}_2)$ such that $\mathsf{P}_\kappa(x, y) = 1$. Let $(\mathbf{E}, \bar{\mathbf{E}}) \leftarrow \mathsf{Pair}(x, y)$. It outputs $M' = \mathsf{ct}_3 / \Omega$ where

$$\Omega = \prod_{\substack{i \in [n_1+1] \\ j \in [m_3]}} e(\mathsf{ct}_{1,i}, \mathsf{sk}_{2,j})^{e_{i,j}} \cdot \prod_{\substack{i \in [n_3] \\ j \in [m_1]}} e(\mathsf{ct}_{2,i}, \mathsf{sk}_{1,j})^{\bar{e}_{i,j}}, \tag{3}$$

and where $\mathsf{ct}_{i,j}$ and $\mathsf{sk}_{i,j}$ refer to the j-th element of ct_i and sk_i, respectively, and $e_{i,j}$ and $\bar{e}_{i,j}$ refer to the (i,j)-th element of $\mathbf{E}$ and $\bar{\mathbf{E}}$, respectively.

Correctness. In defining $\mathsf{ct}_x, \mathsf{sk}_y$, we effectively map variables of PES to vectors/matrice as $s_i \mapsto \mathbf{s}_i^\top \mathbf{A}^\top$, $\hat{s}_j \mapsto \hat{\mathbf{s}}_j^\top$, $r_v \mapsto \mathbf{B}\mathbf{r}_v$, $\hat{r}_u \mapsto \hat{\mathbf{r}}_u$, $\alpha \mapsto \mathbf{h}$, and $w_n \mapsto \mathbf{W}_n$. Therefore, intuitively, the correctness of PES, which we recall that it is the relation: $\sum_{i \in [n_1+1], j \in [m_3]} e_{i,j} s_{i-1} k_j + \sum_{i \in [n_3], j \in [m_1]} \bar{e}_{i,j} c_i r_j = \alpha s_0$, will preserve to exactly the relation $\Omega = [\mathbf{s}_0^\top \mathbf{A}^\top \mathbf{h}]_\mathsf{T}$, where Ω is defined in Eq. (3).

Theorem 9. *Suppose Γ satisfies (ζ, ζ)-KE-ind. Then, our ABE scheme is adaptively secure under the $\mathcal{D}_k$-MDDH assumption. Let q_sk be the maximum number of $\mathcal{A}$'s queries to KeyGen. For any PPT adversary $\mathcal{A}$, there exist PPT adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$ such that*

$$\mathsf{Adv}^{\mathsf{ABE}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathcal{D}_k\text{-}\mathsf{MDDH}}_{\mathcal{B}_1}(\lambda) + q_\mathsf{sk} \mathsf{Adv}^{(\zeta,\zeta)\text{-}\mathsf{KE}\text{-}\mathsf{ind}}_{\mathcal{B}_2, \Gamma}(\lambda).$$

Proof. The proof follows the dual system methodology [36]. We consider a series of hybrids H_1 and $\mathsf{H}_{2,j}$ for $j \in [q_\mathsf{sk}]$. To define each hybrid, we introduce a

so-called semi-functional (SF) ciphertext and secret key, which are generated differently from normal ones. Specifically, an SF-ciphertext is generated as

$$
\begin{aligned}
&(n_1, n_2, \mathbf{c}(\mathbf{s}, \hat{\mathbf{s}}, \mathbf{w})) \leftarrow \mathsf{EncCt}(x),\ \ \mathbf{s}_1, \ldots, \mathbf{s}_{n_1} \leftarrow \mathbb{Z}_p^k,\ \ \boxed{\mathbf{c}_0}, \hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2} \leftarrow \mathbb{Z}_p^{k+\zeta},\\
&\mathbf{S} = (\boxed{\mathbf{c}_0}, \mathbf{A}\mathbf{s}_1, \ldots, \mathbf{A}\mathbf{s}_{n_1}),\ \ \widehat{\mathbf{S}} = (\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_{n_2}),\\
&\mathsf{ct}_x = (\mathsf{ct}_1, \mathsf{ct}_2, \mathsf{ct}_3) = ([\mathbf{S}]_1, [\mathbf{c}(\mathbf{S}, \widehat{\mathbf{S}}, \mathbb{W})]_1, [\boxed{\mathbf{c}_0^\top}\mathbf{h}]_{\mathsf{T}} M).
\end{aligned}
$$

An SF-secret key is generated as

$$
\begin{aligned}
&(m_1, m_2, \mathbf{k}(\mathbf{r}, \hat{\mathbf{r}}, \mathbf{w})) \leftarrow \mathsf{EncKey}(y),\ \mathbf{r}_1, \ldots, \mathbf{r}_{m_1} \leftarrow \mathbb{Z}_p^k,\ \ \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{m_2} \leftarrow \mathbb{Z}_p^{k+\zeta},\\
&\boxed{\mu \leftarrow \mathbb{Z}_p},\ \ \mathbf{R} = (\mathbf{B}\mathbf{r}_1, \ldots, \mathbf{B}\mathbf{r}_{m_1}),\ \ \widehat{\mathbf{R}} = (\mathbf{h} + \boxed{\mu \mathbf{a}_\zeta^*}, \hat{\mathbf{r}}_1, \ldots, \hat{\mathbf{r}}_{m_2}),\\
&\mathsf{sk}_y = (\mathsf{sk}_1, \mathsf{sk}_2) = ([\mathbf{R}]_2, [\mathbf{k}(\mathbf{R}, \widehat{\mathbf{R}}, \mathbb{W})]_2).
\end{aligned}
\tag{4}
$$

In the hybrids, the distribution of secret keys and the challenge ciphertext are modified as follows:

H_1: Same as the original game G except that the challenge ciphertext is SF.
$\mathsf{H}_{2,j}(j \in [q_{\mathsf{sk}}])$: Same as H_1 except that the first j secret keys given to $\mathcal{A}$ are SF.

We prove (in the full version) that $\mathsf{G} \approx_c \mathsf{H}_1 \approx_c \mathsf{H}_{2,1} \approx_c, \ldots, \approx_c \mathsf{H}_{2,q_{\mathsf{sk}}}$ and $\mathcal{A}$'s advantage in $\mathsf{H}_{2,q_{\mathsf{sk}}}$ is statistically close to 0. From these and the fact $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ABE}}(\lambda) = |\Pr[\langle \mathcal{A}, \mathsf{G} \rangle = \beta] - 1/2|$, we have that Theorem 9 holds. □

6 Extensions, Instantiations, and Applications

We obtain many applications in an analogous manner to the applications in [9].

Extended Framework. On the framework level, we obtain key-policy augmentation over *a set of predicate families*, denoted KBF, which is more powerful than the augmentation over a *single* predicate family ($\mathsf{KBF1}$), as done in Sect. 4.3. This follows exactly the same modular approach as in [9]. That is, in our context, we can show that KBF is implied by $\mathsf{KBF1}$ together with the direct sum and $\mathsf{CBF1}_{\mathsf{OR}}$. We defer the details to the full version. Moreover, more applications such as nested-policy ABE can also be obtained analogously to [9].

New Instantiations. On the instantiation level, we have showed the result overview in the introduction. Here, we briefly describe how to obtain such instantiations. The full details are deferred to the full version.

– Completely unbounded ABE for monotone Boolean formulae. Analogously to [9], we have that this predicate (in the key-policy flavor) is exactly $\mathsf{KBF1}[\mathsf{P}^{\mathsf{IBBE}}]$, where $\mathsf{P}^{\mathsf{IBBE}}$ is the predicate for ID-based broadcast encryption. IBBE can then be augmented from IBE, of which we know a PMH-secure PES from *e.g.,* [7]. The CP flavor is obtained by the dual conversion.

- Completely unbounded ABE for non-monotone Boolean formulae (the OSW type). This is also analogous to [9], where we consider two-mode IBBE (TIBBE), which can be then obtained by IBE and its negated predicate.
- Non-monotone KP-ABE with constant-size ciphertexts. A monotone variant is obtained by simply using the PMH-secure PES for IBBE with constant-size ciphertext encodings. Such a PES can be extracted from the PES for doubly spatial predicate in [7]. Since our KBF1-Trans preserves ciphertext encoding sizes, the converted scheme also obtains constant-size ciphertext encodings. For the non-monotone case, such a PES for TIBBE can be obtained by the disjunction of IBBE and negated IBBE (NIBBE). The latter can be viewed as a special case of negated doubly spatial predicate in [7], of which PES with constant-size encodings was reported. We directly construct a new TIBBE, which is two times efficient than the generic one from the disjunction (see the full version).
- CP-ABE with constant-size ciphertexts. First note that we consider schemes with some bound on the size of policies (Boolean formulae), which the same requirement as CP-ABE with constant-size ciphertexts of [1,9,10]. We obtain this by two steps. First we show that, when considering small-universe, KP-ABE implies CP-ABE (for Boolean formulae, with the bounded condition). We use the depth-universal circuit [18] in this conversion. Second we show that CP-ABE with small universe implies CP-ABE with large universe (again for Boolean formulae, with the bounded condition). To the best of our knowledge, these conversions were not known and can be of an independent interest, as they are applied to ABE in general (not necessarily to PES). Note that we cannot do that as Attrapadung *et al.* [10] did, who considered similar implications in the case of more powerful *span programs*.
- ABE with constant-size keys. CP/KP-ABE with constant-size keys is obtained by the dual of KP/CP-ABE with constant-size ciphertexts, respectively.

New Applications. As a new application, we provide a new unified predicate related to *non-monotone* ABE. Previously, there are two types of non-monotone ABE: the OSW type (Ostrovsky, Sahai, and Waters [31]) and the OT type (Okamoto and Takashima [30]). In the OSW type, a sub-predicate $P(y, X)$ amounts to check if an attribute is not in a set, *e.g.,* if $y \notin X$, while the OT type, a label tag is also attached, but a sub-predicate $P'((\mathrm{tag}, y), (\overline{\mathrm{tag}}, x))$ only checks the inequality on the same tag, *e.g.,* if $\mathrm{tag} = \overline{\mathrm{tag}} \wedge y \neq x$. Intuitively, the OSW type has a disadvantage in that the non-membership test takes the complement over the *whole universe* and this may be too much for some applications, where we would like to consider multiple sub-universe and confine the complement to only in the related sub-universe. On the other hand, the OT type confines the non-membership to those with the same tag, but the non-membership test is enabled only with the set of single element, *e.g.,* $\{x\}$. We unify both types to overcome both disadvantages; that is, a sub-predicate $P'((\mathrm{tag}, y), (\overline{\mathrm{tag}}, X))$ would check if $\mathrm{tag} = \overline{\mathrm{tag}} \wedge y \notin X$. We remark that when considering large-universe *monotone* ABE, there is no benefit to consider multiple spaces, since

$\mathbb{Z}_p$ is already exponentially large, and we can just treat a hashed value $H(\mathsf{tag}, y)$ as an attribute in $\mathbb{Z}_p$. In non-monotone ABE, we have to check the equality (of tags) and the non-membership at once, and the approach by hashing does not work. We motivate more on the unified non-monotone ABE, and provide definitions and constructions in the full version.

Acknowledgement. Nuttapong Attrapadung was partly supported by JST CREST Grant Number JPMJCR19F6, and by JSPS KAKENHI Kiban-A Grant Number 19H01109.

References

1. Agrawal, S., Chase, M.: A study of pair encodings: predicate encryption in prime order groups. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9563, pp. 259–288. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49099-0_10
2. Agrawal, S., Chase, M.: FAME: fast attribute-based message encryption. In: ACM CCS 2017, pp. 665–682 (2017)
3. Agrawal, S., Chase, M.: Simplifying design and analysis of complex predicate encryption schemes. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10210, pp. 627–656. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56620-7_22
4. Agrawal, S., Maitra, M., Yamada, S.: Attribute based encryption (and more) for nondeterministic finite automata from LWE. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11693, pp. 765–797. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_26
5. Agrawal, S., Maitra, M., Yamada, S.: Attribute based encryption for deterministic finite automata from DLIN. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019. LNCS, vol. 11892, pp. 91–117. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-36033-7_4
6. Ambrona, M., Barthe, G., Schmidt, B.: Generic transformations of predicate encodings: constructions and applications. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 36–66. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_2
7. Attrapadung, N.: Dual system encryption via doubly selective security: framework, fully secure functional encryption for regular languages, and more. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 557–577. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_31
8. Attrapadung, N.: Dual system encryption framework in prime-order groups via computational pair encodings. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 591–623. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_20
9. Attrapadung, N.: Unbounded dynamic predicate compositions in attribute-based encryption. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11476, pp. 34–67. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_2
10. Attrapadung, N., Hanaoka, G., Yamada, S.: Conversions among several classes of predicate encryption and applications to ABE with various compactness tradeoffs. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 575–601. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_24

11. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 90–108. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_6
12. Attrapadung, N., Tomida, J.: Unbounded Dynamic Predicate Compositions in ABE from Standard Assumptions. Cryptology ePrint Archive, Report 2020/231 (2020). https://eprint.iacr.org/2020/231. (The full version of this paper)
13. Attrapadung, N., Yamada, S.: Duality in ABE: converting attribute based encryption for dual predicate and dual policy via computational encodings. In: Nyberg, K. (ed.) CT-RSA 2015. LNCS, vol. 9048, pp. 87–105. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16715-2_5
14. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
15. Chen, J., Gay, R., Wee, H.: Improved dual system ABE in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 595–624. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_20
16. Chen, J., Gong, J., Kowalczyk, L., Wee, H.: Unbounded ABE via bilinear entropy expansion, revisited. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10820, pp. 503–534. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78381-9_19
17. Chen, J., Wee, H.: Semi-adaptive attribute-based encryption and improved delegation for boolean formula. In: Abdalla, M., De Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 277–297. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10879-7_16
18. Cook, S., Hoover, H.: A depth-universal circuit. SIAM J. Comp. **14**, 4 (1985)
19. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.L.: An algebraic framework for Diffie-Hellman assumptions. J. Cryptol. **30**(1), 242–288 (2017)
20. Gong, J., Dong, X., Chen, J., Cao, Z.: Efficient IBE with tight reduction to standard assumption in the multi-challenge setting. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 624–654. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_21
21. Gong, J., Waters, B., Wee, H.: ABE for DFA from k-Lin. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11693, pp. 732–764. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_25
22. Gong, J., Wee, H.: Adaptively secure ABE for DFA from k-Lin and more. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12107, pp. 278–308. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_10
23. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: ACM STOC 2013, pp. 545–554 (2013)
24. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM CCS 2006, pp. 89–98 (2006)
25. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_9
26. Kowalczyk, L., Wee, H.: Compact adaptively secure ABE for NC^1 from k-lin. J. Cryptol. **33**(3), 954–1002 (2019). https://doi.org/10.1007/s00145-019-09335-x

27. Lewko, A., Waters, B.: Unbounded HIBE and attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 547–567. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_30
28. Lin, H., Luo, J.: Compact adaptively secure ABE from k-lin: Beyond NC^1 and towards NL. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12107, pp. 247–277. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_9
29. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_11
30. Okamoto, T., Takashima, K.: Fully secure unbounded inner-product and attribute-based encryption. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 349–366. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_22
31. Ostrovsky, R., Sahai, A., Water, B.: Attribute-based encryption with non-monotonic access structures. In: ACM CCS 2007, pp. 195–203 (2007)
32. Rouselakis, Y., Waters, B.: Practical constructions and new proof methods for large universe attribute-based encryption. In: ACM CCS 2013, pp. 463–474 (2013)
33. Wang, X., Yu, H.: How to break MD5 and other hash functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_2
34. Takashima, K.: Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. In: Abdalla, M., De Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 298–317. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10879-7_17
35. Tomida, J., Kawahara, Y., Nishimaki, R.: Fast, compact, and expressive attribute-based encryption. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020. LNCS, vol. 12110, pp. 3–33. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45374-9_1
36. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_36
37. Waters, B.: Functional encryption for regular languages. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 218–235. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_14
38. Wee, H.: Dual system encryption via predicate encodings. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 616–637. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_26
39. Yamada, S., Attrapadung, N., Hanaoka, G., Kunihiro, N.: A framework and compact constructions for non-monotonic attribute-based encryption. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 275–292. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54631-0_16