Master-Key KDM-Secure ABE via Predicate Encoding

Shengyuan Feng*, Junqing Gong[✉,**], and Jie Chen[✉,***]

East China Normal University, Shanghai, China

Abstract. In this paper, we propose the first generic framework for attribute-based encryptions (ABE) with master-secret-key-dependent-message security (mKDM security) for affine functions via predicate encodings by Chen, Gay and Wee [Eurocrypt 2015]. The construction is adaptively secure under standard k-Lin assumption in prime-order bilinear groups. By this, we obtain a set of new mKDM-secure ABE schemes with high expressiveness that have never been reached before: we get the first hierarchical IBE (HIBE) scheme and the first ABE scheme for arithmetic branching program (ABP) with mKDM security for affine functions. Thanks to the expressiveness (more concretely, delegability like HIBE), we can obtain mKDM-secure ABE against chosen-ciphertext attack (i.e., CCA security) via a classical CPA-to-CCA transformation that works well in the context of mKDM.

1 Introduction

Semantic security of public-key encryption (PKE) ensures a ciphertext does not leak any information on the message without corresponding secret key. However this might not be true when the message depends on the secret key [ABBC10, CGH12]. The notion of key-dependent message (KDM) security is established to capture this situation [CL01, BRS03]. Specifically, given pk whose corresponding secret key is sk, KDM security means it remains semantically secure even when the message is $f(\mathsf{sk})$ for f from some a-priori function family $\mathcal{F}$.

Although much progress has been made on building KDM-secure PKE [CCS09, Hof13, LLJ15, HLL16, KT18, DGHM18, KM19, KMT19] and even analogous enhancement of other cryptographic primitives [HK07], the study of KDM security

* Supported by National Natural Science Foundation of China (61972156). Email: 51184506007@stu.ecnu.edu.cn

** Supported by National Natural Science Foundation of China (62002120), NSFC-ISF Joint Scientific Research Program (61961146004) and Innovation Program of Shanghai Municipal Education Commission (2021-01-07-00-08-E00101). Email: jqgong@sei.ecnu.edu.cn

*** Supported by National Natural Science Foundation of China (61972156, U1705264, 61632012), NSFC-ISF Joint Scientific Research Program (61961146004) and National Key Research and Development Program of China (2018YFA0704701). The author would like to thank Ant Group for its support and assistance with this work. Email: s080001@e.ntu.edu.sg

in the context of attribute-based encryption (ABE) [SW05, GPSW06], a generalization of PKE, lags behind. In an ABE for predicate P under master key pair $(\mathsf{mpk}, \mathsf{msk})$, a ciphertext encrypts message m under mpk with an attribute x, a user key sk is issued for a policy y by msk; decryption recovers m when $P(x, y) = 1$. The semantic security requires that a key holder cannot get any information on m when $P(x, y) = 0$; typically, we need this to hold even when multiple key holders collude with each other.

State-of-the-art: KDM Security in IBE. To our best knowledge, all existing results on KDM security in ABE only concern the simplest case — identity-based encryption (IBE) [Sha84, BF01]. Here both attribute x and policy y belong to the same domain (say, binary strings of fixed length) and $P(x, y) = 1$ if and only if $x = y$. Due to the presence of two types of secret keys in IBE, two flavors of KDM securities are considered: master-key-dependent-message (mKDM) security [GHV12] and user-key-dependent-message (uKDM) security [AP12]. In this work, we focus on the former one: given mpk whose corresponding master secret key is msk, it remains semantically secure even when the message is $f(\mathsf{msk})$ for f from some a-priori function family $\mathcal{F}$.

The first mKDM-secure IBE scheme [GHV12] has several limitations: the scheme is selectively secure and bounded in the sense that the size of mpk is proportional to the number of encryptions of key-dependent messages. Recently, Garg *et al.* [GGH20] discovered a surprising connection between mKDM security and tight reduction technique in the context of IBE and avoided the above limitations. As a bonus, their scheme also enjoys tight reduction.

This work: KDM Security in expressive ABE. We initiate the study of KDM security in the context of ABE beyond IBE. A classical application and motivation of ABE is to support fine-grained access control. A more expressive ABE (i.e., supporting larger class of policies) means a more flexible and powerful access control system. Apart from this, higher expressiveness may also help us to achieve higher security level. For instance, one can get chosen-ciphertext secure IBE from chosen-plaintext secure HIBE [CHK04] and follow-up works extended the method to the ABE setting [YAHK11, BL16, CMP17].

1.1 Results

This work proposes the first generic framework for ABE with mKDM-security for affine functions via predicate encodings [Wee14, CGW15]. Our construction is adaptively secure under standard k-Lin assumption in the prime-order bilinear group. Thanks to various concrete instantiations of predicate encodings, we can derive a set of new mKDM-secure ABE schemes; they support more complex policies than IBE, which have never been reached since the first KDM-secure IBE was proposed [GHV12, AP12]. In particular, as examples, we obtain

– the first HIBE scheme with mKDM-security for affine functions; users are organized in a tree-based structure and can partially delegate the decryption power (i.e., user secret key) to its children;
– the first ABE for arithmetic branching program (ABP) with mKDM-security for affine functions; note that, ABP covers **NC1**, **LOGSPACE** and the class of arithmetic circuits.

With the high expressiveness (more concretely, delegability like HIBE), we upgrade the generic framework to resist the chosen-ciphertext attack (i.e., achieve CCA security) and obtain CCA-secure variants of all above concrete ABE schemes. We summarize existing KDM-secure ABE (for affine functions) in Table 1.

Reference	**Policy**	**KDM**	**CCA?**
[GHV12]	IBE	mKDM	✘
[AP12]	IBE	uKDM	✘
[GGH20]	IBE	mKDM	✘
§ 6.1	(H)IBE	mKDM	✔
§ 6.2	ABE for ABP	mKDM	✔

Table 1. Comparison among existing KDM-secure ABE for affine functions.

A Brief Technical Overview. Our generic framework (with CPA security) is obtained by extending Garg *et al.*'s mKDM-secure IBE scheme [GGH20]. Recall that their IBE can be viewed as a combination of the KDM-secure PKE scheme from [BHHO08] and tightly-secure IBE from [AHY15, GDCC16]. The latter ingredient is aimed to handle leakage of master secret key in user secret keys in the presence of multiple challenge ciphertexts. We achieve this *in the context of ABE* by combining Chen *et al.*'s dual-system ABE via predicate encodings and nested dual-system technique that has been widely used to achieve unbounded ABE [LW11, OT12, KL15, CGKW18]. The first idea is to handle the afore-mentioned leakage while the second one ensures that this works well with multiple ciphertexts. See Section 1.2 for a more detailed technical overview. To get their CCA variant, we simply employ the classical CPA-to-CCA transformation [CHK04] which relies on delegation and is proved to work in the setting of mKDM security. For those predicates without delegation, we provide a generic way to extend their predicate encodings with a special delegation layer that is sufficient for the CPA-to-CCA transformation; this basically follows [YAHK11, BL16, CMP17]. See the full paper for more details.

Discussion in the Scope of IBE. Our generic framework gives us a new IBE scheme with mKDM-security (see Section 6.1) as [GHV12, GGH20], we make a comparison among them in Table 2 before we move to more technical details. We highlight that, Garg *et al.*'s scheme is the unique one with tight security

but the master public key size is linear in λ; on the other hand, our scheme enjoys constant-size master public key but the security loss is related to the number of queries. It is, of course, the ideal case to have a tightly secure scheme with constant-size master public key. However this has been an open problem in the context of *standard* semantic security for IBE. The only exception is the scheme in [CGW17] over composite-order bilinear groups, but this can only be considered as a partial solution due to the lack of realization of Déjà Q technique [CM14, CMM16] in prime-order bilinear groups. We finally note that our IBE scheme is the unique one with mKDM-security against *chosen-ciphertext attack*; this benefits from the high expressiveness of our generic framework that is able to lead to the first mKDM-secure HIBE (against chosen-plaintext attack).

Reference	Adaptive?	$\lvert\mathsf{mpk}\rvert$	CCA?	Tight?	Assumption
[GHV12]	✘	$O(Q_C)$	✘	✘	DLIN
[GGH20]	✔	$O(\lambda)$	✘	✔	SXDH
§ 6.1	✔	$O(1)$	✔	✘	SXDH

Table 2. Comparison among existing mKDM-secure IBE. Here, λ is the security parameter and Q_C is the number of ciphertexts.

1.2 Technical Overview

Garg *et al.*'s Scheme [GGH20]. We start from the unique mKDM-secure IBE (with adaptive security against unbounded collusion) by Garg *et al.* [GGH20]. Let (p, G_1, G_2, G_T, e) be an asymmetric bilinear groups of prime order p; we use g_1, g_2, g_T to denote random generators of G_1, G_2, G_T and employ the implicit representation of group elements: for a matrix $\mathbf{M}$ over $\mathbb{Z}_p$, we write $[\mathbf{M}]_s \coloneqq g_s^{\mathbf{M}}$ where $s \in \{1, 2, T\}$ and the exponentiation is carried out component-wise. Garg *et al.*'s scheme uses the basis:

$$(\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3) \leftarrow \mathbb{Z}_p^{\ell\times\ell_1} \times \mathbb{Z}_p^{\ell\times\ell_2} \times \mathbb{Z}_p^{\ell\times\ell_3} \tag{1}$$

and its dual basis $(\mathbf{A}_1^\dagger, \mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger) \in \mathbb{Z}_p^{\ell\times\ell_1} \times \mathbb{Z}_p^{\ell\times\ell_2} \times \mathbb{Z}_p^{\ell\times\ell_3}$ where $\ell = \ell_1 + \ell_2 + \ell_3 = \Theta(\log p)$ is much larger than k and $\ell_1, \ell_2, \ell_3 \geq k$; this satisfies orthogonality (i.e, $\mathbf{A}_i^\top \mathbf{A}_j^\dagger = \mathbf{0}$ for $i \neq j$) and non-degeneracy (i.e., $\mathbf{A}_i^\top \mathbf{A}_i^\dagger = \mathbf{I}$ for all $i = 1, 2, 3$).

We review Garg *et al.*'s IBE scheme from k-Lin assumption (with identity space $\{0,1\}^n$) as follows:

$$\begin{aligned}
\mathsf{mpk} &\coloneqq \boxed{[\mathbf{A}_1^\top]_1,\ [\mathbf{A}_1^\top \mathbf{k}]_T},\ [\mathbf{B}]_2,\ \{\,[\mathbf{A}_1^\top \mathbf{W}_{i,b}]_1,\ [\mathbf{W}\mathbf{B}_{i,b}]_2\,\}_{i\in[n],b\in\{0,1\}} \\
\mathsf{msk} &\coloneqq \boxed{[\mathbf{k}]_T} \\
\mathsf{sk}_{\mathsf{id}} &\coloneqq \boxed{[\mathbf{k}]_2} \cdot [(\mathbf{W}_{1,\mathsf{id}[1]} + \cdots + \mathbf{W}_{n,\mathsf{id}[n]})\mathbf{B}\mathbf{r}]_2,\ [\mathbf{B}\mathbf{r}]_2 \\
\mathsf{ct}_{\mathsf{id}} &\coloneqq \boxed{[\mathbf{s}^\top \mathbf{A}_1^\top]_1,\ [\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{k}]_T \cdot m},\ [\mathbf{s}^\top \mathbf{A}_1^\top (\mathbf{W}_{1,\mathsf{id}[1]} + \cdots + \mathbf{W}_{n,\mathsf{id}[n]})]_1
\end{aligned} \tag{2}$$

where $\mathsf{id} \in \{0,1\}^n$, $\mathbf{k} \leftarrow \{0,1\}^\ell$, $\mathbf{W}_{i,b} \leftarrow \mathbb{Z}_p^{\ell \times (k+1)}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{s} \leftarrow \mathbb{Z}_p^{\ell_1}$, $\mathbf{r} \leftarrow \mathbb{Z}_p^k$. Recall that the above scheme is a clever combination of the KDM-secure PKE scheme from [BHHO08] and tightly-secure IBE from [AHY15, GDCC16]; we highlight the two ingredients by solid boxes and gray boxes, respectively. Accordingly, the proof roughly consists of two phases: (a) One first changes all keys and ciphertexts to the following forms by the tight reduction technique [AHY15, GDCC16] using the parts in gray boxes. We highlight the differences by dashed boxes. (Note that the distribution here is slightly different from that in [GGH20]; one more computational transition can fill the gap.)

$$\begin{aligned}
\mathsf{sk}_{\mathsf{id}} &:= \boxed{[\mathbf{k} + \boxed{\mathbf{A}_2^\dagger \widehat{\mathbf{k}}}]_2} \cdot \boxed{[(\mathbf{W}_{1,\mathsf{id}[1]} + \cdots + \mathbf{W}_{n,\mathsf{id}[n]})\mathbf{B}\mathbf{r}]_2, [\mathbf{B}\mathbf{r}]_2}, \quad \widehat{\mathbf{k}} \leftarrow \mathbb{Z}_p^{\ell_2} \\
\mathsf{ct}_{\mathsf{id}} &:= \boxed{[\mathbf{s}^\top \mathbf{A}_1^\top + \boxed{\widehat{\mathbf{s}}^\top \mathbf{A}_2^\top}]_1, [(\mathbf{s}^\top \mathbf{A}_1^\top + \boxed{\widehat{\mathbf{s}}^\top \mathbf{A}_2^\top})\mathbf{k}]_T \cdot m}, \quad \widehat{\mathbf{s}} \leftarrow \mathbb{Z}_p^{\ell_2} \\
&\quad \boxed{[(\mathbf{s}^\top \mathbf{A}_1^\top + \boxed{\widehat{\mathbf{s}}^\top \mathbf{A}_2^\top})(\mathbf{W}_{1,\mathsf{id}[1]} + \cdots + \mathbf{W}_{n,\mathsf{id}[n]})]_1},
\end{aligned} \tag{3}$$

(b) One then carries out the KDM argument for PKE from [BHHO08] using the parts in solid boxes; this benefits from the fact that $\mathbf{A}_2^\dagger \widehat{\mathbf{k}}$ introduced in the first phase "controls" the leakage of $\mathbf{k}$ via $\mathsf{sk}_{\mathsf{id}}$.

Strategy. In order to extend scheme (2) to more expressive ABE, a natural idea is to follow the high-level idea of [GGH20] reviewed above but employ a tightly secure ABE scheme in the parts with gray boxes. However this strategy has two issues. First, to our best knowledge, there only exist tightly secure IBE [AHY15, GDCC16] and HIBE [LP20] in the multiple ciphertexts setting while no known result on the tight reduction for ABE even in the single ciphertext setting. Second, even with the recent progress on tightly secure HIBE [LP20], the construction of mKDM-secure HIBE is not modular, one has to go into the detail of the proof as in [LP20]. To circumvent the issues, we start from the following warm-up scheme presented in [GGH20]:

$$\begin{aligned}
\mathsf{mpk} &:= \boxed{[\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top \mathbf{k}]_T}, \boxed{[\mathbf{B}]_2, [\mathbf{A}_1^\top \mathbf{W}]_1, [\mathbf{A}_1^\top \mathbf{V}]_1, [\mathbf{W}\mathbf{B}]_2, [\mathbf{V}\mathbf{B}]_2} \\
\mathsf{msk} &:= \boxed{[\mathbf{k}]_T} \\
\mathsf{sk}_{\mathsf{id}} &:= \boxed{[\mathbf{k}]_2} \cdot \boxed{[(\mathbf{W} + \mathsf{id} \cdot \mathbf{V})\mathbf{B}\mathbf{r}]_2, [\mathbf{B}\mathbf{r}]_2} \\
\mathsf{ct}_{\mathsf{id}} &:= \boxed{[\mathbf{s}^\top \mathbf{A}_1^\top]_1, [\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{k}]_T \cdot m}, \boxed{[\mathbf{s}^\top \mathbf{A}_1^\top (\mathbf{W} + \mathsf{id} \cdot \mathbf{V})]_1}
\end{aligned} \tag{4}$$

where the gray boxes involve a *non-tightly* secure IBE scheme from [CGW15] with $\mathsf{id} \in \mathbb{Z}_p$. As reported in [GGH20], the scheme is mKDM-secure with respect to affine functions in the *single*-ciphertext setting. Our strategy is to

> upgrade the proof to the *multi-ciphertexts* setting *without* tight reduction technique.

The advantage of this strategy is that we can immediately generalize scheme (4) to more expressive ABE via predicate encodings [CGW15]; this allows us to derive mKDM-secure *ABE for various policies* in an *modular* way. As [GGH20], the proof consists of two phases: in the first phase, we will prove[1]

$$\left(\begin{array}{ll} \mathsf{mpk} : [\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top\mathbf{W}]_1, [\mathbf{A}_1^\top\mathbf{V}]_1, [\mathbf{B}]_2, [\mathbf{W}\mathbf{B}]_2, [\mathbf{V}\mathbf{B}]_2 & \\ \mathsf{sk}_{\mathsf{id}_i} : [\mathbf{B}\mathbf{r}_i]_2, [(\mathbf{W}+\mathsf{id}_i\cdot\mathbf{V})\mathbf{B}\mathbf{r}_i]_2, & \mathbf{r}_i \leftarrow \mathbb{Z}_p^k \\ \mathsf{ct}^*_{\mathsf{id}'_j} : [\mathbf{s}_j^\top\mathbf{A}_1^\top]_1, [\mathbf{s}_j^\top\mathbf{A}_1^\top(\mathbf{W}+\mathsf{id}'_j\cdot\mathbf{V})]_1, & \mathbf{s}_j \leftarrow \mathbb{Z}_p^{\ell_1} \end{array}\right)$$

$$\approx_c \left(\begin{array}{ll} \mathsf{mpk} : [\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top\mathbf{W}]_1, [\mathbf{A}_1^\top\mathbf{V}]_1, [\mathbf{B}]_2, [\mathbf{W}\mathbf{B}]_2, [\mathbf{V}\mathbf{B}]_2 & \\ \mathsf{sk}_{\mathsf{id}_i} : [\mathbf{B}\mathbf{r}_i]_2, [\boxed{\mathbf{A}_2\widehat{\mathbf{k}}_i} + (\mathbf{W}+\mathsf{id}_i\cdot\mathbf{V})\mathbf{B}\mathbf{r}_i]_2, & \mathbf{r}_i \leftarrow \mathbb{Z}_p^k,\ \widehat{\mathbf{k}}_i \leftarrow \mathbb{Z}_p^{\ell_2} \\ \mathsf{ct}^*_{\mathsf{id}'_j} : [\mathbf{s}_j^\top\mathbf{A}_1^\top + \boxed{\widehat{\mathbf{s}}_j^\top\mathbf{A}_2^\top}]_1, & \mathbf{s}_j \leftarrow \mathbb{Z}_p^{\ell_1}, \widehat{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^{\ell_2} \\ \qquad [(\mathbf{s}_j^\top\mathbf{A}_1^\top + \boxed{\widehat{\mathbf{s}}_j^\top\mathbf{A}_2^\top})(\mathbf{W}+\mathsf{id}'_j\cdot\mathbf{V})]_1, & \end{array}\right) \tag{5}$$

where $\mathsf{id}_1, \ldots, \mathsf{id}_{Q_K}$ and $\mathsf{id}'_1, \ldots, \mathsf{id}'_{Q_C}$ are key and ciphertext queries, respectively, this is analogous to the first phase in Garg *et al.*'s proof that changes the key and ciphertext distributions to (3); the second phase is essentially identical to that in Garg *et al.*'s proof with $\widehat{\mathbf{k}}_i$ and $\widehat{\mathbf{s}}_j$. Note that the key and ciphertext structures do not allow us to use known tight reduction techniques as in [GGH20].

Solution: Nested Dual-system Method. To carry out the strategy, we will prove (5) using the so-called *nested dual-system method* [LW11] that was developed to realize *unbounded* HIBE and ABE. To see why this can be useful, we consider unbounded HIBE built from IBE [LW11] as an example: a HIBE ciphertext is composed of a set of IBE ciphertexts while a HIBE key is composed of a set of IBE keys. To get standard semantic security of the unbounded HIBE, one has already been required to handle multiple keys and multiple ciphertexts of underlying IBE; this is essentially the same situation as in (5).

From a high level, the nested dual-system argument works as the standard dual-system argument [Wat09]: we **(i)** change all challenge ciphertexts into semi-functional form and **(ii)** change all keys into the semi-functional form one-by-one. The "nested" means that step **(ii)** employs another dual-system argument where the roles of ciphertexts and keys are exchanged; namely, we are handling a single key in the presence of multiple ciphertexts.

However this method is not compatible with predicate encodings in general. Roughly, the security of predicate encoding [Wee14, CGW15] ensures that, given a ciphertext, a secret key that is not authorized to decrypt has an extra computational entropy such as $\widehat{\mathbf{k}}_i$ in (5) that will be used to hide the master secret. This is compatible with the standard dual-system argument [Wat09, Wee14, CGW15] where we have a single ciphertext and multiple keys and the proof adds entropy

[1] In Section 3.3 and 3.4 where we describe our formal proof, $\widehat{\mathbf{k}}$ indicates a random vector from a subspace of $\mathbb{Z}_p^\ell$, say $\mathsf{span}(\mathbf{A}_2)$.

to each key one by one and always keeps the unique ciphertext "unchanged". However step **(ii)** involves multiple *ciphertexts* and a single *key*; we can not add extra entropy to ciphertexts while keeping the unique key "changed" via predicate encodings. One can circumvent this issue by simply introducing an extra subspace into basis (1) but this complicates the proof. (Note that, even though, this will not hurt the efficiency too much since ℓ is independent of the number of subspaces in our context.)

In this work, we will rely on a variant of nested dual-system argument implicitly used in the proof of entropy expansion lemma from [CGKW18] where they exchanged the roles of ciphertexts and keys at the very beginning in step **(i)**. By this, when step **(ii)** reverses the roles again, we are facing a single ciphertext and multiple keys that is compatible with predicate encodings and can avoid the extra subspace in the aforementioned trivial countermeasure. In particular, we can continue to use the basis (1) as [GGH20] although the proof is different. Note that, even with this special arrangement, [CGKW18] essentially works with IBE (an attribute $i \in \mathbb{Z}_p$ is encoded in an IBE form: $\mathbf{W} + i \cdot \mathbf{V}$); this is the first time to highlight this property and apply this to general ABE via predicate encodings.

Proof Overview. For simplicity, we will illustrate our proof of (5) for the *IBE* functionality in asymmetric *composite*-order bilinear groups (N, G_N, H_N, G_T, e) whose order N is a product of three primes p_1, p_2, p_3. Let g_i, h_i be random generators of subgroups of order p_i in G_N, H_N for $i \in \{1, 2, 3\}$, respectively. The switch between composite- and prime-order groups will rely on the following classical correspondence in [CGKW18]:

$$\begin{array}{rc}
 & g_1, h_{123} \leftrightarrow [\mathbf{A}^\top]_1, [\mathbf{B}]_2 \\
w, v \leftrightarrow \mathbf{W}, \mathbf{V} & g_1^w, g_1^v, h_{123}^w, h_{123}^v \leftrightarrow [\mathbf{A}_1^\top \mathbf{W}]_1, [\mathbf{A}_1^\top \mathbf{V}]_1, [\mathbf{W}\mathbf{B}]_2, [\mathbf{V}\mathbf{B}]_2 \\
s \leftrightarrow \mathbf{s} & g_1^s, g_1^{sw}, g_1^{sv} \leftrightarrow [\mathbf{s}^\top \mathbf{A}_1^\top]_1, [\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{W}]_1, [\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{V}]_1 \\
\hat{s} \leftrightarrow \widehat{\mathbf{s}} & g_2^{\hat{s}}, g_2^{\hat{s}w}, g_2^{\hat{s}v} \leftrightarrow [\widehat{\mathbf{s}}^\top \mathbf{A}_2^\top]_1, [\widehat{\mathbf{s}}^\top \mathbf{A}_2^\top \mathbf{W}]_1, [\widehat{\mathbf{s}}^\top \mathbf{A}_2^\top \mathbf{V}]_1 \\
\hat{\alpha}, r \leftrightarrow \widehat{\mathbf{k}}, \mathbf{r} & h_{123}^r, h_{123}^{wr}, h_{123}^{vr}, h_2^{\hat{\alpha}} \leftrightarrow [\mathbf{B}\mathbf{r}]_2, [\mathbf{W}\mathbf{B}\mathbf{r}]_2, [\mathbf{V}\mathbf{B}\mathbf{r}]_2, [\mathbf{A}_2^\dagger \widehat{\mathbf{k}}]_2
\end{array}$$

by which the statement (5) can be translated into composite-order groups as:

$$\begin{pmatrix} \mathsf{mpk} : g_1,\ g_1^w,\ g_1^v,\ h_{123},\ h_{123}^w,\ h_{123}^v \\ \mathsf{sk}_{\mathsf{id}_i} : h_{123}^{r_i},\ h_{123}^{(w+\mathsf{id}_i \cdot v) r_i} \\ \mathsf{ct}^*_{\mathsf{id}'_j} : g_1^{s_j},\ g_1^{s_j (w+\mathsf{id}'_j \cdot v)} \end{pmatrix} \approx_c \begin{pmatrix} \mathsf{mpk} : g_1,\ g_1^w,\ g_1^v,\ h_{123},\ h_{123}^w,\ h_{123}^v \\ \mathsf{sk}_{\mathsf{id}_i} : h_{123}^{r_i},\ \boxed{h_2^{\hat{\alpha}_i}} \cdot h_{123}^{(w+\mathsf{id}_i \cdot v) r_i} \\ \mathsf{ct}^*_{\mathsf{id}'_j} : g_1^{s_j} \cdot \boxed{g_2^{\hat{s}_j}},\ g_1^{s_j (w+\mathsf{id}'_j \cdot v)} \cdot \boxed{g_2^{\hat{s}_j (w+\mathsf{id}'_j \cdot v)}} \end{pmatrix} \tag{6}$$

where $w, v \leftarrow \mathbb{Z}_N$ and $\hat{\alpha}_i, r_i, s_j, \hat{s}_j \leftarrow \mathbb{Z}_N$ for $i \in [Q_K], j \in [Q_C]$. Following [CGKW18], our proof consists of two steps.

1. We change all secret keys into the following form that is analogous to so-called semi-functional keys in standard (nested) dual-system argument [Wat09, LW11]:
$$\mathsf{sk}_{\mathsf{id}_i} = (h_{123}^{r_i}, \boxed{h_2^{\hat{\alpha}_i}} \cdot h_{123}^{(w+\mathsf{id}_i \cdot v) r_i}).$$
This is basically the step that changes normal keys to semi-functional keys in the standard dual-system argument [Wat09, CGW15]. The indistinguishability employs a standard hybrid argument going through every keys based on (a) subgroup decision assumption: $h_{12}^{r_i} \approx_c h_1^{r_i}$ given g_1, h_{123} and (b) statistical argument: for all $\hat{\alpha}_i, r_i \in \mathbb{Z}_N$, we have $w \bmod p_2 \approx_s w + \hat{\alpha}_i / r_i \bmod p_2$ when $w \leftarrow \mathbb{Z}_N$.
2. We change all ciphertexts into the following form that is analogous to so-called semi-functional ciphertexts in the standard dual-system argument [Wat09]:
$$\mathsf{ct}_{\mathsf{id}'_j} = (g_1^{s_j} \cdot \boxed{g_2^{\hat{s}_j}}, g_1^{s_j (w+\mathsf{id}'_j \cdot v)} \cdot \boxed{g_2^{\hat{s}_j (w+\mathsf{id}'_j \cdot v)}}).$$
Again, we will make the change in a one-by-one manner. However, we cannot simply use subgroup decision assumption for each transition. Instead, we will employ a game sequence with the help of the p_3-subgroup. Let us show how to change the $\hat{\jmath}$-th ciphertext as an example. Given
$$\mathsf{mpk} = (g_1, g_1^w, g_1^v, h_{123}, h_{123}^w, h_{123}^v)$$
and ciphertexts that has been changed (with index $j < \hat{\jmath}$) and has not been changed (with index $j > \hat{\jmath}$):
$$\mathsf{ct}^*_{\mathsf{id}'_j}(j < \hat{\jmath}) : g_1^{s_j} \cdot g_2^{\hat{s}_j}, g_1^{s_j (w+\mathsf{id}'_j \cdot v)} \cdot g_2^{\hat{s}_j (w+\mathsf{id}'_j \cdot v)}$$
$$\mathsf{ct}^*_{\mathsf{id}'_j}(j > \hat{\jmath}) : g_1^{s_j}, \qquad g_1^{s_j (w+\mathsf{id}'_j \cdot v)}$$
we change the $\hat{\jmath}$-th ciphertext along with *all* secret keys via the following hybrid argument:
$$\begin{pmatrix} \mathsf{sk}_{\mathsf{id}_i} : h_{123}^{r_i}, h_2^{\hat{\alpha}_i} \cdot h_{123}^{(w+\mathsf{id}_i \cdot v) r_i}, & \forall i \in [Q_K] \\ \mathsf{ct}^*_{\mathsf{id}'_{\hat{\jmath}}} : g_1^{s_{\hat{\jmath}}}, g_1^{s_{\hat{\jmath}} (w+\mathsf{id}'_{\hat{\jmath}} \cdot v)} & \end{pmatrix}$$
$$\approx_c \begin{pmatrix} \mathsf{sk}_{\mathsf{id}_i} : h_{123}^{r_i}, h_2^{\hat{\alpha}_i} \cdot h_{123}^{(w+\mathsf{id}_i \cdot v) r_i}, & \forall i \in [Q_K] \\ \mathsf{ct}^*_{\mathsf{id}'_{\hat{\jmath}}} : g_1^{s_{\hat{\jmath}}} \cdot \boxed{g_3^{\tilde{s}_{\hat{\jmath}}}}, g_1^{s_{\hat{\jmath}} (w+\mathsf{id}'_{\hat{\jmath}} \cdot v)} \cdot \boxed{g_3^{\tilde{s}_{\hat{\jmath}} (w+\mathsf{id}'_{\hat{\jmath}} \cdot v)}} & \end{pmatrix}$$
$$\approx_c \begin{pmatrix} \mathsf{sk}_{\mathsf{id}_i} : h_{123}^{r_i}, h_2^{\hat{\alpha}_i} \cdot \boxed{h_3^{\tilde{\alpha}_i}} \cdot h_{123}^{(w+\mathsf{id}_i \cdot v) r_i}, & \forall i \in [Q_K] \\ \mathsf{ct}^*_{\mathsf{id}'_{\hat{\jmath}}} : g_1^{s_{\hat{\jmath}}} \cdot g_3^{\tilde{s}_{\hat{\jmath}}}, g_1^{s_{\hat{\jmath}} (w+\mathsf{id}'_{\hat{\jmath}} \cdot v)} \cdot g_3^{\tilde{s}_{\hat{\jmath}} (w+\mathsf{id}'_{\hat{\jmath}} \cdot v)} & \end{pmatrix}$$
$$\approx_c \begin{pmatrix} \mathsf{sk}_{\mathsf{id}_i} : h_{123}^{r_i}, h_2^{\hat{\alpha}_i} \cdot h_3^{\tilde{\alpha}_i} \cdot h_{123}^{(w+\mathsf{id}_i \cdot v) r_i}, & \forall i \in [Q_K] \\ \mathsf{ct}^*_{\mathsf{id}'_{\hat{\jmath}}} : g_1^{s_{\hat{\jmath}}} \cdot \boxed{g_2^{\tilde{s}_{\hat{\jmath}}}}, g_1^{s_{\hat{\jmath}} (w+\mathsf{id}'_{\hat{\jmath}} \cdot v)} \cdot \boxed{g_2^{\tilde{s}_{\hat{\jmath}} (w+\mathsf{id}'_{\hat{\jmath}} \cdot v)}} & \end{pmatrix}$$

$$\approx_c \begin{pmatrix} \mathsf{sk}_{\mathsf{id}_i} : h_{123}^{r_i},\ h_2^{\hat{\alpha}_i} \cdot \cancel{h_3^{\tilde{\alpha}_i}} \cdot h_{123}^{(w+\mathsf{id}_i \cdot v) r_i}, \quad \forall i \in [Q_K] \\ \mathsf{ct}^*_{\mathsf{id}'_{\hat{\jmath}}} : g_1^{s_{\hat{\jmath}}} \cdot g_2^{\hat{s}_{\hat{\jmath}}},\ g_1^{s_{\hat{\jmath}}(w+\mathsf{id}'_{\hat{\jmath}} \cdot v)} \cdot g_2^{\hat{s}_{\hat{\jmath}}(w+\mathsf{id}'_{\hat{\jmath}} \cdot v)} \end{pmatrix}$$

where $\tilde{\alpha}_i, \tilde{s}_{\hat{\jmath}} \leftarrow \mathbb{Z}_N$ for all $i \in [Q_K]$. Here

- the first $\approx_c$ follows from subgroup decision assumption: $g_1^{s_{\hat{\jmath}}} \approx_c g_1^{s_{\hat{\jmath}}} \cdot g_3^{\tilde{s}_{\hat{\jmath}}}$ given g_1, g_2, h_{123}, h_2.
- the second $\approx_c$ is similar to the first step of our proof with (a) subgroup decision assumption: $h_{13}^{r_i} \approx_c h_1^{r_i}$ given g_1, g_2, h_2, h_{123} and (b) statistical argument over p_3-subgroup for a fixed $i \in [Q_K]$: for all $\tilde{\alpha}_i, r_i \in \mathbb{Z}_N$,

$$\overbrace{w + \mathsf{id}_i \cdot v}^{\mathsf{sk}_{\mathsf{id}_i}}, \overbrace{w + \mathsf{id}'_{\hat{\jmath}} \cdot v}^{\mathsf{ct}^*_{\mathsf{id}'_{\hat{\jmath}}}} \approx_s \boxed{\tilde{\alpha}_i / r_i} + w + \mathsf{id}_i \cdot v, w + \mathsf{id}'_{\hat{\jmath}} \cdot v \mod p_3$$

  when $w, v \leftarrow \mathbb{Z}_N$.
- the third $\approx_c$ follows from subgroup decision assumption: $g_3^{\tilde{s}_{\hat{\jmath}}} \approx_c g_2^{\hat{s}_{\hat{\jmath}}}$ given g_1, g_2, h_{123}, h_{23}; h_{23} is a random generator of subgroup of order $p_2 p_3$ that is used to simulate term $\{h_2^{\hat{\alpha}_i} \cdot h_3^{\tilde{\alpha}_i}\}_{i \in [Q_K]}$.
- the last $\approx_c$ is analogous to the second one except that statistical argument becomes: for all $\tilde{\alpha}_i, r_i \in \mathbb{Z}_N$, we have $w \bmod p_3 \approx_s w + \tilde{\alpha}_i / r_i \bmod p_3$ when $w \leftarrow \mathbb{Z}_N$.

In the final proof with *predicate encodings* in *prime-order* bilinear groups, we translate

- subgroup decision assumption over G_N into the prime-order version in [CGKW18] w.r.t. basis (1), cf. Lemma 1;
- subgroup decision assumption over H_N into the MDDH assumption w.r.t. $\mathbf{B}$, see Assumption 1;
- the statistical arguments into the so-called α-privacy of predicate encoding, cf. Section 2.3.

1.3 Discussions and Open Problems

Towards Framework via Pair Encoding. Pair encoding [Att14, AC17] is a primitive similar to the predicate encoding [Wee14, CGW15]. It is also feasible to generalize (4) via pair encodings. Although this will give us even more expressive mKDM-secure ABE, the security would rely on complex q-type assumptions. In this paper, we restrict us to the security based on static assumption notably k-Lin assumption. We leave this as an open problem to get even more expressive ABE that goes beyond predicate encoding.

Towards Multi-instance Setting. As [GGH20], we only study the mKDM-security in the single instance setting. We believe both constructions can be extended to multiple instance setting, as [GHV12], where the message can be

$f(\mathsf{msk}_1, \ldots, \mathsf{msk}_N)$ with msk_i are master secret keys of N independent instances. We leave this as one of future works. In fact, [GHV12] reported that they can reduce the mKDM-security of their IBE scheme in the multiple instance setting to that in the single instance setting. However we point out that this might not be straightforward in the context of ABE: each instance can support different policies which makes the above reduction quite hard.

More Open Problems. We leave several open problems:

- As we have discussed, it is desirable to have a mKDM-secure IBE with tight security under constant-size master public key in the prime-order bilinear group. This will be a breakthrough even for the standard semantic security.
- It would be interesting to build a mKDM-secure ABE from various assumptions such as learning with error (LWE) assumption. Note that, to our best knowledge, there is no LWE-based construction with such security property.
- A formal study of the relation of uKDM-security and mKDM-security is also appealing. For now, we can conjecture that mKDM-security is strictly stronger than uKDM-security. However there's no formal implication and/or separation results on this.

Organization. We describe some background knowledge in Section 2. In Section 3, we present our generic ABE scheme via predicate encoding and prove its mKDM security from k-Lin assumption in the prime-order biliear group. We show how to add delegation and revisit the CPA-to-CCA transformation with mKDM security in Section 4 and Section 5. Several concrete schemes derived from previous generic results will be given out in Section 6.

2 Preliminaries

Notation. We use $s \leftarrow S$ to indicate that s is selected uniformly from finite set S. PPT stands for probabilistic polynomial time. For a matrix $\mathbf{A}$ over $\mathbb{Z}_p$, we use $\mathsf{span}(\mathbf{A})$ to denote the column span of $\mathbf{A}$, and we use $\mathsf{basis}(\mathbf{A})$ to denote a basis of $\mathsf{span}(\mathbf{A})$. We use $\langle \mathsf{G}, \mathcal{A} \rangle = 1$ to denote that adversary $\mathcal{A}$ wins game G. We use $\approx_c$ and $\approx_s$ to denote two distributions being computationally and statistically indistinguishable, respectively.

2.1 Attribute-Based Encryption

Syntax. An attribute-based encryption (ABE) scheme for predicate $P : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ consists of the following PPT algorithms:

- $\mathsf{Setup}(1^\lambda, P) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm takes as input the security parameter 1^λ and a description of predicate P, outputs a master public/secret key pair $(\mathsf{mpk}, \mathsf{msk})$. We assume that mpk contains the description of domains $\mathcal{X}$, $\mathcal{Y}$ of P as well as message space $\mathcal{M}$.

- $\mathsf{Enc}(\mathsf{mpk}, x, m) \to \mathsf{ct}_x$. The encryption algorithm takes as input the master public key mpk, an index $x \in \mathcal{X}$ and a message $m \in \mathcal{M}$, outputs a ciphertext ct_x.
- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y) \to \mathsf{sk}_y$. The key generation algorithm takes as input the master public/secret key pair $(\mathsf{mpk}, \mathsf{msk})$ and an index $y \in \mathcal{Y}$, outputs a secret key sk_y.
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x) \to m$. The decryption algorithm takes as input the master public key mpk, a secret key sk_y and a ciphertext ct_x, outputs a message m or a symbol $\perp$ indicating the ciphertext is invalid.

Correctness. For all $(x, y) \in \mathcal{X} \times \mathcal{Y}$ such that $P(x, y) = 1$ and $m \in \mathcal{M}$, it is required that

$$\Pr\left[m = \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x) \;\middle|\; \begin{array}{c}(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, P) \\ \mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, m) \\ \mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)\end{array}\right] = 1.$$

$\mathcal{F}$-mKDM Security. Let $\mathcal{F}$ be a function family. For all stateful PPT adversaries $\mathcal{A}$, the advantage function is defined as

$$\mathsf{mKDMAdv}^{\mathrm{CPA}}_{\mathcal{A},\mathcal{F}}(\lambda) := \left|\Pr\left[b = b' \;\middle|\; \begin{array}{c} b \leftarrow \{0,1\} \\ (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, P) \\ b' = \mathcal{A}^{\mathsf{O}^b_{\mathsf{Enc}}(\cdot,\cdot), \mathsf{O}_{\mathsf{KeyGen}}(\cdot)}(\mathsf{mpk})\end{array}\right] - \frac{1}{2}\right|$$

where the oracles work as follows:

- $\mathsf{O}^b_{\mathsf{Enc}}(x, F)$, on input $x \in \mathcal{X}$ and $F \in \mathcal{F}$, picks $m \leftarrow \mathcal{M}$, returns ct^b where
$$\mathsf{ct}^0 \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, F(\mathsf{msk})) \quad \text{and} \quad \mathsf{ct}^1 \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, m);$$
- $\mathsf{O}_{\mathsf{KeyGen}}(y)$, on input $y \in \mathcal{Y}$, returns sk_y where
$$\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y);$$

with the restriction that all queries $(x, \cdot)$ and y satisfy $P(x, y) = 0$. An ABE scheme is *master-key-dependent-message* secure with respect to function family $\mathcal{F}$ against *chosen-plaintext attack* if $\mathsf{mKDMAdv}^{\mathrm{CPA}}_{\mathcal{A},\mathcal{F}}(\lambda)$ is negligible in λ. In the following, we use $\mathbf{mKDM}_b$ to denote the above game parameterized by b. We can also define the variant against *chosen-ciphertext attack* analogously by providing $\mathcal{A}$ with a decryption oracle that works as below:

- $\mathsf{O}_{\mathsf{Dec}}(y, \mathsf{ct})$, on input $y \in \mathcal{Y}$ and a ciphertext ct, generates $\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$ and returns
$$m' \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct})$$

with the restriction that ct is not produced by $\mathsf{O}^b_{\mathsf{Enc}}$. In this work, we will always consider $\mathcal{F}$ being an affine function and call $\mathcal{F}$-mKDM as mKDM when the context is clear.

2.2 Prime-order Bilinear Groups

We assume a group generator $\mathcal{G}$ which takes as input a security parameter 1^λ and outputs a group description $\mathbb{G} := (p, G_1, G_2, G_T, e)$. Here G_1, G_2, G_T are cyclic groups of prime order p of $\Theta(\lambda)$ bits and $e : G_1 \times G_2 \to G_T$ is a non-degenerated bilinear map. Typically, the descriptions of G_1, G_2 contain respective generators g_1, g_2. We employ the implicit representation of group elements: for any matrix $\mathbf{A}$ over $\mathbb{Z}_p$ and $s \in \{1, 2, T\}$, we define $[\mathbf{A}]_s := g_s^{\mathbf{A}}$ where the exponentiation is carried out component-wise. Given $[\mathbf{A}]_1$ and $[\mathbf{B}]_2$, we define $[\mathbf{AB}]_T = e([\mathbf{A}]_1, [\mathbf{B}]_2)$.

Matrix Decisional Diffie-Hellman Assumption. We revisit the matrix decisional Diffie-Hellman (MDDH) assumption in the prime-order bilinear group that is a generalization of k-Linear assumption.

Assumption 1 ($\mathbf{MDDH}_{k,\ell}$, [EHK+13]). *Let $k, \ell \in \mathbb{N}$, $s \in \{1, 2, T\}$. For all PPT adversaries $\mathcal{A}$, the advantage function*

$$\mathsf{Adv}^{\mathbf{MDDH}_{k,\ell}}_{\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(\mathbb{G}, [\mathbf{A}]_s, [\mathbf{As}]_s) = 1] - \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{A}]_s, [\mathbf{u}]_s) = 1]|$$

is negligible in λ where $\mathbf{A} \leftarrow \mathbb{Z}_p^{\ell \times k}$, $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and $\mathbf{u} \leftarrow \mathbb{Z}_p^\ell$.

We write $\mathbf{MDDH}_k = \mathbf{MDDH}_{k,k+1}$ and have $\mathbf{MDDH}_k \Rightarrow \mathbf{MDDH}_{k,\ell}$ for $\ell > k$. Note that the assumption unconditionally holds when $\ell \leq k$.

2.3 Predicate Encoding

Syntax. A $\mathbb{Z}_p$-linear predicate encoding [Wee14, CGW15] for $P : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ consists of five deterministic algorithms:

$$\begin{array}{llll} \mathsf{sE} : \mathcal{X} \times \mathbb{Z}_p^n \to \mathbb{Z}_p^{n_s} & & & \mathsf{sD} : \mathcal{X} \times \mathcal{Y} \times \mathbb{Z}_p^{n_s} \to \mathbb{Z}_p \\ \mathsf{rE} : \mathcal{Y} \times \mathbb{Z}_p^n \to \mathbb{Z}_p^{n_r} & \mathsf{kE} : \mathcal{Y} \times \mathbb{Z}_p \to \mathbb{Z}_p^{n_r} & & \mathsf{rD} : \mathcal{X} \times \mathcal{Y} \times \mathbb{Z}_p^{n_r} \to \mathbb{Z}_p \end{array}$$

for some $n, n_s, n_r \in \mathbb{N}$ with the following features:

(linearity). For all $(x, y) \in \mathcal{X} \times \mathcal{Y}$, $\mathsf{sE}(x, \cdot)$, $\mathsf{rE}(y, \cdot)$, $\mathsf{kE}(y, \cdot)$, $\mathsf{sD}(x, y, \cdot)$, $\mathsf{rD}(x, y, \cdot)$ are $\mathbb{Z}_p$-linear. A $\mathbb{Z}_p$-linear function $L : \mathbb{Z}_p^n \to \mathbb{Z}_p^{n'}$ can be encoded as a matrix $\mathbf{L} = (l_{i,j}) \in \mathbb{Z}_p^{n \times n'}$ such that

$$L : (w_1, \ldots, w_n) \to (\textstyle\sum_{i=1}^n l_{i,1} w_i, \ldots, \sum_{i=1}^n l_{i,n'} w_i). \tag{7}$$

(restricted α-reconstruction). For all $(x, y) \in \mathcal{X} \times \mathcal{Y}$ such that $P(x, y) = 1$, $\alpha \in \mathbb{Z}_p$ and $\mathbf{w} \in \mathbb{Z}_p^n$, we have

$$\mathsf{sD}(x, y, \mathsf{sE}(x, \mathbf{w})) = \mathsf{rD}(x, y, \mathsf{rE}(y, \mathbf{w})) \quad \text{and} \quad \mathsf{rD}(x, y, \mathsf{kE}(y, \alpha)) = \alpha. \tag{8}$$

(α-privacy). For all $(x, y) \in \mathcal{X} \times \mathcal{Y}$ such that $P(x, y) = 0$, $\alpha \in \mathbb{Z}_p$ and $\mathbf{w} \leftarrow \mathbb{Z}_p^n$, the following distributions are identical:

$$\begin{array}{rl} & \{\, x, y, \alpha, \mathsf{sE}(x, \mathbf{w}), \mathsf{kE}(y, \alpha) + \mathsf{rE}(y, \mathbf{w}) \,\} \\ \text{and} & \{\, x, y, \alpha, \mathsf{sE}(x, \mathbf{w}), \mathsf{rE}(y, \mathbf{w}) \,\}. \end{array} \tag{9}$$

Notations and Facts. For $s \in \{1, 2, T\}$, we can define an extension of linear function (7) where we replace scalars $w_i \in \mathbb{Z}_p$ with (column) vector $\mathbf{w}_i \in \mathbb{Z}_p^k$ "in the exponent":

$$\begin{array}{rccc} L: & (G_s^k)^n & \to & (G_s^k)^{n'} \\ & ([\mathbf{w}_1]_s, \ldots, [\mathbf{w}_n]_s) & \mapsto & (\prod_{i=1}^n [l_{i,1}\mathbf{w}_i]_s, \ldots, \prod_{i=1}^n [l_{i,n'}\mathbf{w}_i]_s) \end{array} \tag{10}$$

For simplicity, we use the same notation L since they correspond to the same $\mathbf{L}$. Moreover, this works with row vectors and matrices analogously. We conclude this part with some properties of (10):

($L(\cdot)$ and pairing e are commutative). Let $n' = 1$. For all $\mathbf{a}, \mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}_p^k$, we have

$$e([\mathbf{a}^\top]_1, L([\mathbf{b}_1]_2, \ldots, [\mathbf{b}_n]_2)) = L([\mathbf{a}^\top \mathbf{b}_1]_T, \ldots, [\mathbf{a}^\top \mathbf{b}_n]_T), \tag{11}$$

$$e(L([\mathbf{b}_1^\top]_1, \ldots, [\mathbf{b}_n^\top]_1), [\mathbf{a}]_2) = L([\mathbf{b}_1^\top \mathbf{a}]_T, \ldots, [\mathbf{b}_n^\top \mathbf{a}]_T). \tag{12}$$

($L(\cdot)$ and $[\cdot]_s$ are commutative). For all $(\mathbf{w}_1, \ldots, \mathbf{w}_n) \in (\mathbb{Z}_p^k)^n$, we have

$$L([\mathbf{w}_1]_s, \ldots, [\mathbf{w}_n]_s) = [L(\mathbf{w}_1, \ldots, \mathbf{w}_n)]_s. \tag{13}$$

3 Master-Key KDM ABE

In this section, we present our generic ABE via predicate encodings in the prime-order bilinear group. The scheme is adaptively mKDM-CPA secure (with respect to affine functions) against unbounded collusion under k-Lin assumption.

3.1 Basis

Our ABE scheme based on $\mathbf{MDDH}_k$ assumption uses the following basis

$$(\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3) \leftarrow \mathbb{Z}_p^{\ell \times \ell_1} \times \mathbb{Z}_p^{\ell \times \ell_2} \times \mathbb{Z}_p^{\ell \times \ell_3} \tag{14}$$

where $\ell = \ell_1 + \ell_2 + \ell_3 \geq 2(\lambda + k \log p)$ and $\ell_1 = \ell_2 = k$, $\ell_3 \geq k$. We denote their dual basis by $(\mathbf{A}_1^\dagger, \mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger)$ such that $\mathbf{A}_i^\top \mathbf{A}_j^\dagger = \mathbf{0}$ when $i \neq j$ and $\mathbf{A}_i^\top \mathbf{A}_i^\dagger = \mathbf{I}$. We write horizontal concatenation $\mathbf{A}_{ij} = (\mathbf{A}_i | \mathbf{A}_j)$, $\mathbf{A}_{ij}^\dagger = (\mathbf{A}_i^\dagger | \mathbf{A}_j^\dagger)$ for short.

Subgroup Decision Assumption. We describe a three-subgroup variant of prime-order $(\mathbf{A}_1 \mapsto \mathbf{A}_{12})$-subgroup decision assumption [CGKW18], denoted by $\mathbf{SD}_{\mathbf{A}_1 \mapsto \mathbf{A}_{12}}$. By symmetry, we can permute the indices for $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$. One can define the assumption over dual bases $\mathbf{A}_1^\dagger$, $\mathbf{A}_2^\dagger$, $\mathbf{A}_3^\dagger$ analogously.

Lemma 1 ($\mathbf{MDDH}_{\ell_1, \ell_1+\ell_2} \Rightarrow \mathbf{SD}_{\mathbf{A}_1 \mapsto \mathbf{A}_{12}}$). *Under* $\mathbf{MDDH}_{\ell_1, \ell_1+\ell_2}$ *assumption in* G_1*, there exists an efficient sampler outputting random* $([\mathbf{A}_1]_1, [\mathbf{A}_2]_1, [\mathbf{A}_3]_1)$ *along with bases* $\mathsf{basis}(\mathbf{A}_1^\dagger)$, $\mathsf{basis}(\mathbf{A}_1^\dagger, \mathbf{A}_2^\dagger)$, $\mathsf{basis}(\mathbf{A}_3^\dagger)$ *(of arbitrary choice) such that the advantage function*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathbf{SD}_{\mathbf{A}_1 \mapsto \mathbf{A}_{12}}}(\lambda) := |\Pr[\mathcal{A}(D, [\mathbf{t}_0]_1) = 1] - \Pr[\mathcal{A}(D, [\mathbf{t}_1]_1) = 1]|$$

is negligible in λ where

$$D := ([\mathbf{A}_1]_1, [\mathbf{A}_2]_1, [\mathbf{A}_3]_1, \mathsf{basis}(\mathbf{A}_1^\dagger), \mathsf{basis}(\mathbf{A}_1^\dagger, \mathbf{A}_2^\dagger), \mathsf{basis}(\mathbf{A}_3^\dagger)),$$
$$\mathbf{t}_0 \leftarrow \mathsf{span}(\mathbf{A}_1) \quad \textit{and} \quad \mathbf{t}_1 \leftarrow \mathsf{span}(\mathbf{A}_1, \mathbf{A}_2).$$

3.2 Scheme

Construction. Our ABE scheme via predicate encoding is as follows:

– $\mathsf{Setup}(1^\lambda, P)$: Let n be parameter size of predicate encoding $(\mathsf{sE}, \mathsf{rE}, \mathsf{kE}, \mathsf{sD}, \mathsf{rD})$ for P. Run $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda)$, sample $\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{\ell \times k}$ as in (14), $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, pick $\mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow \mathbb{Z}_p^{\ell \times (k+1)}$ and $\mathbf{k} \leftarrow \{0,1\}^\ell$. Output

$$\mathsf{mpk} := \begin{pmatrix} \mathbb{G}, [\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top \mathbf{W}_1]_1, \ldots, [\mathbf{A}_1^\top \mathbf{W}_n]_1, \\ [\mathbf{B}]_2, \ [\mathbf{W}_1\mathbf{B}]_2, \ \ \ldots, [\mathbf{W}_n\mathbf{B}]_2, \ \ [\mathbf{A}_1^\top \mathbf{k}]_T \end{pmatrix}, \quad \mathsf{msk} := [\mathbf{k}]_T.$$

– $\mathsf{Enc}(\mathsf{mpk}, x, m)$: Pick $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and output

$$\mathsf{ct}_x := (\overbrace{[\mathbf{s}^\top \mathbf{A}_1^\top]_1}^{C_0}, \overbrace{\mathsf{sE}(x, [\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{W}_1]_1, \ldots, [\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{W}_n]_1)}^{\vec{C}_1}, \overbrace{[\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{k}]_T \cdot m}^{C}).$$

– $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$: Recover $\mathbf{k} \in \{0,1\}^\ell$ from $\mathsf{msk} = [\mathbf{k}]_T$. Pick $\mathbf{r} \leftarrow \mathbb{Z}_p^k$ and output

$$\mathsf{sk}_y := (\overbrace{[\mathbf{B}\mathbf{r}]_2}^{K_0}, \overbrace{\mathsf{kE}(y, [\mathbf{k}]_2) \cdot \mathsf{rE}(y, [\mathbf{W}_1\mathbf{B}\mathbf{r}]_2, \ldots, [\mathbf{W}_n\mathbf{B}\mathbf{r}]_2)}^{\vec{K}_1}).$$

– $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x)$: Parse $\mathsf{sk}_y = (K_0, \vec{K}_1)$ and $\mathsf{ct}_x = (C_0, \vec{C}_1, C)$, and output

$$m' = C \cdot e(C_0, \mathsf{rD}(x, y, \vec{K}_1))^{-1} \cdot e(\mathsf{sD}(x, y, \vec{C}_1), K_0).$$

The correctness follows from properties in Section 2.3 as in [CGW15]. See the full paper for more details.

Security. We have the following theorem for the above scheme.

Theorem 1 (Main Theorem). *Under* $\mathbf{MDDH}_k$ *assumption (cf. Section 3.1), our ABE scheme described in this section is master-key-dependent-message secure for affine functions mapping G_T^ℓ to G_T against chosen-plaintext attack.*

3.3 Useful Lemmas

We prepare two lemmas with respect to the basis (14) in Section 3.1 which will be used throughout the proof. The first lemma (Lemma 2) is a variant of "$\mathbf{c} \approx_s \mathbf{c} - \mathbf{f}$" where $\mathbf{c} \leftarrow \mathbb{Z}_p^\ell$ and $\mathbf{f} \in \mathbb{Z}_p^\ell$; here we allow $\mathbf{c}$ to live in a subspace and work with groups. The second lemma (Lemma 3) is an extension of leftover hash lemma which additionally gives out an extra term randomly picked from the coset $\mathbf{k} + \mathsf{span}(\mathbf{A}_{23}^\dagger)$. We present the lemmas without proofs.

Lemma 2. *Let $Q \in \mathbb{N}$. For any $\{\mathbf{f}_j\}_{j\in[Q]} \in (\mathbb{Z}_p^\ell)^Q$, we have*

$$\{[\mathbf{c}_j]_1\}_{j\in[Q]} \approx_c \{[\mathbf{c}_j - \mathbf{f}_j]_1\}_{j\in[Q]} \quad \textit{given} \quad \mathbf{A}_1, [\mathbf{A}_2]_1, [\mathbf{A}_3]_1, \mathbf{A}_1^\dagger, \mathsf{basis}(\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger)$$

where $\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \mathbf{A}_2)$. The distinguishing advantage $\mathsf{Adv}_{\mathcal{A}}^{\textsc{CompHide}_Q}(\lambda)$ is bounded by $2Q \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathbf{MDDH}_{k,\ell}}(\lambda)$ for all PPT adversaries $\mathcal{B}$.

Lemma 3. *Within probability $1 - 1/2^\lambda$, we have*

$$(\mathbf{A}_1^\top, \mathbf{A}_2^\top, \mathbf{A}_{23}^\dagger, \mathbf{A}_1^\top\mathbf{k}, \mathbf{k} + \widehat{\mathbf{k}}, \boxed{\mathbf{A}_2^\top\mathbf{k}}) \approx_s (\mathbf{A}_1^\top, \mathbf{A}_2^\top, \mathbf{A}_{23}^\dagger, \mathbf{A}_1^\top\mathbf{k}, \mathbf{k} + \widehat{\mathbf{k}}, \boxed{\mathbf{u}})$$

where $\mathbf{k} \leftarrow \{0,1\}^\ell$, $\mathbf{u} \leftarrow \mathbb{Z}_p^k$ and $\widehat{\mathbf{k}} \leftarrow \mathsf{span}(\mathbf{A}_{23}^\dagger)$.

3.4 Proof

We prove the following technical lemma that implies Theorem 1 (see Section 2.2 and Lemma 1).

Lemma 4. *For all PPT adversaries $\mathcal{A}$ making at most Q_C and Q_K queries to $\mathsf{O}_{\mathsf{Enc}}$ and $\mathsf{O}_{\mathsf{KeyGen}}$, respectively, there exist $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ with $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\begin{aligned}\mathsf{mKDMAdv}_{\mathcal{A}}^{\text{CPA}}(\lambda) \le{}& \mathsf{poly}(\ell, Q_C, Q_K) \cdot \mathsf{Adv}_{\mathcal{B}_1}^{\mathbf{MDDH}_k}(\lambda) \\ &+ 2 \cdot \mathsf{Adv}_{\mathcal{B}_2}^{\textsc{CompHide}_{Q_C}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_3}^{\mathbf{MDDH}_{k,Q_C}}(\lambda) + 1/2^\lambda.\end{aligned}$$

We prove the lemma via the following game sequence, summarized in Fig. 1. For each query (x, F) to $\mathsf{O}_{\mathsf{Enc}}$, we represent the affine function F as $(\mathbf{f}, f) \in \mathbb{Z}_p^\ell \times \mathbb{Z}_p$ and define $F([\mathbf{k}]_T) = [\mathbf{f}^\top\mathbf{k} + f]_T$. Similar to our notation of linear function in Section 2.3, we also use F to indicate the corresponding affine function over $\mathbb{Z}_p$, namely, $F(\mathbf{k}) = \mathbf{f}^\top\mathbf{k} + f$.

Game G_0. This game is the mKDM-CPA security game $\mathbf{mKDM}_0$. Under

$$\mathsf{mpk} = ([\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top\mathbf{W}_1]_1, \ldots, [\mathbf{A}_1^\top\mathbf{W}_n]_1, [\mathbf{B}]_2, [\mathbf{W}_1\mathbf{B}]_2, \ldots, [\mathbf{W}_n\mathbf{B}]_2, [\mathbf{A}_1^\top\mathbf{k}]_T)$$

where $\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{\ell\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow \mathbb{Z}_p^{\ell\times(k+1)}$ and $\mathbf{k} \leftarrow \{0,1\}^\ell$, the oracles work as follows:

- on the i-th query y_i, with $i \in [Q_K]$, $\mathsf{O}_{\mathsf{KeyGen}}$ outputs

$$\mathsf{sk}_i = ([\mathbf{d}_i]_2, \mathsf{kE}(y_i, [\mathbf{k}]_2) \cdot \mathsf{rE}(y_i, [\mathbf{W}_1\mathbf{d}_i]_2, \ldots, [\mathbf{W}_n\mathbf{d}_i]_2)), \qquad \mathbf{d}_i \leftarrow \mathsf{span}(\mathbf{B}),$$

- on the j-th query (x_j, F_j), with $j \in [Q_C]$, $\mathsf{O}_{\mathsf{Enc}}$ parses F_j as $(\mathbf{f}_j, f_j)$ and outputs

$$\mathsf{ct}_j^* = ([\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top\mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top\mathbf{W}_n]_1), [\mathbf{c}_j^\top\mathbf{k} + \overbrace{\mathbf{f}_j^\top\mathbf{k} + f_j}^{F_j(\mathbf{k})}]_T), \quad \mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1).$$

By the definition, for all PPT adversaries $\mathcal{A}$, we have

$$\Pr[\langle \mathbf{mKDM}_0, \mathcal{A}\rangle = 1] = \Pr[\langle \mathsf{G}_0, \mathcal{A}\rangle = 1].$$

Game	sk_i	ct_j^*		Remark	Justification
	$\mathsf{kE}(y_i, ?)$	$C_{0,j}$	C_j		
0	$\mathbf{k}$	$\mathbf{c}_j^\top$	$\mathbf{c}_j^\top\mathbf{k} + \mathbf{f}_j^\top\mathbf{k} + f_j$	$\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1)$	$\mathbf{mKDM}_0$, $F_j(\mathbf{k}) = \mathbf{f}_j^\top\mathbf{k} + f_j$
1	$\mathbf{k} + \boxed{\widehat{\mathbf{k}}_i}$	$\mathbf{c}_j^\top$	$(\mathbf{c}_j^\top + \mathbf{f}_j^\top)\mathbf{k} + f_j$	$\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \boxed{\mathbf{A}_2})$ $\widehat{\mathbf{k}}_i \leftarrow \mathsf{span}(\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger)$	Nested dual-system argument, see Fig. 2
2	$\mathbf{k} + \widehat{\mathbf{k}}_i$	$\boxed{\mathbf{c}_j^\top - \mathbf{f}_j^\top}$	$\boxed{\mathbf{c}_j^\top}\mathbf{k} + f_j$		Lemma 2
3	$\mathbf{k} + \widehat{\mathbf{k}}_i$	$\mathbf{c}_j^\top - \mathbf{f}_j^\top$	$\overline{\mathbf{s}}_j^\top\mathbf{A}_1^\top\mathbf{k} +$ $\underline{\mathbf{s}}_j^\top\boxed{\mathbf{u}} + f_j$	$\mathbf{u}, \overline{\mathbf{s}}_j, \underline{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k$ $\mathbf{c}_j = \mathbf{A}_1\overline{\mathbf{s}}_j + \mathbf{A}_2\underline{\mathbf{s}}_j$	Lemma 3
4	$\mathbf{k} + \widehat{\mathbf{k}}_i$	$\mathbf{c}_j^\top - \mathbf{f}_j^\top$	$\boxed{m_j}$	$m_j \leftarrow \mathbb{Z}_p$	$([\underline{\mathbf{s}}_j^\top]_1, [\overline{\mathbf{s}}_j^\top\mathbf{A}_1^\top\mathbf{k} +$ $\underline{\mathbf{s}}_j^\top\mathbf{u} + f_j]_T) \approx_c$ $([\underline{\mathbf{s}}_j^\top]_1, [m_j]_T)$
5	$\mathbf{k} + \widehat{\mathbf{k}}_i$	$\mathbf{c}_j^\top - \cancel{\mathbf{f}_j^\top}$	m_j		Lemma 2
6	$\mathbf{k} + \widehat{\mathbf{k}}_i$	$\mathbf{c}_j^\top$	$\boxed{\mathbf{c}_j^\top\mathbf{k}} + m_j$		$m_j \approx_s m_j + \mathbf{c}_j^\top\mathbf{k}$
7	$\mathbf{k} + \cancel{\widehat{\mathbf{k}}_i}$	$\mathbf{c}_j^\top$	$\mathbf{c}_j^\top\mathbf{k} + m_j$	$\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \cancel{\mathbf{A}_2})$	$\mathbf{mKDM}_1$, analogous to G_1

Fig. 1. mKDM-CPA security proof of our ABE scheme. In column "sk_i", we let $\mathsf{sk}_i = (K_{0,i}, \vec{K}_{1,i})$ and only present the kE-part in $K_{0,i}$ and omit $[\cdot]_2$; in column "ct_j^*", we let $\mathsf{ct}_j^* = (C_{0,j}, \vec{C}_{1,j}, C_j)$, only show $C_{0,j}$, C_j and omit $[\cdot]_1$, $[\cdot]_T$, respectively. We also note that $\vec{C}_{1,j}$ in ct_j^* depends on $C_{0,j}$ in an obvious way, we do not show it in this figure.

Game G_1. We modify the distribution of all $\{\mathsf{sk}_i\}_{i\in[Q_K]}$ and $\{\mathsf{ct}_j^*\}_{j\in[Q_C]}$ as follows:

$$\mathsf{sk}_i = ([\mathbf{d}_i]_2, \mathsf{kE}(y_i, [\mathbf{k} + \boxed{\widehat{\mathbf{k}}_i}]_2) \cdot \mathsf{rE}(y_i, [\mathbf{W}_1\mathbf{d}_i]_2, \ldots, [\mathbf{W}_n\mathbf{d}_i]_2)),$$
$$\mathbf{d}_i \leftarrow \mathsf{span}(\mathbf{B}), \boxed{\widehat{\mathbf{k}}_i \leftarrow \mathsf{span}(\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger)},$$
$$\mathsf{ct}_j^* = ([\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top\mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top\mathbf{W}_n]_1), [(\mathbf{c}_j^\top + \mathbf{f}_j^\top)\mathbf{k} + f_j]_T),$$
$$\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \boxed{\mathbf{A}_2}).$$

We claim that $\mathsf{G}_0 \approx_c \mathsf{G}_1$ via nested dual system argument. In more detail, we have the following lemma and the detail will be given out in Section 3.5.

Lemma 5 ($\mathsf{G}_0 \approx_c \mathsf{G}_1$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\Pr[\langle \mathsf{G}_0, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{G}_1, \mathcal{A}\rangle = 1]| \le \mathsf{poly}(\ell, Q_C, Q_K) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathbf{MDDH}_k}(\lambda).$$

Game G_2. We modify the distribution of all $\{\mathsf{ct}_j^*\}_{j\in[Q_C]}$ as follows:

$$\mathsf{ct}_j^* = ([\boxed{\mathbf{c}_j^\top - \mathbf{f}_j^\top}]_1, \mathsf{sE}(x_j, [(\boxed{\mathbf{c}_j^\top - \mathbf{f}_j^\top})\mathbf{W}_1]_1, \ldots, [(\boxed{\mathbf{c}_j^\top - \mathbf{f}_j^\top})\mathbf{W}_n]_1), [\boxed{\mathbf{c}_j^\top}\mathbf{k} + f_j]_T).$$

We claim that $\mathsf{G}_1 \approx_c \mathsf{G}_2$. This follows from Lemma 2 which states that for any $\{\mathbf{f}_j\}_{j\in[Q_C]} \in (\mathbb{Z}_p^\ell)^{Q_C}$, we have

$$\{[\mathbf{c}_j]_1\}_{j\in[Q_C]} \approx_c \{[\mathbf{c}_j - \mathbf{f}_j]_1\}_{j\in[Q_C]} \quad \text{given} \quad \mathbf{A}_1, [\mathbf{A}_2]_1, \mathsf{basis}(\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger)$$

where $\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \mathbf{A}_2)$. In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 6 ($\mathsf{G}_1 \approx_c \mathsf{G}_2$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\Pr[\langle \mathsf{G}_1, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{G}_2, \mathcal{A}\rangle = 1]| \le \mathsf{Adv}_{\mathcal{B}}^{\textsc{CompHide}_{Q_C}}(\lambda).$$

Game G_3. We modify the distribution of all $\{\mathsf{ct}_j^*\}_{j\in[Q_C]}$ as follows:

$$\mathsf{ct}_j^* = ([\mathbf{c}_j^\top - \mathbf{f}_j^\top]_1, \mathsf{sE}(x_j, [(\mathbf{c}_j^\top - \mathbf{f}_j^\top)\mathbf{W}_1]_1, \ldots, [(\mathbf{c}_j^\top - \mathbf{f}_j^\top)\mathbf{W}_n]_1), [\bar{\mathbf{s}}_j^\top \mathbf{A}_1^\top \mathbf{k} + \underline{\mathbf{s}}_j^\top \boxed{\mathbf{u}} + f_j]_T)$$

where $\mathbf{u}, \bar{\mathbf{s}}_j, \underline{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k$ and $\mathbf{c}_j = \mathbf{A}_1\bar{\mathbf{s}}_j + \mathbf{A}_2\underline{\mathbf{s}}_j$. We claim that $\mathsf{G}_2 \approx_s \mathsf{G}_3$. This follows from Lemma 3 which asserts that, with probability $1 - 1/2^\lambda$, it holds that

$$(\overbrace{\mathbf{A}_1^\top, \mathbf{A}_1^\top\mathbf{k}}^{\mathsf{mpk}}, \mathbf{A}_2^\top, \underbrace{\boxed{\mathbf{A}_2^\top\mathbf{k}}}_{\mathsf{ct}_j^*}, \overbrace{\mathbf{A}_{23}^\dagger, \mathbf{k} + \widehat{\mathbf{k}}}^{\mathsf{sk}_i}) \approx_s (\mathbf{A}_1^\top, \mathbf{A}_1^\top\mathbf{k}, \mathbf{A}_2^\top, \boxed{\mathbf{u}}, \mathbf{A}_{23}^\dagger, \mathbf{k} + \widehat{\mathbf{k}})$$

where $\mathbf{k} \leftarrow \{0,1\}^\ell$, $\mathbf{u} \leftarrow \mathbb{Z}_p^k$ and $\widehat{\mathbf{k}} \leftarrow \mathsf{span}(\mathbf{A}_{23}^\dagger)$. Here we use $\mathbf{A}_1^\top$, $\mathbf{A}_1^\top\mathbf{k}$ to simulate mpk; all $\{\mathsf{ct}_j^*\}_{j\in[Q_C]}$ are simulated additionally with $\mathbf{A}_2^\top$, $\mathbf{A}_2^\top\mathbf{k}$ or $\mathbf{u}$; all $\{\mathsf{sk}_i\}_{i\in[Q_K]}$ are simulated using $(\mathbf{k} + \widehat{\mathbf{k}}) + \widetilde{\mathbf{k}}_i$ with $\widetilde{\mathbf{k}}_i \leftarrow \mathsf{span}(\mathbf{A}_{23}^\dagger)$, namely we implicitly set $\widehat{\mathbf{k}}_i = \widehat{\mathbf{k}} + \widetilde{\mathbf{k}}_i$. In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 7 ($\mathsf{G}_2 \approx_s \mathsf{G}_3$). *For all PPT adversaries $\mathcal{A}$,*

$$|\Pr[\langle \mathsf{G}_2, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{G}_3, \mathcal{A}\rangle = 1]| \le 1/2^\lambda.$$

Game G_4. We modify the distribution of all $\{\mathsf{ct}_j^*\}_{j\in[Q_C]}$ as follows:

$$\mathsf{ct}_j^* = ([\mathbf{c}_j^\top - \mathbf{f}_j^\top]_1, \mathsf{sE}(x_j, [(\mathbf{c}_j^\top - \mathbf{f}_j^\top)\mathbf{W}_1]_1, \ldots, [(\mathbf{c}_j^\top - \mathbf{f}_j^\top)\mathbf{W}_n]_1), [\boxed{m_j}]_T), \qquad m_j \leftarrow \mathbb{Z}_p,$$

where $\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \mathbf{A}_2)$. We claim that $\mathsf{G}_3 \approx_c \mathsf{G}_4$. This follows from $\mathbf{MDDH}_{k,Q_C}$ which implies that, for all $\{\bar{\mathbf{s}}_j^\top \mathbf{A}_1^\top \mathbf{k} + f_j\}_{j\in[Q_C]} \in \mathbb{Z}_p^{Q_C}$ with $\bar{\mathbf{s}}_j \in \mathbb{Z}_p^k$, we have

$$\{[\underline{\mathbf{s}}_j^\top]_1, [\bar{\mathbf{s}}_j^\top \mathbf{A}_1^\top \mathbf{k} + \underline{\mathbf{s}}_j^\top \mathbf{u} + f_j]_T\}_{j\in[Q_C]} \approx_c \{[\underline{\mathbf{s}}_j^\top]_1, [m_j]_T\}_{j\in[Q_C]}$$

where $\mathbf{u}, \underline{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k$ and $m_j \leftarrow \mathbb{Z}_p$. Note that we will set $\mathbf{c}_j = \mathbf{A}_1\bar{\mathbf{s}}_j + \mathbf{A}_2\underline{\mathbf{s}}_j$. In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 8 ($\mathsf{G}_3 \approx_c \mathsf{G}_4$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\Pr[\langle \mathsf{G}_3, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{G}_4, \mathcal{A}\rangle = 1]| \le \mathsf{Adv}_{\mathcal{B}}^{\mathbf{MDDH}_{k,Q_C}}(\lambda).$$

Game G_5. We modify the distribution of all $\{\mathsf{ct}_j^*\}_{j\in[Q_C]}$ as follows:

$$\mathsf{ct}_j^* = ([\mathbf{c}_j^\top - \cancel{\mathbf{f}_j}]_1, \mathsf{sE}(x_j, [(\mathbf{c}_j^\top - \cancel{\mathbf{f}_j})\mathbf{W}_1]_1, \ldots, [(\mathbf{c}_j^\top - \cancel{\mathbf{f}_j})\mathbf{W}_n]_1), [m_j]_T), \qquad m_j \leftarrow \mathbb{Z}_p.$$

We claim that $\mathsf{G}_4 \approx_c \mathsf{G}_5$ via Lemma 2 that is analogous to $\mathsf{G}_1 \approx_c \mathsf{G}_2$. In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 9 ($\mathsf{G}_4 \approx_c \mathsf{G}_5$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\Pr[\langle \mathsf{G}_4, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{G}_5, \mathcal{A}\rangle = 1]| \leq \mathsf{Adv}_{\mathcal{B}}^{\textsc{CompHide}_{Q_C}}(\lambda).$$

Game G_6. We modify the distribution of all $\{\mathsf{ct}_j^*\}_{j\in[Q_C]}$ as follows:

$$\mathsf{ct}_j^* = ([\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top \mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top \mathbf{W}_n]_1), [\boxed{\mathbf{c}_j^\top \mathbf{k}} + m_j]_T).$$

We claim that $\mathsf{G}_5 \approx_s \mathsf{G}_6$. This follows from the fact that, for all $\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \mathbf{A}_2)$ and $\mathbf{k} \leftarrow \{0,1\}^\ell$, it holds that

$$\{m_j\}_{j\in[Q_C]} \approx_s \{m_j + \mathbf{c}_j^\top \mathbf{k}\}_{j\in[Q_C]}$$

where $m_j \leftarrow \mathbb{Z}_p$. In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 10 ($\mathsf{G}_5 \approx_s \mathsf{G}_6$). *For all PPT adversaries $\mathcal{A}$,*

$$\Pr[\langle \mathsf{G}_5, \mathcal{A}\rangle = 1] = \Pr[\langle \mathsf{G}_6, \mathcal{A}\rangle = 1].$$

Game G_7. We modify the distribution of all $\{\mathsf{sk}_i\}_{i\in[Q_K]}$ and $\{\mathsf{ct}_j^*\}_{j\in[Q_C]}$ as follows:

$$\mathsf{sk}_i = ([\mathbf{d}_i]_2, \mathsf{kE}(y_i, [\mathbf{k} + \cancel{\widehat{\mathbf{k}}_i}]_2) \cdot \mathsf{rE}(y_i, [\mathbf{W}_1\mathbf{d}_i]_2, \ldots, [\mathbf{W}_n\mathbf{d}_i]_2)),$$
$$\mathsf{ct}_j^* = ([\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top \mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top \mathbf{W}_n]_1), [\mathbf{c}_j^\top \mathbf{k} + m_j]_T), \qquad \mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \cancel{\mathbf{A}_2}).$$

We claim that $\mathsf{G}_6 \approx_c \mathsf{G}_7$ via nested dual system argument that is analogous to $\mathsf{G}_0 \approx_c \mathsf{G}_1$. In more detail, we have the following lemma and the detail will be given out in Section 3.5.

Lemma 11 ($\mathsf{G}_6 \approx_c \mathsf{G}_7$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\Pr[\langle \mathsf{G}_6, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{G}_7, \mathcal{A}\rangle = 1]| \leq \mathsf{poly}(\ell, Q_C, Q_K) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathbf{MDDH}_k}(\lambda).$$

Furthermore, G_7 is exactly the same as mKDM-CPA security game $\mathbf{mKDM}_1$. By the definition, for all PPT adversaries $\mathcal{A}$, we have

$$\Pr[\langle \mathsf{G}_7, \mathcal{A}\rangle = 1] = \Pr[\langle \mathbf{mKDM}_1, \mathcal{A}\rangle = 1].$$

This completes the proof of Lemma 4 that implies Theorem 1.

3.5 Nested Dual-System Argument

Overview. This section proves Lemma 5 ($\mathsf{G}_0 \approx_c \mathsf{G}_1$) and Lemma 11 ($\mathsf{G}_6 \approx_c \mathsf{G}_7$). As both arguments are irrelevant to $\mathbf{k}$, we will neglect $\mathbf{k}$-related terms $[(\mathbf{c}_j^\top + \mathbf{f}_j^\top)\mathbf{k} + f_j]_T$ or $[\mathbf{c}_j^\top \mathbf{k} + m_j]_T$ in ct_j^* and $\mathsf{kE}(y_i, [\mathbf{k}]_2)$ in sk_i for now. More concretely, we will focus on the following statement that allows us to simulate the actual ciphertexts and secret keys in Lemma 5 and Lemma 11.

$$\left(\begin{array}{ll} \mathsf{mpk} : [\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top \mathbf{W}_1]_1, \ldots, [\mathbf{A}_1^\top \mathbf{W}_n]_1, [\mathbf{B}]_2, [\mathbf{W}_1\mathbf{B}]_2, \ldots, [\mathbf{W}_n\mathbf{B}]_2 & \\ \mathsf{sk}_i : [\mathbf{d}_i]_2, \boxed{\mathsf{rE}(y_i, [\mathbf{W}_1\mathbf{d}_i]_2, \ldots, [\mathbf{W}_n\mathbf{d}_i]_2)}, & \mathbf{d}_i \leftarrow \mathsf{span}(\mathbf{B}) \\ \mathsf{ct}_j^* : [\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top \mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top \mathbf{W}_n]_1), & \boxed{\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1)} \end{array}\right) \approx_c$$

$$\left(\begin{array}{ll} \mathsf{mpk} : [\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top \mathbf{W}_1]_1, \ldots, [\mathbf{A}_1^\top \mathbf{W}_n]_1, [\mathbf{B}]_2, [\mathbf{W}_1\mathbf{B}]_2, \ldots, [\mathbf{W}_n\mathbf{B}]_2 & \\ \mathsf{sk}_i : [\mathbf{d}_i]_2, \mathsf{kE}(y_i, [\widehat{\mathbf{k}}_i]_2) \cdot \mathsf{rE}(y_i, [\mathbf{W}_1\mathbf{d}_i]_2, \ldots, [\mathbf{W}_n\mathbf{d}_i]_2), & \mathbf{d}_i \leftarrow \mathsf{span}(\mathbf{B}) \\ \mathsf{ct}_j^* : [\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top \mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top \mathbf{W}_n]_1), & \mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_{12}) \end{array}\right) \tag{15}$$

where indices i and j go over $[Q_K]$ and $[Q_C]$, respectively; $\mathbf{W}_1, \ldots, \mathbf{W}_n \leftarrow \mathbb{Z}_p^{\ell \times (k+1)}$, $\widehat{\mathbf{k}}_i \leftarrow \mathsf{span}(\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger)$. Observe that

- for Lemma 5, LHS and RHS in (15) correspond to G_0 and G_1, respectively; we can simulate the omitted terms $[(\mathbf{c}_j^\top + \mathbf{f}_j^\top)\mathbf{k} + f_j]_T$ and $\mathsf{kE}(y_i, [\mathbf{k}]_2)$ by sampling $\mathbf{k} \leftarrow \{0,1\}^\ell$ by ourselves;
- for Lemma 11, LHS and RHS in (15) correspond to G_7 and G_6, respectively; we can simulate the omitted terms $[\mathbf{c}_j^\top \mathbf{k} + m_j]_T$ and $\mathsf{kE}(y_i, [\mathbf{k}]_2)$ by sampling $\mathbf{k} \leftarrow \{0,1\}^\ell$ and $m_j \leftarrow \mathbb{Z}_p$ by ourselves;

More formally, let $\mathsf{Adv}^{\text{NesDualSys}}(\lambda)$ be the advantage function of distinguishing LHS and RHS in (15).

Bounding $\mathsf{Adv}^{\mathbf{NesDualSys}}(\boldsymbol{\lambda})$. In the remaining of this section, we bound $\mathsf{Adv}^{\text{NesDualSys}}(\lambda)$ as follow:

Lemma 12. *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\begin{aligned} \mathsf{Adv}_{\mathcal{A}}^{\text{NesDualSys}}(\lambda) &\le 4Q_K \cdot \mathsf{Adv}^{\mathbf{MDDH}_k}(\lambda) + Q_C \cdot \Big(\mathsf{Adv}^{\mathbf{SD}_{\mathbf{A}_1 \mapsto \mathbf{A}_{13}}}(\lambda) \\ &\qquad + 4Q_K \cdot \mathsf{Adv}^{\mathbf{MDDH}_k}(\lambda) + \mathsf{Adv}^{\mathbf{SD}_{\mathbf{A}_3 \mapsto \mathbf{A}_2}}(\lambda)\Big) \\ &\le \mathsf{poly}(\ell, Q_K, Q_C) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathbf{MDDH}_k}(\lambda). \end{aligned}$$

This readily proves Lemma 5 and Lemma 11. To prove the lemma, we use the following game sequence, summarized in Fig 2, and prove that

$$\mathsf{H}_0 \approx_c \mathsf{H}_{1.0} \approx_c \cdots \approx_c \mathsf{H}_{1.4} = \mathsf{H}_{2.0} \approx_c \cdots \approx_c \mathsf{H}_{Q_C.4} \approx_c \mathsf{H}_{Q_C+1}$$

where "=" and "$\approx_c$" mean two games are exactly identical and computationally indistinguishable, respectively.

Game	sk_i	ct^*_j			Justification
	$\widehat{\mathbf{k}}_i \leftarrow \mathsf{span}(?)$	$\mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, ?)$			
		$j < \hat{\jmath}$	$j = \hat{\jmath}$	$j > \hat{\jmath}$	
0	—	—			LHS in (15)
$\hat{\jmath}.0$	$\mathbf{A}_2^\dagger$	$\mathbf{A}_2$	—		α-privacy, cf. [CGW15] for $\hat{\jmath} = 1$; $\mathsf{H}_{\hat{\jmath}.0} = \mathsf{H}_{\hat{\jmath}-1.4}$ for $\hat{\jmath} > 1$
$\hat{\jmath}.1$	$\mathbf{A}_2^\dagger$	$\mathbf{A}_2$	$\mathbf{A}_3$	—	$(\mathbf{A}_2^\dagger, [\mathsf{span}(\mathbf{A}_1)]_1) \approx_c (\mathbf{A}_2^\dagger, [\mathsf{span}(\mathbf{A}_1, \mathbf{A}_3)]_1)$
$\hat{\jmath}.2$	$\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger$	$\mathbf{A}_2$	$\mathbf{A}_3$	—	α-privacy, cf. [CGW15]
$\hat{\jmath}.3$	$\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger$	$\mathbf{A}_2$	$\mathbf{A}_2$	—	$(\mathsf{basis}(\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger), [\mathsf{span}(\mathbf{A}_3)]_1) \approx_c (\mathsf{basis}(\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger), [\mathsf{span}(\mathbf{A}_2)]_1)$
$\hat{\jmath}.4$	$\mathbf{A}_2^\dagger$	$\mathbf{A}_2$		—	analogous to $\mathsf{H}_{\hat{\jmath}.2}$
$Q_C + 1$	$\mathbf{A}_2^\dagger, \mathbf{A}_3^\dagger$	$\mathbf{A}_2$			RHS in (15), analogous to $\mathsf{H}_{\hat{\jmath}.2}$

Fig. 2. Game sequence for nested dual-system argument ($\hat{\jmath} \in [Q_C]$)

Game H_0. In this game, the adversary $\mathcal{A}$ is given LHS in (15).

Game $\mathsf{H}_{\hat{\jmath}.0}$ ($\hat{\jmath} \in [Q_C]$). In this game, the distribution of all $\{\mathsf{sk}_i\}_{i\in[Q_K]}$ and $\{\mathsf{ct}^*_j\}_{j\in[Q_C]}$ is as follows:

$$\mathsf{sk}_i : [\mathbf{d}_i]_2, \boxed{\mathsf{kE}(y_i, [\widehat{\mathbf{k}}_i]_2)} \cdot \mathsf{rE}(y_i, [\mathbf{W}_1\mathbf{d}_i]_2, \ldots, [\mathbf{W}_n\mathbf{d}_i]_2), \quad \mathbf{d}_i \leftarrow \mathsf{span}(\mathbf{B}), \widehat{\mathbf{k}}_i \leftarrow \mathsf{span}(\mathbf{A}_2^\dagger),$$
$$\mathsf{ct}^*_j(j < \hat{\jmath}) : [\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top\mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top\mathbf{W}_n]_1), \quad \mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \mathbf{A}_2),$$
$$\mathsf{ct}^*_j(j = \hat{\jmath}) : [\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top\mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top\mathbf{W}_n]_1), \quad \mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1),$$
$$\mathsf{ct}^*_j(j > \hat{\jmath}) : [\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top\mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top\mathbf{W}_n]_1), \quad \mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1).$$

We note that $\mathsf{H}_{\hat{\jmath}.0} = \mathsf{H}_{\hat{\jmath}-1.4}$ for $\hat{\jmath} > 1$. Furthermore, we claim that $\mathsf{H}_0 \approx_c \mathsf{H}_{1.0}$. This follows from the dual-system argument in [CGW15]: first switch $\mathbf{d}_i$ to $\mathbb{Z}_p^{k+1}$ by $\mathbf{MDDH}_k$ assumption stating that

$$([\mathbf{B}]_2, [\mathsf{span}(\mathbf{B})]_2) \approx_c ([\mathbf{B}]_2, [\mathbb{Z}_p^{k+1}]_2),$$

program $\mathbf{W}_t$ for all $t \in [n]$ via the change of variable

$$\mathbf{W}_t \mapsto \mathbf{W}_t + \mathbf{A}_2^\dagger \mathbf{w}_t (\mathbf{b}^\dagger)^\top \quad \text{where} \quad \mathbf{w}_t \leftarrow \mathbb{Z}_p^{\ell_2}$$

ensuring $\mathbf{w}_t$ only leaked by sk_i, then use α-privacy of predicate encoding with $\mathbf{w}_t$ (cf. (9)), finally switch $\mathbf{d}_i$ back by $\mathbf{MDDH}_k$ assumption again. In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 13 ($\mathsf{H}_0 \approx_c \mathsf{H}_{1.0}$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\Pr[\langle \mathsf{H}_0, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{H}_{1.0}, \mathcal{A}\rangle = 1]| \le 2Q_K \cdot \mathsf{Adv}^{\mathbf{MDDH}_k}(\lambda).$$

Game $\mathsf{H}_{\hat{\jmath}.1}(\hat{\jmath} \in [Q_C])$. We change the distribution of ct_j^* for $j = \hat{\jmath}$ as follows:

$$\mathsf{ct}_j^*(j = \hat{\jmath}) : [\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top \mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top \mathbf{W}_n]_1), \qquad \mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \boxed{\mathbf{A}_3}).$$

We claim that $\mathsf{H}_{\hat{\jmath}.0} \approx_c \mathsf{H}_{\hat{\jmath}.1}$ for all $\hat{\jmath} \in [Q_C]$ by $\mathbf{SD}_{\mathbf{A}_1 \mapsto \mathbf{A}_{13}}$ assumption (cf. Lemma 1). In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 14 ($\mathsf{H}_{\hat{\jmath}.0} \approx_c \mathsf{H}_{\hat{\jmath}.1}$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\Pr[\langle \mathsf{H}_{\hat{\jmath}.0}, \mathcal{A} \rangle = 1] - \Pr[\langle \mathsf{H}_{\hat{\jmath}.1}, \mathcal{A} \rangle = 1]| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathbf{SD}_{\mathbf{A}_1 \mapsto \mathbf{A}_{13}}}(\lambda).$$

Game $\mathsf{H}_{\hat{\jmath}.2}(\hat{\jmath} \in [Q_C])$. We change the distribution of all $\{\mathsf{sk}_i\}_{i \in [Q_K]}$ as follows:

$$\mathsf{sk}_i : [\mathbf{d}_i]_2, \mathsf{kE}(y_i, [\widehat{\mathbf{k}}_i]_2) \cdot \mathsf{rE}(y_i, [\mathbf{W}_1 \mathbf{d}_i]_2, \ldots, [\mathbf{W}_n \mathbf{d}_i]_2), \qquad \widehat{\mathbf{k}}_i \leftarrow \mathsf{span}(\mathbf{A}_2^\dagger, \boxed{\mathbf{A}_3^\dagger}).$$

We claim that $\mathsf{H}_{\hat{\jmath}.1} \approx_c \mathsf{H}_{\hat{\jmath}.2}$ for all $\hat{\jmath} \in [Q_C]$. This is analogous to $\mathsf{H}_0 \approx_c \mathsf{H}_{1.0}$ except that we ensure $\mathbf{w}_t$ only leaked by sk_i and $\mathsf{ct}_{\hat{\jmath}}$ and then use α-privacy of predicate encoding with $\mathbf{w}_t$ (cf. (9)). In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 15 ($\mathsf{H}_{\hat{\jmath}.1} \approx_c \mathsf{H}_{\hat{\jmath}.2}$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\Pr[\langle \mathsf{H}_{\hat{\jmath}.1}, \mathcal{A} \rangle = 1] - \Pr[\langle \mathsf{H}_{\hat{\jmath}.2}, \mathcal{A} \rangle = 1]| \leq 2Q_K \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathbf{MDDH}_k}(\lambda).$$

Game $\mathsf{H}_{\hat{\jmath}.3}(\hat{\jmath} \in [Q_C])$. We change the distribution of ct_j^* for $j = \hat{\jmath}$ as follows:

$$\mathsf{ct}_j^*(j = \hat{\jmath}) : [\mathbf{c}_j^\top]_1, \mathsf{sE}(x_j, [\mathbf{c}_j^\top \mathbf{W}_1]_1, \ldots, [\mathbf{c}_j^\top \mathbf{W}_n]_1), \qquad \mathbf{c}_j \leftarrow \mathsf{span}(\mathbf{A}_1, \boxed{\mathbf{A}_2}).$$

We claim that $\mathsf{H}_{\hat{\jmath}.2} \approx_c \mathsf{H}_{\hat{\jmath}.3}$ for all $\hat{\jmath} \in [Q_C]$ by $\mathbf{SD}_{\mathbf{A}_3 \mapsto \mathbf{A}_2}$ assumption (cf. Lemma 1). In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 16 ($\mathsf{H}_{\hat{\jmath}.2} \approx_c \mathsf{H}_{\hat{\jmath}.3}$). *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\Pr[\langle \mathsf{H}_{\hat{\jmath}.2}, \mathcal{A} \rangle = 1] - \Pr[\langle \mathsf{H}_{\hat{\jmath}.3}, \mathcal{A} \rangle = 1]| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathbf{SD}_{\mathbf{A}_3 \mapsto \mathbf{A}_2}}(\lambda).$$

Game $\mathsf{H}_{\hat{\jmath}.4}(\hat{\jmath} \in [Q_C])$. We change the distribution of all $\{\mathsf{sk}_i\}_{i \in [Q_K]}$ as follows:

$$\mathsf{sk}_i : [\mathbf{d}_i]_2, \mathsf{kE}(y_i, [\widehat{\mathbf{k}}_i]_2) \cdot \mathsf{rE}(y_i, [\mathbf{W}_1 \mathbf{d}_i]_2, \ldots, [\mathbf{W}_n \mathbf{d}_i]_2), \qquad \widehat{\mathbf{k}}_i \leftarrow \mathsf{span}(\mathbf{A}_2^\dagger, \cancel{\mathbf{A}_3^\dagger}).$$

We claim that $\mathsf{H}_{\hat{\jmath}.3} \approx_c \mathsf{H}_{\hat{\jmath}.4}$ for all $j \in [Q_C]$. This is analogous to $\mathsf{H}_{\hat{\jmath}.1} \approx_c \mathsf{H}_{\hat{\jmath}.2}$. In more detail, we have the following lemma and the proof is deferred to the full paper. We note that $\mathsf{H}_{\hat{\jmath}.4}$ is exactly the same as $\mathsf{H}_{\hat{\jmath}+1.1}$ for all $j \in [Q_C - 1]$.

Lemma 17 ($\mathsf{H}_{\hat{\jmath}.3} \approx_c \mathsf{H}_{\hat{\jmath}.4}$)**.** *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\Pr[\langle \mathsf{H}_{\hat{\jmath}.3}, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{H}_{\hat{\jmath}.4}, \mathcal{A}\rangle = 1]| \leq 2Q_K \cdot \mathsf{Adv}^{\mathbf{MDDH}_k}_{\mathcal{B}}(\lambda).$$

Game H_{Q_C+1}. We change the distribution of all $\{\mathsf{sk}_i\}_{i\in[Q_K]}$ as follows:

$$\mathsf{sk}_i : [\mathbf{d}_i]_2, \mathsf{kE}(y_i, [\widehat{\mathbf{k}}_i]_2) \cdot \mathsf{rE}(y_i, [\mathbf{W}_1\mathbf{d}_i]_2, \ldots, [\mathbf{W}_n\mathbf{d}_i]_2), \qquad \widehat{\mathbf{k}}_i \leftarrow \mathsf{span}(\mathbf{A}_2^\dagger, \boxed{\mathbf{A}_3^\dagger}).$$

We claim that $\mathsf{H}_{Q_C.4} \approx_c \mathsf{H}_{Q_C+1}$. This is analogous to $\mathsf{H}_{\hat{\jmath}.1} \approx_c \mathsf{H}_{\hat{\jmath}.2}$. In more detail, we have the following lemma and the proof is deferred to the full paper.

Lemma 18 ($\mathsf{H}_{Q_C.4} \approx_c \mathsf{H}_{Q_C+1}$)**.** *For all PPT adversaries $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\Pr[\langle \mathsf{H}_{Q_C.4}, \mathcal{A}\rangle = 1] - \Pr[\langle \mathsf{H}_{Q_C+1}, \mathcal{A}\rangle = 1]| \leq 2Q_K \cdot \mathsf{Adv}^{\mathbf{MDDH}_k}_{\mathcal{B}}(\lambda).$$

We note that H_{Q_C+1} is exactly the same as RHS in (15). This is sufficient to bound $\mathsf{Adv}^{\text{NesDualSys}}(\lambda)$.

4 Delegation

In this section, we will show how to support delegable predicates. A predicate $P : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ is said to be delegable if there exists a *strong partial ordering* $\prec$ on $\mathcal{Y}$ such that

$$(y' \prec y) \wedge P(x,y') = 1 \implies P(x,y) = 1 \qquad \forall\, x \in \mathcal{X}.$$

Delegation in ABE. An ABE scheme for a delegable predicate $P : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ consists of algorithms Setup, KeyGen, Enc, Dec as defined in Section 2.1 and an extra delegation algorithm:

- $\mathsf{Del}(\mathsf{mpk}, \mathsf{sk}_y, y') \to \mathsf{sk}_{y'}$. The delegation algorithm takes as input the master public key mpk, a secret key sk_y for $y \in \mathcal{Y}$ and a $y' \in \mathcal{Y}$ satisfying $y' \prec y$, outputs a secret key $\mathsf{sk}_{y'}$ for y'.

We further require that, for all $y, y' \in \mathcal{Y}$ satisfying $y' \prec y$, it holds that

$$\{\, \mathsf{sk}_{y'} \leftarrow \mathsf{Del}(\mathsf{mpk}, \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y), y') \,\} \equiv \{\, \mathsf{sk}_{y'} \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y') \,\}$$

If it does not hold, one should turn to the security model described in [SW08].

Delegable Predicate Encoding. A $\mathbb{Z}_p$-linear predicate encoding for delegable predicate P is composed of algorithms $\mathsf{sE}, \mathsf{sD}, \mathsf{rE}, \mathsf{kE}, \mathsf{rD}$ and an extra algorithm

$$\mathsf{dE} : \mathcal{Y} \times \mathcal{Y} \times \mathbb{Z}_p^{n_r} \to \mathbb{Z}_p^{n'_r}$$

with the following features:

(linearity). For all $y, y' \in \mathcal{Y}$, $\mathsf{dE}(y, y', \cdot)$ is $\mathbb{Z}_p$-linear (see Eq. (7)).
(delegability). For all $y, y' \in \mathcal{Y}$ with $y' \prec y$, $\alpha \in \mathbb{Z}_p$ and $\mathbf{w} \leftarrow \mathbb{Z}_p^n$, it holds

$$\mathsf{dE}(y, y', \mathsf{kE}(y, \alpha) + \mathsf{rE}(y, \mathbf{w})) = \mathsf{kE}(y', \alpha) + \mathsf{rE}(y', \mathbf{w}). \tag{16}$$

Example for n-level HIBE [BBG05]. In a n-level HIBE with $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_p^n$, if $\mathbf{y}$ is a prefix of $\mathbf{y}'$ then we say $\mathbf{y}' \prec \mathbf{y}$. Let $\mathbf{x} = (x_1, \ldots, x_{n_x})$, $\mathbf{y} = (y_1, \ldots, y_{n_y})$, $\mathbf{y}' = (y_1, \ldots, y_{n'_y})$ for $n_x, n_y, n'_y \leq n$ and $\mathbf{y}' \prec \mathbf{y}$. Let $\mathbf{w} \leftarrow \mathbb{Z}_p^{1\times(n+1)}$, we have

$$\mathsf{sE}(\mathbf{x}, \mathbf{w}) \coloneqq \mathbf{w} \left(1 \ \mathbf{x} \ \mathbf{0}_{n-n_x}\right)^\top \qquad \mathsf{sD}(\mathbf{x}, \mathbf{y}, c) \coloneqq c$$

$$\mathsf{rE}(\mathbf{y}, \mathbf{w}) \coloneqq \mathbf{w} \begin{pmatrix} 1 & \mathbf{y} \\ & \mathbf{I}_{n-n_y} \end{pmatrix}^\top \qquad \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{k}) \coloneqq \mathbf{k} \left(1 \ x_{n_y+1} \ \ldots \ x_{n_x} \ \mathbf{0}_{n-n_x}\right)^\top$$

$$\mathsf{kE}(\mathbf{y}, \alpha) \coloneqq \left(\alpha \ \mathbf{0}_{n-n_y}\right) \qquad \mathsf{dE}(\mathbf{y}, \mathbf{y}', \mathbf{k}') \coloneqq \mathbf{k}' \begin{pmatrix} 1 & y_{n_y} & \ldots & y_{n'_y} \\ & & & \mathbf{I}_{n-n'_y} \end{pmatrix}^\top$$

Scheme. Our delegable ABE scheme is basically the ABE scheme in Section 3.2 equipped with an additional algorithm Del that works as follows:

– $\mathsf{Del}(\mathsf{mpk}, \mathsf{sk}_y, y')$: Parse $\mathsf{sk}_y = (K_0, \overrightarrow{K}_1)$, pick $\mathbf{r}' \leftarrow \mathbb{Z}_p^k$ and output

$$\mathsf{sk}_{y'} \coloneqq (K_0 \cdot [\mathbf{B}\mathbf{r}']_2, \mathsf{dE}(y, y', \overrightarrow{K}_1) \cdot \mathsf{rE}(y', [\mathbf{W}_1\mathbf{B}\mathbf{r}']_2, \ldots, [\mathbf{W}_n\mathbf{B}\mathbf{r}']_2)).$$

As secret keys generated by KeyGen and Del are indistinguishable, the proof in Section 3.4 is sufficient to prove that our scheme for delegable predicates can also achieve mKDM-CPA security.

5 CPA-to-CCA Transformation

This section revisits the classical CPA-to-CCA transformation by Canetti, Halevi and Katz [CHK04] (CHK transformation). We remark that the basic idea is not new which is also used in previous work for CCA secure ABE [YAHK11, BL16, CMP17]; this section is to show that the idea indeed works for mKDM security.

IBE-enhanced Predicate. Given a delegable predicate $P : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ with partial ordering $\prec$ on $\mathcal{Y}$, we define its IBE-enhanced version $\overline{P} : \overline{\mathcal{X}} \times \overline{\mathcal{Y}} \to \{0, 1\}$ as

$$\overline{\mathcal{X}} = \mathcal{X} \times \mathbb{Z}_p,$$
$$\overline{\mathcal{Y}} = \mathcal{Y} \times (\mathbb{Z}_p \cup \{\star\}),$$
$$\overline{P}((x, \mathsf{id}), (y, \mathsf{id}')) = \begin{cases} P(x, y) \wedge (\mathsf{id} = \mathsf{id}') & \mathsf{id}' \neq \star \\ P(x, y) & \mathsf{id}' = \star \end{cases}$$

along with strong partial ordering $\overline{\prec}$ on $\overline{\mathcal{Y}}$ is defined as follows:

$$(y', \mathsf{id}) \overline{\prec} (y', \star) \overline{\prec} (y, \star), \quad \forall\, y' \prec y \in \mathcal{Y},\ \mathsf{id} \in \mathbb{Z}_p$$

where $\star$ is a special symbol. Here the first $\overline{\prec}$ involves IBE-part that is used to embed verification key of an one-time signature scheme as CHK transformation; the second $\overline{\prec}$ preserves the delegation in P. Note that we consider *delegable* predicate and all discussions naturally cover the case *without* delegation.

Transformation (informal). Assuming a predicate encoding for $\overline{P} : \overline{\mathcal{X}} \times \overline{\mathcal{Y}} \to \{0,1\}$ as defined above for $P : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, Section 4 gives us a mKDM-CPA secure scheme $(\overline{\mathsf{Setup}}, \overline{\mathsf{Enc}}, \overline{\mathsf{KeyGen}}, \overline{\mathsf{Dec}}, \overline{\mathsf{Del}})$ for $\overline{P}$. Our mKDM-CCA secure ABE $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{KeyGen}, \mathsf{Dec}, \mathsf{Del})$ for P follows the CHK transformation:

- $\mathsf{Setup}(1^\lambda, P) = \overline{\mathsf{Setup}}(1^\lambda, \overline{P})$ outputs $(\mathsf{mpk}, \mathsf{msk})$;
- $\mathsf{Enc}(\mathsf{mpk}, x, m)$ outputs $(\mathsf{vk}, \overline{\mathsf{ct}} = \overline{\mathsf{Enc}}(\mathsf{mpk}, (x, \mathsf{vk}), m), \sigma = \mathsf{Sign}(\mathsf{sigk}, \overline{\mathsf{ct}}))$ where $(\mathsf{sigk}, \mathsf{vk})$ is a fresh key pair of a strong one-time signature scheme;
- $\mathsf{KeyGen}(\mathsf{msk}, y) = \overline{\mathsf{KeyGen}}(\mathsf{msk}, (y, \star))$ outputs sk_y;
- $\mathsf{Del}(\mathsf{msk}, \mathsf{sk}_y, y') = \overline{\mathsf{Del}}(\mathsf{msk}, \mathsf{sk}_y, (y', \star))$ outputs $\mathsf{sk}_{y'}$;
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x)$ outputs $\overline{\mathsf{Dec}}(\mathsf{mpk}, \overline{\mathsf{Del}}(\mathsf{mpk}, \mathsf{sk}_y, (y, \mathsf{vk})), \overline{\mathsf{ct}})$ if σ is a valid signature for $\overline{\mathsf{ct}}$ under vk.

See the full paper for formal transformation and security analysis.

Generic Construction. Given a predicate encoding $(\mathsf{sE}, \mathsf{rE}, \mathsf{kE}, \mathsf{sD}, \mathsf{rD}, \mathsf{dE})$ for $P : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ with parameter n, n_s, n_r, the predicate encoding $(\overline{\mathsf{sE}}, \overline{\mathsf{rE}}, \overline{\mathsf{kE}}, \overline{\mathsf{sD}}, \overline{\mathsf{rD}}, \overline{\mathsf{dE}})$ for $\overline{P} : \overline{\mathcal{X}} \times \overline{\mathcal{Y}} \to \{0,1\}$ has parameter

$$\overline{n} = n + 2, \quad \overline{n}_s = n_s + 1, \quad \overline{n}_r = \begin{cases} n_r + 1 & \mathsf{id}' \neq \star \\ n_r + 2 & \mathsf{id}' = \star \end{cases}$$

and is defined as follows: for $(x, y) \in \mathcal{X} \times \mathcal{Y}$ and $\mathsf{id}, \mathsf{id}' \in \mathbb{Z}_p \cup \{\star\}$,

$$\begin{aligned}
\overline{\mathsf{sE}}((x, \mathsf{id}), (\mathbf{w}, w_1, w_2)) &:= (\mathsf{sE}(x, \mathbf{w}), w_1 + \mathsf{id} \cdot w_2) \quad (\mathsf{id} \neq \star) \\
\overline{\mathsf{rE}}((y, \mathsf{id}), (\mathbf{w}, w_1, w_2)) &:= \begin{cases} (\mathsf{rE}(y, \mathbf{w}), w_1 + \mathsf{id} \cdot w_2) & \mathsf{id} \neq \star \\ (\mathsf{rE}(y, \mathbf{w}), w_1, w_2) & \mathsf{id} = \star \end{cases} \\
\overline{\mathsf{kE}}((y, \mathsf{id}), \alpha) &:= \begin{cases} (\mathsf{kE}(y, \alpha - \delta), \delta) & \mathsf{id} \neq \star \\ (\mathsf{kE}(y, \alpha - \delta), \delta, 0) & \mathsf{id} = \star \end{cases} \\
\overline{\mathsf{sD}}((x, \mathsf{id}), (y, \mathsf{id}'), (\mathbf{c}, c)) &:= \mathsf{sD}(x, y, \mathbf{c}) + c \quad (\mathsf{id} \neq \star, \mathsf{id}' \neq \star) \\
\overline{\mathsf{rD}}((x, \mathsf{id}), (y, \mathsf{id}'), (\mathbf{k}, k)) &:= \mathsf{rD}(x, y, \mathbf{k}) + k \quad (\mathsf{id} \neq \star, \mathsf{id}' \neq \star) \\
\overline{\mathsf{dE}}((y, \mathsf{id}), (y', \mathsf{id}'), (\mathbf{k}, k_1, k_2)) &:= \begin{cases} (\mathbf{k}, k_1 + \mathsf{id}' \cdot k_2) & y' = y, \mathsf{id} = \star, \mathsf{id}' \neq \star \\ (\mathsf{dE}(y, y', \mathbf{k}), (k_1, k_2)) & y' \prec y, \ \mathsf{id} = \star, \ \mathsf{id}' = \star \end{cases}
\end{aligned}$$

where $(\mathbf{w}, w_1, w_2) \leftarrow \mathbb{Z}_p^{\overline{n}}$ and $\alpha, \delta \leftarrow \mathbb{Z}_p$. Note that we only give out $\overline{\mathsf{rD}}$ for the case "$\mathsf{id} \neq \star$, $\mathsf{id}' \neq \star$"; for the case "$\mathsf{id} \neq \star$, $\mathsf{id}' = \star$" where the encoding is in the form $(\mathbf{k}, k_1, k_2)$, we apply $\overline{\mathsf{dE}}$ first.

6 Concrete Schemes

6.1 Concrete mKDM-secure Hierarchical IBE

This section presents a concrete mKDM-CCA secure n-level HIBE scheme derived from our generic construction via predicate encoding in Section 4.

Construction. Assuming $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ is a strongly unforgeable one-time signature scheme against chosen-message attack in the multi-user setting (MU-sUF-CMA security), our mKDM-CCA secure HIBE scheme is as follows:

- $\mathsf{Setup}(1^\lambda, n)$: Run $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda)$, sample $\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{\ell \times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, pick $\mathbf{W}, \mathbf{W}_1, \ldots, \mathbf{W}_{n+1} \leftarrow \mathbb{Z}_p^{\ell \times (k+1)}$ and $\mathbf{k} \leftarrow \{0,1\}^\ell$. Output

$$\mathsf{mpk} := \begin{pmatrix} [\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top \mathbf{W}]_1, [\mathbf{A}_1^\top \mathbf{W}_1]_1, \ldots, [\mathbf{A}_1^\top \mathbf{W}_{n+1}]_1, \\ [\mathbf{B}]_2, \ [\mathbf{W}\mathbf{B}]_2, \ [\mathbf{W}_1\mathbf{B}]_2, \ \ldots, [\mathbf{W}_{n+1}\mathbf{B}]_2, \ [\mathbf{A}_1^\top \mathbf{k}]_T \end{pmatrix}, \quad \mathsf{msk} := [\mathbf{k}]_T.$$

  We assume that group description $\mathbb{G}$ is always contained in mpk.
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, m)$: Parse $\mathsf{id} = (\mathsf{id}_1, \ldots, \mathsf{id}_t)$ where $t \leq n$, run $(\mathsf{sigk}, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda)$, pick $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and compute

$$\overline{\mathsf{ct}} := \big([\mathbf{s}^\top \mathbf{A}_1^\top]_1, [\mathbf{s}^\top (\mathbf{A}_1^\top \mathbf{W} + \textstyle\sum_{i=1}^t \mathsf{id}_i \mathbf{A}_1^\top \mathbf{W}_i + \mathsf{vk} \mathbf{A}_1^\top \mathbf{W}_{n+1})]_1, [\mathbf{s}^\top \mathbf{A}_1^\top \mathbf{k}]_T \cdot m \big).$$

  Output

$$\mathsf{ct}_{\mathsf{id}} := (\mathsf{vk}, \overline{\mathsf{ct}}, \mathsf{Sign}(\mathsf{sigk}, \overline{\mathsf{ct}})).$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$: Recover $\mathbf{k} \in \{0,1\}^\ell$ from $\mathsf{msk} = [\mathbf{k}]_T$. Parse $\mathsf{id} = (\mathsf{id}_1, \ldots, \mathsf{id}_t)$ where $t \leq n$, pick $\mathbf{r} \leftarrow \mathbb{Z}_p^k$ and output

$$\mathsf{sk}_{\mathsf{id}} := \big([\mathbf{B}\mathbf{r}]_2, [\mathbf{k} + (\mathbf{W}\mathbf{B} + \textstyle\sum_{i=1}^t \mathsf{id}_i \mathbf{W}_i \mathbf{B})\mathbf{r}]_2, [\mathbf{W}_{t+1}\mathbf{B}\mathbf{r}]_2, \ldots, [\mathbf{W}_{n+1}\mathbf{B}\mathbf{r}]_2 \big).$$

- $\mathsf{Del}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{id}')$: Parse $\mathsf{sk}_{\mathsf{id}} = (K_0, K_1, K_{t+1}, \ldots, K_{n+1})$ for $\mathsf{id} = (\mathsf{id}_1, \ldots, \mathsf{id}_t)$ and $\mathsf{id}' = (\mathsf{id}, \mathsf{id}_{t+1})$ where $t < n$, pick $\mathbf{r}' \leftarrow \mathbb{Z}_p^k$ and output

$$\mathsf{sk}_{\mathsf{id}'} := \begin{pmatrix} K_0 \cdot [\mathbf{B}\mathbf{r}']_2, \ K_1 \cdot K_{t+1}^{\mathsf{id}_{t+1}} \cdot [(\mathbf{W}\mathbf{B} + \sum_{i=1}^{t+1} \mathsf{id}_i \mathbf{W}_i \mathbf{B})\mathbf{r}']_2, \\ K_{t+2} \cdot [\mathbf{W}_{t+2}\mathbf{B}\mathbf{r}']_2, \ldots, K_{n+1} \cdot [\mathbf{W}_{n+1}\mathbf{B}\mathbf{r}']_2 \end{pmatrix}.$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct}_{\mathsf{id}})$: Parse $\mathsf{ct}_{\mathsf{id}} = (\mathsf{vk}, \overline{\mathsf{ct}}, \sigma)$, output $\perp$ if $\mathsf{Verify}(\mathsf{vk}, \overline{\mathsf{ct}}, \sigma) = 0$. Otherwise, parse $\mathsf{sk}_{\mathsf{id}} = (K_0, K_1, K_{t+1}, \ldots, K_{n+1})$ and $\overline{\mathsf{ct}} = (C_0, C_1, C)$. Output

$$m' = C \cdot e(C_0, K_1 \cdot K_{n+1}^{\mathsf{vk}})^{-1} \cdot e(C_1, K_0).$$

6.2 Concrete mKDM-secure ABE for ABP

This section presents a concrete mKDM-CCA secure ABE for arithmetic branching programs (ABP) derived from our generic construction. We work with arithmetic span programs (ASP) that captures ABP [IW14] and use the predicate encoding from [CGW15].

Arithmetic Span Program [IW14]. An arithmetic span program $(\mathcal{V}, \rho)$ is a collection of row vectors $\mathcal{V} = \{(\mathbf{y}_j, \mathbf{z}_j)\}_{j\in[n']} \in (\mathbb{Z}_p^{\ell'} \times \mathbb{Z}_p^{\ell'})^{n'}$ and $\rho : [n'] \to [n]$. We say that

$$\mathbf{x} \in \mathbb{Z}_p^n \text{ satisfies } (\mathcal{V}, \rho) \quad \text{if} \quad \mathbf{1} \in \mathsf{span}(\mathbf{y}_j + x_{\rho(j)}\mathbf{z}_j),$$

where $\mathbf{1} \coloneqq (1, 0, \ldots, 0)^\top \in \mathbb{Z}_p^{\ell'}$. That is, $\mathbf{x}$ satisfies $(\mathcal{V}, \rho)$ if there exist constants $\omega_1, \ldots, \omega_{n'} \in \mathbb{Z}_p$ such that

$$\textstyle\sum_{j\in[n']} \omega_j(\mathbf{y}_j + x_{\rho(j)}\mathbf{z}_j) = \mathbf{1}.$$

We impose a one-use restriction, that is, ρ is a permutation and $n' = n$. By re-ordering the coordinates in $\mathcal{V}$, we may assume that ρ is the identity map.

Predicate Encodings from [CGW15]. Let $(\mathbf{w}, \mathbf{v}, \mathbf{u}) \leftarrow \mathbb{Z}_p^n \times \mathbb{Z}_p^n \times \mathbb{Z}_p^{\ell'-1}$. Define

$$\begin{aligned}
\mathsf{sE}(\mathbf{x}, (\mathbf{w}, \mathbf{v}, \mathbf{u})) &\coloneqq \left(w_1 + x_1 v_1 \ \ldots \ w_n + x_n v_n\right) \in \mathbb{Z}_p^n \\
\mathsf{rE}(\mathcal{V}, (\mathbf{w}, \mathbf{v}, \mathbf{u})) &\coloneqq \begin{pmatrix} \mathbf{y}_1^\top \left(\begin{smallmatrix} 0 \\ \mathbf{u} \end{smallmatrix}\right) + w_1 & \ldots & \mathbf{y}_n^\top \left(\begin{smallmatrix} 0 \\ \mathbf{u} \end{smallmatrix}\right) + w_n \\ \mathbf{z}_1^\top \left(\begin{smallmatrix} 0 \\ \mathbf{u} \end{smallmatrix}\right) + v_1 & \ldots & \mathbf{z}_n^\top \left(\begin{smallmatrix} 0 \\ \mathbf{u} \end{smallmatrix}\right) + v_n \end{pmatrix} \in \mathbb{Z}_p^{2n} \\
\mathsf{kE}(\mathcal{V}, \alpha) &\coloneqq \begin{pmatrix} \mathbf{y}_1^\top \left(\begin{smallmatrix} \alpha \\ \mathbf{0} \end{smallmatrix}\right) & \cdots & \mathbf{y}_n^\top \left(\begin{smallmatrix} \alpha \\ \mathbf{0} \end{smallmatrix}\right) \\ \mathbf{z}_1^\top \left(\begin{smallmatrix} \alpha \\ \mathbf{0} \end{smallmatrix}\right) & \ldots & \mathbf{z}_n^\top \left(\begin{smallmatrix} \alpha \\ \mathbf{0} \end{smallmatrix}\right) \end{pmatrix} \in \mathbb{Z}_p^{2n} \\
\mathsf{sD}(\mathbf{x}, \mathcal{V}, \mathbf{c}) &\coloneqq \textstyle\sum_{j\in[n]} \omega_j c_j \\
\mathsf{rD}(\mathbf{x}, \mathcal{V}, (\mathbf{d}, \mathbf{d}')) &\coloneqq \textstyle\sum_{j\in[n]} \omega_j (d_j + x_j d'_j)
\end{aligned}$$

Construction. Assuming $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ is a strongly unforgeable one-time signature scheme against chosen-message attack in the multi-user setting (MU-sUF-CMA security), our mKDM-CCA secure ABE scheme for ABP is as follows:

- $\mathsf{Setup}(1^\lambda, n)$: Run $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda)$, sample $\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{\ell\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$, pick $\mathbf{W}, \mathbf{W}_1, \ldots, \mathbf{W}_n, \mathbf{V}, \mathbf{V}_1, \ldots, \mathbf{V}_n \leftarrow \mathbb{Z}_p^{\ell\times(k+1)}$ and $\mathbf{k} \leftarrow \{0,1\}^\ell$. Output

$$\mathsf{mpk} \coloneqq \begin{pmatrix} [\mathbf{A}_1^\top]_1, [\mathbf{A}_1^\top\mathbf{W}]_1, [\mathbf{A}_1^\top\mathbf{W}_1]_1, & \ldots, [\mathbf{A}_1^\top\mathbf{W}_n]_1, \\ \quad [\mathbf{A}_1^\top\mathbf{V}]_1, & [\mathbf{A}_1^\top\mathbf{V}_1]_1, & \ldots, [\mathbf{A}_1^\top\mathbf{V}_n]_1, \\ [\mathbf{B}]_2, & [\mathbf{W}\mathbf{B}]_2, & [\mathbf{W}_1\mathbf{B}]_2, & \ldots, [\mathbf{W}_n\mathbf{B}]_2, \\ \quad [\mathbf{V}\mathbf{B}]_2, & [\mathbf{V}_1\mathbf{B}]_2, & \ldots, [\mathbf{V}_n\mathbf{B}]_2, & [\mathbf{A}_1^\top\mathbf{k}]_T \end{pmatrix}, \quad \mathsf{msk} \coloneqq [\mathbf{k}]_T.$$

  We assume that group description $\mathbb{G}$ is always contained in mpk.
- $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)$: Parse $\mathbf{x} = (x_1, \ldots, x_n)$, run $(\mathsf{sigk}, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda)$, pick $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and compute

$$\overline{\mathsf{ct}} \coloneqq \begin{pmatrix} [\mathbf{s}^\top\mathbf{A}_1^\top]_1, [\mathbf{s}^\top(\mathbf{A}_1^\top\mathbf{W} + \mathsf{vk}\cdot\mathbf{A}_1^\top\mathbf{V})]_1, \\ \{[\mathbf{s}^\top(\mathbf{A}_1^\top\mathbf{W}_j + x_j\cdot\mathbf{A}_1^\top\mathbf{V}_j)]_1\}_{j\in[n]}, [\mathbf{s}^\top\mathbf{A}_1^\top\mathbf{k}]_T \cdot m \end{pmatrix}.$$

  Output

$$\mathsf{ct}_\mathbf{x} \coloneqq (\mathsf{vk}, \overline{\mathsf{ct}}, \mathsf{Sign}(\mathsf{sigk}, \overline{\mathsf{ct}})).$$

– $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathcal{V})$: Recover $\mathbf{k} \in \{0,1\}^\ell$ from $\mathsf{msk} = [\mathbf{k}]_T$. Parse $\mathcal{V} = \{(\mathbf{y}_j, \mathbf{z}_j)\}_{j\in[n]}$, pick $\mathbf{k}' \leftarrow \mathbb{Z}_p^\ell$, $\mathbf{K}' \leftarrow \mathbb{Z}_p^{\ell\times(\ell'-1)}$, $\mathbf{r}, \mathbf{r}_j \leftarrow \mathbb{Z}_p^k$ for all $j \in [n]$ and output

$$\mathsf{sk}_\mathcal{V} := \left([\mathbf{Br}]_2, [\mathbf{k}' + \mathbf{WBr}]_2, \left\{ \begin{matrix} [\mathbf{Br}_j]_2, [((\mathbf{k}-\mathbf{k}')|\mathbf{K}')\mathbf{y}_j + \mathbf{W}_j\mathbf{Br}_j]_2, \\ [((\mathbf{k}-\mathbf{k}')|\mathbf{K}')\mathbf{z}_j + \mathbf{V}_j\mathbf{Br}_j]_2 \end{matrix} \right\}_{j\in[n]} \right).$$

– $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\mathcal{V}, \mathsf{ct}_\mathbf{x})$: Parse $\mathsf{ct}_\mathbf{x} = (\mathsf{vk}, \overline{\mathsf{ct}}, \sigma)$, output $\perp$ if $\mathsf{Verify}(\mathsf{vk}, \overline{\mathsf{ct}}, \sigma) = 0$. Otherwise, parse $\mathsf{sk}_\mathcal{V} = (K_0, K_1, K_2, \{K_{0,j}, K_{1,j}, K_{2,j}\}_{j\in[n]})$ and $\overline{\mathsf{ct}} = (C_0, C_1, \{C_{1,j}\}_{j\in[n]}, C)$. If $\mathbf{x}$ satisfies $\mathcal{V}$, one can compute $\omega_1, \ldots, \omega_n \in \mathbb{Z}_p$ such that $\sum_{j\in[n]} \omega_j(\mathbf{y}_j + x_j \cdot \mathbf{z}_j) = \mathbf{1}$. Output

$$m' = C \cdot \big(e(C_0, K_1 \cdot K_2^{\mathsf{vk}})^{-1} \cdot e(C_1, K_0)\big) \cdot \prod_{j\in[n]} \big(e(C_0, K_{1,j} \cdot {K_{2,j}}^{x_j})^{-1} \cdot e(C_{1,j}, K_{0,j})\big)^{\omega_j}.$$

References

ABBC10. Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash. Cryptographic agility and its relation to circular encryption. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 403–422. Springer, Heidelberg, May / June 2010.

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

AHY15. Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada. A framework for identity-based encryption with almost tight security. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 521–549. Springer, Heidelberg, November / December 2015.

AP12. Jacob Alperin-Sheriff and Chris Peikert. Circular and KDM security for identity-based encryption. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 334–352. Springer, Heidelberg, May 2012.

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

BBG05. Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer, Heidelberg, May 2005.

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

BHHO08. Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision Diffie-Hellman. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 108–125. Springer, Heidelberg, August 2008.

BL16. Johannes Blömer and Gennadij Liske. Construction of fully CCA-secure predicate encryptions from pair encoding schemes. In Kazue Sako, editor, *CT-RSA 2016*, volume 9610 of *LNCS*, pages 431–447. Springer, Heidelberg, February / March 2016.

BRS03. John Black, Phillip Rogaway, and Thomas Shrimpton. Encryption-scheme security in the presence of key-dependent messages. In Kaisa Nyberg and Howard M. Heys, editors, *SAC 2002*, volume 2595 of *LNCS*, pages 62–75. Springer, Heidelberg, August 2003.

CCS09. Jan Camenisch, Nishanth Chandran, and Victor Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 351–368. Springer, Heidelberg, April 2009.

CGH12. David Cash, Matthew Green, and Susan Hohenberger. New definitions and separations for circular security. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 540–557. Springer, Heidelberg, May 2012.

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

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

CGW17. Jie Chen, Junqing Gong, and Jian Weng. Tightly secure IBE under constant-size master public key. In Serge Fehr, editor, *PKC 2017, Part I*, volume 10174 of *LNCS*, pages 207–231. Springer, Heidelberg, March 2017.

CHK04. Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 207–222. Springer, Heidelberg, May 2004.

CL01. Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 93–118. Springer, Heidelberg, May 2001.

CM14. Melissa Chase and Sarah Meiklejohn. Déjà Q: Using dual systems to revisit q-type assumptions. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 622–639. Springer, Heidelberg, May 2014.

CMM16. Melissa Chase, Mary Maller, and Sarah Meiklejohn. Déjà Q all over again: Tighter and broader reductions of q-type assumptions. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 655–681. Springer, Heidelberg, December 2016.

CMP17. Sanjit Chatterjee, Sayantan Mukherjee, and Tapas Pandit. Cca-secure predicate encryption from pair encoding in prime order groups: Generic

and efficient. In Arpita Patra and Nigel P. Smart, editors, *Progress in Cryptology - INDOCRYPT 2017 - 18th International Conference on Cryptology in India, Chennai, India, December 10-13, 2017, Proceedings*, volume 10698 of *Lecture Notes in Computer Science*, pages 85–106. Springer, 2017.

DGHM18. Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, and Daniel Masny. New constructions of identity-based and key-dependent message secure encryption schemes. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part I*, volume 10769 of *LNCS*, pages 3–31. Springer, Heidelberg, March 2018.

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

GDCC16. Junqing Gong, Xiaolei Dong, Jie Chen, and Zhenfu Cao. Efficient IBE with tight reduction to standard assumption in the multi-challenge setting. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 624–654. Springer, Heidelberg, December 2016.

GGH20. Sanjam Garg, Romain Gay, and Mohammad Hajiabadi. Master-key KDM-secure IBE from pairings. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 123–152. Springer, Heidelberg, May 2020.

GHV12. David Galindo, Javier Herranz, and Jorge L. Villar. Identity-based encryption with master key-dependent message security and leakage-resilience. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *ESORICS 2012*, volume 7459 of *LNCS*, pages 627–642. Springer, Heidelberg, September 2012.

GPSW06. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 2006*, pages 89–98. ACM Press, October / November 2006. Available as Cryptology ePrint Archive Report 2006/309.

HK07. Shai Halevi and Hugo Krawczyk. Security under key-dependent inputs. In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *ACM CCS 2007*, pages 466–475. ACM Press, October 2007.

HLL16. Shuai Han, Shengli Liu, and Lin Lyu. Efficient KDM-CCA secure public-key encryption for polynomial functions. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 307–338. Springer, Heidelberg, December 2016.

Hof13. Dennis Hofheinz. Circular chosen-ciphertext security with compact ciphertexts. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 520–536. Springer, Heidelberg, May 2013.

IW14. Yuval Ishai and Hoeteck Wee. Partial garbling schemes and their applications. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *ICALP 2014, Part I*, volume 8572 of *LNCS*, pages 650–662. Springer, Heidelberg, July 2014.

KL15. Lucas Kowalczyk and Allison Bishop Lewko. Bilinear entropy expansion from the decisional linear assumption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 524–541. Springer, Heidelberg, August 2015.

KM19. Fuyuki Kitagawa and Takahiro Matsuda. CPA-to-CCA transformation for KDM security. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part II*, volume 11892 of *LNCS*, pages 118–148. Springer, Heidelberg, December 2019.

KMT19. Fuyuki Kitagawa, Takahiro Matsuda, and Keisuke Tanaka. CCA security and trapdoor functions via key-dependent-message security. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 33–64. Springer, Heidelberg, August 2019.

KT18. Fuyuki Kitagawa and Keisuke Tanaka. A framework for achieving KDM-CCA secure public-key encryption. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 127–157. Springer, Heidelberg, December 2018.

LLJ15. Xianhui Lu, Bao Li, and Dingding Jia. KDM-CCA security from RKA secure authenticated encryption. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 559–583. Springer, Heidelberg, April 2015.

LP20. Roman Langrehr and Jiaxin Pan. Hierarchical identity-based encryption with tight multi-challenge security. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 153–183. Springer, Heidelberg, May 2020.

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

OT12. Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure unbounded inner-product and attribute-based encryption. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 349–366. Springer, Heidelberg, December 2012.

Sha84. Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer, Heidelberg, August 1984.

SW05. Amit Sahai and Brent R. Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Heidelberg, May 2005.

SW08. Elaine Shi and Brent Waters. Delegating capabilities in predicate encryption systems. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 560–578. Springer, Heidelberg, July 2008.

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

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

YAHK11. Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, and Noboru Kunihiro. Generic constructions for chosen-ciphertext secure attribute based encryption. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 71–89. Springer, Heidelberg, March 2011.