Leakage-Resilient Attribute-Based Encryption with Attribute-Hiding

Yijian Zhang[1], Yunhao Ling[1], Jie Chen[1,2(✉)], and Luping Wang[3,4]

[1] Software Engineering Institute, East China Normal University, Shanghai, China
[2] Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China s080001@e.ntu.edu.sg
[3] School of Electronic and Information Engineering, Suzhou University of Science and Technology, Jiangsu, China
[4] Jiangsu Key Laboratory for Elevator Intelligent Safety, Jiangsu, China

Abstract. In this work, we present two generic frameworks for leakage-resilient attribute-based encryption (ABE), which is an improved version of ABE that can be proven secure even when part of the secret key is leaked. Our frameworks rely on the standard assumption (k-Lin) over prime-order groups. The first framework is designed for leakage-resilient ABE with attribute-hiding in the bounded leakage model. Prior to this work, no one had yet derived a generic leakage-resilient ABE framework with attribute-hiding. The second framework provides a generic method to construct leakage-resilient ABE in the continual leakage model. It is compatible with Zhang et al.'s work [DCC 2018] but more generic. Concretely, Zhang et al.'s framework cannot act on some specific ABE schemes while ours manages to do that. Technically, our frameworks are built on the predicate encoding of Chen et al.'s [EUROCRYPT 2015] combined with a method of adding redundancy. At last, several instantiations are derived from our frameworks, which cover the cases of zero inner-product predicate and non-zero inner-product predicate.

Keywords: Leakage-resilient · Attribute-based encryption · Attribute-hiding · Predicate encoding.

1 Introduction

Attribute-based encryption (ABE) [SW05] is a primitive that can provide the confidentiality of data and fine-grained access control simultaneously. In ABE, a ciphertext $\mathsf{ct}_{\mathbf{x}}$ for a message m is associated with an attribute $\mathbf{x} \in \mathcal{X}$, and a secret key $\mathsf{sk}_{\mathbf{y}}$ is associated with a policy $\mathbf{y} \in \mathcal{Y}$. Given a predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, $\mathsf{ct}_{\mathbf{x}}$ can be decrypted by $\mathsf{sk}_{\mathbf{y}}$ if and only if $\mathsf{P}(\mathbf{x},\mathbf{y}) = 1$.

The basic security requirement for ABE is *payload-hiding*. Roughly speaking, an adversary holding the secret key such that $\mathsf{P}(\mathbf{x},\mathbf{y}) = 0$ cannot deduce any information about m from the given ciphertext, and besides, this should be guaranteed even the adversary has more than one such secret key. In some scenarios, the attribute $\mathbf{x}$ may contain user privacy. For example, in the cloud storage [KHPP16], the attribute $\mathbf{x}$ contains identity or address, which may be unsuitable to be exposed. *Attribute-hiding* [LOS+10] is an additional security requirement, and it concerns the privacy of attribute $\mathbf{x}$. Informally, attribute-hiding says that no information about attribute $\mathbf{x}$ can be disclosed to the adversary.

Recently, due to the emergence of side-channel attacks [AARR02,HSH+09,KHF+19] which, through various physical methods, can recover part of the secret key, the leakage-resilient cryptography [DP08] is hence proposed. It is required that a leakage-resilient scheme should be provably secure in the *leakage-resilient model*. In this paper, we are interested in two prominent leakage-resilient models, namely, *bounded leakage model* (BLM) [AGV09] and *continual leakage model* (CLM) [BKKV10]. Both of them assume that an adversary obtains leaked information about the secret key sk via a polynomial-time computable leakage function $f : \{0,1\}^{|\mathsf{sk}|} \to \{0,1\}^L$ where $|\mathsf{sk}|$ is the bit length of sk. In the BLM (resp. CLM), the adversary has access to at most $L < |\mathsf{sk}|$ bits leakage on the secret key over the whole lifetime (resp. any time period) of the system. It is necessary to *update* sk periodically in the CLM. Typically, the security of CLM is stronger than BLM [KR19].

Up to now, various leakage-resilient frameworks have been proposed, while very few of them concentrate on leakage-resilient ABE. There are several generic leakage-resilient frameworks that can convert plain ABE schemes to leakage-resilient ones in the BLM/CLM. The first one is introduced by Yu et al. [YAX+16]. Their generic leakage-resilient framework is able to convert the ABE schemes based on pair encoding [Att14] to leakage-resilient ones. However, their generic leakage-resilient framework cannot provide attribute-hiding feature. Besides, for several concrete constructions, their security must rely on the non-standard computational assumptions, namely, q-type assumptions. Afterward, Zhang et al. [ZZM17] proposed a generic leakage-resilient ABE framework from hash proof system, while it also ignores attribute-hiding feature. Another independent work was proposed by Zhang et al. [ZCG+18]. Their generic leakage-resilient framework is able to convert most ABE schemes based on predicate encoding [Wee14] to leakage-resilient ones. However, their generic leakage-resilient framework cannot guarantee attribute-hiding as well, and besides, cannot act on several specific ABE schemes based on predicate encoding, for example the compact-key ABE for inner-product predicate in [CGW15], to leakage-resilient ones.

In this paper, we will follow the works of Chen et al. [CGW15] and Zhang et al. [ZCG+18], aimed at presenting two generic leakage-resilient frameworks. The first one can provide the attribute-hiding feature. The second one can convert more ABE schemes to leakage-resilient ones.

1.1 Contributions

In this work, we present two generic frameworks for the design of leakage-resilient ABE. Our contributions can be summarized as follows:

- **Leakage-resilient ABE with attribute-hiding in the BLM.**
  We introduce a new encoding called *attribute-hiding-leakage-resilient*. Based on the attribute-hiding techniques of CGW15 and this new encoding, we present a generic leakage-resilient ABE construction with attribute-hiding, which is provably secure under the k-Lin assumption in the BLM.
- **Leakage-resilient ABE in the CLM**.
  We introduce different redundancy into the secret key and the master key to ensure the security against continual leakage and add a linear map to ensure the generation and update of secret keys. Thus, we present a more generic leakage-resilient ABE in the CLM compared with ZCG+18.

A comparison between our frameworks and previous works is shown in Table 1. Note that, although our second framework in Section 4 has the same properties as ZCG+18, it can act on some specific schemes while ZCG+18 cannot do that.

Table 1: Comparison between previous works and ours. “Prime" denotes prime-order groups. “SD" means subgroup assumptions over composite-order groups.

Reference	Leakage model	Attribute-hiding	Prime	Generality	Assumption
[YAX+16]	CLM	✗	✗	$\perp$	SD, q-type
[ZZM17]	BLM	✗	✗	$\perp$	SD
[ZCG+18]	CLM	✗	✓	weak	k-Lin
Section 3	BLM	✓	✓	$\perp$	k-Lin
Section 4	CLM	✗	✓	strong	k-Lin

1.2 Technical Overview

Let $(p, G_1, G_2, G_T, g_1, g_2, e)$ denote an asymmetric bilinear group of prime-order p with pairing $e : G_1 \times G_2 \to G_T$. We use $\mathsf{mpk}, \mathsf{mk}$ to denote the master public key and the master key in ABE, respectively. Let $L \in \mathbb{N}$ be a leakage parameter.

Leakage-resilient ABE with attribute-hiding in the BLM. Based on the ABE with attribute-hiding in CGW15, we propose a generic leakage-resilient ABE construction that possesses attribute-hiding feature even when the secret key can be leaked to the adversary. An overview of our construction is presented as follows [5]:

$$\begin{aligned} &\mathsf{mpk} : g_1, g_2, g_1^{\mathbf{w}}, e(g_1,g_2)^{\alpha}, \qquad \mathsf{mk} : \alpha, \mathbf{w} \\ &\mathsf{sk}_{\mathbf{y}} : \mathbf{z},\ g_2^{r},\ g_2^{\mathsf{rk}\mathsf{E}(\mathbf{y},\mathbf{z},\alpha)+r\cdot \mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w})}, \quad \mathsf{ct}_{\mathbf{x}} : g_1^{s}, g_1^{s\cdot \mathsf{sE}(\mathbf{x},\mathbf{w})}, m\cdot e(g_1,g_2)^{\alpha s} \end{aligned} \tag{1}$$

where $\mathbf{w} \in \mathcal{W}$ is a set of secret values; $\alpha, r, s \leftarrow \mathbb{Z}_p$; $\mathbf{x} \in \mathcal{X}, \mathbf{y} \in \mathcal{Y}$; $\mathsf{rkE}, \mathsf{rE}, \mathsf{sE}$ are linear encoding algorithms; $\mathbf{z} \in \mathcal{Z}$ and $\mathbf{u}$ are "redundant" information. To achieve attribute-hiding security in the BLM, we require that

- **(attribute-hiding.)** For all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 0$ and all $\mathbf{z} \in \mathcal{Z}$, the distributions $\{\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{sE}(\mathbf{x}, \mathbf{w}), \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{w})\}$ and $\{\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{r}\}$ are statistically indistinguishable where the randomness is taken over $\mathbf{w} \leftarrow \mathcal{W}$ and $\mathbf{r} \leftarrow \mathbb{Z}_p^{|\mathsf{sE}(\cdot)|+|\mathsf{rE}(\cdot)|}$.

The above requirement, namely *attribute-hiding* encoding, ensures the attribute-hiding feature. It manages to randomize $\mathbf{x}$ in $\mathsf{sE}(\mathbf{x}, \mathbf{w})$ even after the adversary has got $\mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{w})$ on $\mathsf{sk}_{\mathbf{y}}$. However, this property only holds when $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 0$ and would be broken by the adversary with leak ability, since he can use the leakage function f to acquire the leakage (i.e., $f(\mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{w}))$) on $\mathsf{sk}_{\mathbf{y}}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 1$. The "redundant" information in $\mathsf{sk}_{\mathbf{y}}$ is designed to avoid this problem. Inspired by [ZCG+18] and [LRW11], we additionally require that

- **(attribute-hiding-leakage-resilient.)** For all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 1$ and $\mathbf{z} \in \mathcal{Z}$, the distributions $\{\mathbf{x}, \mathbf{y}, \mathsf{sE}(\mathbf{x}, \mathbf{w}), f(\mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{w}))\}$ and $\{\mathbf{x}, \mathbf{y}, \mathbf{r}\}$ are identical, where $\mathbf{w} \leftarrow \mathcal{W}$ and $\mathbf{r} \leftarrow \mathbb{Z}_p^{|\mathsf{sE}(\cdot)|+|f(\cdot)|}$.

This encoding guarantees that with the leakage of $\mathsf{sk}_{\mathbf{y}}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 1$, the adversary still cannot reveal the attribute $\mathbf{x}$ under $\mathsf{sE}(\mathbf{x}, \mathbf{w})$ since it seems to be sampled uniformly. Thus, the Equation (1) achieves attribute-hiding in the BLM.

Leakage-resilient ABE in the CLM. For the second leakage-resilient ABE framework, we consider the CLM which is stronger than BLM. Although ZCG+18 has proposed a leakage-resilient ABE framework in the CLM, it is not general enough to act on some specific schemes, e.g., compact-key ABE schemes for zero inner-product and non-zero inner-product in CGW15. For these specific schemes, their master keys contain multiple secret values (e.g., α and $\mathbf{w}$), and the adversary can break the security trivially if one of these secret values is leaked. Our solution is to differentiate the redundant information of mk and the redundant information of $\mathsf{sk}_{\mathbf{y}}$, which provides more possibilities to avoid the leakage on secret values. Thus, we present a new leakage-resilient ABE generic construction:

$$\begin{aligned} &\mathsf{mpk} : g_1, g_2, g_1^{\mathbf{w}}, g_2^{\mathbf{w}}, e(g_1,g_2)^{\alpha}, \quad \mathsf{mk} : \mathbf{v}, g_2^{r}, g_2^{\mathsf{mk}\mathsf{E}(\mathbf{v},\alpha)+r\cdot \mathsf{mE}(\mathbf{v},\mathbf{w})}, \\ &\mathsf{sk}_{\mathbf{y}} : \mathbf{z}, g_2^{r}, g_2^{\mathsf{rk}\mathsf{E}(\mathbf{y},\mathbf{z},\alpha)+r\cdot \mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w})}, \quad \mathsf{ct}_{\mathbf{x}} : g_1^{s}, g_1^{s\cdot \mathsf{sE}(\mathbf{x},\mathbf{w})}, m\cdot e(g_1,g_2)^{\alpha s} \end{aligned} \tag{2}$$

where $\mathsf{mkE}, \mathsf{mE}$ are encoding algorithms; $\mathbf{v} \in \mathcal{V}$ and $\mathbf{z} \in \mathcal{Z}$ serve as redundant information for mk and $\mathsf{sk}_{\mathbf{y}}$, respectively. Note that this construction is similar to the Equation (1), while it considers CLM (rather than BLM) and allows the leakage on $\mathsf{sk}_{\mathbf{y}}$ and mk. Here, we require that

[5] Strictly speaking, the Equation (1) is built on composite-order groups. A general approach to transforming schemes over composite-order groups into ones over prime-order groups has been proposed in [CGW15]. Thus, in this section, we decide to abuse constructions over composite-order groups as ones over prime-order groups for simplicity.

1) **(α-privacy.)** For all $(\mathbf{x},\mathbf{y}) \in \mathcal{X}\times\mathcal{Y}$ such that $\mathsf{P}(\mathbf{x},\mathbf{y}) = 0$, the distributions $\{\mathbf{x},\mathbf{y},\mathbf{z},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}),\mathsf{rkE}(\mathbf{y},\mathbf{z},\alpha) + \mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w})\}$ and $\{\mathbf{x},\mathbf{y},\mathbf{z},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}),\mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w})\}$ are identical where the randomness is taken over $\mathbf{w}\leftarrow\mathcal{W}$.
2) **(α-leakage-resilient.)** For all $(\mathbf{x},\mathbf{y}) \in \mathcal{X}\times\mathcal{Y}$ such that $\mathsf{P}(\mathbf{x},\mathbf{y}) = 1$ and all $\alpha\in\mathbb{Z}_p, \mathbf{z}\in\mathcal{Z}$, the distributions $\{\mathbf{x},\mathbf{y},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}), f(\mathbf{z},\mathsf{rkE}(\mathbf{y},\mathbf{z},\alpha)+\mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w}))\}$ and $\{\mathbf{x},\mathbf{y},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}), f(\mathbf{z},\mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w}))\}$ are identical where $\mathbf{w}\leftarrow\mathcal{W}$ and f is a leakage function.
   In addition, the distributions $\{\mathbf{x},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}), f(\mathbf{z},\mathsf{mkE}(\mathbf{v},\alpha)+\mathsf{mE}(\mathbf{v},\mathbf{w}))\}$ and $\{\mathbf{x},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}), f(\mathbf{v},\mathsf{mE}(\mathbf{v},\mathbf{w}))\}$ are identical.
3) (**re-randomizable**.) There exists a update algorithm for $\mathsf{sk}_\mathbf{y}$ and mk.
4) (**delegable**.) There exists an algorithm that takes as input mk and $\mathbf{y}$ and outputs a fresh secret key $\mathsf{sk}_\mathbf{y}$.

α-privacy and *α-leakage-resilient* are aimed at resisting continual leakage on $\mathsf{sk}_\mathbf{y}$ and mk. Since the total leakage bound of the adversary is unlimited in the CLM, *re-randomizable* and *delegable* are proposed to ensure the periodical update for $\mathsf{sk}_\mathbf{y}$ and mk. As a specific case, we let $\mathbf{w} := (w_1,\ldots,w_n,\mathbf{u})\in\mathbb{Z}_p^{n+L}, \mathbf{v} := (\mathbf{v}_0,\mathbf{v}_1,\ldots,\mathbf{v}_n)\in(\mathbb{Z}_p^L)^n$,

$$\mathsf{mkE}(\mathbf{v},\alpha)\stackrel{\text{def}}{=}(\alpha,0,\ldots,0),\ \mathsf{mE}(\mathbf{v},\mathbf{w})\stackrel{\text{def}}{=}(\mathbf{v}_0^\top\mathbf{u}, w_1+\mathbf{v}_1^\top\mathbf{u},\ldots,w_n+\mathbf{v}_n^\top\mathbf{u},\mathbf{u})$$

In the above equality, it is best for the adversary to get the leakage on $(\alpha+\mathbf{v}_0^\top\mathbf{u}_0,\mathbf{v}_0,\mathbf{u})$ or $(w_i+\mathbf{v}_i^\top\mathbf{u}_i,\mathbf{v}_i,\mathbf{u})$ if the adversary tries to leak α or w_i. Note that for any $i\neq j$, $\mathbf{v}_i^\top\mathbf{u}$ is statistically independent from $\mathbf{v}_j^\top\mathbf{u}$ due to the randomness of $\mathbf{v}$. Then based on the subspace lemma in LRW11, α or w_i is hidden as long as the adversary gets a limited amount of leakage on mk during a time period. Thus, the randomness of $\mathbf{w}$ is preserved, then *α-privacy* and *α-leakage-resilient* are satisfied. Besides, *re-randomizable* holds since we have published $g_2^\mathbf{w}$ in mpk. As for *delegable*, we additionally require a linear map $S:\mathcal{Y}\times\mathcal{V}\to\mathcal{Z}$, which enables the redundant information $\mathbf{z}$ in $\mathsf{sk}_\mathbf{y}$ to be computed from $\mathbf{v}$ and $\mathbf{y}$. Thus, $\mathsf{sk}_\mathbf{y}$ can be generated from mk and $\mathbf{y}$ correctly. At last, we apply our second framework (in Section 4) to compact-key ABE schemes for zero inner-product and non-zero inner-product in CGW15, and hence obtain several leakage-resilient instantiations in Section 5.

1.3 Related Work

Other leakage-resilient models. Dziembowski et al. [CLW06] defined the *bounded retrieval model* (BRM), placing rigorous performance requirements on the leakage-resilient scheme. Dodis et al. [DKL09] proposed the *auxiliary input leakage model* (ALM). It only requires that the leakage function f is hard to invert. Besides, Yuen at al. [YCZY12] defined the *continual auxiliary leakage model* (CAL) that captures the benefits of both CLM and ALM.

Leakage-resilient ABE. Lewko et al. [LRW11] proposed the first identity-based encryption (IBE) and ABE which are proved in the CLM. Zhang and Mu [ZM16] constructed a leakage-resilient anonymous inner-product encryption (IPE) scheme over composite-order groups in the BLM. Nishimaki and Yamakawa [NY19] proposed several constructions of leakage-resilient public-key encryption and leakage-resilient IBE in the BRM, which reach nearly optimal leakage rates under standard assumptions in the standard model. To deal with potential side-channel attacks in the distributed environment, Li et al. [LYZS19,LYZ19] designed a key-policy ABE in the CAL and a hierarchical ABE in the CLM.

Organization. We recall the related definition and security models in §2. The first leakage-resilient ABE framework is presented in §3. The Second leakage-resilient ABE framework is shown in §4. We present some instantiations in §5.

2 Preliminaries

Notations. For $n \in \mathbb{N}$, $[n]$ denote the set $\{1, 2, \ldots, n\}$. We use $s \leftarrow \mathcal{S}$ to denote that s is picked randomly from set $\mathcal{S}$. By PPT, we denote a probabilistic polynomial-time algorithm. We use $\overset{c}{\approx}$ and $\overset{s}{\approx}$ to denote two distributions being computationally and statistically indistinguishable, respectively.

2.1 The Definition of ABE

Given attribute universe $\mathcal{X}$, predicate universe $\mathcal{Y}$ and predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$, an ABE scheme consists of four algorithms (Setup, KeyGen, Enc, Dec):

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{mk})$. Take as input a security parameter λ. Then return the public parameters mpk and the master key mk.
- $\mathsf{KeyGen}(\mathsf{mk}, \mathbf{y}) \to \mathsf{sk}_\mathbf{y}$. Take as input mk, $\mathbf{y} \in \mathcal{Y}$, and return a secret key $\mathsf{sk}_\mathbf{y}$.
- $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m) \to \mathsf{ct}_\mathbf{x}$. Take as input mpk, an attribute $\mathbf{x} \in \mathcal{X}$, and a message m. Return a ciphertext $\mathsf{ct}_\mathbf{x}$.
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\mathbf{y}, \mathsf{ct}_\mathbf{x}) \to m$ or $\perp$. Take as input $\mathsf{sk}_\mathbf{y}$ and $\mathsf{ct}_\mathbf{x}$. If $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 1$, return message m; otherwise, return $\perp$.

Correctness. For all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 1$ and all $m \in \mathcal{M}$, it holds that $\Pr\left[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\mathbf{y}, \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)) = m\right] = 1$ where $(\mathsf{mpk}, \mathsf{mk}) \leftarrow \mathsf{Setup}(1^\lambda, 1^n)$, $\mathsf{sk}_\mathbf{y} \leftarrow \mathsf{KeyGen}(\mathsf{mk}, \mathbf{y})$.
Additional algorithm. If we take the presence of continual leakage into account, an extra algorithm should be provided:

- $\mathsf{Update}(\mathsf{mpk}, \mathsf{sk}_\mathbf{y})$: Take as input a secret key $\mathsf{sk}_\mathbf{y}$, and outputs a re-randomized key $\mathsf{sk}'_\mathbf{y}$.

It is equivalent to generating a fresh secret key $\mathsf{sk}'_\mathbf{y} \leftarrow \mathsf{KeyGen}(\mathsf{mk}, \mathbf{y})$. We stress that mk can be seen as a secret key $\mathsf{sk}_\mathbf{y}$ (where $\mathbf{y}$ is an empty string ϵ) and algorithm Update also acts on mk.

2.2 Security Models

Here, we would define two leakage-resilient models, both of which are parameterized by security parameter λ and leakage bounds $L_{\mathsf{mk}} = L_{\mathsf{mk}}(\lambda), L_{\mathsf{sk}} = L_{\mathsf{sk}}(\lambda)$.

Definition 1. *We say that an ABE scheme is $(L_{\mathsf{mk}}, L_{\mathsf{sk}})$-bounded-leakage secure and attribute-hiding if for all* PPT *adversaries $\mathcal{A}$, the advantage function*

$$\mathsf{Adv}^{\text{BLR-AH}}_{\mathcal{A}}(\lambda) := \left| \Pr\left[b' = b \;\middle|\; \begin{array}{l} (\mathsf{mpk}, \mathsf{mk}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathbf{x}^{(0)}, \mathbf{x}^{(1)}, m^{(0)}, m^{(1)}) \leftarrow \mathcal{A}^{\mathsf{O}_1, \mathsf{O}_2, \mathsf{O}_3}(\mathsf{mpk}) \\ b \leftarrow \{0, 1\}; \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}^{(b)}, m^{(b)}) \\ b' \leftarrow \mathcal{A}^{\mathsf{O}_1, \mathsf{O}_2, \mathsf{O}_3}(\mathsf{mpk}, \mathsf{ct}^*) \end{array} \right] - \frac{1}{2} \right|.$$

is negligible.

In the above definition, $\mathcal{A}$ has access to oracles $\mathsf{O}_1, \mathsf{O}_2, \mathsf{O}_3$. These oracles maintain sets $\mathcal{H}$ and $\mathcal{R}$ which store some tuples.

– $\mathsf{O}_1(h, \mathbf{y})$: h is a handle to a tuple of $\mathcal{H}$ that must refer to a master key and $\mathbf{y}$ must be a vector in $\mathcal{Y}$. After receiving the input, this oracle finds the tuple t with handle h in $\mathcal{H}$ and answers $\mathcal{A}$ as follows:
  1) If the vector part of t is ϵ, then let $t := (h, \epsilon, \mathsf{mk}, l)$. It runs KeyGen algorithm to obtain a key $\mathsf{sk}_\mathbf{y}$ and adds the tuple $(H + 1, \mathbf{y}, \mathsf{sk}_\mathbf{y}, 0)$ to $\mathcal{H}$. Then it updates $H \leftarrow H + 1$;
  2) Otherwise, it returns $\perp$ to $\mathcal{A}$.

– $\mathsf{O}_2(h, f)$: f is a polynomial-time computable function of constant output size. After receiving the input, it finds the tuple t with handle h in $\mathcal{H}$ and answers $\mathcal{A}$ as follows:
  1) If t is of the form $(h, \epsilon, \mathsf{mk}, l)$, it checks whether $l + |f(\mathsf{mk})| \leq L_{\mathsf{mk}}$. If $l + |f(\mathsf{mk})| \leq L_{\mathsf{mk}}$ holds, the challenger returns $f(\mathsf{mk})$ to $\mathcal{A}$ and updates $l \leftarrow l + |f(\mathsf{mk})|$. Otherwise, it returns $\perp$ to $\mathcal{A}$;
  2) Else, t is of the form $(h, \mathbf{y}, \mathsf{sk}_{\mathbf{y}}, l)$ and then it checks whether $l + |f(\mathsf{sk}_{\mathbf{y}})| \leq L_{\mathsf{sk}}$. If $l + |f(\mathsf{sk}_{\mathbf{y}})| \leq L_{\mathsf{sk}}$ holds, the challenger returns $f(\mathsf{sk}_{\mathbf{y}})$ to $\mathcal{A}$ and updates $l \leftarrow l + |f(\mathsf{sk}_{\mathbf{y}})|$. Otherwise, it returns $\perp$.
– $\mathsf{O}_3(h)$: It finds the tuple with handle h in $\mathcal{H}$. If the vector part of the tuple is ϵ, then it returns $\perp$ to $\mathcal{A}$. Otherwise, the tuple is of the form $(h, \mathbf{y}, \mathsf{sk}_{\mathbf{y}}, l)$. It returns $\mathsf{sk}_{\mathbf{y}}$ and then add $\mathbf{y}$ to $\mathcal{R}$.

Note that after $\mathcal{A}$ receives the challenge ciphertext ct^*, only queries on $\mathsf{sk}_{\mathbf{y}}$ such that $\mathsf{P}(\mathbf{x}^{(0)}, \mathbf{y}) = 0$ and $\mathsf{P}(\mathbf{x}^{(1)}, \mathbf{y}) = 0$ are allowed when $\mathcal{A}$ access to $\mathsf{O}_2, \mathsf{O}_3$.

Definition 2. *We say that an* ABE *scheme is* $(L_{\mathsf{mk}}, L_{\mathsf{sk}})$*-continual-leakage secure if for all* PPT *adversaries* $\mathcal{A}$*, the advantage function*

$$\mathsf{Adv}^{\text{CLR-PH}}_{\mathcal{A}}(\lambda) := \left| \Pr\left[b' = b \;\middle|\; \begin{array}{l} (\mathsf{mpk}, \mathsf{mk}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathbf{x}, m^{(0)}, m^{(1)}) \leftarrow \mathcal{A}^{\mathsf{O}'_1, \mathsf{O}'_2, \mathsf{O}'_3}(\mathsf{mpk}) \\ b \leftarrow \{0,1\}; \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m^{(b)}) \\ b' \leftarrow \mathcal{A}^{\mathsf{O}'_1, \mathsf{O}'_2, \mathsf{O}'_3}(\mathsf{mpk}, \mathsf{ct}^*) \end{array} \right] - \frac{1}{2} \right|.$$

is negligible.

Here, $\mathcal{A}$ has access to oracles $\mathsf{O}'_1, \mathsf{O}'_2, \mathsf{O}'_3$. These oracles maintain sets $\mathcal{H}'$ and $\mathcal{R}'$.

– $\mathsf{O}'_1(h, \mathbf{y})$: This oracle is similar to O_1 except that the input $\mathbf{y}$ can also be an empty string ϵ. If $\mathcal{A}$ makes a query for $\mathbf{y} = \epsilon$, it will run Update algorithm to get a fresh master key mk' and add the tuple $(H+1, \epsilon, \mathsf{mk}', 0)$ to the set $\mathcal{H}$.
– $\mathsf{O}'_2(h, f)$: This oracle is the same as O_2.
– $\mathsf{O}'_3(h)$: This oracle is the same as O_3.

Note that after $\mathcal{A}$ receives the challenge ciphertext ct^*, only queries on $\mathsf{sk}_{\mathbf{y}}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 0$ are allowed when $\mathcal{A}$ access to $\mathsf{O}'_2, \mathsf{O}'_3$.

2.3 Assumption

Let $\mathcal{G}$ be a probabilistic polynomial-time algorithm that takes as input a security parameter 1^λ and outputs a group description $\mathbb{G} := (p, G_1, G_2, G_T, g_1, g_2, e)$, where p is a $\Theta(\lambda)$-bit prime and G_1, G_2, G_T are cyclic groups of order p. g_1 and g_2 are generators of G_1 and G_2 respectively and $e : G_1 \times G_2 \to G_T$ is a computationally efficient and non-degenerate bilinear map. We let $g_T = e(g_1, g_2)$ be the generator of G_T.

For $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_p$, we define $[a]_s = g_s^a$ as the implicit representation of a in G_s. Similarly, for a matrix $\mathbf{A}$ over $\mathbb{Z}_p$, we define $[\mathbf{A}]_s = g_s^{\mathbf{A}}$, where exponentiations are carried out component-wise. Given $[\mathbf{A}]_1$ and $[\mathbf{B}]_2$, we define $e([\mathbf{A}]_1, [\mathbf{B}]_2) := [\mathbf{A}^\top \mathbf{B}]_T$. Now we review the definition of k-Lin assumption.

Definition 3 (k-Lin Assumption). *Let* $s \in \{1, 2, T\}$*. We say that the k-Lin assumption holds with respect to* $\mathcal{G}$ *on* G_s *if for all* PPT *adversaries* $\mathcal{A}$*, the following advantage function is negligible in* λ*.*

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

where $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda), \mathbf{t} \leftarrow \mathbb{Z}_p^k, \mathbf{u} \leftarrow \mathbb{Z}_p^{k+1}, (a_1, \ldots, a_k) \leftarrow \mathbb{Z}_p^k$, *then*

$$\mathbf{A} := \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_k \\ 1 & \cdots & 1 \end{pmatrix} \in \mathbb{Z}_p^{(k+1)\times k} \tag{3}$$

Note that we can trivially set $(\mathbf{a}^\perp)^\top := (a_1^{-1}, \ldots, a_k^{-1}, -1)$ such that $\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{0}$.

3 Leakage-resilient ABE with Attribute-hiding in the BLM

In this section, we will present the first leakage-resilient ABE framework along with the predicate encoding, generic construction and corresponding security analysis.

3.1 Leakage-resilient Predicate Encoding

A $\mathbb{Z}_p$-linear leakage-resilient predicate encoding with attribute-hiding for predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, which contains a set of deterministic algorithms $(\mathsf{rkE}, \mathsf{rE}, \mathsf{sE}, \mathsf{sD}, \mathsf{rD})$, satisfies the following properties:

- **(linearity.)** For all $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, $\mathsf{rkE}(\mathbf{y}, \mathbf{z}, \cdot)$, $\mathsf{rE}(\mathbf{y}, \mathbf{z}, \cdot)$, $\mathsf{sE}(\mathbf{x}, \cdot)$, $\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \cdot)$, $\mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \cdot)$ are $\mathbb{Z}_p$-linear functions. A $\mathbb{Z}_p$-linear function F can be encoded as a matrix $\mathbf{T} = (t_{i,j}) \in \mathbb{Z}_p^{n\times m}$ such that $F : (w_1, \ldots, w_n) \longmapsto (\sum_{i=1}^n t_{i,1} w_i, \ldots, \sum_{i=1}^n t_{i,m} w_i)$.
- **(restricted α-reconstruction.)** For all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 1$, all $\mathbf{w} \in \mathcal{W}, \mathbf{z} \in \mathcal{Z}$, it holds that $\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{sE}(\mathbf{x}, \mathbf{w})) = \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{w}))$ and $\mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, \alpha)) = \alpha$.
- **(x-oblivious α-reconstruction.)** $\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \cdot), \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \cdot)$ are independent of $\mathbf{x}$. It is a basic requirement for achieving attribute-hiding.
- **(attribute-hiding.)** For all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 0$ and all $\mathbf{z} \in \mathcal{Z}$, the distributions $\{\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{sE}(\mathbf{x}, \mathbf{w}), \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{w})\}$ and $\{\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{r}\}$ are identical, where $\mathbf{w} \leftarrow \mathcal{W}$ and $\mathbf{r} \leftarrow \mathbb{Z}_p^{|\mathsf{sE}(\cdot)|+|\mathsf{rE}(\cdot)|}$.
- **(attribute-hiding-leakage-resilient.)** In order to achieve leakage-resilience on $\mathsf{sk}_\mathbf{y}$, we require that for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 1$ and $\mathbf{z} \in \mathcal{Z}$, the distributions $\{\mathbf{x}, \mathbf{y}, \mathsf{sE}(\mathbf{x}, \mathbf{w}), f(\mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{w}))\}$ and $\{\mathbf{x}, \mathbf{y}, \mathbf{r}\}$ are identical, where $\mathbf{w} \leftarrow \mathcal{W}$ and $\mathbf{r} \leftarrow \mathbb{Z}_p^{|\mathsf{sE}(\cdot)|+|f(\cdot)|}$.

3.2 Generic Construction

An overview of our generic construction has been present in Section (1). As mentioned in Section 1.2, a general approach [CGW15] to transform schemes over composite-order groups into ones over prime-order groups can be applied to Equation (1). Concretely, we replace g_1, g_2 with $[\mathbf{A}]_1, [\mathbf{B}]_2$, where $(\mathbf{A}, \mathbf{a}^\perp), (\mathbf{B}, \mathbf{b}^\perp) \leftarrow \mathcal{D}_{k+1,k}$ and other variables are transformed as follows:

$$\alpha \mapsto \mathbf{k} \in \mathbb{Z}_p^{k+1},\ u, w_i \mapsto \mathbf{U},\ \mathbf{W}_i \in \mathbb{Z}_p^{(k+1)\times(k+1)},\ s \mapsto \mathbf{s} \in \mathbb{Z}_p^k,\ r \mapsto \mathbf{r} \in \mathbb{Z}_p^k,$$
$$g_1^s \mapsto [\mathbf{As}]_1,\ g_1^{w_i s} \mapsto [\mathbf{W}_i^\top \mathbf{As}]_1,\ g_2^r \mapsto [\mathbf{Br}]_2,\ g_2^{w_i r} \mapsto [\mathbf{W}_i \mathbf{Br}]_2$$

The above transformation is also suitable to our second framework in Section 4.

Now, we provide the details of our generic construction. Given a $\mathbb{Z}_p$-linear leakage-resilient predicate encoding with attribute-hiding for predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$,

- $\mathsf{Setup}(1^\lambda)$: Let $N \in \mathbb{N}$ be the parameter of the $\mathbb{Z}_p$-linear leakage-resilient predicate encoding with attribute-hiding for predicate P and N is related to 1^λ. Run $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda)$, sample $(\mathbf{A}, \mathbf{a}^\perp)$, $(\mathbf{B}, \mathbf{b}^\perp)$ as in Equation (3), pick $\mathbf{k} \leftarrow \mathbb{Z}_p^{k+1}, \mathbf{W}_1, \ldots, \mathbf{W}_N \leftarrow \mathbb{Z}_p^{(k+1)\times(k+1)}$. Then pick $\mathbf{r} \leftarrow \mathbb{Z}_p^k, \mathbf{v} \leftarrow \mathcal{V}$, output

$$\mathsf{mpk} := \left(\mathbb{G}; [\mathbf{A}]_1, [\mathbf{W}_1^\top \mathbf{A}]_1, \ldots, [\mathbf{W}_N^\top \mathbf{A}]_1, [\mathbf{A}^\top \mathbf{k}]_T\right), \ \mathsf{mk} := \left(\mathbf{B}, \mathbf{k}, \mathbf{W}_1, \ldots, \mathbf{W}_N\right)$$

- $\mathsf{KeyGen}(\mathsf{mk}, \mathbf{y})$: Pick $\mathbf{r} \leftarrow \mathbb{Z}_p^k, \mathbf{z} \leftarrow \mathcal{Z}$ and output $\mathsf{sk}_\mathbf{y} := \left(\mathbf{z}, K_0, \mathbf{K}\right)$, where

$$K_0 := [\mathbf{B}\mathbf{r}]_2, \ \mathbf{K} := \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\mathbf{k}]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, [\mathbf{W}_1\mathbf{B}\mathbf{r}]_2, \ldots, [\mathbf{W}_N\mathbf{B}\mathbf{r}]_2)$$

- $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)$: Pick $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and output $\mathsf{ct}_\mathbf{x} := (C_0, \mathbf{C}, C_T)$, where

$$C_0 := [\mathbf{A}\mathbf{s}]_1, \mathbf{C} := \mathsf{sE}(\mathbf{x}, [\mathbf{W}_1^\top \mathbf{A}\mathbf{s}]_1, \ldots, [\mathbf{W}_N^\top \mathbf{A}\mathbf{s}]_1), C_T = [\mathbf{k}^\top \mathbf{A}\mathbf{s}]_T \cdot m$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\mathbf{y}, \mathsf{ct}_\mathbf{x})$: output $m' = C_T \cdot e(C_0, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{K}))^{-1} \cdot e(\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{C}), K_0)$.

Correctness. For any $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}, \mathbf{y}) = 1$, we have

$$\begin{aligned}
& C_T \cdot e(C_0, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{K}))^{-1} \\
&= m \cdot [\mathbf{k}^\top \mathbf{A}\mathbf{s}]_T \cdot e([\mathbf{A}\mathbf{s}]_1, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\mathbf{k}]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, [\mathbf{W}_1\mathbf{B}\mathbf{r}]_2, \ldots, [\mathbf{W}_N\mathbf{B}\mathbf{r}]_2)))^{-1} \\
&= m \cdot [\mathbf{k}^\top \mathbf{A}\mathbf{s}]_T \cdot e([\mathbf{A}\mathbf{s}]_1, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\mathbf{k}]_2))^{-1} \\
&\qquad \cdot e([\mathbf{A}\mathbf{s}]_1, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, [\mathbf{W}_1\mathbf{B}\mathbf{r}]_2, \ldots, [\mathbf{W}_N\mathbf{B}\mathbf{r}]_2)))^{-1} \\
&= m \cdot [\mathbf{k}^\top \mathbf{A}\mathbf{s}]_T \cdot e([\mathbf{A}\mathbf{s}]_1, [\mathbf{k}]_2)^{-1} \cdot e([\mathbf{A}\mathbf{s}]_1, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, [\mathbf{W}_1\mathbf{B}\mathbf{r}]_2, \ldots, [\mathbf{W}_N\mathbf{B}\mathbf{r}]_2)))^{-1} \\
&= m \cdot e([\mathbf{A}\mathbf{s}]_1, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, [\mathbf{W}_1\mathbf{B}\mathbf{r}]_2, \ldots, [\mathbf{W}_N\mathbf{B}\mathbf{r}]_2)))^{-1} \\
&= m \cdot \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, e([\mathbf{A}\mathbf{s}]_1, [\mathbf{W}_1\mathbf{B}\mathbf{r}]_2), \ldots, e([\mathbf{A}\mathbf{s}]_1, [\mathbf{W}_N\mathbf{B}\mathbf{r}]_2)))^{-1} \\
&= m \cdot \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, e([\mathbf{W}_1^\top \mathbf{A}\mathbf{s}]_1, [\mathbf{B}\mathbf{r}]_2), \ldots, e([\mathbf{W}_N^\top \mathbf{A}\mathbf{s}]_1, [\mathbf{B}\mathbf{r}]_2)))^{-1} \\
&= m \cdot \mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{sE}(\mathbf{x}, e([\mathbf{W}_1^\top \mathbf{A}\mathbf{s}]_1, [\mathbf{B}\mathbf{r}]_2), \ldots, e([\mathbf{W}_N^\top \mathbf{A}\mathbf{s}]_1, [\mathbf{B}\mathbf{r}]_2)))^{-1} \\
&= m \cdot e(\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{sE}(\mathbf{x}, [\mathbf{W}_1^\top \mathbf{A}\mathbf{s}]_1, \ldots, [\mathbf{W}_N^\top \mathbf{A}\mathbf{s}]_1)), [\mathbf{B}\mathbf{r}]_2)^{-1} \\
&= m \cdot e(\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{C}), \mathbf{K}_0)^{-1}
\end{aligned}$$

In the above equality, we exploit *linearity* (for lines 3, 6, 9) and *restricted α-reconstruction* (for lines 4, 8) mentioned in Section 3.1. Thus, $C_T \cdot e(C_0, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{K}))^{-1} \cdot e(\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{C}), K_0) = m$ and the correctness follows readily.

3.3 Security

We start by giving some lemmas of [CGW15,LRW11] which will be used throughout the security proof of our framework.

Lemma 1 ([LRW11]). *Let an integer $m \geq 3$ and let p be a prime. Let $\delta \leftarrow \mathbb{Z}_p^m, \tau \leftarrow \mathbb{Z}_p^m$, and let τ' be chosen uniformly from the set of vectors in $\mathbb{Z}_p^m$ which are orthogonal to δ under the dot product modulo p. Let $f : \mathbb{Z}_p^m \to \mathbf{W}$ be some function. Then there exists any positive constant c, such that $dist\big((\delta, f(\tau')), (\delta, f(\tau))\big) \leq p^{-c}$, as long as $|\mathbf{W}| \leq 4 \cdot \left(1 - \frac{1}{p}\right) \cdot p^{m-2c-2}$.*

Suppose that $\mathbf{A}$ and $\mathbf{B}$ have the same form as Equation (3), then we set

$$\begin{aligned}
\mathsf{PP} &:= \begin{pmatrix} \mathbb{G}; & [\mathbf{A}]_1, [\mathbf{W}_1^\top \mathbf{A}]_1, \ldots, [\mathbf{W}_N^\top \mathbf{A}]_1, \\ & [\mathbf{B}]_2, \ [\mathbf{W}_1\mathbf{B}]_2, \ldots, [\mathbf{W}_N\mathbf{B}]_2 \end{pmatrix}, \\
\mathsf{PP}^- &:= \left(\mathbb{G}; \ [\mathbf{A}]_1, [\mathbf{W}_1^\top \mathbf{A}]_1, \ldots, [\mathbf{W}_N^\top \mathbf{A}]_1, [\mathbf{B}]_2\right)
\end{aligned} \tag{4}$$

where $\mathbf{W}_1, \ldots, \mathbf{W}_N \leftarrow \mathbb{Z}_p^{(k+1)\times(k+1)}$.

Lemma 2 (Parameter-Hiding[CGW15]). *The following distributions are statistically indistinguishable:*

$$\left\{\mathsf{PP}, [\mathbf{a}^\perp]_2, \begin{array}{l}[\mathbf{b}^\perp \hat{s}]_1, [\mathbf{W}_1^\top \mathbf{b}^\perp \hat{s}]_1, \ldots, [\mathbf{W}_N^\top \mathbf{b}^\perp \hat{s}]_1 \\ [\mathbf{a}^\perp \hat{r}]_2, [\mathbf{W}_1 \mathbf{a}^\perp \hat{r}]_2, \ldots, [\mathbf{W}_N \mathbf{a}^\perp \hat{r}]_2\end{array}\right\} \text{ and}$$

$$\left\{\mathsf{PP}, [\mathbf{a}^\perp]_2, \begin{array}{l}[\mathbf{b}^\perp \hat{s}]_1, [(\mathbf{W}_1^\top \mathbf{b}^\perp + u_1 \mathbf{b}^\perp)\hat{s}]_1, \ldots, [(\mathbf{W}_N^\top \mathbf{b}^\perp + u_N \mathbf{b}^\perp)\hat{s}]_1 \\ [\mathbf{a}^\perp \hat{r}]_2, [(\mathbf{W}_1 \mathbf{a}^\perp + u_1 \mathbf{a}^\perp)\hat{r}]_2, \ldots, [(\mathbf{W}_N \mathbf{a}^\perp + u_N \mathbf{a}^\perp)\hat{r}]_2\end{array}\right\}$$

where $\hat{s}, \hat{r} \leftarrow \mathbb{Z}_p^*, \mathbf{u} := (u_1, \ldots, u_N) \leftarrow \mathbb{Z}_p^N$.

Lemma 3 ($\mathbb{H}$-hiding[CGW15]). *The following distributions are statistically indistinguishable:*

$$\{\mathsf{PP}^-, [\mathbf{a}^\perp]_2, [\mathbf{Br}]_2, [\mathbf{W}_1 \mathbf{Br} + \hat{v}_1 \mathbf{a}^\perp]_2, \ldots, [\mathbf{W}_N \mathbf{Br} + \hat{v}_N \mathbf{a}^\perp]_2\} \text{ and}$$

$$\{\mathsf{PP}^-, [\mathbf{a}^\perp]_2, [\mathbf{Br}]_2, [\hat{\mathbf{u}}_1]_2, \ldots, [\hat{\mathbf{u}}_N]_2\}$$

where $\mathbf{r} \leftarrow \mathbb{Z}_p^k, \hat{\mathbf{v}} := (\hat{v}_1, \ldots, \hat{v}_N) \leftarrow \mathbb{Z}_p^N$ *and for* $i = 1, \ldots, N$, $\hat{\mathbf{u}}_i \leftarrow \mathbb{Z}_p^{k+1}$ *subject to the constraint* $\mathbf{A}^\top \hat{\mathbf{u}}_i = (\mathbf{W}_i^\top \mathbf{A})^\top \mathbf{Br}$.

Lemma 4 ($\mathbb{G}$-uniformity[CGW15]). *The following distributions are statistically indistinguishable:*

$$\{\mathsf{PP}^-, [\mathbf{a}^\perp]_1, [\mathbf{As} + \mathbf{b}^\perp \hat{s}]_2, [\mathbf{W}_1^\top (\mathbf{As} + \mathbf{b}^\perp \hat{s})]_1, \ldots, [\mathbf{W}_N (\mathbf{As} + \mathbf{b}^\perp \hat{s})]_1\} \text{ and}$$

$$\{\mathsf{PP}^-, [\mathbf{a}^\perp]_2, [\mathbf{As} + \mathbf{b}^\perp \hat{s}]_1, [\hat{\mathbf{w}}_1]_1, \ldots, [\hat{\mathbf{w}}_N]_1\}$$

where $\mathbf{s} \leftarrow \mathbb{Z}_p^k, \hat{s} \leftarrow \mathbb{Z}_p^*; \hat{\mathbf{w}}_1, \ldots, \hat{\mathbf{w}}_N \leftarrow \mathbb{Z}_p^{k+1}$.

Theorem 1. *If k-Lin assumption holds, the construction described in Section 3.2 is* $(0, L_{\mathsf{sk}})$*-bounded-leakage secure and attribute-hiding. More precisely, for all* PPT *adversaries* $\mathcal{A}$ *subject to the restrictions: (1)* $\mathcal{A}$ *queries* O_2 *and* O_3 *at most q times; (2) The leakage on* mk *is not allowed and the leakage amount of* sk *are at most* L_{sk} *bits. There exists an algorithm* $\mathcal{B}$ *such that* $\mathsf{Adv}_{\mathcal{A}}^{\text{BLR-AH}}(\lambda) \leq (2q+1)\mathsf{Adv}_{\mathcal{B}}^{k\text{-Lin}}(\lambda) + \mathsf{negl}(\lambda)$.

Proof. Our proof sketch for the game sequence is shown in Table 2. In Table 2, we use a box to highlight the difference between two adjacent games and the cell marked by "—" means that the corresponding part of $\mathsf{sk}_{\mathbf{y}}$ or ct^* is the same as the last game. For the transition from $\mathsf{Game}_{2,i,1}$ to $\mathsf{Game}_{2,i,2}$, we employ Parameter-Hiding lemma, attribute-hiding encoding and attribute-hiding-leakage-resilient encoding mentioned in Section 3.1. In Game_3 and Game_4, m' denotes a random message and $\mathbf{x}'$ denotes a random attribute. Game_0 is the same as $\mathsf{Game}_{\text{BLM-AH}}$. In Game_4, the advantage of $\mathcal{A}$ is 0.

Table 2: Our proof sketch for the game sequence.

game	i-th queried secret key $\mathsf{sk}_{\mathbf{y}}$			ct^*			justification
	K_0	$\mathsf{rkE}(\mathbf{y}, \mathbf{z}, \cdot)$	$\mathsf{rE}(\mathbf{y}, \mathbf{z}, \cdot)$	C_0	$\mathsf{sE}(\cdot, \cdot)$	C_T	
Game_0	$[\mathbf{Br}]_2$	$[\mathbf{k}]_2$	$[\mathbf{W}_k \mathbf{Br}]_2$	$[\mathbf{As}]_1$	$\mathbf{x}^{(b)}, [\mathbf{W}_j^\top \mathbf{As}]_1$	$e([\mathbf{As}]_1, [\mathbf{k}]_2) \cdot m$	real game
Game_1	—	—	—	$[\boxed{\mathbf{As} + \mathbf{b}^\perp \hat{s}}]_1$	$\mathbf{x}^{(b)}, [\boxed{\mathbf{W}_j^\top (\mathbf{As} + \mathbf{b}^\perp \hat{s})}]_1$	$e([\boxed{\mathbf{As} + \mathbf{b}^\perp \hat{s}}]_1, [\mathbf{k}]_2) \cdot m$	k-Lin
$\mathsf{Game}_{2,i,1}$	$[\boxed{\mathbf{Br} + \mathbf{a}^\perp \hat{r}}]_2$	—	$[\boxed{\mathbf{W}_k(\mathbf{Br} + \mathbf{a}^\perp \hat{r})}]_2$	—	—	—	k-Lin
$\mathsf{Game}_{2,i,2}$	—	$[\boxed{\hat{\mathbf{k}}}]_2$	$[\mathbf{W}_k(\mathbf{Br} + \mathbf{a}^\perp \hat{r}) + \boxed{\hat{v}_k^i \mathbf{a}^\perp}]_2$	—	—	—	attribute-hiding, Parameter-Hiding, attribute-hiding-leakage-resilient
$\mathsf{Game}_{2,i,3}$	$[\mathbf{Br}]_2$	—	$[\boxed{\mathbf{W}_k \mathbf{Br} + \hat{v}_k^j \mathbf{a}^\perp}]_2$	—	—	—	k-Lin
Game_3	—	—	—	—	—	$e([\mathbf{As} + \mathbf{b}^\perp \hat{s}]_1, [\mathbf{k}]_2) \cdot \boxed{m'}$	statistically identical
Game_4	—	—	—	—	$\boxed{\mathbf{x}'}, [\mathbf{W}_j^\top (\mathbf{As} + \mathbf{b}^\perp \hat{s})]_1$	—	$\mathbb{H}$-hiding, $\mathbb{G}$-uniformity, attribute-hiding, attribute-hiding-leakage-resilient

We denote the advantage of $\mathcal{A}$ in Game_i by $\mathsf{Adv}_i(\lambda)$. Then we will show Theorem 1 by proving the indistinguishability among these games with the following lemmas.

Lemma 5 ($\mathsf{Game}_0 \overset{c}{\approx} \mathsf{Game}_1$). *For all* PPT *adversary* $\mathcal{A}$*, there exists an algorithm* $\mathcal{B}_1$ *such that* $|\mathsf{Adv}_0(\lambda) - \mathsf{Adv}_1(\lambda)| \leq \mathsf{Adv}^{k\text{-Lin}}_{\mathcal{B}_1}(\lambda) + 2/p$.

Proof. The proof is a simpler case of the proof of Lemma 6, we omit it here. □

Lemma 6 ($\mathsf{Game}_{2,i-1,3} \overset{c}{\approx} \mathsf{Game}_{2,i,1}$). *For all* PPT *adversary* $\mathcal{A}$ *and* $i = 1, \ldots, q$*, there exists an algorithm* $\mathcal{B}_2$ *such that* $|\mathsf{Adv}_{2,i-1,3}(\lambda) - \mathsf{Adv}_{2,i,1}(\lambda)| \leq \mathsf{Adv}^{k\text{-Lin}}_{\mathcal{B}_2}(\lambda) + 2/p$.

Proof. $\mathcal{B}_2$ samples $(\mathbf{A}, \mathbf{a}^\perp) \leftarrow \mathcal{D}_{k+1,k}$ along with $\mathbf{W}_1, \ldots, \mathbf{W}_N \leftarrow \mathbb{Z}_p^{(k+1)\times(k+1)}$. We know that $\{\mathbf{Br} + \mathbf{a}^\perp \hat{r} : \mathbf{r} \leftarrow \mathbb{Z}_p^k, \hat{r} \leftarrow \mathbb{Z}_p\}$ is statistically close to the uniform distribution. Then $\mathcal{B}_2$ gets as input $(\mathbb{G}, [\mathbf{B}]_2, [\mathbf{t}]_2) = (\mathbb{G}, [\mathbf{B}]_2, [\mathbf{Br} + \mathbf{a}^\perp \hat{r}]_2)$ where either $\hat{r} = 0$ or $\hat{r} \leftarrow \mathbb{Z}_p^*$ and proceeds as follows:
Setup. Pick $\mathbf{k} \leftarrow \mathbb{Z}_p^{k+1}, \alpha \leftarrow \mathbb{Z}_p$ and set $\hat{\mathbf{k}} := \mathbf{k} + \alpha \mathbf{a}^\perp$. With $\mathbb{G}, \mathbf{A}, \mathbf{W}_1, \ldots, \mathbf{W}_n, \mathcal{B}_2$ can simulate $\mathsf{mpk} := \big(\mathbb{G}; [\mathbf{A}]_1, [\mathbf{W}_1^\top \mathbf{A}]_1, \ldots, [\mathbf{W}_n^\top \mathbf{A}]_1, [A$
Key Queries. When $\mathcal{A}$ makes the j'th **Leak** (i.e., O_2) or **Reveal** (i.e., O_3) key query,

- When $j < i$, since $\mathbf{a}^\perp, \hat{\mathbf{k}}, \mathbf{W}_1, \ldots, \mathbf{W}_n$ and $[\mathbf{B}]_2$ has been known, semi-functional $\mathsf{sk}_\mathbf{y}$ can be generated properly;
- When $j = i$, $\mathcal{B}_2$ generates

$$\mathsf{sk}_\mathbf{y} := \big(\mathbf{z}, [\mathbf{t}]_2, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\mathbf{k}]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, [\mathbf{W}_1 \mathbf{t}]_2, \ldots, [\mathbf{W}_N \mathbf{t}]_2)\big)$$

- When $j > i$, it is not hard to know that normal $\mathsf{sk}_\mathbf{y}$ can also be generated properly;

Challenge. Since $\mathbf{b}^\perp$ is unknown, $\mathbf{As} + \mathbf{b}^\perp \hat{s}$ is statistically close to the uniform distribution. Thus, $\mathcal{B}_2$ would sample $\tilde{\mathbf{s}} \leftarrow \mathbb{Z}_p^{k+1}$ to replace $\mathbf{As} + \mathbf{b}^\perp \hat{s}$. After receiving challenge messages $(m^{(0)}, m^{(1)})$ and challenge vectors $(\mathbf{x}^{(0)}, \mathbf{x}^{(1)})$, $\mathcal{B}_2$ chooses a random bit $b \in \{0, 1\}$ and returns

$$\mathsf{ct}^* := \big([\tilde{\mathbf{s}}]_1, \mathsf{sE}(\mathbf{x}^{(b)}, [\mathbf{W}_1^\top \tilde{\mathbf{s}}]_1, \ldots, [\mathbf{W}_N^\top \tilde{\mathbf{s}}]_1), e([\tilde{\mathbf{s}}]_1, [\mathbf{k}]_2) \cdot m^{(b)}\big)$$

Observe that if $\mathbf{t} = \mathbf{Br}$, $\mathcal{B}_2$ has properly simulated $\mathsf{Game}_{2,i-1,3}$ and if $\mathbf{t} = \mathbf{Br} + \mathbf{a}^\perp \hat{r}$, $\mathcal{B}_2$ has properly simulated $\mathsf{Game}_{2,i,1}$. Since $\hat{s}, \hat{r} \leftarrow \mathbb{Z}_p^*$ yields a $2/p$ negligible difference in the advantage, Lemma 6 hence holds. □

Lemma 7 ($\mathsf{Game}_{2,i,1} \overset{s}{\approx} \mathsf{Game}_{2,i,2}$). *For* $i = 1, \ldots, q$*, it holds that* $|\mathsf{Adv}_{2,i,1}(\lambda) - \mathsf{Adv}_{2,i,2}(\lambda)| \approx 0$ *as long as the leakage amount of* sk *are at most* L_{sk} *bits.*

Proof. Given PP as in Equation (4), we state that $\mathsf{Game}_{2,i,1}$ and $\mathsf{Game}_{2,i,2}$ are statistically indistinguishable if the following distributions $\{\mathsf{PP}, [\mathbf{k}]_2, [\alpha \mathbf{a}^\perp]_2, \mathsf{ct}^*, \mathsf{sk}_\mathbf{y}\}$ and $\{\mathsf{PP}, [\mathbf{k}]_2, [\alpha \mathbf{a}^\perp]_2, \mathsf{ct}^*, \mathsf{sk}'_\mathbf{y}\}$ are identical where

$$\begin{aligned}\mathsf{ct}^* = &\big([\mathbf{As}]_1, \mathsf{sE}(\mathbf{x}^{(b)}, \{[\mathbf{W}_k^\top \mathbf{As}]_1\}_{k\in[N]}), [\mathbf{k}^\top \mathbf{As}]_T \cdot m^{(b)}\big) \cdot \\ &\big([\mathbf{b}^\perp \hat{s}]_1, \mathsf{sE}(\mathbf{x}^{(b)}, \{[\mathbf{W}_k^\top \mathbf{b}^\perp \hat{s}]_1\}_{k\in[N]}), [\mathbf{k}^\top \mathbf{b}^\perp \hat{s}]_T\big)\end{aligned}$$

and $\mathsf{sk}_\mathbf{y}, \mathsf{sk}'_\mathbf{y}$ are the i'th queried key in $\mathsf{Game}_{2,i,1}$ and $\mathsf{Game}_{2,i,2}$, respectively. Now we consider the following cases:

(1) If $\mathbf{y} \in \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}^{(0)}, \mathbf{y}) = 1$ and $\mathsf{P}(\mathbf{x}^{(1)}, \mathbf{y}) = 1$, we have

$$\begin{aligned}\mathsf{sk}_\mathbf{y} = &\big(\mathbf{1}, [\mathbf{Br}]_2, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\mathbf{k}]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, \{[\mathbf{W}_k \mathbf{Br}]_2\}_{k\in[N]})\big) \cdot \\ &\big(\mathbf{z}, [\mathbf{a}^\perp \hat{r}]_2, \mathsf{rE}(\mathbf{y}, \mathbf{z}, \{[\mathbf{W}_k \mathbf{a}^\perp \hat{r}]_2\}_{k\in[N]})\big) \\ \mathsf{sk}'_\mathbf{y} = &\big(\mathbf{1}, [\mathbf{Br}]_2, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\mathbf{k}]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, \{[\mathbf{W}_k \mathbf{Br}]_2\}_{k\in[N]})\big) \cdot \\ &\big(\mathbf{z}, [\mathbf{a}^\perp \hat{r}]_2, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\alpha \mathbf{a}^\perp]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, \{[\mathbf{W}_k \mathbf{a}^\perp \hat{r} + \hat{v}_k \mathbf{a}^\perp]_2\}_{k\in[N]})\big)\end{aligned}$$

where $\hat{\mathbf{v}} := (\hat{v}_1, \ldots, \hat{v}_N) \leftarrow \mathbb{Z}_p^N$ and the length of vector $\mathbf{1} := (1, \ldots, 1)$ is equal to the length of $\mathbf{z}$. We observe that it suffices to show that

$$\left\{\begin{array}{l} \mathsf{aux} : \mathsf{PP},\ [\mathbf{k}]_2,\ [\mathbf{B}]_2,\ [\alpha\mathbf{a}^\perp]_2 \\ \mathsf{ct}_{\mathbf{x}} :\ [\mathbf{b}^\perp \hat{s}]_1,\ \mathsf{sE}(\mathbf{x}^{(b)}, \left\{[\mathbf{W}_k^\top \mathbf{b}^\perp \hat{s}]_1\right\}_{k\in[N]}),\ [\mathbf{k}^\top \mathbf{b}^\perp \hat{s}]_T \\ \mathsf{sk}_{\mathbf{y}} :\ \mathbf{z},\ [\mathbf{a}^\perp \hat{r}]_2,\ \mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[\mathbf{W}_k \mathbf{a}^\perp \hat{r}]_2\right\}_{k\in[N]}) \end{array}\right\} \text{ and}$$

$$\left\{\begin{array}{l} \mathsf{aux} : \mathsf{PP},\ [\mathbf{k}]_2,\ [\mathbf{B}]_2,\ [\alpha\mathbf{a}^\perp]_2 \\ \mathsf{ct}_{\mathbf{x}} :\ [\mathbf{b}^\perp \hat{s}]_1,\ \mathsf{sE}(\mathbf{x}^{(b)},\ \left\{[\mathbf{W}_k^\top \mathbf{b}^\perp \hat{s}]_1\right\}_{k\in[N]}),\ [\mathbf{k}^\top \mathbf{b}^\perp \hat{s}]_T \\ \mathsf{sk}_{\mathbf{y}} :\ \mathbf{z},\ [\mathbf{a}^\perp \hat{r}]_2,\ \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\alpha\mathbf{a}^\perp]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[\mathbf{W}_k \mathbf{a}^\perp \hat{r} + \hat{v}_k \mathbf{a}^\perp]_2\right\}_{k\in[N]}) \end{array}\right\}$$

are indistinguishable. By parameter-hiding in Lemma 2, it suffices to show that:

$$\left\{\begin{array}{l} \mathsf{aux} : \mathsf{PP},\ [\mathbf{k}]_2,\ [\mathbf{B}]_2,\ [\alpha\mathbf{a}^\perp]_2 \\ \mathsf{ct}_{\mathbf{x}} :\ [\mathbf{b}^\perp \hat{s}]_1,\ \mathsf{sE}(\mathbf{x}^{(b)}, \left\{[(\mathbf{W}_k^\top \mathbf{b}^\perp + u_k \mathbf{b}^\perp)\hat{s}]_1\right\}_{k\in[N]}),\ [\mathbf{k}^\top \mathbf{b}^\perp \hat{s}]_T \\ \mathsf{sk}_{\mathbf{y}} :\ \mathbf{z},\ [\mathbf{a}^\perp \hat{r}]_2,\ \mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[(\mathbf{W}_k \mathbf{a}^\perp + u_k \mathbf{a}^\perp)\hat{r}]_2\right\}_{k\in[N]}) \end{array}\right\} \text{ and}$$

$$\left\{\begin{array}{l} \mathsf{aux} : \mathsf{PP},\ [\mathbf{k}]_2,\ [\mathbf{B}]_2,\ [\alpha\mathbf{a}^\perp]_2 \\ \mathsf{ct}_{\mathbf{x}} :\ [\mathbf{b}^\perp \hat{s}]_1,\ \mathsf{sE}(\mathbf{x}^{(b)},\ \left\{[(\mathbf{W}_k^\top \mathbf{b}^\perp + u_k \mathbf{b}^\perp)\hat{s}]_1\right\}_{k\in[N]}), [\mathbf{k}^\top \mathbf{b}^\perp \hat{s}]_T \\ \mathsf{sk}_{\mathbf{y}} :\ \mathbf{z},\ [\mathbf{a}^\perp \hat{r}]_2,\ \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\alpha\mathbf{a}^\perp]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[(\mathbf{W}_k \mathbf{a}^\perp + u_k \mathbf{a}^\perp)\hat{r} + \hat{v}_k \mathbf{a}^\perp]_2\right\}_{k\in[N]}) \end{array}\right\}$$

are indistinguishable. Let $\hat{g}_0 = [\mathbf{b}^\perp \hat{s}]_1, \hat{h}_0 = [\mathbf{a}^\perp \hat{r}]_2$ and set $[\mathbf{a}^\perp] = (\hat{h}_0)^\beta$, we note that

$$\begin{aligned} &\mathsf{sE}(\mathbf{x}^{(b)}, \left\{[(\mathbf{W}_k^\top \mathbf{b}^\perp + u_k \mathbf{b}^\perp)\hat{s}]_1\right\}_{k\in[N]}) = \mathsf{sE}(\mathbf{x}^{(b)}, \left\{[\mathbf{W}_k^\top \mathbf{b}^\perp \hat{s}]_1\right\}_{k\in[N]}) \cdot \hat{g}_0^{\mathsf{sE}(\mathbf{x}^{(b)}, \mathbf{u})}, \\ &\mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[(\mathbf{W}_k \mathbf{a}^\perp + u_k \mathbf{a}^\perp)\hat{r}]_2\right\}_{k\in[N]}) = \mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[\mathbf{W}_k \mathbf{a}^\perp \hat{r}]_2\right\}_{k\in[N]}) \cdot \hat{h}_0^{\mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{u})}, \\ &\mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\alpha\mathbf{a}^\perp]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[(\mathbf{W}_k \mathbf{a}^\perp + u_k \mathbf{a}^\perp)\hat{r} + \hat{v}_k \mathbf{a}^\perp]_2\right\}_{k\in[N]}) \\ =\ &\mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[\mathbf{W}_k \mathbf{a}^\perp \hat{r}]_2\right\}_{k\in[N]}) \cdot \hat{h}_0^{\mathsf{rkE}(\mathbf{y}, \mathbf{z}, \beta\alpha) + \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{u}) + \mathsf{rE}(\mathbf{y}, \mathbf{z}, \beta\hat{\mathbf{v}})}. \end{aligned}$$

Since $\mathcal{A}$ can only make **Leak** query on $\mathsf{sk}_{\mathbf{y}}$, according to *attribute-hiding-leakage-resilient* encoding, it holds that $\{\mathbf{x}, \mathbf{y}, \mathsf{sE}(\mathbf{x}, \mathbf{u}), f(\mathbf{z}, \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{u}))\}$ and $\{\mathbf{x}, \mathbf{y}, \mathbf{r}\}$ are indistinguishable. In other words, the adversary $\mathcal{A}$ cannot get any useful information to distinguish between $\mathsf{sk}_{\mathbf{y}}$ and $\mathsf{sk}'_{\mathbf{y}}$.

(2) If $\mathbf{y} \in \mathcal{Y}$ such that $\mathsf{P}(\mathbf{x}^{(0)}, \mathbf{y}) = 0$ and $\mathsf{P}(\mathbf{x}^{(1)}, \mathbf{y}) = 0$, the proof is also analogous to the proof of last case. Except that we should use *attribute-hiding* encoding, which claims that $\{\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathsf{sE}(\mathbf{x}, \mathbf{u}), \mathsf{rE}(\mathbf{y}, \mathbf{z}, \mathbf{u})\}$ and $\{\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{r}\}$ are indistinguishable.

Finally, Lemma 7 holds. □

Lemma 8 ($\mathsf{Game}_{2,i,2} \overset{c}{\approx} \mathsf{Game}_{2,i,3}$)**.** *For all* PPT *adversary* $\mathcal{A}$ *and* $i = 1, \ldots, q$*, there exists an algorithm* $\mathcal{B}_3$ *such that* $|\mathsf{Adv}_{2,i,2}(\lambda) - \mathsf{Adv}_{2,i,3}(\lambda)| \leq \mathsf{Adv}^{k\text{-Lin}}_{\mathcal{B}_3}(\lambda) + 2/p$

Proof. The proof is completely analogous to Lemma 6. □

Lemma 9 ($\mathsf{Game}_{2,q,3} \overset{s}{\approx} \mathsf{Game}_3$)**.** *For* $i = 1, \ldots, q$*, it holds that* $|\mathsf{Adv}_{2,q,3}(\lambda) - \mathsf{Adv}_3(\lambda)| \approx 0$

Proof. First, pick $\hat{\mathbf{k}} \leftarrow \mathbb{Z}_p^{k+1}, \alpha \leftarrow \mathbb{Z}_p$ and set $\mathbf{k} := \hat{\mathbf{k}} - \alpha\mathbf{a}^\perp$. Given just $(\mathsf{PP}, [\mathbf{a}^\perp]_2, [\hat{\mathbf{k}}]_2)$, we can simulate the setup phase and answer key queries as follows:

Setup. Since $e([\mathbf{A}]_1, [\hat{\mathbf{k}}]_2) := [\mathbf{A}^\top \mathbf{k} - \alpha \mathbf{A}^\top \mathbf{a}^\perp]_T = [\mathbf{A}^\top \mathbf{k}]_T$, then we can simulate $\mathsf{mpk} := \left(\mathbb{G}; [\mathbf{A}]_1, [\mathbf{W}_1^\top \mathbf{A}]_1, \ldots, [\mathbf{W}_N^\top \mathbf{A}]_1, [\mathbf{A}^\top \mathbf{k}]_T\right)$.

Key Queries. For the j'th key query for $\mathbf{y}$, we can generate a *semi-functional* secret key properly:

$$\mathsf{sk}_{\mathbf{y}} := \left(\mathbf{z}, [\mathbf{B}\mathbf{r}]_2, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\hat{\mathbf{k}}]_2) \cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, \left\{[\mathbf{W}_k \mathbf{B}\mathbf{r} + \hat{v}_k^j \mathbf{a}^\perp]_2\right\}_{k\in[N]})\right)$$

Challenge. Now, observe that the challenge ciphertext in $\mathsf{Game}_{2,q,3}$ is given by:

$$\begin{aligned}\mathsf{ct}^* :=& \big(C_0 = [\mathbf{As}+\mathbf{b}^\perp \hat{s}]_1, \mathbf{C} := \mathsf{sE}(\mathbf{x}^{(b)}, \{[\mathbf{W}_k^\top(\mathbf{As}+\mathbf{b}^\perp\hat{s})\}_{k\in[N]})]_1),\\ & C' = e([\mathbf{As}+\mathbf{b}^\perp\hat{s}]_1, [\mathbf{k}]_2)\cdot m^{(b)}\big)\end{aligned}$$

where we can rewrite $C' = e([\mathbf{As}+\mathbf{b}^\perp\hat{s}]_1, [\hat{\mathbf{k}}]_2)\cdot \boxed{e([\mathbf{b}^\perp\hat{s}]_1, [\mathbf{a}^\perp]_2)^{-\alpha}\cdot m^{(b)}}$.

Recall that $(\mathsf{mpk}, [\mathbf{B}]_2, \hat{\mathbf{k}})$ and $(C_0, \mathbf{C})$ are statistically independent of $\alpha \leftarrow \mathbb{Z}_p$, then we can say that $e([\mathbf{b}^\perp\hat{s}]_1, [\mathbf{a}^\perp]_2)^{-\alpha}$ is uniformly distributed over $\mathbb{G}_T$. This implies ct^* is identically distributed to semi-functional encryption of a random message in G_T, as in Game_3. Thus, Lemma 9 holds. □

Lemma 10 ($\mathsf{Game}_3 \overset{s}{\approx} \mathsf{Game}_4$). *For $i = 1, \ldots, q$, it holds that* $|\mathsf{Adv}_3(\lambda) - \mathsf{Adv}_4(\lambda)| \approx 0$

Proof. Pick $\hat{\mathbf{k}} \leftarrow \mathbb{Z}_p^{k+1}, \alpha \leftarrow \mathbb{Z}_p$ and set $\mathbf{k} := \hat{\mathbf{k}} - \alpha\mathbf{a}^\perp$. Given just $(\mathsf{PP}^-, [\mathbf{a}^\perp]_2, [\hat{\mathbf{k}}]_2)$, we note that $[\mathbf{W}_i\mathbf{B}]_2$ will not be simulated to ensure $\mathbb{G}$-uniformity holds. But we can still simulate the setup phase and answer key queries as follows:

Setup. We can simulate $\mathsf{mpk} := \big(\mathbb{G}; [\mathbf{A}]_1, [\mathbf{W}_1^\top\mathbf{A}]_1, \ldots, [\mathbf{W}_N^\top\mathbf{A}]_1, [\mathbf{A}^\top\mathbf{k}]_T\big)$.

Key Queries. For the j'th key query for $\mathbf{y}$, by $\mathbb{H}$-hiding in Lemma 3, we can simulate a *semi-functional* secret key:

$$\mathsf{sk}_\mathbf{y} := \big(\mathbf{z}, [\mathbf{Br}]_2, \mathsf{rkE}(\mathbf{y}, \mathbf{z}, [\hat{\mathbf{k}}]_2)\cdot \mathsf{rE}(\mathbf{y}, \mathbf{z}, [\hat{\mathbf{u}}_1^j]_2, \ldots, [\hat{\mathbf{u}}_N^j]_2)\big)$$

where for $i = 1, \ldots, N$, $\hat{\mathbf{u}}_i^j \leftarrow \mathbb{Z}_p^{k+1}$ subject to the constraint $\mathbf{A}^\top\hat{\mathbf{u}}_i^j = (\mathbf{W}_i^\top\mathbf{A})^\top\mathbf{Br}$.

Challenge. Now, observe that the challenge ciphertext in $\mathsf{Game}_{2,q,3}$ is given by:

$$C_0 = [\mathbf{As}+\mathbf{b}^\perp\hat{s}]_1, \mathbf{C} := \mathsf{sE}(\mathbf{x}^{(b)}, \{[\mathbf{W}_k^\top(\mathbf{As}+\mathbf{b}^\perp\hat{s})]_1\}_{k\in[N]}), C' = e([\mathbf{As}+\mathbf{b}^\perp\hat{s}]_1, [\hat{\mathbf{k}}]_2)\cdot m'$$

where C' is is uniformly distributed over G_T. By $\mathbb{G}$-uniformity in Lemma 4, then

$$\begin{aligned}&\{[\mathbf{As}+\mathbf{b}^\perp\hat{s}]_1, [\mathbf{W}_1^\top(\mathbf{As}+\mathbf{b}^\perp\hat{s})]_1, \ldots, [\mathbf{W}_N^\top(\mathbf{As}+\mathbf{b}^\perp\hat{s})]_1\}\\ \overset{s}{\approx}&\{[\mathbf{As}+\mathbf{b}^\perp\hat{s}]_1, [\hat{\mathbf{w}}_1]_1, \ldots, [\hat{\mathbf{w}}_N]_1\}\end{aligned}$$

where $\hat{\mathbf{w}}_1, \ldots, \hat{\mathbf{w}}_N \leftarrow \mathbb{Z}_p^{k+1}$. Note that $\mathcal{A}$ has no idea any information about $\mathbf{W}_i\mathbf{B}$ from $\mathsf{sk}_\mathbf{y}$ and mpk and hence $\mathbb{G}$-uniformity holds. So we can rewrite $\mathbf{C} := \mathsf{sE}(\mathbf{x}^{(b)}, [\hat{\mathbf{w}}_1]_1, \ldots, [\hat{\mathbf{w}}_N]_1)$. From *attribute-hiding* and *attribute-hiding-leakage-resilient* encoding, we can say that $\mathbf{C}$ is uniformly distributed over $G_1^{\mathsf{sE}(\cdot)}$. Thus, Lemma 10 holds. □

Finally, we complete the proof of Theorem 1 by showing the above lemmas which imply the indistinguishability between Game_0 and Game_4.

4 Leakage-resilient ABE in the CLM

In this section, we present our second leakage-resilient ABE framework, which is compatible with ZCG+18 but more versatile. Note that an overview of this generic construction has been present in Equation (2).

4.1 Leakage-resilient Predicate Encoding

We define a $\mathbb{Z}_p$-linear leakage-resilient predicate encoding for predicate $\mathsf{P} : \mathcal{X}\times\mathcal{Y} \to \{0,1\}$. It consists of a set of deterministic algorithms $(\mathsf{mkE}, \mathsf{mE}, \mathsf{rkE}, \mathsf{rE}, \mathsf{sE}, \mathsf{sD}, \mathsf{rD})$ and satisfies the following properties:

– **(linearity.)** For all $(\mathbf{x}, \mathbf{y}, \mathbf{v}, \mathbf{z}) \in \mathcal{X}\times\mathcal{Y}\times\mathcal{V}\times\mathcal{Z}$, $\mathsf{mkE}(\mathbf{v}, \cdot)$, $\mathsf{mE}(\mathbf{v}, \cdot)$, $\mathsf{rkE}(\mathbf{y}, \mathbf{z}, \cdot)$, $\mathsf{rE}(\mathbf{y}, \mathbf{z}, \cdot)$, $\mathsf{sE}(\mathbf{x}, \cdot)$, $\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \cdot)$, $\mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \cdot)$ are $\mathbb{Z}_p$-linear.

– **(restricted α-reconstruction.)** This property is the same as *restricted α-reconstruction* in Section 3.1.
– **(α-privacy.)** For all $(\mathbf{x},\mathbf{y}) \in \mathcal{X}\times\mathcal{Y}$ such that $\mathsf{P}(\mathbf{x},\mathbf{y}) = 0$, the distributions $\{\mathbf{x},\mathbf{y},\mathbf{z},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}),\mathsf{rkE}(\mathbf{y},\mathbf{z},\alpha) + \mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w})\}$ and $\{\mathbf{x},\mathbf{y},\mathbf{z},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}),\mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w})\}$ are identical, where the randomness is taken over $\mathbf{w}\leftarrow\mathcal{W}$.
– **(α-leakage-resilient.)** For all $(\mathbf{x},\mathbf{y})\in\mathcal{X}\times\mathcal{Y}$ such that $\mathsf{P}(\mathbf{x},\mathbf{y}) = 1$ and all $\alpha\in\mathbb{Z}_p, \mathbf{z}\in\mathcal{Z}, \mathbf{v}\in\mathcal{V}$, the distributions $\{\mathbf{x},\mathbf{y},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}), f(\mathbf{z},\mathsf{rkE}(\mathbf{y},\mathbf{z},\alpha)+\mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w}))\}$ and $\{\mathbf{x},\mathbf{y},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}), f(\mathbf{z},\mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w}))\}$ are identical, where $\mathbf{w}\leftarrow\mathcal{W}$. In addition, the distributions $\{\mathbf{x},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}), f(\mathbf{v},\mathsf{mkE}(\mathbf{v},\alpha)+\mathsf{mE}(\mathbf{v},\mathbf{w}))\}$ and $\{\mathbf{x},\alpha,\mathsf{sE}(\mathbf{x},\mathbf{w}), f(\mathbf{v},\mathsf{mE}(\mathbf{v},\mathbf{w}))\}$ are also identical.
– **(delegable.)** There exits a linear algorithm dE such that for all $\alpha\in\mathbb{Z}_p, \mathbf{v}\in\mathcal{V}, \mathbf{z}\in\mathcal{Z}, \mathbf{w}\in\mathcal{W}, \mathbf{y}\in\mathcal{Y}$, it holds that $\mathsf{dE}(\mathbf{y},\mathsf{mkE}(\mathbf{v},\alpha) + \mathsf{mE}(\mathbf{v},\mathbf{w})) = \mathsf{rkE}(\mathbf{y},\mathbf{z},\alpha) + \mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w})$. Note that the algorithm dE implies a linear map $\underline{S:\mathcal{Y}\times\mathcal{V}\to\mathcal{Z}}$.
– **(re-randomizable.)** For all $\alpha\in\mathbb{Z}_p, \mathbf{v},\mathbf{v}'\in\mathcal{V}, \mathbf{w}\in\mathcal{W}$, there exists a linear algorithm mR such that $\mathsf{mR}(\mathbf{v},\mathbf{v}',\mathsf{mkE}(\mathbf{v},\alpha)+\mathsf{mE}(\mathbf{v},\mathbf{w})) = \mathsf{mkE}(\mathbf{v}',\alpha) + \mathsf{mE}(\mathbf{v}',\mathbf{w})$. Similarly, for all $\alpha\in\mathbb{Z}_p, \mathbf{z},\mathbf{z}'\in\mathcal{Z}, \mathbf{w}\in\mathcal{W}, \mathbf{y}\in\mathcal{Y}$, there exists a linear algorithm kR such that $\mathsf{kR}(\mathbf{z},\mathbf{z}',\mathsf{rkE}(\mathbf{y},\mathbf{z},\alpha)+\mathsf{rE}(\mathbf{y},\mathbf{z},\mathbf{w})) = \mathsf{rkE}(\mathbf{y},\mathbf{z}',\alpha)+\mathsf{rE}(\mathbf{y},\mathbf{z}',\mathbf{w})$.

4.2 Generic Construction

Given a $\mathbb{Z}_p$-linear leakage-resilient predicate encoding for predicate $\mathsf{P}:\mathcal{X}\times\mathcal{Y}\to\{0,1\}$,

- $\mathsf{Setup}(1^\lambda)$: This algorithm is similar to the setup algorithm in Section 3.2. Run $\mathbb{G}\leftarrow\mathcal{G}(1^\lambda)$, sample $(\mathbf{A},\mathbf{a}^\perp)$, $(\mathbf{B},\mathbf{b}^\perp)$ as in Equation (3), pick $\mathbf{k}\leftarrow\mathbb{Z}_p^{k+1}, \mathbf{W}_1,\ldots,\mathbf{W}_N\leftarrow\mathbb{Z}_p^{(k+1)\times(k+1)}, \mathbf{r}\leftarrow\mathbb{Z}_p^k, \mathbf{v}\leftarrow\mathcal{V}$, output

$$\mathsf{mpk} := \begin{pmatrix}\mathbb{G};\ & [\mathbf{A}]_1,\ [\mathbf{W}_1^\top\mathbf{A}]_1,\ldots,[\mathbf{W}_N^\top\mathbf{A}]_1,\ [\mathbf{A}^\top\mathbf{k}]_T,\\ & [\mathbf{B}]_2,\ \ [\mathbf{W}_1\mathbf{B}]_2,\ldots,[\mathbf{W}_N\mathbf{B}]_2\end{pmatrix},$$
$$\mathsf{mk} := \left(\mathbf{v},[\mathbf{Br}]_2,\mathsf{mkE}(\mathbf{v},[\mathbf{k}]_2)\cdot\mathsf{mE}(\mathbf{v},[\mathbf{W}_1\mathbf{Br}]_2,\ldots,[\mathbf{W}_N\mathbf{Br}]_2)\right)$$

  where we set $K_0 = [\mathbf{Br}]_2, \mathbf{K} = \mathsf{mkE}(\mathbf{v},[\mathbf{k}]_2)\cdot\mathsf{mE}(\mathbf{v},[\mathbf{W}_1\mathbf{Br}]_2,\ldots,[\mathbf{W}_N\mathbf{Br}]_2)$.
- $\mathsf{Update}(\mathsf{mpk},\mathsf{sk}_\mathbf{y})$: If $\mathbf{y}=\epsilon$, then $\mathsf{sk}_\mathbf{y}$ is a master key and we rewrite it as $\mathsf{mk} := (\mathbf{v},[\mathbf{Br}]_2,\mathbf{K})$. Pick $\tilde{\mathbf{r}}\leftarrow\mathbb{Z}_p^k, \mathbf{v}'\leftarrow\mathcal{V}$, we set $\mathbf{r}' = \mathbf{r}+\tilde{\mathbf{r}}$ and output

$$\mathsf{mk}' := \left(\mathbf{v}',[\mathbf{Br}']_2,\mathsf{mR}(\mathbf{v},\mathbf{v}',\mathbf{K})\cdot\mathsf{mE}(\mathbf{v}',[\mathbf{W}_1\mathbf{B}\tilde{\mathbf{r}}]_2,\ldots,[\mathbf{W}_N\mathbf{B}\tilde{\mathbf{r}}]_2)\right)$$
$$\Downarrow$$
$$\mathsf{mk}' := \left(\mathbf{v}',[\mathbf{Br}']_2,\mathsf{mkE}(\mathbf{v}',[\mathbf{k}]_2)\cdot\mathsf{mE}(\mathbf{v}',[\mathbf{W}_1\mathbf{Br}']_2,\ldots,[\mathbf{W}_N\mathbf{Br}']_2)\right)$$

  Thus, we can generate a new master key mk' with the same distribution as mk. If $\mathbf{y}\in\mathcal{Y}$, $\mathsf{sk}_\mathbf{y}$ is a user secret key. Similarly, we can generate a new secret key $\mathsf{sk}'_\mathbf{y}$ using the algorithm kR.
- $\mathsf{KeyGen}(\mathsf{mk},\mathbf{y})$: Parse $\mathsf{mk} := (v,[\mathbf{Br}]_2,\mathbf{K})$. we compute $\mathbf{z}\leftarrow S(\mathbf{y},\mathbf{v})$ and

$$\mathsf{dE}(\mathbf{y},\mathbf{K}) = \mathsf{rkE}(\mathbf{y},\mathbf{z},[\mathbf{k}]_2)\cdot\mathsf{rE}(\mathbf{y},\mathbf{z},[\mathbf{W}_1\mathbf{Br}]_2,\ldots,[\mathbf{W}_N\mathbf{Br}]_2)$$

  Then pick $\tilde{\mathbf{r}}\leftarrow\mathbb{Z}_p^k, \mathbf{z}'\leftarrow\mathcal{Z}$ and set $\mathbf{r}' = \mathbf{r}+\tilde{\mathbf{r}}$. Output

$$\mathsf{sk}_\mathbf{y} := \left(\mathbf{z}',[\mathbf{Br}']_2,\mathsf{kR}(\mathbf{z},\mathbf{z}',\mathsf{dE}(\mathbf{y},\mathbf{K}))\cdot\mathsf{rE}(\mathbf{y},\mathbf{z}',[\mathbf{W}_1\mathbf{B}\tilde{\mathbf{r}}]_2,\ldots,[\mathbf{W}_N\mathbf{B}\tilde{\mathbf{r}}]_2)\right)$$
$$\Downarrow$$
$$\mathsf{sk}_\mathbf{y} := \left(\mathbf{z}',[\mathbf{Br}']_2,\mathsf{rkE}(\mathbf{y},\mathbf{z}',[\mathbf{k}]_2)\cdot\mathsf{rE}(\mathbf{y},\mathbf{z}',[\mathbf{W}_1\mathbf{Br}']_2,\ldots,[\mathbf{W}_N\mathbf{Br}']_2)\right)$$

  Similar to mk, here we also set $K_0 = [\mathbf{Br}']_2$ and

$$\mathbf{K} = \mathsf{rkE}(\mathbf{y},\mathbf{z}',[\mathbf{k}]_2)\cdot\mathsf{rE}(\mathbf{y},\mathbf{z}',[\mathbf{W}_1\mathbf{Br}']_2,\ldots,[\mathbf{W}_N\mathbf{Br}']_2)$$

- $\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)$: Pick $\mathsf{s} \leftarrow \mathbb{Z}_p^k$ and output $\mathsf{ct}_{\mathbf{x}} := (C_0, \mathbf{C}, C_T)$, where

$$C_0 := [\mathbf{As}]_1, \mathbf{C} := \mathsf{sE}(\mathbf{x}, [\mathbf{W}_1^\top \mathbf{As}]_1, \ldots, [\mathbf{W}_N^\top \mathbf{As}]_1), C_T = [\mathbf{k}^\top \mathbf{As}]_T \cdot m$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathbf{y}}, \mathsf{ct}_{\mathbf{x}})$: Parse $\mathsf{sk}_{\mathbf{y}} := (\mathbf{z}, K_0, \mathbf{K})$, $\mathsf{ct}_{\mathbf{x}} := (C_0, \mathbf{C}, C_T)$ and output $m' = C_T \cdot e(C_0, \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{K}))^{-1} \cdot e(\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{C}), K_0)$.

Correctness. Since linearity and restricted α-reconstruction (for $\mathsf{rkE}(\mathbf{y}, \mathbf{z}, \cdot), \mathsf{rE}(\mathbf{y}, \mathbf{z}, \cdot), \mathsf{sE}(\mathbf{x}, \cdot), \mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \cdot), \mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \cdot)$) are similar to ones in Section 3.1, the correctness also follows Section 3.2.

4.3 Security

Theorem 2. *If k-Lin assumption holds, the scheme described in Section 4.2 is $(L_{\mathsf{mk}}, L_{\mathsf{sk}})$-continual-leakage secure. More precisely, for all* PPT *adversaries $\mathcal{A}$ subject to the restrictions: (1) $\mathcal{A}$ makes at most q O'_2 and O'_3 queries; (2) The leakage amount of* mk *and* sk *are at most L_{mk}, L_{sk} bits, respectively. There exists an algorithm $\mathcal{B}$ such that* $\mathsf{Adv}^{\text{CLR-PH}}_{\mathcal{A}}(\lambda) \leq (2q+1)\mathsf{Adv}^{k\text{-Lin}}_{\mathcal{B}}(\lambda) + \mathsf{negl}(\lambda)$.

Proof. The proof sketch of Theorem 2 is similar to the proof of our first framework. It still designs a sequence of games which are the same as Table 2 except that Game_4 is canceled and there is no need to add $\hat{v}_k \mathbf{a}^\perp$ in $\mathsf{Game}_{2,i,2}$, $\mathsf{Game}_{2,i,3}$ and Game_3. Besides, we replace *attribute-hiding* and *attribute-hiding-leakage-resilient* with *α-privacy* and *α-privacy-leakage-resilient*. We omit details due to the page limitation.

5 Instantiations

In this section, we apply our frameworks to the compact-key ABE schemes for zero inner-product and non-zero inner-product in CGW15 and hence obtain several leakage-resilient instantiations.

5.1 Instantiation for the First Framework

Zero Inner-product Predicate. Let $\mathcal{X} = \mathcal{Y} := \mathbb{Z}_p^n, \mathcal{Z} := \mathbb{Z}_p^L, \mathcal{W} := \mathbb{Z}_p \times \mathbb{Z}_p^n \times \mathbb{Z}_p^L$, where n is the dimension of vector space. Let $L_{\mathsf{sk}} = (L - 2c - 1)\log p$ where c is a fixed positive constant. Pick $(u, \mathbf{w}, \mathbf{u}) \leftarrow \mathcal{W}, \mathbf{z} \leftarrow \mathcal{Z}$, then we have

- $\mathsf{rkE}(\mathbf{y}, \mathbf{z}, \alpha) := (\alpha, \mathbf{0}) \in \mathbb{Z}_p^{L+1}$,
- $\mathsf{sE}(\mathbf{x}, (u, \mathbf{w}, \mathbf{u})) := u\mathbf{x} + \mathbf{w} \in \mathbb{Z}_p^n$,
- $\mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, (d', \mathbf{d}) := d' - \mathbf{z}^\top \mathbf{d}$
- $\mathsf{rE}(\mathbf{y}, \mathbf{z}, (u, \mathbf{w}, \mathbf{u})) := (\mathbf{y}^\top \mathbf{w} + \mathbf{z}^\top \mathbf{u}, \mathbf{u})$,
- $\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{c}) := \mathbf{c}^\top \mathbf{y}$,

5.2 Instantiations for the Second Framework

Zero Inner-product Predicate. Let $\mathcal{X} = \mathcal{Y} := \mathbb{Z}_p^n, \mathcal{V} := \mathbb{Z}_p^{(n+1)\times L}, \mathcal{Z} := \mathbb{Z}_p^L, \mathcal{W} := \mathbb{Z}_p \times \mathbb{Z}_p^n \times \mathbb{Z}_p^L$, where n is the dimension of vector space. Let $L_{\mathsf{mk}} = L_{\mathsf{sk}} = (L - 2c - 1)\log p$ where c is a fixed positive constant. Pick $(u, \mathbf{w}, \mathbf{u}) \leftarrow \mathcal{W}, \mathbf{v} \leftarrow \mathcal{V}, \mathbf{z} \leftarrow \mathcal{Z}$. We denote the i's row vector by $\mathbf{v}_{i-1}^\top \in \mathbb{Z}_p^{1\times L}$ for $i = 1, 2, \ldots, n+1$ and the last n rows by $\vec{\mathbf{v}} \in \mathbb{Z}_p^{n\times L}$, respectively. Define

- $\mathsf{mkE}(\mathbf{v}, \alpha) := (\alpha, \mathbf{0}) \in \mathbb{Z}_p^{n+L+1}$,
- $\mathsf{rkE}(\mathbf{y}, \mathbf{z}, \alpha) := (\alpha, \mathbf{0}) \in \mathbb{Z}_p^{L+1}$,
- $\mathsf{sE}(\mathbf{x}, (u, \mathbf{w}, \mathbf{u})) := u\mathbf{x} + \mathbf{w} \in \mathbb{Z}_p^n$,
- $\mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, (d', \mathbf{d}) := d' - \mathbf{z}^\top \mathbf{d}$
- $\mathsf{mE}(\mathbf{v}, (u, \mathbf{w}, \mathbf{u})) := (\mathbf{v}_0^\top \mathbf{u}, \mathbf{w} + \vec{\mathbf{v}}\mathbf{u}, \mathbf{u})$,
- $\mathsf{rE}(\mathbf{y}, \mathbf{z}, (u, \mathbf{w}, \mathbf{u})) := (\mathbf{y}^\top \mathbf{w} + \mathbf{z}^\top \mathbf{u}, \mathbf{u})$,
- $\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{c}) := \mathbf{c}^\top \mathbf{y}$,

Non-zore Inner-product Predicate. Let $\mathcal{X} = \mathcal{Y} := \mathbb{Z}_p^n, \mathcal{V} := \mathbb{Z}_p^{n\times L}, \mathcal{Z} := \mathbb{Z}_p^L, \mathcal{W} := \mathbb{Z}_p \times \mathbb{Z}_p^n \times \mathbb{Z}_p^L$. Pick $(u, \mathbf{w}, \mathbf{u}) \leftarrow \mathcal{W}, \mathbf{v} \leftarrow \mathcal{V}, \mathbf{z} \leftarrow \mathcal{Z}$. Define

- $\mathsf{mkE}(\mathbf{v}, \alpha) := (\alpha, \mathbf{0}) \in \mathbb{Z}_p^{n+L+1}$,
- $\mathsf{rkE}(\mathbf{y}, \mathbf{z}, \alpha) := (\alpha, \mathbf{0}) \in \mathbb{Z}_p^{L+2}$,
- $\mathsf{sD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{c}) := \mathbf{c}^\top \mathbf{y} \cdot (\mathbf{x}^\top \mathbf{y})^{-1}$,
- $\mathsf{sE}(\mathbf{x}, (u, \mathbf{w}, \mathbf{u})) := u\mathbf{x} + \mathbf{w} \in \mathbb{Z}_p^n$
- $\mathsf{mE}(\mathbf{v}, (u, \mathbf{w}, \mathbf{u})) := (u, \mathbf{w} + \mathbf{v}\mathbf{u}, \mathbf{u})$,
- $\mathsf{rE}(\mathbf{y}, \mathbf{z}, (u, \mathbf{w}, \mathbf{u})) := (u, \mathbf{y}^\top \mathbf{w} + \mathbf{z}^\top \mathbf{u}, \mathbf{u})$,
- $\mathsf{rD}(\mathbf{x}, \mathbf{y}, \mathbf{z}, (d', d, \mathbf{d})) := d' + d \cdot (\mathbf{x}^\top \mathbf{y})^{-1} - \mathbf{z}^\top \mathbf{d}$,

Acknowledgments . This work was supported by National Natural Science Foundation of China (61972156, 62372180), NSFC-ISF Joint Scientific Research Program (61961146004), Innovation Program of ShanghaiMunicipal Education Commission (2021-01-07-00-08-E00101) and the “Digital Silk Road” Shanghai International Joint Lab of Trustworthy Intelligent Software (22510750100), University natural science research project in Jiangsu Province (22KJB520035), Open project of “Jiangsu Key Laboratory for Elevator Intelligent Safety" (JSKLESS202104) and Special teaching project of Jiangsu Computer Society (JSCS2022049).

References

AARR02. Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi. The em side—channel (s). In *International workshop on cryptographic hardware and embedded systems*, pages 29–45. Springer, 2002.

AGV09. Adi Akavia, Shafi Goldwasser, and Vinod Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In *Theory of cryptography conference*, pages 474–495. Springer, 2009.

Att14. Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In *Advances in Cryptology–EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings 33*, pages 557–577. Springer, 2014.

BKKV10. Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz, and Vinod Vaikuntanathan. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 501–510. IEEE, 2010.

CGW15. Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system abe in prime-order groups via predicate encodings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 595–624. Springer, 2015.

CLW06. Giovanni Di Crescenzo, Richard Lipton, and Shabsi Walfish. Perfectly secure password protocols in the bounded retrieval model. In *Theory of Cryptography Conference*, pages 225–244. Springer, 2006.

DKL09. Yevgeniy Dodis, Yael Tauman Kalai, and Shachar Lovett. On cryptography with auxiliary input. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 621–630, 2009.

DP08. Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 293–302. IEEE, 2008.

HSH+09. J Alex Halderman, Seth D Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A Calandrino, Ariel J Feldman, Jacob Appelbaum, and Edward W Felten. Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM*, 52(5):91–98, 2009.

KHF+19. Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, et al. Spectre attacks: Exploiting speculative execution. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1–19. IEEE, 2019.

KHPP16. Intae Kim, Seong Oun Hwang, Jong Hwan Park, and Chanil Park. An efficient predicate encryption with constant pairing computations and minimum costs. *IEEE Transactions on Computers*, 65(10):2947–2958, 2016.

KR19. Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. *IACR Cryptol. ePrint Arch.*, 2019:302, 2019.

LOS+10. Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 62–91. Springer, 2010.

LRW11. Allison Lewko, Yannis Rouselakis, and Brent Waters. Achieving leakage resilience through dual system encryption. In *Theory of Cryptography Conference*, pages 70–88. Springer, 2011.

LYZ19. Jiguo Li, Qihong Yu, and Yichen Zhang. Hierarchical attribute based encryption with continuous leakage-resilience. *Information Sciences*, 484:113–134, 2019.

LYZS19. Jiguo Li, Qihong Yu, Yichen Zhang, and Jian Shen. Key-policy attribute-based encryption against continual auxiliary input leakage. *Information Sciences*, 470:175–188, 2019.

NY19. Ryo Nishimaki and Takashi Yamakawa. Leakage-resilient identity-based encryption in bounded retrieval model with nearly optimal leakage-ratio. In *IACR International Workshop on Public Key Cryptography*, pages 466–495. Springer, 2019.

SW05. Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24*, pages 457–473. Springer, 2005.

Wee14. Hoeteck Wee. Dual system encryption via predicate encodings. In *Theory of Cryptography Conference*, pages 616–637. Springer, 2014.

YAX+16. Zuoxia Yu, Man Ho Au, Qiuliang Xu, Rupeng Yang, and Jinguang Han. Leakage-resilient functional encryption via pair encodings. In *Australasian Conference on Information Security and Privacy*, pages 443–460. Springer, 2016.

YCZY12. Tsz Hon Yuen, Sherman SM Chow, Ye Zhang, and Siu Ming Yiu. Identity-based encryption resilient to continual auxiliary leakage. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 117–134. Springer, 2012.

ZCG+18. Jie Zhang, Jie Chen, Junqing Gong, Aijun Ge, and Chuangui Ma. Leakage-resilient attribute based encryption in prime-order groups via predicate encodings. *Designs, Codes and Cryptography*, 86(6):1339–1366, 2018.

ZM16. Mingwu Zhang and Yi Mu. Token-leakage tolerant and vector obfuscated ipe and application in privacy-preserving two-party point/polynomial evaluations. *The Computer Journal*, 59(4):493–507, 2016.

ZZM17. Leyou Zhang, Jingxia Zhang, and Yi Mu. Novel leakage-resilient attribute-based encryption from hash proof system. *The Computer Journal*, 60(4):541–554, 2017.