Hindawi
Security and Communication Networks
Volume 2017, Article ID 7323158, 19 pages
https://doi.org/10.1155/2017/7323158

WILEY | Hindawi

Research Article

Shorter Decentralized Attribute-Based Encryption via Extended Dual System Groups

Jie Zhang,[1,2] Jie Chen,[2] Aijun Ge,[1] and Chuangui Ma[1,3]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China*
[2]*East China Normal University, Shanghai, China*
[3]*Army Aviation Institute, Beijing, China*

Correspondence should be addressed to Jie Zhang; zhangjie902@sina.cn

Received 10 April 2017; Revised 14 July 2017; Accepted 6 August 2017; Published 18 October 2017

Academic Editor: Zonghua Zhang

Decentralized attribute-based encryption (ABE) is a special form of multiauthority ABE systems, in which no central authority and global coordination are required other than creating the common reference parameters. In this paper, we propose a new decentralized ABE in prime-order groups by using extended dual system groups. We formulate some assumptions used to prove the security of our scheme. Our proposed scheme is fully secure under the standard k-Lin assumption in random oracle model and can support any monotone access structures. Compared with existing fully secure decentralized ABE systems, our construction has shorter ciphertexts and secret keys. Moreover, fast decryption is achieved in our system, in which ciphertexts can be decrypted with a constant number of pairings.

1. Introduction

Attribute-based encryption (ABE), which enables fine-grained access control, was first introduced by Sahai and Waters [1]. Subsequently, Goyal et al. [2] classified ABE as key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, ciphertexts are associated with a set of attributes and secret keys are associated with access policies, while the opposite is true for CP-ABE. The ciphertext can be decrypted by secret keys if and only if the attributes satisfy the access policy.

Over the past decade, there have been a number of ABE schemes [3–9] proposed for supporting fairly expressive policies. However, the classical ABE system has only a single authority, which manages all attributes and issues private keys for all users. This may be unable to meet the requirements of some applications due to the lack of flexibility. There are three major aspects that impact the application value of single authority ABE systems. First, the single authority system failed to achieve the collaboration between different institutions since it cannot verify attributes across different organizations. Second, there exists key escrow problem in single authority system. The authority must be highly trustworthy as it can decrypt any ciphertext. Finally, key generation for all users that relied on a single authority is a huge workload and can easily become a performance bottleneck in the system. Furthermore, failure of the authority affects the whole system.

Multiauthority or decentralized ABE [10, 11] systems are put forward to address this issue. Lewko and Waters [11] provided the first fully secure decentralized ABE system. In their system, any party can become an authority by creating a public key. Authorities can issue private keys independently, and some authorities that go wrong will only affect the attributes in their domain and not the system as a whole. In addition, the scheme in [11] supports any monotone access structures.

Though the Lewko-Waters decentralized ABE scheme is expressive, the construction is based on composite-order bilinear group. The current research [12] showed that prime-order bilinear groups outperform composite-order groups in terms of both time efficiency and space efficiency. To be specific, elements with 3072 or 3248 bits are required for a 128-bit security level in composite-order groups according to NIST or ECRYPT II recommendations, while elements with

256 bits are sufficient in prime-order groups for the same security level. As for the time efficiency, [12] indicated that a pairing over an elliptic curve of composite order is 254 times slower than over a prime-order elliptic curve for the 128-bit security level. For the above reasons, it is preferable to design schemes on prime-order groups. In a subsequent work by Okamoto and Takashima [13], a decentralized ABE system on prime-order groups was presented by using dual pairing vector spaces [5]. The construction improves the efficiency of decentralized ABE systems, but there is still a significant performance penalty due to the required size of the vectors. Hence, it is worth constructing a more compact decentralized ABE system in prime-order setting.

We present a new construction of decentralized ABE by using extended dual system group (EDSG). Our proposed scheme is built on prime-order groups with better space and time efficiency and can be proved fully secure under standard k-Lin assumption in the random oracle model.

To prove that full security of decentralized ABE system is a challenging job, even using the powerful dual system encryption methodology [14, 15], [11] used two subgroups for semifunctional space. The first subgroup is used to hide nominal semifunctionality from the attacker's view by appending blinding factors to each key at a time. The second subgroup is used to avoid leakage of information about the first one by switching the semifunctional components from the first subgroup to it.

Dual system groups (DSG) [16] are an attractive tool for simulating composite-order groups in the prime-order setting. In contrast to prior works [17–19], which attempted to maximize the properties satisfied by both composite-order and prime-order groups, the dual system groups seek to investigate the minimal properties needed for the application to dual system encryption. The benefit is that we can obtain more efficient and compact schemes, and that is why our scheme can reduce the size of ciphertext compared with previous work [13]. Unfortunately, we observe that dual system groups in [16] are insufficient for constructing fully secure decentralized ABE since it only has one semifunctional space. To overcome this, we extend the basis of dual system groups from $2k \times 2k$ matrix to $3k \times 3k$ matrix inspired by [20]. The first k-dimension subspace is the normal space, the next k-dimension subspace is used to construct type 1 semifunctional secret keys, and the last k-dimension subspace is used to construct type 2 semifunctional secret keys. In addition, we also realize the left subgroup indistinguishability, right subgroup indistinguishability 1, and right subgroup indistinguishability 2. These assumptions are used to mimic the effect of the subgroup decision assumption in composite-order groups.

The paper is organized as follows. In Section 2, we introduced the related works. In Section 3, a brief summary of the relevant concepts in multiauthority CP-ABE and prime-order bilinear groups was presented. In Section 4, we gave our revised definition of dual system groups and realized it in the prime-order setting in Section 5. In Section 6, we gave our decentralized CP-ABE system, outlined the security proof, and discussed its efficiency. In Section 7, we concluded the paper.

2. Related Works

Attribute-based encryption was introduced by Sahai and Waters [1], which can encrypt a message for multiple receivers by their attributes, rather than designating recipient in advance. Subsequently, Goyal et al. [2] extended this idea and classified ABE system into two categories: key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). The first fully secure ABE system was presented by Lewko et al. [4]; all ABE systems can only be proved to be selective secure ones before that. In addition, several variants of ABE have been proposed. Ostrovsky et al. [21] showed how to realize negation by incorporating specific revocation schemes into the construction of [2]. Lewko et al. [22] provided a fully secure ABE system which is resilient to continual leakage. With regard to the public parameter optimization problems, large universe ABE system, in which the size of the attribute universe can be exponentially large, was proposed in [23, 24]. The first multiauthority ABE system was introduced in [10] by Chase, which has one central authority (CA) and multiple attribute authorities (AAs). Subsequently, Chase and Chow [25] removed the CA by using a distributed pseudorandom function. Both of [10, 25] can only support AND-gates policy. A multiauthority ABE that supports threshold policy was provided by Lin et al. [26]. CA is not required for their system. However, the authorities are fixed and they must interact with each other during setup. The multiauthority ABE proposed in [10, 25, 26] looked only at the KP-ABE setting. Müller et al. [27] proposed the first multiauthority CP-ABE supported policies written in disjunctive normal form (DNF) with one CA and multiple AAs. The system can be only proved to be secure in generic group model. In addition, all these above systems can only defend selective attacks; that is, the attacker must commit to a target access structure before setup phase. Lewko and Waters [11] first obtained a fully secure multiauthority CP-ABE by using dual system encryption technique [14, 15]. Their system is decentralized; that is, the authorities are equal and with no need for CA and can support any monotone access structures. They proved security under static assumptions in the random oracle model. Liu et al. [28] proposed a multiauthority CP-ABE where there are multiple CAs and AAs. In their system, all of the CAs must work together to issue an identity-related key to the user. They used (n, n) threshold policy to distribute the master secret to prevent the authority decrypting ciphertexts independently. The system can be proved fully secure in the standard model. Scheme [11] is built on the composite-order group, which resulted in low efficiency of the systems. An improvement design was carried out in prime-order bilinear groups in [13]. Recently, Rouselakis and Waters [29] proposed an efficient large universe decentralized ABE system. However, the scheme only achieved static security, in which all queries (about both ciphertexts and secret keys) done by the attacker should be sent to the challenger immediately after seeing the global parameters.

In addition, some extension researches on multiauthority ABE have been proposed. Ma et al. [30] presented a multiauthority ABE with traitor tracing. The system is not

practical due to infeasible large sizes of public key and ciphertext. Li et al. [31] proposed a multiauthority CP-ABE scheme with accountability, which allows tracing the identity of a misbehaving user who leaked the decryption key to others. The system supported AND-gates policy. A large universe decentralized KP-ABE scheme was proposed in [32]. The system supported any monotone access policy and can be proved as selectively secure in the standard model. Gorasia et al. [33] presented a multiauthority CP-ABE with fast decryption, which only supports threshold policy. Zhong et al. [34] proposed a decentralized CP-ABE scheme with hidden policy. It also supported user revocation but only achieved selective security. An adaptively secure multiauthority CP-ABE scheme with verifiable outsourced decryption was given in [35].

3. Preliminaries

Notation. We use $s \leftarrow_R S$ to denote that s is picked randomly from a set S. We denote probabilistic polynomial-time by PPT. $[n]$ denotes the set $\{1, \ldots, n\}$ for any $n \in \mathbb{Z}^+$.

3.1. Prime-Order Bilinear Groups and Computational Assumptions

Prime-Order Bilinear Groups. The asymmetric prime-order group generator $\mathcal{G}$ takes a security parameter λ as input and outputs $(p, G_1, G_2, G_T, g_1, g_2, e)$, where G_1, G_2, and G_T are cyclic groups of prime order p, g_1, g_2 are generators of G_1, G_2, respectively, $e : G_1 \times G_2 \to G_T$ is an effective computable nondegenerate bilinear pairing, that is, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$, and $g_T = e(g_1, g_2) \neq 1$.

Assumption 1 (k-Lin: the k-linear assumption in G_1). For any PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in λ:

$$\mathsf{Adv}_{\mathcal{A}}^{k\text{-Lin}} := \left|\Pr\left[\mathcal{A}\left(D, T_0\right) = 1\right] - \Pr\left[\mathcal{A}\left(D, T_1\right) = 1\right]\right|, \quad (1)$$

where

$$\begin{aligned} D &:= \left(p, G_1, G_2, G_T, e, g_1, g_2, g_1^{a_1}, \ldots, g_1^{a_k}, g_1^{a_{k+1}}, g_1^{a_1 s_1}, \ldots, g_1^{a_k s_k}\right), \\ T_0 &:= g_1^{a_{k+1}(s_1 + \cdots + s_k)}, \\ T_1 &:= g_1^{a_{k+1}(s_1 + \cdots + s_k) + s_{k+1}}, \\ & s_1, \ldots, s_k \longleftarrow \mathbb{Z}_p,\ a_1, \ldots, a_k, a_{k+1}, s_{k+1} \longleftarrow \mathbb{Z}_p^*. \end{aligned} \quad (2)$$

Assumption 2 ((k, ℓ)-LLin: the (k, ℓ)-lifted linear assumption in G_1). For any PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in λ:

$$\begin{aligned} &\mathsf{Adv}_{\mathcal{A}}^{(k,\ell)\text{-LLin}} \\ &\quad := \left|\Pr\left[\mathcal{A}\left(D, T_0\right) = 1\right] - \Pr\left[\mathcal{A}\left(D, T_1\right) = 1\right]\right|, \end{aligned} \quad (3)$$

where

$$\begin{aligned} D &:= \left(p, G_1, G_2, G_T, e, g_1, g_2, g_1^{a_1}, \ldots, g_1^{a_k}, \left\{g_1^{b_{i,j}}\right\}_{i \in [\ell], j \in [k]}, g_1^{a_1 s_1}, \ldots, g_1^{a_k s_k}\right), \\ T_0 &:= \left\{g_1^{b_{i,1} s_1 + \cdots + b_{i,k} s_k}\right\}_{i \in [\ell]}, \\ T_1 &:= \left\{g_1^{b_{i,1} s_1 + \cdots + b_{i,k} s_k + s_{k+i}}\right\}_{i \in [\ell]}, \\ & s_1, \ldots, s_k \longleftarrow \mathbb{Z}_p,\ a_1, \ldots, a_k, b_{i,j}, s_{k+i} \longleftarrow \mathbb{Z}_p^*,\ i \in [\ell],\ j \in [k]. \end{aligned} \quad (4)$$

Lemma 3 (see [20]). *For any PPT adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}_{\mathcal{A}}^{(k,\ell)\text{-LLin}} \leqslant \ell \cdot \mathsf{Adv}_{\mathcal{B}}^{k\text{-Lin}} + \frac{1}{(p-1)}. \quad (5)$$

3.2. Multiauthority CP-ABE

3.2.1. Definition. In this paper, we used the definition of multiauthority CP-ABE and security model presented in [11]. We let U_i denote the attribute set managed by AA_i and $U = \bigcup U_i$ denote the universe of attributes. For $i \neq j$, we assume that $U_i \cap U_j = \Phi$. A multiauthority CP-ABE system consists of the following five algorithms:

$\mathsf{GlobalSetup}(1^\lambda) \to \mathsf{GP}$. This algorithm takes as input a security parameter λ and outputs the global public parameters GP.

$\mathsf{Authority\ Setup}(\mathsf{GP}) \to \mathsf{APK}_i, \mathsf{ASK}_i$. This algorithm is run by attribute authority AA_i. It takes as input global parameters GP and outputs its own public key APK_i and secret key ASK_i.

$\mathsf{KeyGen}(\mathsf{GP}, \mathsf{GID}, \mathsf{ASK}_j, att_i) \to \mathsf{SK}_{GID,i}$. This algorithm is run by AA_j. It takes as input GP, ASK_j, an identity GID and an attribute att_i belonging to AA_j and returns a secret key $\mathsf{SK}_{\mathrm{GID},i}$.

$\mathsf{Enc}(\mathsf{GP}, (\mathbf{M}, \rho), \{\mathsf{APK}_i\}, m) \to \mathsf{CT}$. This algorithm takes as input GP, an access matrix $(\mathbf{M}, \rho)$, the set of public keys for relevant authorities, and a message m and outputs a ciphertext CT.

$\mathsf{Dec}(\mathsf{CT}, \{\mathsf{SK}_{\mathrm{GID},i}\}, \mathsf{GP}) \to m$. This algorithm takes as input GP, $\{\mathsf{SK}_{\mathrm{GID},i}\}$, and CT. If the collection of attributes satisfies the access policy, it outputs the message m; otherwise, it outputs $\perp$.

3.2.2. Security Model. The security of multiauthority CP-ABE is defined by the following game run between a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$.

Setup. The challenger $\mathcal{B}$ executes $\mathsf{GlobalSetup}$ and $\mathsf{Authority\ Setup}$ algorithm. It gives GP and $\{\mathsf{APK}_i\}$ to the adversary $\mathcal{A}$. For corrupt authorities, $\mathcal{B}$ also gives the corresponding $\{\mathsf{ASK}_i\}$ to $\mathcal{A}$.

Key Query Phase 1. In this phase, $\mathcal{A}$ makes key queries by submitting $(\mathsf{GID}, \mathrm{att}_i)$ to $\mathcal{B}$, where att_i belonged to uncorrupted authorities. $\mathcal{B}$ returns $\mathsf{SK}_{\mathsf{GID},i}$ to $\mathcal{A}$.

Challenge. $\mathcal{A}$ submits two equal-length messages m_0, m_1 and an access policy $(\mathbf{M}, \rho)$ with the following constraint. We let V denote the subset of attributes controlled by corrupt AAs. For each identity GID, V_{GID} denotes the subset of attributes att_i which $\mathcal{A}$ has queried. For each GID, we require that $V \cup V_{\mathsf{GID}}$ cannot satisfy $(\mathbf{M}, \rho)$. $\mathcal{B}$ randomly chooses $\beta \in \{0, 1\}$ and encrypts m_β under $(\mathbf{M}, \rho)$. It sends the ciphertext to $\mathcal{A}$.

Key Query Phase 2. $\mathcal{A}$ continually queries $\mathcal{B}$ as in phase 1 in the same constraint.

Guess. $\mathcal{A}$ outputs a guess β' for β.

The adversary's advantage is defined to be $|\Pr[\beta' = \beta] - 1/2|$.

Definition 4. A multiauthority CP-ABE scheme is secure if, for all PPT adversaries, the advantage is negligible in the above security game.

4. Extended Dual System Groups

(i) $\mathsf{SampP}(1^\lambda, 1^n)$: output:

(a) Public parameter, pp, contains group description$(\mathbb{G}, \mathbb{H}, \mathbb{G}_T)$, a nondegenerate bilinear map $e : \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T$, a linear map μ defined on $\mathbb{H}$, and some additional parameters for SampG and SampH.

(b) Secret parameter, sp, contains $\widehat{h}^*, \widetilde{h}^* \in \mathbb{H}$ (where $\widehat{h}^*, \widetilde{h}^* \neq 1$), and some parameters for $\widehat{\mathsf{SampG}}$, $\widehat{\mathsf{SampH}}$, $\widetilde{\mathsf{SampG}}$, and $\widetilde{\mathsf{SampH}}$.

(ii) SampGT: $\mathrm{Im}(\mu) \to \mathbb{G}_T$.

(iii) $\mathsf{SampG}(\mathsf{pp})$: output $\overrightarrow{g} = (g_0, g_1, \ldots, g_n) \in \mathbb{G}^{n+1}$.

(iv) $\mathsf{SampH}(\mathsf{pp})$: output $\overrightarrow{h} = (h_0, h_1, \ldots, h_n) \in \mathbb{H}^{n+1}$.

(v) $\widehat{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp})$: output $\overrightarrow{\widehat{g}} = (\widehat{g}_0, \widehat{g}_1, \ldots, \widehat{g}_n) \in \mathbb{G}^{n+1}$.

(vi) $\widehat{\mathsf{SampH}}(\mathsf{pp}, \mathsf{sp})$: output $\overrightarrow{\widehat{h}} = (\widehat{h}_0, \widehat{h}_1, \ldots, \widehat{h}_n) \in \mathbb{H}^{n+1}$.

(vii) $\widetilde{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp})$: output $\overrightarrow{\widetilde{g}} = (\widetilde{g}_0, \widetilde{g}_1, \ldots, \widetilde{g}_n) \in \mathbb{G}^{n+1}$.

(viii) $\widetilde{\mathsf{SampH}}(\mathsf{pp}, \mathsf{sp})$: output $\overrightarrow{\widetilde{h}} = (\widetilde{h}_0, \widetilde{h}_1, \ldots, \widetilde{h}_n) \in \mathbb{H}^{n+1}$.

The first four algorithms are used for normal ciphertexts and secret keys in the real system, while the remaining are only used for semifunctional ones in the security proof. We use SampG_0 to indicate the first element of $\overrightarrow{g}$, that is, g_0.

Correctness. It needs to meet the following conditions.

(Projective). For $h \in \mathbb{H}$ and a random variable s, $\mathsf{SampGT}(\mu(h); s) = e(\mathsf{SampG}_0(\mathsf{pp}; s), h)$.

(Associative). For all $\overrightarrow{g} \leftarrow \mathsf{SampG}(\mathsf{pp})$ and $\overrightarrow{h} \leftarrow \mathsf{SampH}(\mathsf{pp})$,

$$e(g_0, h_i) = e(g_i, h_0), \quad i = 1, \ldots, n. \tag{6}$$

Security. It needs to meet the following conditions.

(Orthogonality)

(i) $\mu(\widehat{h}^*) = \mu(\widetilde{h}^*) = 1$.

(ii) $e(\widehat{g}_0, \widetilde{h}^*) = 1$.

(iii) $e(\widetilde{g}_0, \widehat{h}^*) = 1$.

(Nondegeneracy). For all $\widehat{g}_0 \leftarrow \widehat{\mathsf{SampG}}_0(\mathsf{pp}, \mathsf{sp})$ and $\widetilde{g}_0 \leftarrow \widetilde{\mathsf{SampG}}_0(\mathsf{pp}, \mathsf{sp})$, $e(\widehat{g}_0, \widehat{h}^*)$ and $e(\widetilde{g}_0, \widetilde{h}^*)$ are distributed uniformly over $\mathbb{G}_T$.

($\mathbb{H}$-Subgroup). The output of $\mathsf{SampH}(\mathsf{pp})$ is distributed uniformly over a subgroup of $\mathbb{H}^{n+1}$.

(Left Subgroup Indistinguishability). For any PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in λ:

$$\begin{aligned}\mathsf{Adv}^{\mathrm{LS}}_{\mathcal{A}}(\lambda) \coloneqq \Bigg| &\Pr\left[\mathcal{A}\left(\mathsf{pp}, \boxed{\overrightarrow{g}}\right) = 1\right] \\ &- \Pr\left[\mathcal{A}\left(\mathsf{pp}, \boxed{\overrightarrow{g} \cdot \overrightarrow{\widehat{g}} \cdot \overrightarrow{\widetilde{g}}}\right) = 1\right]\Bigg|,\end{aligned} \tag{7}$$

where

$$\begin{aligned}(\mathsf{pp}, \mathsf{sp}) &\longleftarrow \mathsf{SampP}\left(1^\lambda, 1^n\right); \\ \overrightarrow{g} &\longleftarrow \mathsf{SampP}(\mathsf{pp}); \\ \overrightarrow{\widehat{g}} &\longleftarrow \widehat{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp}); \\ \overrightarrow{\widetilde{g}} &\longleftarrow \widetilde{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp}).\end{aligned} \tag{8}$$

(Right Subgroup Indistinguishability 1). For any PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in λ:

$$\begin{aligned}\mathsf{Adv}^{\mathrm{RSI}}_{\mathcal{A}}(\lambda) \coloneqq \Bigg| &\Pr\left[\mathcal{A}\left(\mathsf{pp}, \overrightarrow{g} \cdot \overrightarrow{\widehat{g}}, \overrightarrow{\widetilde{g}}, \boxed{\overrightarrow{h}}\right) = 1\right] \\ &- \Pr\left[\mathcal{A}\left(\mathsf{pp}, \overrightarrow{g} \cdot \overrightarrow{\widehat{g}}, \overrightarrow{\widetilde{g}}, \boxed{\overrightarrow{h} \cdot \overrightarrow{\widehat{h}}}\right) = 1\right]\Bigg|,\end{aligned} \tag{9}$$

where

$$\begin{aligned}(\mathsf{pp}, \mathsf{sp}) &\longleftarrow \mathsf{SampP}\left(1^\lambda, 1^n\right); \\ \overrightarrow{g} &\longleftarrow \mathsf{SampP}(\mathsf{pp}); \\ \overrightarrow{\widehat{g}} &\longleftarrow \widehat{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp}); \\ \overrightarrow{\widetilde{g}} &\longleftarrow \widetilde{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp}); \\ \overrightarrow{h} &\longleftarrow \mathsf{SampH}(\mathsf{pp}); \\ \overrightarrow{\widehat{h}} &\longleftarrow \widehat{\mathsf{SampH}}(\mathsf{pp}, \mathsf{sp}).\end{aligned} \tag{10}$$

(Right Subgroup Indistinguishability 2). For any PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in λ:

$$\begin{aligned}\mathsf{Adv}_{\mathcal{A}}^{\mathrm{RS2}}(\lambda) \coloneqq \Bigg| &\Pr\left[\mathcal{A}\left(\mathsf{pp}, \overrightarrow{g}, \widehat{\overrightarrow{g}}\cdot\widetilde{\overrightarrow{g}}, \boxed{\overrightarrow{h}\cdot\widehat{\overrightarrow{h}}}\right) = 1\right] \\ &- \Pr\left[\mathcal{A}\left(\mathsf{pp}, \overrightarrow{g}, \widehat{\overrightarrow{g}}\cdot\widetilde{\overrightarrow{g}}, \boxed{\overrightarrow{h}\cdot\widetilde{\overrightarrow{h}}}\right) = 1\right]\Bigg|,\end{aligned} \tag{11}$$

where

$$\begin{aligned}(\mathsf{pp}, \mathsf{sp}) &\longleftarrow \mathsf{SampP}\left(1^{\lambda}, 1^{n}\right);\\ \overrightarrow{g} &\longleftarrow \mathsf{SampP}(\mathsf{pp});\\ \widehat{\overrightarrow{g}} &\longleftarrow \widehat{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp});\\ \widetilde{\overrightarrow{g}} &\longleftarrow \widetilde{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp});\\ \overrightarrow{h} &\longleftarrow \mathsf{SampH}(\mathsf{pp});\\ \widehat{\overrightarrow{h}} &\longleftarrow \widehat{\mathsf{SampH}}(\mathsf{pp}, \mathsf{sp});\\ \widetilde{\overrightarrow{h}} &\longleftarrow \widetilde{\mathsf{SampH}}(\mathsf{pp}, \mathsf{sp}).\end{aligned} \tag{12}$$

(Parameter Hiding). The following two distributions are identical:

$$\begin{aligned}&\left\{\mathsf{pp}, \boxed{\widehat{\overrightarrow{g}}\cdot\widetilde{\overrightarrow{g}}, \widehat{\overrightarrow{h}}\cdot\widetilde{\overrightarrow{h}}}\right\},\\ &\left\{\mathsf{pp}, \boxed{\widehat{\overrightarrow{g}}\cdot\widehat{\overrightarrow{g}}'\cdot\widetilde{\overrightarrow{g}}\cdot\widetilde{\overrightarrow{g}}', \widehat{\overrightarrow{h}}\cdot\widehat{\overrightarrow{h}}'\cdot\widetilde{\overrightarrow{h}}\cdot\widetilde{\overrightarrow{h}}'}\right\},\end{aligned} \tag{13}$$

where

$$\begin{aligned}(\mathsf{pp}, \mathsf{sp}) &\longleftarrow \mathsf{SampP}\left(1^{\lambda}, 1^{n+l}\right);\\ \widehat{\overrightarrow{g}} &= \left(\widehat{g}_0, \ldots\right) \longleftarrow \widehat{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp});\\ \widehat{\overrightarrow{h}} &= \left(\widehat{h}_0, \ldots\right) \longleftarrow \widehat{\mathsf{SampH}}(\mathsf{pp}, \mathsf{sp});\\ \widetilde{\overrightarrow{g}} &= \left(\widetilde{g}_0, \ldots\right) \longleftarrow \widetilde{\mathsf{SampG}}(\mathsf{pp}, \mathsf{sp});\\ \widetilde{\overrightarrow{h}} &= \left(\widetilde{h}_0, \ldots\right) \longleftarrow \widetilde{\mathsf{SampH}}(\mathsf{pp}, \mathsf{sp});\\ \widehat{\overrightarrow{g}}' &= \left(1, \widehat{g}_0^{\widehat{u}_1}, \ldots, \widehat{g}_0^{\widehat{u}_n}\right);\\ \widehat{\overrightarrow{h}}' &= \left(1, \widehat{h}_0^{\widehat{u}_1}, \ldots, \widehat{h}_0^{\widehat{u}_n}\right),\\ &\qquad \widehat{u}_1, \ldots, \widehat{u}_n \longleftarrow_R \mathbb{Z}_p;\\ \widetilde{\overrightarrow{g}}' &= \left(1, \widetilde{g}_0^{\widetilde{u}_1}, \ldots, \widetilde{g}_0^{\widetilde{u}_n}\right);\\ \widetilde{\overrightarrow{h}}' &= \left(1, \widetilde{h}_0^{\widetilde{u}_1}, \ldots, \widetilde{h}_0^{\widetilde{u}_n}\right),\\ &\qquad \widetilde{u}_1, \ldots, \widetilde{u}_n \longleftarrow_R \mathbb{Z}_p.\end{aligned} \tag{14}$$

5. Instantiating EDSG

We let $\pi_L(\cdot), \pi_M(\cdot)$ and $\pi_R(\cdot)$ be functions mapping from a $3k\times 3k$ matrix to its left-most k columns, the middle k columns, and the right-most k columns, respectively.

$\mathsf{SampP}(1^{\lambda}, 1^{n})$

(i) Run $(p, G_1, G_2, G_T, g_1, g_2, e) \leftarrow \mathcal{G}(1^{\lambda})$.

(ii) Define $(\mathbb{G}, \mathbb{H}, \mathbb{G}_T, e) \coloneqq (G_1^{3k}, G_2^{3k}, G_T, e)$.

(iii) Sample $\mathbf{B} \leftarrow_R \mathrm{GL}_{3k}(\mathbb{Z}_p)$, and set $\mathbf{B}^* \coloneqq (\mathbf{B}^{-1})^{\top}$, $\mathbf{Y}_1, \ldots, \mathbf{Y}_n \leftarrow_R \mathbb{Z}_p^{3k\times 3k}$; $\mathbf{R}$ is a random full-rank diagonal matrix in $\mathbb{Z}_p^{3k}$ whose bottom-right entry is a $2k$-dimensional unit matrix; define

$$\begin{aligned}\mathbf{D} &\coloneqq \pi_L(\mathbf{B}),\\ \mathbf{D}_i &\coloneqq \mathbf{Y}_i^{\top}\pi_L(\mathbf{B}),\\ \mathbf{E} &\coloneqq \pi_M(\mathbf{B}),\\ \mathbf{E}_i &\coloneqq \mathbf{Y}_i^{\top}\pi_M(\mathbf{B}),\\ \mathbf{F} &\coloneqq \pi_R(\mathbf{B}),\\ \mathbf{F}_i &\coloneqq \mathbf{Y}_i^{\top}\pi_R(\mathbf{B}),\\ \mathbf{D}^* &\coloneqq \pi_L(\mathbf{B}^*\mathbf{R}),\\ \mathbf{D}_i^* &\coloneqq \mathbf{Y}_i\pi_L(\mathbf{B}^*\mathbf{R}),\\ \mathbf{E}^* &\coloneqq \pi_M(\mathbf{B}^*\mathbf{R}),\\ \mathbf{E}_i^* &\coloneqq \mathbf{Y}_i\pi_M(\mathbf{B}^*\mathbf{R}),\\ \mathbf{F}^* &\coloneqq \pi_R(\mathbf{B}^*\mathbf{R}),\\ \mathbf{F}_i^* &\coloneqq \mathbf{Y}_i\pi_R(\mathbf{B}^*\mathbf{R}).\end{aligned} \tag{15}$$

(iv) define $\mu([\overrightarrow{k}]_2) = [\mathbf{D}^{\top}\overrightarrow{k}]_T$ for all $\overrightarrow{k} \in \mathbb{Z}_p^{3k}$.

Output

$$\begin{aligned}\mathsf{pp} \coloneqq \Bigg(&(p, \mathbb{G}, \mathbb{H}, \mathbb{G}_T, e),\\ &[\mathbf{D}]_1, [\mathbf{Y}_1^{\top}\mathbf{D}]_1, \ldots, [\mathbf{Y}_n^{\top}\mathbf{D}]_1\\ &[\mathbf{D}^*]_2, [\mathbf{Y}_1\mathbf{D}^*]_2, \ldots, [\mathbf{Y}_n\mathbf{D}^*]_2\Bigg).\end{aligned} \tag{16}$$

$\mathsf{SampGT}([\overrightarrow{p}]_T)$. Pick $\overrightarrow{s} \leftarrow \mathbb{Z}_p^k$ and output $[\overrightarrow{s}^{\top}\overrightarrow{p}]_T \in G_T$.

$\mathsf{SampG}(\mathsf{pp})$. Pick $\overrightarrow{s} \leftarrow \mathbb{Z}_p^k$ and output

$$\left(\left[\mathbf{D}\overrightarrow{s}\right]_1, \left[\mathbf{Y}_1^{\top}\mathbf{D}\overrightarrow{s}\right]_1, \ldots, \left[\mathbf{Y}_n^{\top}\mathbf{D}\overrightarrow{s}\right]_1\right) \in \left(G_1^{3k}\right)^{n+1}. \tag{17}$$

$\mathsf{SampH}(\mathsf{pp})$. Pick $\overrightarrow{r} \leftarrow \mathbb{Z}_p^k$ and output

$$\left(\left[\mathbf{D}^*\overrightarrow{r}\right]_2, \left[\mathbf{Y}_1\mathbf{D}^*\overrightarrow{r}\right]_2, \ldots, \left[\mathbf{Y}_n\mathbf{D}^*\overrightarrow{r}\right]_2\right) \in \left(G_2^{3k}\right)^{n+1}. \tag{18}$$

$\widehat{\mathsf{SampG}}(\mathsf{pp},\mathsf{sp})$. Pick $\widehat{\vec{s}} \leftarrow \mathbb{Z}_p^k$ and output

$$\left(\left[\mathbf{E}\widehat{\vec{s}}\right]_1, \left[\mathbf{Y}_1^\top \mathbf{E}\widehat{\vec{s}}\right]_1, \ldots, \left[\mathbf{Y}_n^\top \mathbf{E}\widehat{\vec{s}}\right]_1\right) \in \left(G_1^{3k}\right)^{n+1}. \quad (19)$$

$\widehat{\mathsf{SampH}}(\mathsf{pp},\mathsf{sp})$. Pick $\widehat{\vec{r}} \leftarrow \mathbb{Z}_p^k$ and output

$$\left(\left[\mathbf{E}^*\widehat{\vec{r}}\right]_2, \left[\mathbf{Y}_1\mathbf{E}^*\widehat{\vec{r}}\right]_2, \ldots, \left[\mathbf{Y}_n\mathbf{E}^*\widehat{\vec{r}}\right]_2\right) \in \left(G_2^{3k}\right)^{n+1}. \quad (20)$$

$\widetilde{\mathsf{SampG}}(\mathsf{pp},\mathsf{sp})$. Pick $\widetilde{\vec{s}} \leftarrow \mathbb{Z}_p^k$ and output

$$\left(\left[\mathbf{F}\widetilde{\vec{s}}\right]_1, \left[\mathbf{Y}_1^\top \mathbf{F}\widetilde{\vec{s}}\right]_1, \ldots, \left[\mathbf{Y}_n^\top \mathbf{F}\widetilde{\vec{s}}\right]_1\right) \in \left(G_1^{3k}\right)^{n+1}. \quad (21)$$

$\widetilde{\mathsf{SampH}}(\mathsf{pp},\mathsf{sp})$. Pick $\widetilde{\vec{r}} \leftarrow \mathbb{Z}_p^k$ and output

$$\left(\left[\mathbf{F}^*\widetilde{\vec{r}}\right]_2, \left[\mathbf{Y}_1\mathbf{F}^*\widetilde{\vec{r}}\right]_2, \ldots, \left[\mathbf{Y}_n\mathbf{F}^*\widetilde{\vec{r}}\right]_2\right) \in \left(G_2^{3k}\right)^{n+1}. \quad (22)$$

Set $\widehat{h}^* := [\mathbf{E}^*\widehat{\vec{r}}]_2, \widetilde{h}^* := [\mathbf{F}^*\widetilde{\vec{r}}]_2$.

Correctness. We check correctness properties as follows.

(Projective). For all $\vec{k} \in \mathbb{Z}_p^{3k}, \vec{s} \in \mathbb{Z}_p^k$:

$$\begin{aligned}\mathsf{SampGT}\left(\mu\left(\left[\vec{k}\right]_2\right); \vec{s}\right) &= \left[\vec{s}^\top \mathbf{D}^\top \vec{k}\right]_T \\ &= \left[\left(\mathbf{D}\vec{s}\right)^\top \vec{k}\right]_T = e\left(\mathsf{SampG}_0\left(\mathsf{pp}; \vec{s}\right), \left[\vec{k}\right]_2\right).\end{aligned} \quad (23)$$

(Associative). For all $\vec{s} \in \mathbb{Z}_p^k, \vec{r} \in \mathbb{Z}_p^k, \mathbf{W}_i \in \mathbb{Z}_p^{3k\times 3k}$:

$$\begin{aligned}e\left(g_0, h_i\right) &= \left(\mathbf{D}\vec{s}\right)^\top \left(\mathbf{Y}_i\mathbf{D}^*\vec{r}\right) = \left(\mathbf{Y}_i^\top \mathbf{D}\vec{s}\right)^\top \left(\mathbf{D}^*\vec{r}\right) \\ &= e\left(g_i, h_0\right), \quad i = 1, \ldots, n.\end{aligned} \quad (24)$$

Security. We check the following security properties.

(Orthogonality)

(i) $\mu(\widehat{h}^*) = \mu(\widetilde{h}^*) = (1, \ldots, 1)^\top \in G_T^k$.

(ii) $e([\mathbf{E}\widehat{\vec{s}}]_1, [\mathbf{F}^*\widetilde{\vec{r}}]_2) = 1_{G_T}$.

(iii) $e([\mathbf{F}\widetilde{\vec{s}}]_1, [\mathbf{E}^*\widehat{\vec{r}}]_2) = 1_{G_T}$.

(Nondegeneracy)

(i) $e([\mathbf{E}\widehat{\vec{s}}]_1, [\mathbf{E}^*\widehat{\vec{r}}]_2) = e(g_1, g_2)^{\widehat{\vec{s}}^\top \widehat{\vec{r}}}$.

(ii) $e([\mathbf{F}\widetilde{\vec{s}}]_1, [\mathbf{F}^*\widetilde{\vec{r}}]_2) = e(g_1, g_2)^{\widetilde{\vec{s}}^\top \widetilde{\vec{r}}}$.

With overwhelming probability, the inner product $\widehat{\vec{s}}^\top \widehat{\vec{r}}$ is distributed uniformly over $\mathbb{Z}_p$ and therefore $e([\mathbf{E}\widehat{\vec{s}}]_1, [\mathbf{E}^*\widehat{\vec{r}}]_2)$ is distributed uniformly over G_T, and the same is true for $e([\mathbf{F}\widetilde{\vec{s}}]_1, [\mathbf{F}^*\widetilde{\vec{r}}]_2)$.

(ℍ-Subgroup). This follows from the fact that $\mathbb{Z}_p^{3k}$ is an additive group.

Lemma 5 (left subgroup indistinguishability). *For any PPT adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}_{\mathcal{A}}^{LS}(\lambda) \leqslant \mathsf{Adv}_{\mathcal{B}}^{(k,2k)\text{-}LLin}. \quad (25)$$

We may rewrite the LS advantage function as follows:

$$\begin{aligned}\mathsf{Adv}_{\mathcal{A}}^{\mathrm{LS}}(\lambda) := \Bigg|&\Pr\left[\mathcal{A}\left(\mathsf{pp}, \boxed{\vec{g}}\right) = 1\right] \\ &- \Pr\left[\mathcal{A}\left(\mathsf{pp}, \boxed{\vec{g}\cdot\widehat{\vec{g}}\cdot\widetilde{\vec{g}}}\right) = 1\right]\Bigg|,\end{aligned} \quad (26)$$

where

$$(\mathsf{pp},\mathsf{sp}) \longleftarrow \mathsf{SampP}\left(1^\lambda, 1^n\right);$$

$$\vec{s}, \widehat{\vec{s}}, \widetilde{\vec{s}} \longleftarrow_R \mathbb{Z}_p^k;$$

$$\begin{aligned}\vec{g} := \Bigg(&\left[\mathbf{B}\begin{pmatrix}\vec{s}\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1, \left[\mathbf{Y}_1^\top\mathbf{B}\begin{pmatrix}\vec{s}\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1, \ldots, \\ &\left[\mathbf{Y}_n^\top\mathbf{B}\begin{pmatrix}\vec{s}\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1\Bigg);\end{aligned} \quad (27)$$

$$\begin{aligned}\vec{g}\cdot\widehat{\vec{g}}\cdot\widetilde{\vec{g}} := \Bigg(&\left[\mathbf{B}\begin{pmatrix}\vec{s}\\ \widehat{\vec{s}}\\ \widetilde{\vec{s}}\end{pmatrix}\right]_1, \left[\mathbf{Y}_1^\top\mathbf{B}\begin{pmatrix}\vec{s}\\ \widehat{\vec{s}}\\ \widetilde{\vec{s}}\end{pmatrix}\right]_1, \ldots, \\ &\left[\mathbf{Y}_n^\top\mathbf{B}\begin{pmatrix}\vec{s}\\ \widehat{\vec{s}}\\ \widetilde{\vec{s}}\end{pmatrix}\right]_1\Bigg).\end{aligned}$$

Proof. Given an instance of $(k, 2k)$-LLin problem (i.e., $\ell = 2k$)

$$\begin{aligned}\Big(&g_1, g_2, g_1^{a_1}, \ldots, g_1^{a_k}, \left\{g_1^{b_{i,j}}\right\}_{i\in[2k], j\in[k]}, g_1^{a_1 s_1}, \ldots, g_k^{a_k s_k}, \\ &\left\{g_1^{b_{i,1}s_1+\cdots+b_{i,k}s_k+s_{k+i}}\right\}_{i\in[2k]}\Big)\end{aligned} \quad (28)$$

as input, where all s_{k+i} are either 0 or uniformly chosen from $\mathbb{Z}_p^*$. $\mathcal{B}$ implicitly sets

$$\begin{aligned}\vec{s} &= \left(s_1, \ldots, s_k\right)^\top, \\ \widehat{\vec{s}} &= \left(s_{k+1}, \ldots, s_{2k}\right)^\top, \\ \widetilde{\vec{s}} &= \left(s_{2k+1,}, \ldots, s_{3k}\right)^\top.\end{aligned} \quad (29)$$

Define $\mathbf{W} \in \mathbb{Z}_p^{3k\times 3k}$ as

$$\mathbf{W} \coloneqq \left(\begin{array}{ccc|c|c} a_1 & & & & \\ & \ddots & & & \\ & & a_k & & \\ \hline b_{1,1} & \cdots & b_{1,k} & 1 & \\ \vdots & & \vdots & & \ddots \\ b_{k,1} & \cdots & b_{k,k} & & 1 \\ \hline b_{k+1,1} & \cdots & b_{k+1,k} & & \\ \vdots & & \vdots & & \\ b_{2k,1} & \cdots & b_{2k,k} & & \end{array}\right), \tag{30}$$

$$\mathbf{W}^* \coloneqq \left(\mathbf{W}^{-1}\right)^{\top} \coloneqq \left(\begin{array}{ccc|ccc|ccc} a_1^{-1} & & & -a_1^{-1}b_{1,1} & \cdots & -a_1^{-1}b_{k,1} & -a_1^{-1}b_{k+1,1} & \cdots & -a_1^{-1}b_{2k,1} \\ & \ddots & & \vdots & & \vdots & \vdots & & \vdots \\ & & a_k^{-1} & -a_k^{-1}b_{1,k} & \cdots & -a_k^{-1}b_{k,k} & -a_k^{-1}b_{k+1,k} & \cdots & -a_k^{-1}b_{2k,k} \\ \hline & & & 1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & 1 & & & \\ \hline & & & & & & 1 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 1 \end{array}\right).$$

Sample $\overline{\mathbf{B}} \leftarrow \mathsf{GL}_{3k}(\mathbb{Z}_p)$, $\mathbf{Y}_1, \ldots, \mathbf{Y}_n \leftarrow \mathbb{Z}_p^{3k\times 3k}$, $\overline{r}_1, \ldots, \overline{r}_k \leftarrow \mathbb{Z}_p^*$, set $\overline{\mathbf{B}}^* \coloneqq (\overline{\mathbf{B}}^{-1})^{\top}$, and implicitly set

$$\left(\mathbf{B}, \mathbf{B}^*\right) \coloneqq \left(\overline{\mathbf{B}}\mathbf{W}, \overline{\mathbf{B}}^*\mathbf{W}^*\right)$$

$$\mathbf{R} \coloneqq \left(\begin{array}{ccc|c|c} a_1\overline{r}_1 & & & & \\ & \ddots & & & \\ & & a_k\overline{r}_k & & \\ \hline & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \\ \hline & & & & & 1 \\ & & & & & & \ddots \\ & & & & & & & 1 \end{array}\right). \tag{31}$$

Then we can compute

$$\pi_L\left(\mathbf{W}^*\mathbf{R}\right) \coloneqq \left(\begin{array}{ccc} \overline{r}_1 & & \\ & \ddots & \\ & & \overline{r}_k \\ \hline & \overrightarrow{0}^{2k\times k} & \end{array}\right). \tag{32}$$

Simulating pp

$$\begin{aligned} \left[\pi_L(\mathbf{B})\right]_1 &= \left[\overline{\mathbf{B}}\pi_L(\mathbf{W})\right]_1, \\ \left[\mathbf{Y}_i^{\top}\pi_L(\mathbf{B})\right]_1 &= \left[\mathbf{Y}_i^{\top}\overline{\mathbf{B}}\pi_L(\mathbf{W})\right]_1, \\ \left[\pi_L(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\overline{\mathbf{B}}^*\pi_L(\mathbf{W}^*\mathbf{R})\right]_2, \\ \left[\mathbf{Y}_i\pi_L(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}^*\pi_L(\mathbf{W}^*\mathbf{R})\right]_2. \end{aligned} \tag{33}$$

Simulating the Challenge. $\mathscr{B}$ simulates the challenge as

$$\left[\mathbf{B}\begin{pmatrix}\overrightarrow{s}\\ \overrightarrow{\hat{s}}\\ \overrightarrow{\tilde{s}}\end{pmatrix}\right]_1 = \left[\overline{\mathbf{B}}\mathbf{W}\begin{pmatrix}\overrightarrow{s}\\ \overrightarrow{\hat{s}}\\ \overrightarrow{\tilde{s}}\end{pmatrix}\right]_1,$$

$$\left[\mathbf{Y}_i^{\top}\mathbf{B}\begin{pmatrix}\overrightarrow{s}\\ \overrightarrow{\hat{s}}\\ \overrightarrow{\tilde{s}}\end{pmatrix}\right]_1 = \left[\mathbf{Y}_i^{\top}\overline{\mathbf{B}}\mathbf{W}\begin{pmatrix}\overrightarrow{s}\\ \overrightarrow{\hat{s}}\\ \overrightarrow{\tilde{s}}\end{pmatrix}\right]_1,$$

$$\mathbf{W}\begin{pmatrix}\overrightarrow{s}\\ \widehat{\overrightarrow{s}}\\ \widetilde{\overrightarrow{s}}\end{pmatrix}=\begin{pmatrix}a_1s_1\\ \vdots\\ a_ks_k\\ b_{1,1}s_1+\cdots+b_{1,k}s_k+s_{k+1}\\ \vdots\\ b_{2k,1}s_1+\cdots+b_{2k,k}s_k+s_{3k}\end{pmatrix}. \tag{34}$$

If $s_{k+i}=0$, $i=1,\ldots,2k$, that is, $\widehat{\overrightarrow{s}}=\widetilde{\overrightarrow{s}}=\overrightarrow{0}$, the output is $\overrightarrow{g}$; otherwise, the output is $\overrightarrow{g}\cdot\widehat{\overrightarrow{g}}\cdot\widetilde{\overrightarrow{g}}$. □

Lemma 6 (right subgroup indistinguishability 1). *For any PPT adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}^{RS1}_{\mathcal{A}}(\lambda)\leqslant\mathsf{Adv}^{(k,k)\text{-}LLin}_{\mathcal{B}}. \tag{35}$$

We may rewrite the RS1 advantage function as follows:

$$\begin{aligned}\mathsf{Adv}^{\mathrm{RS1}}_{\mathcal{A}}(\lambda)\coloneqq&\left|\Pr\left[\mathcal{A}\left(\mathsf{pp},\overrightarrow{g}\cdot\widehat{\overrightarrow{g}},\widetilde{\overrightarrow{g}},\boxed{\overrightarrow{h}}\right)=1\right]\right.\\&\left.-\Pr\left[\mathcal{A}\left(\mathsf{pp},\overrightarrow{g}\cdot\widehat{\overrightarrow{g}},\widetilde{\overrightarrow{g}},\boxed{\overrightarrow{h}\cdot\widehat{\overrightarrow{h}}}\right)=1\right]\right|,\end{aligned} \tag{36}$$

where

$$(\mathsf{pp},\mathsf{sp})\longleftarrow\mathsf{SampP}\left(1^{\lambda},1^{n}\right);$$

$$\overrightarrow{s},\widehat{\overrightarrow{s}},\widetilde{\overrightarrow{s}},\overrightarrow{r},\widehat{\overrightarrow{r}}\longleftarrow_R\mathbb{Z}_p^k;$$

$$\overrightarrow{g}\cdot\widehat{\overrightarrow{g}}\coloneqq\left(\left[\mathbf{B}\begin{pmatrix}\overrightarrow{s}\\ \widehat{\overrightarrow{s}}\\ \overrightarrow{0}\end{pmatrix}\right]_1,\left[\mathbf{Y}_1^{\top}\mathbf{B}\begin{pmatrix}\overrightarrow{s}\\ \widehat{\overrightarrow{s}}\\ \overrightarrow{0}\end{pmatrix}\right]_1,\ldots,\left[\mathbf{Y}_n^{\top}\mathbf{B}\begin{pmatrix}\overrightarrow{s}\\ \widehat{\overrightarrow{s}}\\ \overrightarrow{0}\end{pmatrix}\right]_1\right);$$

$$\widetilde{\overrightarrow{g}}\coloneqq\left(\left[\mathbf{B}\begin{pmatrix}\overrightarrow{0}\\ \overrightarrow{0}\\ \widetilde{\overrightarrow{s}}\end{pmatrix}\right]_1,\left[\mathbf{Y}_1^{\top}\mathbf{B}\begin{pmatrix}\overrightarrow{0}\\ \overrightarrow{0}\\ \widetilde{\overrightarrow{s}}\end{pmatrix}\right]_1,\ldots,\left[\mathbf{Y}_n^{\top}\mathbf{B}\begin{pmatrix}\overrightarrow{0}\\ \overrightarrow{0}\\ \widetilde{\overrightarrow{s}}\end{pmatrix}\right]_1\right);$$

$$\overrightarrow{h}\coloneqq\left(\left[\mathbf{B}^*\mathbf{R}\begin{pmatrix}\overrightarrow{r}\\ \overrightarrow{0}\\ \overrightarrow{0}\end{pmatrix}\right]_2,\left[\mathbf{Y}_1\mathbf{B}^*\mathbf{R}\begin{pmatrix}\overrightarrow{r}\\ \overrightarrow{0}\\ \overrightarrow{0}\end{pmatrix}\right]_2,\ldots,\left[\mathbf{Y}_n\mathbf{B}^*\mathbf{R}\begin{pmatrix}\overrightarrow{r}\\ \overrightarrow{0}\\ \overrightarrow{0}\end{pmatrix}\right]_2\right);$$

$$\overrightarrow{h}\cdot\widehat{\overrightarrow{h}}\coloneqq\left(\left[\mathbf{B}^*\mathbf{R}\begin{pmatrix}\overrightarrow{r}\\ \widehat{\overrightarrow{r}}\\ \overrightarrow{0}\end{pmatrix}\right]_2,\left[\mathbf{Y}_1\mathbf{B}^*\mathbf{R}\begin{pmatrix}\overrightarrow{r}\\ \widehat{\overrightarrow{r}}\\ \overrightarrow{0}\end{pmatrix}\right]_2,\ldots,\left[\mathbf{Y}_n\mathbf{B}^*\mathbf{R}\begin{pmatrix}\overrightarrow{r}\\ \widehat{\overrightarrow{r}}\\ \overrightarrow{0}\end{pmatrix}\right]_2\right). \tag{37}$$

Proof. Given an instance of (k,k)-LLin problem (i.e., $\ell=k$)

$$\left(g_1,g_2,g_2^{a_1},\ldots,g_2^{a_k},\left\{g_2^{b_{i,j}}\right\}_{i,j\in[k]},g_2^{a_1r_1},\ldots,g_2^{a_kr_k},\left\{g_2^{b_{i,1}r_1+\cdots+b_{i,k}r_k+s_{k+i}}\right\}_{i\in[k]}\right) \tag{38}$$

as input, where all s_{k+i} are either 0 or uniformly chosen from $\mathbb{Z}_p^*$. $\mathcal{B}$ samples $\bar{r}_1,\ldots,\bar{r}_k\leftarrow\mathbb{Z}_p^*$ and implicitly sets

$$\begin{aligned}\overrightarrow{r}&=\left(\bar{r}_1^{-1}r_1,\ldots,\bar{r}_k^{-1}r_k\right)^{\top},\\ \widehat{\overrightarrow{r}}&=\left(r_{k+1},\ldots,r_{2k}\right)^{\top}.\end{aligned} \tag{39}$$

Define $\mathbf{W}^*\in\mathbb{Z}_p^{3k\times3k}$ as

$$\mathbf{W}^*\coloneqq\left(\begin{array}{ccc|ccc|ccc}1&&&&&&&&\\&\ddots&&&&&&&\\&&1&&&&&&\\\hline a_1^{-1}b_{1,1}&\cdots&a_k^{-1}b_{1,k}&1&&&&&\\\vdots&&\vdots&&\ddots&&&&\\a_1^{-1}b_{k,1}&\cdots&a_k^{-1}b_{k,k}&&&1&&&\\\hline&&&&&&1&&\\&&&&&&&\ddots&\\&&&&&&&&1\end{array}\right),$$

$$\mathbf{W}^{-1}\coloneqq\left(\begin{array}{ccc|ccc|ccc}1&&&a_1^{-1}b_{1,1}&\cdots&a_1^{-1}b_{k,1}&&&\\&\ddots&&\vdots&&\vdots&&&\\&&1&a_k^{-1}b_{1,k}&\cdots&a_k^{-1}b_{k,k}&&&\\\hline&&&1&&&&&\\&&&&\ddots&&&&\\&&&&&1&&&\\\hline&&&&&&1&&\\&&&&&&&\ddots&\\&&&&&&&&1\end{array}\right),$$

$$\mathbf{W} \coloneqq \left(\begin{array}{ccc|ccc|cc} 1 & & & -a_1^{-1}b_{1,1} & \cdots & -a_1^{-1}b_{k,1} & & \\ & \ddots & & \vdots & & \vdots & & \\ & & 1 & -a_k^{-1}b_{1,k} & \cdots & -a_k^{-1}b_{k,k} & & \\ \hline & & & 1 & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ \hline & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{array}\right). \tag{40}$$

Sample $\overline{\mathbf{B}} \leftarrow \mathsf{GL}_{3k}(\mathbb{Z}_p)$, $\mathbf{Y}_1, \ldots, \mathbf{Y}_n \leftarrow \mathbb{Z}_p^{3k\times 3k}$, set $\overline{\mathbf{B}}^* \coloneqq (\overline{\mathbf{B}}^{-1})^\top$, and implicitly set

$$(\mathbf{B}, \mathbf{B}^*) \coloneqq \left(\overline{\mathbf{B}}\mathbf{W}, \overline{\mathbf{B}}^*\mathbf{W}^*\right),$$

$$\mathbf{R} \coloneqq \left(\begin{array}{ccc|c|c} a_1\overline{r}_1 & & & & \\ & \ddots & & & \\ & & a_k\overline{r}_k & & \\ \hline & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \\ \hline & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{array}\right). \tag{41}$$

Then we can compute

$$\mathbf{W}^*\mathbf{R} \coloneqq \left(\begin{array}{ccc|c|c} a_1\overline{r}_1 & & & & \\ & \ddots & & & \\ & & a_k\overline{r}_k & & \\ \hline b_{1,1}\overline{r}_1 & \cdots & b_{1,k}\overline{r}_k & 1 & \\ \vdots & & \vdots & & \ddots \\ b_{k,1}\overline{r}_1 & \cdots & b_{k,k}\overline{r}_k & & 1 \\ \hline & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \end{array}\right). \tag{42}$$

Simulating pp

$$\begin{aligned} \left[\pi_L(\mathbf{B})\right]_1 &= \left[\overline{\mathbf{B}}\pi_L(\mathbf{W})\right]_1, \\ \left[\mathbf{Y}_i^\top \pi_L(\mathbf{B})\right]_1 &= \left[\mathbf{Y}_i^\top \overline{\mathbf{B}}\pi_L(\mathbf{W})\right]_1, \\ \left[\pi_L(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\overline{\mathbf{B}}^*\pi_L(\mathbf{W}^*\mathbf{R})\right]_2, \\ \left[\mathbf{Y}_i\pi_L(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}^*\pi_L(\mathbf{W}^*\mathbf{R})\right]_2, \\ \left[\pi_R(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\overline{\mathbf{B}}^*\pi_R(\mathbf{W}^*\mathbf{R})\right]_2, \\ \left[\mathbf{Y}_i\pi_R(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}^*\pi_R(\mathbf{W}^*\mathbf{R})\right]_2. \end{aligned} \tag{43}$$

Simulating $\overrightarrow{g}\cdot\widehat{\overrightarrow{g}}, \widetilde{\overrightarrow{g}}$. Sample $\overrightarrow{s}', \widehat{\overrightarrow{s}}', \widetilde{\overrightarrow{s}}' \leftarrow \mathbb{Z}_p^K$ and implicitly set

$$\begin{aligned} \begin{pmatrix} \overrightarrow{s} \\ \widehat{\overrightarrow{s}} \\ \overrightarrow{0} \end{pmatrix} &= \mathbf{W}^{-1}\begin{pmatrix} \overrightarrow{s}' \\ \widehat{\overrightarrow{s}}' \\ \overrightarrow{0} \end{pmatrix}, \\ \begin{pmatrix} \overrightarrow{0} \\ \overrightarrow{0} \\ \widetilde{\overrightarrow{s}} \end{pmatrix} &= \mathbf{W}^{-1}\begin{pmatrix} \overrightarrow{0} \\ \overrightarrow{0} \\ \widetilde{\overrightarrow{s}}' \end{pmatrix}. \end{aligned} \tag{44}$$

Then we can compute

$$\begin{aligned} \left[\mathbf{B}\begin{pmatrix} \overrightarrow{s} \\ \widehat{\overrightarrow{s}} \\ \overrightarrow{0} \end{pmatrix}\right]_1 &= \left[\overline{\mathbf{B}}\begin{pmatrix} \overrightarrow{s}' \\ \widehat{\overrightarrow{s}}' \\ \overrightarrow{0} \end{pmatrix}\right]_1, \\ \left[\mathbf{Y}_i\mathbf{B}\begin{pmatrix} \overrightarrow{s} \\ \widehat{\overrightarrow{s}} \\ \overrightarrow{0} \end{pmatrix}\right]_1 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}\begin{pmatrix} \overrightarrow{s}' \\ \widehat{\overrightarrow{s}}' \\ \overrightarrow{0} \end{pmatrix}\right]_1, \\ \left[\overline{\mathbf{B}}\begin{pmatrix} \overrightarrow{0} \\ \overrightarrow{0} \\ \widetilde{\overrightarrow{s}} \end{pmatrix}\right]_1 &= \left[\overline{\mathbf{B}}\begin{pmatrix} \overrightarrow{0} \\ \overrightarrow{0} \\ \widetilde{\overrightarrow{s}}' \end{pmatrix}\right]_1, \\ \left[\mathbf{Y}_i\mathbf{B}\begin{pmatrix} \overrightarrow{0} \\ \overrightarrow{0} \\ \widetilde{\overrightarrow{s}} \end{pmatrix}\right]_1 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}\begin{pmatrix} \overrightarrow{0} \\ \overrightarrow{0} \\ \widetilde{\overrightarrow{s}}' \end{pmatrix}\right]_1. \end{aligned} \tag{45}$$

Simulating the Challenge. $\mathcal{B}$ simulates the challenge as

$$\left[\mathbf{B}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{0}\end{pmatrix}\right]_1 = \left[\overline{\mathbf{B}}^*\mathbf{W}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{0}\end{pmatrix}\right]_2,$$

$$\left[\mathbf{Y}_i\mathbf{B}^*\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{0}\end{pmatrix}\right]_1 = \left[\mathbf{Y}_i\overline{\mathbf{B}}^*\mathbf{W}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{0}\end{pmatrix}\right]_2, \tag{46}$$

$$\mathbf{W}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{0}\end{pmatrix} = \begin{pmatrix} a_1r_1\\ \vdots\\ a_kr_k\\ b_{1,1}r_1+\cdots+b_{1,k}r_k+r_{k+1}\\ \vdots\\ b_{k,1}r_1+\cdots+b_{k,k}r_k+r_{2k}\\ \vec{0}\end{pmatrix}.$$

If $r_{k+i} = 0, i = 1,\ldots,2k$, that is, $\vec{\hat{r}} = \vec{0}$, the output is $\vec{h}$; otherwise, the output is $\vec{h}\cdot\vec{\hat{h}}$. □

Lemma 7 (right subgroup indistinguishability $2'$). *For any PPT adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}^{RS2'}_{\mathcal{A}}(\lambda) \leqslant \mathsf{Adv}^{(k,k)\text{-}LLin}_{\mathcal{B}}. \tag{47}$$

The RS2′ advantage function:

$$\mathsf{Adv}^{\mathrm{RS2}'}_{\mathcal{A}}(\lambda) := \left|\Pr\left[\mathcal{A}\left(\mathsf{pp}, \vec{g}, \vec{\hat{g}}\cdot\vec{\tilde{g}}, \boxed{\vec{h}\cdot\vec{\hat{h}}}\right)=1\right] - \Pr\left[\mathcal{A}\left(\mathsf{pp}, \vec{g}, \vec{\hat{g}}\cdot\vec{\tilde{g}}, \boxed{\vec{h}\cdot\vec{\hat{h}}\cdot\vec{\tilde{h}}}\right)=1\right]\right|, \tag{48}$$

where

$$(\mathsf{pp},\mathsf{sp}) \longleftarrow \mathsf{SampP}\left(1^\lambda, 1^n\right);$$

$$\vec{s}, \vec{\hat{s}}, \vec{\tilde{s}}, \vec{r}, \vec{\hat{r}}, \vec{\tilde{r}} \longleftarrow_R \mathbb{Z}_p^k;$$

$$\vec{g} := \left(\left[\mathbf{B}\begin{pmatrix}\vec{s}\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1, \left[\mathbf{Y}_1^\top\mathbf{B}\begin{pmatrix}\vec{s}\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1, \ldots, \left[\mathbf{Y}_n^\top\mathbf{B}\begin{pmatrix}\vec{s}\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1\right);$$

$$\vec{\hat{g}}\cdot\vec{\tilde{g}} := \left(\left[\mathbf{B}\begin{pmatrix}\vec{0}\\ \vec{\hat{s}}\\ \vec{\tilde{s}}\end{pmatrix}\right]_1, \left[\mathbf{Y}_1^\top\mathbf{B}\begin{pmatrix}\vec{0}\\ \vec{\hat{s}}\\ \vec{\tilde{s}}\end{pmatrix}\right]_1, \ldots, \left[\mathbf{Y}_n^\top\mathbf{B}\begin{pmatrix}\vec{0}\\ \vec{\hat{s}}\\ \vec{\tilde{s}}\end{pmatrix}\right]_1\right);$$

$$\vec{h}\cdot\vec{\hat{h}} := \left(\left[\mathbf{B}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{0}\end{pmatrix}\right]_2, \left[\mathbf{Y}_1\mathbf{B}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{0}\end{pmatrix}\right]_2, \ldots, \left[\mathbf{Y}_n^\top\mathbf{B}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{0}\end{pmatrix}\right]_2\right);$$

$$\vec{h}\cdot\vec{\hat{h}}\cdot\vec{\tilde{h}} := \left(\left[\mathbf{B}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{\tilde{r}}\end{pmatrix}\right]_2, \left[\mathbf{Y}_1\mathbf{B}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{\tilde{r}}\end{pmatrix}\right]_2, \ldots, \left[\mathbf{Y}_n\mathbf{B}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \vec{\hat{r}}\\ \vec{\tilde{r}}\end{pmatrix}\right]_2\right). \tag{49}$$

Proof. Given an instance of (k,k)-LLin problem (i.e., $\ell = k$)

$$\left(g_1, g_2, g_2^{a_1}, \ldots, g_2^{a_k}, \left\{g_2^{b_{i,j}}\right\}_{i,j\in[k]}, g_2^{a_1r_1}, \ldots, g_2^{a_kr_k}, \left\{g_2^{b_{i,1}r_1+\cdots+b_{i,k}r_k+r_{k+i}}\right\}_{i\in[k]}\right) \tag{50}$$

as input, where all s_{k+i} are either 0 or uniformly chosen from $\mathbb{Z}_p^*$. $\mathcal{B}$ samples $r_1', \ldots, r_k' \leftarrow \mathbb{Z}_p^*$ and implicitly sets

$$\vec{r} = \left(r_1', \ldots, r_k'\right)^\top,$$

$$\vec{\hat{r}} = \left(r_1, \ldots, r_k\right)^\top, \tag{51}$$

$$\vec{\tilde{r}} = \left(r_{k+1}, \ldots, r_{2k}\right)^\top.$$

Define $\mathbf{W}^* \in \mathbb{Z}_p^{3k\times 3k}$ as

$$\mathbf{W}^* \coloneqq \left(\begin{array}{ccc|ccc|c} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ \hline & & & a_1 & & & \\ & & & & \ddots & & \\ & & & & & a_k & \\ \hline & & & b_{1,1} & \cdots & b_{1,k} & 1 \\ & & & \vdots & & \vdots & & \ddots \\ & & & b_{k,1} & \cdots & b_{k,k} & & 1 \end{array}\right),$$

$$\mathbf{W}^{-1} \coloneqq \left(\begin{array}{ccc|ccc|c} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ \hline & & & a_1 & & & b_{1,1} \cdots b_{k,1} \\ & & & & \ddots & & \vdots \quad \vdots \\ & & & & & a_k & b_{1,k} \cdots b_{k,k} \\ \hline & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{array}\right), \tag{52}$$

$\mathbf{W}$

$$\coloneqq \left(\begin{array}{ccc|ccc|c} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ \hline & & & a_1^{-1} & & & -a_1^{-1}b_{1,1} \cdots -a_1^{-1}b_{k,1} \\ & & & & \ddots & & \vdots \quad \vdots \\ & & & & & a_k^{-1} & -a_k^{-1}b_{1,k} \cdots -a_k^{-1}b_{k,k} \\ \hline & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{array}\right).$$

Sample $\overline{\mathbf{B}} \leftarrow \mathsf{GL}_{3k}(\mathbb{Z}_p)$, $\mathbf{Y}_1, \ldots, \mathbf{Y}_n \leftarrow \mathbb{Z}_p^{3k\times 3k}$, set $\overline{\mathbf{B}}^* \coloneqq (\overline{\mathbf{B}}^{-1})^\top$, and implicitly set

$$(\mathbf{B}, \mathbf{B}^*) \coloneqq \left(\overline{\mathbf{B}}\mathbf{W}, \overline{\mathbf{B}}^*\mathbf{W}^*\right),$$

$$\mathbf{R} \coloneqq \left(\begin{array}{ccc|ccc|c} r_{11} & & & & & & \\ & \ddots & & & & & \\ & & r_{kk} & & & & \\ \hline & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ \hline & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{array}\right). \tag{53}$$

Then we can compute

$\mathbf{W}^*\mathbf{R}$

$$\coloneqq \left(\begin{array}{ccc|ccc|c} r_{11} & & & & & & \\ & \ddots & & & & & \\ & & r_{kk} & & & & \\ \hline & & & a_1 & & & \\ & & & & \ddots & & \\ & & & & & a_k & \\ \hline & & & b_{1,1} & \cdots & b_{1,k} & 1 \\ & & & \vdots & & \vdots & & \ddots \\ & & & b_{k,1} & \cdots & b_{k,k} & & 1 \end{array}\right). \tag{54}$$

Simulating pp

$$\begin{aligned} \left[\pi_L(\mathbf{B})\right]_1 &= \left[\overline{\mathbf{B}}\pi_L(\mathbf{W})\right]_1, \\ \left[\mathbf{Y}_i^\top \pi_L(\mathbf{B})\right]_1 &= \left[\mathbf{Y}_i^\top \overline{\mathbf{B}}\pi_L(\mathbf{W})\right]_1, \end{aligned} \tag{55}$$

$$\begin{aligned} \left[\pi_L(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\overline{\mathbf{B}}^*\pi_L(\mathbf{W}^*\mathbf{R})\right]_2, \\ \left[\mathbf{Y}_i\pi_L(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}^*\pi_L(\mathbf{W}^*\mathbf{R})\right]_2, \end{aligned} \tag{56}$$

$$\begin{aligned} \left[\pi_R(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\overline{\mathbf{B}}^*\pi_R(\mathbf{W}^*\mathbf{R})\right]_2, \\ \left[\mathbf{Y}_i\pi_R(\mathbf{B}^*\mathbf{R})\right]_2 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}^*\pi_R(\mathbf{W}^*\mathbf{R})\right]_2. \end{aligned} \tag{57}$$

Simulating $\overrightarrow{g}, \widehat{\overrightarrow{g}} \cdot \widetilde{\overrightarrow{g}}$. Sample $\overrightarrow{s}', \widehat{\overrightarrow{s}}', \widetilde{\overrightarrow{s}}' \leftarrow \mathbb{Z}_p^K$ and implicitly set

$$\begin{aligned} \begin{pmatrix} \overrightarrow{s} \\ \overrightarrow{0} \\ \overrightarrow{0} \end{pmatrix} &= \mathbf{W}^{-1}\begin{pmatrix} \overrightarrow{s}' \\ \overrightarrow{0} \\ \overrightarrow{0} \end{pmatrix}, \\ \begin{pmatrix} \overrightarrow{0} \\ \widehat{\overrightarrow{s}} \\ \widetilde{\overrightarrow{s}} \end{pmatrix} &= \mathbf{W}^{-1}\begin{pmatrix} \overrightarrow{0} \\ \widehat{\overrightarrow{s}}' \\ \widetilde{\overrightarrow{s}}' \end{pmatrix}. \end{aligned} \tag{58}$$

Then we can compute

$$\begin{aligned}
\left[\mathbf{B}\begin{pmatrix}\vec{s}\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1 &= \left[\overline{\mathbf{B}}\begin{pmatrix}\vec{s}'\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1,\\
\left[\mathbf{Y}_i\mathbf{B}\begin{pmatrix}\vec{s}\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}\begin{pmatrix}\vec{s}'\\ \vec{0}\\ \vec{0}\end{pmatrix}\right]_1,\\
\left[\overline{\mathbf{B}}\begin{pmatrix}\vec{0}\\ \widehat{\vec{s}}\\ \widetilde{\vec{s}}\end{pmatrix}\right]_1 &= \left[\overline{\mathbf{B}}\begin{pmatrix}\vec{0}\\ \widehat{\vec{s}}'\\ \widetilde{\vec{s}}'\end{pmatrix}\right]_1,\\
\left[\mathbf{Y}_i\mathbf{B}\begin{pmatrix}\vec{0}\\ \widehat{\vec{s}}\\ \widetilde{\vec{s}}\end{pmatrix}\right]_1 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}\begin{pmatrix}\vec{0}\\ \widehat{\vec{s}}'\\ \widetilde{\vec{s}}'\end{pmatrix}\right]_1.
\end{aligned} \tag{59}$$

Simulating the Challenge. $\mathscr{B}$ simulates the challenge as

$$\begin{aligned}
\left[\mathbf{B}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \widehat{\vec{r}}\\ \widetilde{\vec{r}}\end{pmatrix}\right]_1 &= \left[\overline{\mathbf{B}}^*\mathbf{W}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \widehat{\vec{r}}\\ \widetilde{\vec{r}}\end{pmatrix}\right]_2,\\
\left[\mathbf{Y}_i\mathbf{B}^*\begin{pmatrix}\vec{r}\\ \widehat{\vec{r}}\\ \widetilde{\vec{r}}\end{pmatrix}\right]_1 &= \left[\mathbf{Y}_i\overline{\mathbf{B}}^*\mathbf{W}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \widehat{\vec{r}}\\ \widetilde{\vec{r}}\end{pmatrix}\right]_2,
\end{aligned}$$

$$\mathbf{W}^*\mathbf{R}\begin{pmatrix}\vec{r}\\ \widehat{\vec{r}}\\ \widetilde{\vec{r}}\end{pmatrix} = \begin{pmatrix} r_{11}r_1'\\ \vdots\\ r_{k,k}r_k'\\ a_1r_1\\ \vdots\\ a_kr_k\\ b_{1,1}r_1+\cdots+b_{1,k}r_k+r_{k+1}\\ \vdots\\ b_{k,1}r_1+\cdots+b_{k,k}r_k+r_{2k}\end{pmatrix}. \tag{60}$$

If $r_{k+i}=0$, $i=1,\ldots,2k$, that is, $\widetilde{\vec{r}}=\vec{0}$, the output is $\vec{h}\cdot\widehat{\vec{h}}$; otherwise, the output is $\vec{h}\cdot\widehat{\vec{h}}\cdot\widetilde{\vec{h}}$. □

Similarly, we can proof

$$\begin{aligned}
&\left|\Pr\left[\mathscr{A}\left(\mathsf{pp},\vec{g},\widehat{\vec{g}}\cdot\widetilde{\vec{g}},\boxed{\vec{h}\cdot\widetilde{\vec{h}}}\right)=1\right]\right.\\
&\left.-\Pr\left[\mathscr{A}\left(\mathsf{pp},\vec{g},\widehat{\vec{g}}\cdot\widetilde{\vec{g}},\boxed{\vec{h}\cdot\widehat{\vec{h}}\cdot\widetilde{\vec{h}}}\right)=1\right]\right|\\
&\leqslant \mathsf{Adv}^{(k,k)\text{-LLin}}_{\mathscr{B}}.
\end{aligned} \tag{61}$$

Hence, right subgroup indistinguishability 2 is true.

Lemma 8 (parameter hiding). *The following are identically distributed:*

$$\left\{\mathsf{pp},\begin{matrix}\left[\pi_M(\mathbf{B})\widehat{\vec{s}}+\pi_R(\mathbf{B})\widetilde{\vec{s}}\right]_1,\left[\mathbf{Y}_i^\top\left(\pi_M(\mathbf{B})\widehat{\vec{s}}+\pi_R(\mathbf{B})\widetilde{\vec{s}}\right)\right]_1\\ \left[\pi_M(\mathbf{B}^*\mathbf{R})\widehat{\vec{r}}+\pi_R(\mathbf{B}^*\mathbf{R})\widetilde{\vec{r}}\right]_2,\left[\mathbf{Y}_i\left(\pi_M(\mathbf{B}^*\mathbf{R})\widehat{\vec{r}}+\pi_R(\mathbf{B}^*\mathbf{R})\widetilde{\vec{r}}\right)\right]_2\end{matrix}\right\}_{i\in[n]},$$

$$\left\{\mathsf{pp},\begin{matrix}\left[\pi_M(\mathbf{B})\widehat{\vec{s}}+\pi_R(\mathbf{B})\widetilde{\vec{s}}\right]_1,\left[\left(\mathbf{Y}_i^\top\pi_M(\mathbf{B})+\widehat{u}_i\pi_M(\mathbf{B})\right)\widehat{\vec{s}}+\left(\mathbf{Y}_i^\top\pi_R(\mathbf{B})+\widetilde{u}_i\pi_R(\mathbf{B})\right)\widetilde{\vec{s}}\right]_1\\ \left[\pi_M(\mathbf{B}^*\mathbf{R})\widehat{\vec{r}}+\pi_R(\mathbf{B}^*\mathbf{R})\widetilde{\vec{r}}\right]_2,\\ \left[\left(\mathbf{Y}_i\pi_M(\mathbf{B}^*\mathbf{R})+\widehat{u}_i\pi_M(\mathbf{B}^*\mathbf{R})\right)\widehat{\vec{r}}+\left(\mathbf{Y}_i\pi_R(\mathbf{B}^*\mathbf{R})+\widetilde{u}_i\pi_R(\mathbf{B}^*\mathbf{R})\right)\widetilde{\vec{r}}\right]_2\end{matrix}\right\}_{i\in[n]}, \tag{62}$$

where $\widehat{\vec{s}},\widetilde{\vec{s}},\widehat{\vec{r}},\widetilde{\vec{r}}\leftarrow_R\mathbb{Z}_p^k$ *and* $\widehat{u}_i,\widetilde{u}_i\leftarrow_R\mathbb{Z}_p$.

Proof. Sample $\mathbf{B}\leftarrow_R\mathrm{GL}_{3k}(\mathbb{Z}_p)$, and set $\mathbf{B}^*:=(\mathbf{B}^{-1})^\top$, $\mathbf{Y}_1,\ldots,\mathbf{Y}_n\leftarrow_R\mathbb{Z}_p^{3k\times 3k}$; $\mathbf{R}$ is a random full-rank diagonal matrix in $\mathbb{Z}_p^{3k}$ whose bottom-right entry is a $2k$-dimensional unit matrix:

$$\begin{aligned}
\mathbf{D}&:=\pi_L(\mathbf{B}),\\
\mathbf{D}_i&:=\mathbf{Y}_i^\top\pi_L(\mathbf{B}),\\
\mathbf{E}&:=\pi_M(\mathbf{B}),\\
\mathbf{E}_i&:=\mathbf{Y}_i^\top\pi_M(\mathbf{B}),\\
\mathbf{F}&:=\pi_R(\mathbf{B}),
\end{aligned}$$

$$\begin{aligned}
\mathbf{F}_i &\coloneqq \mathbf{Y}_i^{\top}\pi_R(\mathbf{B}),\\
\mathbf{D}^* &\coloneqq \pi_L(\mathbf{B}^*\mathbf{R}),\\
\mathbf{D}_i^* &\coloneqq \mathbf{Y}_i\pi_L(\mathbf{B}^*\mathbf{R}),\\
\mathbf{E}^* &\coloneqq \pi_M(\mathbf{B}^*\mathbf{R}),\\
\mathbf{E}_i^* &\coloneqq \mathbf{Y}_i\pi_M(\mathbf{B}^*\mathbf{R}),\\
\mathbf{F}^* &\coloneqq \pi_R(\mathbf{B}^*\mathbf{R}),\\
\mathbf{F}_i^* &\coloneqq \mathbf{Y}_i\pi_R(\mathbf{B}^*\mathbf{R}).
\end{aligned} \tag{63}$$

Define $\mathbf{V}_1 = \pi_M(\mathbf{B}^*)\pi_M(\mathbf{B})^{\top}$, $\mathbf{V}_2 = \pi_R(\mathbf{B}^*)\pi_R(\mathbf{B})^{\top}$, and $\mathbf{Y}_i' = \mathbf{Y}_i + \widehat{u}_i\mathbf{V}_1 + \widetilde{u}_i\mathbf{V}_2$. Then

$$\begin{aligned}
\mathbf{Y}_i'^{\top}\mathbf{B} &= \mathbf{Y}_i^{\top}\mathbf{B} + \widehat{u}_i\mathbf{V}_1^{\top}\mathbf{B} + \widetilde{u}_i\mathbf{V}_2^{\top}\mathbf{B},\\
\mathbf{Y}_i'\mathbf{B}^*\mathbf{R} &= \mathbf{Y}_i\mathbf{B}^*\mathbf{R} + \widehat{u}_i\mathbf{V}_1\mathbf{B}^*\mathbf{R} + \widetilde{u}_i\mathbf{V}_2\mathbf{B}^*\mathbf{R}.
\end{aligned} \tag{64}$$

Observe that

$$\begin{aligned}
\mathbf{V}_1^{\top}\mathbf{B} &= \pi_M(\mathbf{B})\left(\pi_M(\mathbf{B}^*)^{\top}\mathbf{B}\right)\\
&= \pi_M(\mathbf{B})\begin{pmatrix} 0 & \cdots & 0 & 1 & & 0 & \cdots & 0\\ \vdots & & \vdots & & \ddots & \vdots & & \vdots\\ 0 & \cdots & 0 & & 1 & 0 & \cdots & 0 \end{pmatrix}\\
&= \left(\overrightarrow{0}^{3k\times k} \parallel \pi_M(\mathbf{B}) \parallel \overrightarrow{0}^{3k\times k}\right),\\
\mathbf{V}_2^{\top}\mathbf{B} &= \pi_R(\mathbf{B})\left(\pi_R(\mathbf{B}^*)^{\top}\mathbf{B}\right)\\
&= \left(\overrightarrow{0}^{3k\times k} \parallel \overrightarrow{0}^{3k\times k} \parallel \pi_R(\mathbf{B})\right),\\
\mathbf{V}_1\mathbf{B}^*\mathbf{R} &= \pi_M(\mathbf{B})^*\left(\pi_M(\mathbf{B})^{\top}\mathbf{B}^*\right)\mathbf{R}\\
&= \left(\overrightarrow{0}^{3k\times k} \parallel \pi_M(\mathbf{B}^*) \parallel \overrightarrow{0}^{3k\times k}\right),\\
\mathbf{V}_2\mathbf{B}^*\mathbf{R} &= \pi_R(\mathbf{B})^*\left(\pi_R(\mathbf{B})^{\top}\mathbf{B}^*\right)\mathbf{R}\\
&= \left(\overrightarrow{0}^{3k\times k} \parallel \overrightarrow{0}^{3k\times k} \parallel \pi_R(\mathbf{B}^*)\right).
\end{aligned} \tag{65}$$

Hence,

$$\begin{aligned}
\mathbf{Y}_i'^{\top}\mathbf{B} &= \left(\mathbf{D}_i \parallel \mathbf{E}_i + \widehat{u}_i\mathbf{E} \parallel \mathbf{F}_i + \widetilde{u}_i\mathbf{F}\right),\\
\mathbf{Y}_i'\mathbf{B}^*\mathbf{R} &= \left(\mathbf{D}_i^* \parallel \mathbf{E}_i^* + \widehat{u}_i\mathbf{E}^* \parallel \mathbf{F}_i^* + \widetilde{u}_i\mathbf{F}^*\right).
\end{aligned} \tag{66}$$

(i) If $\widehat{u}_i = \widetilde{u}_i = 0$, then we obtain the first distribution.

(ii) If $\widehat{u}_i, \widetilde{u}_i \leftarrow \mathbb{Z}_p$, then we obtain the second distribution.

□

6. Our Scheme

This section presents our decentralized CP-ABE system. Recall that $\pi_L(\cdot)$, $\pi_M(\cdot)$, and $\pi_R(\cdot)$ are functions mapping from a $3k \times 3k$ matrix to its left k columns, middle k columns, and right k columns, respectively. We use the left k-dimension subspaces to generate the normal ciphertexts and secret keys. The next two ones are only used in the security proof. The hash function H maps global identities to random elements in $\mathbb{H}$, which is used as a random oracle in the security proof.

6.1. Construction

$\mathsf{GlobalSetup}(1^{\lambda})$. Sample $\mathbf{B} \leftarrow \mathrm{GL}_{3k}(\mathbb{Z}_p)$ and set $\mathbf{B}^* = (\mathbf{B}^{-1})^{\top}$. Output

$$\mathsf{GP} = \left(p, G_1^{3k}, G_2^{3k}, G_T, e; \left[\pi_L(\mathbf{B})\right]_1, H\right). \tag{68}$$

$\mathsf{Authority\ Setup}(\mathsf{GP})$. For each attribute att_i belonging to the authority, the authority samples $\overrightarrow{k}_i \leftarrow \mathbb{Z}_p^{3k}$, $\mathbf{Y}_i \leftarrow \mathbb{Z}_p^{3k\times 3k}$ and outputs

$$\begin{aligned}
&\mathsf{APK}\\
&\coloneqq \left(\left[\pi_L(\mathbf{B})\right]_1, \left[\mathbf{Y}_i^{\top}\pi_L(\mathbf{B})\right]_1, e\left(\left[\pi_L(\mathbf{B})\right]_1, \left[\overrightarrow{k}_i\right]_2\right)\right),\\
&\mathsf{ASK} \coloneqq \left(\overrightarrow{k}_i, \mathbf{Y}_i\right).
\end{aligned} \tag{69}$$

$\mathsf{Enc}(\{\mathsf{APK}\}, \mathsf{GP}, (\mathbf{M}, \rho), m)$. Input a message m, a matrix $\mathbf{M} \in \mathbb{Z}_p^{l\times l'}$ with ρ (in our system, we restrict the fact that ρ is injective) mapping its rows to attributes, the global parameters, and the public keys of the relevant authorities. Pick $\mathbf{U}_2, \ldots, \mathbf{U}_{l'} \leftarrow_R \mathbb{Z}_p^{3k\times 3k}$, $\overrightarrow{s} \leftarrow_R \mathbb{Z}_p^k$, $\overrightarrow{v} = (s_0, v_2, \ldots, v_{l'}) \leftarrow_R \mathbb{Z}_p^{l'}$. We let $\mathbf{M}_x$ denote row x of $\mathbf{M}$, and $\lambda_x = \mathbf{M}_x \cdot \overrightarrow{v}$. The ciphertext is

$$\begin{aligned}
C &= m \cdot e(g_1, g_2)^{s_0},\\
C_0 &= \left[\pi_L(\mathbf{B})\overrightarrow{s}\right]_1,\\
C_{1,x} &= e(g_1, g_2)^{\lambda_x} e(g_1, g_2)^{k_{\rho(x)}^{\top}\pi_L(\mathbf{B})\overrightarrow{s}},\\
C_{2,x} &= \left[\left(\overrightarrow{0} \parallel \mathbf{U}_2^{\top}\pi_L(\mathbf{B})\overrightarrow{s} \parallel \cdots \parallel \mathbf{U}_{l'}^{\top}\pi_L(\mathbf{B})\overrightarrow{s}\right)\mathbf{M}_x^{\top}\right.\\
&\quad \left. + \mathbf{Y}_{\rho(x)}^{\top}\pi_L(\mathbf{B})\overrightarrow{s}\right]_1.
\end{aligned} \tag{70}$$

$\mathsf{KeyGen}(\mathsf{GP}, \mathsf{GID}, \mathsf{ASK}_j, att_i)$. Compute a key for GID for attribute att_i belonging to authority AA_j as follows:

$$\mathsf{SK}_{\mathsf{GID},i} = g_2^{\overrightarrow{k}_i} H(\mathsf{GID})^{\mathbf{Y}_i}. \tag{71}$$

$\mathsf{Dec}(\mathsf{GP}, \mathsf{SK}_{\mathsf{GID},i}, \mathsf{CT})$. The secret keys $\{\mathsf{SK}_{\mathsf{GID},i}\}$ correspond to a subset of rows $\mathbf{M}_x$ of $\mathbf{M}$. If $(1, 0, \ldots, 0)$ is in the span of $\mathbf{M}_x$, then $\omega_1, \ldots, \omega_l \in \mathbb{Z}_p$ is computed such that

$$\sum_x \omega_x \mathbf{M}_x = (1, 0, \ldots, 0). \tag{72}$$

Then, compute

$$\begin{aligned}
&\prod_x \left(C_{1,x} \cdot \frac{e\left(H\left(\mathsf{GID}\right), C_{2,x}\right)}{e\left(\mathsf{SK}_{\mathsf{GID},\rho(x)}, C_0\right)} \right)^{\omega_x} \\
&= \frac{\prod_x C_{1,x}^{\omega_x} \cdot e\left(H\left(\mathsf{GID}\right), \prod_x C_{2,x}^{\omega_x}\right)}{e\left(\prod_x \mathsf{SK}_{\mathsf{GID},\rho(x)}^{\omega_x}, C_0\right)} \\
&= e\left(g_1, g_2\right)^{\sum_x \omega_x \mathbf{M}_x \overrightarrow{v}} e\left(g_1, g_2\right)^{\overrightarrow{r}^\top \overrightarrow{0}} = e\left(g_1, g_2\right)^{s_0}, \\
&m = \frac{C}{e\left(g_1, g_2\right)^{s_0}}.
\end{aligned} \tag{73}$$

6.2. Security Proof. We define the semifunctional ciphertext and secret key as follows.

Semifunctional Ciphertext. We let $C', C_0', C_{1,x}', C_{2,x}'$ denote the normal ciphertext. The semifunctional ciphertext takes the following form:

$$\begin{aligned}
&C = C', \\
&C_0 = C_0' \cdot \left[\pi_M\left(\mathbf{B}\right) \widehat{\overrightarrow{s}} + \pi_R\left(\mathbf{B}\right) \widetilde{\overrightarrow{s}} \right]_1, \\
&C_{1,x} = C_{1,x}' \cdot e\left(g_1, g_2\right)^{k_{\rho(x)}^\top \left(\pi_M(\mathbf{B}) \widehat{\overrightarrow{s}} + \pi_R(\mathbf{B}) \widetilde{\overrightarrow{s}}\right)}, \\
&C_{2,x} = C_{2,x}' \cdot \left[\left(\widehat{s} \pi_M\left(\mathbf{B}\right) \widehat{\overrightarrow{s}} \parallel \mathbf{U}_2^\top \pi_M\left(\mathbf{B}\right) \right.\right. \\
&\quad \left. \cdot \widehat{\overrightarrow{s}} \parallel \cdots \parallel \mathbf{U}_{l'}^\top \pi_M\left(\mathbf{B}\right) \widehat{\overrightarrow{s}} \right) \mathbf{M}_x^\top + \mathbf{Y}_{\rho(x)}^\top \pi_M\left(\mathbf{B}\right) \widehat{\overrightarrow{s}} \Big]_1 \\
&\quad \cdot \left[\left(\widetilde{s} \pi_R\left(\mathbf{B}\right) \widetilde{\overrightarrow{s}} \parallel \mathbf{U}_2^\top \pi_R\left(\mathbf{B}\right) \widetilde{\overrightarrow{s}} \parallel \cdots \parallel \mathbf{U}_{l'}^\top \pi_R\left(\mathbf{B}\right) \widetilde{\overrightarrow{s}} \right) \right. \\
&\quad \left. \cdot \mathbf{M}_x^\top + \mathbf{Y}_{\rho(x)}^\top \pi_R\left(\mathbf{B}\right) \widetilde{\overrightarrow{s}} \right]_1,
\end{aligned} \tag{74}$$

where $\widehat{\overrightarrow{s}}, \widetilde{\overrightarrow{s}} \leftarrow_R \mathbb{Z}_p^k, \mathbf{U}_2, \ldots, \mathbf{U}_{l'} \leftarrow_R \mathbb{Z}_p^{3k \times 3k}$.

Semifunctional Secret Key. There are two types of semifunctional keys. Type 1 semifunctional key takes the following form:

$$\begin{aligned}
&H\left(\mathrm{GID}\right) = \left[\pi_L\left(\mathbf{B}^* \mathbf{R}\right) \overrightarrow{r} + \pi_M\left(\mathbf{B}^* \mathbf{R}\right) \widehat{\overrightarrow{r}} \right]_2, \\
&\mathsf{SK}_{\mathrm{GID},i} = g_2^{\overrightarrow{k}_i} H\left(\mathrm{GID}\right)^{\mathbf{Y}_i} \\
&\quad = \left[\overrightarrow{k}_i + \mathbf{Y}_i \left(\pi_L\left(\mathbf{B}^* \mathbf{R}\right) \overrightarrow{r} + \pi_M\left(\mathbf{B}^* \mathbf{R}\right) \widehat{\overrightarrow{r}} \right) \right]_2.
\end{aligned} \tag{75}$$

Type 2 semifunctional key takes the following form:

$$\begin{aligned}
&H\left(\mathrm{GID}\right) = \left[\pi_L\left(\mathbf{B}^* \mathbf{R}\right) \overrightarrow{r} + \pi_R\left(\mathbf{B}^* \mathbf{R}\right) \widetilde{\overrightarrow{r}} \right]_2, \\
&\mathsf{SK}_{\mathrm{GID},i} = g_2^{\overrightarrow{k}_i} H\left(\mathrm{GID}\right)^{\mathbf{Y}_i} \\
&\quad = \left[\overrightarrow{k}_i + \mathbf{Y}_i \left(\pi_L\left(\mathbf{B}^* \mathbf{R}\right) \overrightarrow{r} + \pi_R\left(\mathbf{B}^* \mathbf{R}\right) \widetilde{\overrightarrow{r}} \right) \right]_2.
\end{aligned} \tag{76}$$

When a semifunctional key is used to decrypt a semifunctional ciphertext, the additional terms

(i) type 1 semifunctional key: $e(g_1, g_2)^{\widehat{s}\widehat{\overrightarrow{r}}^\top \pi_M(\mathbf{B}^* \mathbf{R})^\top \pi_M(\mathbf{B}) \widehat{\overrightarrow{s}}}$,

(ii) type 2 semifunctional key: $e(g_1, g_2)^{\widetilde{s}\widetilde{\overrightarrow{r}}^\top \pi_R(\mathbf{B}^* \mathbf{R})^\top \pi_R(\mathbf{B}) \widetilde{\overrightarrow{s}}}$

prevent decryption.

Game Sequence. We let $\mathsf{Adv}_{\mathscr{A}}^{\mathsf{Game}_X}$ denote the advantage of $\mathscr{A}$ in Game_X.

(i) Game_0: it is the real security game.

(ii) Game_1: there is no difference with Game_0 except that challenge ciphertext becomes semifunctional.

(iii) $\mathsf{Game}_{2,j,1}$ for $j = 1, \ldots, q$: there is no difference with Game_1 except that the first $j-1$ keys revealed to $\mathscr{A}$ become semifunctional of type 2, and the j'th key becomes semifunctional of type 1.

(iv) $\mathsf{Game}_{2,j,2}$ for $j = 1, \ldots, q$: there is no difference with Game_1 except that the first j keys revealed to $\mathscr{A}$ become semifunctional of type 2. We let $\mathsf{Game}_{2,0,2}$ denote Game_1.

(v) Game_3: there is no difference with $\mathsf{Game}_{2,q,2}$ except that we generate a semifunctional ciphertext of a random message $m' \in \mathbb{G}_T$ as the challenge ciphertext.

Lemma 9 (from Game_0 to Game_1). *For any PPT adversary $\mathscr{A}$, there exists an adversary $\mathscr{B}$ such that* $|\mathsf{Adv}_{\mathscr{A}}^{\mathsf{Game}_0}(\lambda) - \mathsf{Adv}_{\mathscr{A}}^{\mathsf{Game}_1}(\lambda)| \leqslant \mathsf{Adv}_{\mathscr{B}}^{LS}(\lambda)$.

Proof. The adversary $\mathscr{B}$ gets input

$$\left(\mathsf{pp}, \overrightarrow{t}\right), \tag{77}$$

where $\overrightarrow{t}$ is $\overrightarrow{g}$ or $\overrightarrow{g} \cdot \widehat{\overrightarrow{g}} \cdot \widetilde{\overrightarrow{g}}$.

Setup. Pick $\overrightarrow{k}_i$ and output

$$\mathsf{APK} := \left(\mathsf{pp}, e\left(\left[\pi_L\left(\mathbf{B}\right)\right]_1, \left[\overrightarrow{k}_i\right]_2\right)\right). \tag{78}$$

Key Queries. When $\mathscr{A}$ queries the random oracle for $H(\mathrm{GID})$, $\mathscr{B}$ chooses $\overrightarrow{r} \leftarrow \mathbb{Z}_p^k$, sets $H(\mathrm{GID}) = [\pi_L(\mathbf{B}^* \mathbf{R}) \overrightarrow{r}]_2$, and stores this value. $\mathscr{B}$ creates secret keys as follows:

$$\mathsf{SK}_{\mathrm{GID},i} = \left[\overrightarrow{k}_i + \mathbf{Y}_i \pi_L\left(\mathbf{B}^* \mathbf{R}\right) \overrightarrow{r} \right]_2. \tag{79}$$

Challenge. Upon receiving $(\mathbf{M}, \rho)$, m_0, and m_1, $\mathscr{B}$ can compute the ciphertext by using $\overrightarrow{t}$. We note that the ciphertext

is properly distributed except $C_{2,x}$, which take the following forms:

$$\begin{aligned} C_{2,x} = & \left[\left(\overrightarrow{0} \parallel \mathbf{U}_2^{\top}\pi_L(\mathbf{B})\overrightarrow{s} \parallel \cdots \parallel \mathbf{U}_{l'}^{\top}\pi_L(\mathbf{B})\overrightarrow{s}\right)\mathbf{M}_x^{\top}\right. \\ & \left. + \mathbf{Y}_i^{\top}\pi_L(\mathbf{B})\overrightarrow{s}\right]_1 \\ & \cdot \left[\left(\boxed{\overrightarrow{0}} \parallel \mathbf{U}_2^{\top}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}} \parallel \cdots \parallel \mathbf{U}_{l'}^{\top}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\right)\mathbf{M}_x^{\top}\right. \\ & \left. + \mathbf{Y}_i^{\top}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\right]_1 \\ & \cdot \left[\left(\boxed{\overrightarrow{0}} \parallel \mathbf{U}_2^{\top}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}} \parallel \cdots \parallel \mathbf{U}_{l'}^{\top}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\right)\mathbf{M}_x^{\top}\right. \\ & \left. + \mathbf{Y}_i^{\top}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\right]_1, \end{aligned} \tag{80}$$

where $\overrightarrow{s}, \widehat{\overrightarrow{s}}, \widetilde{\overrightarrow{s}} \leftarrow_R \mathbb{Z}_p^k, \mathbf{U}_2, \ldots, \mathbf{U}_{l'} \leftarrow_R \mathbb{Z}_p^{3k\times 3k}$. We must argue that there is no difference in $\mathcal{A}$'s view.

By parameter hiding, it suffices to show that

$$\begin{aligned} & \left[\left(\boxed{\overrightarrow{0}} \parallel \cdots\right)\mathbf{M}_x^{\top} + \widehat{u}_i\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\right]_1 \cdot \left[\left(\boxed{\overrightarrow{0}} \parallel \cdots\right)\mathbf{M}_x^{\top} + \widetilde{u}_i\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\right]_1, \\ & \left[\left(\boxed{\widehat{s}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}} \parallel \cdots\right)\mathbf{M}_x^{\top} + \widehat{u}_i\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\right]_1 \cdot \left[\left(\boxed{\widetilde{s}\pi_M(\mathbf{B})\widetilde{\overrightarrow{s}}} \parallel \cdots\right)\mathbf{M}_x^{\top} + \widetilde{u}_i\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\right]_1 \end{aligned} \tag{81}$$

are identically distributed. This follows readily from the fact that

(i) the space spanned by rows of $\mathbf{M}$ whose corresponding attributes belong to corrupt authorities cannot include the vector $(1, 0, \ldots, 0)$; it reveals no information about $\widehat{s}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}$ and $\widetilde{s}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}$;

(ii) rows of $\mathbf{M}$ whose corresponding attributes belong to good authorities are masked by $\widehat{u}_i\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}$ and $\widetilde{u}_i\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}$, respectively.

If $\overrightarrow{t} = \overrightarrow{g}$, $\mathcal{B}$ properly simulates Game_0; if $\overrightarrow{t} = \overrightarrow{g}\cdot\widehat{\overrightarrow{g}}\cdot\widetilde{\overrightarrow{g}}$, $\mathcal{B}$ properly simulates Game_1. Hence, $\mathcal{B}$ can determine the distribution of $\overrightarrow{t}$ by using adversary $\mathcal{A}$. □

Lemma 10 (from $\mathsf{Game}_{2,j-1,2}$ to $\mathsf{Game}_{2,j,1}$). *For any PPT adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{2,j-1,2}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{2,j,1}}(\lambda)| \leqslant \mathsf{Adv}_{\mathcal{B}}^{RS1}(\lambda)$.

Proof. The adversary $\mathcal{B}$ gets input

$$\left(\mathsf{pp}, \overrightarrow{g}\cdot\widehat{\overrightarrow{g}}, \widetilde{\overrightarrow{g}}, \overrightarrow{t}\right), \tag{82}$$

where $\overrightarrow{t}$ is $\overrightarrow{h}$ or $\overrightarrow{h}\cdot\widehat{\overrightarrow{h}}$.

Setup. Pick $\overrightarrow{k}_i$ and output

$$\mathsf{APK} := \left(\mathsf{pp}, e\left(\left[\pi_L(\mathbf{B})\right]_1, \left[\overrightarrow{k}_i\right]_2\right)\right). \tag{83}$$

Key Queries. We let GID_k denote the kth identity queried by $\mathcal{A}$.

(i) $k < j$: $\mathcal{B}$ chooses $\overrightarrow{r} \leftarrow \mathbb{Z}_p^k$ and sets $H(\mathrm{GID}_k) = [(\pi_L(\mathbf{B}^*\mathbf{R}) + \pi_R(\mathbf{B}^*\mathbf{R}))\overrightarrow{r}]_2$.

(ii) $k > j$: $\mathcal{B}$ chooses $\overrightarrow{r} \leftarrow \mathbb{Z}_p^k$ and sets $H(\mathrm{GID}_k) = [\pi_L(\mathbf{B}^*\mathbf{R})\overrightarrow{r}]_2$.

(iii) $k = j$: $H(\mathrm{GID}) = \overrightarrow{t}_0$, where $\overrightarrow{t}_0$ is the first element in $\overrightarrow{t}$.

$\mathcal{B}$ creates secret keys as follows:

$$\mathsf{SK}_{\mathrm{GID},i} = g_2^{\overrightarrow{k}_i} H(\mathrm{GID})^{\mathbf{Y}_i}. \tag{84}$$

Challenge. Upon receiving $(\mathbf{M}, \rho)$, m_0, and m_1, $\mathcal{B}$ computes the ciphertext by using $\overrightarrow{g}\cdot\widehat{\overrightarrow{g}}, \widetilde{\overrightarrow{g}}$ as follows:

$$\begin{aligned} C' &= m\cdot e(g_1, g_2)^{s_0}, \\ C_0 &= \left[\pi_L(\mathbf{B})\overrightarrow{s} + \pi_M(\mathbf{B})\widehat{\overrightarrow{s}} + \pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\right]_1, \\ C_{1,x} &= e(g_1, g_2)^{\lambda_x} e(g_1, g_2)^{\overrightarrow{k}_x^{\top}(\pi_L(\mathbf{B})\overrightarrow{s} + \pi_M(\mathbf{B})\widehat{\overrightarrow{s}} + \pi_R(\mathbf{B})\widetilde{\overrightarrow{s}})}, \\ C_{2,x} &= \left[\left(\overrightarrow{0} \parallel \mathbf{U}_2^{\top}\pi_L(\mathbf{B})\overrightarrow{s} \parallel \cdots \parallel \mathbf{U}_{l'}^{\top}\pi_L(\mathbf{B})\overrightarrow{s}\right)\mathbf{M}_x^{\top}\right. \\ &\quad \left. + \mathbf{Y}_i^{\top}\pi_L(\mathbf{B})\overrightarrow{s}\right]_1 \\ &\quad \cdot \left[\left(\overrightarrow{0} \parallel \mathbf{U}_2^{\top}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}} \parallel \cdots \parallel \mathbf{U}_{l'}^{\top}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\right)\mathbf{M}_x^{\top}\right. \\ &\quad \left. + \mathbf{Y}_i^{\top}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\right]_1 \\ &\quad \cdot \left[\left(\widetilde{s}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}} \parallel \mathbf{U}_2^{\top}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}} \parallel \cdots \parallel \mathbf{U}_{l'}^{\top}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\right)\right. \\ &\quad \left. \cdot \mathbf{M}_x^{\top} + \mathbf{Y}_i^{\top}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\right]_1, \end{aligned} \tag{85}$$

where $\widehat{\overrightarrow{s}}, \widetilde{\overrightarrow{s}} \leftarrow_R \mathbb{Z}_p^k, \mathbf{U}_2, \ldots, \mathbf{U}_{l'} \leftarrow_R \mathbb{Z}_p^{3k\times 3k}$. The ciphertext is properly distributed except that the second components of

$C_{2,x}$ are shares of 0. We must argue that there is no difference in $\mathcal{A}$'s view.

By parameter hiding, it suffices to show that

$$\begin{aligned}&\left[\left(\overrightarrow{0} \parallel \cdots\right)\mathbf{M}_x^\top + \widehat{u}_i\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\right]_1,\\&\left[\left(\widehat{s}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}} \parallel \cdots\right)\mathbf{M}_x^\top + \widehat{u}_i\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\right]_1\end{aligned} \tag{86}$$

are identically distributed. This follows readily from the fact that

(i) for $k > j$ and $k < j$, $H(\mathrm{GID}_k)$ have nothing to do with $\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}$;

(ii) the space spanned by rows of $\mathbf{M}$ whose corresponding attributes belong to corrupted authorities or queried with GID_j cannot include the vector $(1, 0, \ldots, 0)$; it reveals no information about $\widehat{s}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}$;

(iii) the remaining rows of $\mathbf{M}$ are masked by $\widehat{u}_i\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}$.

If $\overrightarrow{t} = \overrightarrow{h}$, $\mathcal{B}$ properly simulates $\mathsf{Game}_{2,j-1,2}$; if $\overrightarrow{t} = \overrightarrow{h}\cdot\widehat{\overrightarrow{h}}$, $\mathcal{B}$ properly simulates $\mathsf{Game}_{2,j,1}$. Hence, $\mathcal{B}$ can determine the distribution of $\overrightarrow{t}$ by using adversary $\mathcal{A}$. □

Lemma 11 (from $\mathsf{Game}_{2,j,1}$ to $\mathsf{Game}_{2,j,2}$). *For any PPT adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{2,j,1}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{2,j,2}}(\lambda)| \leqslant \mathsf{Adv}_{\mathcal{B}}^{RS2}(\lambda)$.

Proof. The adversary $\mathcal{B}$ gets input

$$\left(\mathsf{pp}, \overrightarrow{g}, \widehat{\overrightarrow{g}}\cdot\widetilde{\overrightarrow{g}}, \overrightarrow{t}\right), \tag{87}$$

where $\overrightarrow{t}$ is $\overrightarrow{h}\cdot\widehat{\overrightarrow{h}}$ or $\overrightarrow{h}\cdot\widetilde{\overrightarrow{h}}$.

Setup. Pick $\overrightarrow{k}_i$ and output

$$\mathsf{PK} := \left(\mathsf{pp}, e\left(\left[\pi_L(\mathbf{B})\right]_1, \left[\overrightarrow{k}_i\right]_2\right)\right). \tag{88}$$

Key Queries. We let GID_k denote the kth identity queried by $\mathcal{A}$.

(i) $k < j$: $\mathcal{B}$ chooses $\overrightarrow{r} \leftarrow \mathbb{Z}_p^k$ and sets $H(\mathrm{GID}_k) = [(\pi_L(\mathbf{B}^*\mathbf{R}) + \pi_R(\mathbf{B}^*\mathbf{R}))\overrightarrow{r}]_2$.

(ii) $k > j$: $\mathcal{B}$ chooses $\overrightarrow{r} \leftarrow \mathbb{Z}_p^k$ and sets $H(\mathrm{GID}_k) = [\pi_L(\mathbf{B}^*\mathbf{R})\overrightarrow{r}]_2$.

(iii) $k = j$: $H(\mathrm{GID}) = \overrightarrow{t}_0$, where $\overrightarrow{t}_0$ is the first element in $\overrightarrow{t}$.

$\mathcal{B}$ creates secret keys as follows:

$$K_{\mathrm{GID},i} = g_2^{\overrightarrow{k}_i} H(\mathrm{GID})^{\mathbf{Y}_i}. \tag{89}$$

Challenge. Upon receiving $(\mathbf{M}, \rho)$, m_0, and m_1, $\mathcal{B}$ computes the ciphertext as follows:

$$\begin{aligned}C' &= m\cdot e(g_1, g_2)^{s_0},\\C_0 &= \left[\pi_L(\mathbf{B})\overrightarrow{s} + \pi_M(\mathbf{B})\widehat{\overrightarrow{s}} + \pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\right]_1,\\C_{1,x} &= e(g_1, g_2)^{\lambda_x} e(g_1, g_2)^{\overrightarrow{k}_x^\top(\pi_L(\mathbf{B})\overrightarrow{s} + \pi_M(\mathbf{B})\widehat{\overrightarrow{s}} + \pi_R(\mathbf{B})\widetilde{\overrightarrow{s}})},\\C_{2,x} &= \Big[\Big(\overrightarrow{0} \parallel \mathbf{U}_2^\top\pi_L(\mathbf{B})\overrightarrow{s} \parallel \cdots \parallel \mathbf{U}_{l'}^\top\pi_L(\mathbf{B})\overrightarrow{s}\Big)\mathbf{M}_x^\top\\&\quad + \mathbf{Y}_i^\top\pi_L(\mathbf{B})\overrightarrow{s}\Big]_1 \cdot \Big[\Big(\widehat{s}\pi_M(\mathbf{B})\widehat{\overrightarrow{s}} \parallel \mathbf{U}_2^\top\pi_M(\mathbf{B})\\&\quad \cdot\widehat{\overrightarrow{s}} \parallel \cdots \parallel \mathbf{U}_{l'}^\top\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\Big)\mathbf{M}_x^\top + \mathbf{Y}_i^\top\pi_M(\mathbf{B})\widehat{\overrightarrow{s}}\Big]_1\\&\quad \cdot\Big[\Big(\widetilde{s}\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}} \parallel \mathbf{U}_2^\top\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}} \parallel \cdots \parallel \mathbf{U}_{l'}^\top\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\Big)\\&\quad \cdot\mathbf{M}_x^\top + \mathbf{Y}_i^\top\pi_R(\mathbf{B})\widetilde{\overrightarrow{s}}\Big]_1,\end{aligned} \tag{90}$$

where $\widehat{\overrightarrow{s}}, \widetilde{\overrightarrow{s}} \leftarrow_R \mathbb{Z}_p^k$, $\mathbf{U}_2, \ldots, \mathbf{U}_{l'} \leftarrow_R \mathbb{Z}_p^{3k\times 3k}$, $\widehat{s}, \widetilde{s} \leftarrow_R \mathbb{Z}_p$, and we implicitly set $\widehat{s} = \widetilde{s}$.

If $\overrightarrow{t} = \overrightarrow{h}\cdot\widetilde{\overrightarrow{h}}$, $\mathcal{B}$ properly simulates $\mathsf{Game}_{2,j,1}$; if $\overrightarrow{t} = \overrightarrow{h}\cdot\widehat{\overrightarrow{h}}$, $\mathcal{B}$ properly simulates $\mathsf{Game}_{2,j,2}$. Hence, $\mathcal{B}$ can determine the distribution of $\overrightarrow{t}$ by using adversary $\mathcal{A}$. □

Lemma 12 (from $\mathsf{Game}_{2,q,2}$ to Game_3). *For any PPT adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\left|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_{2,q,2}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_3}(\lambda)\right| = 0. \tag{91}$$

Proof.

Setup. $\mathcal{B}$ samples $\mathbf{B} \leftarrow \mathrm{GL}_{3k}(\mathbb{Z}_p)$ and sets $\mathbf{B}^* = (\mathbf{B}^{-1})^\top$. Output

$$\mathsf{GP} = \left(p, G_1^{3k}, G_2^{3k}, G_T, e; \left[\pi_L(\mathbf{B})\right]_1, H\right). \tag{92}$$

$\mathcal{B}$ also samples $\overrightarrow{k}_i \leftarrow \mathbb{Z}_p^{3k}$, $\mathbf{Y}_i \leftarrow \mathbb{Z}_p^{3k\times 3k}$ for each attribute and sets

$$\begin{aligned}&\mathsf{APK}\\&:= \left(\left[\pi_L(\mathbf{B})\right]_1, \left[\mathbf{Y}_i^\top\pi_L(\mathbf{B})\right]_1, e\left(\left[\pi_L(\mathbf{B})\right]_1, \left[\overrightarrow{k}_i\right]_2\right)\right),\\&\mathsf{ASK} := \left(\overrightarrow{k}_i, \mathbf{Y}_i\right).\end{aligned} \tag{93}$$

Key Queries. In both games, the secret keys take the following form:

$$\mathsf{SK}_{\mathrm{GID},i} = \left[\overrightarrow{k}_i + \mathbf{Y}_i\left(\pi_L(\mathbf{B}^*\mathbf{R})\overrightarrow{r} + \pi_R(\mathbf{B}^*\mathbf{R})\overrightarrow{r}\right)\right]_2, \tag{94}$$

which means they leak no information whatsoever about $\pi_M(\mathbf{B})$.

Table 1: Comparing among existing decentralized CP-ABE schemes. |APK|, |SK|, and |CT| represent the size of authority's public keys, user's secret keys, and ciphertexts. n is the number of attributes present in authority or secret keys. ℓ is number of rows in the access matrix. T_{Dec} represents decryption cost, "Pair" and "Exp" represent the number of pairings and exponentiations in groups. ℓ' is the number of attributes used during decryption. $|G|$ indicates the group order, "P" is for prime, and "C" is for composite order, respectively. "Assu." and "Secu." are abbreviation of assumption and security, respectively.

Ref.	|APK|		|SK|	|CT|		T_{Dec}		Assu.	$\|G\|$	Secu.
	G_1	G_T	G_1/G_2	G_1	G_T	Pair	Exp			
[11]	n	n	n	2ℓ	$\ell+1$	$\ell'+1$	$3\ell'$	Static	C	Full
[29]	1	1	$2n$	3ℓ	$\ell+1$	$2\ell'+1$	$4\ell'$	q-type	P	Static
[13]	$55n$	1	$11n$	11ℓ	1	$11\ell'$	ℓ'	DLIN	P	Full
Ours	$3k^2(n+1)$	kn	$3kn$	$3k(\ell+1)$	$\ell+1$	$6k$	$6k\ell'+\ell'$	k-Lin	P	Full
	$3(n+1)$	n	$3n$	$3(\ell+1)$	$\ell+1$	6	$7\ell'$	SXDH		
	$12(n+1)$	$2n$	$6n$	$6(\ell+1)$	$\ell+1$	12	$13\ell'$	DLIN		

Challenge. Upon receiving $(\mathbf{M}, \rho)$, m_0, and m_1, $\mathscr{B}$ computes the semifunctional ciphertext of m_0 or m_1. Observe that

$$C_{1,x} = e(g_1, g_2)^{\lambda_x} e(g_1, g_2)^{\vec{k}_x^{\top}(\pi_L(\mathbf{B})\vec{s}+\pi_R(\mathbf{B})\widetilde{\vec{s}})} \cdot e(g_1, g_2)^{\vec{k}_x^{\top}\pi_M(\mathbf{B})\widehat{\vec{s}}}, \tag{95}$$

and the quantity $e(g_1, g_2)^{\vec{k}_x^{\top}\pi_M(\mathbf{B})\widehat{\vec{s}}}$ is uniformly distributed over $\mathbb{G}_T$. This implies the challenge ciphertext is identically distributed to a semifunctional encryption of a random message in $\mathbb{G}_T$, as in Game_3. □

6.3. Performance Discussions. In this section, we provided analysis regarding the space and computation cost of the proposed scheme by comparing it with existing decentralized ABE schemes.

As shown in Table 1, [11] is built on composite-order groups. We recall that composite-order elements are 12 times larger than prime-order ones and pairing is 250 times slower in composite-order groups than in prime-order ones [12]. Though [29] is efficient, the scheme can be only proved static security under a q-type assumption. Both [13] and ours are based on prime-order groups; the secret key size and the ciphertext size in ours are reduced by about 40% compared with [13] under the same assumption (DLIN). We will see further improvement if we instantiate our construction under the SXDH assumption. In addition, the ciphertexts in our setting can be decrypted with a constant number of pairings at the cost of increasing some exponentiations. We believe that this is a good deal since pairing is about 5 times slower than group exponentiation according to [29]. The advantage of decryption performance in our scheme will become more and more obvious as the number of attributes used for decryption increases.

7. Conclusions

In this paper, we presented a fully secure decentralized CP-ABE scheme under the standard k-Lin assumptions in prime-order groups. To prove the security of our scheme, we extended the basis of dual system groups from $2k \times 2k$ matrix to $3k \times 3k$ matrix and realized some assumptions to mimic the effect of the subgroup decision assumption in composite-order groups. Our scheme achieved lower computational cost thanks to decryption which only needs constant number of pairing operations. We discussed the performance of our scheme from the theoretical points of view. Compared with other existing decentralized CP-ABE schemes, our scheme is more compact to implement and can provide better efficiency in terms of the communication and computation cost.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China (nos. 61502529, 61379150, 61472142, and 61602512) and the Science and Technology Commission of Shanghai Municipality (no. 14YF1404200).

References

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT 2005*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 457–473, Springer, Berlin, Heidelberg, Germany, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, New York, NY, USA, November 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Oakland, Calif, USA, May 2007.

[4] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology—EUROCRYPT 2010*, vol. 6110 of *Lecture Notes*

in Computer Science, pp. 62–91, Springer, Berlin, Heidelberg, Germany, 2010.

[5] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Advances in Cryptology—CRYPTO 2010*, vol. 6223 of *Lecture Notes in Computer Science*, pp. 191–208, Springer, Berlin, Heidelberg, Germany, 2010.

[6] K. Emura, A. Miyaji, K. Omote, A. Nomura, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," *International Journal of Applied Cryptography*, vol. 2, no. 1, pp. 46–59, 2010.

[7] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu, and K.-K. R. Choo, "Fine-grained Database Field Search Using Attribute-Based Encryption for E-Healthcare Clouds," *Journal of Medical Systems*, vol. 40, no. 11, article 235, 2016.

[8] L. Liu, J. Lai, R. H. Deng, and Y. Li, "Ciphertext-policy attribute-based encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment," *Security and Communication Networks*, vol. 9, no. 18, pp. 4897–4913, 2016.

[9] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1265–1277, 2016.

[10] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography*, vol. 4392 of *Lecture Notes in Computer Science*, pp. 515–534, Springer, Berlin, Germany, 2007.

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology—EUROCRYPT 2011*, vol. 6632 of *Lecture Notes in Computer Science*, pp. 568–588, Springer, Berlin, Heidelberg, Germany, 2011.

[12] A. Guillevic, "Comparing the pairing efficiency over composite-order and prime-order elliptic curves," in *Proceedings of the Applied Cryptography and Network Security: 11th International Conference (ACNS '13)*, vol. 7954 of *Lecture Notes in Computer Science*, pp. 357–372, Springer, Berlin, Heidelberg, Germany, 2013.

[13] T. Okamoto and K. Takashima, "Decentralized attribute-based signatures," in *Public-Key Cryptography—PKC 2013*, vol. 7778 of *Lecture Notes in Computer Science*, pp. 125–142, Springer, Berlin, Heidelberg, Germany, 2013.

[14] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *Proceedings of the Theory of Cryptography Conference (TCC '10)*, vol. 5978 of *Lecture Notes in Computer Science*, pp. 455–479, Springer, Berlin, Heidelberg, Germany, 2010.

[15] B. Waters, "Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology—CRYPTO 2009*, vol. 5677 of *Lecture Notes in Computer Science*, pp. 619–636, Springer, Berlin, Heidelberg, Germany, 2009.

[16] J. Chen and H. Wee, "Fully, (almost) tightly secure IBE and dual system groups," in *Advances in Cryptology—CRYPTO 2013. Part II*, vol. 8043 of *Lecture Notes in Computer Science*, pp. 435–460, Springer, Berlin, Heidelberg, Germany, 2013.

[17] D. M. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in *Advances in Cryptology—EUROCRYPT 2010*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 44–61, Springer, Berlin, Heidelberg, Germany, 2010.

[18] A. Lewko, "Tools for simulating features of composite order bilinear groups in the prime order setting," in *Advances in Cryptology—EUROCRYPT 2012*, vol. 7237 of *Lecture Notes in Computer Science*, pp. 318–335, Springer, Berlin, Heidelberg, Germany, 2012.

[19] T. Okamoto and K. Takashima, "Hierarchical predicate encryption for inner-products," in *Advances in Cryptology—ASIACRYPT 2009*, vol. 5912 of *Lecture Notes in Computer Science*, pp. 214–231, Springer, Berlin, Heidelberg, Germany, 2009.

[20] J. Gong, J. Chen, X. Dong, Z. Cao, and S. Tang, "Extended nested dual system groups, revisited," in *Public-Key Cryptography—PKC 2016. Part I*, vol. 9614 of *Lecture Notes in Computer Science*, pp. 133–163, Springer, Berlin, Heidelberg, Germany, 2016.

[21] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 195–203, November 2007.

[22] A. Lewko, Y. Rouselakis, and B. Waters, "Achieving leakage resilience through dual system encryption," in *Theory of Cryptography—TCC 2011*, vol. 6597 of *Lecture Notes in Computer Science*, pp. 70–88, Springer, Berlin, Heidelberg, Germany, 2011.

[23] A. Lewko and B. Waters, "Unbounded HIBE and attribute-based encryption," in *Advances in Cryptology—EUROCRYPT 2011*, vol. 6632 of *Lecture Notes in Computer Science*, pp. 547–567, Springer, Berlin, Heidelberg, Germany, 2011.

[24] T. Okamoto and K. Takashima, "Fully secure unbounded inner-product and attribute-based encryption," in *Advances in Cryptology—ASIACRYPT 2012*, vol. 7658 of *Lecture Notes in Computer Science*, pp. 349–366, Springer, Berlin, Heidelberg, Germany, 2012.

[25] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, pp. 121–130, New York, NY, USA, November 2009.

[26] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," *Information Sciences*, vol. 180, no. 13, pp. 2618–2632, 2010.

[27] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," *Bulletin of the Korean Mathematical Society*, vol. 46, no. 4, pp. 803–819, 2009.

[28] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *Computer Security—ESORICS 2011*, vol. 6879 of *Lecture Notes in Computer Science*, pp. 278–297, Springer, Berlin, Heidelberg, Germany, 2011.

[29] Y. Rouselakis and B. Waters, "Efficient statically-secure large-universe multi-authority attribute-based encryption," in *Financial Cryptography And Data Security*, vol. 8975 of *Lecture Notes in Computer Science*, pp. 315–332, Springer, Berlin, Heidelberg, Germany, 2015.

[30] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traitor tracing," *Journal of Computational Information Systems*, vol. 9, no. 7, pp. 2792–2800, 2013.

[31] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in *Proceedings of the 6th International Symposium on Information, Computer and Communications Security (ASIACCS '11)*, pp. 386–390, New York, NY, USA, March 2011.

[32] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, "Large universe decentralized key-policy attribute-based encryption," *Security and Communication Networks*, vol. 8, no. 3, pp. 501–509, 2015.

[33] N. Gorasia, R. R. Srikanth, N. Doshi, and J. Rupareliya, "Improving security in multi authority attribute based encryption with

fast decryption," *Procedia Computer Science*, vol. 79, pp. 632–639, 2016.

[34] H. Zhong, W. Zhu, Y. Xu, and J. Cui, "Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage," *Soft Computing*, pp. 1–9, 2016.

[35] K. Zhang, J. Ma, J. Liu, and H. Li, "Adaptively secure multi-authority attribute-based encryption with verifiable outsourced decryption," *Science China Information Sciences*, vol. 59, no. 9, pp. 99–105, 2016.