Improved Fully Adaptive Decentralized MA-ABE for NC1 from MDDH

Jie Chen[1], Qiaohan Chu[1(✉)], Ying Gao[2,3], Jianting Ning[4], and Luping Wang[5]

[1] Shanghai Key Laboratory of Trustworthy Computing, Software Engineering Institute, East China Normal University, Shanghai, China
52205902004@stu.ecnu.edu.cn
[2] School of Cyber Science and Technology, Beihang University, Beijing, China
[3] Zhongguancun Laboratory, Beijing, China
[4] College of Computer and Cyberspace Security, Fujian Normal University, Fuzhou, China
[5] School of Electronic and Information Engineering, Suzhou University of Science and Technology, Suzhou, China

Abstract. We improve the first and the only existing prime-order fully adaptively secure decentralized Multi-Authority Attribute-Based Encryption (MA-ABE) scheme for NC1 in Datta-Komargodski-Waters [Eurocrypt '23]. Compared with Datta-Komargodski-Waters, our decentralized MA-ABE scheme extra enjoys shorter parameters and meanwhile supports many-use of attribute. Shorter parameters is always the goal for Attribute-Based Encryption (ABE), and many-use of attribute is a native property of decentralized MA-ABE for NC1. Our scheme relies on the Matrix Decision Diffie-Hellman (MDDH) assumption and is in the random oracle model, as Datta-Komargodski-Waters.

Keywords: Attribute-Based Encryption · Decentralized · Fully Adaptive Security

1 Introduction

Attribute-Based Encryption (ABE) [22,36] is a public key encryption primitive that supports fine-grained access control for encrypted data. Concretely, ABE allows the encryptor to embed some attribute vector or policy into the ciphertext, and only the user who holds a secret key associated with a satisfied policy or satisfied attribute vector can decrypt the ciphertext successfully. Since the introduction of ABE, there have been plenty of works focusing on ABE, about security, efficiency, expressiveness and more [1,3,6,9,10,19–21,23,25–27,30,31,33,38,40,41].

Decentralized Multi-authority ABE. Traditional ABE requires a central authority that is in charge of generating and storing the master secret key. With

J. Guo and R. Steinfeld (Eds.): ASIACRYPT 2023, LNCS 14442, pp. 3–32, 2023.
https://doi.org/10.1007/978-981-99-8733-7_1

the master secret key, this central authority can generate any secret key and thus decrypt all the ciphertexts. Therefore, if this central authority is malicious, the security of the ABE system is destroyed. To mitigate such a trust reliance on the central authority, the notion of Multi-Authority Attribute-Based Encryption (MA-ABE) has been introduced and studied. There have been some earlier works about MA-ABE [7,8,29,32], however, these earlier works are limited in either functionality or security. Later, Lewko and Waters [28] proposed the first truly decentralized MA-ABE scheme for NC1 (it is well known that NC1 can be realized by (monotone) Linear Secret Sharing Scheme (LSSS) [4,28,33], below, we use the policy NC1 and LSSS interchangeably) in composite-order groups under the Subgroup Decision (SD) assumptions achieving adaptive security. In decentralized MA-ABE, anyone can become an authority, and each authority controls a set of attributes. Each authority generates the public keys and the master secret keys associated with the attributes he controls, and issues the corresponding secret keys to the users. Since the encryption algorithm takes as input the public keys, which are generated by different authorities, each authority cannot generate valid secret keys associated with the attributes that are not controlled by him, thus the central trust is distributed. The decryption of decentralized MA-ABE requires a user to collect the secret keys associated with the attributes that satisfy the policy embedded in the ciphertext, from a set of authorities. In decentralized MA-ABE, no global coordination is needed, except the creation of an initial set of common reference parameters, i.e., the global parameters.

Fully Adaptive Security. For the security of decentralized MA-ABE, it is required that for a challenge ciphertext, it is collusion-resistant against an arbitrary number of unauthorized secret keys, which corresponds to an arbitrary number of unauthoried secret key queries in the security game (below, we regard secret key queries as an arbitrary number of unauthorized secret key queries, by default), and is against corruptions of some authorities, which corresponds to some corruption queries in the security game. Before Datta, Komargodski, and Waters [15], the best security level of decentralized MA-ABE is against static corruption queries of some authorities (which means the corruption queries of some authorities should be made at the beginning, even before seeing any secret key), and adaptive ciphertext and secret key queries (which means the ciphertext and secret key queries can be made at any time). Recently, Datta, Komargodski, and Waters [15] proposed the first fully adaptively secure decentralized MA-ABE schemes, which are against not only adaptive ciphertext and secret key queries, but also adaptive corruption queries of some authorities (which means the corruption queries of some authorities can be made at any time).

A Sequence of Works. Subsequent to Lewko and Waters's work [28], a number of decentralized MA-ABE constructions have been proposed. Rouselakis and Waters [35] proposed a decentralized MA-ABE scheme for NC1 that improves the efficiency, but under the non-standard q-type assumption and achieving only static security. Okamoto and Takashima [34] proposed a decentralized MA-ABE

scheme for NC1 in prime-order groups under the Decision Linear (DLin) assumption [5] and achieving adaptive security. Ambrona and Gay [2] proposed decentralized MA-ABE schemes for NC1 either achieving adaptive security in the generic group model (GGM), or achieving selective security under the Symmetric External Diffie-Hellman (SXDH) assumption. Datta, Komargodski, and Waters [12] proposed the first decentralized MA-ABE scheme under the Learning With Errors (LWE) assumption, but supporting a non-trivial DNF access policy and achieving only static security. Datta, Komargodski, and Waters [13] also proposed the first decentralized MA-ABE scheme for NC1 under the standard computational or decisional bilinear Diffie-Hellman (C/DBDH) assumptions, but achieving only static security. Waters, Wee, and Wu [39] proposed a decentralized MA-ABE scheme for DNF without random oracles, under the recently-introduced evasive LWE assumption [37,42], but achieving only static security. Recently, Datta, Komargodski, and Waters [15] proposed the first decentralized MA-ABE schemes for NC1 achieving fully adaptive security, under the SD assumptions and MDDH assumption.

Many-Use of Attribute. Traditionally, pairing-based ABE for LSSS usually confronts the one-use of attribute limitation, which means that the mapping ρ of LSSS is restricted to be injective. This is because in the security analysis, we usually need the property that the master secret key $\mathbf{W}_{\rho(x)}$ is random. However, it is expected that the attribute can be used for many times, since many-use of attribute is closer to the real world in the sense that attributes are usually reused. One rescue for one-use limitation is using a simple encoding technique [26,28], but this will incur the ciphertext size growing with the policy size. Rouselakis and Waters [35] proposed a decentralized MA-ABE scheme for LSSS allowing many-use of attribute without sacrificing the ciphertext size. In [35], they use the random oracle to overcome the one-use limitation. Later, Kowalczyk and Wee [24] proposed ABE schemes for LSSS that allow many-use of attribute without sacrficing the ciphertext size. In [24], they mainly rely on a single-queried adaptively secure ABE for LSSS (which is called Core 1-ABE in [24]) to achieve many-use of attribute. Ambrona and Gay [2] also constructed decentralized MA-ABE schemes for LSSS without the one-use limitation. In [2], the one-use limitation is overcome by the underlying Identity-Based Functional Encryption scheme for inner products.

1.1 Results

We improve the first and the only existing fully adaptively secure decentralized MA-ABE scheme in prime-order groups of [15]. Concretely, our construction is almost in the same style as the construction of [15], except that

- we prove that our construction allows many-use of attribute without sacrificing the ciphertext size;

– in our construction, the dimension of the ciphertext matrix is of $2k + 1$ and the dimension of secret key matrix is of $3k$, while in the construction of [15], both the ciphertext matrix and the secret key matrix are of $3k$-dimension, where k is the parameter of the MDDH assumption.

Our construction relies on the MDDH assumption and is in the random oracle model, as [15].

We present detailed comparisons in Table 1 and Table 2.

Table 1. A comparison of current decentralized MA-ABE schemes for NC1

Scheme	Assumption	Security	Bounded Policy Size?	Many-Use?
AG21 [2]	GGM	Adaptive	No	Yes
AG21 [2]	SXDH	Selective	No	Yes
LW11 [28]	SD	Adaptive	No	No
OT20 [34]	DLin	Adaptive	No	No
RW15 [35]	q-type	Static	No	Yes
DKW21b [13]	C/DBDH	Static	Yes	No
DKW23 [15]	SD	Fully Adaptive	No	No
DKW23 [15]	MDDH	Fully Adaptive	No	No
Ours	MDDH	Fully Adaptive	No	Yes

- Adaptive security means the corruption queries are made at the beginning, but the ciphertext and secret key queries can be made adaptively; Selective security means the ciphertext and corruption queries are made before the secret key queries, while the secret key queries can be made adaptively; Static security means the ciphertext, secret key and corruption queries are made before the public key of any attribute authority is published; Fully adaptive security means the ciphertext, secret key and corruption queries can all be made adaptively.
- For "Bounded Policy Size?", "No" denotes that the corresponding scheme is not required to declare the maximal size of policy during the system setup, and "Yes" denotes that the corresponding scheme is required to declare the maximal size of policy during the system setup.
- For "Many-Use?", "No" denotes that the corresponding scheme does not allow many-use of attribute without parameter size expansion, and "Yes" denotes that the corresponding scheme allows many-use of attribute without parameter size expansion.
- All the schemes in the Table are in the random oracle model.

1.2 Technical Overview

Before we proceed to the details of our technical overview, we first provide a summary in Fig. 1 to make our approaches clear.

Table 2. A comparison of fully adaptively secure decentralized MA-ABE in prime-order groups

Scheme	$\lvert\mathsf{PK}_u\rvert$	$\lvert\mathsf{MSK}_u\rvert$	$\lvert\mathsf{CT}\rvert$	$\lvert\mathsf{sk}_{\mathsf{GID},u}\rvert$	Many-Use?
DKW23 [15]	$6k^2\lvert G_1\rvert$	$18k^2\lvert\mathbb{Z}_p\rvert$	$12k\ell\lvert G_1\rvert$	$6k\lvert G_2\rvert$	No
Ours	$6k^2\lvert G_1\rvert$	$(12k^2+6k)\lvert\mathbb{Z}_p\rvert$	$(10k\ell+2\ell)\lvert G_1\rvert$	$(4k+2)\lvert G_2\rvert$	Yes

- We omit C and the access policy $(\mathbf{M},\rho)$ in CT.
- k denotes the parameter of the MDDH assumption, and ℓ denotes the number of the rows of $\mathbf{M}$ in access policy $(\mathbf{M},\rho)$.
- We assume that each authority controls a single attribute, thus the subscripts of $\mathsf{PK}, \mathsf{MSK}$ and $\mathsf{sk}_{\mathsf{GID}}$ are all u.

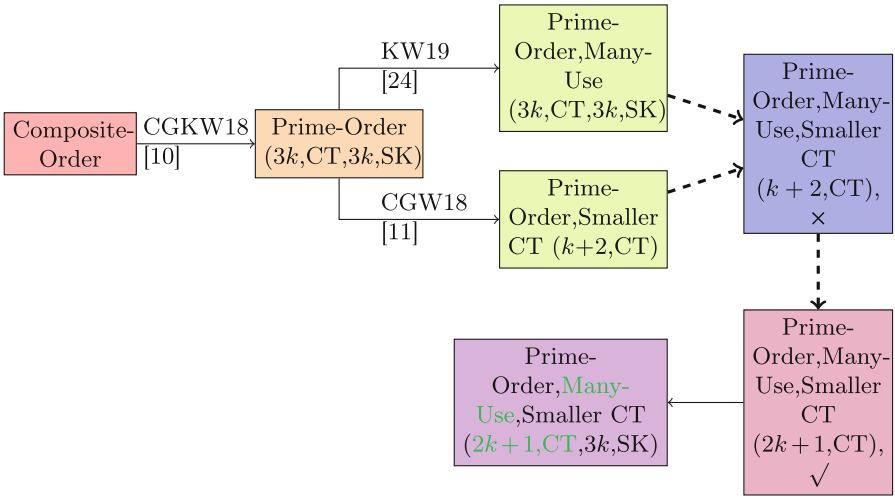

Fig. 1. Summary of our approaches. The dashed line shows an attempt, which is described in the pointed box. The cross shows that we failed in the attempt, and the check mark shows that we succeeded in the attempt. For the format like "$(2k+1$, CT, $3k$, SK)", $2k+1$ describes the matrix size of the ciphertext and $3k$ describes the matrix size of the secret key. We highlight our contributions in green (Color figure online).

Recap of Datta-Komargodski-Waters Composite-Order Decentralized MA-ABE. We start with recapping the security proofs of the composite-order decentralized MA-ABE construction in [15], which is shown in Table 3.

Observe that throughout the hybrids, three subgroups are involved, thus, for the prime-order construction, it should involve three subspaces. For CT and h, it needs the SD assumptions of "g_1 to g_{13}", and "g_1 to g_{12}", which are both based on the first subgroup g_1. For $\mathsf{H}(\mathsf{GID})$, it needs the SD assumptions of "g_{123} to g_1", "g_1 to g_{12}", "g_{12} to g_1", which are based on the first subgroup g_1, and "g_{12} to g_{123}", which is implicitly based on the second subgroup g_2, and "g_{13} to g_{123}", "g_{123} to g_{13}", which are implicitly based on the third subgroup g_3. Note that

Table 3. Hybrid sequence for the composite-order decentralized MA-ABE in [15]

Hybrid	CT	H(GID)	h	Justification
0	g_1	g_{123}	g_1	–
1	g_1	$g_1, \boxed{g_{123} \mapsto g_1}$	g_1	SD
2	$g_{13}, \boxed{g_1 \mapsto g_{13}}$	g_1	g_1	SD
3	g_{13}	g_1	g_1	Statistical
4	$g_{123}, \boxed{g_1 \mapsto g_{12}}$	g_1	g_1	SD
5:j:1	g_{123}	$g_{12}, \boxed{g_1 \mapsto g_{12}}$	g_1	SD
5:j:2	g_{123}	g_{12}	g_1	Statistical
5:j:3	g_{123}	$g_{123}, \boxed{g_{12} \mapsto g_{123}}$	g_1	SD
5:j:4	g_{123}	g_{123}	g_1	Statistical
5:(j+1)	g_{123}	$g_{13}, \boxed{g_{12} \mapsto g_1}$	g_1	SD
6	g_{123}	g_{13}	$g_{12}, \boxed{g_1 \mapsto g_{12}}$	SD
7	g_{123}	g_{13}	g_{12}	Statistical
8	g_{123}	$g_{123}, \boxed{g_{13} \mapsto g_{123}}$	g_{12}	SD
9	g_{123}	g_{123}	g_{12}	Identical
10	g_{123}	$g_{13}, \boxed{g_{123} \mapsto g_{13}}$	g_{12}	SD
11	g_{123}	g_{13}	g_{12}	Statistical
12	g_{123}	g_{13}	g_{12}	Statistical

- We use g_i to simply denote the elements in the i-th subgroup, for which i belongs to the power set of $\{1, 2, 3\}$.
- The box describes which kind of Subgroup Decision assumption is used.

for CT, the "based on" subgroup consists of only g_1, and for H(GID) and h, the (implicitly) "based on" subgroups consist of g_1, g_2 and g_3. The analysis of the "based on" subgroups is prepared for the later "horter matrix" part. Roughly speaking, the subspace corresponding to the "based on" subgroup must be of k-dimension, where k is the parameter of the MDDH assumption.

Straight-Forward Transformation from Composite-Order to Prime-Order. We transform the above composite-order construction into prime-order construction by using the framework of [10] in a straight-forward way. Let's recall the framework of [10]. In the framework, there is a correspondence as follows:

$$\begin{aligned} &\text{for } \mathsf{CT},\ g_i \mapsto [\mathbf{A}_i]_1, g_i^{s_i} \mapsto [\mathbf{s}_i \mathbf{A}_i^\top]_1, \\ &\text{for } \mathsf{H}(\mathsf{GID}) \text{ and } h,\ g_j \mapsto [\mathbf{B}_j]_2, g_j^{r_j} \mapsto [\mathbf{B}_j \mathbf{r}_j]_2, \end{aligned}$$

where $i, j \in \{1, 2, 3\}$, $\mathbf{A}_i \in \mathbb{Z}_p^{\ell'_A \times \ell_i}, \mathbf{s}_i \leftarrow_R \mathbb{Z}_p^{1 \times \ell_i}$, $\mathbf{B}_j \in \mathbb{Z}_p^{\ell'_B \times \ell_j}, \mathbf{r}_j \leftarrow_R \mathbb{Z}_p^{\ell_j \times 1}$, and $\ell'_A = \sum_i \ell_i, \ell'_B = \sum_j \ell_j$.

Naturally, as in [17,18], we would like to set $\ell_i = \ell_j = k$, for all $i, j \in \{1, 2, 3\}$, where k is the parameter of the MDDH assumption, and below we default k to

this meaning. Then, the ℓ'_A and ℓ'_B are equal to $3k$, which is the same as in the prime-order decentralized MA-ABE construction of [15].

Equipped with Many-Use of Attribute. To equip the above prime-order construction with many-use of attribute, we roughly leverage the technique in Kowalczyk and Wee's work [24]. Roughly speaking, their technique can be regarded as replacing statistical indistinguishability with computational indistinguishability. Recall that in [24], Kowalczyk and Wee first defined a single-queried ABE, called Core 1-ABE, which demonstrates the indistinguishability between the random secrets μ_0 and μ_1 of LSSS. Then they programmed the Core 1-ABE into a centralized ABE scheme, and changed the secret in the central ABE scheme into a random value. Note that in their work, the Core 1-ABE is applied into a centralized ABE, while we hope to apply it into a decentralized ABE. Fortunately, in a similar way, we can successfully program the Core 1-ABE to change the secrets in our construction. Following the technique in [24] directly, we need to set the ℓ'_A in our construction as $3k$. This is because the Core 1-ABE is based on a MDDH-based CPA-secure symmetric encryption, when changing a secret, we need a k-dimensional space to assist to program it. Since throughout the proofs, two kinds of secrets need to be changed, thus, intuitively, we need a $2k$-dimensional space. That is, the number of the columns of $\mathbf{A}_2$ and $\mathbf{A}_3$ (i.e., the ℓ_2 and ℓ_3 of "$\mathbf{A}$") should be set as k, thus, plus the number of the columns of $\mathbf{A}_1$ (i.e., the ℓ_1 of "$\mathbf{A}$"), which is k, we have $\ell'_A = 3k$. Note that this exactly matches the ℓ'_A we have set in the last section. That is, from the aspect of many-use of attribute, the ℓ'_A is $3k$, and from the aspect of straight-forward transformation in the last section, the ℓ'_A is also $3k$.

Smaller Ciphertext Matrix. Inspired by Chen, Gong, and Wee's work [11], we would like to explore whether we can improve $3k$ to a smaller dimension, like $k+2$. Recall that for ciphertext, the "based on" subgroup consists of only g_1, therefore, when transforming composite-order into prime-order, it is sufficient to set $\mathbf{A}_1 \in \mathbb{Z}_p^{(k+2)\times k}$ and $\mathbf{A}_2, \mathbf{A}_3 \in \mathbb{Z}_p^{(k+2)\times 1}$, rather than set $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3 \in \mathbb{Z}_p^{3k\times k}$, if we don't consider many-use of attribute.

Challenge: Many-Use of Attribute and Smaller Ciphertext Matrix Simultaneously. To program the Core 1-ABE, we require the ℓ_2, ℓ_3 of "$\mathbf{A}$" to be k. While, for smaller ciphertext matrix, we expect the ℓ_2, ℓ_3 of "$\mathbf{A}$" to be 1. This seems to tell us that many-use of attribute cannot coexist with smaller ciphertext matrix.

An Attempt. Our observation is that in fact, we only need one "k" matrix to help us to program the Core 1-ABE. That is, the "two kinds of secrets" can share one k-dimensional space. Then, can we use $\mathbf{A}_1$ to help us to program the Core 1-ABE and finally achieve $(k+2)$-dimensional ciphertext matrix? The answer is negative. The essential point is that the simulator can only query a proportion of the secret keys of the CPA-secure symmetric encryption, thus the simulator cannot simulate all the public keys of the decentralized MA-ABE construction.

Final Solution. The fact that gaining "k" from $\mathbf{A}_1$ cannot work suggests that we have to use another shared "k" matrix, so that we can preserve the public keys unchanged (by the orthogonality). However, to successfully program the Core 1-ABE, we need this another "k" matrix not to be orthogonal to the matrices that have existed in the ciphertext. Fortunately, when we set $\mathbf{A}_3$ as the another "k" matrix, we can successfully program the Core 1-ABE in all the related proofs (while, if we set $\mathbf{A}_2$ as the another "k" matrix, we cannot successfully program the Core 1-ABE in some proofs). Then by setting $\mathbf{A}_1, \mathbf{A}_3 \in \mathbb{Z}_p^{(2k+1)\times k}, \mathbf{A}_2 \in \mathbb{Z}_p^{(2k+1)\times 1}$, we finally achieve $(2k+1)$-dimensional ciphertext matrix and meanwhile achieve many-use of attribute.

To better demonstrate our construction, we provide a summary of the hybrid sequence of our construction in Table 4.

Table 4. Hybrid sequence for our prime-order decentralized MA-ABE

Hybrid	CT	H(GID)	h	Justification
0	$\mathbf{A}_1$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$	$\mathbf{B}_1$	-
1	$\mathbf{A}_1$	$\mathbf{B}_1$, $\boxed{\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3 \mapsto \mathbf{B}_1}$	$\mathbf{B}_1$	MDDH
2	$\mathbf{A}_1, \mathbf{A}_3$, $\boxed{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{A}_3}$	$\mathbf{B}_1$	$\mathbf{B}_1$	MDDH
3	$\mathbf{A}_1, \mathbf{A}_3$	$\mathbf{B}_1$	$\mathbf{B}_1$	Core 1-ABE
4	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$, $\boxed{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{A}_2}$	$\mathbf{B}_1$	$\mathbf{B}_1$	MDDH
5:j:1	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_2$, $\boxed{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_2}$	$\mathbf{B}_1$	MDDH
5:j:2	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_2$	$\mathbf{B}_1$	Core 1-ABE
5:j:3	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$, $\boxed{\mathbf{B}_2 \mapsto \mathbf{B}_2, \mathbf{B}_3}$	$\mathbf{B}_1$	MDDH
5:j:4	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$	$\mathbf{B}_1$	Core 1-ABE
5:(j+1)	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_3$, $\boxed{\mathbf{B}_1, \mathbf{B}_2 \mapsto \mathbf{B}_1}$	$\mathbf{B}_1$	MDDH
6	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_3$	$\mathbf{B}_1, \mathbf{B}_2$, $\boxed{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_2}$	MDDH
7	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_3$	$\mathbf{B}_1, \mathbf{B}_2$	Core 1-ABE
8	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$, $\boxed{\mathbf{B}_3 \mapsto \mathbf{B}_2, \mathbf{B}_3}$	$\mathbf{B}_1, \mathbf{B}_2$	MDDH
9	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$	$\mathbf{B}_1, \mathbf{B}_2$	Identical
10	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_3$, $\boxed{\mathbf{B}_2, \mathbf{B}_3 \mapsto \mathbf{B}_3}$	$\mathbf{B}_1, \mathbf{B}_2$	MDDH
11	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_3$	$\mathbf{B}_1, \mathbf{B}_2$	Core 1-ABE
12	$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$	$\mathbf{B}_1, \mathbf{B}_3$	$\mathbf{B}_1, \mathbf{B}_2$	Statistical

- We use $\mathbf{A}_1 \in \mathbb{Z}_p^{(2k+1)\times k}, \mathbf{A}_2 \in \mathbb{Z}_p^{(2k+1)\times 1}, \mathbf{A}_3 \in \mathbb{Z}_p^{(2k+1)\times k}$ and $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3 \in \mathbb{Z}_p^{3k\times k}$ to denote the subspaces in CT and the subspaces in $\mathsf{H}(\mathsf{GID}), h$, respectively.
- The box describes the transition of the subspaces.

2 Preliminaries

2.1 Notations

We use $\leftarrow_R$ to denote random sampling, and use $\|$ to denote concatenation of matrices. For an integer N, we use $[N]$ to denote the set $\{1, ..., N\}$. We use $\equiv$ to denote two distributions being identically indistinguishable. For a matrix $\mathbf{A}$, we use $\mathsf{span}(\mathbf{A})$ to denote the column span of $\mathbf{A}$ and use $\mathsf{basis}(\mathbf{A})$ to denote a basis of $\mathsf{span}(\mathbf{A})$. We use $\mathbf{I}$ to denote an identity matrix of proper size, and use $\mathbf{0}$ to denote a zero matrix of proper size.

2.2 Prime-Order Bilinear Groups

A prime-order group generator $\mathcal{G}$ takes as input the security parameter λ in unary notation and outputs a description $\mathbb{G} = (p, G_1, G_2, G_T, e)$, where p is a prime, G_1, G_2, G_T are cyclic groups of order p, and $e : G_1 \times G_2 \to G_T$ is an asymmetric non-degenerated bilinear mapping. Let $[1]_1 = g_1 \in G_1, [1]_2 = g_2 \in G_2$ and $[1]_T = g_T = e(g_1, g_2) \in G_T$ be the respective generators. For any $a, b \in \mathbb{Z}_p$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} = g_T^{ab} = [ab]_T$. We define $[\mathbf{M}]_1 = g_1^{\mathbf{M}}, [\mathbf{M}]_2 = g_2^{\mathbf{M}}$ and $[\mathbf{M}]_T = g_T^{\mathbf{M}}$, where $\mathbf{M}$ is a matrix over $\mathbb{Z}_p$, and exponentiation is carried out component-wise. We also define $e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{AB}]_T$, where $\mathbf{A}, \mathbf{B}$ are matrices over $\mathbb{Z}_p$.

2.3 Basis Structure

Fix parameters $\ell_1, \ell_2, \ell_3 \geq 1$. Sample

$$\mathbf{A}_1 \leftarrow_R \mathbb{Z}_p^{\ell' \times \ell_1}, \mathbf{A}_2 \leftarrow_R \mathbb{Z}_p^{\ell' \times \ell_2}, \mathbf{A}_3 \leftarrow_R \mathbb{Z}_p^{\ell' \times \ell_3},$$

where $\ell' := \ell_1 + \ell_2 + \ell_3$. Let $(\mathbf{A}_1^{\parallel} \| \mathbf{A}_2^{\parallel} \| \mathbf{A}_3^{\parallel})^\top$ denote the inverse of $(\mathbf{A}_1 \| \mathbf{A}_2 \| \mathbf{A}_3)$, so that $\mathbf{A}_i^\top \mathbf{A}_i^{\parallel} = \mathbf{I}$ (known as non-degeneracy) and $\mathbf{A}_i^\top \mathbf{A}_j^{\parallel} = \mathbf{0}$ if $i \neq j$ (known as orthogonality), as depicted in Fig. 2.

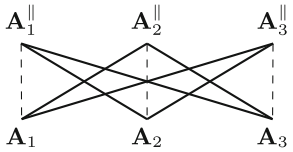

Fig. 2. Basis relations. Solid lines mean orthogonal, dashed lines mean non-degeneracy. Similar relations hold in composite-order groups.

By symmetry, we can permute the indexes for $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$.

2.4 Assumptions

Matrix Decision Diffie-Hellman Assumption. Let $k, l, d \in \mathbb{N}$. The Matrix Decision Diffie-Hellman (MDDH) assumption [16] says that for all p.p.t adversaries $\mathcal{A}$, the following advantage function is negligible in λ:

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{MDDH}^d_{k,l}}(\lambda) := |\mathsf{Pr}[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{MS}]_1) = 1] - \mathsf{Pr}[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{U}]_1) = 1]|,$$

where $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda), \mathbf{M} \leftarrow_R \mathbb{Z}_p^{l\times k}, \mathbf{S} \leftarrow_R \mathbb{Z}_p^{k\times d}$, and $\mathbf{U} \leftarrow_R \mathbb{Z}_p^{l\times d}$.

MDDH assumption also holds similarly in G_2.

Lemma 1 ($\mathbf{MDDH}_{\ell_1\to\ell_1+\ell_2} \Longrightarrow SD^{G_1}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_2}$). *Under the $MDDH_{\ell_1,\ell_1+\ell_2}$ assumption in G_1, there exists an efficient sampler outputting random $([\mathbf{A}_1]_1, [\mathbf{A}_2]_1, [\mathbf{A}_3]_1)$ (as described in Sect. 2.3) along with base $\mathsf{basis}(\mathbf{A}_1^{\parallel}), \mathsf{basis}(\mathbf{A}_3^{\parallel}), \mathsf{basis}(\mathbf{A}_1^{\parallel}, \mathbf{A}_2^{\parallel})$ (of arbitrary choice) such that the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{SD^{G_1}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_2}}(\lambda) := |\mathsf{Pr}[\mathcal{A}(D, [T_0]_1) = 1] - \mathsf{Pr}[\mathcal{A}(D, [T_1]_1) = 1]|,$$

where

$$D := ([\mathbf{A}_1]_1, [\mathbf{A}_2]_1, [\mathbf{A}_3]_1, \mathsf{basis}(\mathbf{A}_1^{\parallel}), \mathsf{basis}(\mathbf{A}_3^{\parallel}), \mathsf{basis}(\mathbf{A}_1^{\parallel}, \mathbf{A}_2^{\parallel})),$$
$$T_0 \leftarrow_R \mathsf{span}(\mathbf{A}_1), T_1 \leftarrow_R \mathsf{span}(\mathbf{A}_1, \mathbf{A}_2).$$

Remark 1. Lemma 1 is similarly stated in [10,11,17,18], and similar lemma also holds in G_2.

2.5 Decentralized Multi-authority Attribute-Based Encryption for LSSS

Syntax. We assume that each authority controls a single attribute. A decentralized Multi-Authority Attribute-Based Encryption scheme for Linear Secret Sharing Scheme consists of five efficient algorithms:

- $\mathsf{GlobalSetup}(1^\lambda) \to \mathsf{GP}$: The global setup algorithm takes as input the security parameter λ in unary notation, and outputs the global parameters GP for the system.
- $\mathsf{AuthSetup}(\mathsf{GP}, u \in \mathcal{AU}) \to (\mathsf{PK}_u, \mathsf{MSK}_u)$: The authority setup algorithm takes as input the global parameters GP and an attribute $u \in \mathcal{AU}$, where $\mathcal{AU}$ is the universe of attributes, and outputs the public key PK_u of u as well as the master secret key MSK_u of u.
- $\mathsf{Enc}(\mathsf{GP}, msg, (\mathbf{M}, \rho), \{\mathsf{PK}_{u'}\}_{u'\in\rho([\ell])}) \to \mathsf{CT}$: The encryption algorithm takes as input the global parameters GP, a message $msg \in \mathbb{M}$, where $\mathbb{M}$ is the message space, an LSSS access policy $(\mathbf{M}, \rho)$ in which ρ maps each row of $\mathbf{M}$ to an attribute in $\mathcal{AU}$, and the public keys set $\{\mathsf{PK}_{u'}\}_{u'\in\rho([\ell])}$ for all the attributes in the range of ρ on the constraint of $[\ell]$. Then output a ciphertext CT.

- $\mathsf{KeyGen}(\mathsf{GP}, \mathsf{GID}, \mathsf{MSK}_u) \to \mathsf{sk}_{\mathsf{GID},u}$: The key generation algorithm takes as input the global parameters GP, a user's global identifier $\mathsf{GID} \in \mathcal{GID}$, where $\mathcal{GID}$ is the universe of global identifiers, and a master secret key of attribute $u \in \mathcal{AU}$. Then output a secret key of GID and u.
- $\mathsf{Dec}(\mathsf{GP}, \mathsf{CT}, \{\mathsf{sk}_{\mathsf{GID},u''}\}_{u'' \in \mathcal{U}}) \to msg' / \perp$: The decryption algorithm takes as input the global parameters GP, a ciphertext CT and a collection of secret keys $\{\mathsf{sk}_{\mathsf{GID},u''}\}_{u'' \in \mathcal{U}}$ of the user ID-attribute pairs $\{(\mathsf{GID}, u'')\}$ possessed by a user with global identifier GID, and $u'' \in \mathcal{U} \subseteq \mathcal{AU}$, where $\mathcal{U}$ is a subset of $\mathcal{AU}$. Then output a message msg', or $\perp$.

Correctness. A decentralized MA-ABE scheme for LSSS is correct, if for all $\lambda \in \mathbb{N}$, $msg \in \mathbb{M}$, $\mathsf{GID} \in \mathcal{GID}$, LSSS access policy $(\mathbf{M}, \rho)$, and $\mathcal{U} \subseteq \mathcal{AU}$ containing attributes that satisfy the LSSS access structure, we have

$$\mathsf{Pr}\left[msg' = msg \;\middle|\; \begin{array}{l} \mathsf{GP} \leftarrow \mathsf{GlobalSetup}(1^\lambda); \\ \forall u \in \mathcal{AU}, \mathsf{PK}_u, \mathsf{MSK}_u \leftarrow \mathsf{AuthSetup}(\mathsf{GP}, u); \\ \mathsf{CT} \leftarrow \mathsf{Enc}(\mathsf{GP}, msg, (\mathbf{M}, \rho), \{\mathsf{PK}_{u'}\}_{u' \in \rho([\ell])}); \\ \forall u'' \in \mathcal{U}, \mathsf{sk}_{\mathsf{GID},u''} \leftarrow \mathsf{KeyGen}(\mathsf{GP}, \mathsf{GID}, \mathsf{MSK}_{u''}); \\ msg' = \mathsf{Dec}(\mathsf{GP}, \mathsf{CT}, \{\mathsf{sk}_{\mathsf{GID},u''}\}_{u'' \in \mathcal{U}}); \end{array} \right] = 1.$$

Fully Adaptive Security. For a stateful adversary $\mathcal{A}$, define the advantage function $\mathsf{Adv}_{\mathcal{A}}^{\text{MA-ABE}}(\lambda) :=$

$$\mathsf{Pr}\left[b' = b \;\middle|\; \begin{array}{l} \mathsf{GP} \leftarrow \mathsf{GlobalSetup}(1^\lambda); \\ \forall u \in \mathcal{AU}, \mathsf{PK}_u, \mathsf{MSK}_u \leftarrow \mathsf{AuthSetup}(\mathsf{GP}, u); \\ ((\mathbf{M}, \rho), msg_0, msg_1) \leftarrow \\ \mathcal{A}^{\mathsf{AuthSetup}(\mathsf{GP},\cdot),\mathsf{KeyGen}(\mathsf{GP},\cdot,\mathsf{MSK}_u)}(\mathsf{GP}, \{\mathsf{PK}_u\}_{u \in \mathcal{AU}}); \\ b \leftarrow_R \{0,1\}; \\ \mathsf{CT}_b \leftarrow \mathsf{Enc}(\mathsf{GP}, msg_b, (\mathbf{M}, \rho), \{\mathsf{PK}_{u'}\}_{u' \in \rho([\ell])}); \\ b' \leftarrow \mathcal{A}^{\mathsf{AuthSetup}(\mathsf{GP},\cdot),\mathsf{KeyGen}(\mathsf{GP},\cdot,\mathsf{MSK}_u)}(\mathsf{GP}, \{\mathsf{PK}_u\}_{u \in \mathcal{AU}}, \mathsf{CT}_b); \end{array} \right] - \frac{1}{2},$$

where $\mathsf{AuthSetup}(\mathsf{GP}, \cdot)$ denotes that $\mathcal{A}$ can make authority setup queries and authority master key queries adaptively, and $\mathsf{KeyGen}(\mathsf{GP}, \cdot, \mathsf{MSK}_u)$ denotes that $\mathcal{A}$ can make secret key queries adaptively, with the restriction that all the information that $\mathcal{A}$ gets from the queries cannot make $\mathcal{A}$ decrypt the challenge ciphertext CT_b successfully by following a legitimate decryption process. A decentralized MA-ABE scheme is fully adaptively secure, if for all $\mathsf{p.p.t}$ adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\text{MA-ABE}}(\lambda)$ is a negligible function in λ.

Many-Use of Attribute. If the mapping ρ in the LSSS access policy $(\mathbf{M}, \rho)$ is not restricted to be an injective mapping, then we say the attributes in $\mathcal{AU}$ can be used for many times, i.e., many-use of attribute.

Core 1-ABE. Core 1-ABE is defined in [24]. For a stateful adversary $\mathcal{A}$, define the advantage function $\mathsf{Adv}^{\text{1-ABE}}_{\mathcal{A}}(\lambda) :=$

$$\mathsf{Pr}\left[b' = b \;\middle|\; \begin{array}{l} \mathbf{w}_i \leftarrow \mathsf{CPA.Setup}(1^\lambda); \\ (\mu_0, \mu_1) \leftarrow \mathcal{A}^{\mathcal{O}_X(\cdot), \mathcal{O}_E(\cdot,\cdot)}; \\ b \leftarrow_R \{0,1\}; \\ \mathsf{ct}_b \leftarrow \mathcal{O}_F((f, \mu_b)); \\ b' \leftarrow \mathcal{A}^{\mathcal{O}_X(\cdot), \mathcal{O}_E(\cdot,\cdot)}(\mathsf{ct}_b); \end{array}\right] - \frac{1}{2},$$

where $\mathcal{O}_F((f, \mu_b)) = \mathsf{ct} := \{\mathsf{sk}'_f = \{\mu_j\}_{\rho'(j)=0} \cup \{\mathsf{CPA.Enc}(\mathbf{w}_{\rho'(j)}, \mu_j)\}_{\rho'(j)\neq 0}\}$, $(\{\mu_j\}, \rho') \leftarrow \mathsf{share}(f, \mu_b)$, and $\mathcal{O}_X(x) := (\mathsf{ct}'_x = \{\mathbf{w}_i\}_{x_i=1})$, and $\mathcal{O}_E(i, m) := \mathsf{CPA.Enc}(\mathbf{w}_i, m)$, with the restriction that (i) only one query is made to each $\mathcal{O}_F(\cdot)$ and $\mathcal{O}_X(\cdot)$, and (ii) the queries f and x to $\mathcal{O}_F(\cdot), \mathcal{O}_X(\cdot)$ respectively, satisfy $f(x) = 0$.

The CPA-secure symmetric encryption scheme in [24] is constructed as follows:

- $\mathsf{CPA.Setup}(1^\lambda)$: Run $\mathbb{G} \leftarrow \mathcal{G}(1^\lambda)$. Sample $\mathbf{w} \leftarrow_R \mathbb{Z}_p^{1\times k}$. Output $\mathsf{sk} = \mathbf{w}$.
- $\mathsf{CPA.Enc}(\mathsf{sk}, [M]_2)$: Sample $\mathbf{r} \leftarrow_R \mathbb{Z}_p^{k\times 1}$. Output $(ct_1, ct_2) = ([M + \mathbf{wr}]_2, [\mathbf{r}]_2)$.
- $\mathsf{CPA.Dec}(\mathsf{sk}, (ct_1, ct_2))$: Output $ct_1 \cdot (\mathsf{sk} \cdot ct_2)^{-1}$.

The correctness follows that $ct_1 \cdot (\mathsf{sk} \cdot ct_2)^{-1} = [M + \mathbf{wr} - \mathbf{wr}]_2 = [M]_2$.

In [24], $\mathsf{Adv}^{\text{1-ABE}}_{\mathcal{A}}(\lambda)$ is proved to be a negligible function in λ under the MDDH assumption.

3 Decentralized MA-ABE in Prime-Order Groups

We assume that each authority controls a single attribute. The hash function H is modeled as a random oracle in the security analysis.

3.1 Construction

- $\mathsf{GlobalSetup}(1^\lambda)$: Take as input the security parameter λ in unary notation. Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. We use a strong seeded randomness extractor $\mathsf{Ext} : G_T \times \mathsf{S} \to \mathbb{M}$, where $\mathbb{M} \subset \{0,1\}^*$ is the message space and $\mathsf{S} \subset \{0,1\}^*$ is the seed space. Sample $\mathsf{seed} \leftarrow_R \mathsf{S}, \mathbf{A}_1 \leftarrow_R \mathbb{Z}_p^{(2k+1)\times k}, \mathbf{B}_1 \leftarrow_R \mathbb{Z}_p^{3k\times k}, \mathbf{r} \leftarrow_R \mathbb{Z}_p^{k\times 1}$. We also use a hash function $\mathsf{H} : \{0,1\}^* \to G_2^{3k\times 1}$, which maps global identifier $\mathsf{GID} \in \mathcal{GID} \subset \{0,1\}^*$ to elements in $G_2^{3k\times 1}$, where $\mathcal{GID}$ is the universe of global identifiers. Concretely, for a $\mathsf{GID} \in \mathcal{GID}$, $\mathsf{H}(\mathsf{GID}) = [\mathbf{h}_{\mathsf{GID}}]_2$, where $\mathbf{h}_{\mathsf{GID}} \leftarrow_R \mathbb{Z}_p^{3k\times 1}$. Output $\mathsf{GP} = (\mathbb{G}, [\mathbf{A}_1]_1, h = [\mathbf{B}_1\mathbf{r}]_2, \mathsf{seed})$.
- $\mathsf{AuthSetup}(\mathsf{GP}, u \in \mathcal{AU})$: Take as input GP and an attribute $u \in \mathcal{AU}$, where $\mathcal{AU}$ is the universe of attributes. Sample $\mathbf{W}_{A,u}, \mathbf{W}_{B,u} \leftarrow_R \mathbb{Z}_p^{(2k+1)\times 3k}$. Output

$$\mathsf{PK}_u = ([P_{A,u}]_1 = [\mathbf{A}_1^\top \mathbf{W}_{A,u}]_1, [P_{B,u}]_1 = [\mathbf{A}_1^\top \mathbf{W}_{B,u}]_1),$$
$$\mathsf{MSK}_u = (\mathbf{W}_{A,u}, \mathbf{W}_{B,u}).$$

– $\mathsf{Enc}(\mathsf{GP}, msg, (\mathbf{M} \in \mathbb{Z}_p^{\ell \times d}, \rho : [\ell] \to \mathcal{AU}), \{\mathsf{PK}_{u'}\}_{u' \in \rho([\ell])})$: Take as input GP, the message msg, an LSSS access structure $(\mathbf{M} \in \mathbb{Z}_p^{\ell \times d}, \rho : [\ell] \to \mathcal{AU})$, and the public keys $\{\mathsf{PK}_{u'}\}_{u' \in \rho([\ell])}$ used for encryption. Sample

$$\mathbf{K} \leftarrow_R \mathbb{Z}_p^{1\times 3k}, \mathbf{K}'_A \leftarrow_R \mathbb{Z}_p^{(d-1)\times 3k}, \mathbf{K}'_B \leftarrow_R \mathbb{Z}_p^{(d-1)\times 3k},$$
$$\mathbf{s}_{A,x}, \mathbf{s}_{B,x} \leftarrow_R \mathbb{Z}_p^{1\times k}.$$

Output $\mathsf{CT} = ((\mathbf{M}, \rho), C, \{C_{1,A,x}, C_{1,B,x}, C_{2,A,x}, C_{2,B,x}\}_{x\in[\ell]})$, where

$$\begin{aligned}
C &= msg \oplus \mathsf{Ext}(e([\mathbf{K}]_1, h), \mathsf{seed}),\\
C_{1,A,x} &= [\mathbf{s}_{A,x}\mathbf{A}_1^\top]_1,\\
C_{1,B,x} &= [\mathbf{s}_{B,x}\mathbf{A}_1^\top]_1,\\
C_{2,A,x} &= [\mathbf{s}_{A,x}\mathbf{A}_1^\top \mathbf{W}_{A,\rho(x)} + \mathbf{M}_x \begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix}]_1,\\
C_{2,B,x} &= [\mathbf{s}_{B,x}\mathbf{A}_1^\top \mathbf{W}_{B,\rho(x)} + \mathbf{M}_x \begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix}]_1,
\end{aligned}$$

and $\mathbf{M}_x$ denotes the x-th row of $\mathbf{M}$.

– $\mathsf{KeyGen}(\mathsf{GP}, \mathsf{H}, \mathsf{GID} \in \mathcal{GID}, \mathsf{MSK}_u)$: Take as input $\mathsf{GP}, \mathsf{H}, \mathsf{GID} \in \mathcal{GID}, \mathsf{MSK}_u$. Output $\mathsf{sk}_{\mathsf{GID},u} = (K_{\mathsf{GID},A,u}, K_{\mathsf{GID},B,u})$, where

$$\begin{aligned}
K_{\mathsf{GID},A,u} &= [\mathbf{W}_{A,u}\mathbf{h}_{\mathsf{GID}} + \mathbf{W}_{A,u}\mathbf{B}_1\mathbf{r}]_2,\\
K_{\mathsf{GID},B,u} &= [\mathbf{W}_{B,u}\mathbf{h}_{\mathsf{GID}}]_2.
\end{aligned}$$

– $\mathsf{Dec}(\mathsf{GP}, \mathsf{H}, \mathsf{CT}, \mathsf{GID}, \{\mathsf{sk}_{\mathsf{GID},u''}\}_{u''\in\rho(\mathbf{I})})$: Compute $\{\omega_x \in \mathbb{Z}_p\}_{x\in\mathbf{I}}$, such that $\sum_{x\in\mathbf{I}} \omega_x \cdot \mathbf{M}_x = (1, 0, ..., 0)$. Then compute

$$\begin{aligned}
D_{A,x} &= e(C_{2,A,x}, \mathsf{H}(\mathsf{GID}) \cdot h) \cdot e(C_{1,A,x}, K_{\mathsf{GID},A,\rho(x)})^{-1},\\
D_{B,x} &= e(C_{2,B,x}, \mathsf{H}(\mathsf{GID})) \cdot e(C_{1,B,x}, K_{\mathsf{GID},B,\rho(x)})^{-1}.
\end{aligned}$$

And compute

$$D = \prod_{x\in\mathbf{I}} (D_{A,x} \cdot D_{B,x})^{\omega_x}.$$

Output

$$C \oplus \mathsf{Ext}(D, \mathsf{seed}).$$

Correctness. We have

$$\begin{aligned}
D_{A,x} =& e(C_{2,A,x}, \mathsf{H}(\mathsf{GID}) \cdot h) \cdot e(C_{1,A,x}, K_{\mathsf{GID},A,\rho(x)})^{-1} \\
=& e([\mathbf{s}_{A,x}\mathbf{A}_1^\top \mathbf{W}_{A,\rho(x)} + \mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix}]_1, [\mathbf{h}_{\mathsf{GID}} + \mathbf{B}_1\mathbf{r}]_2) \cdot \\
& e([\mathbf{s}_{A,x}\mathbf{A}_1^\top]_1, [\mathbf{W}_{A,\rho(x)}\mathbf{h}_{\mathsf{GID}} + \mathbf{W}_{A,\rho(x)}\mathbf{B}_1\mathbf{r}]_2)^{-1} \\
=& [\mathbf{s}_{A,x}\mathbf{A}_1^\top \mathbf{W}_{A,\rho(x)}\mathbf{h}_{\mathsf{GID}} + \mathbf{s}_{A,x}\mathbf{A}_1^\top \mathbf{W}_{A,\rho(x)}\mathbf{B}_1\mathbf{r} + \mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix} \mathbf{h}_{\mathsf{GID}} + \\
& \mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix} \mathbf{B}_1\mathbf{r} - \mathbf{s}_{A,x}\mathbf{A}_1^\top \mathbf{W}_{A,\rho(x)}\mathbf{h}_{\mathsf{GID}} - \mathbf{s}_{A,x}\mathbf{A}_1^\top \mathbf{W}_{A,\rho(x)}\mathbf{B}_1\mathbf{r}]_T \\
=& [\mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix} \mathbf{h}_{\mathsf{GID}} + \mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix} \mathbf{B}_1\mathbf{r}]_T,
\end{aligned}$$

and

$$\begin{aligned}
D_{B,x} =& e(C_{2,B,x}, \mathsf{H}(\mathsf{GID})) \cdot e(C_{1,B,x}, K_{\mathsf{GID},B,\rho(x)})^{-1} \\
=& e([\mathbf{s}_{B,x}\mathbf{A}_1^\top \mathbf{W}_{B,\rho(x)} + \mathbf{M}_x \begin{pmatrix} -\mathbf{K} \\ \mathbf{K}'_B \end{pmatrix}]_1, [\mathbf{h}_{\mathsf{GID}}]_2) \cdot \\
& e([\mathbf{s}_{B,x}\mathbf{A}_1^\top]_1, [\mathbf{W}_{B,\rho(x)}\mathbf{h}_{\mathsf{GID}}]_2)^{-1} \\
=& [\mathbf{s}_{B,x}\mathbf{A}_1^\top \mathbf{W}_{B,\rho(x)}\mathbf{h}_{\mathsf{GID}} + \mathbf{M}_x \begin{pmatrix} -\mathbf{K} \\ \mathbf{K}'_B \end{pmatrix} \mathbf{h}_{\mathsf{GID}} - \mathbf{s}_{B,x}\mathbf{A}_1^\top \mathbf{W}_{B,\rho(x)}\mathbf{h}_{\mathsf{GID}}]_T \\
=& [\mathbf{M}_x \begin{pmatrix} -\mathbf{K} \\ \mathbf{K}'_B \end{pmatrix} \mathbf{h}_{\mathsf{GID}}]_T.
\end{aligned}$$

Then if $\sum_{x\in\mathbf{I}} \omega_x \cdot \mathbf{M}_x = (1, 0, ..., 0)$, we have

$$\begin{aligned}
D =& \prod_{x\in\mathbf{I}} (D_{A,x} \cdot D_{B,x})^{\omega_x} \\
=& \prod_{x\in\mathbf{I}} [\omega_x \mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix} \mathbf{h}_{\mathsf{GID}} + \omega_x \mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix} \mathbf{B}_1\mathbf{r} + \omega_x \mathbf{M}_x \begin{pmatrix} -\mathbf{K} \\ \mathbf{K}'_B \end{pmatrix} \mathbf{h}_{\mathsf{GID}}]_T \\
=& [\mathbf{K}\mathbf{B}_1\mathbf{r}]_T \\
=& e([\mathbf{K}]_1, [\mathbf{B}_1\mathbf{r}]_2) \\
=& e([\mathbf{K}]_1, h).
\end{aligned}$$

3.2 Security Analysis

Theorem 1. *The above decentralized MA-ABE scheme for NC1 is fully adaptively secure and allows many-use of attribute, under the MDDH assumption in the random oracle model. Moreover, we have*

$$\begin{aligned}\mathsf{Adv}_{\mathcal{A}}^{MA\text{-}ABE}(\lambda) \leq & \mathsf{Adv}_{\mathcal{B}^1}^{MDDH^q_{G_2,k,3k}}(\lambda) + \mathsf{Adv}_{\mathcal{B}^2}^{SD^{G_1}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_3}}(\lambda) + \mathsf{Adv}_{\mathcal{B}^3}^{SD^{G_1}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_2}}(\lambda) \\ & + (2q+1)\cdot \mathsf{Adv}_{\mathcal{B}^4}^{SD^{G_2}_{\mathbf{B}_1\mapsto\mathbf{B}_1,\mathbf{B}_2}}(\lambda) + q\cdot \mathsf{Adv}_{\mathcal{B}^5}^{SD^{G_2}_{\mathbf{B}_2\mapsto\mathbf{B}_2,\mathbf{B}_3}}(\lambda) \\ & + 2\cdot \mathsf{Adv}_{\mathcal{B}^6}^{SD^{G_2}_{\mathbf{B}_3\mapsto\mathbf{B}_2,\mathbf{B}_3}}(\lambda) + (4q+4)\cdot \mathsf{Adv}_{\mathcal{B}^7}^{1\text{-}ABE}(\lambda) + \mathsf{negl}(\lambda),\end{aligned}$$

where q is the total number of global identifiers GID *that the simulator generates the* H *oracle outputs for, $\mathcal{B}^1$ is a* p.p.t *adversary for the $MDDH^q_{k,3k}$ assumption in G_2, $\mathcal{B}^2$ is a* p.p.t *adversary for the $SD_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_3}$ assumption in G_1, $\mathcal{B}^3$ is a* p.p.t *adversary for the $SD_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_2}$ assumption in G_1, $\mathcal{B}^4$ is a* p.p.t *adversary for the $SD_{\mathbf{B}_1\mapsto\mathbf{B}_1,\mathbf{B}_2}$ assumption in G_2, $\mathcal{B}^5$ is a* p.p.t *adversary for the $SD_{\mathbf{B}_2\mapsto\mathbf{B}_2,\mathbf{B}_3}$ assumption in G_2, $\mathcal{B}^6$ is a* p.p.t *adversary for the $SD_{\mathbf{B}_3\mapsto\mathbf{B}_2,\mathbf{B}_3}$ assumption in G_2, $\mathcal{B}^7$ is a* p.p.t *adversary for the Core 1-ABE, which is based on the MDDH assumption and with polynomial security loss, and* $\mathsf{negl}(\lambda)$ *is a negligible function in λ incurred by a statistical indistinguishability from* Ext.

Hybrids. Before we proceed to the details of security analysis, we clarify some notations and explain some complicated points.

Notations. In the security analysis, we set

$$\begin{aligned}&\mathbf{A}_1 \leftarrow_R \mathbb{Z}_p^{(2k+1)\times k}, \mathbf{A}_2 \leftarrow_R \mathbb{Z}_p^{(2k+1)\times 1}, \mathbf{A}_3 \leftarrow_R \mathbb{Z}_p^{(2k+1)\times k},\\ &\mathbf{A}_1^{\parallel} \leftarrow_R \mathbb{Z}_p^{(2k+1)\times k}, \mathbf{A}_2^{\parallel} \leftarrow_R \mathbb{Z}_p^{(2k+1)\times 1}, \mathbf{A}_3^{\parallel} \leftarrow_R \mathbb{Z}_p^{(2k+1)\times k},\\ &\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3 \leftarrow_R \mathbb{Z}_p^{3k\times k},\\ &\mathbf{B}_1^{\parallel}, \mathbf{B}_2^{\parallel}, \mathbf{B}_3^{\parallel} \leftarrow_R \mathbb{Z}_p^{3k\times k},\end{aligned}$$

which satisfy the basis structure in Sect. 2.3, respectively.

Let Y denote the subset of rows of the challenge access matrix $\mathbf{M}$ labeled by the authorities for which $\mathcal{A}$ supplies the authority public keys $\{\mathsf{PK}_{u'} = ([P_{A,u'}]_1, [P_{B,u'}]_1)\}$. Let $\bar{Y} = [\ell]\backslash Y$.

Below, we use $\mathsf{Reconstruct}(\{\mathsf{share}_i\})$ to denote the secret from the reconstruction of shares $\{\mathsf{share}_i\}$.

Sampling of Secrets. This statement is similarly stated in Lemma 4.3 of [14]. Recall that we require the information $\mathcal{A}$ gain from the corruption and secret key queries cannot help $\mathcal{A}$ decrypt the challenge ciphertext CT_b successfully following a legitimate decryption process. For the form of the secret $\mathbf{K}$, this means that there must exist a vector $\mathbf{u} \in \mathbb{Z}_p^d$ such that $\mathbf{u}$ is orthogonal to all the rows of $\mathbf{M}$ labeled by corrupted authorities, but is not orthogonal to $(1, 0, ..., 0)$, i.e., the first entry of $\mathbf{u}$ is non-zero, and the truly secret values of $\mathbf{K}$ are attached to $\mathbf{u}$. Concretely, consider a basis $\mathbb{U}$ of $\mathbb{Z}_p^d$ involving the vector $\mathbf{u}$, set

$$\mathbf{v}_A^{'(1)} = \widehat{\mathbf{v}_A}^{(1)} + a_1\mathbf{u},$$
$$\vdots$$
$$\mathbf{v}_A^{'(3k)} = \widehat{\mathbf{v}_A}^{(3k)} + a_{3k}\mathbf{u},$$

where for each $i \in [3k]$, $\widehat{\mathbf{v}_A}^{(i)}$ is in the span of $\mathbb{U}\backslash\{\mathbf{u}\}$, and $a_i \leftarrow_R \mathbb{Z}_p$ is the truly secret value of $\mathbf{K}$. Set

$$\begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix} = \begin{pmatrix} \mathbf{v}_A^{'(1)} \\ \vdots \\ \mathbf{v}_A^{'(3k)} \end{pmatrix}^\top.$$

Then we have $\mathbf{K} = (\widehat{\mathbf{v}_A}_1^{(1)}, ..., \widehat{\mathbf{v}_A}_1^{(3k)}) + (a_1u_1, ..., a_{3k}u_1) \in \mathbb{Z}_p^{1\times 3k}$.

Similarly, we can set

$$\mathbf{v}_B^{'(1)} = \widehat{\mathbf{v}_B}^{(1)} - a_1\mathbf{u},$$
$$\vdots$$
$$\mathbf{v}_B^{'(3k)} = \widehat{\mathbf{v}_B}^{(3k)} - a_{3k}\mathbf{u},$$

and set

$$\begin{pmatrix} -\mathbf{K} \\ \mathbf{K}'_B \end{pmatrix} = \begin{pmatrix} \mathbf{v}_B^{'(1)} \\ \vdots \\ \mathbf{v}_B^{'(3k)} \end{pmatrix}^\top,$$

where

$$\widehat{\mathbf{v}_B}_1^{(1)} = -\widehat{\mathbf{v}_A}_1^{(1)},$$
$$\vdots$$
$$\widehat{\mathbf{v}_B}_1^{(3k)} = -\widehat{\mathbf{v}_A}_1^{(3k)},$$

and for each $i \in [3k]$, $\widehat{\mathbf{v}_B}^{(i)}$ is in the span of $\mathbb{U}\backslash\{\mathbf{u}\}$.

For simplicity, below, we just write $\mathbf{K} \leftarrow_R \mathbb{Z}_p^{1\times 3k}, \mathbf{K}'_A, \mathbf{K}'_B \leftarrow_R \mathbb{Z}_p^{(d-1)\times 3k}$ to implicitly mean that $\mathbf{K}, \mathbf{K}'_A, \mathbf{K}'_B$ satisfy the above conditions.

- Hybrid_0: This is as the real hybrid.
- Hybrid_1: This is the same as Hybrid_0, except that we replace $\mathsf{H}(\mathsf{GID}) = [\mathbf{h}_{\mathsf{GID}}]_2$ with $[\mathbf{B}_1\mathbf{r}_{\mathsf{GID}}]_2$, where $\mathbf{r}_{\mathsf{GID}} \leftarrow_R \mathbb{Z}_p^{k\times 1}$. Thus, $\mathsf{sk}_{\mathsf{GID},u}$ becomes

$$K_{\mathsf{GID},A,u} = [\mathbf{W}_{A,u}\boxed{\mathbf{B}_1\mathbf{r}_{\mathsf{GID}}} + \mathbf{W}_{A,u}\mathbf{B}_1\mathbf{r}]_2, K_{\mathsf{GID},B,u} = [\mathbf{W}_{B,u}\boxed{\mathbf{B}_1\mathbf{r}_{\mathsf{GID}}}]_2.$$

– Hybrid_2: This is the same as Hybrid_1, except that for $x \in \bar{Y}$, we replace the challenge CT generated by the simulator with

$$C_{1,A,x} = [\boxed{\mathbf{s}_{A,x}^{(13)}(\mathbf{A}_1\|\mathbf{A}_3)^\top}]_1, C_{1,B,x} = [\boxed{\mathbf{s}_{B,x}^{(13)}(\mathbf{A}_1\|\mathbf{A}_3)^\top}]_1,$$
$$C_{2,A,x} = [\boxed{\mathbf{s}_{A,x}^{(13)}(\mathbf{A}_1\|\mathbf{A}_3)^\top}\mathbf{W}_{A,\rho(x)} + \mathbf{M}_x \begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix}]_1,$$
$$C_{2,B,x} = [\boxed{\mathbf{s}_{B,x}^{(13)}(\mathbf{A}_1\|\mathbf{A}_3)^\top}\mathbf{W}_{B,\rho(x)} + \mathbf{M}_x \begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix}]_1,$$

where $\mathbf{s}_{A,x}^{(13)}, \mathbf{s}_{B,x}^{(13)} \leftarrow_R \mathbb{Z}_p^{1\times 2k}$.

– Hybrid_3: This is the same as Hybrid_2, except that for $x \in \bar{Y}$, we replace the challenge CT generated by the simulator with

$$C_{1,A,x} = [\mathbf{s}_{A,x}^{(13)}(\mathbf{A}_1\|\mathbf{A}_3)^\top]_1, C_{1,B,x} = [\mathbf{s}_{B,x}^{(13)}(\mathbf{A}_1\|\mathbf{A}_3)^\top]_1,$$
$$C_{2,A,x} = [\mathbf{s}_{A,x}^{(13)}(\mathbf{A}_1\|\mathbf{A}_3)^\top\mathbf{W}_{A,\rho(x)} + \mathbf{M}_x \begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix} + \boxed{\sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top}}]_1,$$
$$C_{2,B,x} = [\mathbf{s}_{B,x}^{(13)}(\mathbf{A}_1\|\mathbf{A}_3)^\top\mathbf{W}_{B,\rho(x)} + \mathbf{M}_x \begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix} + \boxed{\sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top}}]_1,$$

where

$$\mathbf{N}'_A, \mathbf{N}'_B \leftarrow_R \mathbb{Z}_p^{1\times k},$$
$$\sigma'_{A,x} = \mathbf{M}_x \begin{pmatrix}\sigma'_A\\ \mathbf{k}_A^{(3)}\end{pmatrix}, \sigma'_A \leftarrow_R \mathbb{Z}_p, \mathbf{k}_A^{(3)} \leftarrow_R \mathbb{Z}_p^{(d-1)\times 1},$$
$$\sigma'_{B,x} = \mathbf{M}_x \begin{pmatrix}\sigma'_B\\ \mathbf{k}_B^{(3)}\end{pmatrix}, \sigma'_B \leftarrow_R \mathbb{Z}_p, \mathbf{k}_B^{(3)} \leftarrow_R \mathbb{Z}_p^{(d-1)\times 1}.$$

– Hybrid_4: This is the same as Hybrid_3, except that for $x \in \bar{Y}$, we replace the challenge CT generated by the simulator with

$$C_{1,A,x} = [\boxed{\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top}]_1, C_{1,B,x} = [\boxed{\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top}]_1,$$
$$C_{2,A,x} = [\boxed{\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top}\mathbf{W}_{A,\rho(x)} + \mathbf{M}_x \begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix} + \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top}]_1,$$
$$C_{2,B,x} = [\boxed{\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top}\mathbf{W}_{B,\rho(x)} + \mathbf{M}_x \begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix} + \sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top}]_1,$$

where $\mathbf{s}_{A,x}^{(123)}, \mathbf{s}_{B,x}^{(123)} \leftarrow_R \mathbb{Z}_p^{1\times(2k+1)}$.

– $\mathsf{Hybrid}_{5:j}(j \in [q])$: In this hybrid, for $t \le j$, $\mathsf{H}(\mathsf{GID}_t) = [(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}_t}^{(13)}]_2$, where $\mathbf{r}_{\mathsf{GID}_t}^{(13)} \leftarrow_R \mathbb{Z}_p^{2k\times 1}$; for $t > j$, $\mathsf{H}(\mathsf{GID}_t) = [\mathbf{B}_1\mathbf{r}_{\mathsf{GID}_t}]_2$, where $\mathbf{r}_{\mathsf{GID}_t} \leftarrow_R \mathbb{Z}_p^{k\times 1}$. And $\mathsf{Hybrid}_{5:0}$ is Hybrid_4.

– $\mathsf{Hybrid}_{5:j:1}(j \in [q])$: This is the same as $\mathsf{Hybrid}_{5:(j-1)}$, except that for the j-th global identifier GID_j, we replace $\mathsf{H}(\mathsf{GID}_j) = [\mathbf{B}_1\mathbf{r}_{\mathsf{GID}_j}]_2$ with $\mathsf{H}(\mathsf{GID}_j) = [(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_j}]_2$, where $\mathbf{r}^{(12)}_{\mathsf{GID}_j} \leftarrow_R \mathbb{Z}_p^{2k\times 1}$. Thus, $\mathsf{sk}_{\mathsf{GID}_j,u}$ becomes

$$K_{\mathsf{GID}_j,A,u} = [\mathbf{W}_{A,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_j}} + \mathbf{W}_{A,u}\mathbf{B}_1\mathbf{r}]_2,$$
$$K_{\mathsf{GID}_j,B,u} = [\mathbf{W}_{B,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_j}}]_2.$$

– $\mathsf{Hybrid}_{5:j:2}(j \in [q])$: This is the same as $\mathsf{Hybrid}_{5:j:1}$, except that for $x \in \bar{Y}$, we replace the challenge CT generated by the simulator with

$$C_{1,A,x} = [\mathbf{s}^{(123)}_{A,x}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1, C_{1,B,x} = [\mathbf{s}^{(123)}_{B,x}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1,$$
$$C_{2,A,x} = [\mathbf{s}^{(123)}_{A,x}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{A,\rho(x)} + \mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix} +$$
$$\boxed{\sigma''_{A,x}\mathbf{N}''_A\mathbf{B}_2^{\|\top}} + \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top}]_1,$$
$$C_{2,B,x} = [\mathbf{s}^{(123)}_{B,x}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{B,\rho(x)} + \mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix} +$$
$$\boxed{\sigma''_{B,x}\mathbf{N}''_B\mathbf{B}_2^{\|\top}} + \sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top}]_1,$$

where

$$\mathbf{N}''_A, \mathbf{N}''_B \leftarrow_R \mathbb{Z}_p^{1\times k},$$
$$\sigma''_{A,x} = \mathbf{M}_x\begin{pmatrix}\sigma''_A\\ \mathbf{k}^{(2)}_A\end{pmatrix}, \sigma''_A \leftarrow_R \mathbb{Z}_p, \mathbf{k}^{(2)}_A \leftarrow_R \mathbb{Z}_p^{(d-1)\times 1},$$
$$\sigma''_{B,x} = \mathbf{M}_x\begin{pmatrix}\sigma''_B\\ \mathbf{k}^{(2)}_B\end{pmatrix}, \sigma''_B \leftarrow_R \mathbb{Z}_p, \mathbf{k}^{(2)}_B \leftarrow_R \mathbb{Z}_p^{(d-1)\times 1}.$$

– $\mathsf{Hybrid}_{5:j:3}(j \in [q])$: This is the same as $\mathsf{Hybrid}_{5:j:2}$, except that for the j-th global identifier GID_j, we replace $\mathsf{H}(\mathsf{GID}_j) = [(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_j}]_2$ with $\mathsf{H}(\mathsf{GID}_j) = [(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}^{(123)}_{\mathsf{GID}_j}]_2$, where $\mathbf{r}^{(123)}_{\mathsf{GID}_j} \leftarrow_R \mathbb{Z}_p^{3k\times 1}$. Thus, $\mathsf{sk}_{\mathsf{GID}_j,u}$ becomes

$$K_{\mathsf{GID}_j,A,u} = [\mathbf{W}_{A,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}^{(123)}_{\mathsf{GID}_j}} + \mathbf{W}_{A,u}\mathbf{B}_1\mathbf{r}]_2,$$
$$K_{\mathsf{GID}_j,B,u} = [\mathbf{W}_{B,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}^{(123)}_{\mathsf{GID}_j}}]_2.$$

– $\mathsf{Hybrid}_{5:j:4}(j \in [q])$: This is the same as $\mathsf{Hybrid}_{5:j:3}$, except that for $x \in \bar{Y}$, we replace the challenge CT generated by the simulator back with

$$C_{1,A,x} = [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1, C_{1,B,x} = [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1,$$
$$C_{2,A,x} = [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{A,\rho(x)} + \mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix} +$$
$$\boxed{\cancel{\sigma''_{A,x}\mathbf{N}''_A\mathbf{B}_2^{\|\top}} + \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top}}]_1,$$
$$C_{2,B,x} = [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{B,\rho(x)} + \mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix} +$$
$$\boxed{\cancel{\sigma''_{B,x}\mathbf{N}''_B\mathbf{B}_2^{\|\top}} + \sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top}}]_1.$$

– $\mathsf{Hybrid}_{5:(j+1)}(j \in [q])$: This is the same as $\mathsf{Hybrid}_{5:j:4}$, except that for the j-th global identifier GID_j, we replace $\mathsf{H}(\mathsf{GID}_j) = [(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}_j}^{(123)}]_2$ with $\mathsf{H}(\mathsf{GID}_j) = [(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}_j}^{(13)}]_2$, where $\mathbf{r}_{\mathsf{GID}_j}^{(13)} \leftarrow_R \mathbb{Z}_p^{2k\times 1}$. Thus, $\mathsf{sk}_{\mathsf{GID}_j,u}$ becomes

$$K_{\mathsf{GID}_j,A,u} = [\mathbf{W}_{A,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}_j}^{(13)}} + \mathbf{W}_{A,u}\mathbf{B}_1\mathbf{r}]_2,$$
$$K_{\mathsf{GID}_j,B,u} = [\mathbf{W}_{B,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}_j}^{(13)}}]_2.$$

– Hybrid_6: This is the same as $\mathsf{Hybrid}_{5:(q+1)}$, except that we replace $h = [\mathbf{B}_1\mathbf{r}]_2$ in GP with $h = [(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}]_2$, where $\mathbf{r}^{(12)} \leftarrow_R \mathbb{Z}_p^{2k\times 1}$. Then C in the challenge CT generated by the simulator becomes

$$C = msg_b \oplus \mathsf{Ext}(e([\mathbf{K}]_1, \boxed{(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}}]_2), \mathsf{seed}).$$

And $\mathsf{sk}_{\mathsf{GID},u}$ becomes

$$K_{\mathsf{GID},A,u} = [\mathbf{W}_{A,u}(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(13)} + \mathbf{W}_{A,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}}]_2,$$
$$K_{\mathsf{GID},B,u} = [\mathbf{W}_{B,u}(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(13)}]_2.$$

– Hybrid_7: This is the same as Hybrid_6, except that for $x \in \bar{Y}$, we replace the challenge CT generated by the simulator with

$$C_{1,A,x} = [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1, C_{1,B,x} = [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1,$$
$$C_{2,A,x} = [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{A,\rho(x)} + \mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix} + \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top}]_1,$$
$$C_{2,B,x} = [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{B,\rho(x)} + \mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix} + \boxed{\sigma''_{B,x}\mathbf{N}''_B\mathbf{B}_2^{\|\top}} +$$
$$\sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top}]_1,$$

where

$$\mathbf{N}''_B \leftarrow_R \mathbb{Z}_p^{1\times k}, \sigma''_{B,x} = \mathbf{M}_x \begin{pmatrix} \sigma''_B \\ \mathbf{k}_B^{(2)} \end{pmatrix}, \sigma''_B \leftarrow_R \mathbb{Z}_p, \mathbf{k}_B^{(2)} \leftarrow_R \mathbb{Z}_p^{(d-1)\times 1}.$$

– Hybrid_8: This is the same as Hybrid_7, except that we replace $\mathsf{H}(\mathsf{GID}) = [(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(13)}]_2$ with $\mathsf{H}(\mathsf{GID}) = [(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(123)}]_2$, where $\mathbf{r}_{\mathsf{GID}}^{(123)} \leftarrow_R \mathbb{Z}_p^{3k\times 1}$. Thus, $\mathsf{sk}_{\mathsf{GID},u}$ becomes

$$K_{\mathsf{GID},A,u} = [\mathbf{W}_{A,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(123)}} + \mathbf{W}_{A,u}(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}]_2,$$
$$K_{\mathsf{GID},B,u} = [\mathbf{W}_{B,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(123)}}]_2.$$

– Hybrid_9: This is the same as Hybrid_8, except that we replace $\mathsf{H}(\mathsf{GID}) = [(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(123)}]_2$ with $\mathsf{H}(\mathsf{GID}) \equiv \mathsf{H}(\mathsf{GID})/h = [(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(123)} - (\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}]_2$, where $h = [(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}]_2$. Thus, $\mathsf{sk}_{\mathsf{GID},u}$ becomes

$$K_{\mathsf{GID},A,u} = [\mathbf{W}_{A,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(123)}}]_2,$$
$$K_{\mathsf{GID},B,u} = [\mathbf{W}_{B,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(123)}} - \mathbf{W}_{B,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}}]_2.$$

– Hybrid_{10}: This is the same as Hybrid_9, except that we replace $\mathsf{H}(\mathsf{GID}) = [(\mathbf{B}_1\|\mathbf{B}_2\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(123)} - (\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}]_2$ with $\mathsf{H}(\mathsf{GID}) = [(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(13)} - (\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}]_2$, where $\mathbf{r}_{\mathsf{GID}}^{(13)} \leftarrow_R \mathbb{Z}^{2k\times 1}$. Thus, $\mathsf{sk}_{\mathsf{GID},u}$ becomes

$$K_{\mathsf{GID},A,u} = [\mathbf{W}_{A,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(13)}}]_2,$$
$$K_{\mathsf{GID},B,u} = [\mathbf{W}_{B,u}\boxed{(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}_{\mathsf{GID}}^{(13)}} - \mathbf{W}_{B,u}(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}]_2.$$

– Hybrid_{11}: This is the same as Hybrid_{10}, except that for $x \in \bar{Y}$, we replace the challenge CT generated by the simulator back with

$$C_{1,A,x} = [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1, C_{1,B,x} = [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1,$$
$$C_{2,A,x} = [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{A,\rho(x)} + \mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix} + \boxed{\sigma''_{A,x}\mathbf{N}''_A\mathbf{B}_2^{\|\top}} +$$
$$\sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top}]_1,$$
$$C_{2,B,x} = [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{B,\rho(x)} + \mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix} + \sigma''_{B,x}\mathbf{N}''_B\mathbf{B}_2^{\|\top} +$$
$$\sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top}]_1,$$

where

$$\sigma''_{A,x} = \mathbf{M}_x\begin{pmatrix}\sigma''_A\\ \mathbf{k}_A^{(2)}\end{pmatrix}, \sigma''_A \leftarrow_R \mathbb{Z}_p, \mathbf{k}_A^{(2)} \leftarrow_R \mathbb{Z}_p^{(d-1)\times 1}.$$

– Hybrid_{12}: This is the same as Hybrid_{11}, except that we replace msg_b with $\boxed{msg_R} \leftarrow_R \mathbb{M}$.

Proofs.

Lemma 2. *We have* $|\mathsf{Adv}^{\mathsf{Hybrid}_0}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hybrid}_1}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{MDDH^q_{G_2,k,3k}}_{\mathcal{B}_1}(\lambda)$*, where* $\mathcal{B}_1$ *is the adversary for the* $MDDH^q_{k,3k}$ *assumption in* G_2*.*

Proof. This proof is a conventional use of the MDDH assumption, we leave the proof in the full version.

Lemma 3. *We have* $|\mathsf{Adv}^{\mathsf{Hybrid}_1}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hybrid}_2}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{SD^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1,\mathbf{A}_3}}_{\mathcal{B}_2}(\lambda)$*, where* $\mathcal{B}_2$ *is the adversary for the* $SD_{\mathbf{A}_1 \mapsto \mathbf{A}_1,\mathbf{A}_3}$ *assumption in* G_1*.*

Proof. Since this proof is similar to the proof of Lemma 6, we leave this proof in the full version.

Lemma 4. *We have* $|\mathsf{Adv}^{\mathsf{Hybrid}_2}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hybrid}_3}_{\mathcal{A}}(\lambda)| \leq 2 \cdot \mathsf{Adv}^{1\text{-}ABE}_{\mathcal{B}_3}(\lambda)$*, where* $\mathcal{B}_3$ *is the adversary for the Core 1-ABE.*

Proof. Since this proof is similar to the proof of Lemma 7, and the proof of Lemma 7 is more illustrative for the use of Core 1-ABE, thus we leave this proof in the full version.

Lemma 5. *We have* $|\mathsf{Adv}^{\mathsf{Hybrid}_3}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hybrid}_4}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{SD^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1,\mathbf{A}_2}}_{\mathcal{B}_4}(\lambda)$*, where* $\mathcal{B}_4$ *is the adversary for the* $SD_{\mathbf{A}_1 \mapsto \mathbf{A}_1,\mathbf{A}_2}$ *assumption in* G_1*.*

Proof. Since this proof is similar to the proof of Lemma 6, we leave the proof in the full version.

Lemma 6. *We have* $|\mathsf{Adv}^{\mathsf{Hybrid}_{5:(j-1)}}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hybrid}_{5:j:1}}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{SD^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_2}}_{\mathcal{B}_5}(\lambda)$*, where* $\mathcal{B}_5$ *is the adversary for the* $SD_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_2}$ *assumption in* G_2*.*

Proof. Suppose there exists a simulator $\mathcal{B}_5$. $\mathcal{B}_5$ receives

$$(\mathbb{G}, [\mathbf{B}_1]_2, [\mathbf{B}_2]_2, [\mathbf{B}_3]_2, \mathsf{basis}(\mathbf{B}_1^{\parallel}), \mathsf{basis}(\mathbf{B}_1^{\parallel}, \mathbf{B}_2^{\parallel}), \mathsf{basis}(\mathbf{B}_3^{\parallel})), \text{ and } [T]_2.$$

$\mathcal{B}_5$ uses a strong seeded randomness extractor $\mathsf{Ext} : G_T \times \mathsf{S} \to \mathbb{M}$, and a hash function $\mathsf{H} : \{0,1\}^* \to G_2^{3k \times 1}$, which is modeled as a random oracle. Then $\mathcal{B}_5$ proceeds as follows:

Generating the Global Public Parameters: Sample $\mathsf{seed} \leftarrow_R \mathsf{S}, \mathbf{r} \leftarrow_R \mathbb{Z}_p^{k \times 1}$. Output

$$\mathsf{GP} = (\mathbb{G}, [\mathbf{A}_1]_1, h = [\mathbf{B}_1\mathbf{r}]_2, \mathsf{seed}).$$

Generating Authority Public-Master Keys: For a valid Authority Setup query of $u \in \mathcal{AU}$, $\mathcal{B}_5$ samples $\mathbf{W}_{A,u}, \mathbf{W}_{B,u} \leftarrow_R \mathbb{Z}_p^{(2k+1)\times 3k}$. $\mathcal{B}_5$ sets

$$\mathsf{PK}_u = ([\mathbf{A}_1^\top \mathbf{W}_{A,u}]_1, [\mathbf{A}_1^\top \mathbf{W}_{B,u}]_1),$$
$$\mathsf{MSK}_u = (\mathbf{W}_{A,u}, \mathbf{W}_{B,u}).$$

$\mathcal{B}_5$ sends PK_u to $\mathcal{A}$, and stores $(\mathsf{PK}_u, \mathsf{MSK}_u)$. Whenever $\mathcal{A}$ requests MSK_u at a later time, $\mathcal{B}_5$ provides it to $\mathcal{A}$.

Generating the H Oracle Outputs: Whenever $\mathcal{A}$ queries the random oracle H for some $\mathsf{GID} \in \mathcal{GID}$, $\mathcal{B}_5$ proceeds as follows: For $t \leq j-1$, $\mathcal{B}_5$ sets $\mathsf{H}(\mathsf{GID}_t) = [(\mathbf{B}_1 \| \mathbf{B}_3)\mathbf{r}^{(13)}_{\mathsf{GID}_t}]_2$, where $\mathbf{r}^{(13)}_{\mathsf{GID}_t} \leftarrow_R \mathbb{Z}_p^{2k\times 1}$; For $t = j$, $\mathcal{B}_5$ sets $\mathsf{H}(\mathsf{GID}_t) = [T]_2$; For $t \geq j+1$, $\mathcal{B}_5$ sets $\mathsf{H}(\mathsf{GID}_t) = [\mathbf{B}_1\mathbf{r}^{(1)}_{\mathsf{GID}_t}]_2$, where $\mathbf{r}^{(1)}_{\mathsf{GID}_t} \leftarrow_R \mathbb{Z}_p^{k\times 1}$. It stores $\mathsf{H}(\mathsf{GID}_t)$ so that it can respond consistently if $\mathsf{H}(\mathsf{GID}_t)$ is queried again.

Generating Secret Keys: For a valid Secret Key query of $(\mathsf{GID}_t, u) \in \mathcal{GID} \times \mathcal{AU}$, $\mathcal{B}_5$ runs the real KeyGen to generate $\mathsf{sk}_{\mathsf{GID}_t,u}$ with $\mathsf{H}(\mathsf{GID}_t), h = [\mathbf{B}_1\mathbf{r}]_2$ and $\mathsf{MSK}_u = (\mathbf{W}_{A,u}, \mathbf{W}_{B,u})$. If $\mathsf{H}(\mathsf{GID}_t)$ has not been generated before, then generate it following the above procedure.

Generating the Challenge Ciphertext: At some point, $\mathcal{A}$ queries the challenge $(msg_0, msg_1, \mathbf{M}, \rho)$, and also submits the public keys $\{\mathsf{PK}_{u'} = ([P_{A,u'}]_1, [P_{B,u'}]_1)\}$ for a subset U_A of attribute authorities appearing in the LSSS access structure $(\mathbf{M}, \rho)$. If U_A passes the validation test, $\mathcal{B}_5$ flips a random coin $b \leftarrow_R \{0,1\}$ and generates CT as follows:

Let Y denote the subset of rows of the challenge access matrix $\mathbf{M}$ labeled by the authorities for which $\mathcal{A}$ supplies the authority public keys $\{\mathsf{PK}_{u'} = ([P_{A,u'}]_1, [P_{B,u'}]_1)\}$. Let $\bar{Y} = [\ell]\backslash Y$. $\mathcal{B}_5$ samples $\mathbf{K} \leftarrow_R \mathbb{Z}_p^{1\times 3k}, \mathbf{K}'_A \leftarrow_R \mathbb{Z}_p^{(d-1)\times 3k}, \mathbf{K}'_B \leftarrow_R \mathbb{Z}_p^{(d-1)\times 3k}, \mathbf{s}^{(1)}_{A,x}, \mathbf{s}^{(1)}_{B,x} \leftarrow_R \mathbb{Z}_p^{1\times k}, \mathbf{s}^{(23)}_{A,x}, \mathbf{s}^{(23)}_{B,x} \leftarrow_R \mathbb{Z}_p^{1\times(k+1)}$, and $\mathbf{N}'_A, \mathbf{N}'_B \leftarrow_R \mathbb{Z}_p^{1\times k}, \sigma'_A \leftarrow_R \mathbb{Z}_p, \mathbf{k}^{(3)}_A \leftarrow_R \mathbb{Z}_p^{(d-1)\times 1}, \sigma'_B \leftarrow_R \mathbb{Z}_p, \mathbf{k}^{(3)}_B \leftarrow_R \mathbb{Z}_p^{(d-1)\times 1}$. Set

$$\mathbf{s}^{(123)}_{A,x} = (\mathbf{s}^{(1)}_{A,x} \| \mathbf{s}^{(23)}_{A,x}), \mathbf{s}^{(123)}_{B,x} = (\mathbf{s}^{(1)}_{B,x} \| \mathbf{s}^{(23)}_{B,x}),$$
$$\sigma'_{A,x} = \mathbf{M}_x \begin{pmatrix} \sigma'_A \\ \mathbf{k}^{(3)}_A \end{pmatrix}, \sigma'_{B,x} = \mathbf{M}_x \begin{pmatrix} \sigma'_B \\ \mathbf{k}^{(3)}_B \end{pmatrix}.$$

$\mathcal{B}_5$ sets $C = msg_b \oplus \mathsf{Ext}(e([\mathbf{K}]_1, h), \mathsf{seed})$.
For each $x \in Y$, $\mathcal{B}_5$ forms $C_{1,A,x}, C_{1,B,x}, C_{2,A,x}, C_{2,B,x}$ as:

$$C_{1,A,x} = [\mathbf{s}^{(1)}_{A,x}\mathbf{A}_1^\top]_1, C_{1,B,x} = [\mathbf{s}^{(1)}_{B,x}\mathbf{A}_1^\top]_1,$$
$$C_{2,A,x} = [\mathbf{s}^{(1)}_{A,x}P_{A,\rho(x)} + \mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix}]_1, C_{2,B,x} = [\mathbf{s}^{(1)}_{B,x}P_{B,\rho(x)} + \mathbf{M}_x \begin{pmatrix} -\mathbf{K} \\ \mathbf{K}'_B \end{pmatrix}]_1.$$

For each $x \in \bar{Y}$, $\mathcal{B}_5$ forms $C_{1,A,x}, C_{1,B,x}, C_{2,A,x}, C_{2,B,x}$ as:

$$C_{1,A,x} = [\mathbf{s}^{(123)}_{A,x}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1, C_{1,B,x} = [\mathbf{s}^{(123)}_{B,x}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1,$$
$$C_{2,A,x} = [\mathbf{s}^{(123)}_{A,x}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{A,\rho(x)} + \mathbf{M}_x \begin{pmatrix} \mathbf{K} \\ \mathbf{K}'_A \end{pmatrix} + \sigma'_{A,x}\mathbf{N}'_A\mathsf{basis}(\mathbf{B}_3^{\|})^\top]_1,$$
$$C_{2,B,x} = [\mathbf{s}^{(123)}_{B,x}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top\mathbf{W}_{B,\rho(x)} + \mathbf{M}_x \begin{pmatrix} -\mathbf{K} \\ \mathbf{K}'_B \end{pmatrix} + \sigma'_{B,x}\mathbf{N}'_B\mathsf{basis}(\mathbf{B}_3^{\|})^\top]_1.$$

$\mathcal{B}_5$ sends $\mathsf{CT} = (C, \{C_{1,A,x}, C_{1,B,x}, C_{2,A,x}, C_{2,B,x}\}_{x\in[\ell]})$ to $\mathcal{A}$.

Guess: $\mathcal{A}$ eventually outputs a guess bit $b' \in \{0,1\}$. $\mathcal{B}_5$ outputs 1 if $b = b'$ and 0 otherwise.

Observe that if $T = \mathbf{B}_1\mathbf{r}^{(1)}_{\mathsf{GID}_j}$, where $\mathbf{r}^{(1)}_{\mathsf{GID}_j} \leftarrow_R \mathbb{Z}_p^{k\times 1}$, the distributions are exactly as in $\mathsf{Hybrid}_{5:(j-1)}$; if $T = (\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_j}$, where $\mathbf{r}^{(12)\top}_{\mathsf{GID}_j} = (\mathbf{r}^{(1)\top}_{\mathsf{GID}_j}\|\mathbf{r}^{(2)\top}_{\mathsf{GID}_j}), \mathbf{r}^{(2)}_{\mathsf{GID}_j} \leftarrow_R \mathbb{Z}_p^{k\times 1}$, the distributions are exactly as in $\mathsf{Hybrid}_{5:j:1}$. Then if $\mathcal{A}$ can distinguish $\mathsf{Hybrid}_{5:(j-1)}$ and $\mathsf{Hybrid}_{5:j:1}$, $\mathcal{B}_5$ can use $\mathcal{A}$ to break the $\mathrm{SD}_{\mathbf{B}_1\mapsto\mathbf{B}_1,\mathbf{B}_2}$ assumption in G_2. Thus, we obtain a contradiction.

Lemma 7. *We have* $|\mathsf{Adv}^{\mathsf{Hybrid}_{5:j:1}}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hybrid}_{5:j:2}}_{\mathcal{A}}(\lambda)| \le 2\cdot\mathsf{Adv}^{1\text{-}ABE}_{\mathcal{B}_6}(\lambda)$*, where* $\mathcal{B}_6$ *is the adversary for the Core 1-ABE.*

Proof. Suppose there exists a simulator $\mathcal{B}_6$. $\mathcal{B}_6$ challenges

$$(\mu_{0,A} = \mu_0, \mu_{1,A}) \text{ and } (-\mu_{0,B} = -\mu_0, -\mu_{1,B}),$$

respectively, to the underlying Core 1-ABE, where $\mu_0, \mu_{1,A}, \mu_{1,B} \leftarrow_R \mathbb{Z}_p$, and queries $\mathcal{O}_F(((\mathbf{M},\rho),\mu_{\beta,A})), \mathcal{O}_{X,A}(\{u\}), \mathcal{O}_F(((\mathbf{M},\rho),-\mu_{\beta,B})), \mathcal{O}_{X,B}(\{u\})$, which are defined in Sect. 2.5. Then $\mathcal{B}_6$ receives

$$\{[\mu_{\beta,A,x} + \eta_{A,\rho(x)}\mathbf{s}^{(3)}_{A,x}]_1, [\mathbf{s}^{(3)}_{A,x}]_1\}, \{\eta_{A,u}\},$$

and

$$\{[-\mu_{\beta,B,x} + \eta_{B,\rho(x)}\mathbf{s}^{(3)}_{B,x}]_1, [\mathbf{s}^{(3)}_{B,x}]_1\}, \{\eta_{B,u}\},$$

respectively.

$\mathcal{B}_6$ samples $\mathbf{N}''_A, \mathbf{N}''_B \leftarrow_R \mathbb{Z}_p^{1\times k}$, and for $\mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix}$, sets

$$\mathbf{K} = \widetilde{\mathbf{K}} + \mu_{\beta,A}\mathbf{N}''_A\mathbf{B}_2^{\|\top},$$

for $\mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix}$, sets

$$\mathbf{K} = \widetilde{\mathbf{K}} + \mu_{\beta,B}\mathbf{N}''_B\mathbf{B}_2^{\|\top},$$

where $\widetilde{\mathbf{K}} \leftarrow_R \mathbb{Z}_p^{1\times 3k}$. Then set

$$\mathbf{W}_{A,u} = \widetilde{\mathbf{W}_{A,u}} + \mathbf{A}_3^{\|}\eta_{A,u}\mathbf{N}''_A\mathbf{B}_2^{\|\top}, \mathbf{W}_{B,u} = \widetilde{\mathbf{W}_{B,u}} + \mathbf{A}_3^{\|}\eta_{B,u}\mathbf{N}''_B\mathbf{B}_2^{\|\top},$$

where $\widetilde{\mathbf{W}_{A,u}}, \widetilde{\mathbf{W}_{B,u}} \leftarrow_R \mathbb{Z}_p^{(2k+1)\times 3k}$, and $\eta_{A,u}, \eta_{B,u} \in \mathbb{Z}_p^{k\times 1}$ are from the answers of $\mathcal{O}_{X,A}(\{u\}), \mathcal{O}_{X,B}(\{u\})$, respectively.

Observe that, when we change $\mathbf{W}_{A,u}, \mathbf{W}_{B,u}$ and $\mathbf{K}$, only $\mathsf{PK}_u, \mathsf{sk}_{\mathsf{GID}_t,u}$ and CT are changed.

For PK_u, we have

$$\mathbf{A}_1^\top \mathbf{W}_{A,u} \equiv \mathbf{A}_1^\top (\widetilde{\mathbf{W}_{A,u}} + \mathbf{A}_3^{\|} \eta_{A,u} \mathbf{N}''_A \mathbf{B}_2^{\|\top}) = \mathbf{A}_1^\top \widetilde{\mathbf{W}_{A,u}},$$

and

$$\mathbf{A}_1^\top \mathbf{W}_{B,u} \equiv \mathbf{A}_1^\top (\widetilde{\mathbf{W}_{B,u}} + \mathbf{A}_3^{\|} \eta_{B,u} \mathbf{N}''_B \mathbf{B}_2^{\|\top}) = \mathbf{A}_1^\top \widetilde{\mathbf{W}_{B,u}}.$$

Thus, PK_u remains unchanged.

For $\mathsf{sk}_{\mathsf{GID}_t,u}$, we have

when $t \leq j-1$,

$$\begin{aligned}\mathbf{W}_{A,u}((\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}^{(13)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}) \equiv & (\widetilde{\mathbf{W}_{A,u}} + \mathbf{A}_3^{\|} \eta_{A,u} \mathbf{N}''_A \mathbf{B}_2^{\|\top})((\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}^{(13)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}) \\ = & \widetilde{\mathbf{W}_{A,u}}((\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}^{(13)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}),\end{aligned}$$

and

$$\begin{aligned}\mathbf{W}_{B,u}(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}^{(13)}_{\mathsf{GID}_t} \equiv & (\widetilde{\mathbf{W}_{B,u}} + \mathbf{A}_3^{\|} \eta_{B,u} \mathbf{N}''_B \mathbf{B}_2^{\|\top})(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}^{(13)}_{\mathsf{GID}_t} \\ = & \widetilde{\mathbf{W}_{B,u}}(\mathbf{B}_1\|\mathbf{B}_3)\mathbf{r}^{(13)}_{\mathsf{GID}_t},\end{aligned}$$

where $\mathbf{r}^{(13)}_{\mathsf{GID}_t} \leftarrow_R \mathbb{Z}_p^{2k\times 1}$;

when $t = j$,

$$\begin{aligned}\mathbf{W}_{A,u}((\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}) \equiv & (\widetilde{\mathbf{W}_{A,u}} + \mathbf{A}_3^{\|} \eta_{A,u} \mathbf{N}''_A \mathbf{B}_2^{\|\top})((\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}) \\ = & \widetilde{\mathbf{W}_{A,u}}((\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}) + \mathbf{A}_3^{\|}\eta_{A,u}\mathbf{N}''_A\mathbf{r}^{(2)}_{\mathsf{GID}_t},\end{aligned}$$

and

$$\begin{aligned}\mathbf{W}_{B,u}(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_t} \equiv & (\widetilde{\mathbf{W}_{B,u}} + \mathbf{A}_3^{\|} \eta_{B,u} \mathbf{N}''_B \mathbf{B}_2^{\|\top})(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_t} \\ = & \widetilde{\mathbf{W}_{B,u}}(\mathbf{B}_1\|\mathbf{B}_2)\mathbf{r}^{(12)}_{\mathsf{GID}_t} + \mathbf{A}_3^{\|}\eta_{B,u}\mathbf{N}''_B\mathbf{r}^{(2)}_{\mathsf{GID}_t},\end{aligned}$$

where $\mathbf{r}^{(1)}_{\mathsf{GID}_t}, \mathbf{r}^{(2)}_{\mathsf{GID}_t} \leftarrow_R \mathbb{Z}_p^{k\times 1}$,$\mathbf{r}^{(12)\top}_{\mathsf{GID}_t} = (\mathbf{r}^{(1)\top}_{\mathsf{GID}_t}\|\mathbf{r}^{(2)\top}_{\mathsf{GID}_t})$, and $\eta_{A,u}$, $\eta_{B,u}$ are from the answers of $\mathcal{O}_{X,A}(\{u\}), \mathcal{O}_{X,B}(\{u\})$;

when $t \geq j+1$,

$$\begin{aligned}\mathbf{W}_{A,u}(\mathbf{B}_1\mathbf{r}^{(1)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}) \equiv & (\widetilde{\mathbf{W}_{A,u}} + \mathbf{A}_3^{\|} \eta_{A,u} \mathbf{A}_2^\top \mathbf{N}''_A \mathbf{B}_2^{\|\top})(\mathbf{B}_1\mathbf{r}^{(1)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}) \\ = & \widetilde{\mathbf{W}_{A,u}}(\mathbf{B}_1\mathbf{r}^{(1)}_{\mathsf{GID}_t} + \mathbf{B}_1\mathbf{r}),\end{aligned}$$

and

$$\begin{aligned}\mathbf{W}_{B,u}\mathbf{B}_1\mathbf{r}^{(1)}_{\mathsf{GID}_t} \equiv & (\widetilde{\mathbf{W}_{B,u}} + \mathbf{A}_3^{\|} \eta_{B,u} \mathbf{N}''_B \mathbf{B}_2^{\|\top})\mathbf{B}_1\mathbf{r}^{(1)}_{\mathsf{GID}_t} \\ = & \widetilde{\mathbf{W}_{B,u}}\mathbf{B}_1\mathbf{r}^{(1)}_{\mathsf{GID}_t},\end{aligned}$$

where $\mathbf{r}^{(1)}_{\mathsf{GID}_t} \leftarrow_R \mathbb{Z}_p^{k\times 1}$.

For the challenge CT, observe that only the components of $x \in \bar{Y}$ are changed. Then for each $x \in \bar{Y}$, $C_{1,A,x}, C_{1,B,x}, C_{2,A,x}, C_{2,B,x}$ are formed as

$$
\begin{aligned}
C_{1,A,x} =& [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1, C_{1,B,x} = [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top]_1,\\
C_{2,A,x} =& [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \mathbf{W}_{A,\rho(x)} + \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top} + \mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix}]_1\\
\equiv& [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \widetilde{\mathbf{W}_{A,\rho(x)}} + \mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \mathbf{A}_3^{\|}\eta_{A,\rho(x)}\mathbf{N}''_A\mathbf{B}_2^{\|\top} +\\
& \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top} + \mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix}]_1\\
=& [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \widetilde{\mathbf{W}_{A,\rho(x)}} + \mathbf{s}_{A,x}^{(3)}\mathbf{A}_3^\top\mathbf{A}_3^{\|}\eta_{A,\rho(x)}\mathbf{N}''_A\mathbf{B}_2^{\|\top} + \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top} +\\
& \mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix}]_1\\
=& [\mathbf{s}_{A,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \widetilde{\mathbf{W}_{A,\rho(x)}} + \mathbf{s}_{A,x}^{(3)}\eta_{A,\rho(x)}\mathbf{N}''_A\mathbf{B}_2^{\|\top} +\\
& \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top} + \mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix}]_1\\
\equiv& [\mathbf{s}_{A,x}^{(12)}(\mathbf{A}_1\|\mathbf{A}_2)^\top \widetilde{\mathbf{W}_{A,\rho(x)}} + \sigma'_{A,x}\mathbf{N}'_A\mathbf{B}_3^{\|\top} +\\
& \underbrace{\mathbf{M}_x\begin{pmatrix}\widetilde{\mathbf{K}}\\ \mathbf{K}'_A\end{pmatrix} + \mathbf{s}_{A,x}^{(3)}\mathbf{A}_3^\top\widetilde{\mathbf{W}_{A,\rho(x)}} + (\mu_{\beta,A,x} + \mathbf{s}_{A,x}^{(3)}\eta_{A,\rho(x)})\mathbf{N}''_A\mathbf{B}_2^{\|\top}}_{\mathbf{M}_x\begin{pmatrix}\mathbf{K}\\ \mathbf{K}'_A\end{pmatrix} + \mathbf{s}_{A,x}^{(3)}\mathbf{A}_3^\top\mathbf{W}_{A,\rho(x)}}]_1,\\
C_{2,B,x} =& [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \mathbf{W}_{B,\rho(x)} + \sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top} + \mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix}]_1\\
\equiv& [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \widetilde{\mathbf{W}_{B,\rho(x)}} + \mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \mathbf{A}_3^{\|}\eta_{B,\rho(x)}\mathbf{N}''_B\mathbf{B}_2^{\|\top} +\\
& \sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top} + \mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix}]_1\\
=& [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \widetilde{\mathbf{W}_{B,\rho(x)}} + \mathbf{s}_{B,x}^{(3)}\mathbf{A}_3^\top\mathbf{A}_3^{\|}\eta_{B,\rho(x)}\mathbf{N}''_B\mathbf{B}_2^{\|\top} + \sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top} +\\
& \mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix}]_1\\
=& [\mathbf{s}_{B,x}^{(123)}(\mathbf{A}_1\|\mathbf{A}_2\|\mathbf{A}_3)^\top \widetilde{\mathbf{W}_{B,\rho(x)}} + \mathbf{s}_{B,x}^{(3)}\eta_{B,\rho(x)}\mathbf{N}''_B\mathbf{B}_2^{\|\top} + \sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top} +\\
& \mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix}]_1\\
\equiv& [\mathbf{s}_{B,x}^{(12)}(\mathbf{A}_1\|\mathbf{A}_2)^\top \widetilde{\mathbf{W}_{B,\rho(x)}} + \sigma'_{B,x}\mathbf{N}'_B\mathbf{B}_3^{\|\top} +\\
& \underbrace{\mathbf{M}_x\begin{pmatrix}-\widetilde{\mathbf{K}}\\ \mathbf{K}'_B\end{pmatrix} + \mathbf{s}_{B,x}^{(3)}\mathbf{A}_3^\top\widetilde{\mathbf{W}_{B,\rho(x)}} + (-\mu_{\beta,B,x} + \mathbf{s}_{B,x}^{(3)}\eta_{B,\rho(x)})\mathbf{N}''_B\mathbf{B}_2^{\|\top}}_{\mathbf{M}_x\begin{pmatrix}-\mathbf{K}\\ \mathbf{K}'_B\end{pmatrix} + \mathbf{s}_{B,x}^{(3)}\mathbf{A}_3^\top\mathbf{W}_{B,\rho(x)}}]_1
\end{aligned}
$$

where $\mathbf{N}'_A, \mathbf{N}'_B \leftarrow_R \mathbb{Z}_p^{1\times k}$, $\mathbf{s}_{A,x}^{(1)}, \mathbf{s}_{B,x}^{(1)} \leftarrow_R \mathbb{Z}_p^{1\times k}$, $\mathbf{s}_{A,x}^{(2)}, \mathbf{s}_{B,x}^{(2)} \leftarrow_R \mathbb{Z}_p$, and $\mathbf{s}_{A,x}^{(123)} = (\mathbf{s}_{A,x}^{(1)} \| \mathbf{s}_{A,x}^{(2)} \| \mathbf{s}_{A,x}^{(3)}), \mathbf{s}_{B,x}^{(123)} = (\mathbf{s}_{B,x}^{(1)} \| \mathbf{s}_{B,x}^{(2)} \| \mathbf{s}_{B,x}^{(3)})$, $\mathbf{s}_{A,x}^{(12)} = (\mathbf{s}_{A,x}^{(1)} \| \mathbf{s}_{A,x}^{(2)}), \mathbf{s}_{B,x}^{(12)} = (\mathbf{s}_{B,x}^{(1)} \| \mathbf{s}_{B,x}^{(2)})$, and $([\mu_{\beta,A,x} + \mathbf{s}_{A,x}^{(3)} \eta_{A,\rho(x)}]_1, [\mathbf{s}_{A,x}^{(3)}]_1)$, $([-\mu_{\beta,B,x} + \mathbf{s}_{B,x}^{(3)} \eta_{B,\rho(x)}]_1, [\mathbf{s}_{B,x}^{(3)}]_1)$ are from the answers of $\mathcal{O}_F(((\mathbf{M}, \rho), \mu_{\beta,A}))$, $\mathcal{O}_F(((\mathbf{M}, \rho), -\mu_{\beta,B}))$, respectively.

Observe that if $\mu_{\beta,A} = \mu_{0,A}$ and $\mu_{\beta,B} = \mu_{0,B}$, the distributions are as in $\mathsf{Hybrid}_{5:j:1}$; if $\mu_{\beta,A} = \mu_{1,A}$ and $\mu_{\beta,B} = \mu_{1,B}$, the distributions are as in $\mathsf{Hybrid}_{5:j:2}$, which implicitly sets $\sigma''_A = \mathsf{Reconstruct}(\{\sigma''_{A,x}\}) = \mu_{1,A} - \mu_{0,A}$, and $\sigma''_B = \mathsf{Reconstruct}(\{\sigma''_{B,x}\}) = \mu_{1,B} - \mu_{0,B}$.

We can conclude that $\mathsf{Hybrid}_{5:j:1}$ and $\mathsf{Hybrid}_{5:j:2}$ are indistinguishable under the Core 1-ABE.

Lemma 8. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{5:j:2}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{5:j:3}}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_7}^{SD^{G_2}_{\mathbf{B}_2 \mapsto \mathbf{B}_2, \mathbf{B}_3}}(\lambda)$, *where* $\mathcal{B}_7$ *is the adversary for the* $SD_{\mathbf{B}_2 \mapsto \mathbf{B}_2, \mathbf{B}_3}$ *assumption in* G_2.

Proof. Since this proof is similar to the proof of Lemma 6, we leave the proof in the full version.

Lemma 9. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{5:j:3}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{5:j:4}}(\lambda)| \leq 2 \cdot \mathsf{Adv}_{\mathcal{B}_8}^{1\text{-}ABE}(\lambda)$, *where* $\mathcal{B}_8$ *is the adversary for the Core 1-ABE.*

Proof. Since this proof is similar to the proof of Lemma 7, we leave the proof in the full version.

Lemma 10.
We have $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{5:j:4}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{5:(j+1)}}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_9}^{SD^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_2}}(\lambda)$, *where* $\mathcal{B}_9$ *is the adversary for the* $SD_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_2}$ *assumption in* G_2.

Proof. Since this proof is similar to the proof of Lemma 6, we leave the proof in the full version.

Lemma 11. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{5:(q+1)}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{6}}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{10}}^{SD^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_2}}(\lambda)$, *where* $\mathcal{B}_{10}$ *is the adversary for the* $SD_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_2}$ *assumption in* G_2.

Proof. Since this proof is similar to the proof of Lemma 6, we leave the proof in the full version.

Lemma 12. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{6}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{7}}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{11}}^{1\text{-}ABE}(\lambda)$, *where* $\mathcal{B}_{11}$ *is the adversary for the Core 1-ABE.*

Proof. Since this proof is similar to the proof of Lemma 7, we leave the proof in the full version.

Lemma 13. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{7}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{8}}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{12}}^{SD^{G_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_2, \mathbf{B}_3}}(\lambda)$, *where* $\mathcal{B}_{12}$ *is the adversary for the* $SD_{\mathbf{B}_3 \mapsto \mathbf{B}_2, \mathbf{B}_3}$ *assumption in* G_2.

Proof. Since this proof is similar to the proof of Lemma 6, we leave the proof in the full version.

Lemma 14. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_8}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_9}(\lambda)| = 0$.

Proof. By simply setting $\mathsf{H}(\mathsf{GID}) \equiv \mathsf{H}(\mathsf{GID})/h$ for the queried $\mathsf{GID} \in \mathcal{GID}$ of H, where h is the component in GP, we can easily conclude that Hybrid_8 and Hybrid_9 are identically distributed.

Lemma 15. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_9}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{10}}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{13}}^{SD^{G_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_2, \mathbf{B}_3}}(\lambda)$, *where* $\mathcal{B}_{13}$ *is the adversary for the* $SD_{\mathbf{B}_3 \mapsto \mathbf{B}_2, \mathbf{B}_3}$ *assumption in* G_2.

Proof. Since this proof is similar to the proof of Lemma 6, we leave the proof in the full version.

Lemma 16. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{10}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{11}}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{14}}^{1\text{-}ABE}(\lambda)$, *where* $\mathcal{B}_{14}$ *is the adversary for the Core 1-ABE.*

Proof. Since this proof is similar to the proof of Lemma 7, we leave the proof in the full version.

Lemma 17. *We have* $|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{11}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Hybrid}_{12}}(\lambda)| \leq \mathsf{negl}(\lambda)$.

Proof. Since the symmetric key $e([\mathbf{K}]_1, [(\mathbf{B}_1 \| \mathbf{B}_2)\mathbf{r}^{(12)}]_2)$ is masked by the randomness from the second subspace, we can replace msg_b with $msg_R \leftarrow_R \mathbb{M}$ with a negligible difference by the statistical indistinguishability from Ext, if Ext is parameterized correctly.

Acknowledgements. We thank all the anonymous reviewers for helpful feedback on the write-up. This work is supported by the National Key Research and Development Program of China (2022YFB2701600, 2018YFA0704701), National Natural Science Foundation of China (61972156, 62372180, 61972094, 62032005), NSFC-ISF Joint Scientific Research Program (61961146004), "Digital Silk Road" Shanghai International Joint Lab of Trustworthy Intelligent Software (22510750100) and Innovation Program of Shanghai Municipal Education Commission (2021-01-07-00-08-E00101).

References

1. Agrawal, S., Yamada, S.: Optimal broadcast encryption from pairings and LWE. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Paqrt I. LNCS, vol. 12105, pp. 13–43. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45721-1_2
2. Ambrona, M., Gay, R.: Multi-authority abe, revisited. IACR Cryptol. ePrint Arch. p. 1381 (2021)
3. Attrapadung, N.: Dual system encryption framework in prime-order groups via computational pair encodings. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 591–623. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_20
4. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 27–35. Springer, New York (1990). https://doi.org/10.1007/0-387-34799-2_3

5. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_3
6. Boneh, D., et al.: Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 533–556. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_30
7. Chase, M.: Multi-authority Attribute Based Encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-70936-7_28
8. Chase, M., Chow, S.S.M.: Improving privacy and security in multi-authority attribute-based encryption. In: Al-Shaer, E., Jha, S., Keromytis, A.D. (eds.) CCS 2009, pp. 121–130. ACM (2009)
9. Chen, J., Gay, R., Wee, H.: Improved dual system ABE in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 595–624. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_20
10. Chen, J., Gong, J., Kowalczyk, L., Wee, H.: Unbounded ABE via bilinear entropy expansion, revisited. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part I. LNCS, vol. 10820, pp. 503–534. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78381-9_19
11. Chen, J., Gong, J., Wee, H.: Improved inner-product encryption with adaptive security and full attribute-hiding. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part II. LNCS, vol. 11273, pp. 673–702. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03329-3_23
12. Datta, P., Komargodski, I., Waters, B.: Decentralized multi-authority ABE for DNFs from LWE. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021, Part I. LNCS, vol. 12696, pp. 177–209. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77870-5_7
13. Datta, P., Komargodski, I., Waters, B.: Decentralized multi-authority ABE for nc^1 from computational-bdh. IACR Cryptol. ePrint Arch. p. 1325 (2021)
14. Datta, P., Komargodski, I., Waters, B.: Fully adaptive decentralized multi-authority ABE. IACR Cryptol. ePrint Arch. p. 1311 (2022). https://eprint.iacr.org/2022/1311
15. Datta, P., Komargodski, I., Waters, B.: Fully adaptive decentralized multi-authority ABE. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part III. LNCS, vol. 14006, pp. 447–478. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30620-4_15
16. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_8
17. Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 1–27. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_1
18. Gong, J., Dong, X., Chen, J., Cao, Z.: Efficient IBE with tight reduction to standard assumption in the multi-challenge setting. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 624–654. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_21

19. Gong, J., Waters, B., Wee, H.: ABE for DFA from k-Lin. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11693, pp. 732–764. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_25
20. Gong, J., Wee, H.: Adaptively secure ABE for DFA from k-Lin and more. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12107, pp. 278–308. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_10
21. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) STOC'13, 2013, pp. 545–554. ACM (2013)
22. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Juels, A., Wright, R.N., di Vimercati, S.D.C. (eds.) CCS 2006, pp. 89–98. ACM (2006)
23. Jain, A., Lin, H., Luo, J.: On the optimal succinctness and efficiency of functional encryption and attribute-based encryption. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part III. LNCS, vol. 14006, pp. 479–510. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30620-4_16
24. Kowalczyk, L., Wee, H.: Compact adaptively secure ABE for NC^1 from k-lin. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part I. LNCS, vol. 11476, pp. 3–33. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_1
25. Lewko, A.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_20
26. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_4
27. Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure hibe with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_27
28. Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_31
29. Lin, H., Cao, Z., Liang, X., Shao, J.: Secure threshold multi authority attribute based encryption without a central authority. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 426–436. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89754-5_33
30. Lin, H., Luo, J.: Compact adaptively secure ABE from k-lin: Beyond NC^1 and towards NL. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part III. LNCS, vol. 12107, pp. 247–277. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_9
31. Liu, T., Vaikuntanathan, V., Wee, H.: Conditional disclosure of secrets via non-linear reconstruction. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 758–790. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_25
32. Müller, S., Katzenbeisser, S., Eckert, C.: Distributed attribute-based encryption. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 20–36. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00730-9_2

33. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_11
34. Okamoto, T., Takashima, K.: Decentralized attribute-based encryption and signatures. IEICE **103**–**A**(1), 41–73 (2020)
35. Rouselakis, Y., Waters, B.: Efficient statically-secure large-universe multi-authority attribute-based encryption. In: Böhme, R., Okamoto, T. (eds.) FC 2015. LNCS, vol. 8975, pp. 315–332. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47854-7_19
36. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27
37. Tsabary, R.: Candidate witness encryption from lattice techniques. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, Part I. LNCS, vol. 13507, pp. 535–559. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-15802-5_19
38. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_36
39. Waters, B., Wee, H., Wu, D.J.: Multi-authority ABE from lattices without random oracles. In: Kiltz, E., Vaikuntanathan, V. (eds.) TCC 2022, Part I. LNCS, vol. 13747, pp. 651–679. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-22318-1_23
40. Wee, H.: Dual system encryption via predicate encodings. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 616–637. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_26
41. Wee, H.: Broadcast encryption with size $N^{1/3}$ and more from k-lin. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part IV. LNCS, vol. 12828, pp. 155–178. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-84259-8_6
42. Wee, H.: Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part II. LNCS, vol. 13276, pp. 217–241. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-07085-3_8