Decentralized Multi-Authority Attribute-Based Inner-Product FE: Large Universe and Unbounded

Pratish Datta[1] and Tapas Pal[2(✉)]

[1] NTT Research, Inc., Sunnyvale, CA 94085, USA
pratish.datta@ntt-research.com
[2] NTT Social Informatics Laboratories, Musashino-shi, Tokyo 180-8585, Japan
tapas.pal.wh@hco.ntt.co.jp, tapas.real@gmail.com

Abstract. This paper presents the *first* decentralized multi-authority attribute-based inner product functional encryption (MA-ABIPFE) schemes supporting vectors of a priori unbounded lengths. The notion of AB-IPFE, introduced by Abdalla et al. [ASIACRYPT 2020], combines the access control functionality of attribute-based encryption (ABE) with the possibility of evaluating linear functions on encrypted data. A decentralized MA-ABIPFE defined by Agrawal et al. [TCC 2021] essentially enhances the ABE component of AB-IPFE to the decentralized multi-authority setting where several authorities can independently issue user keys involving attributes under their control. In MA-ABIPFE for unbounded vectors (MA-ABUIPFE), encryptors can encrypt vectors of arbitrary length under access policies of their choice whereas authorities can issue secret keys to users involving attributes under their control and vectors of arbitrary lengths. Decryption works in the same way as for MA-ABIPFE provided the lengths of the vectors within the ciphertext and secret keys match.

We present two MA-ABUIPFE schemes supporting access policies realizable by linear secret sharing schemes (LSSS), in the significantly faster prime-order bilinear groups under decisional assumptions based on the target groups which are known to be weaker compared to their counterparts based in the source groups. The proposed schemes demonstrate different trade-offs between versatility and underlying assumptions. The first scheme allows each authority to control a bounded number of attributes and is proven secure under the well-studied decisional bilinear Diffie-Hellman (DBDH) assumption. On the other hand, the second scheme allows authorities to control exponentially many attributes and attributes are not required to be enumerated at the setup, that is, supports large attribute universe, and is proven secure under a non-interactive q-type variant of the DBDH assumption called L-DBDH, similar to what was used in prior large-universe multi-authority ABE (MA-ABE) construction.

When compared with the only known MA-ABIPFE scheme due to Agrawal et al. [TCC 2021], our schemes offer significantly higher efficiency while offering greater flexibility and security under weaker assumptions at the same time. Moreover, unlike Agrawal et al., our schemes can support the appearance of the same attributes within an access policy arbitrarily many times. Since efficiency and practicality are the prime focus of this work, we prove the security of our constructions in the random oracle model against static adversaries similar to prior works on MA-ABE with similar motivations and assumptions. On

A. Boldyreva and V. Kolesnikov (Eds.): PKC 2023, LNCS 13940, pp. 587–621, 2023.
https://doi.org/10.1007/978-3-031-31368-4_21

the technical side, we extend the unbounded IPFE techniques of Dufour-Sans and Pointcheval [ACNS 2019] to the context of MA-ABUIPFE by introducing a novel *hash-decomposition* technique.

Keywords: multi-authority · attribute-based · unbounded · inner product · functional encryption · large universe · static model

1 Introduction

Functional encryption (FE), introduced by Boneh, Sahai and Waters [15] and O'Neill [34] is an advanced form of public key encryption (PKE) designed for computing on encrypted data while maintaining its confidentiality beyond the computed results. FE delivers cryptographic solutions to a wide variety of privacy-enhancing technologies from enabling finer access control to outsourcing computations on sensitive data to the cloud. Starting with the work of Abdalla et al. [3], a long sequence of works [2,4,10,18,40] studied FE schemes for the class of linear functions, also known as inner product FE (IPFE). In IPFE, the ciphertexts and functional secret keys are associated with vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ respectively while a decrypter only learns the inner product $\boldsymbol{x} \cdot \boldsymbol{y}$ and nothing else about $\boldsymbol{x}$. Although the functionality is simple, IPFE has found a great amount of applications in both theory, for example, designing more expressive FE schemes for quadratic [23,27] and general functions [26,28] and in practice, for example, performing statistical studies on encrypted data, evaluating polynomials, computing conjunctions and disjunctions [3], or calculating hamming weights in biometric authentications [29,45], constructing trace and revoke schemes [6]. However, any IPFE system suffers from an inherent leakage of data due to it's linear functionality. In fact, releasing a set of secret keys for vectors forming a basis of the underlying vector space would result in a complete break of the system since it enables the recovery of the master secret key of the IPFE system and hence uncover all the encrypted data in the system.

One natural way to control such leakage of data in IPFE is to combine it with attribute-based encryption (ABE), that is, to additionally associate access policies/attributes within the ciphertexts/secret keys (or the other way around) in the same spirit as attribute-based encryption (ABE) such that the eligibility for computing on the encrypted data requires a prior validation of the attributes by the policy. Such access control mechanism in IPFE was introduced by Abdalla et al. [5] where they termed this upgraded notion as *attribute-based* IPFE (AB-IPFE). The notion of AB-IPFE [5,8,35] has been mostly explored in the setting where a single authority is responsible for managing all the attributes in the system and issuing secret keys to users. This not only is a limitation from the point of view of trust, but also it is problematic for practical applications. In fact, in reality, different attributes are governed by different authorities, for example, academic degrees are handled by universities, medical attributes are managed by hospitals while driving licenses are controlled by transportation or automobile agencies.

Multi Authority AB-IPFE: Inspired by the notion of *multi-authority* ABE (MA-ABE) [19–21,30,33,36,43] which deals with the decentralization of attribute management in the context of ABE, Agrawal et al. [9] initiated the study of *multi-authority* AB-IPFE (MA-ABIPFE) which enhances the ABE segment of AB-IPFE to the multi-authority setting. That is, just like MA-ABE, in MA-ABIPFE individual authorities are allowed to generate their own master key pairs and provide secret keys for attributes *only* under their control without interacting with the other authorities. A user learns $\boldsymbol{x} \cdot \boldsymbol{y}$ by decrypting a ciphertext generated with respect to a policy P and a vector $\boldsymbol{x}$ using various secret keys associated to a vector $\boldsymbol{y}$ and the different attributes it possesses that are obtained from the authorities controlling those attributes. Some potential practical application of MA-ABIPFE could be computing average salary of employees in an organization possessing a driving license and holding a Ph.D, statistics determining mental health of students of different departments in a university, etc.

Despite its countless potential applications, so far the only candidate MA-ABIPFE scheme, is due to Agrawal et al. [9] which supports access policies realizable by linear secret sharing schemes (LSSS) and is designed in a composite-order group and the security is based on variants of the subgroup decision assumptions which are source group assumptions, that is, assumptions made about the source groups of the underlying bilinear pairing. It is a well-known fact that composite-order bilinear groups are very expensive both in terms of computation and communication/storage. This is reflected in the MA-ABIPFE of [9], especially the decryption takes an unacceptable time of around five days (as shown in Table 2) when run using reasonable parameters, which clearly makes the scheme impractical. In order to address this efficiency bottleneck, a possible way to avoid this heavy efficiency bottleneck is to look for a construction in the prime-order bilinear groups which are way better in terms of the above parameters compared to their composite-order counterparts [22,25,31].

Another significant drawback of the MA-ABIPFE is that the vector lengths are fixed and the number of authorities or attributes are bounded in the setup. Consequently, the system must provision for a vector length bound that captures all possible plaintext vectors that would be encrypted during the lifetime of the system. Further, the size of ciphertexts and the encryption time, however small the length of the plaintext vector $\boldsymbol{x}$ is, scale with the worst-case vector length bound. Also, in the [9] construction, each authority can control at most a bounded number of attributes. This could be a bottleneck in certain applications, for instance, a university may introduce a new academic degree program over time which would require its potential to freely expand the attribute list under its control. Moreover, in the MA-ABIPFE system of [9], new authorities/attributes could not join beyond the upper limit set in the setup. This is clearly a disadvantage for several applications from the point of view of sustainability since it is often impossible to visualize all possible attributes/authorities that can ever come into existence at the time of setting up the system. For instance, new universities may be included in the survey of analyzing mental health of their students, which amplifies the number of authorities/attributes as well as the length of data. Additionally, the MA-ABIPFE scheme of [9] suffer from the so-called "one-use" restriction, that is, an attribute can appear within an access policy at most a bounded number of times, which clearly limits the class of access policies and negatively impacts efficiency. Lastly, in order to gain confidence

in a new cryptographic primitive such as MA-ABIPFE, it is always important to have more and more candidates for that primitive under qualitatively weaker computational assumptions. We thus consider the following open problem:

Open Problem: Is it possible to construct efficient MA-ABIPFE schemes for any expressive class of policies, e.g., LSSS, and avoiding the one-use restriction in prime-order bilinear groups under any (possibly qualitatively weaker) computational assumption such that an arbitrary number of authorities (possibly having an unbounded number of attributes under their control) can join at any point of time and an unbounded length data can be processed?

Our Results: In this paper, we answer the above open problem affirmatively. More precisely, we start by formulating the notion of (decentralized) multi-authority attribute-based *unbounded* IPFE (MA-ABUIPFE) which has all the features discussed above, namely, (a) several independent authorities can control different attributes in the system, (b) authorities can join the system at any time and there is no upper bound on the number of authorities that can ever exist in the system, and (c) unbounded length message and key vectors can be processed, that is, each authority can generate their public and master secret keys without fixing the length of vectors that can be processed with their keys. Next, we construct MA-ABUIPFE supporting LSSS access structures in the significantly faster prime-order bilinear group setting under computational assumptions based in the target group which are known to be qualitatively weaker compared to those based in the source group [11,21]. The efficiency improvements achieved by our scheme as compared to the only known MA-ABIPFE scheme [9] is quite significant (see Tables 1 and 2 for a concrete comparison of the schemes). On a more positive note, we are able to overcome the "one-use restriction", that is, support the appearance of attributes within access policies arbitrarily many times.

We present two MA-ABUIPFE schemes with varying trade-offs between versatility and underlying assumptions.

- **Small-Universe MA-ABUIPFE Scheme:** We construct an MA-ABUIPFE scheme where an authority is allowed to control a single (or a bounded number of) attribute(s), but the number of authorities that could be added to the system is still arbitrary. The construction is proven secure under the decisional bilinear Diffie-Hellman (DBDH) assumption [13,38] which is a very well-studied computational assumption based in the target groups. Note that the DBDH assumption underlies the security of classical ABE schemes [24,37,42] and has recently been shown to realize MA-ABE [21]. Our MA-ABUIPFE scheme demonstrates that it is possible to base the security of an even richer functionality on DBDH as well.
- **Large-Universe MA-ABUIPFE Scheme:** We further upgrade our small-universe MA-ABUIPFE scheme to support large attribute universe, that is, where each authority can control exponentially many attributes and attributes need not be enumerated at the setup. We present the security of this construction under a parameterized version of the DBDH assumption which we call the L-DBDH assumption. We justify the validity of this new computational assumption in the generic bilinear group model [12,39] as is done for nearly if not all bilinear group-based computational assumptions used today. Note that, so far, there is no known

MA-ABE scheme supporting large universe in the literature that is proven secure without parameterized assumption. The efficiency of the proposed large-universe scheme is well comparable to the small-universe one. Thus, our large-universe MA-ABUIPFE (LMA-ABUIPFE) scheme addresses several efficiency and practicality issues towards deploying this primitive in practice.

Since our focus on this paper is on efficiency and practicality, we content with proving the security of our schemes in the static model where the adversary has to declare all its ciphertext, secret key, and authority corruption queries upfront following prior work on MA-ABE with similar motivations [36]. However, we would like to mention that while we could not prove our schemes secure against selective adversaries under DBDH or similar target-group-based assumptions, that is, adversaries who must send the challenge ciphertext and authority corruption queries upfront but are allowed to make user secret key queries adaptively afterwards, as considered in [9], we could not identify any vulnerability in our proposed schemes against such adversaries. Also, just like prior MA-ABE schemes proven secure under standard computational assumptions, we make use of the random oracle model[1].

In order to design our small-universe MA-ABUIPFE, we build on the techniques used in the MA-ABE construction from DBDH by [21] and the unbounded IPFE construction from DBDH by [38]. However, as explained in Sect. 2 below, a straightforward combination of those techniques does not work. We devise a novel hash-decomposition technique to decompose the evaluation of the hash values, used as randomizers for tying together the different secret keys for the same user, between the encryption and key generation/decryption algorithms and also for handling satisfying and non-satisfying secret key queries of the adversary during the security proof differently. (Please see Sect. 2 for more details on the hash-decomposition technique.)

Along the way to our small universe MA-ABUIPFE scheme, we also present a single authority ABUIPFE for LSSS access policies in prime-order bilinear groups under the DBDH assumption. Prior to this work, there was no known AB-IPFE scheme even for bounded length vectors that was proven secure under a target group assumption. Thus, the proposed ABUIPFE expands the portfolio of computational assumptions on which this useful primitive can be based on and thereby increasing the confidence in the existence of this primitive in turn. Further, our construction also demonstrates that despite of being a more expressive functionality, MA-ABIPFE is still possible under the same assumption as ABE or MA-ABE. In fact, our AB-IPFE is the first target-group assumption-based FE scheme that goes beyond the "all-or-nothing" paradigm.

[1] Very recently, Waters, Wee, and Wu [43] presented a lattice-based MA-ABE scheme that does not make use of random oracles. However, the scheme relies on a recently introduced complexity assumption called evasive LWE [44] which is a strong knowledge type assumption and is not yet cryptanalyzed in detail.

Table 1. Efficiency Comparison of [9] and Our Scheme with 128-bit Security

Scheme	Group order length (in bits)	$\lvert\mathsf{PK}_t\rvert/\lvert\mathsf{PK}_\theta\rvert$	$\lvert\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\rvert$ $\mathsf{T}(t)=\theta$	$\lvert\mathsf{CT}\rvert$	Encrypt Time	Decrypt Time
Agrawal et al. [9]	3072	$6054n$	3072	$(n+\ell+2n\ell)3072$	$(n+n\ell)\mathsf{E}_{N,T}+(\ell+n\ell)\mathsf{E}_{N,S}$	$(\ell+1)\mathsf{P}_N+(n+n\ell^2)\mathsf{E}_{N,T}+(\ell+n\ell^2)\mathsf{E}_{N,S}$
MA-ABUIPFE (Sect. 5)	256	$\lvert\mathsf{PK}_t\rvert=256s_{\mathsf{max}}$	256	$[n+\ell s_{\mathsf{max}}(n+1)]256$	$(n+n\ell)\mathsf{E}_{q,T}+[\ell s_{\mathsf{max}}(n+2)-\ell(n+1)]\mathsf{E}_{q,S}+(2\ell n(s_{\mathsf{max}}-1))\mathsf{P}_q$	$[\ell+n(s_{\mathsf{max}}-1)](\mathsf{P}_q+\mathsf{E}_{q,T})+n\mathsf{E}_{q,S}$
LMA-ABUIPFE (Sect. 6)	256	$\lvert\mathsf{PK}_\theta\rvert=256s_{\mathsf{max}}$	$256(s_{\mathsf{max}}+1)$	$[n+\ell s_{\mathsf{max}}(n+2)]256$	$(n+n\ell)\mathsf{E}_{q,T}+[\ell s_{\mathsf{max}}(n+3)-\ell(n+1)]\mathsf{E}_{q,S}+(2\ell n(s_{\mathsf{max}}-1))\mathsf{P}_q$	$[\ell+n(s_{\mathsf{max}}-1)](\mathsf{P}_q+\mathsf{E}_{q,T})+\ell s_{\mathsf{max}}\mathsf{P}_q+n\mathsf{E}_{q,S}$

The notations from Table 1 are described below:

- $\lvert\mathsf{PK}_t\rvert/\lvert\mathsf{PK}_\theta\rvert$: size of the public key associated to the attribute t or authority θ
- $\lvert\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\rvert$: size of the secret key associated to the tuple $(\mathsf{GID}, t, \boldsymbol{u})$
- $\lvert\mathsf{CT}\rvert$: size of the ciphertext
- n: length of vectors; ℓ, s_{max}: number of rows and columns in LSSS matrix respectively
- $\mathsf{E}_{N,S}, \mathsf{E}_{q,S}$: exponentiation time in composite and prime order source groups respectively
- $\mathsf{E}_{N,T}, \mathsf{E}_{q,T}$: exponentiation time in composite and prime order target groups respectively
- $\mathsf{P}_N, \mathsf{P}_q$: time to compute a pairing in composite and prime order groups respectively

Table 2. Concrete Efficiency Comparison for 128-bit Security, $n = 200, \ell = 50, s_{\mathsf{max}} = 20$.

Scheme	$\lvert\mathsf{PK}_\theta\rvert$	$\lvert\mathsf{CT}\rvert$	Encrypt Time	Decrypt Time
Agrawal et al. [9]	$\approx$ 147.8 KB	$\approx$ 7.78 MB	$\approx$ 143.7 mins	$\approx$ 4.9 days
MA-ABUIPFE (Sect. 5)	$\approx$ 0.64 KB	$\approx$ 6.44 MB	$\approx$ 63.14 mins	$\approx$ 7.27 mins
LMA-ABUIPFE (Sect. 6)	$\approx$ 0.64 KB	$\approx$ 6.47 MB	$\approx$ 63.2 mins	$\approx$ 7.35 mins

Advantages of Our Schemes Over Agrawal et al. [9] Beyond Unboundedness: Our MA-ABUIPFE schemes have notable advantages in terms of versatility and performance over the MA-ABIPFE of [9], named as AGT-FE hereafter beyond the unboundedness property that we achieve in this work. Firstly, the composite-order group-based AGT-FE is significantly slower than our prime-order constructions [22,25] because of the inherent efficiency gains offered by prime-order bilinear groups. Especially, the size of group elements of a composite-order group $\mathbb{G}_N$ is much larger than that of a prime-order group $\mathbb{G}_q$ for the same security level: 3072-bit length of $\mathbb{G}_N$ compared to 256-bit length of $\mathbb{G}_q$ for the 128-bit security level. Moreover, one pairing operation is more than 250 times slower in $\mathbb{G}_N$ compared to its prime-order counterpart. A concrete comparison of efficiency is depicted in Tables 1 and 2. As we can see, at 128-bit security level, while AGT-FE takes nearly 5 days for a decryption, our scheme only takes several minutes. We also bring down the public key size (which is constant for any arbitrary length vector) by around 99% and at the same time the ciphertext size

is comparable to that of AGT-FE. Thus our constructions mark a significant progress towards the practical deployment of this primitive. Secondly, the security of AGT-FE is based on source-group-assumptions, precisely, various types of subgroup decision assumptions, which are known to be qualitatively stronger than the target-group-based assumptions [11] such as the DBDH assumption considered in this work. The existing transformations from composite-order group-based systems to analogous prime-order group-based systems [16,22,31] that could be applied to AGT-FE, technically replaces the subgroup structures by some vector space structures. Consequently, it incurs additional overheads and potential loss in the efficiency to the resulting prime-order system. Further, the translated scheme would still depend on source group assumptions, e.g. the k-linear or its variants.

Thus, our MA-ABUIPFE exhibits a substantial boost with respect to the performance and at the same time it is secure under a weaker assumption. Furthermore, we extend our MA-ABUIPFE to the large universe setting which has the flexibility to include an unbounded number of attributes under different authorities to the system at any point of time.

Static Security: Our Motivation: The static security may not be the dream security model for MA-ABUIPFE. However, in this work, our main motivation is on performance and versatility. Moreover, as we already mentioned above, we could not find any vulnerability of our schemes against stronger adversaries, e.g., selective adversaries as considered in [9], even though we could not prove it based on the computational assumptions we considered in this paper. Schemes with greater performance and weaker provable security have often found to suit better in practical deployments. Further, weaker security notions have often been a major stepping stone to obtain more advanced security, e.g., adaptive security, for the same primitive. Please note that many primitives like ABE [24,37,42], MA-ABE [19,21,36,43], IPFE [3], and MC-IPFE [1,17], were first built only with selective/static security before being upgraded to adaptive security [10,20,32] based on the same assumptions. Moreover, from a sustainability point of view, it is always important to have a portfolio of candidates for a primitive under various computational assumptions so that if one of the assumptions gets broken, candidates under a different assumption can be deployed. Another motivation for designing a DBDH or related assumption-based scheme is to innovate new techniques that could possibly be translated to the LWE setting, as has previously been done for other FE primitives, e.g., [7,13,19,21].

Paper Organization: The paper is organized as follows. We provide technical overview of our small and large universe MA-ABUIPFE schemes in Sect. 2. Important notations and computational assumptions are given in Sect. 3. The other prerequisites such as definitions of bilinear groups, access structures, LSSS and justification of our newly introduced L-DBDH assumption are given in the full version. We formalize the notion of small and large universe MA-ABUIPFEs for LSSS in Sect. 4. In Sect. 5, we present the construction of small universe MA-ABUIPFE and formally discuss its correctness and security analysis. Next, our LMA-ABUIPFE scheme is described in Sect. 6 whereas its correctness and the security analysis are shifted to the full version. The small universe single authority ABUIPFE scheme along with its correctness and security analysis are provided in the full version.

2 Technical Overview

In this technical overview, we focus on discussing the high level technical details of constructing small universe MA-ABUIPFE since this is where most of our technical ideas lie. For extending it to large universe setting, we depend on the technique of Rouselakis and Waters [36] which we discuss later in this section. Since our goal is to construct the schemes under target-group-based assumptions, we start with the only existing UIPFE scheme of [38] whose security relies on the DBDH assumption. In fact, their UIPFE is designed from the selectively secure (bounded) IPFE of Abdalla et al. [3] using a hash and pairing mechanism.

2.1 Constructing the Small Universe MA-ABUIPFE

In this overview, we denote by q a prime number and by $[\![x]\!]_i$ an element in a group $\mathbb{G}_i$ for $i \in \{1, 2, T\}$. At a high level, given a public key $[\![\alpha]\!]_1$, the encryption algorithm of [38] amplifies entropy by pairing the public key with the outputs of a hash function applied on the indices of the message vectors. More precisely, the ciphertext and secret keys in the [38] UIPFE (DP-UIPFE) takes the following forms.

$$\begin{array}{ll} \mathsf{CT}_{\boldsymbol{v}}: & C_0 = [\![r]\!]_1, \quad \{C_i = [\![v_i]\!]_T \cdot e([\![\alpha]\!]_1, r[\![\mathsf{H}(i)]\!]_2)\}_{i \in \mathcal{I}_{\boldsymbol{v}}}; \quad r \leftarrow \mathbb{Z}_q \\ \mathsf{SK}_{\boldsymbol{u}}: & \qquad\qquad -\alpha \prod_{j \in \mathcal{I}_{\boldsymbol{u}}} \mathsf{H}(j)^{u_j} \end{array}$$

where $\mathcal{I}_{\boldsymbol{u}}, \mathcal{I}_{\boldsymbol{v}} \subset \mathbb{N}$ are the index sets of $\boldsymbol{u}, \boldsymbol{v}$ respectively, the hash function H maps the indices to elements in $\mathbb{G}_2$ and $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ is a prime-order bilinear group. If the index sets are equal, i.e. $\mathcal{I}_{\boldsymbol{u}} = \mathcal{I}_{\boldsymbol{v}} = \mathcal{I}$ then one can use the key vector $\boldsymbol{u}$ to extract $[\![\boldsymbol{u} \cdot \boldsymbol{v}]\!]_T$ from the product $\prod_{j \in \mathcal{I}} C_j^{u_j}$ and a single pairing $e(C_0, \mathsf{SK}_{\boldsymbol{u}})$. As a natural first step, we seek to utilize the DP-UIPFE to upgrade an existing MA-ABE to a small universe MA-ABUIPFE scheme.

As the aim is to rely on the target-group-based assumption, we consider the DBDH-based MA-ABE of Datta, Komargodski and Waters (DKW-MA-ABE) [21] for this upgrade. As a simpler first step, we investigate the primitive in the bounded and small universe setting, that is, the number of authorities and vector lengths are bounded and each authority controls a single attribute.

2.1.1 The First Step: A Bounded MA-ABIPFE Scheme

Let us start by adding the functionality of IPFE on top of DKW-MA-ABE. For each authority t, the public key and master secret key in the DKW-MA-ABE construction are given by $\mathsf{PK}_t = ([\![\alpha_t]\!]_T, [\![y_{t,2}]\!]_1, \ldots, [\![y_{t,s_{\max}}]\!]_1)$ and $\mathsf{MSK}_t = (\alpha_t, y_{t,2}, \ldots, y_{t,s_{\max}})$ where $s_{\max}$ is a bound on the maximum number of columns in the LSSS access structure and $\alpha_t, y_{t,2}, \ldots, y_{t,s_{\max}} \leftarrow \mathbb{Z}_q$. In order to construct an MA-ABIPFE scheme from the DKW-MA-ABE, we convert the components of MSK_t from scalars to vectors whose lengths are fixed according to the vector length bound of the system. All the other components are similarly upgraded to either vectors or matrices of *fixed* dimensions. In particular, the resulting MA-ABIPFE derived from DKW-MA-ABE can be described in

the following way where $P = (\mathbf{M} = (M_{i,j})_{\ell \times s_{\max}}, \rho : [\ell] \to \mathcal{AU})$ is the LSSS access policy associated with the ciphertexts, $\mathcal{AU}$ is the set of all authorities, and $\boldsymbol{M}_i$ denotes the i-th row of $\mathbf{M}$.

$$
\begin{aligned}
\mathsf{PK}_t : \quad & (\llbracket \boldsymbol{\alpha}_t \rrbracket_T, \llbracket \boldsymbol{y}_{t,2} \rrbracket_1, \ldots, \llbracket \boldsymbol{y}_{t,s_{\max}} \rrbracket_1) \\
\mathsf{MSK}_t : \quad & (\boldsymbol{\alpha}_t, \boldsymbol{y}_{t,2}, \ldots, \boldsymbol{y}_{t,s_{\max}}) \\
\mathsf{CT}_{\boldsymbol{v},P} : \quad & C_0 = \llbracket \boldsymbol{v} + \boldsymbol{z} \rrbracket_T, \quad C_{1,i} = \llbracket \boldsymbol{M}_i \mathbf{B} + r_i \boldsymbol{\alpha}_{\rho(i)} \rrbracket_T, \\
& C_{2,i} = \llbracket r_i \rrbracket_1, \qquad C_{3,i,j} = \llbracket M_{i,j} \boldsymbol{x}_j + r_i \boldsymbol{y}_{\rho(i),j} \rrbracket_1 \ \ \forall i \in [\ell], j \in [2, s_{\max}] \\
\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}} : \quad & \llbracket \boldsymbol{\alpha}_t \cdot \boldsymbol{u} \rrbracket_2 \cdot \prod_{j=2}^{s_{\max}} \mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j)^{\boldsymbol{y}_{t,j} \cdot \boldsymbol{u}}
\end{aligned}
$$

where $\boldsymbol{z} \leftarrow \mathbb{Z}_q^n, r_i \leftarrow \mathbb{Z}_q$ and n represents the length of $\boldsymbol{u}, \boldsymbol{v}$. Further, $\mathbf{B} \in \mathbb{Z}_q^{s_{\max} \times n}$ and $\{\boldsymbol{x}_j \leftarrow \mathbb{Z}_q^n\}_{j \in [2, s_{\max}]}$ are the secret shares of $\boldsymbol{z}$ and $\mathbf{0}$ respectively. Recall that the decryption algorithm of MA-ABIPFE requires a set of secret keys $\{\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\}_{t \in S}$ for the same user identifier GID and an authorized subset S of attributes featuring in the LSSS access policy associated with the ciphertext in order to decrypt it. Given such a collection of keys , the decryption algorithm gets rid of the masking term from $C_0 \cdot \boldsymbol{u}$ by computing

$$
\llbracket \boldsymbol{u} \cdot \boldsymbol{z} \rrbracket_T = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \boldsymbol{u} \cdot \prod_{j=2}^{s_{\max}} e\left(\mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j), C_{3,i,j} \cdot \boldsymbol{u}\right)}{e\left(\mathsf{SK}_{\mathsf{GID},\rho(i),\boldsymbol{u}}, C_{2,i}\right)} \right]^{w_i} \tag{2.1}
$$

where I represents the rows of $\mathbf{M}$ associated to S. Note that the Eq. (2.1) holds as the decryption algorithm can efficiently find a coefficients $\{w_i \in \mathbb{Z}_q\}_{i \in I}$ satisfying $(1, 0, \ldots, 0) = \sum_{i \in I} w_i \boldsymbol{M}_i$ whenever the attributes linked to the rows in I satisfies the policy $(\mathbf{M}, \rho)$.

The role of the public hash function H is to tie together a set of independently generated secret keys under the same user identifier GID while decrypting. In the security proof, H is treated as a random oracle to ensure that a fresh randomness is produced for each user identity GID that links together the different secret keys generated for it and it is infeasible for an adversary to mix and match secret keys generated with respect to different global identifiers even if the attributes associated with those secret keys satisfy the access policy associated with the ciphertext.

In fact, the above bounded MA-ABIPFE scheme can be proven secure in the static model under the DBDH assumption. Let us now proceed to transform the bounded scheme into an unbounded one using the idea of DP-UIPFE sketched above. Unfortunately, a straightforward approach does not work. In particular, we face a few difficulties while incorporating the hash and pairing mechanism of [38] with the DKW-MA-ABE as we describe below.

2.1.2 Challenges in Expanding Authority Keys on the Fly and Our Approach

The foremost problem arises in vectorizing the components of the authority master secret keys MSK_t. This is because there being no upper bound on the length of vectors, we cannot simply use random vectors of predetermined sizes in the vectorization process. Rather, we must provision for generating the components of the vectors on the fly as needed during encryption/key generation. Similar to the idea of [38], we use hash functions modeled as random oracles in order to resolve this issue. More precisely,we proceed as follows: An authority t generates the public/master secret keys as $(\mathsf{PK}_t = ([\![\alpha_t]\!]_T, [\![y_{t,2}]\!]_1, \ldots, [\![y_{t,s_{\max}}]\!]_1), \mathsf{MSK}_t = (\alpha_t, y_{t,2}, \ldots, y_{t,s_{\max}}))$ without knowing the vector lengths where $\alpha, y_{t,2}, \ldots, y_{t,smx}$ are still scalars. To maintain the simplicity of this overview, we assume that the vectors $\boldsymbol{u} = (u_k)_{k \in \mathcal{I}_u}$ and $\boldsymbol{v} = (v_k)_{k \in \mathcal{I}_v}$ are both associated with the index set $\mathcal{I}_{\boldsymbol{u}} = \mathcal{I}_{\boldsymbol{v}} = \mathcal{I} = [n]$ which is unknown to the authority setup. Then the scalar α_t could be vectorized using a hash function H_1 as follows.

$$\begin{aligned} \text{during encryption}: \quad & C_{1,i} = [\![\boldsymbol{M}_i \mathbf{B} + \boldsymbol{\vartheta}_i]\!]_T \\ & \text{where } [\![\vartheta_{i,k}]\!]_T = e(r_i [\![\alpha_{\rho(i)}]\!]_1, \mathsf{H}_1(\rho(i) \parallel k \parallel \mathcal{I})) \\ \text{during key generation}: \quad & \boldsymbol{\alpha}_t \cdot \boldsymbol{u} = \prod_{k=1}^{n} \mathsf{H}_1(t \parallel k \parallel \mathcal{I})^{\alpha_t \cdot u_k} \end{aligned}$$

The next step is to vectorize the authority master secret key components $y_{t,j}$ according to the vector lengths. One may hope to apply [38] idea to extend $y_{t,j}$ to the same length of the vectors on the fly in a similar way. To see whether it works, let us assume that the hash function H used in the key generation in the above bounded MA-ABIPFE additionally takes an index position and an index set as inputs. That is, let us do the following modification for the key generation of the bounded MA-ABIPFE scheme

$$\mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j)^{y_{t,j} \cdot \boldsymbol{u}} \longrightarrow \prod_{k=1}^{n} \mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k \parallel \mathcal{I})^{y_{t,j} \cdot u_k}$$

Thus, using this idea, it is possible to expand $y_{t,j}$ to a vector $\boldsymbol{y}_{t,j}$ of the same length as the key vector $\boldsymbol{u}$ and eventually enabling an authority to compute the term $\mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k \parallel \mathcal{I})^{\boldsymbol{y}_{t,j} \cdot \boldsymbol{u}}$ while generating keys for an unbounded length vector. Note that, the hash value $\mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k \parallel \mathcal{I})$ has GID and $\boldsymbol{u}$ as inputs. Therefore, this would call for the following modification in the ciphertext computation.

$$\begin{aligned} & C_{3,i,j} = [\![M_{i,j} \boldsymbol{x}_j + \varsigma_{i,j}]\!]_T \\ & \text{where } [\![\varsigma_{i,j,k}]\!]_T = e(r_i [\![y_{\rho(i),j}]\!]_1, \mathsf{H}(\boxed{\mathsf{GID}} \parallel \boxed{\boldsymbol{u}} \parallel j \parallel k \parallel \mathcal{I})) \end{aligned}$$

However, such a vector $[\![\boldsymbol{y}_{t,j}]\!]_1$ is not known or rather the k-th element $e([\![y_{t,j}]\!]_1, \mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k \parallel \mathcal{I}))$ can not be computed during encryption. The main reason is that the global identity GID and the vector $\boldsymbol{u}$ are available when an authority generates a secret key, but the encryption algorithm is oblivious of which GID or $\boldsymbol{u}$ will be used to decrypt the ciphertext. In fact, it is natural that the same ciphertext would

be decrypted by several users with different GID and $\boldsymbol{u}$ vectors. Hence, a simple hash and pairing technique similar to DP-UIPFE is not sufficient for a data owner to encrypt unbounded length vectors.

At this point, we devise a correlated "hash-decomposition" mechanism which enables us to compute the value of a hash function by combining the outputs of several hash functions applied on different segments of the input to the original hash function. More precisely, our idea is to define the hash value $\mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k \parallel \mathcal{I})$ by grouping two independently generated hash values as

$$\mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k \parallel \mathcal{I}) = \mathsf{H}_2(j \parallel k \parallel \mathcal{I}) \cdot \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k) \tag{2.2}$$

where H_2 and H_3 are two new public hash functions generated during global setup. Now, we observe that the first hash value $\mathsf{H}_2(j \parallel k \parallel \mathcal{I})$ in the product can be computed without knowing GID, which in turn enable the encryptor to expand an authority public key component $[\![y_{t,j}]\!]_1$ into a vector $[\![\boldsymbol{y}^{(2)}_{t,j}]\!]_T$ as $[\![y^{(2)}_{t,j,k}]\!]_T = e([\![y_{t,j}]\!]_1, \mathsf{H}_2(j \parallel k \parallel \mathcal{I}))$. Similarly, an authority expands the master secret key component $y_{t,j}$ into vectors $[\![\boldsymbol{y}^{(2)}_{t,j}]\!]_2$ and $[\![\boldsymbol{y}^{(3)}_{t,j}]\!]_2$ as $[\![y^{(2)}_{t,j,k}]\!]_2 = \mathsf{H}_2(j \parallel k \parallel \mathcal{I}))^{y_{t,j}}$ and $[\![y^{(3)}_{t,j,k}]\!]_2 = \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k)^{y_{t,j}}$ respectively while generating a secret key for a vector $\boldsymbol{u}$. However, at this point, it is not immediate how would the vector $[\![\boldsymbol{y}^{(2)}_{t,j}]\!]_T$ be useful for the encryption algorithm.

Next, we carefully look into the decryption equation of the bounded MA-ABIPFE scheme described above (Eq. (2.1)) and try to adapt it for the MA-ABUIPFE setting with the modifications we did so far. We note that the pairing operation in the numerator can be rearranged with the hash function H replaced by H_2 as

$$\begin{aligned} e\left(\mathsf{H}_2(j \parallel k \parallel \mathcal{I}), C_{3,i,j} \cdot \boldsymbol{u}\right) &= e(\mathsf{H}_2(j \parallel k \parallel \mathcal{I}), (M_{i,j}\boldsymbol{x}_j + r_i \boldsymbol{y}_{\rho(i),j}) \cdot \boldsymbol{u}) \\ &= e(\mathsf{H}_2(j \parallel k \parallel \mathcal{I}), M_{i,j}\boldsymbol{x}_j \cdot \boldsymbol{u}) \cdot [\![r_i \boldsymbol{y}^{(2)}_{\rho(i),j} \cdot \boldsymbol{u}]\!]_T \end{aligned}$$

Since $\boldsymbol{u}$ is not available during encryption, we only compute the above term without multiplying by $\boldsymbol{u}$ and represent it as a single element

$$C_{3,i,j,k} = e([\![M_{i,j}x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel k \parallel \mathcal{I})) \cdot [\![r_i y^{(2)}_{\rho(i),j,k}]\!]_T.$$

Therefore, the hash-decomposition mechanism allows the encryptor to simulate the *first* part of the hash value $\mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k \parallel \mathcal{I})$ from Eq. (2.2) using the hash function H_2. The second part of the hash value still remains to be handled. For this, we generate an additional layer of secret share of zero by sampling $f_2, \ldots, f_{s_{\mathsf{max}}} \in \mathbb{Z}_q$ and introduce the encodings $C_{4,i,j} = [\![M_{i,j}f_j + r_i y_{\rho(i),j}]\!]_1$ for all $i \in [\ell], j \in [2, s_{\mathsf{max}}]$ within the ciphertext. At the time of decryption, $C_{4,i,j}$ will be paired with the term $\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k)^{u_k}$. Thus, combining $C_{3,i,j,k}$ and $C_{4,i,j}$ via the hash-decomposition mechanism we are able to distribute the execution of the pairing operation from (Eq. (2.1)) among the encryption and decryption algorithms as follows:

$$
\begin{aligned}
& e\left(\mathsf{H}(\mathsf{GID} \parallel \boldsymbol{u} \parallel j), C_{3,i,j} \cdot \boldsymbol{u}\right) && \text{as in MA-ABIPFE decryption (ref: Eq. (2.1))} \\
& \longrightarrow \prod_{k=1}^{n} C_{3,i,j,k} \cdot u_k \ \cdot \ e(C_{4,i,j}, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k)^{u_k}) && \text{new decryption strategy for MA-ABUIPFE} \\
& = C_{i,j}^{(3,4)}(\boldsymbol{u}) && \text{(say)}
\end{aligned}
$$

Equipped with these concepts, we state our final MA-ABUIPFE scheme below by assuming $\mathcal{I}_{\boldsymbol{u}} = \mathcal{I}_{\boldsymbol{v}} = \mathcal{I} = [n]$.

$$
\begin{aligned}
\mathsf{PK}_t : \ & (\llbracket \alpha_t \rrbracket_T, \llbracket y_{t,2} \rrbracket_1, \ldots, \llbracket y_{t,s_{\mathsf{max}}} \rrbracket_1) \\
\mathsf{MSK}_t : \ & (\alpha_t, y_{t,2}, \ldots, y_{t,s_{\mathsf{max}}}) \\
\mathsf{CT}_{\boldsymbol{v},P} : \ & C_0 = \llbracket \boldsymbol{v} + \boldsymbol{z} \rrbracket_T, \quad C_{1,i} = \llbracket \boldsymbol{M}_i \mathbf{B} + \boldsymbol{\vartheta}_i \rrbracket_T, \quad C_{2,i} = \llbracket r_i \rrbracket_1, \\
& C_{3,i,j,k} = e(\llbracket M_{i,j} x_{j,k} \rrbracket_1, \mathsf{H}_2(j \parallel k \parallel \mathcal{I})) \cdot \llbracket r_i y^{(2)}_{\rho(i),j,k} \rrbracket_T, \\
& C_{4,i,j} = \llbracket M_{i,j} f_j + r_i y_{\rho(i),j} \rrbracket_1, \quad \forall i \in [\ell], \ j \in [2, s_{\mathsf{max}}], \ k \in [n] \\
\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}} : \ & \prod_{k=1}^{n} \mathsf{H}_1(t \parallel k \parallel \mathcal{I})^{\alpha_t \cdot u_k} \cdot \prod_{j=2}^{s_{\mathsf{max}}} \prod_{k=1}^{n} (\llbracket y^{(2)}_{t,j,k} \rrbracket_2 \cdot \llbracket y^{(3)}_{t,j,k} \rrbracket_2)^{u_k}
\end{aligned}
$$

The components $\boldsymbol{\vartheta}_i, y^{(2)}_{t,j,k}, y^{(3)}_{t,j,k}$ are defined as above. The decryption follows by canceling the masking term from $C_0 \cdot \boldsymbol{u}$ using a similar computation like in Eq. (2.1) executed as

$$
\llbracket \boldsymbol{u} \cdot \boldsymbol{z} \rrbracket_T = \prod_{i \in I} \left[\frac{C_{1,i} \cdot \boldsymbol{u} \cdot \prod_{j=2}^{s_{\mathsf{max}}} C_{i,j}^{(3,4)}(\boldsymbol{u})}{e\left(\mathsf{SK}_{\mathsf{GID},\rho(i),\boldsymbol{u}}, C_{2,i}\right)} \right]^{w_i} \tag{2.3}
$$

We next look into the security of the proposed construction. Here again, we face several challenges while adapting the security proof of [21,38] into our setting.

2.1.3 Challenges in the Security Analysis and Our Approach

The main difference between the MA-ABE and MA-ABUIPFE security model is in the secret key queries made by the adversary. This is because MA-ABUIPFE is more like an FE scheme and the adversary is entitled to ask for secret keys that would decrypt the challenge ciphertext which is in contrast to any MA-ABE scheme where only non-authorized keys are released. On the other hand, proving security of MA-ABUIPFE is more technically challenging compared to the (bounded) MA-ABIPFE (like AGT-FE [9]) as an authorized key which always leads to a successful decryption in case of MA-ABIPFE, may not be eligible for decrypting a ciphertext of MA-ABUIPFE. The index set associated with the authorized key must match to the index set of the encrypted vector for successful decryption in MA-ABUIPFE. In other words, the adversary should be restricted to infer any information about the encrypted message vector from the authorized keys whose index sets are not equal to the index set of the message vector. Moreover, AGT-FE is proven secure under subgroup decision assumptions which are

source group assumptions while our target is to prove security under DBDH which is a target group assumption, thus the dual system encryption technique [41] used for the security proof of AGT-FE does not work in our case. Hence, we design a different proof strategy that works coherently with the hash-decomposition mechanism and for target group assumptions in the prime-order bilinear group.

We prove the security of our MA-ABUIPFE in the static model similar to the DKW-MA-ABE. The adversary is asked to submit all it's queries including the challenge message vectors $\boldsymbol{v}_0, \boldsymbol{v}_1$ with a common index set $\mathcal{I}^*$ and an associated challenge access structure $(\mathbf{M}, \rho)$. Recall that the adversary can also corrupt or even maliciously generate some of the authorities indicated by a set $\mathcal{C}$ of corrupted authorities or attributes. Let us consider a DBDH instance $([\![a]\!]_1, [\![b]\!]_2, [\![c]\!]_1, [\![\tau]\!]_T)$ where τ is either abc or random. In the first step, we use the information-theoretic *partitioning* lemma, the so-called "zero-out" lemma [36, Lemma 1], to isolate and ignore the set of rows of $\mathbf{M}$ that correspond to the corrupted authorities throughout the analysis. In particular, the lemma allows us to replace the LSSS matrix $\mathbf{M}$ with an updated simpler matrix $\mathbf{M}'$ such that a subset of columns, say $C_{\mathbf{M}'}$, of $\mathbf{M}'$ can be set to zero that are related to the corrupted authorities. Next, we follow the proof techniques of [3,38] and sample a basis $\widetilde{S} = \{(\boldsymbol{v}_0 - \boldsymbol{v}_1), \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ of $\mathbb{Z}_q^n$ where n denotes the size of $\mathcal{I}^*$ to represent key vectors $\boldsymbol{u}$ whose lengths are equal to n. However, answering the hash and secret key queries require a careful treatment while embedding the DBDH challenge instance. The role of the hash function of DKW-MA-ABE was limited to simulating the non-authorized keys of a fixed length. However, in our case, we need to deal with both authorized and unauthorized keys and here again, our hash-decomposition mechanism plays a crucial role. Moreover, a key can be non-authorized with respect to the index set or the associated policy, or both.

Let S be the set of attributes queried under a user identifier GID as a part of secret key queries such that S contains at least an attribute involved in the challenge policy. The main idea of simulating secret keys of DKW-MA-ABE was to sample a special vector $\boldsymbol{d} \in \mathbb{Z}_q^{s_{\max}}$ such that the inner product of $\boldsymbol{d}$ with $\boldsymbol{M}_i'$ is zero for all $i \in \rho^{-1}(S \cup \mathcal{C})$ and to set the hash values as

$$\mathsf{H}(\mathsf{GID} \parallel j) = (g_2^b)^{d_j} \cdot g_2^{h_j},\ \forall j \in C_{\mathbf{M}'},\ \text{and uniform otherwise.} \tag{2.4}$$

This, in fact, enables in simulating the secret keys using the properties of $\boldsymbol{d}$ and by embedding the matrix $\mathbf{M}'$ into the public keys of authorities linked to the challenge policy. Unfortunately, we observe that such encoding of hash values is not compatible with our hash-decomposition mechanism. Firstly, the hash function H_2 does not take a GID as input and hence it is not possible to encode the hash values depending on a vector like $\boldsymbol{d}$ which is sampled according to an unauthorized set of attributes $(S \cup \mathcal{C})$ under a given global identity. In our case, H_2 should generate a good amount of entropy for indices of key vectors irrespective of any global identity. This would restrict an adversary to gain any illegitimate information about the encrypted message from any secret key where the associated index set does not match with $\mathcal{I}^*$ even though the attributes associated to the key satisfy the challenge policy. Secondly, H_3 takes a GID as it's input along with a key vector, a column number and an index set. The role of H_3

is to make a secret key generated under a given GID useless to the adversary whenever the associated attributes does not satisfy the challenge policy.

In the static security model the simulator knows all the secret key queries in advance. We exploit this fact to prepare encodings for the hash values keeping in mind their roles in the security experiment. Our idea is to sample all possible $\{\boldsymbol{d}_\phi\}_\phi$ vectors corresponding to the sets $\{S_\phi \cup \mathcal{C}\}_\phi$ such that $S_\phi \cup \mathcal{C}$ constitutes an unauthorized subset of row of $\mathbf{M}$ and use the information of $\{\boldsymbol{d}_\phi\}_\phi$ in the encodings of the hash functions. More precisely, we use an *add and subtract* technique to set the hash values as follows

$$\mathsf{H}_2(j \parallel k \parallel \mathcal{I}^*) = (g_2^b)^{\sum_\phi d_{\phi,j}} \cdot g_2^{h_{2,j}},\ \forall j \in C_{\mathbf{M}'},\ \text{and uniform otherwise.}$$
$$\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_{\phi'} \parallel j \parallel k) = (g_2^b)^{\sum_{\phi \neq \phi'} -d_{\phi,j}} \cdot g_2^{h_{3,j}},\ \forall j \in C_{\mathbf{M}'},\ \text{and uniform otherwise.}$$

Now, we multiply the above hash encodings while simulating non-authorized secret key queries and obtain a hash encoding similar to Eq. (2.4).

$$\mathsf{H}_2(j \parallel k \parallel \mathcal{I}^*) \cdot \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_{\phi'} \parallel j \parallel k) = (g_2^b)^{d_{\phi',j}} \cdot g_2^{h_{2,j}+h_{3,j}}\ \forall j \in C_{\mathbf{M}'}.$$

For simplicity of this section, we have ignored a few additional elements in the above encodings that connect the hash values with the H_1 encodings which actually facilitates in using the fact that $\boldsymbol{d}_\phi \cdot \boldsymbol{M}_i' = 0$ for all $i \in \rho^{-1}(S_\phi \cup \mathcal{C})$ for non-authorized keys such that $\mathcal{I}_{\boldsymbol{u}_\phi} = \mathcal{I}^*$. Lastly, when simulating authorized secret keys we use the basis $\widetilde{S}$ to obtain a vector $\boldsymbol{\eta}$ satisfying $\boldsymbol{\eta} \cdot \boldsymbol{u}_\phi = 0$ with the help of the admissibility condition $\boldsymbol{u}_\phi \cdot (\boldsymbol{v}_0 - \boldsymbol{v}_1) = 0$ for all keys leading to a successful decryption of the challenge ciphertext. The full security analysis can be found in Sect. 5.3.

2.2 Constructing the Large Universe MA-ABUIPFE

We recall that in the large universe setting each authority is allowed to control exponentially many attributes. We upgrade our small universe scheme to a large universe MA-ABUIPFE (LMA-ABUIPFE) by extending the techniques presented in [36] from encrypting a fixed length message to encrypting an unbounded length vector in the context of MA-ABUIPFE. To support exponentially many attributes, we use an additional hash function R which maps arbitrary attributes to elements of $\mathbb{G}_2$. We replace the map ρ of the LSSS access structure $(\mathbf{M}, \rho)$ by decomposition of two mappings T and δ, that is $\rho(i) = \mathsf{T}(\delta(i)) = \theta$ where δ labels row numbers i of the LSSS access matrix to some attributes $\delta(i)$ and T assigns the attributes $\delta(i)$ to its respective authorities denoted by θ. Our LMA-ABUIPFE is described as follows.

$$
\begin{aligned}
\mathsf{PK}_\theta &: ([\![\alpha_\theta]\!]_T, [\![y_{\theta,2}]\!]_1, \ldots, [\![y_{\theta,s_{\max}}]\!]_1)\\
\mathsf{MSK}_\theta &: (\alpha_\theta, y_{\theta,2}, \ldots, y_{\theta,s_{\max}})\\
\mathsf{CT}_{\boldsymbol{v},P} &: \begin{array}{c} C_0 = [\![\boldsymbol{v}+\boldsymbol{z}]\!]_T, \quad C_{1,i} = [\![\boldsymbol{M}_i\mathbf{B}+\boldsymbol{\vartheta}_i]\!]_T, \quad C_{2,i} = [\![r_i]\!],\\ C_{3,i,j,k} = e([\![M_{i,j}x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel k \parallel \mathcal{I})) \cdot [\![r_i y^{(2)}_{\rho(i),j,k}]\!]_T,\\ C_{4,i,j} = [\![M_{i,j}f_j + r_i y_{\rho(i),j}]\!]_1, \quad C_{5,i,j} = \mathsf{R}(\delta(i) \parallel j \parallel \mathcal{I})\\ \forall i \in [\ell],\ j \in [2, s_{\max}],\ k \in [n] \end{array}\\
\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}} &: \begin{array}{l} \prod_{k=1}^{n} \mathsf{H}_1(t \parallel k \parallel \mathcal{I})^{\alpha_\theta \cdot u_k} \cdot \prod_{j=2}^{s_{\max}} \prod_{k=1}^{n} ([\![y^{(2)}_{\theta,j,k}]\!]_2 \cdot [\![y^{(3)}_{\theta,j,k}]\!]_2)^{u_k} \cdot \prod_{j=1}^{s_{\max}} \mathsf{R}(t \parallel j \parallel \mathcal{I})^{\tau_j},\\ \mathsf{Z}_{t,j} = [\![\tau_j]\!]_1, \ \ \forall j \in [s_{\max}] \end{array}
\end{aligned}
$$

The components $\boldsymbol{\vartheta}_i, \boldsymbol{y}^{(2)}_{\theta,j}, \boldsymbol{y}^{(3)}_{\theta,j}$ are defined similarly as in our MA-ABUIPFE scheme.

$$
\begin{aligned}
[\![\vartheta_{i,k}]\!]_T &= e(r_i[\![\alpha_{\rho(i)}]\!]_1, \mathsf{H}_1(\rho(i) \parallel k \parallel \mathcal{I}_{\boldsymbol{v}})),\\
[\![y^{(2)}_{\theta,j,k}]\!]_T &= e([\![y_{\theta,j}]\!]_1, \mathsf{H}_2(j \parallel k \parallel \mathcal{I})), \ \ [\![y^{(2)}_{\theta,j,k}]\!]_2 = \mathsf{H}_2(j \parallel k \parallel \mathcal{I})^{y_{\theta,j}},\\
[\![y^{(3)}_{\theta,j,k}]\!]_2 &= \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel k)^{y_{\theta,j}}, \ \ \forall k \in [n].
\end{aligned}
$$

The decryption procedure is similar to our MA-ABUIPFE scheme. We consider static security of LMA-ABUIPFE and model the hash functions as random oracles. However, it may not be possible to base security on the plain DBDH assumption. Following the same notations that we used to sketch the proof technique of our MA-ABUIPFE, we discuss the main reason which prevent using the DBDH assumption as before. The R-values related to the authorities in the challenge policy in our proposed LMA-ABUIPFE scheme described above are roughly set as $\mathsf{R}(t \parallel j \parallel \mathcal{I}^*) = g_2^{\zeta_{t,j}} g_2^{aM'_{i,j}}$, where $\zeta_{t,j}$ is a random $\mathbb{Z}_q$-element and $M'_{i,j}$ is the (i,j)-th entry of the updated LSSS matrix $\mathbf{M}'$ in the challenge policy. On the other hand, the randomness r_i used in the encryption[2] are set as $r_i = c$. Hence, the reduction requires the group element g_2^{ac} in order to simulate the components $C_{5,i,j}$ of the challenge ciphertext. However, the DBDH assumption does not make it possible to make g^{ac} available to an adversary.

Thus, for basing the security, we look into the parameterized versions of the DBDH assumptions. Unlike [36] where they consider a much more complex parameterized assumption, a primary motivation of our security reduction is to depend on a simpler parameterized assumption that is as close as possible to the plain DBDH assumption. More specifically, [36] consider an *exponent* type assumption where each instance consists of at least $O(L^3_{\max})$ group elements and $L_{\max} \geq \max\{\ell, s_{\max}\}$, where $\ell, s_{\max}$ is the number of rows and columns of the challenge LSSS access matrix respectively. Consequently, the reduction becomes more involved and complex. In contrast, we prove the security of LMA-ABUIPFE based on the newly introduced L-DBDH assumption where each instance has $O(L^2)$ group elements with $L \geq \ell$. We show that the L-DBDH assumption is generically secure using the techniques of [12,36]. Although incomparable with the assumption used in [36], it seems that our L-DBDH assumption is weaker as it contains fewer elements. Therefore, our LMA-ABUIPFE improves upon the previous results of [36] even without considering the enhanced functionality of UIPFE.

[2] The ciphertext is re-randomized to ensure the distribution of its components is unharmed.

There are some other technical hurdles in the security reduction that does not directly allow using the *program and cancel* technique similar to [36] while simulating secret key queries. This is due to the fact that we are handling unbounded length messages and using a hash-decomposition mechanism on top of large universe paradigm. In contrast to the small universe scheme, an authority in a queried secret key of LMA-ABUIPFE may be present in the challenge policy but none of their attributes are linked to it. We use our *add and subtract* technique which enables the reduction to combine the decomposed hash values into a single hash value that eventually produces an adequate amount of randomness preventing the leakage of unwanted information about the underlying message vector from such secret keys.

On the other hand, if the authorities as well as some of their controlled attributes are present in the challenge policy but the associated secret key is unauthorized then we observe that the program and cancel technique of [36] is not sufficient to handle an adversary of LMA-ABUIPFE given the fact that it can query for secret keys corresponding to vectors of arbitrary lengths. In order to make these secret keys useless for an adversary irrespective of the associated lengths of vectors, we delicately program the hash queries that enables the reduction to procreate additional entropy via an interplay between the *program and cancel* technique of [36] and *add and subtract* mechanism of ours at the time of simulating such unauthorized secret keys. Although the high-level proof technique is inspired from [36], the technical obstacles mentioned above prevent applying their approach straightforwardly into our setting. As a whole, we carefully embed the L-DBDH instance into the adversary's queries by extending the [36] technique in the context of amplifying entropy for supporting computation over unbounded length vectors and at the same time making it compatible for hash-decomposition mechanism used in our scheme. We present a detailed security analysis in the full version.

3 Preliminaries

In this section, we present the notations used in this paper and the new L-DBDH assumption we introduce.

3.1 Notations

We will denote the underlying security parameter by λ throughout the paper. A function $\mathsf{negl} : \mathbb{N} \rightarrow \mathbb{R}$ is said to be a negligible function of λ, if for every $c \in \mathbb{N}$, there exists a $\lambda_c \in \mathbb{N}$ such that $\forall \lambda > \lambda_c$, $\mathsf{negl}(\lambda) < \lambda^{-c}$. We denote the set of positive integers $\{1, \ldots, n\}$ as $[n]$. We denote $\emptyset$ as the empty set. We use the abbreviation PPT for probabilistic polynomial-time. For a set X, we write $x \leftarrow X$ to denote that x is sampled according to the uniform distribution over the elements of X. Also for any set X, we denote by $|X|$ and 2^X the cardinality and the power set of the set X respectively. We use bold lower case letters, such as $\boldsymbol{v}$, to denote vectors and upper-case, such as $\mathbf{M}$, for matrices. We assume all vectors, by default, are row vectors. The i^{th} row of a matrix is denoted by $\boldsymbol{M}_i$ and analogously for a set of row indices I, we denote $\mathbf{M}_I$ for the sub-matrix of $\mathbf{M}$ that consists of the rows $\mathbf{M}_i, \forall i \in I$. By $\mathsf{rowspan}(\mathbf{M})$, we denote the linear span of the rows of a matrix $\mathbf{M}$.

For an integer $q \geq 2$, we let $\mathbb{Z}_q$ denote the ring of integers modulo q. We represent $\mathbb{Z}_q$ as integers in the range $(-q/2, q/2]$. The set of matrices of size $m \times n$ with elements in $\mathbb{Z}_q$ is denoted by $\mathbb{Z}_q^{m \times n}$. The operation $(\cdot)^\top$ denotes the transpose of vectors/matrices. Let $\boldsymbol{u} = (u_i)_{i \in \mathcal{I}_u} \in \mathbb{Z}_q^{|\mathcal{I}_u|}, \boldsymbol{v} = (v_i)_{i \in \mathcal{I}_v} \in \mathbb{Z}_q^{|\mathcal{I}_v|}$ where $\mathcal{I}_{\boldsymbol{u}}$ and $\mathcal{I}_{\boldsymbol{v}}$ are the associated index sets, then the inner product between the vectors is denoted as $\boldsymbol{v} \cdot \boldsymbol{u} = \boldsymbol{u}^\top \boldsymbol{u} = \sum_{i \in \mathcal{I}} u_i v_i \in \mathbb{Z}_q$ whenever $\mathcal{I}_{\boldsymbol{u}} = \mathcal{I}_{\boldsymbol{v}} = \mathcal{I}$.

3.2 Complexity Assumptions

We use bilinear groups of prime order to build our MA-ABUIPFE schemes.

Here, we formally define the DBDH assumption and a parameterized version of it, we call L-DBDH which would underlie of security of our small and large universe MA-ABUIPFE schemes respectively.

Assumption 3.1 (Decisional Bilinear Diffie-Hellman (DBDH). [14,38]) *For a security parameter $\lambda \in \mathbb{N}$, let $\mathsf{G} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g, e) \leftarrow \mathcal{G}(1^\lambda)$ be a bilinear group and let $a, b, c \leftarrow \mathbb{Z}_q$. The* DBDH *assumption states that for any* PPT *adversary $\mathcal{A}$, there exists a negligible function* negl *such that for any security parameter $\lambda \in \mathbb{N}$, given the distribution $(\mathsf{G}, [\![a]\!]_1, [\![c]\!]_1, [\![a]\!]_2, [\![b]\!]_2, [\![\tau]\!]_T)$, $\mathcal{A}$ has advantage*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DBDH}}(\lambda) = \left| \Pr\left[1 \leftarrow \mathcal{A}\left(1^\lambda, \mathcal{D}, [\![abc]\!]_T\right)\right] - \Pr\left[1 \leftarrow \mathcal{A}\left(1^\lambda, \mathcal{D}, [\![\tau]\!]_T\right)\right] \right| \leq \mathsf{negl}(\lambda),$$

Assumption 3.2 (L-Decisional Bilinear Diffie-Hellman (L-DBDH)). *Let $\mathsf{G} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g, e) \leftarrow \mathcal{G}(1^\lambda)$ be a bilinear group and let $a, b, c, \mu_1, \ldots, \mu_L \leftarrow \mathbb{Z}_q$. The L-*DBDH *assumption states that for any* PPT *adversary $\mathcal{A}$, there exists a negligible function* negl *such that for any security parameter $\lambda \in \mathbb{N}$, given the distribution*

$$\left(\mathsf{G}, \begin{pmatrix} [\![b]\!]_1, [\![c]\!]_1, \\ [\![a]\!]_2, [\![b]\!]_2 \end{pmatrix}, \left\{ \begin{matrix} [\![a\mu_i]\!]_1, [\![c/\mu_i]\!]_1, \\ [\![a\mu_i]\!]_2 \end{matrix} \right\}_{i \in [L]}, \left\{ \begin{matrix} [\![c\mu_\iota/\mu_i]\!]_1, [\![ac\mu_\iota/\mu_i]\!]_1, \\ [\![ac\mu_\iota/\mu_i]\!]_2 \end{matrix} \right\}_{\substack{i, \iota \in [L], \\ i \neq \iota}}, [\![\tau]\!]_T \right)$$

$\mathcal{A}$ has advantage

$$\mathsf{Adv}_{\mathcal{A}}^{L\text{-}\mathsf{DBDH}}(\lambda) = \left| \Pr\left[1 \leftarrow \mathcal{A}\left(1^\lambda, \mathcal{D}, [\![abc]\!]_T\right)\right] - \Pr\left[1 \leftarrow \mathcal{A}\left(1^\lambda, \mathcal{D}, [\![\tau]\!]_T\right)\right] \right| \leq \mathsf{negl}(\lambda),$$

4 Decentralized (Large Universe) MA-ABUIPFE for LSSS

A large universe decentralized multi-authority attribute-based inner-product functional encryption (LMA-ABUIPFE) scheme $\mathsf{LMA\text{-}ABUIPFE} = (\mathsf{GlobalSetup}, \mathsf{LocalSetup}, \mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ for access structures captured by linear secret sharing schemes (LSSS) over some finite field $\mathbb{Z}_q$ with $q = q(\lambda)$ and inner product value space $\mathcal{U}$ consists of five algorithms with the following syntax. We denote by $\mathcal{AU}$ the authority universe and by $\mathcal{GID}$ the universe of users' global identifiers in the system. The attribute universe is denoted as $\mathsf{U}_{\mathsf{att}}$ which may be arbitrary. Further, an authority $\theta \in \mathcal{AU}$ may have any arbitrary number of attributes from $\mathsf{U}_{\mathsf{att}}$ under its control. Following [36], we assume a publicly computable function $\mathsf{T} : \mathsf{U}_{\mathsf{att}} \to \mathcal{AU}$ that maps each attribute $t \in \mathsf{U}_{\mathsf{att}}$ to a unique authority $\theta = T(t)$. The algorithms proceed as follows:

$\mathbf{GlobalSetup}(1^\lambda, s_{\mathsf{max}})$: It is the global setup algorithm which on input the security parameter λ and a maximum width s_{max} of the LSSS matrix, and outputs the global public parameters GP. We assume that GP includes the descriptions of $\mathcal{AU}$ and $\mathcal{GID}$.
$\mathbf{LocalSetup}(\mathsf{GP}, \theta)$: The authority $\theta \in \mathcal{AU}$ runs the local setup algorithm during its initialization with the global parameters GP and generates its public parameters and a master secret key pair $(\mathsf{PK}_\theta, \mathsf{MSK}_\theta)$.
$\mathbf{KeyGen}(\mathsf{GP}, \mathsf{GID}, \mathsf{MSK}_\theta, t, \boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}})$: The key generation algorithm takes input the global parameter GP, a user's global identifier $\mathsf{GID} \in \mathcal{GID}$, a master secret key MSK_θ for authority θ controlling an attribute $t \in \mathsf{U}_{\mathsf{att}}$, and a vector $\boldsymbol{u} \in \mathbb{Z}_q^{|\mathcal{I}_{\boldsymbol{u}}|}$ with an associated index set $\mathcal{I}_{\boldsymbol{u}}$. It outputs a secret key $\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}$ which contains $(\boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}})$.

$\mathbf{Encrypt}(\mathsf{GP}, (\mathbf{M}, \delta), \{\mathsf{PK}_\theta\}_\theta, \boldsymbol{v}, \mathcal{I}_{\boldsymbol{v}})$: The encryption algorithm takes input the global parameter GP, an LSSS access structure $(\mathbf{M}, \delta)$ where $\mathbf{M}$ is a matrix over $\mathbb{Z}_q$ and δ is a row-labeling function that assigns to each row of $\mathbf{M}$ an attribute in $\mathsf{U}_{\mathsf{att}}$. We define the function $\rho : [\ell] \to \mathcal{AU}$ as $\rho(\cdot) := \mathsf{T}(\delta(\cdot))$ which maps row indices of $\mathbf{M}$ to authorities $\theta \in \mathcal{AU}$. Accordingly, the encryption algorithm further takes a set $\{\mathsf{PK}_\theta\}_\theta$ of public keys for all the authorities in the range of ρ, and a message vector $\boldsymbol{v} \in \mathbb{Z}_q^{|\mathcal{I}_{\boldsymbol{v}}|}$ with an associated index set $\mathcal{I}_{\boldsymbol{v}}$. It outputs a ciphertext CT. We assume that CT implicitly contains the description of $(\mathbf{M}, \delta)$ and $\mathcal{I}_{\boldsymbol{v}}$.
$\mathbf{Decrypt}(\mathsf{GP}, \mathsf{GID}, \mathsf{CT}, \{\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\}_t)$: The decryption algorithm takes in the global parameters GP, a ciphertext CT generated with respect to some LSSS access policy $(\mathbf{M}, \delta)$ and an index set $\mathcal{I}$ associated to the message, and a collection of keys $\{\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\}_t$ corresponding to user ID-attribute pairs $(\mathsf{GID}, S \subseteq \mathsf{U}_{\mathsf{att}})$ and a key vector $(\boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}})$ possessed by a user with global identifier GID. It outputs a message ζ when the collection of attributes associated with the secret keys $\{\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\}_t$ satisfies the LSSS access policy $(\mathbf{M}, \delta)$, i.e., when the vector $(1, 0, \ldots, 0)$ belongs to the linear span of those rows of $\mathbf{M}$ which are mapped by δ to the set of attributes in S that corresponds to the secret keys $\{\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\}_{t \in S}$ possessed by the user with global identifier GID. Otherwise, decryption returns $\perp$.
Correctness: An LMA-ABUIPFE scheme for LSSS-realizable access structures and inner product message space $\mathcal{U}$ is said to be correct if for every $\lambda \in \mathbb{N}$, every message vector $\boldsymbol{v} \in \mathbb{Z}_q^{|\mathcal{I}_{\boldsymbol{v}}|}$, key vector $\boldsymbol{u} \in \mathbb{Z}_q^{|\mathcal{I}_{\boldsymbol{u}}|}$ such that $\mathcal{I} = \mathcal{I}_{\boldsymbol{v}} = \mathcal{I}_{\boldsymbol{u}}$, and $\mathsf{GID} \in \mathcal{GID}$, every LSSS access policy $(\mathbf{M}, \delta)$, and every subset of authorities $S \subseteq \mathsf{U}_{\mathsf{att}}$ controlling attributes which satisfy the access structure it holds that

$$\Pr\left[\Gamma = \boldsymbol{v} \cdot \boldsymbol{u} \;\middle|\; \begin{array}{c} \mathsf{GP} \leftarrow \mathsf{GlobalSetup}(1^\lambda, 1^n), \\ (\mathsf{PK}_\theta, \mathsf{MSK}_\theta) \leftarrow \mathsf{LocalSetup}(\mathsf{GP}, \theta), \\ \mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}} \leftarrow \mathsf{KeyGen}(\mathsf{GP}, \mathsf{GID}, \mathsf{MSK}_\theta, t, \boldsymbol{u}), \\ \mathsf{CT} \leftarrow \mathsf{Encrypt}(\mathsf{GP}, (\mathbf{M}, \delta), \{\mathsf{PK}_\theta\}_\theta, \boldsymbol{v}), \\ \Gamma = \mathsf{Decrypt}(\mathsf{GP}, \mathsf{CT}, \{\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\}_{t \in S}) \end{array}\right] = 1.$$

Static Security: In this paper, we consider static security for LMA-ABUIPFE formalized by the following game between a challenger and an adversary. The static security model is adapted from [36], defined for MA-ABE, to the context of LMA-ABUIPFE. We emphasize that unlike MA-ABE, our static security model allows the adversary to ask for secret keys which are capable of decrypting the challenge ciphertext.

Global Setup: The challenger runs $\mathsf{GlobalSetup}(1^\lambda, s_{\max})$ to get and send the global public parameters GP to the attacker.

Adversary's Queries: The adversary sends the following queries:

1. A list $\mathcal{C} \subset \mathcal{AU}$ of corrupt authorities and their respective public parameters $\{\mathsf{PK}_\theta\}_{\theta\in\mathcal{C}}$, which it might have created in a malicious way.
2. A set $\mathcal{N} \subset \mathcal{AU}$ of non-corrupt authorities, i.e., $\mathcal{C} \cap \mathcal{N} = \emptyset$, for which the adversary requests the public keys.
3. A set $\mathcal{Q} = \{(\mathsf{GID}, S, \boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}})\}$ of secret key queries with $\mathsf{GID} \in \mathcal{GID}, S \subseteq \mathsf{U}_{\mathsf{att}}$ such that $\mathsf{T}(S) \cap \mathcal{C} = \emptyset$, $\boldsymbol{u} \in \mathbb{Z}^{|\mathcal{I}_{\boldsymbol{u}}|}$ and $\mathcal{I}_{\boldsymbol{u}} \subset \mathbb{Z}$ where GIDs are distinct in each of these tuples.
4. Two message vectors $\boldsymbol{v}_0, \boldsymbol{v}_1 \in \mathbb{Z}_q^{|\mathcal{I}^*|}$ having the same index set $\mathcal{I}^*$, and a challenge LSSS access policy $(\mathbf{M}, \delta)$ with $\mathbf{M} = (M_{i,j})_{\ell\times s_{\max}} = (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_\ell)^\top \in \mathbb{Z}_q^{\ell\times s_{\max}}$, $\delta : [\ell] \to \mathsf{U}_{\mathsf{att}}$ and satisfying the constraint that for each $(\mathsf{GID}, S, \boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}}) \in \mathcal{Q}$, either $S \cup \bigcup_{\theta\in\mathcal{C}} \mathsf{T}^{-1}(\theta) \subseteq [\ell]$ constitutes an unauthorized subset of rows of the access matrix $\mathbf{M}$ or the secret key vector $\boldsymbol{u}$ satisfies the relation $(\boldsymbol{v}_0 - \boldsymbol{v}_1) \cdot \boldsymbol{u} = 0$ whenever $\mathcal{I}_{\boldsymbol{u}} = \mathcal{I}^*$. Note that the set $\bigcup_{\theta\in\mathcal{C}} \mathsf{T}^{-1}(\theta)$ contains the attributes belonging to the corrupt authorities.

Challenger's Replies: The challenger flips a random coin $\beta \leftarrow \{0, 1\}$ and replies with the following:

1. The public keys $\mathsf{PK}_\theta \leftarrow \mathsf{LocalSetup}(\mathsf{GP}, \theta)$ for all $\theta \in \mathcal{N}$.
2. The secret keys $\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}} \leftarrow \mathsf{KeyGen}(\mathsf{GP}, \mathsf{GID}, \mathsf{MSK}_\theta, t, \boldsymbol{u})$ for all $(\mathsf{GID}, S, \boldsymbol{u}) \in \mathcal{Q}, t \in S$.
3. The challenge ciphertext $\mathsf{CT} \leftarrow \mathsf{Encrypt}(\mathsf{GP}, (\mathbf{M}, \delta), \{\mathsf{PK}_\theta\}_{\theta\in\mathcal{C}\cup\mathcal{N}}, \boldsymbol{v}_\beta)$.

Guess: The adversary outputs a guess β' for β.

The advantage of the adversary $\mathcal{A}$ is $\mathsf{Adv}^{\mathsf{LMA\text{-}ABUIPFE}}_{\mathcal{A},\mathsf{SS\text{-}CPA}}(\lambda) \triangleq |\Pr[\beta = \beta'] - 1/2|$.

Definition 4.1 (Static Security for LMA-ABUIPFE for LSSS) *An* LMA-ABUIPFE *scheme for* LSSS*-realizable access structures satisfies static security if for any* PPT *adversary* $\mathcal{A}$ *there exists* $\mathsf{negl}(\cdot)$ *such that for all* $\lambda \in \mathbb{N}$*, we have* $\mathsf{Adv}^{\mathsf{LMA\text{-}ABUIPFE}}_{\mathcal{A},\mathsf{SS\text{-}CPA}}(\lambda) \leq \mathsf{negl}(\lambda)$.

Remark 4.1 (Static Security in the Random Oracle Model.) *Similar to [19,21,36], we additionally consider the aforementioned notion of selective security with static corruption in the ROM. In this context, we assume a global hash function* H *published as part of the global public parameters and accessible by all the parties in the system. In the security proof, we will model* H *as a random oracle programmed by the challenger. In the security game, therefore, we let the adversary* $\mathcal{A}$ *submit a collection of* H*-oracle queries to the challenger immediately after seeing the global public parameters, along with all the other queries it makes in the static security game as described above.*

Remark 4.2 (Small Universe MA-ABUIPFE.) *The above definition of* LMA-ABUIPFE *captures the large universe scenario where one authority can control multiple attributes. We can similarly define a small universe* MA-ABUIPFE *or simply* MA-ABUIPFE *by restricting each authority to control only a single attribute [36]. Hence, we would use the words* "authority" *and* "attribute" *interchangeably in the case of* MA-ABUIPFE. *There are a few syntactic and semantic changes in the above definition when adapted for the small universe setting:*

1. *There is a bijection between the attribute universe* $\mathsf{U}_{\mathsf{att}}$ *and the authority universe* $\mathcal{AU}$.
2. $\mathsf{LocalSetup}(\mathsf{GP}, t)$ *outputs* $(\mathsf{PK}_t, \mathsf{MSK}_t)$ *for an authority/attribute* $t \in \mathcal{AU}$.
3. $\mathsf{KeyGen}(\mathsf{GP}, \mathsf{GID}, \mathsf{MSK}_t, \boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}})$ *outputs* $\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}$.
4. *For an* LSSS *access structure* (M, δ), *we have* $\rho(\cdot) = \delta(\cdot)$ *is an injective map.*
5. *The changes in the security definition follow accordingly. Due to space constraints, we state them directly in the proof of our small universe scheme in Sect. 5.3.*

5 The Proposed Small Universe MA-ABUIPFE from DBDH

In this section, we describe the formal construction and proof for our MA-ABUIPFE scheme. The construction is in prime-order groups and uses a hash functions that will be modeled as a random oracle in the security proof.

5.1 The Construction

GlobalSetup$(1^\lambda, s_{\mathsf{max}})$: The global setup algorithm takes input the security parameter λ, the maximum width of an LSSS matrix supported by the scheme $s_{\mathsf{max}} = s_{\mathsf{max}}(\lambda)$ and the vector length n in unary. It generates $\mathsf{G} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g, e)$. Consider the hash functions $\mathsf{H}_1 : \mathsf{U}_{\mathsf{att}} \times \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{G}_2$, $\mathsf{H}_2 : [s_{\mathsf{max}}] \times \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{G}_2$, $\mathsf{H}_3 : \mathcal{GID} \times \mathbb{Z}^* \times [s_{\mathsf{max}}] \to \mathbb{G}_2$. It outputs a global parameter $\mathsf{GP} = (\mathsf{G}, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3)$.
LocalSetup(GP, t): The authority setup algorithm takes as input GP and an authority index/attribute $t \in \mathcal{AU}$. It samples vectors $\alpha_t, y_{t,2}, \ldots, y_{t,s_{\mathsf{max}}} \leftarrow \mathbb{Z}_q$ and outputs

$$\mathsf{PK} = \left(\{[\![\alpha_t]\!]_1, \{[\![y_{t,j}]\!]_1\}_{j\in\{2,\ldots,s_{\mathsf{max}}\}}\}_{t\in\mathsf{U}_{\mathsf{att}}}\right), \quad \mathsf{MSK} = \{\{\alpha_t, \{y_{t,j}\}_{j\in\{2,\ldots,s_{\mathsf{max}}\}}\}_{t\in\mathsf{U}_{\mathsf{att}}}\}$$

KeyGen$(\mathsf{GP}, \mathsf{GID}, \mathsf{MSK}_t, \boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}})$: The key generation algorithm takes input GP, the user's global identifier GID, the authority's secret key MSK_t and a vector $\boldsymbol{u} \in \mathbb{Z}_q^{|\mathcal{I}_{\boldsymbol{u}}|}$. It proceeds as follows

1. Parse $\mathcal{I}_{\boldsymbol{u}} = \{\iota_1, \ldots, \iota_n\}$ and $\boldsymbol{u} = (u_{\iota_1}, \ldots, u_{\iota_n})$.
2. Compute

$$\mathsf{SK}_{t,\boldsymbol{u}} = \prod_{k=1}^{n} \mathsf{H}_1(t \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}})^{\alpha_t u_{\iota_k}} \cdot \prod_{j=2}^{s_{\mathsf{max}}} \prod_{k=1}^{n} (\mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}}) \cdot \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k))^{y_{t,j} u_{\iota_k}}.$$

3. Output $\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}} = (\mathsf{GID}, \boldsymbol{u}, \mathsf{SK}_{t,\boldsymbol{u}}, \mathcal{I}_{\boldsymbol{u}})$ as the secret key.

Encrypt$(\mathsf{GP}, (\mathbf{M}, \rho), \{\mathsf{PK}_t\}, \boldsymbol{v}, \mathcal{I}_{\boldsymbol{v}})$: The encryption algorithm takes input the global parameter GP, an LSSS access structure $(\mathbf{M}, \rho)$ where $\mathbf{M} = (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_\ell)^\top \in \mathbb{Z}_q^{\ell \times s_{\mathsf{max}}}$ and $\rho : [\ell] \to \mathcal{AU}$, a set $\{\mathsf{PK}_t\}$ of public keys for all the authorities in the range of ρ, and a message vector $\boldsymbol{v} \in \mathbb{Z}_q^m$. The function maps the row indices of $\mathbf{M}$ to authorities or attributes. We assume ρ is an injective function, that is, an authority/attribute is associated with at most one row of $\mathbf{M}$. The algorithm proceeds as follows:

1. Parse $\mathcal{I}_{\boldsymbol{v}} = \{\iota_1, \ldots, \iota_m\}$ and $\boldsymbol{v} = (v_{\iota_1}, \ldots, v_{\iota_m})$.

2. Sample $\{r_i \leftarrow \mathbb{Z}_q\}_{i\in[\ell]}$ and $\boldsymbol{f} = (f_2, \ldots, f_{s_{\max}}) \leftarrow \mathbb{Z}_q^{s_{\max}-1}$.
3. Sample $\boldsymbol{z}, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{s_{\max}}, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{s_{\max}} \leftarrow \mathbb{Z}_q^m$.
4. Set the matrix $\mathbf{B} = \left[\boldsymbol{z}, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{s_{\max}}\right]^\top_{s_{\max}\times m}$.
5. Compute $\vartheta_{i,k} = e(r_i[\![\alpha_{\rho(i)}]\!]_1, \mathsf{H}_1(\rho(i) \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{v}}))$ and set $\boldsymbol{\vartheta}_i := (\vartheta_{i,1}, \ldots, \vartheta_{i,m})$.
6. Compute the following terms:

$$C_0 = [\![\boldsymbol{v} + \boldsymbol{z}]\!]_T, \quad C_{1,i} = [\![\boldsymbol{M}_i\mathbf{B} + \boldsymbol{\vartheta}_i]\!]_T, \quad C_{2,i} = [\![r_i]\!]_1,$$
$$C_{3,i,j,k} = e([\![M_{i,j}x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{v}})) \cdot e(r_i[\![y_{\rho(i),j}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{v}})),$$
$$C_{4,i,j} = [\![M_{i,j}f_j + y_{\rho(i),j}r_i]\!]_1$$

for all $i \in [\ell], j \in \{2, \ldots, s_{\max}\}, k \in [m]$.

7. Output the ciphertext

$$\mathsf{CT} = \left((\mathbf{M}, \rho), C_0, \{C_{1,i}, C_{2,i,}, C_{3,i,j,k}, C_{4,i,j}\}_{i\in[\ell], j\in\{2,\ldots,s_{\max}\}, k\in[m]}, \mathcal{I}_{\boldsymbol{v}}\right).$$

Decrypt(GP, GID, CT, $\{\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\}$): The decryption algorithm takes input the public key PK, a secret key $\mathsf{SK}_{S,\boldsymbol{u}}$ for an attribute set $S \subseteq \mathsf{U}_{\mathsf{att}}$ and a vector $\boldsymbol{u} \in \mathbb{Z}_q^n$ and a ciphertext CT for an access structure $(\mathbf{M}, \rho)$ with $\mathbf{M} \in \mathbb{Z}_q^{\ell\times s_{\max}}$ and an injective map $\rho : [\ell] \to \mathsf{U}_{\mathsf{att}}$.

Parse $\mathsf{SK}_{\mathsf{GID},S,\boldsymbol{u}} = \left(\mathsf{GID}, \boldsymbol{u}, \{\mathsf{SK}_{\rho(i),\boldsymbol{u}}\}_{\rho(i)\in S}, \mathcal{I}_{\boldsymbol{u}}\right)$, where $i \in [\ell]$ and $\mathsf{CT} = ((\mathbf{M}, \rho), C_0, \{C_{1,i}, C_{2,i,}, C_{3,i,j,k}, C_{4,i,j}\}_{i\in[\ell], j\in\{2,\ldots,s_{\max}\}, k\in[m]}, \mathcal{I}_{\boldsymbol{v}})$. Denote $I = \{i|\rho(i) \in S\} \subseteq [\ell]$. If $(1, 0, \ldots, 0)$ is not in the span of $\mathbf{M}_I$ (i.e., $\mathbf{M}$ restricted to the set of rows from I) or $\mathcal{I}_{\boldsymbol{u}} \neq \mathcal{I}_{\boldsymbol{v}}$ decryption returns $\perp$. Else, when S satisfies $(\mathbf{M}, \rho)$, the algorithm finds $\{w_i \in \mathbb{Z}_q\}_{i\in I}$ such that $(1, 0, \ldots, 0) = \sum_{i\in I} w_i\mathbf{M}_i$. It then computes $[\![\Gamma]\!]_T = C_0 \bullet \boldsymbol{u} \cdot [\![\mu]\!]_T$ where $[\![\mu]\!]_T$ is given by

$$\left(\prod_{i\in I}\left[\frac{C_{1,i} \bullet \boldsymbol{u} \cdot \prod_{j=2}^{s_{\max}}\prod_{k=1}^{n} u_{\iota_k} \cdot C_{3,i,j,k} \cdot e(C_{4,i,j}, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k)^{u_{\iota_k}})}{e\left(\mathsf{SK}_{\rho(i),\boldsymbol{u}}, C_{2,i}\right)}\right]^{w_i}\right)^{-1}$$

and outputs $\log_{g_T}([\![\Gamma]\!]_T)$.

5.2 Correctness

Consider a secret key $\mathsf{SK}_{\mathsf{GID},S,\boldsymbol{u}} = (\mathsf{GID}, \boldsymbol{u}, \{\mathsf{SK}_{t,\boldsymbol{u}}\}_{t\in S}, \mathcal{I}_{\boldsymbol{u}})$ consisting of a set of attributes satisfying the LSSS access structure $(\mathbf{M}, \rho)$ associated with a ciphertext $\mathsf{CT} = \left((\mathbf{M}, \rho), C_0, \{C_{1,i}, C_{2,i,}, C_{3,i,j,k}, C_{4,i,j}\}_{i\in[\ell], j\in\{2,\ldots,s_{\max}\}, k\in[m]}, \mathcal{I}_{\boldsymbol{v}}\right)$ such that $\mathcal{I}_{\boldsymbol{u}} = \mathcal{I}_{\boldsymbol{v}} = \mathcal{I}$. In particular, the vector $(1, 0, \ldots, 0) \in \mathsf{rowspan}(\mathbf{M}_I)$ corresponding to the set of indices $I = \{i \in I|\rho(i) = t \in S\}$.
For each $i \in I$, we have the following:

$$e(\mathsf{SK}_{\rho(i),\boldsymbol{u}}, C_{2,i}) = \prod_{k=1}^{n} e(g_1, \mathsf{H}_1(\rho(i) \parallel \iota_k \parallel \mathcal{I}))^{r_i\alpha_{\rho(i)}u_{\iota_k}} \cdot$$
$$\prod_{j=2}^{s_{\max}}\prod_{k=1}^{n}(e(g_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I})) \cdot e(g_1, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k)))^{r_i y_{\rho(i),j}u_{\iota_k}}$$

For $i \in I, j \in \{2, \ldots, s_{\mathsf{max}}\}, k \in [n]$,

$$u_{\iota_k} C_{3,i,j,k} = e([\![M_{i,j} x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}))^{u_{\iota_k}} \cdot e(g_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}))^{r_i y_{\rho(i),j} u_{\iota_k}}$$

For $i \in I, j \in \{2, \ldots, s_{\mathsf{max}}\}, k \in [n]$,

$$e(C_{4,i,j}, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k)^{u_{\iota_k}}) = e([\![M_{i,j} f_j]\!]_1, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k))^{u_{\iota_k}} \cdot e(g_1, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k))^{r_i y_{\rho(i),j} u_{\iota_k}}$$

Finally, for each $i \in I$, we have $C_{1,i} = [\![\boldsymbol{M}_i \mathbf{B} + \boldsymbol{\vartheta}_i]\!]_T$ and so

$$\frac{C_{1,i} \cdot \boldsymbol{u} \cdot \prod_{j=2}^{s_{\mathsf{max}}} \prod_{k=1}^{n} (u_{\iota_k} \cdot C_{3,i,j,k} \cdot e(C_{4,i,j}, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k)^{u_{\iota_k}}))}{e\left(\mathsf{SK}_{\rho(i),\boldsymbol{u}}, C_{2,i}\right)}$$

$$= [\![\boldsymbol{M}_i \mathbf{B} \cdot \boldsymbol{u}]\!]_T \prod_{k=1}^{n} e(g_1, \mathsf{H}_1(\rho(i) \parallel \iota_k \parallel \mathcal{I}))^{r_i \alpha_{\rho(i)} u_{\iota_k}} \cdot \frac{\prod_{j=2}^{s_{\mathsf{max}}} \prod_{k=1}^{n} (u_{\iota_k} \cdot C_{3,i,j,k} \cdot e(C_{4,i,j}, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k)^{u_{\iota_k}}))}{e\left(\mathsf{SK}_{\rho(i),\boldsymbol{u}}, C_{2,i}\right)}$$

$$= [\![\boldsymbol{M}_i \mathbf{B} \cdot \boldsymbol{u}]\!]_T \cdot \prod_{j=2}^{s_{\mathsf{max}}} \prod_{k=1}^{n} e([\![M_{i,j} x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}))^{u_{\iota_k}} \cdot \prod_{j=2}^{s_{\mathsf{max}}} \prod_{k=1}^{n} e([\![M_{i,j} f_j]\!]_1, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k))^{u_{\iota_k}}$$

Since $\mathsf{SK}_{S,\boldsymbol{u}}$ corresponds to a set of qualified authorities, $\exists \{w_i \in \mathbb{Z}_q\}_{i \in I}$ such that $\sum_{i \in I} w_i \boldsymbol{M}_i \mathbf{B} \cdot \boldsymbol{u} = (1, 0, \ldots, 0) \mathbf{B} \cdot \boldsymbol{u} = \boldsymbol{z} \cdot \boldsymbol{u}$ and it holds that $\sum_{i \in I} w_i M_{i,j} = 0, \forall j \in \{2, \ldots, s_{\mathsf{max}}\}$. Hence, we have

$$\prod_{i \in I} \left[\frac{C_{1,i} \cdot \boldsymbol{u} \cdot \prod_{j=2}^{s_{\mathsf{max}}} \prod_{k=1}^{n} (u_{\iota_k} \cdot C_{3,i,j,k} \cdot e(C_{4,i,j}, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k)^{u_{\iota_k}}))}{e\left(\mathsf{SK}_{\rho(i),\boldsymbol{u}}, C_{2,i}\right)} \right]^{w_i}$$

$$= [\![\sum_{i \in I} w_i \boldsymbol{M}_i \mathbf{B} \cdot \boldsymbol{u}]\!]_T = [\![\boldsymbol{z} \cdot \boldsymbol{u}]\!]_T$$

Finally, the message is recovered as $\log_{g_T}([\![\Gamma]\!]_T)$ where

$$[\![\Gamma]\!]_T = (C_0 \cdot \boldsymbol{u}) / [\![\boldsymbol{z} \cdot \boldsymbol{u}]\!]_T = [\![\boldsymbol{v} \cdot \boldsymbol{u} + \boldsymbol{z} \cdot \boldsymbol{u}]\!]_T / [\![\boldsymbol{z} \cdot \boldsymbol{u}]\!]_T = [\![\boldsymbol{v} \cdot \boldsymbol{u}]\!]_T$$

5.3 Security Analysis

Theorem 5.1. *If the* DBDH *assumption holds, then all* PPT *adversaries have a negligible advantage in breaking the static security of the proposed small universe* MA-ABUIPFE *scheme in the random oracle model.*

Proof. We prove this theorem by showing that if there is any PPT adversary $\mathcal{A}$ who breaks the static security of MA-ABUIPFE then there is a PPT adversary $\mathcal{B}$ who solves the DBDH problem with a non-negligible advantage. Suppose, $\mathcal{B}$ gets an instance $(\mathsf{G}, [\![a]\!]_1, [\![c]\!]_1, [\![a]\!]_2, [\![b]\!]_2, [\![\tau]\!]_T)$ of the DBDH problem where $\mathsf{G} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g, e) \leftarrow \mathcal{G}(1^\lambda)$ is a group description, the elements $a, b, c \leftarrow \mathbb{Z}_q$ are random integers, and the element $\tau \in \mathbb{Z}_q$ is either abc or a random element of $\mathbb{Z}_q$. The algorithm $\mathcal{B}$ works as follows: On input λ, $\mathcal{A}$ outputs $s_{\mathsf{max}}, \mathsf{U}_{\mathsf{att}}$ and queries the following.

Attacker's Queries: Upon initialization, the adversary $\mathcal{A}$ sends the following to $\mathcal{B}$:

(a) A list $\mathcal{C} \subset \mathcal{AU}$ of corrupt authorities and their respective public keys

$$\{\mathsf{PK}_t = (\mathrm{Y}_{t,1}, \mathrm{Y}_{t,2}, \ldots, \mathrm{Y}_{t,s_{\mathsf{max}}})\}_{t \in \mathcal{C}},$$

where $\mathrm{Y}_{t,1}, \mathrm{Y}_{t,2}, \ldots, \mathrm{Y}_{t,s_{\mathsf{max}}} \in \mathbb{G}_1$ for all $t \in \mathcal{C}$.

(b) A set $\mathcal{N} \subset \mathcal{AU}$ of non-corrupt authorities, i.e., $\mathcal{C} \cap \mathcal{N} = \emptyset$, for which $\mathcal{A}$ requests the public keys.

(c) A collection of hash queries $\mathcal{H}_1 = \{(t, \iota_k, \mathcal{I}) : t \in \mathsf{U}_{\mathsf{att}}, \iota_k \in \mathbb{Z}, \mathcal{I} \subset \mathbb{N}\}$, $\mathcal{H}_2 = \{(j, \iota_k, \mathcal{I}) : j \in \{2, \ldots, s_{\mathsf{max}}\}, \iota_k \in \mathbb{Z}, \mathcal{I} \subset \mathbb{N}\}$ and $\mathcal{H}_3 = \{(\mathsf{GID}, \boldsymbol{u}, j, \iota_k) : \mathsf{GID} \in \mathcal{GID}, \boldsymbol{u} \in \mathbb{Z}^*, j \in \{2, \ldots, s_{\mathsf{max}}\}, \iota_k \in \mathbb{Z}\}$.

(d) A set $\mathcal{Q} = \{(\mathsf{GID}, S, \boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}})\}$ of secret key queries with $\mathsf{GID} \in \mathcal{GID}, S \subseteq \mathsf{U}_{\mathsf{att}}$, $\boldsymbol{u} \in \mathbb{Z}^{|\mathcal{I}_{\boldsymbol{u}}|}$ and $\mathcal{I}_{\boldsymbol{u}} \subset \mathbb{Z}$.

(e) Two message vectors $\boldsymbol{v}_0, \boldsymbol{v}_1 \in \mathbb{Z}_q^n$ having the same index set $\mathcal{I}^*$, and a challenge LSSS access policy $(\mathbf{M}, \rho)$ with $\mathbf{M} = (M_{i,j})_{\ell \times s_{\mathsf{max}}} = (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_\ell)^\top \in \mathbb{Z}_q^{\ell \times s_{\mathsf{max}}}$ and $\rho : [\ell] \to \mathcal{C} \cup \mathcal{N}$ injective and satisfying the constraint that for each $(S, \boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}}) \in \mathcal{Q}_{\boldsymbol{u}}$, either $\rho^{-1}(\mathcal{C} \cup S) \subseteq [\ell]$ constitutes an unauthorized subset of rows of the access matrix $\mathbf{M}$ or the secret key vector $\boldsymbol{u}$ satisfies the relation $(\boldsymbol{v}_0 - \boldsymbol{v}_1) \cdot \boldsymbol{u} = 0$ whenever $\mathcal{I}_{\boldsymbol{u}} = \mathcal{I}^*$.

Before answering $\mathcal{A}$'s queries, the adversary $\mathcal{B}$ substitute the secret sharing matrix $\mathbf{M}$ with the matrix $\mathbf{M}'$ from Lemma 3.1 of [36] computed using $\rho^{-1}(\mathcal{C})$ as the unauthorized subset of rows. Lemma 3.1 of [36] guarantees the fact that if $\mathcal{B}$ uses $\mathbf{M}'$ instead of $\mathbf{M}$ in the simulation, the view of $\mathcal{A}$ in the simulated game is information theoretically the same as if $\mathcal{B}$ would have used the original matrix $\mathbf{M}$. Furthermore, Lemma 3.1 of [36] implies that if we assume the subspace spanned by $\mathbf{M}_{\rho^{-1}(\mathcal{C})}$ has dimension $\widetilde{c}$, then so is the dimension of the subspace spanned by $\mathbf{M}'_{\rho^{-1}(\mathcal{C})}$ and $M'_{i,j} = 0$ for all $(i, j) \in \rho^{-1}(\mathcal{C}) \times [s_{\mathsf{max}} - \widetilde{c}]$. $\mathcal{B}$ now proceeds to answer the queries of $\mathcal{A}$. Denote $\widehat{s_{\mathsf{max}}} = s_{\mathsf{max}} - \widetilde{c}$, where $\widetilde{c}$ is the dimension of the sequence spanned by the rows of $\mathbf{M}_{\rho^{-1}(\mathcal{C})}$, the latter being the rows of $\mathbf{M}$ controlled by corrupted authorities, $\mathcal{C}$.

Note that $\mathcal{I}^*$ can be any subset of $\mathbb{Z}$ and w.l.o.g one can consider $\mathcal{I}^* = [n]$[3] for some $n \in \mathbb{N}$. Inspired by the proof techniques of prior works [3,38], the reduction first compute a basis of $(\boldsymbol{v}_0 - \boldsymbol{v}_1)^\perp$ as $\{\widetilde{\boldsymbol{b}}_1, \ldots, \widetilde{\boldsymbol{b}}_{n-1}\}$. Then the set $\widetilde{\mathcal{S}} = \{\boldsymbol{v}_0 - \boldsymbol{v}_1, \widetilde{\boldsymbol{b}}_1, \ldots, \widetilde{\boldsymbol{b}}_{n-1}\}$ form a basis of $\mathbb{Z}_q^n$. For any vector $\boldsymbol{u} \in \mathbb{Z}_q^n$, if we represent it as the linear combination of the vectors in $\widetilde{\mathcal{S}}$ as

$$\boldsymbol{u} = \zeta \cdot (\boldsymbol{v}_0 - \boldsymbol{v}_1) + \sum_{k=1}^{n-1} \zeta_k \widetilde{\boldsymbol{b}}_k, \quad \text{for some } \zeta, \zeta_k \in \mathbb{Z}_q$$

then $\zeta = 0$ whenever it holds that $(\boldsymbol{v}_0 - \boldsymbol{v}_1) \cdot \boldsymbol{u} = 0$. Let $\boldsymbol{e}_k$ be the k-th vector in the standard basis of $\mathbb{Z}_q^n$. We write $\boldsymbol{e}_i$ for each $i \in [n]$ as

$$\boldsymbol{e}_i = \eta_i \cdot (\boldsymbol{v}_0 - \boldsymbol{v}_1) + \sum_{k=1}^{n-1} \lambda_{i,k} \widetilde{\boldsymbol{b}}_k \quad \text{for some } \eta, \lambda_{i,k} \in \mathbb{Z}_q.$$

Generating Public Key: There are two cases to consider:

1. **Case 1** — $t \in \mathcal{N} \setminus \rho([\ell])$ (i.e., attribute t is absent in the challenge policy $(\mathbf{M}, \rho)$ but it belongs to a non-corrupt authority) — In this case, $\mathcal{B}$ executes the Setup algorithm according to the real experiment. It samples $\alpha_t, y_{t,2}, \ldots, y_{t,s_{\mathsf{max}}} \leftarrow \mathbb{Z}_q$ by itself, and computes the public key component corresponding to attribute t as $([\![\alpha_t]\!]_1, [\![y_{t,2}]\!]_1, \ldots, [\![y_{t,s_{\mathsf{max}}}]\!]_1)$.
2. **Case 2**—$t \in \rho([\ell]) \setminus \mathcal{C}$ (i.e., attribute t appears in the challenge policy $(\mathbf{M}, \rho)$ and it does not belong to a corrupt authority) — In this case, $\mathcal{B}$ samples $\alpha'_t, y'_{t,2}, \ldots, y'_{t,s_{\mathsf{max}}} \leftarrow \mathbb{Z}_q$ and implicitly sets $\alpha_t = \alpha'_t + a \cdot M'_{\rho^{-1}(t),1}$ and $y_{t,j} = y'_{t,j} + aM'_{\rho^{-1}(t),j}$ for $j \in \{2, \ldots, \widehat{s_{\mathsf{max}}}\}$ and $y_{t,j} = y'_{t,j}$ for $j \in \{\widehat{s_{\mathsf{max}}} + 1, \ldots, s_{\mathsf{max}}\}$(these are well-defined as ρ is injective), and sets the public key elements w.r.t. attribute t as $([\![\alpha_t]\!]_1, [\![y_{t,2}]\!]_1, \ldots, [\![y_{t,s_{\mathsf{max}}}]\!]_1)$ where the elements $[\![\alpha_t]\!]_1$ and $[\![y_{t,j}]\!]_1$ for $j \in \{2, \ldots, \widehat{s_{\mathsf{max}}}\}$ are computed as follows:

$$[\![\alpha_t]\!]_1 = [\![\alpha'_t]\!]_1 \cdot M'_{\rho^{-1}(t),1} [\![a]\!]_1, \quad [\![y_{t,j}]\!]_1 = [\![y'_{t,j}]\!]_1 \cdot M'_{\rho^{-1}(t),j} [\![a]\!]_1 \tag{5.1}$$

for all $j \in [2, \widehat{s_{\mathsf{max}}}]$. Note that, α_t and $\{y_{t,j}\}_{j \in \{2,\ldots,s_{\mathsf{max}}\}}$ are distributed uniformly over $\mathbb{Z}_q$ and hence each of these elements of the public key is properly distributed.

Answering Hash Queries:

1. $\mathsf{H_1}$ **queries.** If $(\iota_k \in \mathcal{I}^* \wedge \mathcal{I} = \mathcal{I}^*)$, then sample uniformly random elements $h_{1,\widehat{k}}, h_{1,t,\iota_k}$ from $\mathbb{Z}_q$ and set

[3] In particular, we consider a map $\gamma : \mathcal{I}^* \to [n]$ and use $\gamma(k) = \iota_k$ throughout the security analysis.

$$\mathsf{H}_1(t \parallel \iota_k \parallel \mathcal{I}) = (g_2^b)^{\eta_k} \cdot \prod_{\widehat{k}=1}^{n-1} g_2^{h_{1,\widehat{k}}\lambda_{k,\widehat{k}}} \cdot g_2^{h_{1,t,\iota_k}}. \tag{5.2}$$

Otherwise, if $(\iota_k \notin \mathcal{I}^* \vee \mathcal{I} \neq \mathcal{I}^*)$, then output a random $\mathbb{G}_2$ element, i.e., sample uniformly random element h'_{1,t,ι_k} from $\mathbb{Z}_q$ and set $\mathsf{H}_1(t \parallel \iota_k \parallel \mathcal{I}) = g_2^{h'_{1,t,\iota_k}}$. The reduction stores the hash queries for future use.

2. $\mathsf{H_2}$ **queries.** If $(\iota_k \in \mathcal{I}^* \wedge \mathcal{I} = \mathcal{I}^*)$, then sample uniformly random elements $h_{2,\widehat{k}}, h_{2,j,\iota_k}$ for $j \in \{2, \ldots, \widehat{s_{\mathsf{max}}}\}$ (in Eq. 5.3) and elements h'_{2,j,ι_k} for $j \in \{\widehat{s_{\mathsf{max}}} + 1, \ldots, s_{\mathsf{max}}\}$ from $\mathbb{Z}_q$ (in Eq. 5.4) and set

$$\mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}) = (g_2^b)^{\eta_k \sum_{\phi=1}^{Q} d_{\phi,j}} \cdot \prod_{\widehat{k}=1}^{n-1} g_2^{h_{2,\widehat{k}}\lambda_{k,\widehat{k}}} \cdot g_2^{h_{2,j,\iota_k}} \tag{5.3}$$

$$\mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}) = g_2^{h'_{2,j,\iota_k}} \tag{5.4}$$

where Q denotes the total number of *non-accepting* key queries $\{(S_\phi, \boldsymbol{u}_\phi, \mathcal{I}_{\boldsymbol{u}_\phi})\}_{\phi \in [Q]}$ made by the adversary in the case where $\mathcal{I}_{\boldsymbol{u}_\phi} = \mathcal{I}^*$ but the attributes in S_ϕ does not satisfy the challenge policy $(\mathbf{M}, \rho)$. Note that, for such secret key queries, there exists a vector $\boldsymbol{d}_\phi = (d_{\phi,1}, \ldots, d_{\phi,s_{\mathsf{max}}}) \in \mathbb{Z}_q^{s_{\mathsf{max}}}$ such that $d_{\phi,1} = 1$ and the inner product $\boldsymbol{M}'_i \cdot \boldsymbol{d}_\phi = 0$ for all $i \in \rho^{-1}(\mathcal{C} \cup S_\phi)$, where $\boldsymbol{M}'_i$ denotes the i-th row of $\mathbf{M}'$. Additionally, the set of rows $\mathcal{R} = \{\boldsymbol{M}'_i \in \mathbb{Z}_q^{s_{\mathsf{max}}} : i \in \rho^{-1}(\mathcal{C})\}$ has dimension c and $M'_{i,j} = 0$ for all $(i,j) \in \rho^{-1}(\mathcal{C}) \times [\widehat{s_{\mathsf{max}}}]$. Therefore, $\mathcal{R}$ spans the entire subspace $\mathbb{V} = \left\{ (\overbrace{0, \ldots, 0}^{\widehat{s_{\mathsf{max}}}}, \boldsymbol{\nu}) : \boldsymbol{\nu} \in \mathbb{Z}_q^c \right\}$. Thus, it follows that $\boldsymbol{d}_\phi$ is orthogonal to any of the vectors

$$\left\{ (\overbrace{0, \ldots, 0}^{\widehat{s_{\mathsf{max}}}}, \overbrace{0, \ldots, 0}^{j-1}, 1, \overbrace{0, \ldots, 0}^{c-j}) \right\}_{j \in \{\widehat{s_{\mathsf{max}}}+1, \ldots, s_{\mathsf{max}}\}}.$$

In other words, $d_{\phi,j} = 0$ for all $j \in \{\widehat{s_{\mathsf{max}}} + 1, \ldots, s_{\mathsf{max}}\}$. Combining the above two facts, we have $(\boldsymbol{M}'_i|_{[\widehat{s_{\mathsf{max}}}]}) \cdot (\boldsymbol{d}_\phi|_{[\widehat{s_{\mathsf{max}}}]}) = 0$ for all $i \in \rho^{-1}(S_\phi)$, where for a vector $\boldsymbol{x}$, $\boldsymbol{x}|_X$ denotes a vector formed by taking the entries of $\boldsymbol{x}$ having indices in the set $X \in \mathbb{N}$. For simplicity of notation, let us denote $\boldsymbol{M}'_i \star \boldsymbol{d}_\phi = (\boldsymbol{M}'_i|_{[\widehat{s_{\mathsf{max}}}]}) \cdot (\boldsymbol{d}_\phi|_{[\widehat{s_{\mathsf{max}}}]})$ for $i \in \rho^{-1}(S_\phi)$.
Otherwise, if $(\iota_k \notin \mathcal{I}^* \vee \mathcal{I} \neq \mathcal{I}^*)$, then output a random $\mathbb{G}_2$ element, i.e., sample uniformly random element h''_{2,t,ι_k} from $\mathbb{Z}_q$ and set $\mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}) = g_2^{h''_{2,t,\iota_k}}$. The reduction stores the hash queries for future use.

3. $\mathsf{H_3}$ **queries.** If $(\mathsf{GID}, S_\phi, \boldsymbol{u}_\phi, \mathcal{I}_{\boldsymbol{u}_\phi}) \in \mathcal{Q}$ and $S_\phi \cap \rho([\ell]) \neq \emptyset$ and $\rho^{-1}(S_\phi \cup \mathcal{C})$ constitutes an unauthorized subset of the rows of $\mathbf{M}$ then sample h_{3,j,ι_k} for

$j \in \{2, \ldots, \widehat{s_{\max}}\}$ (in Eq. 5.5) and elements h'_{3,j,ι_k} for $j \in \{\widehat{s_{\max}}+1, \ldots, s_{\max}\}$ from $\mathbb{Z}_q$ (in Eq. 5.6) and set

$$\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_\phi \parallel j \parallel \iota_k) = (g_2^b)^{\eta_k \sum_{\phi' \in [Q] \setminus \{\phi\}} -d_{\phi',j}} \cdot g_2^{h_{3,j,\iota_k}} \tag{5.5}$$

$$\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_\phi \parallel j \parallel \iota_k) = g_2^{h'_{3,j,\iota_k}} \tag{5.6}$$

for all $\iota_k \in \mathcal{I}_{\boldsymbol{u}_\phi}$ such that $\mathcal{I}_{\boldsymbol{u}_\phi} = \mathcal{I}^*$ and $\boldsymbol{d}_\phi$ is as defined above.
If $(\mathsf{GID}, S_\phi, \boldsymbol{u}_\phi, \mathcal{I}_{\boldsymbol{u}_\phi}) \in \mathcal{Q}$ and $S_\phi \cap \rho([\ell]) \neq \emptyset$ and $\mathcal{I}_{\boldsymbol{u}_\phi} \neq \mathcal{I}^*$ then sample h''_{3,j,ι_k} uniformly at random from $\mathbb{Z}_q$ and set $\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_\phi \parallel j \parallel \iota_k) = g_2^{h''_{3,j,\iota_k}}$.
On the other hand, if $(\mathsf{GID}, S_\phi, \boldsymbol{u}_\phi, \mathcal{I}_{\boldsymbol{u}_\phi}) \in \mathcal{Q}$ and $S_\phi \cap \rho([\ell]) \neq \emptyset$ and $\rho^{-1}(S_\phi \cup \mathcal{C})$ constitutes an authorized subset of the rows of $\mathbf{M}$ then sample $h'''_{3,j,\iota_k} \leftarrow \mathbb{Z}_q$ and set $\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_\phi \parallel j \parallel \iota_k) = g_2^{h'''_{3,j,\iota_k}}$. The reduction stores the hash queries for future use. For all other cases, the reduction simple outputs a uniformly random element from $\mathbb{G}_2$ to answer the hash query $\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_\phi \parallel j \parallel \iota_k)$.

Generating Secret Keys: For any $(\mathsf{GID}, S_\phi, \boldsymbol{u}_\phi, \mathcal{I}_{\boldsymbol{u}_\phi}) \in \mathcal{Q}$, $\mathcal{B}$ returns a secret key $\mathsf{SK}_{\mathsf{GID},S_\phi,\boldsymbol{u}_\phi} = \left(\mathsf{GID}, \boldsymbol{u}_\phi, \{\mathsf{SK}_{t,\boldsymbol{u}_\phi}\}_{t \in S_\phi}, \mathcal{I}_{\boldsymbol{u}_\phi}\right)$, where it computes each of its components as follows. We denote

$$\mathsf{H}_{2\cdot3}(\mathsf{GID}, \boldsymbol{u}_\phi, j, k) = \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}_\phi}) \cdot \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_\phi \parallel j \parallel \iota_k)$$

for simplifying the representation of equations. For each $t \in S_\phi$ and $\mathcal{I}_{\boldsymbol{u}_\phi}$, it has four different cases to consider:

1. **Case 1**—($t \in S_\phi \setminus \rho([\ell])$) (i.e., the attribute is absent in the challenge policy (M, ρ))—In this case, $\mathcal{B}$ simulates the secret keys according to the real experiment. It knows $\alpha_t, y_{t,j}$ for all $j \in \{2, \ldots, s_{\max}\}$ in clear and hence can compute

$$\mathsf{SK}_{\phi,t,\boldsymbol{u}_\phi} = \left(\prod_{k=1}^{n} \mathsf{H}_1(t \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}_\phi})^{\alpha_t u_{\iota_k}}\right) \cdot \prod_{j=2}^{s_{\max}} \prod_{k=1}^{n} \mathsf{H}_{2\cdot3}(\mathsf{GID}, \boldsymbol{u}_\phi, j, k)^{y_{t,j} u_{\iota_k}}$$

   where $\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_\phi \parallel j \parallel \iota_k)$ were sampled uniformly.
2. **Case 2**—($t \in S_\phi \cap \rho([\ell]) \wedge \mathcal{I}_{\boldsymbol{u}_\phi} \neq \mathcal{I}^*$) (i.e., the attribute is present in the challenge policy, but the associated index set does not match with the challenge index set) In this case, $\mathcal{B}$ extracts the corresponding exponents of the hash values from the list of hash queries and computes

$$\mathsf{SK}_{\phi,t,\boldsymbol{u}_\phi} = \left(\prod_{k=1}^{n} \mathsf{H}_1(t \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}_\phi})^{\alpha_t u_{\iota_k}}\right) \cdot \prod_{j=2}^{s_{\max}} \prod_{k=1}^{n} \mathsf{H}_{2\cdot3}(\mathsf{GID}, \boldsymbol{u}_\phi, j, k)^{y_{t,j} u_{\iota_k}}$$

   where $\mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u}_\phi \parallel j \parallel \iota_k) = g_2^{h''_{3,j,\iota_k}}$ were sampled uniformly from $\mathbb{Z}_q$.
3. **Case 3**—($t \in S_\phi \cap \rho([\ell]) \wedge \mathcal{I}_{\boldsymbol{u}_\phi} = \mathcal{I}^*$) and $\rho^{-1}(\mathcal{C} \cup S_\phi)$ constitutes an unauthorized subset of the rows of $\mathbf{M}$ (i.e., S_ϕ does not satisfy the challenge policy $(\mathbf{M}, \rho)$). Note that the inner product value $(\boldsymbol{v}_0 - \boldsymbol{v}_1) \cdot \boldsymbol{u}_\phi$ can be either zero or non-zero

in this case. Since S_ϕ does not satisfy the challenge policy $(\mathbf{M}, \rho)$, there exists a vector $\boldsymbol{d}_\phi = (d_{\phi,1}, \ldots, d_{\phi,s_{\max}}) \in \mathbb{Z}_q^{s_{\max}}$ such that $d_{\phi,1} = 1$ and the inner product $\boldsymbol{M}'_i \star \boldsymbol{d}_\phi = 0$ for all $i \in \rho^{-1}(S_\phi)$, where $\boldsymbol{M}'_i$ denotes the i-th row of $\mathbf{M}'$. $\mathcal{B}$ computes the secret key $\mathsf{SK}_{t,\boldsymbol{u}}$ as follows.

$$\begin{aligned}
\mathsf{SK}_{\phi,t,\boldsymbol{u}_\phi} &= \Big(\prod_{k=1}^{n} \mathsf{H}_1(t \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}_\phi})^{\alpha_t u_{\iota_k}}\Big) \cdot \prod_{j=2}^{s_{\max}} \prod_{k=1}^{n} \mathsf{H}_{2\cdot 3}(\mathsf{GID}, \boldsymbol{u}_\phi, j, k)^{y_{t,j} u_{\iota_k}} \\
&= \Big(\prod_{k=1}^{n} (g_2^{ab})^{\eta_k M'_{\rho^{-1}(t),1} u_{\iota_k}}\Big) \cdot \prod_{j=2}^{\widehat{s_{\max}}} \prod_{k=1}^{n} (g_2^{ab})^{\eta_k d_{\phi,j} M'_{\rho^{-1}(t),j} u_{\iota_k}} \cdot g_2^{L_\phi(a,b)} \\
&= \prod_{j=1}^{\widehat{s_{\max}}} \prod_{k=1}^{n} (g_2^{ab})^{\eta_k d_{\phi,j} M'_{\rho^{-1}(t),j} u_{\iota_k}} \cdot g_2^{L_\phi(a,b)} \\
&= \prod_{k=1}^{n} (g_2^{ab})^{\eta_k u_{\iota_k} (\boldsymbol{M}'_{\rho^{-1}(t)} \star \boldsymbol{d}_\phi)} \cdot g_2^{L_\phi(a,b)} = g_2^{L_\phi(a,b)}
\end{aligned}$$

where $L_\phi(a,b)$ represents a linear function in a, b and hence $g_2^{L_\phi(a,b)}$ can be efficiently computable by $\mathcal{B}$. The first equality follows from the definition of $\alpha_t, y_{t,j}$ (Eq. (5.1)) and the hash functions H_1 (Eq. (5.2)), H_2 (Eqs. (5.3) and (5.4)) and H_3 (Eqs. (5.5) and (5.6)). The last equality holds since $\boldsymbol{M}'_{\rho^{-1}(t)} \star \boldsymbol{d}_\phi = 0$ and the second last equality holds since $d_{\phi,1} = 1$.

4. **Case 4**—$(t \in S_\phi \cap \rho([\ell]) \wedge \mathcal{I}_{\boldsymbol{u}_\phi} = \mathcal{I}^*)$ and $\rho^{-1}(S_\phi)$ constitutes an authorized subset of rows of $\mathbf{M}$ (i.e., S_ϕ satisfies the challenge policy $(\mathbf{M}, \rho)$) – In this case, $\mathcal{B}$ computes the secret key $\mathsf{SK}_{\phi,t,\boldsymbol{u}_\phi}$ as follows.

$$\begin{aligned}
\mathsf{SK}_{\phi,t,\boldsymbol{u}_\phi} &= \Big(\prod_{k=1}^{n} \mathsf{H}_1(t \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}_\phi})^{\alpha_t u_{\iota_k}}\Big) \cdot \prod_{j=2}^{s_{\max}} \prod_{k=1}^{n} \mathsf{H}_{2\cdot 3}(\mathsf{GID}, \boldsymbol{u}_\phi, j, k)^{y_{t,j} u_{\iota_k}} \\
&= \Big(\prod_{k=1}^{n} (g_2^{ab})^{\eta_k M'_{\rho^{-1}(t),1} u_{\iota_k}}\Big) \cdot \prod_{j=2}^{\widehat{s_{\max}}} \prod_{k=1}^{n} \big((g_2^{ab})^{\eta_k \sum_{\phi=1}^{Q} d_{\phi,j}}\big)^{M'_{\rho^{-1}(t),j} u_{\iota_k}} \cdot g_2^{L_\phi(a,b)} \\
&= \left[(g_2^{ab})^{\eta_k M'_{\rho^{-1}(t),1}} \cdot \prod_{j=2}^{\widehat{s_{\max}}} (g_2^{ab})^{\eta_k \sum_{\phi=1}^{Q} d_{\phi,j} M'_{\rho^{-1}(t),j}}\right]^{\boldsymbol{\eta} \cdot \boldsymbol{u}_\phi} \cdot g_2^{L_\phi(a,b)} = g_2^{L_\phi(a,b)}
\end{aligned}$$

where the last equality follows from the fact that $\boldsymbol{\eta} \cdot \boldsymbol{u}_\phi = 0$ if the secret key query satisfies the condition $(\boldsymbol{v}_0 - \boldsymbol{v}_1) \cdot \boldsymbol{u}_\phi = 0$ as S_ϕ is authorized. Hence, in this case, $\mathcal{B}$ can efficiently simulates the secret key as $L_\phi(a,b)$ is linear in a, b.

Generating the Challenge Ciphertext: $\mathcal{B}$ implicitly sets the vectors

$$\begin{aligned}
\boldsymbol{z} &= -abc \cdot \boldsymbol{\eta} = -abc(\eta_1, \ldots, \eta_n) \in \mathbb{Z}_q^n, \\
\boldsymbol{x}_j &= -(ac, \ldots, ac) \in \mathbb{Z}_q^n, f_j = -ac \in \mathbb{Z}_q, \quad \forall j \in \{2, \ldots, \widehat{s_{\max}}\}, \\
\boldsymbol{x}_j &= \mathbf{0} \in \mathbb{Z}_q^n, \quad f_j = 0 \in \mathbb{Z}_q, \quad \forall j \in \{\widehat{s_{\max}} + 1, \ldots, s_{\max}\}
\end{aligned}$$

There are two cases to consider according to the authority whether it is corrupted or non-corrupted.

1. **Case 1**—$\rho(i) \in \mathcal{C}$ (meaning that the authority associated with this row is corrupted)—In this case, it holds that $\boldsymbol{M}_i'\mathbf{B} = \mathbf{0}$ and $M'_{i,j}\boldsymbol{x}_j = 0$ for all $(i,j) \in \rho^{-1}(\mathcal{C}) \times [\widehat{s_{\mathsf{max}}}]$ since $\boldsymbol{M}_i'|_{[\widehat{s_{\mathsf{max}}}]} = \left\{\overbrace{0,\ldots,0}^{\widehat{s_{\mathsf{max}}}}\right\}$ and due to the above implicit setting of $\mathbf{B}, \boldsymbol{x}_j$. Thus, for each such row, $\mathcal{B}$ picks $r_i \leftarrow \mathbb{Z}_q$, and using the authority public key $\mathsf{PK}_{\rho(i)} = (\mathrm{Y}_{\rho(i),1}, \mathrm{Y}_{\rho(i),2}, \ldots, \mathrm{Y}_{\rho(i),s_{\mathsf{max}}})$ obtained from $\mathcal{A}$, it computes

$$\begin{aligned} C_0 &= [\![\boldsymbol{v}_\beta + z]\!]_T,\ \ C_{1,i} = [\![\boldsymbol{M}_i'\mathbf{B} + \boldsymbol{\vartheta}_i]\!]_T = [\![\boldsymbol{\vartheta}_i]\!]_T,\ \ C_{2,i} = [\![r_i]\!]_1, \\ C_{3,i,j,k} &= e([\![M'_{i,j}x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \cdot e(r_i[\![\mathrm{Y}_{\rho(i),j}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \\ &= e(r_i[\![\mathrm{Y}_{\rho(i),j}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \\ C_{4,i,j} &= [\![M'_{i,j}f_j + \mathrm{Y}_{\rho(i),j}r_i]\!]_1 = [\![\mathrm{Y}_{\rho(i),j}r_i]\!]_1 \end{aligned}$$

for all $i \in [\ell], j \in \{2,\ldots,s_{\mathsf{max}}\}$ and $k \in [n]$, where $\boldsymbol{\vartheta}_i = (\vartheta_{i,1},\ldots,\vartheta_{i,m})$ and

$$\vartheta_{i,k} = e(r_i[\![\mathrm{Y}_{\rho(i)}]\!]_1, \mathsf{H}_1(\rho(i) \parallel \iota_k \parallel \mathcal{I}^*)).$$

2. **Case 2**—$\rho(i) \in \mathcal{N}$ (meaning that the authority associated with this row is uncorrupted)—Firstly, $\mathcal{B}$ sets $C_0 = [\![\boldsymbol{v}_\beta + \boldsymbol{z}]\!]_T$ where β is the challenge bit for $\mathcal{A}$. It also implicitly sets $r_i = c$ and the matrix $\mathbf{B} = (\boldsymbol{z}, \mathbf{0}, \cdots, \mathbf{0})^\top \in \mathbb{Z}_q^{s_{\mathsf{max}} \times n}$. This implies $\boldsymbol{M}_i'\mathbf{B} = M'_{i,1}\boldsymbol{z} = -M'_{i,1} \cdot abc \cdot \boldsymbol{\eta}$ and the k-th element of the vector is $(\boldsymbol{M}_i'\mathbf{B})_k = -M'_{i,1}abc\eta_k$. Recall that, for each $i \in [\ell]$, we have $\alpha_{\rho(i)} = \alpha'_{\rho(i)} + a \cdot M'_{i,1}$ and $y_{\rho(i),j} = y'_{\rho(i),j} + aM'_{i,j}$. Now, $\mathcal{B}$ implicitly computes the vector $\boldsymbol{\vartheta}_i := (\vartheta_{i,1},\ldots,\vartheta_{i,m})$ as

$$\begin{aligned} \vartheta_{i,k} &= e(r_i[\![\alpha_{\rho(i)}]\!]_1, \mathsf{H}_1(\rho(i) \parallel \iota_k \parallel \mathcal{I}^*)) \\ &= e([\![c\alpha'_{\rho(i)} + ac \cdot M'_{i,1}]\!]_1, [\![b\eta_k + \sum_{\widehat{k}=1}^{n-1} h_{1,\widehat{k}}\lambda_{k,\widehat{k}} + h_{1,\rho(i),\iota_k}]\!]_2) \\ &= [\![bc\alpha'_{\rho(i)}\eta_k + M'_{i,1}abc\eta_k + (c\alpha'_{\rho(i)} + ac \cdot M'_{i,1})\mathfrak{h}_{1,i,k}]\!]_T \end{aligned}$$

where $\mathfrak{h}_{1,i,k} = \sum_{\widehat{k}=1}^{n-1} h_{1,\widehat{k}}\lambda_{k,\widehat{k}} + h_{1,\rho(i),\iota_k}$. We write $\boldsymbol{\mathfrak{h}}_{1,i} = (h_{1,\rho(i),\iota_k})_{k=1}^n$. Thus, for each $i \in [\ell]$, $\mathcal{B}$ sets $C_{2,i} = [\![c]\!]_1$ and computes

$$\begin{aligned} C_{1,i} &= [\![\boldsymbol{M}_i\mathbf{B} + \boldsymbol{\vartheta}_i]\!]_T = [\![bc\alpha'_{\rho(i)}\boldsymbol{\eta} + (c\alpha'_{\rho(i)} + ac \cdot M'_{i,1})\boldsymbol{\mathfrak{h}}_{1,i}]\!]_T \\ &= e(g_1^c, g_2^b)^{\alpha'_{\rho(i)}\boldsymbol{\eta}} \cdot e(g_1^c, g_2)^{\alpha'_{\rho(i)}\boldsymbol{\mathfrak{h}}_i} \cdot e(g_1^c, g_2^a)^{M'_{i,1}\boldsymbol{\mathfrak{h}}_{1,i}} \end{aligned}$$

Next, $\mathcal{B}$ computes $C_{3,i,j,k}$ as follows. Recall that $C_{3,i,j,k}$ is a product of two pairing operations. Note that, $M'_{i,j}x_{j,k} = 0$ if $j \in \{\widehat{s_{\mathsf{max}}} + 1,\ldots,s_{\mathsf{max}}\}$. Thus, for $j \in \{2,\ldots,\widehat{s_{\mathsf{max}}}\}$, the first pairing is computed as

$$\begin{aligned} &e([\![M'_{i,j}x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \\ &= e([\![M'_{i,j}x_{j,k}]\!]_1, (g_2^b)^{\eta_k \sum_{\phi=1}^{Q} d_{\phi,j}} \cdot \prod_{\widehat{k}=1}^{n-1} g_2^{h_{2,\widehat{k}}\lambda_{k,\widehat{k}}} \cdot g_2^{h_{2,\rho(i),\iota_k}}) \\ &= [\![M'_{i,j}x_{j,k}b\eta_k d_j^+ + M'_{i,j}x_{j,k}\mathfrak{h}_{2,i,k}]\!]_T \end{aligned}$$

where $d_j^+ = \sum_{\phi=1}^{Q} d_{\phi,j}$ and $\mathfrak{h}_{2,i,k} = \sum_{\widehat{k}=1}^{n-1} h_{2,\widehat{k}}\lambda_{k,\widehat{k}} + h_{2,\rho(i),\iota_k}$. If $j \in \{2,\ldots,\widehat{s_{\max}}\}$, the second pairing is computed as

$$\begin{aligned}
&e(r_i[\![y_{\rho(i),j}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \\
&= e([\![cy'_{\rho(i),j} + acM'_{i,j}]\!]_1, (g_2^b)^{\eta_k \sum_{\phi=1}^{Q} d_{\phi,j}} \cdot \prod_{\widehat{k}=1}^{n-1} g_2^{h_{2,\widehat{k}}\lambda_{k,\widehat{k}}} \cdot g_2^{h_{2,\rho(i),\iota_k}}) \\
&= [\![bc(y'_{\rho(i),j} + aM'_{i,j})\eta_k d_j^+ + c(y'_{\rho(i),j} + aM'_{i,j})\mathfrak{h}_{2,i,k}]\!]_T
\end{aligned}$$

Finally, for each $i \in [\ell], j \in \{2,\ldots,\widehat{s_{\max}}\}, k \in [n]$, the ciphertext component $C_{3,i,j,k}$ is obtained as

$$\begin{aligned}
C_{3,i,j,k} &= e([\![M'_{i,j}x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \cdot e(r_i[\![y_{\rho(i),j}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \\
&= [\![bcy'_{\rho(i),j}\eta_k d_j^+ + cy'_{\rho(i),j}\mathfrak{h}_{2,i,k}]\!]_T \\
&= e(g_1^c, g_2^b)^{y'_{\rho(i),j}\eta_k d_j^+} \cdot e(g_1^c, g_2)^{y'_{\rho(i),j}\mathfrak{h}_{2,i,k}}
\end{aligned}$$

which $\mathcal{B}$ can compute as a part of the challenge ciphertext. Now, if $j \in \{\widehat{s_{\max}}+1,\ldots,s_{\max}\}$, recall that $y_{\rho(i),j}$ are known is clear and hence $\mathcal{B}$ computes $C_{3,i,j,k}$ as

$$\begin{aligned}
C_{3,i,j,k} &= e([\![M'_{i,j}x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \cdot e(r_i[\![y_{\rho(i),j}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \\
&= e(r_i[\![y_{\rho(i),j}]\!]_1, [\![h'_{2,j,\iota_k}]\!]_2) = e(g_1^c, g_2)^{y_{\rho(i),j}h'_{2,j,\iota_k}}
\end{aligned}$$

for all $i \in [\ell], k \in [n]$. The last remaining part $C_{4,i,j}$ is given by

$$C_{4,i,j} = [\![M'_{i,j}f_j + y_{\rho(i),j}r_i]\!]_1 = [\![-acM'_{i,j} + cy'_{\rho(i),j} + acM'_{i,j}]\!]_1 = (g_1^c)^{y'_{\rho(i),j}}$$

if $i \in [\ell], j \in \{2,\ldots,\widehat{s_{\max}}\}$. Note that, $M'_{i,j}f_j = 0$ and $y_{\rho(i),j}$ are known in clear for $j \in \{\widehat{s_{\max}}+1,\ldots,s_{\max}\}$. Hence, $\mathcal{B}$ computes $C_{4,i,j}$ as

$$C_{4,i,j} = [\![M'_{i,j}f_j + y_{\rho(i),j}r_i]\!]_1 = [\![cy_{\rho(i),j}]\!]_1 = (g_1^c)^{y_{\rho(i),j}}$$

for each $i \in [\ell], j \in \{2,\ldots,s_{\max}\}$. Observe that, the elements $\mathbf{B}, \boldsymbol{x}_j, f_j$ and r_i are not properly distributed. Thus, $\mathcal{B}$ re-randomizes the ciphertext components using the algorithm CTRand described below before it sends to $\mathcal{A}$.

Ciphertext Re-randomization Algorithm: The algorithm described below provides properly distributed ciphertexts even if the randomness used within the ciphertexts inputted into the algorithm are not uniform. The algorithm uses only publicly available information to perform the re-randomization and hence rectify the distribution of the challenge ciphertext in the reduction.

$\mathsf{CTRand}((\mathbf{M},\boldsymbol{\rho}),\mathsf{CT},\mathsf{PK})$: The algorithm takes input an LSSS access policy $(\mathbf{M},\rho)$, where $\mathbf{M} = (M_{i,j})_{\ell \times s_{\max}} = (\boldsymbol{M}_1,\ldots,\boldsymbol{M}_\ell)^\top \in \mathbb{Z}_q^{\ell \times s_{\max}}$ and $\rho : [\ell] \to \mathsf{U}_{\mathsf{att}}$, a ciphertext $\mathsf{CT} = \big((\mathbf{M},\rho), C_0, \{C_{1,i}, C_{2,i}, C_{3,i,j,k}, C_{4,i,j}\}_{i\in[\ell], j\in\{2,\ldots,s_{\max}\}, k\in[m]}, \mathcal{I}_{\boldsymbol{v}}\big)$, and the public key components PK such that $\rho([\ell]) \subseteq \mathsf{U}_{\mathsf{att}}$.

1. Sample

(a) $r'_1, \ldots, r'_\ell \leftarrow \mathbb{Z}_q; \boldsymbol{x}'_2, \ldots, \boldsymbol{x}'_{s_{\mathsf{max}}} \in \mathbb{Z}_q^n; f'_2, \ldots, f'_{s_{\mathsf{max}}} \in \mathbb{Z}_q$,
(b) $\mathbf{B}' = (\boldsymbol{z}', \boldsymbol{b}'_2, \ldots, \boldsymbol{b}'_{s_{\mathsf{max}}})^\top \in \mathbb{Z}_q^{s_{\mathsf{max}} \times n}$,

2. Compute $C'_0 = C_0 \cdot [\![\boldsymbol{z}']\!]_T$.
3. For all $i \in [\ell]$, $j \in \{2, \ldots, s_{\mathsf{max}}\}$ and $k \in [n]$, compute

$$C'_{1,i} = C_{1,i} \cdot [\![\boldsymbol{M}_i \mathbf{B}' + \boldsymbol{\vartheta}'_i]\!]_T, \;\; C'_{2,i} = C_{2,i} \cdot [\![r'_i]\!]_1,$$
$$C'_{3,i,j,k} = C_{3,i,j,k} \cdot e([\![M_{i,j} x'_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*)) \cdot e(r'_i [\![y_{\rho(i),j}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}^*))$$
$$C'_{4,i,j} = C_{4,i,j} \cdot [\![M_{i,j} f'_j + y_{\rho(i),j} r'_i]\!]_1$$

where $\boldsymbol{\vartheta}'_i = (\vartheta'_{i,1}, \ldots, \vartheta'_{i,n})$ and $\vartheta'_{i,k} = e(r'_i [\![\alpha_{\rho(i)}]\!]_1, \mathsf{H}_1(\rho(i) \parallel \iota_k \parallel \mathcal{I}^*))$.

4. Output the ciphertext

$$\mathsf{CT} = \left((\mathbf{M}, \rho), C'_0, \{C'_{1,i}, C'_{2,i,}, C'_{3,i,j,k}, C'_{4,i,j}\}_{i \in [\ell], j \in \{2,\ldots,s_{\mathsf{max}}\}, k \in [m]}, \mathcal{I}_{\boldsymbol{v}} \right).$$

Guess: If $\mathcal{A}$ guesses the challenge bit $\beta \in \{0,1\}$ correctly, $\mathcal{B}$ returns 1; Otherwise $\mathcal{B}$ outputs 0. Now, observe that $\boldsymbol{z} = -\tau \cdot \boldsymbol{\eta}$ where $[\![\tau]\!]_T$ is the DBDH challenge element. If $\tau = abc$, then all the secret keys and the challenge ciphertext are distributed properly, in particular, the challenge ciphertext is an encryption of the message vector $\boldsymbol{v}_\beta$ for $\beta \leftarrow \{0,1\}$. Therefore, in this case, $\mathcal{A}$ outputs $\beta' = \beta$ with probability $1/2 + \epsilon(\lambda)$ where $\epsilon(\lambda)$ is the advantage of $\mathcal{A}$ in the static security game of the MA-ABUIPFE scheme. On the other hand, if τ is a random element of $\mathbb{Z}_q$ then the ciphertext element C_0 is uniformly random in $\mathbb{G}_T$, and hence from $\mathcal{A}$'s point of view there is no information of the challenge bit β in the challenge ciphertext. So, the probability of $\mathcal{A}$ outputting $\beta' = \beta$ is exactly $1/2$. Hence, by the guarantee of DBDH assumption, $\mathcal{A}$ has a non-negligible advantage against the proposed MA-ABUIPFE scheme in the static security game. This completes the proof. □

6 The Proposed Large Universe MA-ABUIPFE from L-DBDH

In this section, we describe the construction of our LMA-ABUIPFE scheme. The construction is in prime-order groups and additionally uses hash functions that are modelled as random oracles in the security proof just like our small universe construction.

GlobalSetup($1^\lambda, s_{\mathsf{max}}$): The global setup algorithm takes input the security parameter λ and a vector length n both in unary, and the maximum width of an LSSS matrix supported by the scheme $s_{\mathsf{max}} = s_{\mathsf{max}}(\lambda)$. It generates $\mathsf{G} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g, e)$ and specify hash functions $\mathsf{H}_1 : \mathsf{U}_{\mathsf{att}} \times \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{G}_2$, $\mathsf{H}_2 : [s_{\mathsf{max}}] \times \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{G}_2$, $\mathsf{H}_3 : \mathcal{GID} \times \mathbb{Z}^* \times [s_{\mathsf{max}}] \times \mathbb{Z} \rightarrow \mathbb{G}_2$ and $\mathsf{R} : \mathsf{U}_{\mathsf{att}} \times [s_{\mathsf{max}}] \times \mathbb{Z}^* \rightarrow \mathbb{G}_2$ mapping strings $(t, j) \in \mathsf{U}_{\mathsf{att}} \times [s_{\mathsf{max}}]$ to elements in $\mathbb{G}_2$. It outputs a global parameter $\mathsf{GP} = (\mathsf{G}, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{R})$.

LocalSetup(GP, θ): The authority setup algorithm takes input the global parameter GP and an authority index $\theta \in \mathcal{AU}$. It samples $\alpha_\theta, y_{\theta,2}, \ldots, y_{\theta,s_{\mathsf{max}}} \leftarrow \mathbb{Z}_q$ and outputs $\mathsf{PK}_\theta = ([\![\alpha_\theta]\!]_1, [\![y_{\theta,2}]\!]_1, \ldots, [\![y_{\theta,s_{\mathsf{max}}}]\!]_1)$ and $\mathsf{MSK}_\theta = (\alpha_\theta, y_{\theta,2}, \ldots, y_{\theta,s_{\mathsf{max}}})$.

KeyGen($\mathsf{GP}, \mathsf{GID}, \mathsf{MSK}_\theta, t, \boldsymbol{u}, \mathcal{I}_{\boldsymbol{u}}$): The key generation algorithm takes input GP, the user's global identifier GID, the authority's secret key MSK_θ, an attribute t controlled by the authority and a vector $\boldsymbol{u} \in \mathbb{Z}_q^{|\mathcal{I}_u|}$. It samples $\tau_j \leftarrow \mathbb{Z}_p$ for $j \in [s_{\mathsf{max}}]$ and proceeds as follows:

1. Parse $\mathcal{I}_{\boldsymbol{u}} = \{\iota_1, \ldots, \iota_n\}$ and $\boldsymbol{u} = (u_{\iota_1}, \ldots, u_{\iota_n})$.
2. Compute

$$\mathsf{K}_{t,\boldsymbol{u}} = (\prod_{k=1}^{n} \mathsf{H}_1(t \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}})^{\alpha_\theta u_{\iota_k}}) \cdot \prod_{j=2}^{s_{\max}} \prod_{k=1}^{n} (\mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{u}}) \cdot \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k))^{y_{\theta,j} u_{\iota_k}}.$$

3. Compute $\mathsf{SK}_{t,\boldsymbol{u}} = \mathsf{K}_{t,\boldsymbol{u}} \cdot \prod_{j=1}^{s_{\max}} \mathsf{R}(t \parallel j \parallel \mathcal{I}_{\boldsymbol{u}})^{\tau_j}$ and $\mathsf{Z}_t^{(j)} = [\![\tau_j]\!]_1 \; \forall \, j \in [s_{\max}]$.

Output $\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}} = (\mathsf{GID}, \boldsymbol{u}, \mathsf{SK}_{t,\boldsymbol{u}}, \mathsf{Z}_t^{(j)}, \mathcal{I}_{\boldsymbol{u}})$.

Encrypt$(\mathbf{GP}, (\mathbf{M}, \boldsymbol{\delta}), \{\mathbf{PK}_\theta\}, \boldsymbol{v}, \boldsymbol{\mathcal{I}_v})$: The encryption algorithm takes input the global parameter GP, an LSSS access structure $(\mathbf{M}, \delta)$ where $\mathbf{M} = (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_\ell)^\top \in \mathbb{Z}_q^{\ell \times s_{\max}}$ and $\delta : [\ell] \to \mathsf{U}_{\mathsf{att}}$, a set $\{\mathsf{PK}_\theta\}$ of public keys for all the relevant authorities, and a message vector $\boldsymbol{v} \in \mathbb{Z}_q^m$. The function δ maps the row indices of $\mathbf{M}$ to attributes. We define the function $\rho : [\ell] \to \mathcal{AU}$ as $\rho(\cdot) = \mathsf{T}(\delta(\cdot))$ which maps row indices of $\mathbf{M}$ to authorities. The algorithm proceeds as follows:

1. Parse $\mathcal{I}_{\boldsymbol{v}} = \{\iota_1, \ldots, \iota_m\}$ and $\boldsymbol{v} = (v_{\iota_1}, \ldots, v_{\iota_m})$.
2. Sample $\{r_i \leftarrow \mathbb{Z}_q\}_{i \in [\ell]}$ and $\boldsymbol{f} = (f_2, \ldots, f_{s_{\max}}) \leftarrow \mathbb{Z}_q^{s_{\max}-1}$.
3. Sample $\boldsymbol{z}, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{s_{\max}}, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{s_{\max}} \leftarrow \mathbb{Z}_q^m$.
4. Set the matrix $\mathbf{B} = \left[\boldsymbol{z}, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{s_{\max}}\right]^\top_{s_{\max} \times m}$.
5. Compute $\vartheta_{i,k} = e(r_i [\![\alpha_{\rho(i)}]\!]_1, \mathsf{H}_1(\rho(i) \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{v}}))$ and set $\boldsymbol{\vartheta}_i := (\vartheta_{i,1}, \ldots, \vartheta_{i,m})$.
6. Compute the following terms:

$$C_0 = [\![\boldsymbol{v} + \boldsymbol{z}]\!]_T, \quad C_{1,i} = [\![\boldsymbol{M}_i \mathbf{B} + \boldsymbol{\vartheta}_i]\!]_T, \quad C_{2,i} = [\![r_i]\!]_1,$$
$$C_{3,i,j,k} = e([\![M_{i,j} x_{j,k}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{v}})) \cdot e(r_i [\![y_{\rho(i),j}]\!]_1, \mathsf{H}_2(j \parallel \iota_k \parallel \mathcal{I}_{\boldsymbol{v}})),$$
$$C_{4,i,j} = [\![M_{i,j} f_j + y_{\rho(i),j} r_i]\!]_1,$$

   for all $i \in [\ell], j \in \{2, \ldots, s_{\max}\}, k \in [m]$.
7. Compute $C_{5,i,j} = \mathsf{R}(\delta(i) \parallel j \parallel \mathcal{I}_{\boldsymbol{v}})^{r_i}$ for all $i \in [\ell], j \in [s_{\max}]$.
8. Output the ciphertext

$$\mathsf{CT} = \left((\mathbf{M}, \delta), C_0, \{C_{1,i}, C_{2,i,}, C_{3,i,j,k}, C_{4,i,j}, C_{5,i,1}, C_{5,i,j}\}_{\substack{j \in \{2,\ldots,s_{\max}\}, \\ i \in [\ell], k \in [m]}}, \mathcal{I}_{\boldsymbol{v}} \right).$$

Decrypt$(\mathbf{GP}, \mathbf{GID}, \mathbf{CT}, \{\mathbf{SK}_{\mathsf{GID},t,\boldsymbol{u}}\})$: It takes input the public key PK, a secret key $\mathsf{SK}_{S,\boldsymbol{u}}$ for an attribute set $S \subseteq \mathsf{U}_{\mathsf{att}}$ and a vector $\boldsymbol{u} \in \mathbb{Z}_q^n$ and a ciphertext CT for an access structure $(\mathbf{M}, \delta)$ with $\mathbf{M} \in \mathbb{Z}_q^{\ell \times s_{\max}}$ and a map $\delta : [\ell] \to \mathsf{U}_{\mathsf{att}}$.

Parse $\mathsf{SK}_{\mathsf{GID},t,\boldsymbol{u}} = (\mathsf{GID}, \boldsymbol{u}, \mathsf{SK}_{t,\boldsymbol{u}}, \mathsf{Z}_t^{(j)}, \mathcal{I}_{\boldsymbol{u}})$, where $i \in [\ell]$ and $\mathsf{CT} = ((\mathbf{M}, \delta), C_0, \{C_{1,i}, C_{2,i,}, C_{3,i,j,k}, C_{4,i,j}, C_{5,i,1}, C_{5,i,j}\}_{i \in [\ell], j \in \{2,\ldots,s_{\max}\}, k \in [m]}, \mathcal{I}_{\boldsymbol{v}})$. Denote a set $I = \{i | \delta(i) \in S\} \subseteq [\ell]$. If $(1, 0, \ldots, 0)$ is not in the span of $\mathbf{M}_I$ (i.e., $\mathbf{M}$ restricted to the set of rows from I) or $\mathcal{I}_{\boldsymbol{u}} \neq \mathcal{I}_{\boldsymbol{v}}$ decryption returns $\perp$. Else, when S satisfies $(\mathbf{M}, \rho)$, the algorithm finds $\{w_i \in \mathbb{Z}_q\}_{i \in I}$ such that $(1, 0, \ldots, 0) = \sum_{i \in I} w_i \mathbf{M}_i$. It first computes

$$[\![\Lambda_i]\!]_T = \prod_{j=2}^{s_{\max}} \prod_{k=1}^{n} u_{\iota_k} \cdot C_{3,i,j,k} \cdot e(C_{4,i,j}, \mathsf{H}_3(\mathsf{GID} \parallel \boldsymbol{u} \parallel j \parallel \iota_k)^{u_{\iota_k}})$$

and outputs $\log_{g_T}([\![\Gamma]\!]_T)$ where $[\![\Gamma]\!]_T = C_0 \cdot \boldsymbol{u} \cdot [\![\mu]\!]_T$ and

$$[\![\mu]\!]_T = \left(\prod_{i \in I} \left[\frac{C_{1,i} \cdot \boldsymbol{u} \cdot [\![\Lambda_i]\!]_T \cdot \prod_{j=1}^{s_{\max}} e(\mathsf{Z}^{(j)}_{\delta(i)}, C_{5,i,j})}{e\left(\mathsf{SK}_{\rho(i),\boldsymbol{u}}, C_{2,i}\right)} \right]^{w_i} \right)^{-1}.$$

Theorem 6.1. *If the* L-DBDH *assumption holds, then all* PPT *adversaries have a negligible advantage in breaking the static security of the proposed* LMA-ABUIPFE *scheme in the random oracle model.*

References

1. Abdalla, M., Benhamouda, F., Gay, R.: From single-input to multi-client inner-product functional encryption. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11923, pp. 552–582. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34618-8_19
2. Abdalla, M., Benhamouda, F., Kohlweiss, M., Waldner, H.: Decentralizing inner-product functional encryption. In: Lin, D., Sako, K. (eds.) PKC 2019. LNCS, vol. 11443, pp. 128–157. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17259-6_5
3. Abdalla, M., Bourse, F., De Caro, A., Pointcheval, D.: Simple functional encryption schemes for inner products. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 733–751. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_33
4. Abdalla, M., Bourse, F., Caro, A.D., Pointcheval, D.: Better security for functional encryption for inner product evaluations. Cryptology ePrint Archive, Paper 2016/011 (2016). https://eprint.iacr.org/2016/011
5. Abdalla, M., Catalano, D., Gay, R., Ursu, B.: Inner-product functional encryption with fine-grained access control. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020. LNCS, vol. 12493, pp. 467–497. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64840-4_16
6. Agrawal, S., Bhattacherjee, S., Phan, D.H., Stehlé, D., Yamada, S.: Efficient public trace and revoke from standard assumptions: Extended abstract. CCS 2017, pp. 2277–2293, New York, NY, USA (2017). Association for Computing Machinery
7. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_28
8. Agrawal, S., Goyal, R., Tomida, J.: Multi-input quadratic functional encryption from pairings. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021. LNCS, vol. 12828, pp. 208–238. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-84259-8_8
9. Agrawal, S., Goyal, R., Tomida, J.: Multi-party functional encryption. In: Nissim, K., Waters, B. (eds.) TCC 2021. LNCS, vol. 13043, pp. 224–255. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90453-1_8
10. Agrawal, S., Libert, B., Stehlé, D.: Fully secure functional encryption for inner products, from standard assumptions. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9816, pp. 333–362. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53015-3_12
11. Benson, K., Shacham, H., Waters, B.: The *k*-BDH assumption family: bilinear map cryptography from progressively weaker assumptions. In: Dawson, E. (ed.) CT-RSA 2013. LNCS, vol. 7779, pp. 310–325. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36095-4_20

12. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_26
13. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
14. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1_30
15. Boneh, D., Sahai, A., Waters, B.: Functional encryption: definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_16
16. Chen, J., Gong, J., Kowalczyk, L., Wee, H.: Unbounded ABE via bilinear entropy expansion, revisited. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10820, pp. 503–534. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78381-9_19
17. Chotard, J., Dufour Sans, E., Gay, R., Phan, D.H., Pointcheval, D.: Decentralized multi-client functional encryption for inner product. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018. LNCS, vol. 11273, pp. 703–732. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03329-3_24
18. Datta, P., Dutta, R., Mukhopadhyay, S.: Functional encryption for inner product with full function privacy. In: Cheng, C.-M., Chung, K.-M., Persiano, G., Yang, B.-Y. (eds.) PKC 2016. LNCS, vol. 9614, pp. 164–195. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49384-7_7
19. Datta, P., Komargodski, I., Waters, B.: Decentralized multi-authority ABE for DNFs from LWE. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12696, pp. 177–209. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77870-5_7
20. Datta, P., Komargodski, I., Waters, B.: Fully adaptive decentralized multi-authority ABE. Cryptology ePrint Archive, Paper 2022/1311 (2022)
21. Datta, P., Komargodski, I., Waters, B.: Decentralized multi-authority ABE from NC^1 from computational-BDH. Cryptology ePrint Archive, Paper 2021/1325, ePrint (2021)
22. Freeman, D.M.: Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 44–61. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_3
23. Gay, R.: A new paradigm for public-key functional encryption for degree-2 polynomials. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020. LNCS, vol. 12110, pp. 95–120. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45374-9_4
24. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98 (2006)
25. Guillevic, A.: Comparing the pairing efficiency over composite-order and prime-order elliptic curves. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds.) ACNS 2013. LNCS, vol. 7954, pp. 357–372. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38980-1_22
26. Jain, A., Lin, H., Matt, C., Sahai, A.: How to leverage hardness of constant-degree expanding polynomials over $\mathbb{R}$ to build $i\mathcal{O}$. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11476, pp. 251–281. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_9
27. Jain, A., Lin, H., Sahai, A.: Simplifying constructions and assumptions for $i\mathcal{O}$. Cryptology ePrint Archive, Paper 2019/1252 (2019)

28. Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from well-founded assumptions. In: Khuller, S., Williams, V.V. (eds.) STOC 2021: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, 21–25 June 2021, pp. 60–73. ACM (2021)
29. Lee, J., Kim, D., Kim, D., Song, Y., Shin, J., Cheon, J.H.: Instant privacy-preserving biometric authentication for hamming distance. Cryptology ePrint Archive, Paper 2018/1214 (2018). https://eprint.iacr.org/2018/1214
30. 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
31. 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
32. Nguyen, K., Phan, D.H., Pointcheval, D.: Multi-client functional encryption with fine-grained access control. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology–ASIACRYPT 2022. ASIACRYPT 2022. LNCS, vol 13791, pp. 95–125. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-22963-3_4
33. Okamoto, T., Takashima, K.: Decentralized attribute-based encryption and signatures. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **103**-A(1), 41–73 (2020)
34. O'Neill, A.: Definitional issues in functional encryption. Cryptology ePrint Archive, Paper 2010/556, ePrint (2010)
35. Pal, T., Dutta, R.: Attribute-based access control for inner product functional encryption from LWE. In: Longa, P., Ràfols, C. (eds.) LATINCRYPT 2021. LNCS, vol. 12912, pp. 127–148. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-88238-9_7
36. 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
37. 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
38. Dufour-Sans, E., Pointcheval, D.: Unbounded inner-product functional encryption with succinct keys. In: Deng, R.H., Gauthier-Umaña, V., Ochoa, M., Yung, M. (eds.) ACNS 2019. LNCS, vol. 11464, pp. 426–441. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21568-2_21
39. Shoup, V.: Lower bounds for discrete logarithms and related problems. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 256–266. Springer, Heidelberg (1997). https://doi.org/10.1007/3-540-69053-0_18
40. Tomida, J.: Tightly secure inner product functional encryption: multi-input and function-hiding constructions. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11923, pp. 459–488. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34618-8_16
41. 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
42. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_4
43. Waters, B., Wee, H., Wu, D.J.: Multi-authority ABE from lattices without random oracles. In: Kiltz, E., Vaikuntanathan, V. (eds.) Theory of Cryptography. TCC 2022. LNCS, vol. 13747, pp. 651–679. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-22318-1_23

44. Wee, H.: Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology–EUROCRYPT 2022. EUROCRYPT 2022. LNCS, vol. 13276, pp. 217–241. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-07085-3_8
45. Zhou, K., Ren, J.: PassBio: privacy-preserving user-centric biometric authentication. IEEE Trans. Inf. Forensics Secur. **13**(12), 3050–3063 (2018)