






# Lattice-based Multi-Authority/Client Attribute-based Encryption for Circuits

Valerio Cini<sup>1</sup> , Russell W. F. Lai<sup>2</sup>  and Ivy K. Y. Woo<sup>2</sup> 

<sup>1</sup> NTT Research, USA

<sup>2</sup> Aalto University, Finland

**Abstract.** Multi-authority/input attribute-based encryption (MA-/MI-ABE) are multi-party extensions of ABE which enable flavours of decentralised cryptographic access control. This work aims to advance research on multi-party ABE and their lattice-based constructions in several directions:

- We introduce the notion of multi-client (MC-)ABE. This can be seen as an augmentation of MI-ABE with the addition of a ciphertext identity (CID) in the syntax, or a specialisation of multi-client functional encryption (MC-FE) to the ABE setting.
- We adapt the 2-input (2I-)ABE of Agrawal et al. (CRYPTO'22), which is heuristically secure yet without a security proof, into a 2-client (2C-)ABE, and prove it satisfies a variant of very-selective security under the learning with errors (LWE) assumption.
- We extend Wee's ciphertext-policy (CP-)ABE (EUROCRYPT'22) to the MA setting, yielding an MA-ABE. Furthermore, combining techniques in Boneh et al.'s key-policy ABE (EUROCRYPT'14) and our MA-ABE, we construct an MC-ABE. We prove that they satisfy variants of very-selective security under the evasive LWE, tensor LWE, and LWE assumptions.

All our constructions support policies expressed as arbitrary polynomial-size circuits, feature distributed key generation (for MA) and encryption (for 2C/MC), and are proven secure in the random oracle model. Although our constructions only achieve limited security against corrupt authorities/clients, the fully distributed key generation/encryption feature makes them nevertheless non-trivial and meaningful. Prior to this work, existing MA-ABEs only support up to NC1 policies regardless of their security against corrupt authorities; existing MI-ABEs only support up to constant-many encryptors/clients and do not achieve any security against corrupt encryptors/clients; and MC-ABEs only existed in the form of MC-FEs for linear and quadratic functions.

## 1 Introduction

Multi-authority attribute-based encryption (MA-ABE) [Cha07] and multi-input ABE (MI-ABE) [BJK<sup>+</sup>18] are multi-party extensions of (single-authority single-input) ABE which enable different flavours of decentralised cryptographic access control. An MA-ABE allows to encrypt a message with respect to an access structure and a set of authorities, so that any user who obtained suitable secret keys from a subset of authorities satisfying the access structure can uncover the message. Similarly, an MI-ABE allows multiple encryptors

---

E-mail: [cini.valerio@gmail.com](mailto:cini.valerio@gmail.com) (Valerio Cini), [russell.lai@aalto.fi](mailto:russell.lai@aalto.fi) (Russell W. F. Lai), [ivy.woo@aalto.fi](mailto:ivy.woo@aalto.fi) (Ivy K. Y. Woo)



to distributedly encrypt with respect to some attributes, so that a user who is granted a secret key associated to a policy accepting those attributes can decrypt.

Leveraging lattice-based homomorphic computation techniques [GSW13] developed originally for fully homomorphic encryption, the community has been relatively successful in constructing (single-authority single-input) ABE supporting complex access structures. Notably, Boneh et al. [BGG<sup>+</sup>14] constructed key-policy (KP-)ABE for circuits from the learning with errors (LWE) assumption, and more recently Wee [Wee22] constructed ciphertext-policy (CP-)ABE for circuits from the evasive LWE and tensor LWE assumptions, both constructions having ciphertext size sublinear in the circuit size.

Less progress has been made in lattice-based multi-party ABE constructions. MA-ABE for DNF formulas have been achieved under LWE [DKW21] based on linear-secret-sharing-scheme (LSSS) techniques borrowed from group-based constructions, and implicitly for NC1 circuits [DKW21] assuming honest authorities. On the MI front, two schemes for the class of conjunction functions from LWE are implicit in the work of [FFMV23] but unfortunately only with single-key security; [ARYY23] constructed constant-many-input ABE from variants of the evasive LWE and tensor LWE assumptions, although both with a stronger flavour than that for Wee’s CP-ABE.

This work seeks to explore the possibility of multi-party ABE under newly introduced lattice-based assumptions, including the evasive LWE and tensor LWE assumptions which have been shown to imply single-authority CP-ABE [Wee22]. Below, we first recall various notions of multi-party ABE, then overview our contributions and highlight differences over existing results.

## 1.1 Background

**MA-ABE.** A multi-authority (MA-)ABE seeks to decentralise the power of the authority in a (single-authority) ABE. In the prominent global-identifier (GID) model, the setting can be summarised as follows: Each user is associated to an identity  $\text{uid}$ . Any authority  $i$  can generate its own master public and secret key pair  $(\text{mpk}_i, \text{msk}_i)$ , and issue key  $\text{sk}_{\text{uid},i,x_i}$  to user  $\text{uid}$  associated with attribute  $x_i$ . An encryptor can encrypt a message  $\mu$  with respect to multiple authorities (identified by)  $(\text{mpk}_i)_{i \in [k]}$  together with a policy  $f$ . A user  $\text{uid}$  can decrypt to  $\mu$  if and only if it obtains keys  $\text{sk}_{\text{uid},i,x_i}$  for all of the authorities  $(\text{mpk}_i)_{i \in [k]}$  specified by the encryptor, and the specified policy  $f$  accepts the attributes  $(x_i)_i$  of  $\text{uid}$ , i.e.  $f(x_1, \dots, x_k) = 0$ . To prevent mix-and-match attack, security commonly requires that an adversary cannot request keys for the same  $\text{uid}$  and from the same authority  $i$ , but associated to different attributes  $x_i$ .

**Multi-Input Functional/Attribute-based Encryption.** Multi-input (MI-)ABE was proposed by [BJK<sup>+</sup>18] as a stepping stone towards witness encryption (WE) and is a special case of multi-input functional encryption (MI-FE) [GGG<sup>+</sup>14]. Analogous to the relation between (single-input) KP-ABE and FE, an MI-ABE for function class  $\mathcal{F}$  and message space  $\mathcal{M}$  can be viewed as an MI-FE for the function class  $\mathcal{G} = \{g_{f,\mu} : f \in \mathcal{F}, \mu \in \mathcal{M}\}$  of policy-checking predicates, where  $g_{f,\mu}(y_1, \dots, y_\ell)$  evaluates to message  $\mu$  if the MI-ABE policy  $f$  is satisfied, else it evaluates to  $\perp$ . More precisely, an MI-ABE can be summarised as follows: A trusted setup generates a master secret key for all  $\ell$  encryptors and the authority. The first encryptor can encrypt a message  $\mu$  with respect to some attribute  $y_1$  as  $\text{ctxt}_{1,y_1}$ , while for  $2 \leq j \leq \ell$  the  $j$ -th encryptor provides a ciphertext  $\text{ctxt}_{j,y_j}$  associated to some attribute  $y_j$  (without specifying any message). Any user, who obtains a secret key  $\text{sk}_f$  associated to a function  $f$  from the authority, can decrypt  $(\text{ctxt}_{1,y_1}, \dots, \text{ctxt}_{\ell,y_\ell})$  to recover  $\mu$  if and only if  $f(y_1, \dots, y_\ell) = 0$ .

A property of both MI-FE and MI-ABE is that mix-and-match is allowed in their security models. In case of MI-ABE, it is said to be secure if the message  $\mu$  remains hidden from an adversary who obtains secret keys for many functions  $f_1, f_2, \dots \in \mathcal{F}$  and

ciphertext components for many attributes  $y_{i,1}, y_{i,2}, \dots \in \mathcal{Y}_i$ , as long as  $f(y_1, \dots, y_\ell) \neq 0$  for all combinations of  $(f, y_1, \dots, y_\ell) \in \mathcal{F} \times \mathcal{Y}_1 \times \dots \times \mathcal{Y}_\ell$ . This makes MI-FE/ABE very powerful primitives, in that MI-FE implies iO [GGG<sup>+</sup>14] and MI-ABE implies witness encryption [BJK<sup>+</sup>18], meaning that they also tend to be hard to construct. Existing MI-FE (for functions beyond predicates) are all either group-based or obfuscation-based. For MI-ABE, [Ayy22] proposed a lattice-based 2-input ABE but no security proof was provided; [FFMV23] constructed two MI-ABE schemes<sup>1</sup> for conjunctions from LWE but which has only single-(authority-)key security; Agrawal et al. [ARYY23] constructed constant-input ABE based on the evasive LWE assumption with private-coin auxiliaries<sup>2</sup> and an extended version of the tensor LWE assumption.

The possibility of mix-and-match has also limited the use cases of MI-FE/ABE. Suppose Alice wishes to disclose a secret message  $\mu$  to Carol under the condition that her input  $y_1$  agrees with Bob’s  $y_2$ , with Mary being the mediator. This scenario captures, for example, a variety of voting. To achieve this, Mary acts as the authority in an MI-ABE and generates  $\text{sk}_f$  for a function  $f$  which checks that  $y_1$  agrees with  $y_2$ ; Alice acts as the first encryptor and generates  $\text{ctxt}_{1,y_1}$  encrypting  $\mu$ ; Bob the second and generates  $\text{ctxt}_{2,y_2}$ . Carol, who collects  $(\text{sk}_f, \text{ctxt}_{1,y_1,m}, \text{ctxt}_{2,y_2})$ , decrypts and learns  $\mu$  if  $f(y_1, y_2) = 0$ . Should Alice and her peers want to release another secret message on different conditions, they would need to set up a new instance of MI-ABE, since  $(\text{ctxt}_{1,y_1}, \text{ctxt}_{2,y_2})$  can be reused, undesirably.

**Multi-Client Functional/Attribute-based Encryption.** For the sake of both feasibility and practicality, MI-FE has been extended to multi-client (MC-)FE [GGG<sup>+</sup>14], which is same as an MI-FE except that each ciphertext from an encryptor is additionally linked to a cid, also called a “tag” or a “label”. Correctness is guaranteed only when a decryptor collects ciphertexts linked to the same cid, and security commonly requires that the adversary does not query on a cid for all  $\ell$  inputs. Same as the GID in an MA-ABE, the CID in an MC-FE serves to prevent mix-and-match attacks. Although the security guarantee becomes weaker, this model is regarded more natural in access control applications, and a handful of constructive results [CDG<sup>+</sup>18, ABKW19, ABG19, LT19, AGT22, NPP22] have been obtained. In the lattice setting, by now we have MC-FE for linear functions with adaptive security from standard LWE [LT19].

Following this line of development, it is natural to ask if there exists an MC-analogue of MI-ABE, which specialises MC-FE to the class of policy-checking predicates and unlocks both feasibility and applications by the introduction of CID. We call this the multi-client (MC-)ABE. Going back to the above example with Alice and her peers, in an MC-ABE the set of ciphertexts  $(\text{ctxt}_{1,y_1}, \text{ctxt}_{2,y_2})$  would be associated to a common ciphertext identifier cid, and cannot be mixed with future ciphertexts associated to  $\text{cid}' \neq \text{cid}$ . The system can thus be reused repeatedly by using different cid in each round, which is more desirable in many real-world applications.

We see MC-ABE (or “MI-ABE in the CID model”) as a dual of MA-ABE in the GID model: Both incorporate an ID to prevent mix-and-match, with the former allowing multiple inputs and the latter multiple authorities. Removing the ID (so that mix-and-match is allowed) results in formulations of MI-ABE and MA-ABE where both of which imply witness encryption. Section D discusses the transformation to WE and why having IDs prevents such in more detail.

## 1.2 Our Contributions

This works extends the boundary of multi-party ABE in the following directions:

<sup>1</sup>Actually they constructed multi-input predicate encryption, which implies MI-ABE, although with the heavy machinery of lockable obfuscation.

<sup>2</sup>See Section 1.4 for a short discussion on variants of evasive LWE.

**Multi-Client ABE.** We formally introduce the notion of multi-client ABE, a natural variant of MI-ABE where syntax and security forbid mix-and-match attacks, which can also be seen as a specialisation of MC-FE to the the class of policy-checking predicates.

**2C-ABE for Circuits from LWE.** We adapt the heuristic 2-input ABE for general circuits of Agrawal et al. [Ayy22] to a (public-key) 2-client ABE, which we prove to satisfy a variant of very-selective security under the (standard) LWE assumption in the random oracle model (ROM).

**MA-ABE and MC-ABE for Circuits.** Adapting techniques from [Wee22] and [BGG<sup>+</sup>14], we construct an MA-ABE and an MC-ABE for general circuits, respectively. We prove variants of very-selective security of both constructions, under the evasive LWE, tensor LWE, and LWE assumptions in the ROM.

All three constructions feature distributed key generation, i.e. authorities in MA-ABE, respectively encryptors in MC-ABE, generate their secret keys independently, thus achieving decentralisation common in MA-ABE works.

All our constructions retain security when no authority/encryptor involved in the challenge ciphertext is corrupt. Alternatively, our MA-ABE is secure if, for each user, at least one authority involved in the challenge ciphertext is honest, and who did not issue any key to this user. Similarly, our MC-ABE are secure if at least one sub-encryptor specified in the challenge ciphertext is honest, and who did not contribute any ciphertext component for the specified slot.<sup>3</sup> Despite these restrictions, we believe that the achieved security notions are still non-trivial and meaningful in presence of distributed key generation, since the latter makes the schemes irreplaceable by their single-authority/encryptor counterparts, and the security of ciphertexts involving different sets of authorities/encryptors are independent.

### 1.3 Related Work

Multi-party ABE is naturally connected to (single-party) ABE and (multi-party) FE, both of which have vast literature. We do not attempt to compare the results in this work exhaustively with every existing multi-party ABE/FE, but instead focused on most related ones. In particular, we omit comparisons with existing MC-FE schemes which support only linear or quadratic functions, and hence cannot be cast as MC-ABE schemes, and any schemes based on indistinguishability obfuscation. We also omit further comparisons with MI-ABE and MI-FE as they are already discussed above, and their security requirement against mix-and-match attacks makes them compete in a higher league<sup>4</sup> than MA-/MC-schemes, despite the syntactical similarity.

Since MC-ABE is a new notion that was not explicitly considered before, we focus our discussion below on MA-ABE, and draw connections to our MC-ABE when appropriate. We first discuss the syntax and the expressiveness of the supported access policies, and then move to the security notions.

**Syntax.** MA-ABE has traditionally [LW11] been considered natively for monotone access policies, and the support for non-monotone policies is often obtained by first converting non-monotone policies to monotone ones (more details below). As such, an attribute secret key  $sk_{uid,i}$  issued by an authority is traditionally associated to a user  $uid$  and an attribute identifier  $i \in [n]$ , but not the value  $x_i$  of the  $i$ -th attribute. By collecting keys for attributes  $i \in A \subseteq [n]$ , a user  $uid$  can decrypt ciphertexts associated to access policies  $\mathbb{A} \subseteq 2^{[n]}$  with

<sup>3</sup>Our 2C-ABE is trivially secure in this case since there is only one sub-encryptor.

<sup>4</sup>They are much more powerful but also likely much more difficult to construct, both conceptually and potentially in terms of required assumptions.

**Table 1:** Overview of selected MA-ABE schemes. P: polynomial-size circuits.  $\text{static}^-$ : static corruption with restrictions. Selective queries refers to adversary declaring all queries at once, before seeing the public parameters.

Scheme	Structure	Policy	Corruption	$\text{sk}_i$ Query
[DKW23b]	Group	NC1	adaptive	adaptive
[DKW21]	Lattice	DNF	static	selective
[DKW21]	Lattice	NC1	none	selective
[WWW22]	Lattice	NC1	static	selective
Section 6	Lattice	P	$\text{static}^-$	selective

$A \in \mathbb{A}$ . When representing an access policy as a circuit  $f(x_1, \dots, x_n)$ , getting a secret key  $\text{sk}_{\text{uid},i}$  could be interpreted as getting authorised for  $x_i = 1$ .

For schemes natively supporting non-monotone policies, however, the above convention becomes problematic since in this case the value  $x_i$  of each attribute  $i$  could influence the acceptance of the policy, and a user must collect keys from all authorities. In this work, we instead following the syntax of ABE for circuits [BGG<sup>+</sup>14, Wee22], where an attribute secret key  $\text{sk}_{\text{uid},i,x_i}$  is additionally associated to the value  $x_i$  of the  $i$ -th attribute. The syntax of MC-ABE is defined analogously.

**Pairing-based MA-ABE for NC1.** A large class of MA-ABE schemes (e.g. [LW11, WFL19, DKW21, DKW23a, DKW23b, AG23], non-exhaustively), especially pairing-based ones, support access policies authorised by (monotone) linear secret sharing schemes (LSSS). It is folklore that any NC1 circuit can be converted into a monotone LSSS by interpreting positive and negative literals of the inputs as independent variables. As such many pairing-based schemes (e.g. [LW11, DKW23a, DKW23b, AG23], see also [DKW23b, Table 1]) can be interpreted as MA-ABE for NC1 circuits.

**Lattice-based MA-ABE for DNF, NC1, and circuits.** All pairing-based cryptographic constructions are vulnerable against quantum adversaries. Currently, all plausibly post-quantum secure candidates are lattice-based, including the schemes of [DKW21, WWW22], and ours. We summarise existing lattice-based MA-ABEs in Table 1, where we also include the state-of-the-art group-based scheme of [DKW23b] for comparison.

In the lattice setting, instantiating the MA-ABE construction of [DKW21] with the above LSSS for NC1 turns out to be insecure since the LSSS needs to additionally satisfy a property known as “linear independence for unauthorised rows”. Instead, they instantiate the construction with an LSSS which captures DNF formulas, thus obtaining an MA-ABE for DNFs under the LWE assumption.

We note, however, that if the MA-ABE of [DKW21] is instantiated with the above LSSS for NC1, then it would be secure in a setting where all authorities involved<sup>5</sup> in the challenge ciphertext are honest (cf. [DKW21, Remark 6.1]).

All (pairing- and lattice-based) MA-ABE constructions discussed so far are proven secure in the random oracle model. An exception is the lattice-based scheme of [WWW22], which also supports DNF formulas, and is proven secure in the standard model under the evasive LWE assumption.

To summarise, all existing pairing-based MA-ABE schemes support up to NC1 circuits, and the only two existing lattice-based schemes both support DNF formulas. If we are willing to (completely) forego security against corrupt authorities, then the lattice-based scheme of [DKW21] supports up to NC1 circuits. In contrast, our MA-ABE constructions

<sup>5</sup>By an authority being involved in the challenge ciphertext, we mean that the ciphertext is associated to a policy  $f(X_1, \dots, X_n)$  where the authority is responsible to some  $X_i$ .

**Table 2:** Overview of selected MI-/MC-ABE/FE schemes. PK/MSK/SK: main/sub encryption algorithm is w.r.t. public-key/master-secret-key(corruption not possible)/user-secret-key. Lin: linear functions, Quad: quadratic functions, P: polynomial-size circuits. -: corruption not allowed by setting, static<sup>-</sup>: static corruption with restrictions. sel: selective, adp: adaptive, ?: no security proof. Selective queries broadly refers to adversary declaring all queries at once, either before or after seeing the public parameters.

Scheme	MC/MI	Encryption		Structure	Policy	Corruption	Query	
		Main	Sub				ctxt <sub>i</sub>	sk <sub>f</sub>
[AGT22]	MC	MSK	MSK	Group	Quad	-	sel	sel
[LT19]	MC	SK	SK	Lattice	Lin	adaptive	adp	adp
Section 5	2C	PK	SK	Lattice	P	static <sup>-</sup>	sel	adp
Section 7	MC	PK	SK	Lattice	P	static <sup>-</sup>	sel	adp
[AGT22]	MI	SK	SK	Group	Quad	static	sel	sel
[Ayy22]	2I	PK	MSK	Lattice	P	-	?	?
[ARY23]	constantI	PK	MSK	Lattice	P	-	sel	sel

is the first to support general polynomial-size circuits with limited but non-trivial security against corrupt authorities. Instead of LSSS, our constructions leverage homomorphic computation, analogous to their single-party counterparts [BGG<sup>+</sup>14, Wee22].

We remark that although the scheme of [Kim19] supports arbitrary polynomial-size circuits, it requires a centralised key generation. In contrast, all other schemes discussed in this work, including ours, feature distributed key generation.

**Security Notions.** MA-ABE with a wide spectrum of security notions have been considered, many being incomparable. Below, we attempt to give a systematic overview.

Security notions of MA-ABE mainly differ in the restrictions imposed to

- (i) corruption queries, i.e. asking for the master secret key of a specified authority,
- (ii) attribute key queries, i.e. asking for an attribute secret key issued by a specified authority to a specified user associated to a specified attribute, and
- (iii) challenge ciphertext queries, i.e. asking for a ciphertext encrypting one of two specified messages associated to a specified access policy.

In the fully adaptive case, the adversary is allowed to adaptively issue all three kinds of queries, so long as the challenge ciphertexts are not trivially decryptable as mandated by the correctness of the scheme. Achieving fully adaptive security is very challenging, and has only been recently achieved by the pairing-based MA-ABE for NC1 of [DKW23b].

All other existing schemes are proven secure under some restricted security model. In particular, existing lattice-based schemes [DKW21, WWW22] are proven secure in a “very-selective” model where the adversary must declare all queries of all three types in advance before receiving even the authorities’ public keys. This is not surprising considering even the single-authority scheme of [Wee22] has the same restrictions.<sup>6</sup>

Putting aside adaptiveness of queries, the default security notion of MA-ABE has been that the adversary cannot distinguish the encrypted message, so long as the challenge ciphertext is not decryptable by its collection of corrupt master secret keys and attribute keys. In particular, achieving security only when all authorities involved in the challenge ciphertext are honest is traditionally deemed too weak.

<sup>6</sup>Except obviously that there cannot be corruption query in the single-authority setting.



However, we make a case for this weak security notion still being non-trivial and meaningful, if the MA-ABE scheme features distributed key generation. Indeed, the utility of such a scheme is irreplaceable by a single-authority scheme, since having distributed key generation means that the encryptor can freely pick any set of authorities to encrypt their message against. Moreover, the insecurity of one ciphertext due to authority corruption has no direct implication towards the security of another independent ciphertext.<sup>7</sup>

Both the scheme of [DKW21, Remark 6.1] for NC1 and our MA-ABE scheme achieve very-selective honest-authorities security. Moreover, unlike the scheme of [DKW21, Remark 6.1] which offers no security in presence of corrupt authorities, the schemes presented in this work retain limited security assuming that keys from at least one honest authority is missing for each user. Our 2C-/MC-ABE achieve similar security in the MC setting. As reference, we summarise existing lattice-based MC- and MI-schemes in Table 2, where we also include the state-of-the-art group-based schemes for comparison. In this realm, constructions for linear and quadratic policies are called MC-/MI-FEs in the literature.

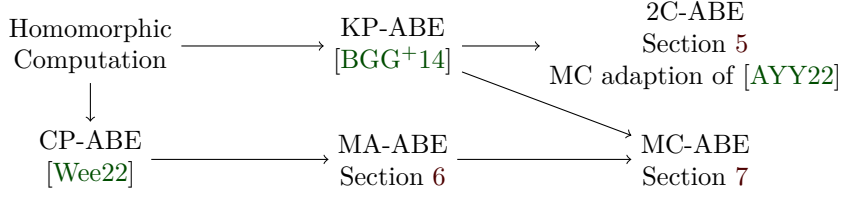
## 1.4 Discussions

**Non-triviality even assuming evasive LWE.** While (some form of) evasive LWE implies advanced primitives including null-iO [VWW22] and witness encryption (WE) [Tsa22], which could be used to build (some flavours of) ABE, we observe the following limitations/obstacles:

- The only existing null-iO and WE constructions [VWW22, Tsa22] rely on evasive LWE assumptions which holds for general, private-coin auxiliary inputs, which are qualitatively stronger assumptions. In particular, as discussed in [Wee22, Wee23], evasive LWE for general private-coin auxiliaries is unlikely to hold in its full generality, and recently counterexamples against certain subclasses of private-coin evasive LWE have been discovered [BUW24]. In contrast, the evasive LWE assumptions used for direct constructions of ABE by [Wee22] and of MA-/MC-ABE in this work involve only public-coin auxiliaries, which is qualitatively weaker than what is currently needed for null-iO and WE.
- Constructions of ABE from null-iO/WE seem to require embedding some form of obfuscation of the access policy in the ciphertext, leading to non-compact ciphertexts, i.e. ciphertext size is dependent on policy size. Explicit constructions of ABE from WE seem to appear only recently [FWW23], which built registered-ABE (RABE) and broadcast encryption (BE) from WE. Indeed, their RABE has non-compact ciphertexts due to the aforementioned obstacle, and the techniques they used for building BE do not seem to translate to an ABE for circuits. In contrast, [Wee22] and our schemes achieve compact ciphertexts.

**On Removing Random Oracles.** For all of our constructions, the random oracles can plausibly be removed by borrowing existing techniques. In a nutshell, for our 2C-ABE, the construction may be modified in a way analogous to existing lattice-based IBE with security in the standard model, for which we discuss in more details in Remark 3 in Section 5. For our MA- and MC-ABEs, the random oracle may be instantiated with a pseudorandom function of e.g. [BLMR13] which consists of subset product of public low-norm matrices, analogous to how [WWW22] achieved MA-ABE for subset policies without random oracles, for which we discuss in more details in Remark 4 in Section 6.

<sup>7</sup>For example, suppose authority 0 is corrupt, 1 and 2 are honest, and  $\text{ctxt}_{0,1}$  (resp.  $\text{ctxt}_{1,2}$ ) involves authorities 0 and 1 (resp. 1 and 2). Then even if  $\text{ctxt}_{0,1}$  is insecure,  $\text{ctxt}_{1,2}$  could still be secure.



**Figure 1:** Logic flow of technical overview.

## 2 Technical Overview

Our constructions heavily rely on lattice-based homomorphic computation [GSW13, BGG<sup>+</sup>14] and the techniques introduced in Wee’s CP-ABE construction [Wee22]. Figure 1 depicts the logic flow of the technical overview over our constructions.

We begin by recalling homomorphic computation techniques [GSW13] and Boneh et al.’s KP-ABE scheme [BGG<sup>+</sup>14], which Agrawal et al.’s 2I-ABE [Ayy22] is based on. We then explain our adaption of Agrawal et al.’s 2I-ABE to the 2-client setting. Moving to a different construction paradigm, we recall the essence of Wee’s CP-ABE [Wee22], as well as the evasive LWE and tensor LWE assumptions used to prove the security of the scheme. This provides a basis for explaining our extension of Wee’s scheme to a MA-ABE. Finally, combining many of the prior techniques, we overview our MC-ABE construction.

All discussion in this technical overview are over  $\mathbb{Z}_q$  where  $q$  is a super-polynomial modulus, and for ease of exposition mod  $q$  operations are suppressed. In order to denote the noisy version of a term, we underline it with a wavy underline  $\underline{\cdot}$ , e.g.  $\underline{\mathbf{s}^T \mathbf{A}}$  means  $\mathbf{s}^T \mathbf{A} + \mathbf{e}^T$  where  $\mathbf{e}$  is short relative to  $q$ . We abuse  $\chi$  to denote any Gaussian distributions over  $\mathbb{Z}$ , even if they are with different Gaussian parameters in the formal constructions. Given any matrices  $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$  and  $\mathbf{Z} \in \mathbb{Z}_q^{n \times k}$ , we use  $\mathbf{A}^{-1}(\mathbf{Z})$  to denote the distribution of matrix  $\mathbf{Y}$  samples according to  $\chi^{m \times k}$  conditioned on  $\mathbf{A}\mathbf{Y} = \mathbf{Z} \bmod q$ .

### 2.1 Homomorphic Computation

We recall the basics of homomorphic computation in lattice-based cryptography by [GSW13, BGG<sup>+</sup>14]. Let  $\mathbf{g}^T := (1, 2, \dots, 2^{\lceil \log q \rceil - 1})$  and  $\mathbf{G} := \mathbf{I}_n \otimes \mathbf{g}^T$  be the gadget vector and matrix respectively [MP12]. Let  $\mathbf{B} = (\mathbf{B}_1, \dots, \mathbf{B}_\ell) \in \mathbb{Z}_q^{n \times \ell m}$ ,  $f : \{0, 1\}^\ell \rightarrow \{0, 1\}$  be a Boolean function represented by a circuit of bounded-polynomial-depth, and  $\mathbf{x} \in \{0, 1\}^\ell$ . For appropriately chosen parameters, there exist efficiently computable short matrices  $\mathbf{H}_{\mathbf{B}, f} \in \mathbb{Z}^{\ell m \times m}$  and  $\mathbf{H}_{\mathbf{B}, f, \mathbf{x}} \in \mathbb{Z}^{\ell m \times m}$  such that

$$\mathbf{B}_f := \mathbf{B}\mathbf{H}_{\mathbf{B}, f}, \quad (\mathbf{B} - \mathbf{x}^T \otimes \mathbf{G}) \cdot \mathbf{H}_{\mathbf{B}, f, \mathbf{x}} = \mathbf{B}_f - f(\mathbf{x}) \cdot \mathbf{G}.$$

### 2.2 Boneh et al.’s KP-ABE

Our starting point is the KP-ABE of Boneh et al. [BGG<sup>+</sup>14] summarised as follows.

- mpk:  $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n \times 2m}$ ,  $\mathbf{B} \leftarrow_{\$} \mathbb{Z}_q^{n \times \ell m}$ ,  $\mathbf{v} \leftarrow_{\$} \mathbb{Z}_q^n$ .
- $sk_f: (\mathbf{A} \mid \mathbf{B}_f)^{-1}(\mathbf{v})$ .
- $ct_{\mathbf{x}, \mu}: \underline{\mathbf{s}^T(\mathbf{A} \mid \mathbf{B} - \mathbf{x}^T \otimes \mathbf{G})}, \underline{\mathbf{s}^T \mathbf{v} + \frac{q}{2}\mu}$ .

The decryptor derives  $\underline{\mathbf{s}^T(\mathbf{A} \mid \mathbf{B}_f)}$  from  $\underline{\mathbf{s}^T(\mathbf{A} \mid \mathbf{B} - \mathbf{x}^T \otimes \mathbf{G})}$ , then multiplies  $(\mathbf{A} \mid \mathbf{B}_f)^{-1}(\mathbf{v})$  to derive  $\underline{\mathbf{s}^T \mathbf{v}}$ , and finally recovers  $\underline{\frac{q}{2}\mu}$  and hence  $\mu$ .



Boneh et al. [BGG<sup>+</sup>14] proved the above construction selectively secure under the LWE assumption. To recall, the selective security experiment of KP-ABE goes as follows: The PPT adversary declares the challenge attribute  $\mathbf{x}^*$  for which they wish to see a challenge ciphertext. They are then given the public parameters and access to a key generation oracle, to which they can query functions  $f$  rejecting  $\mathbf{x}^*$ , i.e.  $f(\mathbf{x}^*) = 1$ . Eventually, the adversary specifies two messages  $\mu_0$  and  $\mu_1$ , and the ciphertext of one of which w.r.t.  $\mathbf{x}^*$  will be given to the adversary. The adversary then continues to interact with the oracle, and eventually guesses which message was encrypted.

A crucial step in the proof of selective security in [BGG<sup>+</sup>14] is to replace  $\mathbf{B}$  with  $\mathbf{B} = \mathbf{A}\mathbf{R} + (\mathbf{x}^*)^\top \otimes \mathbf{G}$  where  $\mathbf{R}$  is some random short matrix. By the leftover hash lemma,  $\mathbf{B}$  generated this way is statistically close to a uniformly random one. This alternative way of generating  $\mathbf{B}$ , however, allows to derive a gadget trapdoor [MP12]  $\mathbf{RH}_{\mathbf{B},f,\mathbf{x}^*}$  for  $(\mathbf{A} \mid \mathbf{B}_f) = (\mathbf{A} \mid \mathbf{A}\mathbf{R}\mathbf{H}_{\mathbf{B},f,\mathbf{x}^*} + \mathbf{G})$  using which the reduction can answer any key query for any  $f$  rejecting  $\mathbf{x}^*$ , i.e.  $f(\mathbf{x}^*) = 1$ , without knowing any trapdoor for  $\mathbf{A}$ .

### 2.3 2-Client Variant of AYY's 2-Input ABE

We start by recalling the core components in the 2I-ABE construction of Agrawal, Yadav, and Yamada (AYY) [AYY22]. The AYY scheme borrows the main idea of the work from Brakerski and Vaikuntanathan [BV22] on CP-ABE, which, in turn, was based on the KP-ABE scheme of Boneh et al. [BGG<sup>+</sup>14] recalled above. We adapt their scheme to the MC setting and prove its security under the LWE assumption in the ROM.

**AYY's 2I-ABE.** AYY describe their scheme so that the authority and both encryptors share a master secret key. We observe that, actually, the authority and encryptor can generate their own keys distributedly, and encryptor 1 requires no secret key. Below, we summarise this distributed version of the AYY scheme:

- pp:  $\{\mathbf{B}_{i,j}\}_{i \in [2], j \in [\ell]} \leftarrow_{\$} (\mathbb{Z}_q^{n \times m})^{2\ell}$ ,  $\mathbf{v} \leftarrow_{\$} \mathbb{Z}_q^n$ .
- apk:  $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n \times 2m}$ .
- epk<sub>2</sub>:  $\{\mathbf{D}_{2,j,b}\}_{j \in [\ell], b \in \{0,1\}} \leftarrow_{\$} (\mathbb{Z}_q^{n \times 4\ell m})^{2\ell}$ .
- sk<sub>f</sub>:  $\mathbf{u}_f \leftarrow_{\$} (\mathbf{A} \mid \mathbf{B}_f)^{-1}(\mathbf{v})$ .
- ctxt<sub>1,x<sub>1</sub>,μ</sub>:  $\mathbf{C}_0$ ,  $(\mathbf{C}_{1,j})_{j \in [\ell]}$ ,  $(\bar{\mathbf{C}}_{2,j,b})_{j \in [\ell], b \in \{0,1\}}$ ,  $\mathbf{c}_3$  where

$$\begin{aligned} \mathbf{C}_0 &= \underline{\mathbf{S}\mathbf{A}}, & \mathbf{C}_{1,j} &= \underline{\mathbf{S}(\mathbf{B}_{1,j} - x_{1,j}\mathbf{G})}, \\ \bar{\mathbf{C}}_{2,j,b} &= \underline{\mathbf{D}_{2,j,b}^\top \cdot \hat{\mathbf{S}}_{2,j,b}^\top + \mathbf{S} \cdot (\mathbf{B}_{2,j} - b\mathbf{G})}, & \mathbf{c}_3 &= \underline{\mathbf{S}\mathbf{v} + \mathbf{g}\mu}, \end{aligned}$$

with  $\mathbf{S} \leftarrow_{\$} \mathbb{Z}_q^{4\ell m \times n}$  and  $\hat{\mathbf{S}}_{2,j,b} \leftarrow_{\$} \mathbb{Z}_q^{m \times n}$  for all  $j \in [\ell]$  and  $b \in \{0,1\}$ .

- ctxt<sub>2,x<sub>2</sub></sub>:  $\mathbf{t}_{\mathbf{x}_2} \leftarrow_{\$} \mathbf{D}_{2,\mathbf{x}_2}^{-1}(\mathbf{0})$  where  $\mathbf{D}_{2,\mathbf{x}_2}$  vertically concatenates  $\{\mathbf{D}_{2,j,x_{2,j}}\}_{j \in [\ell]}$ .

Note that  $\mathbf{t}_{\mathbf{x}_2}$  is a simultaneous solution of the SIS instances  $\mathbf{D}_{2,j,x_{2,j}}$  for all  $j \in [\ell]$ . Such a preimage can be sampled using a trapdoor of a matrix  $\mathbf{D}_2$  which is the vertical concatenation of  $\{\mathbf{D}_{2,j,b}\}_{j \in [\ell], b \in \{0,1\}}$ .

To decrypt, left-multiply  $\mathbf{t}_{\mathbf{x}_2}^\top$  to each of  $\mathbf{C}_0$ ,  $(\mathbf{C}_{1,j})_{j \in [\ell]}$ ,  $(\bar{\mathbf{C}}_{2,j,x_{2,j}})_{j \in [\ell]}$ , and  $\mathbf{c}_3$ . This yields a ciphertext of almost the same form as in Boneh et al.'s KP-ABE:

$$\underline{\mathbf{s}^\top(\mathbf{A} \mid \mathbf{B} - \mathbf{x}^\top \otimes \mathbf{G})}, \quad \underline{\mathbf{s}^\top \mathbf{v} + \mathbf{t}_{\mathbf{x}_2}^\top \mathbf{g}\mu}$$

where  $\mathbf{s}^\top = \mathbf{t}_{\mathbf{x}_2}^\top \mathbf{S}$ . Using the decryption procedure in Boneh et al.'s KP-ABE, the decryptor removes the mask  $\mathbf{s}^\top \mathbf{v}$  and recovers  $\mathbf{t}_{\mathbf{x}_2}^\top \mathbf{g}\mu$ , which is short if  $\mu = 0$ .

While Agrawal et al. [AYY22] did not provide a proof for their 2I-ABE construction, the heuristics for security is that there seems to be no meaningful way to combine two different short vectors  $\mathbf{t}_{\mathbf{x}_2}$  and  $\mathbf{t}_{\mathbf{x}'_2}$  for  $\mathbf{x}_2 \neq \mathbf{x}'_2$  to obtain a new short vector  $\mathbf{t}_{\hat{\mathbf{x}}_2}$  encoding a new attribute  $\hat{\mathbf{x}}_2$ . This allows one to conjecture that  $\mathbf{D}_{2,j,1-x_{2,j}} \mathbf{t}_{\mathbf{x}_2}$  is pseudorandom for all  $j \in [\ell]$ , and hence for all  $j$  the decryptor only has access to one of  $(\mathbf{S}(\mathbf{B}_{2,j} + b\mathbf{G}))_{b \in \{0,1\}}$ .

**Our 2C-ABE.** We adapt the AYY construction to the MC model by introducing ciphertext identifiers  $\text{cid}$ . For this, we will use a hash function  $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^n$  modelled as a random oracle. Similar to AYY,  $\text{ctxt}_1$  with ciphertext identifier  $\text{cid}$  consists of almost the same ciphertext components, except that it now additionally contains  $(\tilde{\mathbf{c}}_{2,j,b})_{j \in [\ell], b \in \{0,1\}}$  where  $\tilde{\mathbf{c}}_{2,j,b} := H(\text{cid}, 2, j, b)^\top \hat{\mathbf{S}}_{2,j,b}^\top$ . We modify  $\text{ctxt}_2$  such that it consists of a short vector

$$\mathbf{t}_{\text{cid}, \mathbf{x}_2} \leftarrow_{\S} \mathbf{D}_{2, \mathbf{x}_2}^{-1} \left( H(\text{cid}, 2, j, x_{2,j}) : j \in [\ell] \right).$$

In other words, it is a short vector satisfying  $\mathbf{D}_{2,j,x_{2,j}} \mathbf{t}_{\text{cid}, \mathbf{x}_2} = H(\text{cid}, 2, j, x_{2,j})$  for all  $j \in [\ell]$  simultaneously. Finally, we modify the decryption procedure so that the step of computing  $\mathbf{t}_{\text{cid}, \mathbf{x}_2}^\top \bar{\mathbf{C}}_{2,j,x_{2,j}}$  is replaced by  $\mathbf{t}_{\text{cid}, \mathbf{x}_2}^\top \bar{\mathbf{C}}_{2,j,x_{2,j}} - \tilde{\mathbf{c}}_{2,j,x_{2,j}}$  for each  $j \in [\ell]$ , so that the masking term  $H(\text{cid}, 2, j, x_{2,j})^\top \hat{\mathbf{S}}_{2,j,x_{2,j}}^\top$  can be cancelled out. The rest then follows the AYY scheme.

**Security Analysis.** The security of the scheme essentially follows from two steps. First, we simulate  $\text{ctxt}_2$  via programming the random oracle  $H$  so that we can abandon the trapdoor of  $\mathbf{D}$ , which is possible since the adversary cannot query more than one attribute  $\mathbf{x}_2$  for a single ciphertext identifier  $\text{cid}$ . Then, to argue

$$\bar{\mathbf{C}}_{2,j,b} = \mathbf{D}_{2,j,b}^\top \cdot \hat{\mathbf{S}}_{2,j,b}^\top + \mathbf{S} \cdot (\mathbf{B}_{2,j} - b\mathbf{G})$$

is pseudorandom for all  $j, b$ , we show that either one of the two summands is so. More precisely, for any attribute  $\mathbf{x}_2$ , we show that for any  $j \in [\ell]$ :

- If  $b = x_{2,j}$ , then  $\mathbf{S}(\mathbf{B}_{2,j} - x_{2,j}\mathbf{G})$  and  $\mathbf{C}_{1,j} = \mathbf{S}(\mathbf{B}_{1,j} - x_{1,j}\mathbf{G})$  are pseudorandom, the proof of which follows that of Boneh et al.'s KP-ABE [BGG<sup>+</sup>14].
- If  $b = 1 - x_{2,j}$ , then  $\mathbf{D}_{2,j,1-x_{2,j}}^\top \hat{\mathbf{S}}_{2,j,1-x_{2,j}}^\top$  and  $\tilde{\mathbf{c}}_{2,j,1-x_{2,j}} = H(\text{cid}, j, 1 - x_{2,j})^\top \hat{\mathbf{S}}_{j,1-x_{2,j}}^\top$  are pseudorandom. This follows directly from LWE (w.r.t. LWE secret  $\hat{\mathbf{S}}_{2,j,1-x_{2,j}}$ ), as the joint distribution of  $\mathbf{D}_{2,j,1-x_{2,j}}$  and  $H(\text{cid}, j, 1 - x_{2,j})$  is uniform random, since the adversary never gets to query more than one attribute  $\mathbf{x}_2$  for the same  $\text{cid}$ .

**Insecurity against Corruption.** We briefly discuss the insecurity of AYY and our adapted 2C-ABE in case the adversary corrupts the second encryptor. Using the trapdoor of  $\mathbf{D}$ , the adversary could compute a short preimage  $\mathbf{t} \leftarrow_{\S} \mathbf{D}^{-1}(\mathbf{0})$ , hence deriving

$$\mathbf{t}^\top \bar{\mathbf{C}}_{2,j,0} = \mathbf{t}^\top \mathbf{S}(\mathbf{B}_{2,j}), \quad \mathbf{t}^\top \bar{\mathbf{C}}_{2,j,1} = \mathbf{t}^\top \mathbf{S}(\mathbf{B}_{2,j} - \mathbf{G}), \quad \mathbf{t}^\top \mathbf{c}_3 = \mathbf{t}^\top \mathbf{S}\mathbf{v} + \mathbf{t}^\top \mathbf{g}\mu.$$

Taking the difference of the first two terms yields  $\mathbf{t}^\top \mathbf{S}\mathbf{G}$ , from which the adversary could recover  $\mathbf{t}^\top \mathbf{S}$  since  $\mathbf{G}$  admits a public trapdoor. Then, the adversary could remove the masking term  $\mathbf{t}^\top \mathbf{S}\mathbf{v}$  and recover  $\mathbf{t}^\top \mathbf{g}\mu$ , which is short if  $\mu = 0$ .

## 2.4 Wee's CP-ABE

To obtain our MA- and MC-ABE schemes, our starting point is the CP-ABE of [Wee22]<sup>8</sup> which can be summarised as follows<sup>9</sup>:

- mpk:  $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n(m+1) \times 2m(m+1)}$ ,  $\mathbf{B} = (\mathbf{B}_1, \dots, \mathbf{B}_\ell) \leftarrow_{\$} \mathbb{Z}_q^{n \times \ell m}$ ,  $\mathbf{P} \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$ ,  $\mathbf{u} \leftarrow_{\$} \chi^m$ .

Denote  $\mathbf{A} = \begin{pmatrix} \overline{\mathbf{A}} \\ \underline{\mathbf{A}} \end{pmatrix}$  where  $\overline{\mathbf{A}} \in \mathbb{Z}_q^{n \times 2m(m+1)}$ ,  $\underline{\mathbf{A}} \in \mathbb{Z}_q^{nm \times 2m(m+1)}$ .

- sk<sub>x</sub>:  $\mathbf{k}_x \in \mathbb{Z}^{2m(m+1)}$ ,  $\mathbf{U}_x \in \mathbb{Z}^{2m^2 \times (\ell m + 1)}$  where

$$\mathbf{k}_x \leftarrow_{\$} \chi^m, \quad \mathbf{U}_x \leftarrow_{\$} \mathbf{A}^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_x \\ (\mathbf{B} - \mathbf{x}^T \otimes \mathbf{G}) \otimes \mathbf{k}_x \end{pmatrix}$$

- ctxt<sub>f,μ</sub>:  $(\mathbf{c}_0, \mathbf{c}_1) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{2m(m+1)}$  where  $\overline{\mathbf{s}} \leftarrow_{\$} \mathbb{Z}_q^n$ ,  $\underline{\mathbf{s}} \leftarrow_{\$} \mathbb{Z}_q^{nm}$ ,

$$\mathbf{c}_0^T = \underbrace{\overline{\mathbf{s}}^T \mathbf{P} + \underline{\mathbf{s}}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m)} + \mu \mathbf{g}^T, \quad \mathbf{c}_1^T = \underbrace{(\overline{\mathbf{s}}^T \mid \underline{\mathbf{s}}^T) \mathbf{A}}.$$

To decrypt, one declares  $\mu = 0$  if  $\mathbf{c}_0^T \mathbf{k}_x - \mathbf{c}_1^T \mathbf{U}_x = \mu \mathbf{g}^T \mathbf{k}_x$  is short.

To prove the very-selective security of the scheme, Wee [Wee22] relied on the LWE, evasive LWE, and tensor LWE assumptions. First, using the evasive LWE assumption, it suffices to argue that the following are pseudorandom:

$$\underbrace{\overline{\mathbf{s}}^T \mathbf{P} + \underline{\mathbf{s}}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m)}, \underbrace{\overline{\mathbf{s}}^T \overline{\mathbf{A}} + \underline{\mathbf{s}}^T \underline{\mathbf{A}}}, \left( \underbrace{\overline{\mathbf{s}}^T \mathbf{P} \mathbf{k}_x, \underline{\mathbf{s}}^T ((\mathbf{B} - \mathbf{x}^T \otimes \mathbf{G}) \otimes \mathbf{k}_x)} \right)_{\mathbf{x} \in \mathcal{X}}$$

where  $\mathcal{X}$  collects attributes for which the adversary asks for secret keys. Writing

$$\underbrace{\overline{\mathbf{s}}^T \mathbf{P} \mathbf{k}_x} = \underbrace{(\overline{\mathbf{s}}^T \mathbf{P} + \underline{\mathbf{s}}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m)) \mathbf{k}_x} - \underbrace{\underline{\mathbf{s}}^T ((\mathbf{B} - \mathbf{x}^T \otimes \mathbf{G}) \otimes \mathbf{k}_x) \mathbf{H}_{\mathbf{B},f,\mathbf{x}} \mathbf{u}} + \underbrace{\underline{\mathbf{s}}^T (\mathbf{G} \mathbf{u} \otimes \mathbf{k}_x)},$$

for each  $\mathbf{x} \in \mathcal{X}$  and resorting to noise flooding, it suffices to argue that

$$\underbrace{\overline{\mathbf{s}}^T \mathbf{P} + \underline{\mathbf{s}}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m)}, \underbrace{\overline{\mathbf{s}}^T \overline{\mathbf{A}} + \underline{\mathbf{s}}^T \underline{\mathbf{A}}}, \left( \underbrace{\underline{\mathbf{s}}^T ((\mathbf{B} - \mathbf{x}^T \otimes \mathbf{G} \mid \mathbf{G} \mathbf{u}) \otimes \mathbf{k}_x)} \right)_{\mathbf{x} \in \mathcal{X}}$$

is pseudorandom. Notice now that the LWE secret  $\overline{\mathbf{s}}$  only appears in the terms  $\overline{\mathbf{s}}^T \mathbf{P}$  and  $\overline{\mathbf{s}}^T \overline{\mathbf{A}}$ , which are pseudorandom by LWE. We are now left with

$$\underbrace{\underline{\mathbf{s}}^T ((\mathbf{B} - \mathbf{x}^T \otimes \mathbf{G} \mid \mathbf{G} \mathbf{u}) \otimes \mathbf{k}_x)}, \forall \mathbf{x} \in \mathcal{X}$$

which is pseudorandom under the tensor LWE assumption.

## 2.5 Our MA-ABE

We extend Wee's CP-ABE to an MA-ABE. The starting idea is two-fold: (i) We replace  $\mathbf{A}$  with  $\mathbf{A}_i$ ,  $i \in [k]$ , where authority  $i$  has a trapdoor for  $\mathbf{A}_i$  and is responsible for handing out keys for  $\mathbf{x}_{\text{uid},i}$  encoded as  $\mathbf{B}_i - \mathbf{x}_{\text{uid},i}^T \otimes \mathbf{G}$ . (ii) We replace the masking term  $\overline{\mathbf{s}}^T \mathbf{P}$  in the ciphertext by  $\mathbf{s}_i^T \mathbf{P}$ , for  $i \in [k]$ . The ciphertext is constructed in such a way that the  $i$ -th masking term  $\mathbf{s}_i^T \mathbf{P}$  can only be removed using key material provided by authority  $i$ . These result in a scheme that is secure when all authorities are honest, but is insufficient in presence of corruption (we elaborate this in Remark 1). Thus, we introduce the third modification, which involves an additional public matrix  $\mathbf{Q}$ , together with the associated term  $\mathbf{Q} \mathbf{K}_{\text{uid}}$  in the secret key and a new component in the ciphertext.

<sup>8</sup>For simplicity, we consider the variant obtained after the ‘‘second modification’’ [Wee22, Section 2.1] and proven secure under the tensor LWE assumption [Wee22, Section 5.4].

<sup>9</sup>We use  $\overline{\mathbf{A}}$  and  $\underline{\mathbf{A}}$  to denote the ‘‘top part’’ and ‘‘bottom part’’ of the matrix  $\mathbf{A}$ . Similarly  $\overline{\mathbf{s}}$  and  $\underline{\mathbf{s}}$  for the first and second chunk of the vector  $\mathbf{s}$ .

**Construction.** Let  $H : \{0, 1\}^* \rightarrow \chi^m \times \chi^{m \times m\ell}$  be a random oracle for deriving common randomness for generating user secret keys for a user identifier  $\text{uid}$ . Our construction can be summarised as follows:

- $\text{pp}$ :  $\mathbf{P} \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$ ,  $\mathbf{Q} \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$ ,  $\mathbf{u} \leftarrow_{\$} \chi^m$ .
- $\text{apk}_i$ :  $\mathbf{A}_i \leftarrow_{\$} \mathbb{Z}_q^{n(m+1) \times 2m(m+1)}$ ,  $\mathbf{B}_i \leftarrow_{\$} \mathbb{Z}_q^{n \times \ell m}$ .
- $\text{sk}_{\text{uid},i}$ :  $\mathbf{U}_{\text{uid},i} \in \mathbb{Z}^{2m}$  where  $(\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}}) := H(\text{uid})$  and

$$\mathbf{U}_{\text{uid},i} \leftarrow_{\$} \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ (\mathbf{B}_i - \mathbf{x}_{\text{uid},i}^{\text{T}} \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}.$$

- $\text{ctxt}$ :  $(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_k, \mathbf{c}) \in \mathbb{Z}_q^{km} \times (\mathbb{Z}_q^{2m(m+1)})^k \times \mathbb{Z}_q^m$  where

$$\begin{aligned} \mathbf{c}_i^{\text{T}} &= \underbrace{(\mathbf{s}_i^{\text{T}} \mid \mathbf{s}^{\text{T}}) \cdot \mathbf{A}_i}_{\text{wavy}} \quad \forall i \in [k], & \mathbf{c}_0^{\text{T}} &= \underbrace{(\mathbf{s}_1^{\text{T}} \mid \dots \mid \mathbf{s}_k^{\text{T}}) \cdot (\mathbf{I}_k \otimes \mathbf{Q})}_{\text{wavy}}, \\ \mathbf{c}^{\text{T}} &= \underbrace{\sum_{i \in [k]} \mathbf{s}_i^{\text{T}} \mathbf{P} + \mathbf{s}^{\text{T}} \cdot (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mu \mathbf{g}^{\text{T}}}_{\text{wavy}}. \end{aligned}$$

The new component  $\mathbf{c}_0$  allows for cancelling out the additional block  $\mathbf{Q}\mathbf{K}_{\text{uid}}$  in the secret key. After that, correctness is analogous to the scheme of Wee [Wee22].

**Security Analysis.** We sketch a proof that the above scheme is very-selectively secure under the evasive LWE and tensor LWE assumptions. In the following, we divide each  $\mathbf{A}_i = \begin{pmatrix} \overline{\mathbf{A}}_i \\ \underline{\mathbf{A}}_i \end{pmatrix}$  into a top part  $\overline{\mathbf{A}}_i \in \mathbb{Z}_q^{n \times 2m(m+1)}$  and a bottom part  $\underline{\mathbf{A}}_i \in \mathbb{Z}_q^{nm \times 2m(m+1)}$ . We use the shorthand  $\hat{\mathbf{B}}_{\text{uid},i} := \mathbf{B}_i - \mathbf{x}_{\text{uid},i}^{\text{T}} \otimes \mathbf{G}$ .

The adversary specifies the following information: (i)  $\mathcal{I}_{\text{corr}} \subset [k]$  the set of corrupt authorities, and (ii)  $Q$  the set of  $(\text{uid}, i, \mathbf{x}_{\text{uid},i})$  tuples for which the adversary requests a secret key for user  $\text{uid}$  associated to attribute  $\mathbf{x}_{\text{uid},i}$ . We write  $\mathcal{U}$  for the set of all  $\text{uid}$  appearing in  $Q$  and, for each  $\text{uid} \in \mathcal{U}$ ,  $\mathcal{I}_{\text{uid}} \subseteq [k]$  for the set of authorities from whom the adversary requests a secret key for user  $\text{uid}$ . In return, the adversary receives the following:

- Public information:  $(\mathbf{A}_i, \mathbf{B}_i)_{i \in [k]}$ ,  $\mathbf{P}$ ,  $\mathbf{Q}$ ,  $(\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}$ ,  $\mathbf{u}$
- Trapdoors for corrupt authorities:  $(\text{td}_{\mathbf{A}_i})_{i \in \mathcal{I}_{\text{corr}}}$
- Attribute secret keys:  $\mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}, \forall (\text{uid}, i, \mathbf{x}_{\text{uid},i}) \in Q$
- Challenge ciphertext:

$$\underbrace{((\mathbf{s}_i^{\text{T}} \mid \mathbf{s}^{\text{T}}) \cdot \mathbf{A}_i)_{i \in [k]}}_{\text{wavy}}, \underbrace{(\mathbf{s}_1^{\text{T}} \mid \dots \mid \mathbf{s}_k^{\text{T}}) \cdot (\mathbf{I}_k \otimes \mathbf{Q})}_{\text{wavy}}, \underbrace{\sum_{i \in [k]} \mathbf{s}_i^{\text{T}} \mathbf{P} + \mathbf{s}^{\text{T}} \cdot (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mu \mathbf{g}^{\text{T}}}_{\text{wavy}}.$$

We would like to show that the term masking  $\mu$  in the challenge ciphertext is pseudorandom in the view of the adversary. We distinguish between two cases:

**Case 1.**  $\mathcal{I}_{\text{corr}} = \emptyset$ , i.e. all authorities are honest.<sup>10</sup>

**Case 2.**  $\mathcal{I}_{\text{corr}} \neq \emptyset$ , i.e. some authorities are corrupt, and  $\mathcal{I}_{\text{uid}} \cup \mathcal{I}_{\text{corr}} \neq [k]$  for all  $\text{uid} \in \mathcal{U}$ , i.e. for each  $\text{uid}$  there exists at least one honest authority  $i_{\text{uid}} \notin \mathcal{I}_{\text{corr}}$  from whom the adversary receives no secret key for user  $\text{uid}$ . A discussion on this corruption setting is given in Section C.

<sup>10</sup>See Remark 2 for a discussion on assuming  $Q = [k] \times \mathcal{U}$ .

Case 1. Notice that the adversary's input can be efficiently simulated given:

$$\begin{aligned} & (\mathbf{A}_i, \mathbf{B}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u}, \\ & \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ & \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}, \forall \text{uid} \in \mathcal{U}, i \in [k] \\ & \underbrace{((\mathbf{s}_i^{\text{T}} | \mathbf{s}^{\text{T}}) \cdot \mathbf{A}_i, \mathbf{s}_i^{\text{T}}\mathbf{Q})}_{i \in [k]}, \underbrace{\sum_{i \in [k]} \mathbf{s}_i^{\text{T}}\mathbf{P} + \mathbf{s}^{\text{T}} \cdot (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m)} \end{aligned}$$

To argue that the masking term is pseudorandom, it suffices to prove that the terms in the last line above are pseudorandom. Invoking the evasive LWE assumption, it suffices to argue that the terms below are pseudorandom:

$$\begin{aligned} & (\mathbf{s}_i^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}}, \mathbf{s}_i^{\text{T}}\mathbf{Q}\mathbf{K}_{\text{uid}}, \mathbf{s}^{\text{T}} \cdot (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}))_{\text{uid} \in \mathcal{U}, i \in [k]}, \\ & (\mathbf{s}_i^{\text{T}}\bar{\mathbf{A}}_i + \mathbf{s}^{\text{T}}\underline{\mathbf{A}}_i, \mathbf{s}_i^{\text{T}}\mathbf{Q})_{i \in [k]}, \underbrace{\sum_{i \in [k]} \mathbf{s}_i^{\text{T}}\mathbf{P} + \mathbf{s}^{\text{T}} \cdot (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m)} \end{aligned}$$

For any uid, we observe the following identity expressing  $\mathbf{s}_1^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}}$  as a short linear combination of the other given terms and an additional term  $\mathbf{s}^{\text{T}}(\mathbf{G}\mathbf{u} \otimes \mathbf{k}_{\text{uid}})$ :

$$\begin{aligned} \mathbf{s}_1^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}} &= \left( \sum_{i \in [k]} \mathbf{s}_i^{\text{T}}\mathbf{P} + \mathbf{s}^{\text{T}} \cdot (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) \right) \mathbf{k}_{\text{uid}} - \sum_{i \in [2, k]} \mathbf{s}_i^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}} \\ &\quad - (\mathbf{s}^{\text{T}} \cdot (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}))_{i \in [k]} \mathbf{H}_{\mathbf{B}, f, \mathbf{x}_{\text{uid}}} \mathbf{u} + \mathbf{s}^{\text{T}} \cdot (\mathbf{G}\mathbf{u} \otimes \mathbf{k}_{\text{uid}}) \end{aligned}$$

This means that, using noise flooding, it suffices to argue that the terms

$$\begin{aligned} & (\mathbf{s}_i^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}})_{i \in [2, k], \text{uid} \in \mathcal{U}}, (\mathbf{s}^{\text{T}} \cdot (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}), \mathbf{s}^{\text{T}} \cdot (\mathbf{G}\mathbf{u} \otimes \mathbf{k}_{\text{uid}}))_{\text{uid} \in \mathcal{U}, i \in [k]}, \\ & (\mathbf{s}_i^{\text{T}}\bar{\mathbf{A}}_i + \mathbf{s}^{\text{T}}\underline{\mathbf{A}}_i, \mathbf{s}_i^{\text{T}}\mathbf{Q})_{i \in [k]}, \underbrace{\sum_{i \in [k]} \mathbf{s}_i^{\text{T}}\mathbf{P} + \mathbf{s}^{\text{T}} \cdot (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m)} \end{aligned}$$

are pseudorandom. Notice that  $\mathbf{s}_1$  only appears in the terms in the second line above. By the LWE assumption, we have that  $\mathbf{s}_1^{\text{T}}\bar{\mathbf{A}}_1$ ,  $\mathbf{s}_1^{\text{T}}\mathbf{Q}$  and  $\mathbf{s}_1^{\text{T}}\mathbf{P}$  are pseudorandom, hence so are  $\mathbf{s}_1^{\text{T}}\bar{\mathbf{A}}_1 + \mathbf{s}^{\text{T}}\underline{\mathbf{A}}_1$  and  $\sum_{i \in [k]} \mathbf{s}_i^{\text{T}}\mathbf{P} + \mathbf{s}^{\text{T}} \cdot (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m)$ . Now it remains to argue pseudorandomness of the following:

$$\begin{aligned} & (\mathbf{s}_i^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}})_{i \in [2, k], \text{uid} \in \mathcal{U}}, (\mathbf{s}^{\text{T}} \cdot (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}), \mathbf{s}^{\text{T}} \cdot (\mathbf{G}\mathbf{u} \otimes \mathbf{k}_{\text{uid}}))_{\text{uid} \in \mathcal{U}, i \in [k]}, \\ & (\mathbf{s}_i^{\text{T}}\bar{\mathbf{A}}_i + \mathbf{s}^{\text{T}}\underline{\mathbf{A}}_i, \mathbf{s}_i^{\text{T}}\mathbf{Q})_{i \in [2, k]} \end{aligned}$$

Using noise flooding, for each  $i \in [2, k]$ , the terms  $(\mathbf{s}_i^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}})_{\text{uid} \in \mathcal{U}}$  is simulatable using  $\mathbf{s}_i^{\text{T}}\mathbf{P}$ . Then, by LWE, we have that  $\mathbf{s}_i^{\text{T}}\mathbf{P}$ ,  $\mathbf{s}_i^{\text{T}}\mathbf{Q}$  and  $\mathbf{s}_i^{\text{T}}\bar{\mathbf{A}}_i$  are pseudorandom for all  $i \in [2, k]$ . We are thus left to argue the pseudorandomness of

$$(\mathbf{s}^{\text{T}} \cdot (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}), \mathbf{s}^{\text{T}} \cdot (\mathbf{G}\mathbf{u} \otimes \mathbf{k}_{\text{uid}}))_{\text{uid} \in \mathcal{U}, i \in [k]}$$

which follows from the tensor LWE assumption.

Case 2. Before describing the security proof, we observe that security in this case cannot rely on the secrecy of the LWE secret  $\mathbf{s}$ , since the adversary can use  $\text{td}_{\mathbf{A}_{i^*}}$  of any corrupt authority  $i^*$  to invert  $(\mathbf{s}_{i^*}^{\text{T}} | \mathbf{s}^{\text{T}}) \cdot \mathbf{A}_{i^*}$  in the ciphertext and recover both  $\mathbf{s}_{i^*}$  and  $\mathbf{s}$ . Security instead relies on the secrecy of  $\mathbf{s}_i$  for an honest authority  $i$ , and the obstacle now is to simulate the secret keys  $\mathbf{U}_{\text{uid},i} = \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ & \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}$  which is correlated to (the

no longer secret)  $\mathbf{s}$  by the relation  $\underbrace{\mathbf{s}^\top \mathbf{A}_i}_{\text{masking}} \cdot \mathbf{U}_{\text{uid},i} \approx (\mathbf{0} \mid \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}})$  for any  $i$ . We obtain two strategies to tackle this issue, both having different trade-offs: One is relatively simple, but relies on a slightly stronger instance of evasive LWE, where the distribution of the preimages is Gaussian not only subject to image evaluation but has to satisfy additional constraints; Another one requires only a weaker evasive LWE instance, with preimages simply distributed Gaussian subject to image evaluation (without further constraints), but at the cost of more complicated simulation techniques and poorer asymptotic parameters. Below we only describe the first and simpler proof, which conceptually resembles the proof of Case 1. In this case, the adversary's input can be efficiently simulated given:

$$\begin{aligned} & (\mathbf{A}_i, \mathbf{B}_i)_{i \in [k] \setminus \mathcal{I}_{\text{corr}}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ \mathbf{U}_{\text{uid},i} = & \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ & \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}, \forall \text{uid} \in \mathcal{U}, i \in [k] \\ & (\underbrace{\mathbf{s}_i^\top \mathbf{A}_i}_{\text{masking}}, \underbrace{\mathbf{s}_i^\top \mathbf{Q}}_{\text{masking}})_{i \in [k] \setminus \mathcal{I}_{\text{corr}}}, \underbrace{\sum_{i \in [k] \setminus \mathcal{I}_{\text{corr}}} \mathbf{s}_i^\top \mathbf{P}}_{\text{masking}} \end{aligned}$$

To argue that the masking term is pseudorandom, we need to show that the terms in the last line above are pseudorandom. By (a stronger<sup>11</sup> instance of) the evasive LWE assumption, it suffices to argue that the terms below are pseudorandom:

$$(\underbrace{\mathbf{s}_i^\top \mathbf{P}\mathbf{k}_{\text{uid}}}_{\text{masking}}, \underbrace{\mathbf{s}_i^\top \mathbf{Q}\mathbf{K}_{\text{uid}}}_{\text{masking}})_{i \in \mathcal{I}_{\text{uid}} \setminus \mathcal{I}_{\text{corr}}, \text{uid} \in \mathcal{U}}, (\underbrace{\mathbf{s}_i^\top \mathbf{A}_i}_{\text{masking}}, \underbrace{\mathbf{s}_i^\top \mathbf{Q}}_{\text{masking}})_{i \in [k] \setminus \mathcal{I}_{\text{corr}}}, \underbrace{\sum_{i \in [k] \setminus \mathcal{I}_{\text{corr}}} \mathbf{s}_i^\top \mathbf{P}}_{\text{masking}}$$

Since  $\mathcal{I}_{\text{corr}} \neq [k]$ , there exists at least one honest  $i^* \in [k] \setminus \mathcal{I}_{\text{corr}}$ . For any uid, if  $i^* \notin \mathcal{I}_{\text{uid}}$ , note that the term  $\underbrace{\mathbf{s}_{i^*}^\top \mathbf{P}\mathbf{k}_{\text{uid}}}_{\text{masking}}$  is not available to the adversary. Otherwise, if  $i^* \in \mathcal{I}_{\text{uid}}$ , we observe the following identity expressing  $\mathbf{s}_{i^*}^\top \mathbf{P}\mathbf{k}_{\text{uid}}$  as a short linear combination of  $\sum_{i \in [k] \setminus \mathcal{I}_{\text{corr}}} \mathbf{s}_i^\top \mathbf{P}$  and  $(\mathbf{s}_i^\top \mathbf{P}\mathbf{k}_{\text{uid}})_i$  for  $i \in [k] \setminus \mathcal{I}_{\text{corr}}, i \neq i^*$ :

$$\mathbf{s}_{i^*}^\top \mathbf{P}\mathbf{k}_{\text{uid}} = (\sum_{i \in [k] \setminus \mathcal{I}_{\text{corr}}} \mathbf{s}_i^\top \mathbf{P})\mathbf{k}_{\text{uid}} - \sum_{i \in [k] \setminus \mathcal{I}_{\text{corr}}: i \neq i^*} \mathbf{s}_i^\top \mathbf{P}\mathbf{k}_{\text{uid}}$$

Similarly,  $(\underbrace{\mathbf{s}_i^\top \mathbf{Q}\mathbf{K}_{\text{uid}}}_{\text{masking}})_{\text{uid} \in \mathcal{U}}$  is simulatable by  $\underbrace{\mathbf{s}_i^\top \mathbf{Q}}_{\text{masking}}$  for all  $i \in [k] \setminus \mathcal{I}_{\text{corr}}$ . This means that, using noise flooding, it suffices to argue that the terms below are pseudorandom:

$$(\underbrace{\mathbf{s}_i^\top \mathbf{P}\mathbf{k}_{\text{uid}}}_{\text{masking}})_{i \in [k] \setminus \mathcal{I}_{\text{corr}}, \text{uid} \in \mathcal{U}: i \neq i^*}, (\underbrace{\mathbf{s}_i^\top \mathbf{A}_i}_{\text{masking}}, \underbrace{\mathbf{s}_i^\top \mathbf{Q}}_{\text{masking}})_{i \in [k] \setminus \mathcal{I}_{\text{corr}}}, \underbrace{\sum_{i \in [k] \setminus \mathcal{I}_{\text{corr}}} \mathbf{s}_i^\top \mathbf{P}}_{\text{masking}}$$

Notice that  $\mathbf{s}_{i^*}$  only appears in the first two terms above. By the LWE assumption, we have that  $\underbrace{\mathbf{s}_{i^*}^\top \mathbf{A}_{i^*}}_{\text{masking}}, \underbrace{\mathbf{s}_{i^*}^\top \mathbf{Q}}_{\text{masking}}$  and  $\underbrace{\mathbf{s}_{i^*}^\top \mathbf{P}}_{\text{masking}}$ , and hence also  $\underbrace{\sum_{i \in [k] \setminus \mathcal{I}_{\text{corr}}} \mathbf{s}_i^\top \mathbf{P}}_{\text{masking}}$ , are pseudorandom. We are left with

$$(\underbrace{\mathbf{s}_i^\top \mathbf{P}\mathbf{k}_{\text{uid}}}_{\text{masking}})_{i \in [k] \setminus \mathcal{I}_{\text{corr}}, \text{uid} \in \mathcal{U}: i \neq i^*}, (\underbrace{\mathbf{s}_i^\top \mathbf{A}_i}_{\text{masking}}, \underbrace{\mathbf{s}_i^\top \mathbf{Q}}_{\text{masking}})_{i \in [k] \setminus \mathcal{I}_{\text{corr}}: i \neq i^*}$$

which, upon noise flooding, are efficiently simulatable from  $\underbrace{\mathbf{s}_i^\top \mathbf{P}}_{\text{masking}}, \underbrace{\mathbf{s}_i^\top \mathbf{A}_i}_{\text{masking}}$  and  $\underbrace{\mathbf{s}_i^\top \mathbf{Q}}_{\text{masking}}$  for all  $i \in [k] \setminus \mathcal{I}_{\text{corr}} : i \neq i^*$ , which are in turn all pseudorandom under the (low-norm) LWE assumption. This concludes the analysis.

*Remark 1.* In Case 1 where no authority is corrupt, the term  $\mathbf{Q}\mathbf{K}_{\text{uid}}$  in the secret key together with  $\mathbf{c}_0$  in the ciphertext can be removed ( $\mathbf{Q}\mathbf{K}_{\text{uid}}$  replaced by  $\mathbf{0}$ ) without affecting correctness and security. In contrast, in Case 2 where at least one authority is corrupt, the scheme becomes insecure without these components, due to the following attack: The

<sup>11</sup>The evasive LWE instance is such that the distribution of a preimage  $\mathbf{U}_{\text{uid},i}$ , in addition to satisfying  $\mathbf{A}_i \cdot \mathbf{U}_{\text{uid},i} = (\mathbf{P}\mathbf{k}_{\text{uid}} \mid \mathbf{Q}\mathbf{K}_{\text{uid}})$ , satisfies also  $\mathbf{A}_i \cdot \mathbf{U}_{\text{uid},i} = (\mathbf{0} \mid \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}})$ . An alternative proof in Section A.2 lifts this additional constraint.



adversary uses  $\text{td}_{\mathbf{A}_{i^*}}$  of any corrupt  $i^*$  to recover  $\mathbf{s}_{i^*}$  and  $\mathbf{s}$ , which allows it to further recover  $\mathbf{s}_i^T \bar{\mathbf{A}}_i$  from  $(\mathbf{s}_i^T | \mathbf{s}^T) \mathbf{A}_i$  for all honest  $i \notin \mathcal{I}_{\text{corr}}$ . Now suppose  $\mathbf{QK}_{\text{uid}}$  is removed, so that  $\bar{\mathbf{A}}_i \cdot \mathbf{U}_{\text{uid},i} = (\mathbf{Pk}_{\text{uid}} | \mathbf{0})$ . By querying sufficiently many preimages for each honest  $i$ , the collection (over all uid) of the right parts of  $\mathbf{U}_{\text{uid},i}$  can be viewed as an Ajtai-trapdoor of  $\bar{\mathbf{A}}_i$ , thus allowing the adversary to further recover  $\mathbf{s}_i$  for all honest  $i$ .

In Section C we discuss stronger security notions in presence of corruption and why it is difficult to achieve.

## 2.6 Our MC-ABE

Equipped with all the above machinery, we combine the ideas in Boneh et al.'s KP-ABE and our MA-ABE into an MC-ABE.

**Construction.** Let  $H : \{0, 1\}^* \rightarrow \chi^m \times \chi^{m \times m\ell}$  be a random oracle for deriving common randomness for generating ciphertexts for a ciphertext identifier cid. Our construction can be summarised as follows:

- pp:  $\mathbf{B}_i \leftarrow_{\$} \mathbb{Z}_q^{n \times \ell m}$ ,  $i \in [k]$ ,  $\mathbf{P} \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$ ,  $\mathbf{Q} \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$ ,  $\mathbf{v} \leftarrow_{\$} \mathbb{Z}_q^n$ .
- apk:  $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n \times 2m}$ .
- epk <sub>$i$</sub> :  $\mathbf{C}_i \leftarrow_{\$} \mathbb{Z}_q^{n(m+1) \times 2m(m+1)}$ .
- sk <sub>$f$</sub> :  $\mathbf{u}_f \in \mathbb{Z}^{2m}$  where  $\mathbf{u}_f \leftarrow_{\$} (\mathbf{A} | \mathbf{B}_f)^{-1}(\mathbf{v})$ .
- ctxt<sub>1</sub>:  $(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_k, \hat{\mathbf{c}}, \mathbf{c}) \in \mathbb{Z}_q^{km+k(2m(m+1))+2m}$  where  $(\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}}) := H(\text{cid})$ ,
 
$$\hat{\mathbf{c}}^T = \mathbf{s}^T \cdot (\mathbf{A} \otimes \mathbf{k}_{\text{cid}}), \quad \mathbf{c}_0 = (\mathbf{s}_2^T | \dots | \mathbf{s}_k^T) \cdot (\mathbf{I}_{k-1} \otimes \mathbf{Q}),$$

$$\mathbf{c}_i^T = \mathbf{s}^T \cdot ((\mathbf{B}_1 - \mathbf{x}_{\text{cid},1}^T \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}}), \quad \mathbf{c}_i^T = (\mathbf{s}_i^T | \mathbf{s}^T) \cdot \mathbf{C}_i \quad \forall i \in [2, k],$$

$$\mathbf{c}^T = \sum_{i \in [2, k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T \cdot (\mathbf{v} \otimes \mathbf{I}_m) + \mu \mathbf{g}^T.$$
- ctxt <sub>$i$</sub>  for  $i > 1$ :  $\mathbf{U}_{\text{cid},i} \in \mathbb{Z}_q^{2m(m+1) \times (\ell m + 1)}$  where  $(\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}}) := H(\text{cid})$  and

$$\mathbf{U}_i \leftarrow_{\$} \mathbf{C}_i^{-1} \begin{pmatrix} \mathbf{Pk}_{\text{cid}} & \mathbf{QK}_{\text{cid}} \\ (\mathbf{B}_i - \mathbf{x}_i^T \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}} \end{pmatrix}$$

The decryptor computes, for all  $i \in [2, k]$ ,  $\mathbf{c}_i^T \mathbf{U}_{\text{cid},i}$  to obtain

$$\underbrace{\mathbf{s}_i^T \mathbf{Pk}_{\text{cid}}}_{\text{Term 1}} \quad \text{and} \quad \underbrace{\mathbf{s}_i^T \mathbf{QK}_{\text{cid}} + \mathbf{s}^T \cdot ((\mathbf{B}_i - \mathbf{x}_{\text{cid},i}^T \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}})}_{\text{Term 2}}.$$

Summing the first term for all  $i \in [2, k]$  gives  $\sum_{i \in [2, k]} \mathbf{s}_i^T \mathbf{Pk}_{\text{cid}}$ , and subtracting the second term from  $\mathbf{s}_i^T \mathbf{Q} \cdot \mathbf{K}_{\text{cid}}$  (where  $\mathbf{s}_i^T \mathbf{Q}$  is the  $i$ -th chunk of  $\mathbf{c}_0^T$ ) gives  $\mathbf{s}^T \cdot ((\mathbf{B}_i - \mathbf{x}_{\text{cid},i}^T \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}})$ .

Then, concatenating the latter for all  $i \in [2, k]$  together with  $\mathbf{c}_1$ , the decryptor recovers  $\mathbf{s}^T \cdot (\mathbf{B}_f \otimes \mathbf{k}_{\text{cid}})$  using homomorphic computation assuming  $f(\mathbf{x}_{\text{cid},1}, \dots, \mathbf{x}_{\text{cid},k}) = 0$ .

Concatenating  $\hat{\mathbf{c}}^T$  and  $\mathbf{s}^T \cdot (\mathbf{B}_f \otimes \mathbf{k}_{\text{cid}})$  yields  $\mathbf{s}^T \cdot ((\mathbf{A} | \mathbf{B}_f) \otimes \mathbf{k}_{\text{cid}})$  to which the decryptor multiplies  $\mathbf{u}_f$  which yields  $\mathbf{s}^T \cdot (\mathbf{v} \otimes \mathbf{k}_{\text{cid}})$ . Finally, linearly combining the above intermediate results with  $\mathbf{c}^T \mathbf{k}_{\text{cid}}$  yields a short element if  $\mu = 0$ , and a random-looking (hence long) element if  $\mu = 1$ .

**Security Analysis.** We sketch a proof that the above scheme is very-selective secure under the evasive LWE and tensor LWE assumptions. We use the shorthand  $\hat{\mathbf{B}}_{\text{cid},i} := \mathbf{B}_i - \mathbf{x}_{\text{cid},i}^T \otimes \mathbf{G}$ .

The adversary specifies the following information: (i)  $\mathcal{J}_{\text{corr}} \subset [2, k]$  the set of corrupt encryptors, (ii)  $\mathcal{F}$  the set of functions for which the adversary requests a secret key, (iii)  $\text{cid}^*$  the identifier of the challenge ciphertext, (iv)  $\mathbf{x}_{\text{cid}^*,1}$  the first attribute associated to the challenge ciphertext, and (v)  $Q$  the set of  $(\text{cid}, i)$  tuples for which the adversary requests a ciphertext from encryptor  $i > 1$  for ciphertext identifier  $\text{cid}$  associated to attribute  $\mathbf{x}_{\text{cid},i}$ . We write  $\mathcal{C}$  for the set of all  $\text{cid}$  appearing in  $Q$  and, for each  $\text{cid} \in \mathcal{C}$ ,  $\mathcal{J}_{\text{cid}} \subseteq [2, k]$  for the set of encryptors from whom the adversary requests a ciphertext for ciphertext identifier  $\text{cid}$ . In return, the adversary receives the following:

- Public information:  $\mathbf{A}, (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v}$
- Trapdoors for corrupt encryptors:  $(\text{td}_{\mathbf{C}_j})_{j \in \mathcal{J}_{\text{corr}}}$
- Policy secret keys:  $((\mathbf{A} \mid \mathbf{B}_f)^{-1}(\mathbf{v}))_{f \in \mathcal{F}}$
- Challenge ciphertext:

$$\begin{aligned} & \underbrace{\mathbf{s}^T \cdot (\mathbf{A} \otimes \mathbf{k}_{\text{cid}^*})}, & \underbrace{(\mathbf{s}_2^T \mid \dots \mid \mathbf{s}_k^T) \cdot (\mathbf{I}_{k-1} \otimes \mathbf{Q})}, & \underbrace{\mathbf{s}^T \cdot (\hat{\mathbf{B}}_{\text{cid}^*,1} \otimes \mathbf{k}_{\text{cid}^*}),} \\ & \underbrace{((\mathbf{s}_i^T \mid \mathbf{s}^T) \cdot \mathbf{C}_i)_{i \in [2,k]},} & \underbrace{\sum_{i \in [2,k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T \cdot (\mathbf{v} \otimes \mathbf{I}_m) + \mu \mathbf{g}^T} \end{aligned}$$

- Other ciphertexts:  $\mathbf{C}_i^{-1} \left( \begin{array}{c} \mathbf{P} \mathbf{k}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{array} \right), \forall (\text{cid}, i) \in Q$

We want to show that the term masking  $\mu$  in the challenge ciphertext is pseudorandom in the view of the adversary. Again, we distinguish between two cases:

**Case 1.**  $\mathcal{J}_{\text{corr}} = \emptyset$ , i.e. all encryptors are honest<sup>12</sup>,  $Q = [2, k] \times \mathcal{C}$ , and  $f((\mathbf{x}_{\text{cid}^*,i})_{i \in [k]}) = 1$  for all  $f \in \mathcal{F}$ .<sup>13</sup>

**Case 2.**  $\mathcal{J}_{\text{corr}} \neq \emptyset$ , i.e. some encryptors are corrupt, and  $\mathcal{J}_{\text{cid}^*} \cup \mathcal{J}_{\text{corr}} \neq [2, k]$ , i.e. there exists at least one honest encryptor  $j \in [2, k] \setminus \mathcal{J}_{\text{corr}}$  from whom the adversary receives no ciphertext for ciphertext identifier  $\text{cid}^*$ . The discussion in Section C applies also here.

Case 1. As in the security proof of Boneh et al.'s KP-ABE, a crucial step in this analysis is to simulate  $\mathbf{B} = (\mathbf{B}_1 \mid \dots \mid \mathbf{B}_k)$  as  $\mathbf{B} := \mathbf{A} \mathbf{R} + \mathbf{x}_{\text{cid}^*}^T \otimes \mathbf{G}$ , where  $\mathbf{x}_{\text{cid}^*}^T := (\mathbf{x}_{\text{cid}^*,1}^T \mid \dots \mid \mathbf{x}_{\text{cid}^*,k}^T)$  and  $\mathbf{R} \leftarrow_{\$} \chi^{2m \times k \ell m}$ , which by the leftover hash lemma is statistically close to a uniformly random  $\mathbf{B}$ . This alternative way of generating  $\mathbf{B}$  then allows to derive a gadget trapdoor [MP12]  $\mathbf{RH}_{\mathbf{B},f,\mathbf{x}_{\text{cid}^*}}$  for  $(\mathbf{A} \mid \mathbf{B}_f) = (\mathbf{A} \mid \mathbf{A} \mathbf{R} \mathbf{H}_{\mathbf{B},f,\mathbf{x}_{\text{cid}^*}} + \mathbf{G})$  using which the reduction can answer to any key query for  $f$  with  $f(\mathbf{x}_{\text{cid}^*}) = 1$ , without knowing any trapdoor for  $\mathbf{A}$ .

Another non-trivial step is that, to simulate the adversary's input, we further assume that the simulator is given  $\underbrace{\mathbf{s}^T (\mathbf{A} \otimes \mathbf{k}_{\text{cid}})}$  and  $\underbrace{\mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}^*,1} \otimes \mathbf{k}_{\text{cid}})}$  for all  $\text{cid} \in \mathcal{C}$  instead of only for  $\text{cid} = \text{cid}^*$ .

<sup>12</sup>In the formal definition, we allow encryptors not specified in the challenge ciphertext to be corrupt.

<sup>13</sup>We again assumed without loss of generality, with the same argument as in the analysis of our MA-ABE scheme, that  $\mathcal{J}_{\text{cid}} = [2, k]$  for all  $\text{cid}$ , i.e. the adversary requests ciphertexts for every  $\text{cid}$  from every encryptor  $i > 1$ .

With the above simulation strategy, the adversary's input can be efficiently simulated given the following information:

$$\begin{aligned} & \mathbf{A}, \mathbf{R}, (\mathbf{C}_i)_{i \in [2, k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v}, \\ & \mathbf{C}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ & \hat{\mathbf{B}}_{\text{cid}, i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix}, \forall i \in [2, k], \text{cid} \in \mathcal{C}, \\ & (\mathbf{s}^T \cdot (\mathbf{A} \otimes \mathbf{k}_{\text{cid}}))_{\text{cid} \in \mathcal{C}}, (\mathbf{s}^T \cdot (\hat{\mathbf{B}}_{\text{cid}^*, 1} \otimes \mathbf{k}_{\text{cid}}))_{\text{cid} \in \mathcal{C}}, \\ & ((\mathbf{s}_i^T \mid \mathbf{s}^T) \cdot \mathbf{C}_i)_{i \in [2, k]}, \sum_{i \in [2, k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T \cdot (\mathbf{v} \otimes \mathbf{I}_m) \end{aligned}$$

To argue that the masking term is pseudorandom, it suffices to argue that the terms in the last two lines above are pseudorandom. From here onwards, the analysis is almost identical to that of Case 1 of our MA-ABE scheme, with the main difference being that we also need to take care of the additional terms  $(\mathbf{s}^T (\mathbf{A} \otimes \mathbf{k}_{\text{cid}}))_{\text{cid} \in \mathcal{C}}$ , but which is easily handled by the tensor LWE assumption. We leave out the rest in this overview.

**Case 2.** The proof for Case 2 is almost identical to that for the MA-ABE scheme, with the main difference being  $\mathcal{J}_{\text{cid}} \subseteq [2, k]$  instead of  $\mathcal{I}_{\text{uid}} \subseteq [k]$ , which we omit from this overview.

### 3 Preliminaries

Let  $\lambda \in \mathbb{N}$  denote the security parameter, and  $\text{poly}(\lambda)$  and  $\text{negl}(\lambda)$  the set of all polynomials and negligible functions in  $\lambda$ , respectively. For  $k, n \in \mathbb{N}$ ,  $k \leq n$ , we write  $[n]$  for  $\{1, \dots, n\}$  and  $[k, n]$  for  $\{k, \dots, n\}$ . If  $S$  is a set, we write  $x \leftarrow S$  for sampling a uniformly random element from  $S$ . If  $\mathcal{D}$  is a distribution over  $S$ , denoted as  $\mathcal{D} \sim S$ , we write  $x \leftarrow \mathcal{D}$  for sampling a random element from  $S$  according to the distribution  $\mathcal{D}$ .

We use bold capital and lower-case letters, e.g.  $\mathbf{A}$  and  $\mathbf{b}$ , to denote matrices and vectors, respectively. We write  $\cdot$  for the usual matrix product, which is sometimes omitted, and  $\otimes$  for the tensor (i.e. Kronecker) product of matrices. The matrix tensor product satisfies the mixed product property: For all matrices  $\mathbf{A}$ ,  $\mathbf{B}$ ,  $\mathbf{C}$  and  $\mathbf{D}$  of suitable dimensions, we have  $(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = \mathbf{AC} \otimes \mathbf{BD}$ . For  $\mathbf{x} \in \mathbb{Z}^n$ , write  $\|\mathbf{x}\| = \max_{i=1}^n |x_i|$  for the  $\ell_\infty$ -norm of  $\mathbf{x}$ .

#### 3.1 Discrete Gaussians

We denote by  $\mathcal{D}_{\Lambda, \chi, \mathbf{c}}$  the discrete Gaussian distribution over a lattice  $\Lambda$  with parameter  $\chi$  and center  $\mathbf{c}$ , i.e. the distribution over  $\Lambda$  where for all  $\mathbf{x}$ , it holds  $\mathcal{D}_{\Lambda, \chi, \mathbf{c}}(\mathbf{x}) \propto \exp(-\pi \sum_{i \in [m]} (x_i - c_i)^2 / \chi^2)$ . If  $\mathbf{c} = \mathbf{0}$ , it is omitted from the subscripts. With an abuse of notation, we will also denote by  $\chi^m$  the zero-centered discrete Gaussian distribution over  $\Lambda = \mathbb{Z}^m$  with parameter  $\chi$ , i.e.  $\mathcal{D}_{\mathbb{Z}^m, \chi}$ .

**Lemma 1** (Derived from [MP12, Section 2.4]). *For any  $m \in \mathbb{N}$ ,  $k > 0$ ,*

$$\Pr[\|\mathbf{x}\| > k\chi \mid \mathbf{x} \leftarrow \chi^m] < 2m \exp(-\pi k^2).$$

*In particular, for  $m = \text{poly}(\lambda)$ , it holds that*

$$\Pr[\|\mathbf{x}\| > \lambda\chi \mid \mathbf{x} \leftarrow \chi^m] = \text{negl}(\lambda).$$

**Lemma 2** (Noise Flooding). *Let  $\Lambda$  be an  $n$ -dimensional lattice. For any real  $\chi > \omega(\sqrt{\log n})$ , and any  $\mathbf{c} \in \mathbb{R}^n$ , it holds  $\text{SD}(\mathcal{D}_{\Lambda, \chi}, \mathcal{D}_{\Lambda, \chi, \mathbf{c}}) \leq \|\mathbf{c}\|/\chi$ . In particular, if  $\chi \geq \lambda^{\omega(1)} \cdot \|\mathbf{c}\|$ , one has  $\mathcal{D}_{\Lambda, \chi} \approx_s \mathcal{D}_{\Lambda, \chi, \mathbf{c}}$ .*

**Lemma 3** (Extended Leftover Hash Lemma [DRS04, ABB10]). *Suppose that  $m > (n + 1) \log q + \omega(\log n)$  and that  $q > 2$  is prime. Let  $\mathbf{R}$  be an  $m \times k$  matrix chosen uniformly*

in  $\{-1, 1\}^{m \times k}$  where  $k = k(n)$  is polynomial in  $n$ . Let  $\mathbf{A}$  and  $\mathbf{B}$  be matrices chosen uniformly in  $\mathbb{Z}_q^{n \times m}$  and  $\mathbb{Z}_q^{n \times k}$  respectively. Then, for all vectors  $\mathbf{w} \in \mathbb{Z}_q^m$ , the distribution  $(\mathbf{A}, \mathbf{A}\mathbf{R}, \mathbf{R}^T\mathbf{w})$  is statistically close to the distribution  $(\mathbf{A}, \mathbf{B}, \mathbf{R}^T\mathbf{w})$ .

**Lemma 4** ([GPV08]). *Let  $n$  and  $q$  be positive integers with  $q$  prime, and let  $m \geq 2n \log q$ . Then for all but a  $2q^{-n}$  fraction of all  $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$  and for any  $s \geq \omega(\sqrt{\log m})$ , the distribution of the syndrome  $\mathbf{u} = \mathbf{A}\mathbf{e} \bmod q$  is statistically close to uniform over  $\mathbb{Z}_q^n$ , where  $\mathbf{e} \sim \mathcal{D}_{\mathbb{Z}^m, s}$ .*

### 3.2 Homomorphic Computation.

We recall the basics of homomorphic computation [GSW13, BGG<sup>+</sup>14]. There exist deterministic polynomial-time algorithms  $\text{EvalF}$  and  $\text{EvalFX}$  which do the following. For  $n, q, \ell \in \mathbb{N}$ ,  $m = n \lceil \log q \rceil$ ,  $\mathbf{g}^T := (1, 2, \dots, 2^{\lceil \log q \rceil - 1})$ , and  $\mathbf{G} := \mathbf{I}_n \otimes \mathbf{g}^T$ , there exists  $\beta \leq (n \log q)^{O(d)}$ , such that for any matrix  $\mathbf{B} = (\mathbf{B}_1, \dots, \mathbf{B}_\ell) \in (\mathbb{Z}^{n \times m})^\ell$ , depth- $d$  Boolean circuit  $f : \{0, 1\}^\ell \rightarrow \{0, 1\}$ , and input  $\mathbf{x} \in \{0, 1\}^\ell$ , the matrices

$$\mathbf{H}_{\mathbf{B}, f} = \text{EvalF}(\mathbf{B}, f) \in \mathbb{Z}^{\ell m \times m}, \quad \mathbf{H}_{\mathbf{B}, f, \mathbf{x}} = \text{EvalFX}(\mathbf{B}, f, \mathbf{x}) \in \mathbb{Z}^{\ell m \times m},$$

satisfy

$$\|\mathbf{H}_{\mathbf{B}, f, \mathbf{x}}\| \leq \beta, \quad (\mathbf{B} - \mathbf{x}^T \otimes \mathbf{G})\mathbf{H}_{\mathbf{B}, f, \mathbf{x}} = \mathbf{B}_f - f(\mathbf{x})\mathbf{G} \bmod q,$$

where  $\mathbf{B}_f := \mathbf{B}\mathbf{H}_{\mathbf{B}, f} \bmod q$ .

### 3.3 Lattice Trapdoors

There exist PPT algorithms  $(\text{TrapGen}, \text{SampPre})$ , such that for appropriately chosen  $n, q, \chi$  parametrised by  $\lambda$ , with  $\chi \geq O(\sqrt{n} \cdot \log q \cdot \log n)$ , the following properties are satisfied [GPV08, MP12, GM18]:

- $(\mathbf{D}, \mathbf{R}) \leftarrow \text{TrapGen}(1^n, q)$  generates a matrix  $\mathbf{D} \in \mathbb{Z}_q^{n \times h}$ , where  $h = 2n \lceil \log q \rceil$ , and a trapdoor  $\mathbf{R} \in \mathbb{Z}^{h \times n \lceil \log q \rceil}$  such that  $\mathbf{D}\mathbf{R} = \mathbf{G} \bmod q$ . The distribution of  $\mathbf{D}$  is statistically close to the uniform distribution over  $\mathbb{Z}_q^{n \times h}$ .
- $\mathbf{u} \leftarrow \text{SampPre}(\mathbf{D}, \mathbf{R}, \mathbf{v}, \chi)$  inputs a target vector  $\mathbf{v} \in \mathbb{Z}_q^n$  and a Gaussian parameter  $\chi$ , and samples a vector  $\mathbf{u} \in \mathbb{Z}^h$ . For any  $\mathbf{D} \in \mathbb{Z}_q^{n \times h}$ ,  $\mathbf{R} \in \mathbb{Z}^{h \times n \lceil \log q \rceil}$  such that  $\mathbf{D}\mathbf{R} = \mathbf{G} \bmod q$  and  $5(s_1(\mathbf{R})^2 + 1) \leq \chi^2$  where  $s_1(\mathbf{R})$  is the maximal singular value of  $\mathbf{R}$  (e.g. when  $(\mathbf{D}, \mathbf{R})$  is output of  $\text{TrapGen}(1^n, q)$ ), it is guaranteed that  $\mathbf{D}\mathbf{u} = \mathbf{v} \bmod q$  and  $\|\mathbf{u}\| \leq \lambda\chi$  with overwhelming probability. Furthermore, for any  $\mathbf{v} \in \mathbb{Z}_q^n$ , the following distributions are statistically close:

$$\left\{ (\mathbf{D}, \mathbf{u}) \left| \begin{array}{l} (\mathbf{D}, \mathbf{R}) \leftarrow \text{TrapGen}(1^n, q) \\ \mathbf{u} \leftarrow \text{SampPre}(\mathbf{D}, \mathbf{R}, \mathbf{v}, \chi) \end{array} \right. \right\} \approx \left\{ (\mathbf{D}, \mathbf{u}) \left| \begin{array}{l} (\mathbf{D}, \mathbf{R}) \leftarrow \text{TrapGen}(1^n, q) \\ \mathbf{u} \leftarrow \mathcal{S} \chi^m : \mathbf{D}\mathbf{u} = \mathbf{v} \bmod q \end{array} \right. \right\}.$$

### 3.4 Lattice Assumptions

**Definition 1** ( $\text{LWE}_{k, n, m, q, \chi, \phi}$  assumption). Let  $k, n, m, q, \chi, \phi$  be parametrised by  $\lambda$ . The (decision)  $\text{LWE}_{k, n, m, q, \chi, \phi}$  assumption, with  $k$  suppressed if  $k = 1$  and  $\phi$  suppressed if it is the uniform distribution over  $\mathbb{Z}_q$ , states that for any PPT adversary  $\mathcal{A}$  it holds that

$$\left| \Pr \left[ b = 1 \left| \begin{array}{l} \mathbf{A} \leftarrow \mathcal{S} \phi^{n \times m} \\ \mathbf{S} \leftarrow \mathcal{S} \mathbb{Z}_q^{k \times n}, \mathbf{E} \leftarrow \mathcal{S} \chi^{k \times m} \\ \mathbf{B} := \mathbf{S}\mathbf{A} + \mathbf{E} \bmod q \\ b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{B}) \end{array} \right. \right] - \Pr \left[ b = 1 \left| \begin{array}{l} \mathbf{A} \leftarrow \mathcal{S} \phi^{n \times m} \\ \mathbf{B} \leftarrow \mathcal{S} \mathbb{Z}_q^{k \times m} \\ b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{B}) \end{array} \right. \right] \right| \leq \text{negl}(\lambda).$$

ExpTensorLWE $_{\mathcal{A}}^0(1^\lambda)$	ExpTensorLWE $_{\mathcal{A}}^1(1^\lambda)$
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times \ell m}, \mathbf{s} \leftarrow \mathbb{Z}_q^{mn}$	$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times \ell m}$
$\mathbf{e}_i \leftarrow \chi_0^{\ell m}, \mathbf{r}_i \leftarrow \chi_1^m \quad \forall i \in [Q]$	$\mathbf{r}_i \leftarrow \chi_1^m \quad \forall i \in [Q]$
$\mathbf{b}_i^\top := \mathbf{s}^\top ((\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{G}) \otimes \mathbf{r}_i) + \mathbf{e}_i^\top \pmod q \quad \forall i \in [Q]$	$\mathbf{b}_i \leftarrow \mathbb{Z}_q^{\ell m} \quad \forall i \in [Q]$
<b>return</b> $\mathcal{A}(\mathbf{A}, (\mathbf{b}_i, \mathbf{x}_i, \mathbf{r}_i)_{i \in [Q]})$	<b>return</b> $\mathcal{A}(\mathbf{A}, (\mathbf{b}_i, \mathbf{x}_i, \mathbf{r}_i)_{i \in [Q]})$

**Figure 2:** Experiments for tensor LWE.

The LWE problem with  $\phi$  being uniformly over  $\{0, 1\}$  or the Gaussian distribution  $\mathcal{D}_{\mathbb{Z}^m, \cdot}$  has been shown to be as hard as the uniform LWE problem [BLMR13].

Below we state the tensor LWE assumption as in [Wee22], and define a version of public-coin evasive LWE assumption closely following [Wee22, WWW22].

**Definition 2** (TensorLWE $_{n,m,q,\chi_0,\chi_1,\ell,\mathcal{Q}}$  assumption). Let the parameters  $n, m, q, \chi_0, \chi_1, \ell, \mathcal{Q}$  be parametrised by  $\lambda$ , where the set  $\mathcal{Q}$  contain  $\mathbf{x}_1, \dots, \mathbf{x}_Q \in \{0, 1\}^\ell$ , where  $|\mathcal{Q}| = Q \in \text{poly}(\lambda)$ . The TensorLWE $_{n,m,q,\chi_0,\chi_1,\ell,\mathcal{Q}}$  assumption states that for any PPT adversary  $\mathcal{A}$  it holds that

$$|\Pr[\text{ExpTensorLWE}_{\mathcal{A}}^0(1^\lambda) = 1] - \Pr[\text{ExpTensorLWE}_{\mathcal{A}}^1(1^\lambda) = 1]| \leq \text{negl}(\lambda)$$

where  $\text{ExpTensorLWE}_{\mathcal{A}}^b$  is defined in Fig. 2.

The tensor LWE assumption has been heuristically justified by that, if the LWE matrices  $(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{G})$  were low-norm<sup>14</sup>, then it could be proven from the standard LWE assumption. We refer to [Wee22] for the details.

**Definition 3** (Public-coin EvasiveLWE assumption). Let the parameters  $\text{param} = (q, k, n, m, n_0, m_0, \mathcal{S}, \chi, (p_i, \chi_i, \psi_i, \sigma_i)_{i \in [k]})$  be parametrised by  $\lambda$ , where  $\mathcal{S} \sim (\mathbb{Z}_q^n)^k \times \mathbb{Z}_q^{n_0}$ ,  $\chi \sim \mathbb{Z}, \chi_i \sim \mathbb{Z}, \psi_i \sim \mathbb{Z}$  are distributions. Let  $\text{Samp}$  be a PPT algorithm which, on input  $1^\lambda$ , outputs

$$(\tilde{\mathbf{A}} \in \mathbb{Z}_q^{n_0 \times m_0}, (\tilde{\mathbf{P}}_i \in \mathbb{Z}_q^{n \times p_i})_{i \in [k]}, \text{aux} \in \{0, 1\}^*)$$

with  $\text{aux}$  containing all coin tosses used by  $\text{Samp}$ . Denote

$$\begin{aligned} \text{Adv}_{\mathcal{A}}^{\text{Pre}}(\lambda) &:= |\Pr[\text{Pre}_{\mathcal{A}}^0(1^\lambda) = 1] - \Pr[\text{Pre}_{\mathcal{A}}^1(1^\lambda) = 1]|, \\ \text{Adv}_{\mathcal{B}}^{\text{Post}}(\lambda) &:= |\Pr[\text{Post}_{\mathcal{B}}^0(1^\lambda) = 1] - \Pr[\text{Post}_{\mathcal{B}}^1(1^\lambda) = 1]|, \end{aligned}$$

where the experiments  $\text{Pre}_{\mathcal{A}}^b$  and  $\text{Post}_{\mathcal{B}}^b$  are defined in Fig. 3. The EvasiveLWE $_{\text{param}}$  assumption states that for any PPT  $\text{Samp}$  and  $\mathcal{B}$  there exists a PPT  $\mathcal{A}$  such that  $\text{Adv}_{\mathcal{A}}^{\text{Pre}}(\lambda) \geq \text{Adv}_{\mathcal{B}}^{\text{Post}}(\lambda)/\text{poly}(\lambda) - \text{negl}(\lambda)$ .

In words, the evasive LWE assumption says that, if LWE w.r.t. the matrices  $\tilde{\mathbf{A}}, \tilde{\mathbf{B}}_i, \tilde{\mathbf{P}}_i$  jointly is hard, then LWE w.r.t. the matrices  $\tilde{\mathbf{A}}, \tilde{\mathbf{B}}_i$  jointly is also hard even when given short preimages  $\tilde{\mathbf{B}}_i^{-1}(\tilde{\mathbf{P}}_i)$  as hints. Behind is the intuition that, there seems no alternative meaningful use of  $\tilde{\mathbf{B}}_i^{-1}(\tilde{\mathbf{P}}_i)$  other than multiplying which to  $\tilde{\mathbf{B}}_i$  to obtain further LWE samples w.r.t.  $\tilde{\mathbf{P}}_i$ . Variants similar to Definition 3 have been studied in the recent work of [BUW24] in form of the wider class of public-coin evasive LWE assumptions. Looking ahead, in the security proofs of our MA- and MC-ABE constructions in Sections 6 and 7, we will make use of the assumption with the following secret distributions  $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2$ :

<sup>14</sup>Although this cannot be true with  $\mathbf{G}$  which is not low-norm.

$\text{Pre}_{\mathcal{A}}^b(1^\lambda)$	$\text{Post}_{\mathcal{B}}^b(1^\lambda)$
$(\tilde{\mathbf{A}}, (\tilde{\mathbf{P}}_i)_{i \in [k]}, \text{aux}) \leftarrow \text{Samp}(1^\lambda)$ $\tilde{\mathbf{B}}_i \leftarrow \mathbb{Z}_q^{n \times m}, \forall i \in [k]$ <b>if</b> $b = 0$ <b>then</b> $((\tilde{\mathbf{s}}_i)_{i \in [k]}, \tilde{\mathbf{s}}) \leftarrow \mathcal{S}$ $\mathbf{e}_0 \leftarrow \mathcal{X}^{m_0}; \quad \mathbf{e}_i \leftarrow \mathcal{X}_i^m, \quad \mathbf{f}_i \leftarrow \mathcal{P}_i^{p_i}, \forall i \in [k]$ $\mathbf{c}_0^\top := \tilde{\mathbf{s}}^\top \tilde{\mathbf{A}} + \mathbf{e}_0^\top \text{ mod } q$ $\mathbf{d}_i^\top := \tilde{\mathbf{s}}_i^\top \tilde{\mathbf{B}}_i + \mathbf{e}_i^\top \text{ mod } q, \forall i \in [k]$ $\mathbf{q}_i^\top := \tilde{\mathbf{s}}_i^\top \tilde{\mathbf{P}}_i + \mathbf{f}_i^\top \text{ mod } q, \forall i \in [k]$ <b>if</b> $b = 1$ <b>then</b> $\mathbf{c}_0 \leftarrow \mathcal{Z}_q^{m_0}; \quad \mathbf{d}_i \leftarrow \mathcal{Z}_q^m, \forall i \in [k]$ $\mathbf{q}_i \leftarrow \mathcal{Z}_q^{p_i}, \forall i \in [k]$ <b>return</b> $\mathcal{A} \left( \begin{array}{c} \tilde{\mathbf{A}}, \quad (\tilde{\mathbf{B}}_i)_{i \in [k]}, \quad (\tilde{\mathbf{P}}_i)_{i \in [k]}, \quad \text{aux} \\ \mathbf{c}_0, \quad (\mathbf{d}_i)_{i \in [k]}, \quad (\mathbf{q}_i)_{i \in [k]} \end{array} \right)$	$(\tilde{\mathbf{A}}, (\tilde{\mathbf{P}}_i)_{i \in [k]}, \text{aux}) \leftarrow \text{Samp}(1^\lambda)$ $\tilde{\mathbf{B}}_i \leftarrow \mathbb{Z}_q^{n \times m}, \forall i \in [k]$ <b>if</b> $b = 0$ <b>then</b> $((\tilde{\mathbf{s}}_i)_{i \in [k]}, \tilde{\mathbf{s}}) \leftarrow \mathcal{S}$ $\mathbf{e}_0 \leftarrow \mathcal{X}^{m_0}; \quad \mathbf{e}_i \leftarrow \mathcal{X}_i^m, \forall i \in [k]$ $\mathbf{c}_0^\top := \tilde{\mathbf{s}}^\top \tilde{\mathbf{A}} + \mathbf{e}_0^\top \text{ mod } q$ $\mathbf{d}_i^\top := \tilde{\mathbf{s}}_i^\top \tilde{\mathbf{B}}_i + \mathbf{e}_i^\top \text{ mod } q, \forall i \in [k]$ $\mathbf{U}_i \leftarrow \mathcal{D}_{\mathbb{Z}, \sigma_i}^{m \times p_i} : \tilde{\mathbf{B}}_i \mathbf{U}_i = \tilde{\mathbf{P}}_i \text{ mod } q, \forall i \in [k]$ <b>if</b> $b = 1$ <b>then</b> $\mathbf{c}_0 \leftarrow \mathcal{Z}_q^{m_0}; \quad \mathbf{d}_i \leftarrow \mathcal{Z}_q^m, \forall i \in [k]$ $\mathbf{U}_i \leftarrow \mathcal{D}_{\mathbb{Z}, \sigma_i}^{m \times p_i} : \tilde{\mathbf{B}}_i \mathbf{U}_i = \tilde{\mathbf{P}}_i \text{ mod } q, \forall i \in [k]$ <b>return</b> $\mathcal{B} \left( \begin{array}{c} \tilde{\mathbf{A}}, \quad (\tilde{\mathbf{B}}_i)_{i \in [k]}, \quad (\tilde{\mathbf{P}}_i)_{i \in [k]}, \quad \text{aux} \\ \mathbf{c}_0, \quad (\mathbf{d}_i)_{i \in [k]}, \quad (\mathbf{U}_i)_{i \in [k]} \end{array} \right)$

**Figure 3:** Experiments Pre and Post for evasive LWE.

- In the non-corrupt setting (Case 1 in Section 2), we let  $\tilde{\mathbf{s}}_i^\top = (\mathbf{s}_i^\top, \mathbf{s}^\top)$  for each  $i \in [k]$ , and  $\tilde{\mathbf{s}}^\top = (\mathbf{s}_1^\top, \dots, \mathbf{s}_k^\top, \mathbf{s}^\top)$  where  $\mathbf{s}_i$ 's and  $\mathbf{s}$  are the uniformly random LWE secrets in the constructions. We call this distribution  $\mathcal{S}_0$ . This closely resembles the evasive LWE of [WWW22], which also consists of  $\tilde{\mathbf{B}}_i, \tilde{\mathbf{P}}_i$  and  $\mathbf{U}_i$  for multiple  $i$ 's, with the only differences being the precise LWE secret and error distributions.<sup>15</sup>
- In the corrupt setting (Case 2 in Section 2), we let  $\tilde{\mathbf{s}}_i^\top = (\mathbf{s}_i^\top, \mathbf{0}^\top)$  for each non-corrupt index  $i \notin \mathcal{I}$ , and  $\tilde{\mathbf{s}}^\top = (\dots, \mathbf{s}_i^\top, \dots)_{i \notin \mathcal{I}}$ . We call this distribution  $\mathcal{S}_1$ .
- We also provide an alternative (and more complicated) proof our MA-ABE in the corrupt setting in Section A.2, where we let  $\tilde{\mathbf{s}}_i^\top = \mathbf{s}_i^\top$  for each non-corrupt index  $i \notin \mathcal{I}$ , and again  $\tilde{\mathbf{s}}^\top = (\dots, \mathbf{s}_i^\top, \dots)_{i \notin \mathcal{I}}$ . We call this distribution  $\mathcal{S}_2$ . This version is essentially identical to that of [WWW22], up to error distributions.

We refer to Section 1.4 for a short discussion on public- vs. private-coin evasive LWE, and to [BUW24] for more details on existing evasive LWEs, their similarity and differences, and known counterexamples against certain private-coin variants (not applicable to the public-coin setting).

## 4 Multi-Authority/Client Attribute-based Encryption

We recall the definition of multi-authority attribute-based encryption (MA-ABE) in our notation, and formally define multi-client attribute-based encryption (MC-ABE).

**MA-ABE** Let  $\mathcal{X}$ ,  $\mathcal{F}$ , and  $\mathcal{M}$  denote the attribute space, the policy space over  $\mathcal{X}^k$ , and the message space respectively for some  $k \in \mathbb{N}$ . An MA-ABE consists of PPT algorithms (Setup, AuthSetup, KGen, Enc, Dec) with the following syntax:

- $\text{pp} \leftarrow \text{Setup}(1^\lambda)$ : The setup algorithm generates the public parameters  $\text{pp}$ .

<sup>15</sup>In [WWW22], the LWE secrets of  $\tilde{\mathbf{B}}_i$  and  $\tilde{\mathbf{A}}$  are  $\mathbf{s}_i^\top$  and  $(\mathbf{s}_1^\top, \dots, \mathbf{s}_k^\top)$  respectively, and each of the error vectors  $\mathbf{e}_i, \mathbf{f}_i$  is restricted to have identical width for all entries.



- $(\text{apk}, \text{ask}) \leftarrow \text{AuthSetup}(\text{pp})$ : The authority setup algorithm generates a pair of authority public key  $\text{apk}$  and secret key  $\text{ask}$  for an authority.
- $\text{sk} \leftarrow \text{KGen}(\text{pp}, \text{apk}, \text{ask}, \text{uid}, \mathbf{x})$ : The key generation algorithm generates a secret key  $\text{sk}$  given a pair of authority public key  $\text{apk}$  and secret key  $\text{ask}$ , a user identity  $\text{uid} \in \{0, 1\}^*$  and an attribute  $\mathbf{x} \in \mathcal{X}$ .
- $\text{ctxt} \leftarrow \text{Enc}(\text{pp}, (\text{apk}_i)_{i \in [k]}, f, \mu)$ : The encryption algorithm encrypts a message  $\mu \in \mathcal{M}$  w.r.t. a tuple of  $k$  authority master public keys  $(\text{apk}_i)_{i \in [k]}$ , and a policy  $f \in \mathcal{F}$ .
- $\mu' \leftarrow \text{Dec}(\text{pp}, (\text{apk}_i)_{i \in [k]}, (\text{sk}_i)_{i \in [k]}, \text{ctxt})$ : The decryption algorithm, on input a tuple of authority master public keys  $(\text{apk}_i)_{i \in [k]}$ , secret keys  $(\text{sk}_i)_{i \in [k]}$  and a ciphertext  $\text{ctxt}$ , outputs a message  $\mu'$ .

**Definition 4** (Correctness). An MA-ABE scheme is correct if for any  $\lambda, k \in \mathbb{N}$ ,  $\text{pp} \in \text{Setup}(1^\lambda)$ ,  $(\text{apk}_i, \text{ask}_i) \in \text{AuthSetup}(\text{pp})$  for  $i \in [k]$ ,  $\text{uid} \in \{0, 1\}^*$ ,  $\mu \in \mathcal{M}$ ,  $(\mathbf{x}_i)_{i \in [k]} \in \mathcal{X}^k$ , and  $f \in \mathcal{F}$  satisfying  $f(\mathbf{x}_1, \dots, \mathbf{x}_k) = 0$ , it holds that

$$\Pr \left[ \mu' = \mu \mid \begin{array}{l} \text{sk}_i \leftarrow \text{KGen}(\text{pp}, \text{apk}, \text{ask}, \text{uid}, \mathbf{x}_i) \forall i \in [k] \\ \text{ctxt} \leftarrow \text{Enc}(\text{pp}, (\text{apk}_i)_{i \in [k]}, f, \mu) \\ \mu' \leftarrow \text{Dec}(\text{pp}, (\text{apk}_i)_{i \in [k]}, (\text{sk}_i)_{i \in [k]}, \text{ctxt}) \end{array} \right] \geq 1 - \text{negl}(\lambda).$$

**Definition 5** (MA-ABE Security). An MA-ABE  $\Pi$  is IND-CPA-secure (under selective authority corruption, key attribute, and ciphertext policy queries), if for any PPT  $\mathcal{A}$ ,

$$\left| \Pr[\text{ExpMA}_{\Pi, \mathcal{A}}^0(1^\lambda) = 1] - \Pr[\text{ExpMA}_{\Pi, \mathcal{A}}^1(1^\lambda) = 1] \right| \leq \text{negl}(\lambda),$$

where  $\text{ExpMA}_{\Pi, \mathcal{A}}^b$  are defined in Fig. 4. Alternatively,  $\Pi$  is IND-CPA-secure without missing keys if the inequality holds conditioning on the event “if  $b_{\text{honest\_security}} = 1$  then  $b_{\text{key\_missing}} = 0$ ”, where  $b_{\text{honest\_security}}$  and  $b_{\text{key\_missing}}$  are defined in Fig. 4.<sup>16</sup>

**MC-ABE** Let  $\mathcal{X}$ ,  $\mathcal{F}$ , and  $\mathcal{M}$  denote the attribute space, the policy space over  $\mathcal{X}^k$ , and the message space respectively for some  $k \in \mathbb{N}$ . An MC-ABE consists of PPT algorithms  $(\text{Setup}, \text{AuthSetup}, \text{EKGen}, \text{KGen}, \text{Enc}_{\text{main}}, \text{Enc}_{\text{sub}}, \text{Dec})$  with the following syntax:

- $\text{pp} \leftarrow \text{Setup}(1^\lambda)$ : The setup algorithm generates the public parameters  $\text{pp}$ .
- $(\text{apk}, \text{ask}) \leftarrow \text{AuthSetup}(\text{pp})$ : The authority setup algorithm generates a pair of authority public key  $\text{apk}$  and secret key  $\text{ask}$  for an authority.
- $(\text{epk}, \text{esk}) \leftarrow \text{EKGen}(\text{pp})$ : The encryptor key generation algorithm generates a pair of encryptor public key  $\text{epk}$  and secret key  $\text{esk}$  for a (sub)-encryptor.
- $\text{sk} \leftarrow \text{KGen}(\text{pp}, \text{ask}, f)$ : The key generation algorithm generates a secret key  $\text{sk}$  given an authority secret key  $\text{ask}$ , and a policy  $f \in \mathcal{F}$ .
- $\text{ctxt}_1 \leftarrow \text{Enc}_{\text{main}}(\text{pp}, \text{apk}, (\text{epk}_i)_{i \in [2, k]}, \text{cid}, \mathbf{x}_1, \mu)$ : The main-encryption algorithm (for slot 1) encrypts a message  $\mu \in \mathcal{M}$  w.r.t. an authority master public key  $\text{apk}$ , a tuple of encryptor master public keys  $(\text{epk}_i)_{i \in [2, k]}$ , a ciphertext identifier  $\text{cid} \in \{0, 1\}^*$ , and an attribute  $\mathbf{x}_1 \in \mathcal{X}$ .
- $\text{ctxt}_i \leftarrow \text{Enc}_{\text{sub}}(\text{pp}, i, \text{esk}, \text{cid}, \mathbf{x}_i)$ : The sub-encryption algorithm (for slot  $i \in [2, k]$ ) inputs the slot number  $i$ , an encryptor secret key  $\text{sk}$ , a ciphertext identifier  $\text{cid}$ , and an attribute  $\mathbf{x}_i$ , and outputs a ciphertext  $\text{ctxt}_i$ .

<sup>16</sup>See Remark 2 for discussion on this condition.

$\text{ExpMA}_{\Pi, \mathcal{A}}^b(1^\lambda)$	
$\left( \begin{array}{l} N \in \mathbb{N}, \\ \mathcal{I}_{\text{corr}} \subseteq [N], \\ \mathcal{U}, (\mathcal{I}_{\text{uid}} \subseteq [N])_{\text{uid} \in \mathcal{U}}, (\mathbf{x}_{\text{uid}, i})_{\text{uid} \in \mathcal{U}, i \in \mathcal{I}_{\text{uid}}}, \\ \mathcal{I}^* \subseteq_k [N], f^*, \end{array} \right) \leftarrow \mathcal{A}(1^\lambda)$	$\begin{array}{l} // \text{ number of authorities} \\ // \text{ authority corruption} \\ // \text{ attribute key queries} \\ // \text{ challenge ciphertext} \end{array}$
$\text{pp} \leftarrow \text{Setup}(1^\lambda)$	
<b>for</b> $i \in [N]$ <b>do</b> $(\text{apk}_i, \text{ask}_i) \leftarrow \text{AuthSetup}(\text{pp})$	
<b>for</b> $\text{uid} \in \mathcal{U}$ , $i \in \mathcal{I}_{\text{uid}}$ <b>do</b> $\text{sk}_{\text{uid}, i} \leftarrow \text{KGen}(\text{pp}, \text{apk}_i, \text{ask}_i, \text{uid}, \mathbf{x}_{\text{uid}, i})$	
$(\mu_0, \mu_1) \leftarrow \mathcal{A}(\text{pp}, (\text{apk}_i)_{i \in [N]}, (\text{ask}_i)_{i \in \mathcal{I}_{\text{corr}}}, (\text{sk}_{\text{uid}, i} : \text{uid} \in \mathcal{U}, i \in \mathcal{I}_{\text{uid}}))$	
$\text{ctxt}^* \leftarrow \text{Enc}(\text{pp}, (\text{apk}_i)_{i \in \mathcal{I}^*}, f^*, \mu_b)$	
$b' \leftarrow \mathcal{A}(\text{ctxt}^*)$	
$b_{\text{honest\_chal\_auth}} := (\mathcal{I}^* \cap \mathcal{I}_{\text{corr}} = \emptyset)$	
$b_{\text{key\_missing}} := (\exists \text{uid} \in \mathcal{U}, \mathcal{I}^* \not\subseteq \mathcal{I}_{\text{uid}})$	
$b_{\text{key\_missing\_or\_policy\_reject}} := (\forall \text{uid} \in \mathcal{U}, (\mathcal{I}^* \not\subseteq \mathcal{I}_{\text{uid}}) \vee (f^*(\mathbf{x}_{\text{uid}, i} : i \in \mathcal{I}^*) \neq 0))$	
$b_{\text{honest\_security}} := b_{\text{honest\_chal\_auth}} \wedge b_{\text{key\_missing\_or\_policy\_reject}}$	
$b_{\text{corrupt\_security}} := (\forall \text{uid} \in \mathcal{U}, \mathcal{I}^* \setminus (\mathcal{I}_{\text{uid}} \cup \mathcal{I}_{\text{corr}}) \neq \emptyset)$	
<b>assert</b> $b_{\text{honest\_security}} \vee b_{\text{corrupt\_security}}$	
<b>return</b> $b'$	

**Figure 4:** Security experiment for MA-ABE.

- $\mu' \leftarrow \text{Dec}(\text{pp}, \text{sk}, (\text{ctxt}_i)_{i \in [k]})$ : The decryption algorithm, on input a secret key  $\text{sk}$  and a tuple of ciphertexts  $(\text{ctxt}_i)_{i \in [k]}$ , outputs a message  $\mu'$ .

**Definition 6** (Correctness). An MC-ABE scheme is correct if for any  $\lambda, k \in \mathbb{N}$ ,  $\text{pp} \in \text{Setup}(1^\lambda)$ ,  $(\text{apk}, \text{ask}) \in \text{AuthSetup}(\text{pp})$ ,  $(\text{epk}_i, \text{esk}_i) \in \text{EKGen}(\text{pp})$  for  $i \in [k]$ ,  $\text{cid} \in \{0, 1\}^*$ , any  $\mu \in \{0, 1\}$ ,  $f \in \mathcal{F}$ ,  $(\mathbf{x}_i)_{i \in [k]} \in \mathcal{X}^k$  satisfying  $f(\mathbf{x}_1, \dots, \mathbf{x}_k) = 0$ , it holds that

$$\Pr \left[ \mu' = \mu \left| \begin{array}{l} \text{sk} \leftarrow \text{KGen}(\text{pp}, \text{ask}, f) \\ \text{ctxt}_1 \leftarrow \text{Enc}_{\text{main}}(\text{pp}, \text{apk}, (\text{epk}_i)_{i \in [2, k]}, \text{cid}, \mathbf{x}_1, \mu) \\ \text{ctxt}_i \leftarrow \text{Enc}_{\text{sub}}(\text{pp}, i, \text{esk}_i, \text{cid}, \mathbf{x}_i) \forall i \in [2, k] \\ \mu' \leftarrow \text{Dec}(\text{pp}, \text{sk}, (\text{ctxt}_i)_{i \in [k]}) \end{array} \right. \right] \geq 1 - \text{negl}(\lambda).$$

**Definition 7** (MC-ABE Security). An MC-ABE scheme  $\Pi$  is IND-CPA-secure (under selective encryptor corruption and ciphertext attribute queries, and adaptive key policy queries), if for any PPT  $\mathcal{A}$ ,

$$|\Pr[\text{ExpMC}_{\Pi, \mathcal{A}}^0(1^\lambda) = 1] - \Pr[\text{ExpMC}_{\Pi, \mathcal{A}}^1(1^\lambda) = 1]| \leq \text{negl}(\lambda),$$

where  $\text{ExpMC}_{\Pi, \mathcal{A}}^b$  are defined in Fig. 5. Alternatively,  $\Pi$  is IND-CPA-secure without missing ciphertexts if the inequality holds conditioning on the event “if  $b_{\text{honest\_security}} = 1$  then  $b_{\text{ctxt\_missing}} = 0$ ”, where  $b_{\text{ctxt\_missing}}$  is defined in Fig. 5.

*Remark 2* (On assuming no key/ciphertext missing). In the MA-ABE security experiment (Fig. 4), suppose the flag  $b_{\text{honest\_security}}$  is set. Then the flag  $b_{\text{key\_missing\_or\_policy\_reject}}$  is set if for each  $\text{uid} \in \mathcal{U}$ , any of the following is true: 1)  $\mathcal{I}^* \not\subseteq \mathcal{I}_{\text{uid}}$ , meaning that at least one attribute key from an authority is missing, or 2)  $f^*(\mathbf{x}_{\text{uid}, i} : i \in \mathcal{I}^*) \neq 0$ , meaning that the policy  $f^*$  rejects the attributes for user  $\text{uid}$  authorised by the authorities  $\mathcal{I}^* \subseteq \mathcal{I}_{\text{uid}}$ . If the first event never happens for any  $\text{uid}$ , then we have  $b_{\text{key\_missing}} = 0$ .

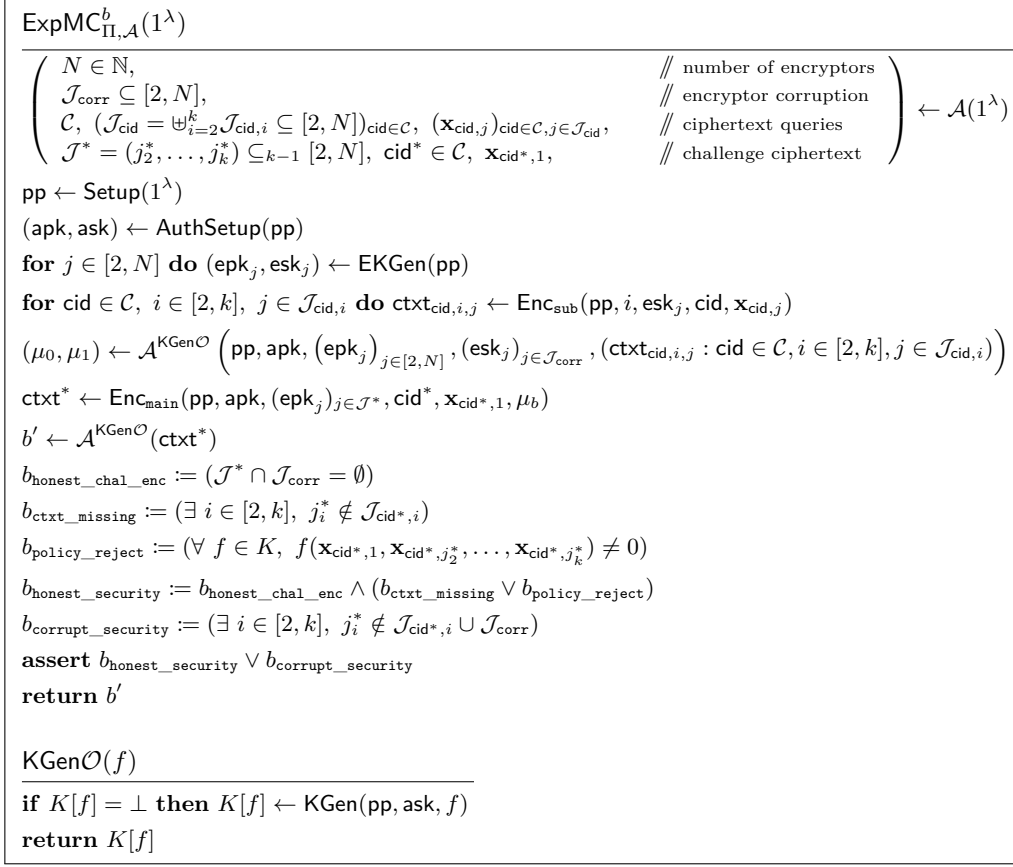


Figure 5: Security experiment for MC-ABE.

We show that an MA-ABE which is IND-CPA-secure without missing keys can be generically turned into another MA-ABE which is IND-CPA-secure without such condition. The transformation can be outlined as follows: We construct wrapped versions  $\text{KGen}'$  and  $\text{Enc}'$  of the  $\text{KGen}$  and  $\text{Enc}$  algorithms respectively. On input an attribute  $\mathbf{x}$ ,  $\text{KGen}'$  calls  $\text{KGen}$  on  $\mathbf{x}' := (0, \mathbf{x})$ , i.e. appending the attribute vector with a 0. On input a function  $f$ , writing  $\mathbf{x}'_i = (b, \mathbf{x}_i)$ ,  $\text{Enc}'$  calls  $\text{Enc}$  on  $f'(\mathbf{x}'_1, \dots, \mathbf{x}'_k)$  which checks if any of the  $b_i$  is 1. If so,  $f'$  returns 1. Else, it returns  $f(\mathbf{x}_1, \dots, \mathbf{x}_k)$ .

Since  $f'((0, \mathbf{x}_1), \dots, (0, \mathbf{x}_k)) = f(\mathbf{x}_1, \dots, \mathbf{x}_k)$ , the wrapped scheme is functionally equivalent to the base scheme. However, in a security reduction, if the flag  $b_{\text{honest\_security}}$  is set, but  $\mathcal{I}^* \not\subseteq \mathcal{I}_{\text{uid}}$  for some  $\text{uid}$ , meaning that  $\mathbf{x}_{\text{uid},i}$  is not specified by the adversary for some  $i \in \mathcal{I}^*$ , the reduction can pick  $\mathbf{x}'_{\text{uid},i} := (1, \mathbf{0})$  for the base scheme. Note that  $\mathbf{x}'_{\text{uid},i}$  picked as such would always be rejected by any wrapped  $f'$ . The security reduction of the base scheme for IND-CPA-security without missing keys thus follows.

A similar discussion applies to the  $b_{\text{ctxt\_missing}}$  flag of the MC-ABE security experiment (Fig. 5) as well. In other words, an MC-ABE which is IND-CPA-secure without missing ciphertexts can be generically turned into another MC-ABE which is IND-CPA-secure. The only difference is that now attributes are associated to ciphertexts and policies are associated to keys. The transformations to a policy  $f$  and an attribute  $\mathbf{x}$  are identical to that of the MA setting described above.

<p><b>Setup</b>(<math>1^\lambda</math>)</p> <hr/> $\mathbf{B}_1, \mathbf{B}_2 \leftarrow \mathbb{Z}_q^{n \times m\ell}, \mathbf{v} \leftarrow \mathbb{Z}_q^n$ <b>return</b> $\text{pp} := (\mathbf{B}_1, \mathbf{B}_2, \mathbf{v})$ <p><b>AuthSetup</b>(pp)</p> <hr/> $(\mathbf{A}, \text{td}_\mathbf{A}) \leftarrow \text{TrapGen}(1^n, q)$ $h := \text{ncol}(\mathbf{A}) \quad // \mathbf{A} \in \mathbb{Z}_q^{n \times h}$ <b>return</b> $(\text{apk}, \text{ask}) := (\mathbf{A}, \text{td}_\mathbf{A})$ <p><b>KGen</b>(pp, ask, <math>f</math>)</p> <hr/> <b>parse</b> $\text{td}_\mathbf{A} \leftarrow \text{ask}$ $\mathbf{H}_{\mathbf{B},f} \leftarrow \text{EvalF}(\mathbf{B}, f), \mathbf{B}_f := \mathbf{B} \cdot \mathbf{H}_{\mathbf{B},f}$ $\text{td}_{(\mathbf{A} \mathbf{B}_f)} \leftarrow (\text{td}_\mathbf{A}^\top   \mathbf{0}^\top)^\top$ $\mathbf{u}_f \leftarrow \text{SampPre}(\mathbf{A}   \mathbf{B}_f, \text{td}_{(\mathbf{A} \mathbf{B}_f)}, \mathbf{v}, \tau)$ <b>return</b> $\text{sk}_f := (\mathbf{u}_f, f)$	<p><b>EKGen</b>(pp)</p> <hr/> $(\mathbf{D}, \text{td}_\mathbf{D}) \leftarrow \text{TrapGen}(1^{(2\ell+2)n}, q)$ $k := \text{ncol}(\mathbf{D}) \quad // \mathbf{D} \in \mathbb{Z}_q^{(2\ell+2)n \times k}$ <b>return</b> $(\text{epk}, \text{esk}) := (\mathbf{D}, \text{td}_\mathbf{D})$ <p><b>Enc<sub>sub</sub></b>(pp, esk, cid, <math>\mathbf{x}_2</math>)</p> <hr/> <b>parse</b> $(\mathbf{D}, \text{td}) \leftarrow \text{esk}$ <b>parse</b> $\left( \begin{array}{c} \mathbf{D}_0 \\ \mathbf{D}_{2,j,b} : j \in [\ell], b \in \{0,1\} \\ \mathbf{D}_3 \end{array} \right) \leftarrow \mathbf{D}$ $\mathbf{D}_{\mathbf{x}_2} := \left( \begin{array}{c} \mathbf{D}_0 \\ \mathbf{D}_{2,j,x_{2,j}} : j \in [\ell] \\ \mathbf{D}_3 \end{array} \right)$ $H(\text{epk}, \text{cid}, \mathbf{x}_2) := \left( \begin{array}{c} H(\text{epk}, \text{cid}, 0) \\ H(\text{epk}, \text{cid}, 2, j, x_{2,j}) : j \in [\ell] \\ H(\text{epk}, \text{cid}, 3) \end{array} \right)$ $\mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2} \leftarrow \text{SampPre}(\mathbf{D}_{\mathbf{x}_2}, \text{td}, H(\text{epk}, \text{cid}, \mathbf{x}_2), \sigma)$ <b>return</b> $\text{ctx}_{\mathbf{x}_2} := (\mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}, \mathbf{x}_2)$
--	---

**Figure 6:** Description of 2C-ABE construction  $\Pi_{2C}$ , except for  $\text{Enc}_{\text{main}}$  and  $\text{Dec}$  algorithms.

**Table 3:** Parameters and shorthands for 2C-ABE (Section 5).

$n \in \mathbb{N}$		Number of rows of $\mathbf{A}$ , $\mathbf{B}_{i,j}$ , and $\mathbf{D}_0, \mathbf{D}_{2,j,b}, \mathbf{D}_3$ , and $\mathbf{G}$
$m \in \mathbb{N}$	$n \lceil \log q \rceil$	Number of columns of $\mathbf{B}_{i,j}$ and $\mathbf{G}$
$h \in \mathbb{N}$	$2m > (n+1) \log q + \omega(\log n)$	Number of columns of $\mathbf{A}$
$k \in \mathbb{N}$	$4(\ell+1)m \geq n(2\ell+2) \log q$	Number of columns of $\mathbf{D}$
$\beta$	$\geq k\ell\lambda^3\sigma\tau(\chi + \hat{\chi} + \bar{\chi})m^{O(d)}$	Correctness bound
$q$	$\geq \lambda^{\omega(1)}\beta$	Modulus
$\ell$		Attribute length per encryptor
$\chi$	$\text{poly}(\lambda)$	Gaussian parameter of $\mathbf{E}_0$ and $\mathbf{e}_3$
$\hat{\chi}$	$\geq \lambda^{\omega(1)}\lambda m\chi$	Gaussian parameter of $\mathbf{E}_{1,j}, \mathbf{E}_{2,j,b}, \hat{\mathbf{E}}_{2,j,b}, \hat{\mathbf{E}}_0$ , and $\hat{\mathbf{e}}_3$
$\bar{\chi}$	$\geq \lambda^{\omega(1)}\lambda^2\tau\hat{\chi}k$	Gaussian parameter of $\bar{\mathbf{e}}_{2,j,b}, \bar{\mathbf{e}}_0$ , and $\bar{\mathbf{e}}_3$
$\tau$	$\geq \ell h^3 m^{O(d)}$	Parameter of KGen algorithm
$\sigma$	$\geq \omega(\sqrt{\log k})$	Parameter of $\text{Enc}_2$ algorithm

## 5 2C-ABE

We construct a 2C-ABE adapting the construction of [Ayy22]. We recall that in this setting there exists a single authority and a public encryptor 1, the latter specifies (the public key of) a single encryptor 2 in its ciphertext. Decryption succeeds if the attributes from encryptors 1 and 2 jointly satisfy the function specified by (the secret key handed out by) the authority.

**Construction.** The construction  $\Pi_{2C}$  is described in Figures 6 to 8, with parameters specified in Table 3. Our construction can support polynomial-size circuits with any depth  $d = d(\lambda) = \text{poly}(\lambda)$ . Formally, it supports attribute space  $\mathcal{X} = \{0, 1\}^\ell$ ,  $\ell = \ell(\lambda) = \text{poly}(\lambda)$ , and any circuit class  $\mathcal{F}$  that is subclass of  $\ell$ -input  $\text{poly}(\lambda)$ -size circuits of depth at most  $d$ .

$\text{Enc}_{\text{main}}(\text{pp}, \text{apk}, \text{epk}, \text{cid}, \mathbf{x}_1, \mu)$

---

**parse**  $(\mathbf{B}_1, \mathbf{B}_2, \mathbf{v}) \leftarrow \text{pp}, (\mathbf{A}, \mathbf{D}) \leftarrow (\text{apk}, \text{epk})$

**parse**  $\left( \begin{array}{c} \mathbf{D}_0 \\ \mathbf{D}_{2,j,b} : j \in [\ell], b \in \{0,1\} \\ \mathbf{D}_3 \end{array} \right) \leftarrow \mathbf{D}; (\mathbf{B}_{1,j} : j \in [\ell]) \leftarrow \mathbf{B}_1; (\mathbf{B}_{2,j} : j \in [\ell]) \leftarrow \mathbf{B}_2$

$\mathbf{S} \leftarrow \mathbb{Z}_q^{k \times n}; \mathbf{E}_0 \leftarrow \mathbb{Z}_q^{k \times h}; \mathbf{e}_3 \leftarrow \mathbb{Z}_q^k; \hat{\mathbf{S}}_0 \leftarrow \mathbb{Z}_q^{h \times n}; \hat{\mathbf{E}}_0 \leftarrow \mathbb{Z}_q^{k \times h}$

$\tilde{\mathbf{e}}_0 \leftarrow \mathbb{Z}_q^h; \hat{\mathbf{s}}_3 \leftarrow \mathbb{Z}_q^n; \hat{\mathbf{e}}_3 \leftarrow \mathbb{Z}_q^k; \tilde{\mathbf{e}}_3 \leftarrow \mathbb{Z}_q^k$

**for**  $j \in [\ell], b \in \{0,1\}$  **do**

$\mathbf{E}_{1,j} \leftarrow \mathbb{Z}_q^{k \times m}; \mathbf{E}_{2,j,b} \leftarrow \mathbb{Z}_q^{k \times m}; \hat{\mathbf{S}}_{2,j,b} \leftarrow \mathbb{Z}_q^{m \times n}; \hat{\mathbf{E}}_{2,j,b} \leftarrow \mathbb{Z}_q^{m \times k}; \tilde{\mathbf{e}}_{2,j,b} \leftarrow \mathbb{Z}_q^m$

$\mathbf{C}_0 := \mathbf{S}\mathbf{A} + \mathbf{E}_0 \bmod q, \quad \hat{\mathbf{C}}_0 := \hat{\mathbf{S}}_0\mathbf{D}_0 + \hat{\mathbf{E}}_0 \bmod q, \quad \bar{\mathbf{C}}_0 := \hat{\mathbf{C}}_0^\top + \mathbf{C}_0 \bmod q$

$\tilde{\mathbf{c}}_0 := \hat{\mathbf{S}}_0 H(\text{epk}, \text{cid}, 0) + \tilde{\mathbf{e}}_0 \bmod q, \quad \mathbf{c}_3 := \mathbf{S}\mathbf{v} + \mathbf{e}_3 + \mathbf{g}\mu \bmod q, \quad \hat{\mathbf{c}}_3^\top := \hat{\mathbf{s}}_3^\top \mathbf{D}_3 + \hat{\mathbf{e}}_3^\top \bmod q$

$\tilde{\mathbf{c}}_3 := \hat{\mathbf{e}}_3 + \mathbf{c}_3 \bmod q, \quad \tilde{\mathbf{c}}_3 := \hat{\mathbf{s}}_3^\top H(\text{epk}, \text{cid}, 3) + \tilde{\mathbf{e}}_3 \bmod q$

**for**  $i \in [\ell]$  **do**

$\mathbf{C}_{1,j} := \mathbf{S}(\mathbf{B}_{1,j} - x_{1,j}\mathbf{G}) + \mathbf{E}_{1,j} \bmod q$

**for**  $i \in [\ell], b \in \{0,1\}$  **do**

$\mathbf{C}_{2,j,b} := \mathbf{S}(\mathbf{B}_{2,j} - b\mathbf{G}) + \mathbf{E}_{2,j,b} \bmod q, \quad \hat{\mathbf{C}}_{2,j,b} := \hat{\mathbf{S}}_{2,j,b}\mathbf{D}_{2,j,b} + \hat{\mathbf{E}}_{2,j,b} \bmod q$

$\bar{\mathbf{C}}_{2,j,b} := \hat{\mathbf{C}}_{2,j,b}^\top + \mathbf{C}_{2,j,b} \bmod q, \quad \tilde{\mathbf{c}}_{2,j,b} := \hat{\mathbf{S}}_{2,j,b} H(\text{epk}, \text{cid}, 2, j, b) + \tilde{\mathbf{e}}_{2,j,b} \bmod q$

$\text{ctxt}_1 := \left( \begin{array}{ccc} \bar{\mathbf{C}}_0, & (\mathbf{C}_{1,j})_{j \in [\ell]}, & (\bar{\mathbf{C}}_{2,j,b})_{j \in [\ell], b \in \{0,1\}}, & \tilde{\mathbf{c}}_3, \\ \tilde{\mathbf{c}}_0, & \mathbf{x}_1, & (\tilde{\mathbf{c}}_{2,j,b})_{j \in [\ell], b \in \{0,1\}}, & \tilde{\mathbf{c}}_3 \end{array} \right)$

**return**  $\text{ctxt}_1$

**Figure 7:** Description of  $\text{Enc}_{\text{main}}$  algorithm of the 2C-ABE construction  $\Pi_{2C}$ .

**Theorem 1** (Correctness). *For parameters as in Table 3,  $\Pi_{2C}$  is correct.*

*Proof.* To analyse correctness, first observe the following facts. One has:

$$\begin{aligned} \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \bar{\mathbf{C}}_0 &= \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top (\mathbf{D}_0^\top \hat{\mathbf{S}}_0^\top + \hat{\mathbf{E}}_0^\top + \mathbf{S}\mathbf{A} + \mathbf{E}_0) \approx H(\text{epk}, \text{cid}, 0)^\top \hat{\mathbf{S}}_0^\top + \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \mathbf{S}\mathbf{A}, \\ \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \mathbf{C}_{1,j} &= \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top (\mathbf{S}(\mathbf{B}_{1,j} - x_{1,j}\mathbf{G}) + \mathbf{E}_{1,j}) \approx \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \mathbf{S}(\mathbf{B}_{1,j} - x_{1,j}\mathbf{G}), \\ \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \bar{\mathbf{C}}_{2,j,x_{2,j}} &= \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top (\mathbf{D}_{2,j,x_{2,j}}^\top \hat{\mathbf{S}}_{2,j,x_{2,j}}^\top + \hat{\mathbf{E}}_{2,j,x_{2,j}}^\top + \mathbf{S}(\mathbf{B}_{2,j} - x_{2,j}\mathbf{G}) + \mathbf{E}_{2,j,x_{2,j}}) \\ &\approx H(\text{epk}, \text{cid}, 2, j, x_{2,j})^\top \hat{\mathbf{S}}_{2,j,x_{2,j}}^\top + \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \mathbf{S}(\mathbf{B}_{2,j} - x_{2,j}\mathbf{G}), \\ \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \tilde{\mathbf{c}} &= \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top (\mathbf{D}_3^\top \hat{\mathbf{s}}_3 + \hat{\mathbf{e}}_3 + \mathbf{S}\mathbf{v} + \mathbf{e}_3 + \mathbf{g}\mu) \\ &\approx H(\text{epk}, \text{cid}, 3)^\top \hat{\mathbf{s}}_3 + \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top (\mathbf{S}\mathbf{v} + \mathbf{g}\mu), \end{aligned}$$

with approximations errors given by

$$\begin{aligned} \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top (\hat{\mathbf{E}}_0^\top + \mathbf{E}_0), & \quad \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \mathbf{E}_{1,j}, \\ \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top (\hat{\mathbf{E}}_{2,j,x_{2,j}}^\top + \mathbf{E}_{2,j,x_{2,j}}), & \quad \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top (\hat{\mathbf{e}}_3 + \mathbf{e}_3) \end{aligned}$$

respectively. It follows that

$$\begin{aligned} \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \bar{\mathbf{C}}_0 - \tilde{\mathbf{c}}_0 &\approx H(\text{epk}, \text{cid}, 0)^\top \hat{\mathbf{S}}_0^\top + \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \mathbf{S}\mathbf{A} - (H(\text{epk}, \text{cid}, 0)^\top \hat{\mathbf{S}}_0^\top + \tilde{\mathbf{e}}_0^\top) \\ &\approx \mathbf{t}_{\text{epk}, \text{cid}, \mathbf{x}_2}^\top \mathbf{S}\mathbf{A}, \end{aligned}$$

```

Dec(pp, skf, (ctxtj)j∈[2])
-----
parse (B1, B2, v) ← pp, (uf = (uf,0T | uf,1T)T, f) ← skf
parse (C̄0, (C1,j)j∈[ℓ], (C̄2,j,b)j∈[ℓ],b∈{0,1}, c̄3) ← ctxt1
           c̄0,           x1           (c̄2,j,b)j∈[ℓ],b∈{0,1}, c̄3
parse (tepk,cid,x2, x2) ← ctxt2
B := (B1 | B2), xT := (x1T | x2T)
HB,f,x ← EvalFX(B, f, x)
C1 := (C1,1 | ... | C1,ℓ)
C̄2 := (C̄2,1,x2,1 | ... | C̄2,ℓ,x2,ℓ)
c̄2T := (c̄2,1,x2,1T | ... | c̄2,ℓ,x2,ℓT)
c0T := tepk,cid,x2T C̄0 - c̄0T mod q
c1T := tepk,cid,x2T C1 mod q
c2T := tepk,cid,x2T C̄2 - c̄2T mod q
c3 := tepk,cid,x2T c̄3 - c̄3 mod q
z := (c0T | ((c1T | c2T) HB,f,x)) uf mod q
y := c3 - z mod q
return (|y| ≥ β)

```

**Figure 8:** Description of Dec algorithm of the 2C-ABE construction  $\Pi_{2c}$ .

$$\begin{aligned}
\mathbf{t}_{\text{cid},\text{id},\mathbf{x}_2}^T \bar{\mathbf{C}}_{2,j,x_{2,j}} - \tilde{\mathbf{c}}_{2,j,x_{2,j}} &\approx H(\text{epk}, \text{cid}, 2, j, x_{2,j})^T \hat{\mathbf{S}}_{2,j,x_{2,j}}^T + \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T \mathbf{S}(\mathbf{B}_{2,j} - x_{2,j} \mathbf{G}) \\
&\quad - (H(\text{epk}, \text{cid}, 2, j, x_{2,j})^T \hat{\mathbf{S}}_{2,j,x_{2,j}}^T + \tilde{\mathbf{e}}_{2,j,x_{2,j}}^T) \\
&\approx \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T \mathbf{S}(\mathbf{B}_{2,j} - x_{2,j} \mathbf{G}), \\
\mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T \bar{\mathbf{c}} - \tilde{\mathbf{c}}_3 &\approx H(\text{epk}, \text{cid}, 3)^T \hat{\mathbf{s}}_3 + \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\mathbf{S}\mathbf{v} + \mathbf{g}\mu) \\
&\quad - (H(\text{epk}, \text{cid}, 3)^T \hat{\mathbf{s}}_3 + \tilde{\mathbf{e}}_3) \\
&\approx \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\mathbf{S}\mathbf{v} + \mathbf{g}\mu),
\end{aligned}$$

with approximations errors given by

$$\mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\hat{\mathbf{E}}_0 + \mathbf{E}_0) - \tilde{\mathbf{e}}_0^T, \quad \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\hat{\mathbf{E}}_{2,j,x_{2,j}} + \mathbf{E}_{2,j,x_{2,j}}) - \tilde{\mathbf{e}}_{2,j,x_{2,j}}^T, \quad \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\hat{\mathbf{e}}_3 + \mathbf{e}_3) - \tilde{\mathbf{e}}_3.$$

respectively.

Let  $\mathbf{c}_0$ ,  $\mathbf{c}_1$ ,  $\mathbf{c}_2$ ,  $c_3$ , and  $z = (\mathbf{c}_0^T | ((\mathbf{c}_1^T | \mathbf{c}_2^T) \mathbf{H}_{\mathbf{B},f,\mathbf{x}})) \mathbf{u}_f \bmod q$  be as computed in the decryption algorithm. Parse  $\mathbf{u}_f^T = (\mathbf{u}_{f,0}^T | \mathbf{u}_{f,1}^T)$  and note that  $\|\mathbf{u}_f\| \leq \tau\lambda$  with overwhelming probability. Write

$$\begin{aligned}
\bar{\mathbf{e}}_0^T &:= \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\hat{\mathbf{E}}_0 + \mathbf{E}_0) - \tilde{\mathbf{e}}_0^T, \\
\bar{\mathbf{e}}_1^T &:= \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\mathbf{E}_{1,1} | \dots | \mathbf{E}_{1,1}), \\
\bar{\mathbf{e}}_2^T &:= \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\hat{\mathbf{E}}_{2,1,x_{2,1}} + \mathbf{E}_{2,1,x_{2,1}} | \dots | \hat{\mathbf{E}}_{2,\ell,x_{2,\ell}} + \mathbf{E}_{2,\ell,x_{2,\ell}}) - (\tilde{\mathbf{e}}_{2,1,x_{2,1}}^T | \dots | \tilde{\mathbf{e}}_{2,\ell,x_{2,\ell}}^T), \\
\bar{\mathbf{e}}_3 &:= \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\hat{\mathbf{e}}_3 + \mathbf{e}_3) - \tilde{\mathbf{e}}_3
\end{aligned}$$

and note that  $\|\bar{\mathbf{e}}_i\| \leq k\lambda^2\sigma(\chi + \hat{\chi} + \tilde{\chi})$  for  $i \in [0, 3]$  with overwhelming probability. We have  $c_3 \approx \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T (\mathbf{S}\mathbf{v} + \mathbf{g}\mu)$ ,  $z \approx \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T \mathbf{S}\mathbf{v}$  and hence  $c_3 - z \approx \mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^T \mathbf{g}\mu$  with approximation error given by

$$e := \bar{\mathbf{e}}_3 - \bar{\mathbf{e}}_0^T \mathbf{u}_{f,0} - (\bar{\mathbf{e}}_1 | \bar{\mathbf{e}}_2)^T \mathbf{H}_{\mathbf{B},f,\mathbf{x}} \mathbf{u}_{f,1}$$



where  $|e| \leq k\ell\lambda^3\sigma\tau(\chi + \hat{\chi} + \tilde{\chi})m^{O(d)} < \beta$  with overwhelming probability. This means that decryption is correct with overwhelming probability when  $\mu = 0$ .

When  $\mu = 1$ , we have  $\|\mathbf{t}_{\text{epk},\text{cid},\mathbf{x}_2}^\top \mathbf{g}\mu\| > 2\beta$  with overwhelming probability since  $q \geq \lambda^{\omega(1)}\beta$ . This completes the proof.  $\square$

**Theorem 2** (Security). *For parameters as in Table 3,  $\Pi_{2C}$  is IND-CPA-secure without missing ciphertexts (c.f. Definition 7) assuming  $\text{LWE}_{m,n,k+1,\hat{\chi},q}$  and  $\text{LWE}_{k,n,m+1,\chi,q}$  in the random oracle model.*

*Proof.* Let  $\mathcal{J}_{\text{corr}}, \mathcal{C}$ ,  $(\mathcal{J}_{\text{cid}} = \uplus_{i=2}^k \mathcal{J}_{\text{cid},i} \subseteq [2, N])_{\text{cid} \in \mathcal{C}}$ ,  $(\mathbf{x}_{\text{cid},j})_{\text{cid} \in \mathcal{C}, j \in \mathcal{J}_{\text{cid}}}$ ,  $\mathcal{J}^* = (j_2^*) \in [2, N]$ ,  $\text{cid}^*$ ,  $\mathbf{x}_{\text{cid}^*,1}$  be the adversary's output. Since we are proving IND-CPA-security without missing ciphertexts, we can assume that if  $b_{\text{honest\_security}} = 1$ , then  $b_{\text{ctxt\_missing}} = 0$ . Also, w.l.o.g. we can assume  $b_{\text{corrupt\_security}} = 0$ , because encryptor  $j_2^*$  cannot be corrupt by definition when  $k = 2$ . Parse  $\mathbf{x}_{\text{cid}^*,j_2^*}$  from  $(\mathbf{x}_{\text{cid},j})_{\text{cid} \in \mathcal{C}, j \in \mathcal{J}_{\text{cid}}}$  and set  $\mathbf{x}^* = (\mathbf{x}_1^*, \mathbf{x}_2^*) := (\mathbf{x}_{\text{cid}^*,1}, \mathbf{x}_{\text{cid}^*,j_2^*})$ . Consider the following sequence of hybrids:

- $H_0$ : This is the real security experiment encrypting  $\mu_b$ .
- $H_1$ : This is the same as  $H_0$ , except for the following modification to how  $\mathbf{t}_{\text{epk}_j,\text{cid},\mathbf{x}_{\text{cid},j}}$  is generated for each ciphertext query  $(\text{pp}, 2, \text{esk}_j, \text{cid}, \mathbf{x}_{\text{cid},j})$  to  $\text{Enc}_{\text{sub}}$ :
  - Sample a random Gaussian  $\mathbf{t}_{\text{epk}_j,\text{cid},\mathbf{x}_{\text{cid},j}} \leftarrow \mathcal{D}_{\mathbb{Z}^k,\sigma}$ ,
  - Set

$$\begin{aligned} H(\text{epk}_j, \text{cid}, 0) &:= \mathbf{D}_0 \mathbf{t}_{\text{epk}_j,\text{cid},\mathbf{x}_{\text{cid},j}}, \\ H(\text{epk}_j, \text{cid}, 2, h, x_{\text{cid},j,h}) &:= \mathbf{D}_{2,h,x_{\text{cid},j,h}} \mathbf{t}_{\text{epk}_j,\text{cid},\mathbf{x}_{\text{cid},j}} \quad \forall h \in [\ell], \\ H(\text{epk}_j, \text{cid}, 3) &:= \mathbf{D}_3 \mathbf{t}_{\text{epk}_j,\text{cid},\mathbf{x}_{\text{cid},j}}. \end{aligned}$$

Using that  $k \geq n(2\ell + 2) \log q$  and  $\sigma \geq \omega(\sqrt{\log k})$ , by Lemma 4 we conclude that  $H_0 \approx_s H_1$ . Notice that the experiment does not use  $\text{td}_{\mathbf{C}}$  any more.

- $H_2$ : This is the same as  $H_1$ , except for the following modification to  $\mathbf{D}$  in  $\text{epk}$ :
  - sample  $\mathbf{D} \leftarrow \mathbb{Z}_q^{n(2\ell+2) \times k}$  instead of  $(\mathbf{D}, \text{td}_{\mathbf{D}}) \leftarrow \text{TrapGen}(1^{n(2\ell+2)}, q)$

By the property of  $\text{TrapGen}$  algorithm (Section 3.3), the distribution of  $\mathbf{D}$  is statistically indistinguishable between  $H_2$  and  $H_1$ . Therefore,  $H_1 \approx_s H_2$ .

- $H_3 = H_{4,0}$ : This is the same as  $H_2$ , except for the following modification to how  $\tilde{\mathbf{c}}_0$ ,  $\tilde{\mathbf{c}}_{2,h,x_{\text{cid}^*,j_2^*,h}} \forall h \in [\ell]$ , and  $\tilde{\mathbf{c}}_3$  for the challenge ciphertext are generated:

- Sample  $\tilde{\mathbf{e}}_{2,h,x_{\text{cid}^*,j_2^*,h}} \leftarrow \tilde{\chi}^m$  for  $h \in [\ell]$ ,  $\tilde{\mathbf{e}}_0 \leftarrow \tilde{\chi}^h$ , and  $\tilde{\mathbf{e}}_3 \leftarrow \tilde{\chi}$
- Set

$$\tilde{\mathbf{c}}_0^\top := \mathbf{t}_{\text{epk}_{j_2^*},\text{cid}^*,\mathbf{x}_{\text{cid}^*,j_2^*}}^\top (\bar{\mathbf{C}}_0^\top - \mathbf{C}_0) + \tilde{\mathbf{e}}_0^\top, \quad \tilde{\mathbf{c}}_3 := \mathbf{t}_{\text{epk}_{j_2^*},\text{cid}^*,\mathbf{x}_{\text{cid}^*,j_2^*}}^\top (\bar{\mathbf{c}}_3 - \mathbf{c}_3) + \tilde{\mathbf{e}}_3,$$

and for  $j \in [\ell]$

$$\tilde{\mathbf{c}}_{2,j,x_{\text{cid}^*,j_2^*,h}}^\top := \mathbf{t}_{\text{epk}_{j_2^*},\text{cid}^*,\mathbf{x}_{\text{cid}^*,j_2^*}}^\top (\bar{\mathbf{C}}_{2,h,x_{\text{cid}^*,j_2^*,h}}^\top - \mathbf{C}_{2,h,x_{\text{cid}^*,j_2^*,h}}) + \tilde{\mathbf{e}}_{2,h,x_{\text{cid}^*,j_2^*,h}}.$$

Observe that

$$\tilde{\mathbf{c}}_{2,h,x_{\text{cid}^*,j_2^*,h}}$$

$$\begin{aligned}
&= \mathbf{t}_{\text{epk}_{j_2^*}, \text{cid}^*, \mathbf{x}_{\text{cid}^*, j_2^*}}^T \left( \hat{\mathbf{C}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T - \mathbf{C}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h} \right) + \tilde{\mathbf{e}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T \\
&= \mathbf{t}_{\text{epk}_{j_2^*}, \text{cid}^*, \mathbf{x}_{\text{cid}^*, j_2^*}}^T \left( \mathbf{D}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T \hat{\mathbf{S}}_{h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T + \hat{\mathbf{E}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T \right) + \tilde{\mathbf{e}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T \\
&= \mathbf{t}_{\text{epk}_{j_2^*}, \text{cid}^*, \mathbf{x}_{\text{cid}^*, j_2^*}}^T \mathbf{D}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T \hat{\mathbf{S}}_{h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T + \mathbf{t}_{\text{epk}_{j_2^*}, \text{cid}^*, \mathbf{x}_{\text{cid}^*, j_2^*}}^T \hat{\mathbf{E}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T + \tilde{\mathbf{e}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T \\
&= H(\text{epk}_{j_2^*}, \text{cid}^*, h, \mathbf{x}_{\text{cid}^*, j_2^*}, h)^T \hat{\mathbf{S}}_{h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T + \mathbf{t}_{\text{epk}_{j_2^*}, \text{cid}^*, \mathbf{x}_{\text{cid}^*, j_2^*}}^T \hat{\mathbf{E}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T + \tilde{\mathbf{e}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T.
\end{aligned}$$

By noise flooding, we have that the distribution of  $\tilde{\mathbf{c}}_{2,j, x_{2,j}^*}$  in  $H_1$  and  $H_2$  are statistically close, as long as  $\tilde{\chi} \geq \lambda^{\omega(1)} \lambda^2 \tau \hat{\chi} k \geq \lambda^{\omega(1)} \left\| \mathbf{t}_{\text{epk}_{j_2^*}, \text{cid}^*, \mathbf{x}_{\text{cid}^*, j_2^*}}^T \hat{\mathbf{E}}_{2,h, \mathbf{x}_{\text{cid}^*, j_2^*}, h}^T \right\|$ . Identical reasoning applies to the distributions of  $\tilde{\mathbf{c}}_0$  and  $\tilde{\mathbf{c}}_3$ . We conclude that  $H_2 \approx_s H_3$ .

- $H_{4,h}$  for  $h \in [\ell]$ : This is the same as  $H_{4,h-1}$ , except for the following modification to  $\tilde{\mathbf{c}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}$  in the challenge ciphertext:

- sample  $\bar{\mathbf{e}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h} \leftarrow \mathbb{S} \hat{\chi}^m$ ,
- set  $\tilde{\mathbf{c}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}^T$  as

$$H(\text{epk}_{j_2^*}, \text{cid}^*, 2, h, 1-x_{\text{cid}^*, j_2^*}, h)^T \hat{\mathbf{S}}_{h, 1-x_{\text{cid}^*, j_2^*}, h}^T + \bar{\mathbf{e}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}^T + \tilde{\mathbf{e}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}^T.$$

By noise flooding, we have that the distribution of  $\tilde{\mathbf{c}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}$  in  $H_{4,h-1}$  and  $H_{4,h}$  are statistically close, as long as  $\tilde{\chi} \geq \lambda^{\omega(1)} \lambda \hat{\chi} \geq \lambda^{\omega(1)} \left\| \bar{\mathbf{e}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}^T \right\|$ .

- $H_{5,h}$  for  $h \in [\ell]$ : This is the same as  $H_{5,h-1}$ , except for the following modification to  $\hat{\mathbf{C}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}$  and  $\tilde{\mathbf{c}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}$  in the challenge ciphertext:

- sample  $\tilde{\mathbf{e}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h} \leftarrow \mathbb{S} \tilde{\chi}^m$
- sample  $\bar{\mathbf{C}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h} \leftarrow \mathbb{S} \mathbb{Z}_q^{k \times m}$ ,  $\tilde{\mathbf{c}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h} \leftarrow \mathbb{S} \mathbb{Z}_q^m$ .
- output  $\hat{\mathbf{C}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}$  and  $\tilde{\mathbf{c}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h} + \tilde{\mathbf{e}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}$ .

To show that  $H_{5,h-1} \approx_c H_{5,h}$ , one reduces to  $\text{LWE}_{m,n,k+1, \tilde{\chi}, q}$ . In particular, the reduction works as follows:

- it parses  $\mathbf{M} = [\mathbf{M}_0 \mid \mathbf{m}_1] \in \mathbb{Z}_q^{n \times k} \times \mathbb{Z}_q^n$  and  $\mathbf{N} = [\mathbf{N}_0 \mid \mathbf{n}_1] \in \mathbb{Z}_q^{m \times k} \times \mathbb{Z}_q^m$  from the  $\text{LWE}_{m,n,k+1, \tilde{\chi}, q}$  instance
- produces the components of

$$\left( \begin{array}{ccc} \bar{\mathbf{C}}_0, & (\mathbf{C}_{1,h})_{h \in [\ell]}, & (\bar{\mathbf{C}}_{2,h,b})_{h \in [\ell], b \in \{0,1\}}, & \bar{\mathbf{c}}_3, \\ \tilde{\mathbf{c}}_0, & \mathbf{x}_1 & (\tilde{\mathbf{c}}_{2,h,b})_{h \in [\ell], b \in \{0,1\}}, & \tilde{\mathbf{c}}_3 \end{array} \right),$$

except  $\bar{\mathbf{C}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}$  and  $\tilde{\mathbf{c}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}$  as before

- it samples  $\tilde{\mathbf{e}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h} \leftarrow \mathbb{S} \tilde{\chi}^m$
- it sets

$$\begin{aligned}
\mathbf{C}_{h, 1-x_{\text{cid}^*, j_2^*}, h} &:= \mathbf{M}_0, & H(\text{epk}_{j_2^*}, \text{cid}^*, 2, h, 1-x_{\text{cid}^*, j_2^*}, h) &:= \mathbf{m}_1, \\
\hat{\mathbf{C}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h} &:= \mathbf{N}_0^T + \mathbf{C}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}, & \tilde{\mathbf{c}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h} &:= \mathbf{n}_1^T + \tilde{\mathbf{e}}_{2,h, 1-x_{\text{cid}^*, j_2^*}, h}.
\end{aligned}$$

Observe that

- if  $(\mathbf{M}, \mathbf{N})$  is a structured  $\text{LWE}_{m,n,k+1,\hat{\chi},q}$  instance, the view of the adversary  $\mathcal{A}$  is identical to  $\text{H}_{5,h-1}$ ;
- if  $(\mathbf{M}, \mathbf{N})$  is a uniform random instance, the view of  $\mathcal{A}$  is identical to  $\text{H}_{5,h}$ .

We conclude that  $\text{H}_{5,h-1} \approx_c \text{H}_{5,h}$  for all  $h \in [\ell]$ .

- $\text{H}_6$ : This is the same as  $\text{H}_{5,\ell}$ , except for the following modification to how  $(\mathbf{B}_i)_{i \in [2]} = (\mathbf{B}_{i,1}, \dots, \mathbf{B}_{i,\ell})_{i \in [2]}$  is generated:
  - Sample  $\mathbf{R}_i = [\mathbf{R}_{i,1} \mid \dots \mid \mathbf{R}_{i,\ell}] \leftarrow_{\$} \{-1, 1\}^{(h \times m)^\ell}$  for  $i \in [2]$
  - Output  $\mathbf{B}_i := \mathbf{A}\mathbf{R}_i + (\mathbf{x}_i^*)^\top \otimes \mathbf{G} \bmod q$  for  $i \in [2]$ .

More compactly, we have that

$$\mathbf{B} = [\mathbf{B}_1 \mid \mathbf{B}_2] = \mathbf{A} \underbrace{[\mathbf{R}_1 \mid \mathbf{R}_2]}_{=: \mathbf{R}} + (\mathbf{x}^*)^\top \otimes \mathbf{G} \bmod q.$$

Since  $h \geq (n+1) \log q + \omega(\log n)$ , indistinguishability ( $\text{H}_{5,\ell} \approx_s \text{H}_6$ ) follows from Lemma 3.

- $\text{H}_7$ : This is the same as  $\text{H}_6$ , except for the following modification to  $\text{KGen}$  queries:
  - recall that  $(\mathbf{B} - \mathbf{x}^\top \otimes \mathbf{G})\mathbf{H}_{\mathbf{B},f,\mathbf{x}} = \mathbf{B}_f - f(\mathbf{x})\mathbf{G} \bmod q$ , which holds for any  $\mathbf{x} \in \{0, 1\}^{2\ell}$  and that a valid adversary can only make  $\text{KGen}$  queries for functions  $f$  for which  $f(\mathbf{x}^*) = 1$ . Using these facts, one has that

$$\begin{aligned} [\mathbf{A} \mid \mathbf{B}_f] &= [\mathbf{A} \mid (\mathbf{B} - (\mathbf{x}^*)^\top \otimes \mathbf{G})\mathbf{H}_{\mathbf{B},f,\mathbf{x}^*} + f(\mathbf{x}^*)\mathbf{G}] \\ &= [\mathbf{A} \mid (\mathbf{A}[\mathbf{R}_1 \mid \mathbf{R}_2] + (\mathbf{x}^*)^\top \otimes \mathbf{G} - (\mathbf{x}^*)^\top \otimes \mathbf{G})\mathbf{H}_{\mathbf{B},f,\mathbf{x}^*} + f(\mathbf{x}^*)\mathbf{G}] \\ &= [\mathbf{A} \mid \underbrace{\mathbf{A}[\mathbf{R}_1 \mid \mathbf{R}_2]\mathbf{H}_{\mathbf{B},f,\mathbf{x}^*}}_{\mathbf{R}_f} + \mathbf{G}] \\ &= [\mathbf{A} \mid \mathbf{A}\mathbf{R}_f + \mathbf{G}] \bmod q. \end{aligned}$$

- compute  $\mathbf{T}_f = \begin{bmatrix} -\mathbf{R}_f \\ \mathbf{I} \end{bmatrix}$  and observe that  $[\mathbf{A} \mid \mathbf{B}_f]\mathbf{T}_f = \mathbf{G} \bmod q$ .
- compute

$$\mathbf{u}_f \leftarrow \text{SampPre}([\mathbf{A} \mid \mathbf{B}_f], \mathbf{T}_f, \mathbf{u}, \tau),$$

to answer  $\text{KGen}$  queries. This works as long as  $\tau \geq \ell h^3 m^{O(d)} \geq O(h^2 \|\mathbf{R}_f\|)$ . Therefore, since  $\tau$  satisfies such constraint by our choice of parameters, we have that  $\text{H}_6 \approx_s \text{H}_7$ . Notice that the reduction does not use  $\text{td}_{\mathbf{A}}$  anymore.

- $\text{H}_8$ : This is the same as  $\text{H}_7$ , except for the following modification to  $\mathbf{A}$  in  $\text{pp}$ :
  - sample  $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$  instead of  $(\mathbf{A}, \text{td}_{\mathbf{A}}) \leftarrow_{\$} \text{TrapGen}(1^n, q)$

By the property of  $\text{TrapGen}$  algorithm (Section 3.3), the distribution of  $\mathbf{A}$  is statistically indistinguishable between  $\text{H}_7$  and  $\text{H}_8$ . Therefore,  $\text{H}_7 \approx_s \text{H}_8$ .

- $\text{H}_9$ : This is the same as  $\text{H}_8$ , except  $(\mathbf{C}_{1,h})_{h \in [\ell]}, (\mathbf{C}_{2,h,x_{\text{cid}^*},j_2^*,h})_{h \in [\ell]}$  in the challenge ciphertext are changed as follows:
  - compute  $\mathbf{C}_0$  and  $\mathbf{c}$  as before,
  - sample  $\mathbf{E}_{1,h} \leftarrow_{\$} \hat{\chi}^{k \times m}$ ,  $\mathbf{E}_{2,h,x_{\text{cid}^*},j_2^*,h} \leftarrow_{\$} \hat{\chi}^{k \times m}$  for all  $h \in [\ell]$ ,
  - set  $\mathbf{C}_{1,h} := \mathbf{C}_0 \mathbf{R}_{1,h} + \mathbf{E}_{1,h}$ ,  $\text{ct}_{h,x_{\text{cid}^*},j_2^*,h} := \mathbf{C}_0 \mathbf{R}_{2,h} + \mathbf{E}_{2,h,x_{\text{cid}^*},j_2^*,h}$ , for all  $h \in [\ell]$ .

By noise flooding, we have that the distribution of  $(\mathbf{C}_{1,h})_{h \in [\ell]}, (\mathbf{ct}_{1,h,x_{\text{cid}^*},j_2^*,h})_{h \in [\ell]}$  in  $\mathbf{H}_8$  and  $\mathbf{H}_9$  are statistically close, as long as  $\hat{\chi} \geq \lambda^{\omega(1)} \lambda m \chi \geq \lambda^{\omega(1)} \|\mathbf{E}_0 \mathbf{R}_{i,h}\|$ , for  $i \in [2]$ .

- $\mathbf{H}_{10}$ : This is the same as  $\mathbf{H}_9$ , except for the following modification to  $\mathbf{C}_0$ , and  $\mathbf{c}_3$  in the challenge ciphertext:

– sample  $\mathbf{C}_0 \leftarrow \mathbb{Z}_q^{k \times h}, \mathbf{c} \leftarrow \mathbb{Z}_q^k$ .

To show that  $\mathbf{H}_9 \approx_c \mathbf{H}_{10}$ , one reduced to  $\text{LWE}_{k,n,m+1,\chi,q}$ . In particular, the reduction works as follows:

- it parses  $\mathbf{M} = [\mathbf{M}_0 \mid \mathbf{m}_1] \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$  and  $\mathbf{N} = [\mathbf{N}_0 \mid \mathbf{n}_1] \in \mathbb{Z}_q^{k \times m} \times \mathbb{Z}_q^k$  obtained from the  $\text{LWE}_{k,n,m+1,\chi,q}$  instance,
- it sets  $\mathbf{A} := \mathbf{M}_0$  and  $\mathbf{u} := \mathbf{m}_1$  in pp,
- it sets  $\mathbf{C}_0 := \mathbf{N}_0$  and  $\mathbf{c}_3 := \mathbf{n}_1$ .

Observe that

- if  $(\mathbf{M}, \mathbf{N})$  is a structured  $\text{LWE}_{k,n,m+1,\chi,q}$  instance, the view of the adversary  $\mathcal{A}$  is identical to  $\mathbf{H}_9$ ;
- if  $(\mathbf{M}, \mathbf{N})$  is a uniform random instance, the view of  $\mathcal{A}$  is identical to  $\mathbf{H}_{10}$ .

We conclude that  $\mathbf{H}_9 \approx_c \mathbf{H}_{10}$ .

Since the message  $\mu_b$  and the challenge bit  $b$  are perfectly hidden in  $\mathbf{H}_{10}$ , this concludes the proof.  $\square$

*Remark 3.* We believe it is possible to remove the random oracle in the above construction. The strategy inspired by the lattice-based IBE literature would be the following:

- We add a uniform random matrix to epk, say  $\mathbf{F}$ .
- In  $\text{Enc}_{\text{main}}$ , the encryption component  $\hat{\mathbf{C}}_{2,j,b}$  is produced by encrypting  $[\mathbf{D} \mid \mathbf{F} + H(\text{cid}) \mathbf{G}]_{2,j,b}$  (i.e., the (j,b)-th block row of  $[\mathbf{D} \mid \mathbf{F} + H(\text{cid}) \mathbf{G}]$ ), where  $H$  denote some appropriate function mapping cid's to matrices.
- $\text{Enc}_{\text{sub}}$  produces the ciphertext for  $(\text{cid}, \mathbf{x}_2)$  by sampling a preimage with respect to the matrix  $[\mathbf{D} \mid \mathbf{F} + H(\text{cid}) \mathbf{G}]_{\mathbf{x}_2}$  (i.e., selecting the block-rows of  $[\mathbf{D} \mid \mathbf{F} + H(\text{cid}) \mathbf{G}]$  that corresponds to the bits of the attribute  $\mathbf{x}_2$ ). This is done by sampling  $\mathbf{D}$  with a corresponding trapdoor, and using such a trapdoor.
- In the security proof, we would sample a random short matrix  $\mathbf{R}$  and set  $\mathbf{F} = \mathbf{D} \cdot \mathbf{R} - H_{\text{cid}^*, \mathbf{x}_2} \mathbf{G}$ , where  $H_{\text{cid}^*, \mathbf{x}_2}$  is a matrix such that the block-rows corresponding to  $\mathbf{1} - \mathbf{x}_2$  are zeros so that we can rely on LWE to prove pseudorandomness of the corresponding  $\hat{\mathbf{C}}$  components, whereas the block-rows corresponding to  $\mathbf{x}_2$  form a full-rank matrix, so that the sampling algorithm can still be run (using  $\mathbf{R}$  as trapdoor) to produce the challenge ciphertext component associated to  $\text{Enc}_{\text{sub}}$ .

A property required from the function  $H$  is that any subset of rows of  $H(\text{cid}) - H(\text{cid}')$  form a primitive matrix for  $\text{cid} \neq \text{cid}'$ . Such functions exist in the literature (e.g., [ABB10, Section 5]).

## 6 MA-ABE

We construct an MA-ABE scheme based on the techniques from [Wee22] on CP-ABE.

<p><b>Setup</b>(<math>1^\lambda</math>)</p> <hr/> $\mathbf{P} \leftarrow \mathbb{Z}_q^{n \times m}$ , $\mathbf{Q} \leftarrow \mathbb{Z}_q^{n \times m}$ , $\mathbf{u} \leftarrow \chi_{(0)}^m$ <b>return</b> $\text{pp} := (\mathbf{P}, \mathbf{Q}, \mathbf{u})$ <hr/> <p><b>KGen</b>(<math>\text{pp}, \text{apk}, \text{ask}, \text{uid}, \mathbf{x}</math>)</p> <hr/> <b>parse</b> $((\mathbf{A}, \mathbf{B}), \text{td}_A) \leftarrow (\text{apk}, \text{ask})$ $(\mathbf{K}_{\text{uid}}, \mathbf{K}_{\text{uid}}) := H(\text{uid})$ $\mathbf{M} := \begin{pmatrix} \mathbf{P}\mathbf{K}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ (\mathbf{B} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{K}_{\text{uid}} \end{pmatrix} \bmod q$ $\mathbf{U} \leftarrow \text{SampPre}(\mathbf{A}, \text{td}_A, \mathbf{M}, \tau)$ <b>return</b> $\text{sk} := (\mathbf{U}, \mathbf{x}, \mathbf{K}_{\text{uid}}, \mathbf{K}_{\text{uid}})$ <hr/> <p><b>Enc</b>(<math>\text{pp}, (\text{apk}_i)_{i \in [k]}, f, \mu</math>)</p> <hr/> <b>parse</b> $(\mathbf{A}_i, \mathbf{B}_i)_{i \in [k]} \leftarrow (\text{apk}_i)_{i \in [k]}$ $\mathbf{B} := (\mathbf{B}_1 \mid \dots \mid \mathbf{B}_k)$ $\mathbf{H}_{\mathbf{B}, f} \leftarrow \text{EvalF}(\mathbf{B}, f)$ , $\mathbf{B}_f := \mathbf{B}\mathbf{H}_{\mathbf{B}, f}$ $\mathbf{s} \leftarrow \mathbb{Z}_q^{nm}$ , $\mathbf{e}_0 \leftarrow \chi_{(1)}^{km}$ , $\mathbf{e} \leftarrow \chi_{(1)}^m$ $\mathbf{s}_i \leftarrow \mathbb{Z}_q^n$ , $\mathbf{e}_i \leftarrow \chi_{(1)}^{2m(m+1)}$ , $\forall i \in [k]$ $\mathbf{c}_i^\top := (\mathbf{s}_i^\top \mid \mathbf{s}^\top)\mathbf{A}_i + \mathbf{e}_i^\top \bmod q$ , $\forall i \in [k]$ $\mathbf{c}_0^\top := (\mathbf{s}_1^\top \mid \dots \mid \mathbf{s}_k^\top)(\mathbf{I}_k \otimes \mathbf{Q}) + \mathbf{e}_0^\top \bmod q$ $\mathbf{c}^\top := \sum_{i \in [k]} \mathbf{s}_i^\top \mathbf{P} + \mathbf{s}^\top (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mathbf{e}^\top + \mu \mathbf{g}^\top \bmod q$ <b>return</b> $\text{ctxt} := (\mathbf{c}, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_k)$	<p><b>AuthSetup</b>(<math>\text{pp}</math>)</p> <hr/> $(\mathbf{A}, \text{td}_A) \leftarrow \text{TrapGen}(1^{n(m+1)}, q)$ , $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m\ell}$ $\parallel \mathbf{A} \in \mathbb{Z}_q^{n(m+1) \times 2m(m+1)}$ <b>return</b> $(\text{apk}, \text{ask}) := ((\mathbf{A}, \mathbf{B}), \text{td}_A)$ <hr/> <p><b>Dec</b>(<math>\text{pp}, (\text{apk}_i)_{i \in [k]}, (\text{sk}_i)_{i \in [k]}, \text{ctxt}</math>)</p> <hr/> <b>for</b> $i \in [k]$ <b>do</b> <b>parse</b> $(\mathbf{A}_i, \mathbf{B}_i) \leftarrow \text{apk}_i$ <b>parse</b> $(\mathbf{U}_i, \mathbf{x}_i, \mathbf{K}_{\text{uid}}, \mathbf{K}_{\text{uid}}) \leftarrow \text{sk}_i$ <b>parse</b> $(\mathbf{c}, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_k) \leftarrow \text{ctxt}$ $(\mathbf{c}_{0,1}^\top \mid \dots \mid \mathbf{c}_{0,k}^\top) := \mathbf{c}_0^\top$ $\mathbf{B} := (\mathbf{B}_1 \mid \dots \mid \mathbf{B}_k)$ $\mathbf{x}^\top := (\mathbf{x}_1^\top \mid \dots \mid \mathbf{x}_k^\top)$ $\mathbf{H}_{\mathbf{B}, f, \mathbf{x}} \leftarrow \text{EvalFX}(\mathbf{B}, f, \mathbf{x})$ <b>for</b> $i \in [k]$ <b>do</b> $(d_{i,0} \mid \mathbf{d}_{i,1}^\top) := \mathbf{c}_i^\top \mathbf{U}_i \bmod q$ $\mathbf{d}_{i,2}^\top := \mathbf{d}_{i,1}^\top - \mathbf{c}_{0,i}^\top \mathbf{K}_{\text{uid}} \bmod q$ $z_0 := \sum_{i \in [k]} d_{i,0} \bmod q$ $z_1 := (\mathbf{d}_{1,2}^\top \mid \dots \mid \mathbf{d}_{k,2}^\top) \mathbf{H}_{\mathbf{B}, f, \mathbf{x}} \mathbf{u} \bmod q$ $z_2 := \mathbf{c}^\top \mathbf{K}_{\text{uid}} \bmod q$ $y := z_2 - z_1 - z_0 \bmod q$ <b>return</b> $( y  \geq \beta_0)$
---	---

Figure 9: MA-ABE construction  $\Pi_{\text{MA}}$ .

**Construction.** Let  $H : \{0, 1\}^* \rightarrow \chi_{(1)}^m \times \chi_{(1)}^{m \times m\ell}$  be a random oracle.<sup>17</sup> In Fig. 9 is our MA-ABE construction  $\Pi_{\text{MA}}$  for polynomial-size circuits with any depth  $d = d(\lambda) = \text{poly}(\lambda)$ . It supports attribute space  $\mathcal{X} = \{0, 1\}^\ell$ ,  $\ell = \ell(\lambda) = \text{poly}(\lambda)$ , and the class  $\mathcal{F}$  of  $\ell$ -input  $\text{poly}(\lambda)$ -size circuits of depth at most  $d$ .

**Theorem 3** (Correctness). *For parameters as in Table 4,  $\Pi_{\text{MA}}$  is correct.*

*Proof.* For each of the  $i$ -th secret key the decryptor computes

$$\begin{aligned} (d_{i,0} \mid \mathbf{d}_{i,1}^\top) &= \mathbf{c}_i^\top \mathbf{U}_i \bmod q \\ &\approx (\mathbf{s}_i^\top \mathbf{P} \mathbf{K}_{\text{uid}} \mid \mathbf{s}_i^\top \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{s}^\top ((\mathbf{B}_i - \mathbf{x}_i^\top \otimes \mathbf{G}) \otimes \mathbf{K}_{\text{uid}})) \bmod q \end{aligned}$$

with approximation error  $\mathbf{e}_i^\top \cdot \mathbf{U}_i$ . Let  $\mathbf{U}_i = (\mathbf{u}_{i,0} \mid \mathbf{U}_{i,1})$ , then

$$\begin{aligned} \mathbf{d}_{i,2}^\top &= \mathbf{d}_{i,1}^\top - \mathbf{c}_{0,i}^\top \mathbf{K}_{\text{uid}} \bmod q \\ &= \mathbf{s}_i^\top \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{s}^\top ((\mathbf{B}_i - \mathbf{x}_i^\top \otimes \mathbf{G}) \otimes \mathbf{K}_{\text{uid}}) + \mathbf{e}_i^\top \mathbf{U}_{i,1} - (\mathbf{s}_i^\top \mathbf{Q} + \mathbf{e}_0^\top) \mathbf{K}_{\text{uid}} \bmod q \\ &\approx \mathbf{s}^\top ((\mathbf{B}_i - \mathbf{x}_i^\top \otimes \mathbf{G}) \otimes \mathbf{K}_{\text{uid}}) \bmod q \end{aligned}$$

with approximation error  $\mathbf{e}_i^\top \mathbf{U}_{i,1} + \mathbf{e}_0^\top \mathbf{K}_{\text{uid}}$ . We have  $z_0 \approx \sum_{i \in [k]} \mathbf{s}_i^\top \mathbf{P} \mathbf{K}_{\text{uid}} \bmod q$ , with approximation error  $\sum_{i \in [k]} \mathbf{e}_i^\top \cdot \mathbf{u}_{i,0}$ ,

$$\begin{aligned} z_1 &= (\mathbf{d}_{1,2}^\top \mid \dots \mid \mathbf{d}_{k,2}^\top) \cdot \mathbf{H}_{\mathbf{B}, f, \mathbf{x}} \mathbf{u} \bmod q \\ &= (\mathbf{s}^\top ((\mathbf{B} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{K}_{\text{uid}}) + (\mathbf{e}_1^\top \mathbf{U}_{1,1} + \mathbf{e}_0^\top \mathbf{K}_{\text{uid}} \mid \dots \mid \mathbf{e}_k^\top \mathbf{U}_{k,1} + \mathbf{e}_0^\top \mathbf{K}_{\text{uid}})) \end{aligned}$$

<sup>17</sup>We refer to Remark 4 for a short discussion on how the random oracle can plausibly be removed.

**Table 4:** Parameters and shorthands for MA-ABE scheme (Section 6).

$n \in \mathbb{N}$		Parameter for matrix dimension
$m \in \mathbb{N}$	$= n \lceil \log q \rceil$	Parameter for matrix dimension
$\ell \in \mathbb{N}$		Attribute length per authority
$k \in \mathbb{N}$		Number of authorities
$\beta_0$	$\geq \text{poly}(\lambda, m) \chi_{(1)}^2 (k\tau + 2\ell m^{O(d)} \chi_{(0)})$	Correctness bound
$q$	$\geq \lambda^{\omega(1)} \cdot \beta_0$	Modulus
$\tau$		Parameter of KGen algorithm
$\chi_{(1)}$	$\geq O(\lambda)$	Gaussian width of $\mathbf{u}$ , $\mathbf{k}_{\text{uid}}$ , $\mathbf{K}_{\text{uid}}$ , $\mathbf{e}$ , $\mathbf{e}_0 = (\mathbf{e}_{i,Q})_i$ , $(\mathbf{e}_i)_{i \in [k]}$ , and of $\tilde{\mathbf{e}}_{\text{uid},i,P}$ in proofs
$\chi_{(2)}$	$\geq \lambda^{\omega(1)} \cdot \chi_{(1)}^2$	Gaussian width of $\mathbf{e}_{\text{uid},i,B}$ , $\mathbf{e}_{\text{uid},i,P}$ , $\mathbf{e}_{\text{uid},i,Q}$ in proofs
$\chi_{(3)}$	$\geq \lambda^{\omega(1)} \cdot \chi_{(2)} \cdot m^{O(d)}$	Gaussian width of $e_{i^*,\text{uid},P}$ in proofs
$\mathcal{I}, z$	$z :=  [k] \setminus \mathcal{I} $	Set $\mathcal{I}$ of corrupt authorities in proofs
$\text{param}_0$	$(q, k, n(m+1), 2m(m+1), (k+m)n, (k+1)m, \mathcal{S}_0, \chi_{(1)}, (\text{poly}(\lambda), \chi_{(1)}, \psi_i, \tau)_{i \in [k]})$ where $\psi_1 = \chi_{(3)}$ , $\psi_i = \chi_{(2)}$ , $i \neq 1$	Evasive LWE parameter
$\text{param}_1$	$(q, z, n(m+1), 2m(m+1), zn, (z+1)m, \mathcal{S}_1, \chi_{(1)}, (\text{poly}(\lambda), \chi_{(1)}, \psi_i, \tau)_{i \in [z]})$ where $\psi_{i^*} = \chi_{(3)}$ , $\psi_i = \chi_{(2)}$ , $i \neq i^*$	Evasive LWE parameter

$$\begin{aligned}
& \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}} \mathbf{u} \bmod q \\
& \approx (\mathbf{s}^T ((\mathbf{B} - \mathbf{x}^T \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{uid}})) \cdot (\mathbf{H}_{\mathbf{B},f,\mathbf{x}} \otimes \mathbf{1}) \mathbf{u} \bmod q \\
& = \mathbf{s}^T \cdot \underbrace{((\mathbf{B}_f - f(\mathbf{x}) \mathbf{G}) \mathbf{u} \otimes \mathbf{k}_{\text{uid}})}_{=0} \bmod q \\
& = \mathbf{s}^T (\mathbf{B}_f \otimes \mathbf{k}_{\text{uid}}) \bmod q,
\end{aligned}$$

with approximation error  $((\mathbf{e}_1^T \mathbf{U}_{1,1} \mid \dots \mid \mathbf{e}_k^T \mathbf{U}_{k,1}) + \mathbf{e}_0^T (\mathbf{I}_k \otimes \mathbf{K}_{\text{uid}})) \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}} \mathbf{u}$ ,

$$\begin{aligned}
z_2 = \mathbf{c}^T \mathbf{k}_{\text{uid}} &= \left( \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mathbf{e}^T + \mu \mathbf{g}^T \right) \cdot \mathbf{k}_{\text{uid}} \\
&\approx \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{k}_{\text{uid}}) + \mu \mathbf{g}^T \mathbf{k}_{\text{uid}}
\end{aligned}$$

with approximation error  $\mathbf{e}^T \mathbf{k}_{\text{uid}}$ . Therefore

$$y \approx \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{k}_{\text{uid}}) + \mu \mathbf{g}^T \mathbf{k}_{\text{uid}} - \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} - \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{k}_{\text{uid}}) = \mu \mathbf{g}^T \mathbf{k}_{\text{uid}} \bmod q,$$

where the error term involved in  $y$  is given by

$$\mathbf{e}^T \mathbf{k}_{\text{uid}} + \sum_{i \in [k]} \mathbf{e}_i^T \cdot \mathbf{u}_{i,0} + ((\mathbf{e}_1^T \mathbf{U}_{1,1} \mid \dots \mid \mathbf{e}_k^T \mathbf{U}_{k,1}) + \mathbf{e}_0^T (\mathbf{I}_k \otimes \mathbf{K}_{\text{uid}})) \mathbf{H}_{\mathbf{B},f,\mathbf{x}} \mathbf{u}$$

and whose norm is upper-bounded by

$$\beta_0 \geq \text{poly}(\lambda, m) \cdot (\chi_{(1)} \cdot \chi_{(1)} + k \cdot \chi_{(1)} \cdot \tau + \chi_{(1)} \cdot \ell \cdot m^{O(d)} \cdot \chi_{(0)} + \chi_{(1)}^2 \cdot m^{O(d)} \cdot \chi_{(0)}).$$

Since  $\mathbf{k}_{\text{uid}}$  is random short,  $\mathbf{g}^T \mathbf{k}_{\text{uid}}$  is statistically close to uniform over  $\mathbb{Z}_q$ , and correctness follows as long as  $q \geq \beta_0 \lambda^{\omega(1)}$ .  $\square$



## 6.1 Security

We present the security proof for the MA-ABE construction. W.l.o.g. we assume the adversary only queries keys from authorities  $i \in [k]$  which are associated to the challenge ciphertext. We recall some notation: We let  $\mathcal{U}$  be the set of all uid every queried by an adversary, and  $\mathcal{I}_{\text{uid}} \subseteq [k]$  be the set of authorities from whom the adversary requests a secret key for user uid.

We will also use the following notation: We let  $\mathbf{A}_i = \begin{pmatrix} \overline{\mathbf{A}}_i \\ \underline{\mathbf{A}}_i \end{pmatrix}$  where  $\overline{\mathbf{A}}_i \in \mathbb{Z}_q^{n \times 2m(m+1)}$  and  $\underline{\mathbf{A}}_i \in \mathbb{Z}_q^{nm \times 2m(m+1)}$  are the ‘‘top part’’ and ‘‘bottom part’’ of  $\mathbf{A}_i$  respectively. For ease of exposition, for any matrices  $\mathbf{A}$  and  $\mathbf{B}$  we abuse notation and write  $\mathbf{A}^{-1}(\mathbf{B})$  for an element in the domain  $\mathbf{A}^{-1}(\mathbf{B})$  output by  $\text{SampPre}(\text{td}_{\mathbf{A}}, \mathbf{B})$ . We use the shorthand  $\hat{\mathbf{B}}_{\text{uid},i} = \mathbf{B}_i - \mathbf{x}_{\text{uid},i}^{\text{T}} \otimes \mathbf{G}$  for any query  $\mathbf{x}_{\text{uid},i}$  on the  $i$ -th authority associated to uid.

**Theorem 4** (Security). *For parameters as in Table 4,  $\Pi_{\text{MA}}$  is IND-CPA-secure without missing keys (Definition 5) assuming*

$$\begin{aligned} & \text{LWE}_{n,2m(m+2),q,\mathcal{X}(1)}, & & \text{LWE}_{m,\text{poly}(n),q,\mathcal{X}(2),\mathcal{X}(1)}, \\ & \text{TensorLWE}_{n,km+1,q,\mathcal{X}(2),\mathcal{X}(1),\ell,\mathcal{Q}}, & & \text{EvasiveLWE}_{\text{param}_0} \quad \text{and} \quad \text{EvasiveLWE}_{\text{param}_1} \end{aligned}$$

in the (non-programmable) random oracle model.

*Proof.* Recall that in the experiment in Fig. 4, (at least) one of the two cases below holds:

- (1)  $b_{\text{honest\_security}} = 1$ , that is, all authorities  $i \in [k]$  involved in the challenge ciphertext  $\text{ctxt}^*$  are not corrupt by the adversary, and  $f^*(\mathbf{x}_{\text{uid},1}, \dots, \mathbf{x}_{\text{uid},k}) = 1$  for all  $\text{uid} \in \mathcal{U}$ . In this case, due to Remark 2, it suffices to consider the case where the adversary queries all  $k$  authorities for secret keys for all uid, so that  $\mathcal{I}_{\text{uid}} = [k]$  for all uid.
- (2)  $b_{\text{corrupt\_security}} = 1$ , that is, for all  $\text{uid} \in \mathcal{U}$  there exists an honest authority  $i \in [k]$  such that a key  $\text{sk}_{\text{uid},i}$  from  $i$  has not been queried.

Below we focus on that Case (1) happens. That of Case (2) is analogous, we defer repeating the very similar arguments to Section A.1.

We define the following sequence of hybrids<sup>18</sup>:

- $\text{Hyb}_{b,0}^{(h)}$ : This is the real security experiment for the scheme in Fig. 9, encrypting  $\mu_b$ , and conditioned on that  $b_{\text{honest\_security}} = 1$ .

Recall that in this hybrid the adversary is given the following:

$$\begin{aligned} & (\mathbf{B}_i)_{i \in [k]}, (\mathbf{A}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ & \mathbf{U}_{\text{uid},i} = \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ & \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \quad \forall i \in [k], \text{uid} \in \mathcal{U} \\ & \mathbf{c}_i^{\text{T}} = (\mathbf{s}_i^{\text{T}} \mid \mathbf{s}^{\text{T}}) \mathbf{A}_i + \mathbf{e}_i^{\text{T}} \quad \forall i \in [k] \\ & \mathbf{c}_0^{\text{T}} = (\mathbf{s}_1^{\text{T}} \mid \dots \mid \mathbf{s}_k^{\text{T}}) (\mathbf{I}_k \otimes \mathbf{Q}) + \mathbf{e}_0^{\text{T}} \\ & \mathbf{c}^{\text{T}} = \sum_{i \in [k]} \mathbf{s}_i^{\text{T}} \mathbf{P} + \mathbf{s}^{\text{T}} (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mathbf{e}^{\text{T}} + \mu \mathbf{g}^{\text{T}} \end{aligned}$$

where all terms are sampled according to the distribution as in the scheme. We recall each  $\mathbf{U}_{\text{uid},i}$  is sampled with  $\text{td}_{\mathbf{A}_i}$ . Below we write  $\mathbf{c}_0^{\text{T}} = (\mathbf{c}_{1,Q}^{\text{T}} \mid \dots \mid \mathbf{c}_{k,Q}^{\text{T}})$  where  $\mathbf{c}_{i,Q}^{\text{T}} = \mathbf{s}_i^{\text{T}} \mathbf{Q} + \mathbf{e}_{i,Q}^{\text{T}}$ .

<sup>18</sup>We use the superscript  $(h)$  to identify Case (1) honest authorities. In the continued proof we use  $(c)$  to identify Case (2) corrupt authorities.

- $\text{Hyb}_{b,1}^{(h)}$ : Same as  $\text{Hyb}_{b,0}^{(h)}$ , except that for all  $i \in [k]$ ,  $\mathbf{A}_i$  is sampled uniformly randomly and all (entries of the) corresponding preimages  $\mathbf{U}_{\text{uid},i}$  are sampled (inefficiently) from the Gaussian distribution with parameter  $\tau$ , subject to

$$\mathbf{A}_i \mathbf{U}_{\text{uid},i} = \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}.$$

We have  $\text{Hyb}_{b,0}^{(h)} \stackrel{s}{\approx} \text{Hyb}_{b,1}^{(h)}$  by the properties of  $\text{TrapGen}$  from Section 3.3.

- $\text{Hyb}_{b,2}^{(h)}$ : Same as  $\text{Hyb}_{b,1}^{(h)}$ , except that  $(\mathbf{c}_i)_{i \in [k]}$ ,  $\mathbf{c}_0, \mathbf{c}$  are sampled uniformly randomly.

We show in the following that  $\text{Hyb}_{b,1}^{(h)} \stackrel{s}{\approx} \text{Hyb}_{b,2}^{(h)}$ . Then, the theorem follows from noting that  $\text{Hyb}_{0,2}^{(h)} \stackrel{p}{=} \text{Hyb}_{1,2}^{(h)}$ , since in both hybrids the component  $\mathbf{c}$  in the challenge ciphertext is chosen uniformly randomly.

Define the distribution

$$\mathcal{D}_{1,1}^{(h)} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{A}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ \left( \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \right)_{i \in [k], \text{uid} \in \mathcal{U}} \\ ((\mathbf{s}_i^T | \mathbf{s}^T) \mathbf{A}_i + \mathbf{e}_i^T)_{i \in [k]} \\ (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T)_{i \in [k]} \\ \mathbf{c}^T = \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mathbf{e}^T \end{pmatrix} \quad (1)$$

where all terms are distributed same as in  $\text{Hyb}_{b,1}^{(h)}$ . Define also the distribution

$$\mathcal{D}_{2,1}^{(h)} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{A}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ \left( \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \right)_{i \in [k], \text{uid} \in \mathcal{U}} \\ (\mathbf{c}_i^T)_{i \in [k]} \\ (\mathbf{c}_{i,Q}^T)_{i \in [k]} \\ \mathbf{c}^T \end{pmatrix} \quad (2)$$

where all elements are distributed same as in  $\text{Hyb}_{b,2}^{(h)}$ , i.e. this is same as  $\mathcal{D}_{1,1}^{(h)}$  except that  $(\mathbf{c}_i^T, \mathbf{c}_{i,Q}^T)_{i \in [k]}$  and  $\mathbf{c}$  are all uniformly random.

Suppose there exists a PPT  $\mathcal{A}$  that distinguishes  $\text{Hyb}_{b,1}^{(h)}$  and  $\text{Hyb}_{b,2}^{(h)}$  with non-negligible probability. It is easy to verify that there then exists a PPT  $\mathcal{B}$  that distinguishes  $\mathcal{D}_{1,1}^{(h)}$  and  $\mathcal{D}_{2,1}^{(h)}$  defined above with non-negligible probability.

Now consider a PPT  $\text{Samp}$  which on input  $\lambda$  outputs the following:

$$\tilde{\mathbf{A}} := \left[ \begin{pmatrix} \mathbf{1} \otimes \mathbf{P} \\ \mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m \end{pmatrix} \mid \begin{pmatrix} \mathbf{I}_k \otimes \mathbf{Q} \\ \mathbf{0} \end{pmatrix} \right], \quad \tilde{\mathbf{P}}_i := \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}_{\text{uid} \in \mathcal{U}} \quad \forall i \in [k]$$

where  $\mathbf{1} \in \{0, 1\}^k$  is the all-one vector, and  $\text{aux}$  containing  $(\mathbf{B}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u}$  together with all random coins used.

By the  $\text{EvasiveLWE}_{\text{param}_0}$  assumption (c.f. Table 4) w.r.t.  $\text{Samp}$ , there exists a PPT  $\mathcal{E}$  that distinguishes the distributions  $\mathcal{D}_{1,2}^{(h)}$  and  $\mathcal{D}_{2,2}^{(h)}$  with non-negligible probability, where  $\mathcal{D}_{1,2}^{(h)}$  and  $\mathcal{D}_{2,2}^{(h)}$  are defined as follows:

$$\mathcal{D}_{1,2}^{(h)} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{A}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ \left( \mathbf{s}_i^T \mathbf{P}\mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}, \mathbf{s}_i^T \mathbf{Q}\mathbf{K}_{\text{uid}} + \mathbf{s}^T (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},i,B}^T \right)_{i \in [k], \text{uid} \in \mathcal{U}}, \\ (\mathbf{s}_i^T \tilde{\mathbf{A}}_i + \mathbf{s}^T \tilde{\mathbf{A}}_i + \mathbf{e}_i^T)_{i \in [k]} \\ (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T)_{i \in [k]} \\ \mathbf{c}^T = \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mathbf{e}^T \end{pmatrix} \quad (3)$$

where all terms are distributed as in  $\mathcal{D}_{1,1}$ , additionally  $e_{1,\text{uid},P} \leftarrow_{\S} \chi(3)$ ,  $e_{\text{uid},i,P} \leftarrow_{\S} \chi(2)$  for all  $i \neq 1$ , and  $\mathbf{e}_{\text{uid},i,B} \leftarrow_{\S} \chi_{(2)}^{m\ell}$  for all  $i$ .

$$\mathcal{D}_{2,2}^{(h)} := \left( \begin{array}{c} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{A}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ \left( c_{\text{uid},i,P}, \mathbf{c}_{\text{uid},i,B}^T \right)_{i \in [k], \text{uid} \in \mathcal{U}}, \\ \left( \mathbf{c}_{i,A}^T \right)_{i \in [k]} \\ \left( \mathbf{c}_{i,Q}^T \right)_{i \in [k]} \\ \mathbf{c}^T \end{array} \right) \quad (4)$$

which is same as  $\mathcal{D}_{1,2}^{(h)}$  except that  $(\mathbf{c}_i^T, \mathbf{c}_{i,Q}^T)_{i \in [k]}$  and  $\mathbf{c}$  are all uniformly random. However, under the  $\text{LWE}_{n,2m(m+2),q,\chi(1)}$  and  $\text{TensorLWE}_{n,km+1,q,\chi(2),\chi(1),\ell,\mathcal{Q}}$  assumptions, this is not possible by Lemma 5. Thus we have a contradiction.

Similarly, in Section A.1 we show that Case (2) happening would contradict either of the  $\text{LWE}_{n,2m(m+2),q,\chi(1)}$ ,  $\text{LWE}_{m,\text{poly}(n),q,\chi(2),\chi(1)}$ , and  $\text{EvasiveLWE}_{\text{param}_1}$  assumptions, the latter with appropriate parameters. The theorem then follows.  $\square$

**Lemma 5.** *For the distributions  $\mathcal{D}_{1,2}^{(h)}$  and  $\mathcal{D}_{2,2}^{(h)}$  defined in Eq. (3) and Eq. (4), we have  $\mathcal{D}_{1,2}^{(h)} \stackrel{c}{\approx} \mathcal{D}_{2,2}^{(h)}$  assuming*

$$\text{LWE}_{n,2m(m+2),q,\chi(1)}, \quad \text{LWE}_{m,\text{poly}(n),q,\chi(2),\chi(1)}, \quad \text{and} \quad \text{TensorLWE}_{n,km+1,q,\chi(2),\chi(1),\ell,\mathcal{Q}}.$$

*Proof.* We consider the following sequence of hybrid distributions:

- $\mathcal{D}_{1,2}^{(h)}$  as in Eq. (3).
- $\mathcal{D}_{1,2,1}$ : For each  $\text{uid} \in \mathcal{U}$ , we swap  $\mathbf{s}_1^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{1,\text{uid},P}$  to

$$\begin{aligned} & \left( \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mathbf{e}^T \right) \mathbf{k}_{\text{uid}} - \left( \sum_{i \in [2,k]} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \right) \\ & - (\mathbf{s}^T (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},i,B}^T)_{i \in [k]} \mathbf{H}_{\mathbf{B},f,\mathbf{x}_{\text{uid}}} \mathbf{u} + \mathbf{s}^T (\mathbf{G} \mathbf{u} \otimes \mathbf{k}_{\text{uid}}) + e_{\text{uid},G} + e_{1,\text{uid},P} \end{aligned}$$

where  $(\mathbf{s}^T (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},i,B}^T)_{i \in [k]}$  is the horizontal concatenation of  $\mathbf{s}^T (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},i,B}^T$  for all  $i \in [k]$ , and  $e_{\text{uid},G} \leftarrow_{\S} \chi(2)$ .

We have  $\mathcal{D}_{1,2}^{(h)} \stackrel{c}{\approx} \mathcal{D}_{1,2,1}$  by noise flooding, which is due to the equality

$$\begin{aligned} \mathbf{s}_1^T \mathbf{P} \mathbf{k}_{\text{uid}} &= \left( \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) \right) \mathbf{k}_{\text{uid}} - \sum_{i \in [2,k]} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} \\ &\quad - (\mathbf{s}^T (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}))_{i \in [k]} \mathbf{H}_{\mathbf{B},f,\mathbf{x}_{\text{uid}}} \mathbf{u} + \mathbf{s}^T (\mathbf{G} \mathbf{u} \otimes \mathbf{k}_{\text{uid}}) \end{aligned}$$

and that

$$e_{1,\text{uid},P} \stackrel{c}{\approx} \mathbf{e}^T \mathbf{k}_{\text{uid}} - \sum_{i \in [2,k]} e_{\text{uid},i,P} - (\mathbf{e}_{\text{uid},i,B}^T)_{i \in [k]} \mathbf{H}_{\mathbf{B},f,\mathbf{x}_{\text{uid}}} \mathbf{u} + e_{\text{uid},G} + e_{1,\text{uid},P}$$

since

$$\begin{aligned} \chi(3) &\geq \lambda^{\omega(1)} \text{poly}(\lambda, m) \left( \chi_{(1)}^2 + k\chi(2) + \chi(0)\chi(2)\ell m^{O(d)} \right) \\ &\geq \lambda^{\omega(1)} \left\| \mathbf{e}^T \mathbf{k}_{\text{uid}} - \sum_{i \in [2,k]} e_{\text{uid},i,P} - (\mathbf{e}_{\text{uid},i,B}^T)_{i \in [k]} \mathbf{H}_{\mathbf{B},f,\mathbf{x}_{\text{uid}}} \mathbf{u} + e_{\text{uid},G} \right\| \end{aligned}$$

Notice that the only remaining terms in  $\mathcal{D}_{1,2,1}$  involving  $\mathbf{s}_1$  are  $\mathbf{s}_1^\top \overline{\mathbf{A}}_1 + \overline{\mathbf{e}}_{1,A}^\top$ ,  $\mathbf{s}_1^\top \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{s}^\top (\hat{\mathbf{B}}_{\text{uid},1} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},1,B}^\top$ ,  $\mathbf{s}_1^\top \mathbf{Q} + \mathbf{e}_{1,Q}^\top$  and  $\mathbf{s}_1^\top \mathbf{P} + \mathbf{e}^\top$ . Also, looking ahead, to argue the above simulation is pseudorandom, it suffices to argue  $\mathbf{s}^\top (\mathbf{G} \mathbf{u} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},G}^\top$  is.

- $\mathcal{D}_{1,2,2}$ : For all  $\text{uid} \in \mathcal{U}$ , all  $i \in [k]$ , we swap

$$\begin{aligned} & \mathbf{s}_i^\top \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{s}^\top (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},i,B}^\top \\ \text{to } & (\mathbf{s}_i^\top \mathbf{Q} + \mathbf{e}_{i,Q}^\top) \mathbf{K}_{\text{uid}} + \mathbf{s}^\top (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},i,B}^\top. \end{aligned}$$

We have  $\mathcal{D}_{1,2,1} \stackrel{\approx}{\approx} \mathcal{D}_{1,2,2}$  by noise flooding, since  $\chi_{(2)} \geq \lambda^{\omega(1)} \cdot \lambda \cdot \chi_{(1)} \cdot \chi_{(1)} \cdot n \geq \lambda^{\omega(1)} \cdot \|\mathbf{e}_{i,Q}^\top \cdot \mathbf{K}_{\text{uid}}\|$ . Now in  $\mathcal{D}_{1,2,2}$  the remaining terms involving  $\mathbf{s}_1$  are  $\mathbf{s}_1^\top \overline{\mathbf{A}}_1 + \overline{\mathbf{e}}_{1,A}^\top$ ,  $\mathbf{s}_1^\top \mathbf{Q} + \mathbf{e}_{1,Q}^\top$  and  $\mathbf{s}_1^\top \mathbf{P} + \mathbf{e}_{1,P}^\top$ .

- $\mathcal{D}_{1,2,3}$ : We swap

$$\mathbf{s}_1^\top \overline{\mathbf{A}}_1 + \overline{\mathbf{e}}_1^\top, \quad \mathbf{s}_1^\top \mathbf{Q} + \mathbf{e}_{1,Q}^\top \quad \text{and} \quad \mathbf{s}_1^\top \mathbf{P} + \mathbf{e}^\top$$

to uniformly random.

We have  $\mathcal{D}_{1,2,2} \stackrel{\approx}{\approx} \mathcal{D}_{1,2,3}$  by the  $\text{LWE}_{n,2m(m+2),q,\chi_{(1)}}$  assumption.

Notice that as a result  $\mathbf{c}$  is also uniformly random.

- $\mathcal{D}_{1,2,4}$ : For each  $i \in [2, k]$  and all  $\text{uid} \in \mathcal{U}$ , we swap

$$\mathbf{s}_i^\top \mathbf{P} \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \quad \text{to} \quad (\mathbf{s}_i^\top \mathbf{P} + \tilde{\mathbf{e}}_{\text{uid},i,P}^\top) \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}.$$

where  $\tilde{\mathbf{e}}_{\text{uid},i,P} \leftarrow \chi_{(1)}^m$ .

We have  $\mathcal{D}_{1,2,3} \stackrel{\approx}{\approx} \mathcal{D}_{1,2,4}$  by noise flooding, due to  $\tilde{\mathbf{e}}_{\text{uid},i,P}^\top \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \stackrel{\approx}{\approx} e_{\text{uid},i,P}$  since  $\chi_{(2)} \geq \lambda^{\omega(1)} \lambda^2 \chi_{(1)}^2 \geq \lambda^{\omega(1)} \|\tilde{\mathbf{e}}_{\text{uid},i,P}^\top \mathbf{k}_{\text{uid}}\|$ .

- $\mathcal{D}_{1,2,5}$ : For each  $i \in [2, k]$  and all  $\text{uid} \in \mathcal{U}$ , we swap

$$(\mathbf{s}_i^\top \mathbf{P} + \tilde{\mathbf{e}}_{\text{uid},i,P}^\top) \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \quad \text{to} \quad \mathbf{b}_{\text{uid},i,P}^\top \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$$

where  $\mathbf{b}_{\text{uid},i,P}^\top$  is uniformly random, and we also swap

$$\mathbf{s}_i^\top \overline{\mathbf{A}}_i + \overline{\mathbf{e}}_i^\top \quad \text{and} \quad \mathbf{s}_i^\top \mathbf{Q} + \mathbf{e}_{i,Q}^\top$$

to uniformly random.

We have  $\mathcal{D}_{1,2,4} \stackrel{\approx}{\approx} \mathcal{D}_{1,2,5}$  by the  $\text{LWE}_{n,2m(m+2),q,\chi_{(1)}}$  assumption.

- $\mathcal{D}_{1,2,6}$ : For all  $\text{uid} \in \mathcal{U}$ , all  $i \in [k] \setminus \{1\}$ , we swap

$$\mathbf{b}_{i,P}^\top \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$$

to uniformly random.

We have  $\mathcal{D}_{1,2,5} \stackrel{\approx}{\approx} \mathcal{D}_{1,2,6}$  by the (low-norm)  $\text{LWE}_{m,\text{poly}(n),q,\chi_{(2)},\chi_{(1)}}$  assumption.

- $\mathcal{D}_{1,2,7}$ : For all  $i \in [k]$ , all  $\text{uid} \in \mathcal{U}$ , we swap the terms

$$(\mathbf{s}_i^\top \mathbf{Q} + \mathbf{e}_{i,Q}^\top) \mathbf{K}_{\text{uid}} + \mathbf{s}^\top (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}}) + \mathbf{e}_{\text{uid},i,B}^\top \quad \text{and} \quad \mathbf{s}^\top (\mathbf{G} \mathbf{u} \otimes \mathbf{k}_{\text{uid}}) + e_{\text{uid},G}$$

to uniformly random.

Note that  $\mathbf{G} \mathbf{u} \bmod q$  is statistically close to uniformly random. Then, we have  $\mathcal{D}_{1,2,6} \stackrel{\approx}{\approx} \mathcal{D}_{1,2,7}$  by the  $\text{TensorLWE}_{n,km+1,q,\chi_{(2)},\chi_{(1)},\ell,\mathcal{Q}}$  assumption (applied on LWE samples with secret  $\mathbf{s}$ ), where the set  $\mathcal{Q}$  contains all queries  $\mathbf{x}_{\text{uid},i}$  from the adversary.

Observe that  $\mathcal{D}_{1,2,7} \stackrel{\text{d}}{=} \mathcal{D}_{2,2}^{(h)}$  in Eq. (12), which concludes the proof.  $\square$

*Remark 4* (Removing RO). The work of Waters, Wee, and Wu [WWW22] showed how to construct MA-ABE for subset policies from lattices in the standard model, i.e. without random oracles. They achieved this by instantiating the random oracle with a subset product of public low-norm matrices, and relying on the fact that multiplying a secret key by such subset products (plus noise) yields a pseudorandom function (PRF) [BLMR13], in addition to the evasive LWE assumption. We believe similar techniques can be applied to our construction in Fig. 9 to remove the random oracle. More concretely,  $H(\text{uid})$  can be instantiated as the PRF of [BLMR13], so that  $\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}}$  are replaced by  $\prod_j \mathbf{X}_{\text{uid}_j}, \prod_j \mathbf{Y}_{\text{uid}_j}$  respectively, where  $\mathbf{X}_{\text{uid}_j}, \mathbf{Y}_{\text{uid}_j}$  are random low-norm matrices and  $\text{uid} = (\text{uid}_j)_j$ . Invoking the evasive LWE assumption, one is left to argue pseudorandomness of the LWE samples of the forms  $\underbrace{\mathbf{s}_i^T \mathbf{P} \cdot \prod_j \mathbf{X}_{\text{uid}_j}, \mathbf{s}_i^T \mathbf{Q} \cdot \prod_j \mathbf{Y}_{\text{uid}_j} + \mathbf{s}^T (\hat{\mathbf{B}}_{\text{uid},i} \otimes \prod_j \mathbf{X}_{\text{uid}_j})}_{\text{are not bound to the hash/PRF values}}$  (and some more that are not bound to the hash/PRF values), which can be handled by a hybrid argument analogous to that of Lemma 5. We note that handling the term  $\mathbf{s}^T (\hat{\mathbf{B}}_{\text{uid},i} \otimes \prod_j \mathbf{X}_{\text{uid}_j})$  requires a strengthening of the tensor LWE assumption. However, since this is not the focus of this work, we do not attempt formalisation.

## 7 MC-ABE

We construct an MC-ABE scheme, which combines the techniques from both [BGG<sup>+</sup>14] and [Wee22].

**Construction.** Let  $H : \{0, 1\}^* \rightarrow \chi_{(0)}^m \times \chi_{(0)}^{m \times m\ell}$  be a random oracle.<sup>19</sup> In Fig. 10 is our MC-ABE construction  $\Pi_{\text{MC}}$  for polynomial-size circuits with any depth  $d = d(\lambda) = \text{poly}(\lambda)$ . It supports attribute space  $\mathcal{X} = \{0, 1\}^\ell$ ,  $\ell = \ell(\lambda) = \text{poly}(\lambda)$ , and the class  $\mathcal{F}$  of  $\ell$ -input  $\text{poly}(\lambda)$ -size circuits of depth at most  $d$ .

**Theorem 5** (Correctness). *For parameters as in Table 5,  $\Pi_{\text{MC}}$  is correct.*

*Proof.* During decryption, the decryptor computes for each  $i \in [k] \setminus \{1\}$

$$\begin{aligned} (d_{i,0} \mid \mathbf{d}_{i,1}^T) &= \mathbf{c}_i^T \cdot \mathbf{U}_i \\ &= (\mathbf{s}^T \mathbf{C}_i + \mathbf{e}_i^T) \cdot \mathbf{U}_i \\ &\approx (\mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}} \mid \mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{s}^T ((\mathbf{B}_i - \mathbf{x}_i \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}})) \bmod q, \end{aligned}$$

with approximation error  $\mathbf{e}_i^T \cdot \mathbf{U}_i$ . Let  $\mathbf{U}_i = (\mathbf{u}_{i,0} \mid \mathbf{U}_{i,1})$ , hence

$$\begin{aligned} \mathbf{d}_{i,2}^T &= \mathbf{d}_{i,1}^T - \mathbf{c}_{0,i}^T \mathbf{K}_{\text{cid}} \bmod q \\ &= \mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{s}^T ((\mathbf{B}_i - \mathbf{x}_i^T \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_i^T \mathbf{U}_{i,1} - (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_0^T) \mathbf{K}_{\text{cid}} \bmod q \\ &\approx \mathbf{s}^T ((\mathbf{B}_i - \mathbf{x}_i^T \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}}) \bmod q \end{aligned}$$

with approximation error  $\mathbf{e}_i^T \mathbf{U}_{i,1} + \mathbf{e}_0^T \mathbf{K}_{\text{cid}}$ . We have

$$z_0 \approx \sum_{i=2}^k \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}} \bmod q$$

with approximation error  $\sum_{i=2}^k \mathbf{e}_i^T \cdot \mathbf{u}_{i,0}$ , Hence

$$\mathbf{z}_1^T = (\mathbf{c}_1^T \mid \mathbf{d}_{2,2}^T \mid \dots \mid \mathbf{d}_{k,2}^T) \mathbf{H}_{\mathbf{B},f,\mathbf{x}} \bmod q$$

<sup>19</sup>The discussion in Remark 4 again applies here.

<p><b>Setup</b>(<math>1^\lambda</math>)</p> <hr/> $\mathbf{B}_i \leftarrow \mathbb{Z}_q^{n \times m\ell} \forall i \in [k]$ $\mathbf{P} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{Q} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{v} \leftarrow \mathbb{Z}_q^n$ <b>return</b> $\text{pp} := ((\mathbf{B}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, \mathbf{v})$ <p><b>AuthSetup</b>(<math>\text{pp}</math>)</p> <hr/> $(\mathbf{A}, \text{td}_\mathbf{A}) \leftarrow \text{TrapGen}(1^n, q) \quad // \mathbf{A} \in \mathbb{Z}_q^{n \times 2m}$ <b>return</b> $(\text{apk}, \text{ask}) := (\mathbf{A}, \text{td}_\mathbf{A})$ <p><b>KGen</b>(<math>\text{pp}, \text{ask}, f</math>)</p> <hr/> <b>parse</b> $\text{td}_\mathbf{A} \leftarrow \text{ask}$ $\mathbf{H}_{\mathbf{B},f} \leftarrow \text{EvalF}(\mathbf{B}, f), \mathbf{B}_f := \mathbf{B}\mathbf{H}_{\mathbf{B},f}$ $\mathbf{r}_f \leftarrow \text{SampPre}(\text{td}_{(\mathbf{A} \mathbf{B}_f)}, \mathbf{v}, \sigma)$ <b>return</b> $\text{sk}_f := (\mathbf{r}_f, f)$ <p><b>EKGen</b>(<math>\text{pp}</math>)</p> <hr/> $(\mathbf{C}, \text{td}_\mathbf{C}) \leftarrow \text{TrapGen}(1^{n(m+1)}, q)$ $// \mathbf{C} \in \mathbb{Z}_q^{n(m+1) \times 2m(m+1)}$ <b>return</b> $(\text{epk}, \text{esk}) := (\mathbf{C}, \text{td}_\mathbf{C})$ <p><b>Enc<sub>sub</sub></b>(<math>\text{pp}, i, \text{esk}, \text{cid}, \mathbf{x}</math>)</p> <hr/> $(\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}}) := H(\text{cid})$ $\mathbf{M} := \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ (\mathbf{B}_i - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}} \end{pmatrix} \bmod q$ $\mathbf{U} \leftarrow \text{SampPre}(\text{td}_\mathbf{C}, \mathbf{M}, \tau)$ <b>return</b> $\text{ctxt}_i := (\mathbf{U}, \mathbf{x}, \mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})$	<p><b>Enc<sub>main</sub></b>(<math>\text{pp}, \text{apk}, (\text{epk}_i)_{i \in [k] \setminus \{1\}}, \text{cid}, \mathbf{x}, \mu</math>)</p> <hr/> <b>parse</b> $\mathbf{A} \leftarrow \text{apk}, \mathbf{C}_i \leftarrow \text{epk}_i \forall i \in [k] \setminus \{1\}$ $(\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}}) := H(\text{cid}); \mathbf{s}_i \leftarrow \mathbb{Z}_q^n; \mathbf{s} \leftarrow \mathbb{Z}_q^{nm}$ $\mathbf{e} \leftarrow \mathbb{Z}_q^m, \hat{\mathbf{e}} \leftarrow \mathbb{Z}_q^{2m}, \mathbf{e}_0 \leftarrow \mathbb{Z}_q^{km}, \mathbf{e}_1 \leftarrow \mathbb{Z}_q^{m\ell}$ $\mathbf{e}_i \leftarrow \mathbb{Z}_q^{2m(m+1)} \forall i \in \cup[k] \setminus \{1\}$ $\hat{\mathbf{c}}^\top := \mathbf{s}^\top(\mathbf{A} \otimes \mathbf{k}_{\text{cid}}) + \hat{\mathbf{e}}^\top$ $\mathbf{c}_1^\top := \mathbf{s}^\top((\mathbf{B}_1 - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_1^\top$ $\mathbf{c}_i^\top := (\mathbf{s}_i^\top   \mathbf{s}^\top) \mathbf{C}_i + \mathbf{e}_i^\top \forall i \in [k] \setminus \{1\}$ $\mathbf{c}_0^\top := (\mathbf{s}_2^\top   \dots   \mathbf{s}_k^\top)(\mathbf{I}_{k-1} \otimes \mathbf{Q}) + \mathbf{e}_0^\top \bmod q$ $\mathbf{c}^\top = \sum_{i=2}^k \mathbf{s}_i^\top \mathbf{P} + \mathbf{s}^\top(\mathbf{v} \otimes \mathbf{I}_m) + \mathbf{e}^\top + \mu \mathbf{g}^\top \bmod q$ <b>return</b> $\text{ctxt}_1 := ((\mathbf{c}_i)_{i \in \{0\} \cup [k]}, \hat{\mathbf{c}}, \mathbf{c}, \mathbf{x}, \mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})$ <p><b>Dec</b>(<math>\text{pp}, \text{sk}_f, (\text{ctxt}_i)_{i \in [k]}</math>)</p> <hr/> <b>parse</b> $(\mathbf{r}_f, f) \leftarrow \text{sk}_f$ <b>parse</b> $((\mathbf{c}_i)_{i \in \{0\} \cup [k]}, \hat{\mathbf{c}}, \mathbf{c}, \mathbf{x}_1, \mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}}) \leftarrow \text{ctxt}_1$ $(\mathbf{c}_{0,2}^\top   \dots   \mathbf{c}_{0,k}^\top) := \mathbf{c}_0^\top$ <b>for</b> $i \in [k] \setminus \{1\}$ <b>do</b> <b>parse</b> $(\mathbf{U}_i, \mathbf{x}_i, \mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}}) \leftarrow \text{ctxt}_i$ $(d_{i,0}   \mathbf{d}_{i,1}^\top) := \mathbf{c}_i^\top \cdot \mathbf{U}_i \bmod q$ $\mathbf{d}_{i,2}^\top := \mathbf{d}_{i,1}^\top - \mathbf{c}_{0,i}^\top \mathbf{K}_{\text{cid}} \bmod q$ $\mathbf{B} := (\mathbf{B}_1   \dots   \mathbf{B}_k), \mathbf{x}^\top := (\mathbf{x}_1^\top   \dots   \mathbf{x}_k^\top)$ $\mathbf{H}_{\mathbf{B},f,\mathbf{x}} \leftarrow \text{EvalFX}(\mathbf{B}, f, \mathbf{x})$ $z_0 := \sum_{i=2}^k d_{i,0} \bmod q$ $\mathbf{z}_1^\top := (\mathbf{c}_1^\top   \mathbf{d}_{2,2}^\top   \dots   \mathbf{d}_{k,2}^\top) \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}} \bmod q$ $y := \mathbf{c}^\top \mathbf{k}_{\text{cid}} - z_0 - (\hat{\mathbf{c}}^\top   \mathbf{z}_1^\top) \cdot \mathbf{r}_f \bmod q$ <b>return</b> $( y  \geq \beta_0)$
--	--

Figure 10: MC-ABE construction  $\Pi_{\text{MC}}$ .

$$\begin{aligned}
&\approx \mathbf{s}^\top((\mathbf{B} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}})(\mathbf{H}_{\mathbf{B},f,\mathbf{x}} \otimes \mathbf{1}) \bmod q \\
&= \mathbf{s}^\top((\mathbf{B}_f - \underbrace{f(\mathbf{x})}_{=0} \mathbf{G}) \otimes \mathbf{k}_{\text{cid}}) \bmod q \\
&= \mathbf{s}^\top(\mathbf{B}_f \otimes \mathbf{k}_{\text{cid}}) \bmod q,
\end{aligned}$$

with approximation error  $(\mathbf{e}_1^\top | (\mathbf{e}_2^\top \mathbf{U}_{2,1} | \dots | \mathbf{e}_k^\top \mathbf{U}_{k,1}) + \mathbf{e}_0^\top(\mathbf{I}_k \otimes \mathbf{K}_{\text{cid}})) \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}}$ . Therefore

$$\begin{aligned}
&(\mathbf{c}_0^\top | \mathbf{z}_1^\top) \cdot \mathbf{r}_f \\
&= (\mathbf{s}^\top((\mathbf{A} | \mathbf{B}_f) \otimes \mathbf{k}_{\text{cid}}) + (\mathbf{e}_0^\top | (\mathbf{e}_1^\top | \mathbf{e}_2^\top \mathbf{U}_{2,1} | \dots | \mathbf{e}_k^\top \mathbf{U}_{k,1}) \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}})) \cdot \mathbf{r}_f \bmod q \\
&\approx \mathbf{s}^\top((\mathbf{A} | \mathbf{B}_f) \otimes \mathbf{k}_{\text{cid}}) \mathbf{r}_f \bmod q \\
&= \mathbf{s}^\top(\mathbf{v} \otimes \mathbf{k}_{\text{cid}}) \bmod q
\end{aligned}$$

with approximation error  $(\hat{\mathbf{e}}^\top | (\mathbf{e}_1^\top | (\mathbf{e}_2^\top \mathbf{U}_{2,1} | \dots | \mathbf{e}_k^\top \mathbf{U}_{k,1}) + \mathbf{e}_0^\top(\mathbf{I}_k \otimes \mathbf{K}_{\text{cid}})) \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}}) \cdot \mathbf{r}_f$ . We have

$$y \approx \left( \sum_{i=2}^k \mathbf{s}_i^\top \mathbf{P} + \mathbf{s}^\top(\mathbf{v} \otimes \mathbf{I}_m) + \mu \mathbf{g}^\top \right) \cdot \mathbf{k}_{\text{cid}} - \sum_{i=2}^k \mathbf{s}_i^\top \mathbf{P} \mathbf{k}_{\text{cid}} - \mathbf{s}^\top(\mathbf{v} \otimes \mathbf{k}_{\text{cid}}) \bmod q$$

**Table 5:** Parameters and shorthands for MC-ABE scheme (Section 7).

$n \in \mathbb{N}$	Parameter for matrix dimension
$m \in \mathbb{N}$ $n \lceil \log q \rceil$	Parameter for matrix dimension
$\ell \in \mathbb{N}$	Attribute length per encryptor
$k \in \mathbb{N}$	Number of encryptors
$\beta_0 \geq \text{poly}(\lambda, m) \cdot \chi_{(0)}(\chi_{(0)} + k\tau + \sigma + 2\tau\ell m^{O(d)} \cdot \sigma)$	Correctness bound
$q \geq \lambda^{\omega(1)} \beta_0$	Modulus
$\tau$	Parameter of $\text{Enc}_{\text{sub}}$ algorithm
$\sigma \geq \ell m^{O(d)}$	Parameter of KGen algorithm
$\chi_{(0)} \geq O(\lambda)$	Gaussian width of $\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}}, \mathbf{e}, \hat{\mathbf{e}}, (\mathbf{e}_i)_{i \in [k]}, \mathbf{e}_0 = (\mathbf{e}_{i,Q})_{i \in [2,k]}$ , and of $\mathbf{e}_{\text{cid},A}, \mathbf{e}_{\text{cid},i,P}, e_{f^*,\text{cid}}, \mathbf{e}_{\text{cid}^*,\text{cid},1,B}$ in proofs
$\chi_{(1)} \geq \lambda^{\omega(1)} \chi_{(0)}^2$	Gaussian width of $\mathbf{e}_{\text{cid},i,B}, e_{\text{cid},i,P}, \mathbf{e}_{\text{cid},i,Q}$ in proofs
$\chi_{(2)} \geq \lambda^{\omega(1)} \cdot \chi_{(1)} \cdot m^{O(d)}$	Gaussian width of $e_{i^*,\text{cid},P}$ in proofs
$\mathcal{J}, z \quad z :=  [2, k] \setminus \mathcal{J} $	Set $\mathcal{J}$ of corrupt encryptors in proofs
$\text{param}_0 (q, k-1, n(m+1), 2m(m+1), (k-1+m)n, \text{poly}(\lambda), \mathcal{S}_0, \chi_{(0)}, (\text{poly}(\lambda), \chi_{(0)}, \psi_i, \tau)_{i \in [2,k]})$ where $\psi_2 = \chi_{(2)}, \psi_i = \chi_{(1)}, i \neq 2$	Evasive LWE parameter
$\text{param}_1 (q, z, n(m+1), 2m(m+1), zn, (z+1)m, \mathcal{S}_1, \chi_{(0)}, (\text{poly}(\lambda), \chi_{(0)}, \psi_i, \tau)_{i \in [z]})$ where $\psi_{i^*} = \chi_{(2)}, \psi_i = \chi_{(1)}, i \neq i^*$	Evasive LWE parameter

$$= \mu \mathbf{g}^T \mathbf{k}_{\text{cid}} \bmod q,$$

where the error term involved in  $y$  is given by

$$\mathbf{e}^T \mathbf{k}_{\text{cid}} - \sum_{i=2}^k \mathbf{e}_i^T \cdot \mathbf{u}_{i,0} - (\hat{\mathbf{e}}^T | (\mathbf{e}_1^T | (\mathbf{e}_2^T \mathbf{U}_{2,1} | \dots | \mathbf{e}_k^T \mathbf{U}_{k,1}) + \mathbf{e}_0^T (\mathbf{I}_k \otimes \mathbf{K}_{\text{cid}})) \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}}) \cdot \mathbf{r}_f$$

and whose norm is upper-bounded by

$$\beta_0 \geq \text{poly}(\lambda, m) \cdot (\chi_{(0)}^2 + k \cdot \chi_{(0)} \cdot \tau + \chi_{(0)} \cdot \sigma + (\chi_{(0)} + \chi_{(0)}) \cdot \tau \cdot \ell \cdot m^{O(d)} \cdot \sigma)$$

Since  $\mathbf{k}_{\text{cid}}$  is random short,  $\mathbf{g}^T \cdot \mathbf{k}_{\text{cid}}$  is statistically close to uniform over  $\mathbb{Z}_q$ , and correctness follows as long as  $q \geq \beta_0 \lambda^{\omega(1)}$ .  $\square$

## 7.1 Security

We present the security proof for the MC-ABE construction. W.l.o.g. we assume the adversary only queries keys from encryptors  $i \in [2, k]$  which are associated to the challenge ciphertext. We recall some notation (analogous to that in the MA-ABE setting): We let  $\mathcal{C}$  be the set of all cid ever queried by the adversary, and  $\mathcal{J}_{\text{cid}} \subseteq [2, k]$  be the set of encryptors from whom the adversary requests a ciphertext for identity cid. Let  $\mathcal{F}$  denote the set of functions  $f$  queried to the authority by the adversary.

We will also use the following notation: We let  $\mathbf{C}_i = \begin{pmatrix} \overline{\mathbf{C}}_i \\ \underline{\mathbf{C}}_i \end{pmatrix}$ , where  $\overline{\mathbf{C}}_i \in \mathbb{Z}_q^{n \times 2m(m+1)}$

and  $\underline{\mathbf{C}}_i \in \mathbb{Z}_q^{nm \times 2m(m+1)}$  are the ‘‘top part’’ and ‘‘bottom part’’ of  $\mathbf{C}_i$  respectively. For ease of exposition, for any matrices  $\mathbf{A}$  and  $\mathbf{B}$  we abuse notation and write  $\mathbf{A}^{-1}(\mathbf{B})$  for an element in the domain  $\mathbf{A}^{-1}(\mathbf{B})$  output by  $\text{SampPre}(\text{td}_{\mathbf{A}}, \mathbf{B})$ . We use the shorthand  $\hat{\mathbf{B}}_{\text{cid},i} = \mathbf{B}_i - \mathbf{x}_{\text{cid},i}^T \otimes \mathbf{G}$  for any query  $\mathbf{x}_{\text{cid},i}$  on the  $i$ -th encryptor associated to cid.

**Theorem 6.** For parameters as in Table 5,  $\Pi_{\text{MC}}$  is IND-CPA-secure without missing ciphertexts (Definition 7) assuming

$$\begin{aligned} & \text{LWE}_{n,2m(m+2),q,\chi(0)}, & & \text{LWE}_{m,\text{poly}(n),q,\chi(1),\chi(0)}, \\ & \text{TensorLWE}_{n,(k+2)m+1,q,\chi(0),\chi(0),\ell,\mathcal{Q}}, & & \text{EvasiveLWE}_{\text{param}_0} \quad \text{and} \quad \text{EvasiveLWE}_{\text{param}_1} \end{aligned}$$

in the (non-programmable) random oracle model.

*Proof.* Recall that in the experiment in Fig. 5, (at least) one of the two cases below holds:

- (1)  $b_{\text{honest\_security}} = 1$ , that is, all encryptors  $i \in [k]$  involved in the challenge ciphertext  $\text{ctxt}^*$  are not corrupt by the adversary, and  $f(\mathbf{x}_{\text{cid}^*,1}, \dots, \mathbf{x}_{\text{cid}^*,k}) = 1$  for all  $f \in \mathcal{F}$ . In this case, due to Remark 2, it suffices to consider the case where the adversary queries all  $k - 1$  encryptors on ciphertext for all cid, so that  $\mathcal{J}_{\text{cid}} = [2, k]$  for all cid.
- (2)  $b_{\text{corrupt\_security}} = 1$ , that is, for all cid  $\in \mathcal{C}$  there exists an honest encryptor  $i \in [k]$  such that a ciphertext  $\text{ctxt}_{\text{cid},i,\mathbf{x}}$  from  $i$  has not been queried.

Below we focus on that Case (1) happens. That of Case (2) is analogous, we defer repeating the very similar arguments to Section B.2.

We define the following sequence of hybrids:

- $\text{Hyb}_{b,0}^{(h)}$ : This is the real very-selective security experiment for the scheme in Fig. 10, encrypting  $\mu_b$ .

Recall that in this hybrid the adversary is given the following:

$$\begin{aligned} & \mathbf{A}, (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v} \\ & \mathbf{r}_f = (\mathbf{A} \mid \mathbf{B}_f)^{-1}(\mathbf{v}) \quad \forall f \in \mathcal{F} \\ & \mathbf{U}_{\text{cid},i} = \mathbf{C}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix} \quad \forall \text{cid} \in \mathcal{C}, i \in [2, k] \\ & \hat{\mathbf{c}}^T = \mathbf{s}^T(\mathbf{A} \otimes \mathbf{k}_{\text{cid}^*}) + \hat{\mathbf{e}}^T \\ & \mathbf{c}_1^T = \mathbf{s}^T(\hat{\mathbf{B}}_{\text{cid}^*,1} \otimes \mathbf{k}_{\text{cid}^*}) + \mathbf{e}_1^T \\ & \mathbf{c}_i^T = (\mathbf{s}_i^T \mid \mathbf{s}^T)\mathbf{C}_i + \mathbf{e}_i^T \quad \forall i \in [2, k] \\ & \mathbf{c}_0^T := (\mathbf{s}_2^T \mid \dots \mid \mathbf{s}_k^T)(\mathbf{I}_{k-1} \otimes \mathbf{Q}) + \mathbf{e}_0^T \\ & \mathbf{c}^T = \sum_{i \in [2,k]} \mathbf{s}^T \mathbf{P} + \mathbf{s}^T(\mathbf{v} \otimes \mathbf{I}_m) + \mathbf{e}^T + \mu \cdot \mathbf{g}^T \end{aligned}$$

where all terms are sampled according to the distribution as in the scheme. We recall each  $\mathbf{r}_f$  is sampled with  $\text{td}_{\mathbf{A}}$ .

- $\text{Hyb}_{b,1}^{(h)}$ : We change how secret keys queries are answered. For a query on any  $f$ , do the following:
  - Let  $\mathbf{x}_{\text{cid}^*}^T := (\mathbf{x}_{\text{cid}^*,1}^T \mid \dots \mid \mathbf{x}_{\text{cid}^*,k}^T)$ , which satisfies  $f(\mathbf{x}_{\text{cid}^*}) = 1$  by design of security experiment. If, for any  $i \in [2, k]$ ,  $\mathbf{x}_{\text{cid}^*,i}$  has not been queried by the adversary, pick an arbitrary one such that the above holds.
  - Sample  $\mathbf{R} \leftarrow_{\$} \{0, 1\}^{m \times m\ell}$ , and let  $\mathbf{B} = (\mathbf{B}_1, \dots, \mathbf{B}_k) := \mathbf{A}\mathbf{R} + \mathbf{x}_{\text{cid}^*}^T \otimes \mathbf{G} \bmod q$ . Note that  $\mathbf{B} - \mathbf{x}_{\text{cid}^*}^T \otimes \mathbf{G} = \mathbf{A}\mathbf{R} \bmod q$ .
  - Compute  $\mathbf{H}_{\mathbf{B},f,\mathbf{x}_{\text{cid}^*}} \leftarrow \text{EvalFX}(\mathbf{B}, f, \mathbf{x}_{\text{cid}^*})$ . Let  $\mathbf{R}^* := \mathbf{R} \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}_{\text{cid}^*}}$ .
  - When answering  $\text{KGenO}(f)$  query, use  $\mathbf{R}^*$  as a gadget-trapdoor for  $(\mathbf{A} \mid \mathbf{B}_f)$  to generate  $\mathbf{r}_f = (\mathbf{A} \mid \mathbf{B}_f)^{-1}(\mathbf{v})$ . Note that this is possible since  $f(\mathbf{x}_{\text{cid}^*}) = 1$ , and hence  $\mathbf{B}_f = (\mathbf{B} - \mathbf{x}_{\text{cid}^*}^T \otimes \mathbf{G}) \cdot \mathbf{H}_{\mathbf{B},f,\mathbf{x}_{\text{cid}^*}} + f(\mathbf{x}_{\text{cid}^*})\mathbf{G} = \mathbf{A} \cdot \mathbf{R}^* + \mathbf{G} \bmod q$ .



We have  $\text{Hyb}_{b,0}^{(h)} \stackrel{s}{\approx} \text{Hyb}_{b,1}^{(h)}$  by the properties of TrapGen from Section 3.3.

- $\text{Hyb}_{b,2}^{(h)}$ : Same as  $\text{Hyb}_{b,1}^{(h)}$ , except that for all  $i \in [k]$ ,  $\mathbf{C}_i$  is sampled uniformly randomly and all (entries of the) corresponding preimages  $\mathbf{U}_{\text{cid},i}$  are sampled (inefficiently) from the Gaussian distribution with parameter  $\tau$ , subject to

$$\mathbf{C}_i \mathbf{U}_{\text{cid},i} = \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix}.$$

We have  $\text{Hyb}_{b,1}^{(h)} \stackrel{s}{\approx} \text{Hyb}_{b,2}^{(h)}$  by the properties of TrapGen from Section 3.3.

- $\text{Hyb}_{b,3}^{(h)}$ : Same as  $\text{Hyb}_{b,2}^{(h)}$ , except  $\hat{\mathbf{c}}, (\mathbf{c}_i)_{i \in [k]}, \mathbf{c}_0, \mathbf{c}$  are sampled uniformly randomly.

We show in the following that  $\text{Hyb}_{b,2}^{(h)} \stackrel{s}{\approx} \text{Hyb}_{b,3}^{(h)}$ . Then, the theorem follows from noting that  $\text{Hyb}_{0,3}^{(h)} \stackrel{p}{=} \text{Hyb}_{1,3}^{(h)}$ , since in both hybrids the component  $\mathbf{c}$  in the challenge ciphertext is chosen uniformly randomly.

W.l.o.g. assume  $\mathcal{C}$  contains  $\text{cid}^*$ . Define the distribution

$$\mathcal{D}_{1,1}^{(h)} := \left( \begin{array}{l} \mathbf{A}, \mathbf{R}, (\mathbf{C}_i)_{i \in [2,k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v}, \\ \left( \mathbf{C}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix} \right)_{i \in [2,k], \text{cid} \in \mathcal{C}} \\ (\mathbf{s}^T(\mathbf{A} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid},A}^T)_{\text{cid} \in \mathcal{C}}, (\mathbf{s}^T(\hat{\mathbf{B}}_{\text{cid}^*,1} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}^*,\text{cid},1,B}^T)_{\text{cid} \in \mathcal{C}} \\ ((\mathbf{s}_i^T \mid \mathbf{s}^T)\mathbf{C}_i + \mathbf{e}_i^T)_{i \in [2,k]} \\ (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T)_{i \in [2,k]} \\ \mathbf{c}^T = \sum_{i \in [2,k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T(\mathbf{v} \otimes \mathbf{I}_m) + \mathbf{e}^T \end{array} \right) \quad (5)$$

where all terms are distributed as in  $\text{Hyb}_{b,2}$ , and additionally  $\mathbf{e}_{\text{cid},A} \leftarrow_{\$} \chi_{(0)}^{2m}$ ,  $\mathbf{e}_{\text{cid}^*,\text{cid},1,B} \leftarrow_{\$} \chi_{(0)}^{m\ell}$ . Define also the distribution

$$\mathcal{D}_{2,1}^{(h)} := \left( \begin{array}{l} \mathbf{A}, \mathbf{R}, (\mathbf{C}_i)_{i \in [2,k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v}, \\ \left( \mathbf{C}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix} \right)_{i \in [2,k], \text{cid} \in \mathcal{C}} \\ (\mathbf{c}_{\text{cid},A}^T)_{\text{cid} \in \mathcal{C}}, (\mathbf{c}_{\text{cid}^*,\text{cid},1,B}^T)_{\text{cid} \in \mathcal{C}} \\ (\mathbf{c}_{i,C}^T)_{i \in [2,k]}, \\ (\mathbf{c}_{i,Q}^T)_{i \in [2,k]} \\ \mathbf{c}^T \end{array} \right) \quad (6)$$

where all elements are distributed same as in  $\text{Hyb}_{b,3}^{(h)}$ , i.e. this is same as  $\mathcal{D}_{1,1}^{(h)}$  except that  $(\mathbf{c}_{\text{cid},A}^T)_{\text{cid} \in \mathcal{C}}, (\mathbf{c}_{\text{cid}^*,\text{cid},1,B}^T)_{\text{cid} \in \mathcal{C}}, (\mathbf{c}_{i,C}^T)_{i \in [2,k]}, (\mathbf{c}_{i,Q}^T)_{i \in [2,k]}$  and  $\mathbf{c}$  are all uniformly random.

Suppose there exists a PPT  $\mathcal{A}$  that distinguishes  $\text{Hyb}_{b,2}^{(h)}$  and  $\text{Hyb}_{b,3}^{(h)}$  with non-negligible probability, it is easy to verify that then there exists a PPT  $\mathcal{B}$  that distinguishes  $\mathcal{D}_{1,1}^{(h)}$  and  $\mathcal{D}_{2,1}^{(h)}$  defined above with non-negligible probability. In more details, the only difference between the distribution in  $\text{Hyb}_{b,2}^{(h)}$  and  $\mathcal{D}_{1,1}^{(h)}$  is that  $\mathcal{D}_{1,1}^{(h)}$  additionally contains  $\mathbf{s}^T(\mathbf{A} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid},A}^T$  and  $\mathbf{s}^T(\hat{\mathbf{B}}_{\text{cid}^*,1} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}^*,\text{cid},1,B}^T$  for all  $\text{cid} \in \mathcal{C}$ . A trivial reduction simply hides these components. (These additional components will be used in the proof of Lemma 6.)

Now consider a PPT Samp which on input  $\lambda$  outputs the following:

$$\tilde{\mathbf{A}} := \left[ \begin{array}{c} \left( \mathbf{1} \otimes \mathbf{P} \right) \\ \left( \mathbf{v} \otimes \mathbf{I}_m \right) \end{array} \middle| \left( \mathbf{I}_{k-1} \otimes \mathbf{Q} \right) \middle| \left( \begin{array}{c} \mathbf{0} \\ \mathbf{A} \otimes \mathbf{k}_{\text{cid}} \end{array} \right)_{\text{cid} \in \mathcal{C}} \right],$$

$$\tilde{\mathbf{P}}_i := \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} & \mathbf{k}_{\text{cid}} \end{pmatrix}_{\text{cid} \in \mathcal{C}} \quad \forall i \in [2, k],$$

where  $\mathbf{1} \in \{0, 1\}^{k-1}$  is the all-one vector, and  $\text{aux}$  containing  $\mathbf{A}, \mathbf{R}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v}$  together with all random coins used.

By the  $\text{EvasiveLWE}_{\text{param}_0}$  assumption (c.f. Table 5), there then exists a PPT  $\mathcal{E}$  that distinguishes the distributions  $\mathcal{D}_{1,2}^{(h)}$  and  $\mathcal{D}_{2,2}^{(h)}$  with non-negligible probability, where  $\mathcal{D}_{1,2}^{(h)}$  and  $\mathcal{D}_{2,2}^{(h)}$  are defined as follows:

$$\mathcal{D}_{1,2}^{(h)} := \begin{pmatrix} \mathbf{A}, \mathbf{R}, (\mathbf{C}_i)_{i \in [2, k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v}, \\ \left( \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}} + e_{\text{cid}, i, P}, \mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}, i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}, i, B}^T \right)_{i \in [2, k], \text{cid} \in \mathcal{C}}, \\ \left( \mathbf{s}^T (\mathbf{A} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}, A}^T \right)_{\text{cid} \in \mathcal{C}}, \left( \mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}^*, 1} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}^*, \text{cid}, 1, B}^T \right)_{\text{cid} \in \mathcal{C}}, \\ \left( \mathbf{s}_i^T \mathbf{C}_i + \mathbf{s}^T \mathbf{C}_i + \mathbf{e}_i^T \right)_{i \in [2, k]}, \\ \left( \mathbf{c}_{i, Q}^T = \mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i, Q}^T \right)_{i \in [2, k]} \\ \sum_{i \in [2, k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{v} \otimes \mathbf{I}_m) + \mathbf{e}^T \end{pmatrix} \quad (7)$$

where all terms are distributed as in  $\mathcal{D}_{1,1}^{(h)}$ , additionally  $e_{2, \text{cid}, P} \leftarrow_{\$} \chi(2)$ ,  $e_{\text{cid}, i, P} \leftarrow_{\$} \chi(1)$  for all  $i \neq 2$ , and  $\mathbf{e}_{\text{cid}, i, B} \leftarrow_{\$} \chi_{(2)}^{m\ell}$ .

$$\mathcal{D}_{2,2}^{(h)} := \begin{pmatrix} \mathbf{A}, \mathbf{R}, (\mathbf{C}_i)_{i \in [2, k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v}, \\ \left( c_{\text{cid}, i, P}, \mathbf{c}_{\text{cid}, i, B}^T \right)_{i \in [2, k], \text{cid} \in \mathcal{C}}, \\ \left( \mathbf{c}_{\text{cid}, A}^T \right)_{\text{cid} \in \mathcal{C}}, \left( \mathbf{c}_{\text{cid}^*, \text{cid}, 1, B}^T \right)_{\text{cid} \in \mathcal{C}} \\ \left( \mathbf{c}_{i, C}^T \right)_{i \in [2, k]}, \\ \left( \mathbf{c}_{i, Q}^T \right)_{i \in [2, k]} \\ \mathbf{c}^T \end{pmatrix} \quad (8)$$

where  $(c_{\text{cid}, i, P}, \mathbf{c}_{\text{cid}, i, B}^T)_{i \in [2, k], \text{cid} \in \mathcal{C}}, (\mathbf{c}_{\text{cid}, A}^T)_{\text{cid} \in \mathcal{C}}, (\mathbf{c}_{\text{cid}^*, \text{cid}, 1, B}^T)_{\text{cid} \in \mathcal{C}}, (\mathbf{c}_{i, C}^T)_{i \in [2, k]}, (\mathbf{c}_{i, Q}^T)_{i \in [2, k]}$  and  $\mathbf{c}$  are all uniformly random.

But under the  $\text{LWE}_{n, 2m(m+2), q, \chi(0)}$  and  $\text{TensorLWE}_{n, (k+2)m+1, q, \chi(0), \chi(0), \ell, \mathcal{Q}}$  assumptions this is not possible by Lemma 6.

Similarly, in Section B.2 we show that Case (2) happening would contradict either of the  $\text{LWE}_{n, 2m(m+2), q, \chi(0)}$ ,  $\text{LWE}_{m, \text{poly}(n), q, \chi(1), \chi(0)}$  and  $\text{EvasiveLWE}_{\text{param}_1}$  assumptions, the latter with appropriate parameters. The theorem then follows.  $\square$

**Lemma 6.** *For the distributions  $\mathcal{D}_{1,2}^{(h)}$  and  $\mathcal{D}_{2,2}^{(h)}$  defined in Eq. (7) and Eq. (8), we have  $\mathcal{D}_{1,2}^{(h)} \stackrel{c}{\approx} \mathcal{D}_{2,2}^{(h)}$  assuming*

$$\text{LWE}_{n, 2m(m+2), q, \chi(0)} \quad \text{and} \quad \text{TensorLWE}_{n, (k+2)m+1, q, \chi(0), \chi(0), \ell, \mathcal{Q}}.$$

A proof of Lemma 6 is analogous to that of Lemma 5, which we defer to Section B.1.

## Acknowledgments

Russell W. F. Lai and Ivy K. Y. Woo are supported by the Research Council of Finland grants 358951 and 358950 respectively. We thank Chris Brzuska for helpful discussion at the early stage of this project.

## References

- [ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 553–572. Springer, Berlin, Heidelberg, May / June 2010. doi:10.1007/978-3-642-13190-5\_28.
- [ABG19] Michel Abdalla, Fabrice Benhamouda, and Romain Gay. From single-input to multi-client inner-product functional encryption. In Steven D. Galbraith and Shihoh Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 552–582. Springer, Cham, December 2019. doi:10.1007/978-3-030-34618-8\_19.
- [ABKW19] Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss, and Hendrik Waldner. Decentralizing inner-product functional encryption. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 128–157. Springer, Cham, April 2019. doi:10.1007/978-3-030-17259-6\_5.
- [AG23] Miguel Ambrona and Romain Gay. Multi-authority ABE for non-monotonic access structures. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *PKC 2023, Part II*, volume 13941 of *LNCS*, pages 306–335. Springer, Cham, May 2023. doi:10.1007/978-3-031-31371-4\_11.
- [AGT22] Shweta Agrawal, Rishab Goyal, and Junichi Tomida. Multi-input quadratic functional encryption: Stronger security, broader functionality. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 711–740. Springer, Cham, November 2022. doi:10.1007/978-3-031-22318-1\_25.
- [ARYY23] Shweta Agrawal, Mélissa Rossi, Anshu Yadav, and Shota Yamada. Constant input attribute based (and predicate) encryption from evasive and tensor LWE. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part IV*, volume 14084 of *LNCS*, pages 532–564. Springer, Cham, August 2023. doi:10.1007/978-3-031-38551-3\_17.
- [Ayy22] Shweta Agrawal, Anshu Yadav, and Shota Yamada. Multi-input attribute based encryption and predicate encryption. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 590–621. Springer, Cham, August 2022. doi:10.1007/978-3-031-15802-5\_21.
- [BGG<sup>+</sup>14] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 533–556. Springer, Berlin, Heidelberg, May 2014. doi:10.1007/978-3-642-55220-5\_30.
- [BJK<sup>+</sup>18] Zvika Brakerski, Aayush Jain, Ilan Komargodski, Alain Passelègue, and Daniel Wichs. Non-trivial witness encryption and null-iO from standard assumptions. In Dario Catalano and Roberto De Prisco, editors, *SCN 18*, volume 11035 of *LNCS*, pages 425–441. Springer, Cham, September 2018. doi:10.1007/978-3-319-98113-0\_23.
- [BLMR13] Dan Boneh, Kevin Lewi, Hart William Montgomery, and Ananth Raghunathan. Key homomorphic PRFs and their applications. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 410–428.

- Springer, Berlin, Heidelberg, August 2013. doi:[10.1007/978-3-642-40041-4\\_23](https://doi.org/10.1007/978-3-642-40041-4_23).
- [BUW24] Chris Brzuska, Akin Ünäl, and Ivy K. Y. Woo. Evasive lwe assumptions: Definitions, classes, and counterexamples. In *To appear in ASIACRYPT 2024*. Springer, 2024.
- [BV22] Zvika Brakerski and Vinod Vaikuntanathan. Lattice-inspired broadcast encryption and succinct ciphertext-policy ABE. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPICs*, pages 28:1–28:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. doi:[10.4230/LIPICs.ITCS.2022.28](https://doi.org/10.4230/LIPICs.ITCS.2022.28).
- [CDG<sup>+</sup>18] Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval. Decentralized multi-client functional encryption for inner product. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 703–732. Springer, Cham, December 2018. doi:[10.1007/978-3-030-03329-3\\_24](https://doi.org/10.1007/978-3-030-03329-3_24).
- [Cha07] Melissa Chase. Multi-authority attribute based encryption. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 515–534. Springer, Berlin, Heidelberg, February 2007. doi:[10.1007/978-3-540-70936-7\\_28](https://doi.org/10.1007/978-3-540-70936-7_28).
- [DKW21] Pratish Datta, Ilan Komargodski, and Brent Waters. Decentralized multi-authority ABE for DNFs from LWE. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 177–209. Springer, Cham, October 2021. doi:[10.1007/978-3-030-77870-5\\_7](https://doi.org/10.1007/978-3-030-77870-5_7).
- [DKW23a] Pratish Datta, Ilan Komargodski, and Brent Waters. Decentralized multi-authority ABE for NC<sup>1</sup> from BDH. *Journal of Cryptology*, 36(2):6, April 2023. doi:[10.1007/s00145-023-09445-7](https://doi.org/10.1007/s00145-023-09445-7).
- [DKW23b] Pratish Datta, Ilan Komargodski, and Brent Waters. Fully adaptive decentralized multi-authority ABE. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 447–478. Springer, Cham, April 2023. doi:[10.1007/978-3-031-30620-4\\_15](https://doi.org/10.1007/978-3-031-30620-4_15).
- [DRS04] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 523–540. Springer, Berlin, Heidelberg, May 2004. doi:[10.1007/978-3-540-24676-3\\_31](https://doi.org/10.1007/978-3-540-24676-3_31).
- [FFMV23] Danilo Francati, Daniele Friolo, Giulio Malavolta, and Daniele Venturi. Multi-key and multi-input predicate encryption from learning with errors. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 573–604. Springer, Cham, April 2023. doi:[10.1007/978-3-031-30620-4\\_19](https://doi.org/10.1007/978-3-031-30620-4_19).
- [FWW23] Cody Freitag, Brent Waters, and David J. Wu. How to use (plain) witness encryption: Registered ABE, flexible broadcast, and more. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part IV*, volume 14084 of *LNCS*, pages 498–531. Springer, Cham, August 2023. doi:[10.1007/978-3-031-38551-3\\_16](https://doi.org/10.1007/978-3-031-38551-3_16).

- [GGG<sup>+</sup>14] Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou. Multi-input functional encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 578–602. Springer, Berlin, Heidelberg, May 2014. doi:[10.1007/978-3-642-55220-5\\_32](https://doi.org/10.1007/978-3-642-55220-5_32).
- [GM18] Nicholas Genise and Daniele Micciancio. Faster Gaussian sampling for trapdoor lattices with arbitrary modulus. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 174–203. Springer, Cham, April / May 2018. doi:[10.1007/978-3-319-78381-9\\_7](https://doi.org/10.1007/978-3-319-78381-9_7).
- [GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008. doi:[10.1145/1374376.1374407](https://doi.org/10.1145/1374376.1374407).
- [GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 75–92. Springer, Berlin, Heidelberg, August 2013. doi:[10.1007/978-3-642-40041-4\\_5](https://doi.org/10.1007/978-3-642-40041-4_5).
- [Kim19] Sam Kim. Multi-authority attribute-based encryption from LWE in the OT model. Cryptology ePrint Archive, Report 2019/280, 2019. URL: <https://eprint.iacr.org/2019/280>.
- [LT19] Benoît Libert and Radu Titiu. Multi-client functional encryption for linear functions in the standard model from LWE. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 520–551. Springer, Cham, December 2019. doi:[10.1007/978-3-030-34618-8\\_18](https://doi.org/10.1007/978-3-030-34618-8_18).
- [LW11] Allison B. Lewko and Brent Waters. Decentralizing attribute-based encryption. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 568–588. Springer, Berlin, Heidelberg, May 2011. doi:[10.1007/978-3-642-20465-4\\_31](https://doi.org/10.1007/978-3-642-20465-4_31).
- [MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718. Springer, Berlin, Heidelberg, April 2012. doi:[10.1007/978-3-642-29011-4\\_41](https://doi.org/10.1007/978-3-642-29011-4_41).
- [NPP22] Ky Nguyen, Duong Hieu Phan, and David Pointcheval. Multi-client functional encryption with fine-grained access control. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part I*, volume 13791 of *LNCS*, pages 95–125. Springer, Cham, December 2022. doi:[10.1007/978-3-031-22963-3\\_4](https://doi.org/10.1007/978-3-031-22963-3_4).
- [Tsa22] Rotem Tsabary. Candidate witness encryption from lattice techniques. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 535–559. Springer, Cham, August 2022. doi:[10.1007/978-3-031-15802-5\\_19](https://doi.org/10.1007/978-3-031-15802-5_19).
- [VWW22] Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. Witness encryption and null-IO from evasive LWE. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part I*, volume 13791 of *LNCS*, pages 195–221. Springer, Cham, December 2022. doi:[10.1007/978-3-031-22963-3\\_7](https://doi.org/10.1007/978-3-031-22963-3_7).

- [Wee22] Hoeteck Wee. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 217–241. Springer, Cham, May / June 2022. doi:10.1007/978-3-031-07085-3\_8.
- [Wee23] Hoeteck Wee. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. Cryptology ePrint Archive, Report 2023/906, 2023. URL: <https://eprint.iacr.org/2023/906>.
- [WFL19] Zhedong Wang, Xiong Fan, and Feng-Hao Liu. FE for inner products and its application to decentralized ABE. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 97–127. Springer, Cham, April 2019. doi:10.1007/978-3-030-17259-6\_4.
- [WWW22] Brent Waters, Hoeteck Wee, and David J. Wu. Multi-authority ABE from lattices without random oracles. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 651–679. Springer, Cham, November 2022. doi:10.1007/978-3-031-22318-1\_23.

## A Proofs for MA-ABE

We provide the remaining proofs for the MA-ABE construction. For clarity we also restate the theorem appeared in the main content.

### A.1 Continued proof of Theorem 4 (corruption)

**Theorem 4 (Security).** *For parameters as in Table 4,  $\Pi_{\text{MA}}$  is IND-CPA-secure without missing keys (Definition 5) assuming*

$$\begin{aligned} & \text{LWE}_{n, 2m(m+2), q, \mathcal{X}(1)}, & & \text{LWE}_{m, \text{poly}(n), q, \mathcal{X}(2), \mathcal{X}(1)}, \\ & \text{TensorLWE}_{n, km+1, q, \mathcal{X}(2), \mathcal{X}(1), \ell, \mathcal{Q}}, & & \text{EvasiveLWE}_{\text{param}_0} \quad \text{and} \quad \text{EvasiveLWE}_{\text{param}_1} \end{aligned}$$

in the (non-programmable) random oracle model.

*Proof.* (Continued.) Below write  $\mathcal{I} = \mathcal{I}_{\text{corr}} \subset [k]$  for the set of corrupt authorities. In this continued proof we focus on that Case (2)  $b_{\text{corrupt\_security}} = 1$  happens. That is, for all  $\text{uid} \in \mathcal{U}$  there exists an honest authority  $i \in [k] \setminus \mathcal{I}$  such that a key  $\text{sk}_{\text{uid}, i}$  from  $i$  has not been queried.

Fix arbitrary honest authority  $i^* \in [k] \setminus \mathcal{I}$ , which exists since  $[k] \neq \mathcal{I}$ . For each  $\text{uid} \in \mathcal{U}$ , denote by  $\tilde{i}_{\text{uid}}$  an arbitrarily fixed honest authority from whom  $\text{uid}$  has not been queried by the adversary, which exists by design of the security experiment.

We define the following sequence of hybrids:

- $\text{Hyb}_{b,0}^{(c)}$ : This is the real security experiment for the scheme in Fig. 9, encrypting  $\mu_b$ , and conditioned on that  $b_{\text{corrupt\_security}} = 1$ .

Recall that in this hybrid the adversary is given the following:

$$\begin{aligned} & (\mathbf{B}_i)_{i \in [k]}, (\mathbf{A}_i)_{i \in [k]}, (\text{td}_{\mathbf{A}_i})_{i \in \mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ & \mathbf{U}_{\text{uid}, i} = \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ & \hat{\mathbf{B}}_{\text{uid}, i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \quad \forall \text{uid} \in \mathcal{U}, i \in \mathcal{I}_{\text{uid}} \cap ([k] \setminus \mathcal{I}) \\ & \mathbf{c}_i^{\text{T}} = (\mathbf{s}_i^{\text{T}} \mid \mathbf{s}^{\text{T}}) \mathbf{A}_i + \mathbf{e}_i^{\text{T}} \quad \forall i \in [k] \\ & \mathbf{c}_0^{\text{T}} = (\mathbf{s}_1^{\text{T}} \mid \dots \mid \mathbf{s}_k^{\text{T}}) (\mathbf{I}_k \otimes \mathbf{Q}) + \mathbf{e}_0^{\text{T}} \end{aligned}$$

$$\mathbf{c}^T = \sum_{i \in [k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mathbf{e}^T + \mu_b \mathbf{g}^T$$

where all terms are sampled according to the distribution as in the scheme. We recall each  $\mathbf{U}_{\text{uid},i}$  is sampled with  $\text{td}_{\mathbf{A}_i}$ . Relative to the case in the honest model, here the adversary is additionally given  $\text{ask}_i = \text{td}_{\mathbf{A}_i}$  for the corrupted authorities  $i \in \mathcal{I}$ . Below we write  $\mathbf{c}_0^T = (\mathbf{c}_{1,Q}^T \mid \dots \mid \mathbf{c}_{k,Q}^T)$  where  $\mathbf{c}_{i,Q}^T = \mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T$ .

- $\text{Hyb}_{b,1}^{(c)}$ : Same as  $\text{Hyb}_{b,0}^{(c)}$ , except that for all  $i \in [k] \setminus \mathcal{I}$ ,  $\mathbf{A}_i$  is sampled uniformly randomly and all (entries of the) corresponding preimages  $\mathbf{U}_{\text{uid},i}$  are sampled (inefficiently) from the Gaussian distribution with parameter  $\tau$ , subject to

$$\mathbf{A}_i \mathbf{U}_{\text{uid},i} = \begin{pmatrix} \mathbf{P} \mathbf{k}_{\text{uid}} & \mathbf{Q} \mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}.$$

We have  $\text{Hyb}_{b,0}^{(c)} \stackrel{s}{\approx} \text{Hyb}_{b,1}^{(c)}$  by the properties of  $\text{TrapGen}$  from Section 3.3.

- $\text{Hyb}_{b,2}^{(c)}$ : Same as  $\text{Hyb}_{b,1}^{(c)}$ , except:
  - we sample uniformly random  $\mathbf{c} \leftarrow \mathbb{Z}_q^m$ ,
  - for each  $i \in [k] \setminus \mathcal{I}$ , we sample uniformly random  $\mathbf{c}_i$ , and
  - for each  $i \in [k] \setminus \mathcal{I}$ , we sample the  $i$ -th chunk  $\mathbf{c}_{i,Q}$  in  $\mathbf{c}_0$  uniformly randomly.

We show in the following that  $\text{Hyb}_{b,1}^{(c)} \stackrel{c}{\approx} \text{Hyb}_{b,2}^{(c)}$ . Then, the theorem follows from noting that  $\text{Hyb}_{0,2}^{(c)} \stackrel{p}{=} \text{Hyb}_{1,2}^{(c)}$ , since in both hybrids the component  $\mathbf{c}$  in the challenge ciphertext is chosen uniformly randomly.

Define the distribution

$$\mathcal{D}_{1,1}^{(c)} := \left( \begin{array}{l} (\mathbf{B}_i)_{i \in [k] \setminus \mathcal{I}}, (\mathbf{A}_i)_{i \in [k] \setminus \mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ \left( \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P} \mathbf{k}_{\text{uid}} & \mathbf{Q} \mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \right)_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\bar{\mathbf{c}}_i^T = \mathbf{s}_i^T \bar{\mathbf{A}}_i + \mathbf{e}_i^T)_{i \in [k] \setminus \mathcal{I}} \\ (\mathbf{c}_{i,Q}^T = \mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T)_{i \in [k] \setminus \mathcal{I}} \\ \tilde{\mathbf{c}}^T = \sum_{i \in [k] \setminus \mathcal{I}} \mathbf{s}_i^T \mathbf{P} + \mathbf{e}^T \end{array} \right) \quad (9)$$

where all terms are distributed as in  $\text{Hyb}_{b,1}^{(c)}$ . We note that in the above distribution, the LWE samples  $\mathbf{c}_i$  are w.r.t.  $\bar{\mathbf{A}}_i$ , whereas the preimages are w.r.t. (the full)  $\mathbf{A}_i$ . Moreover, for each  $\text{uid} \in \mathcal{U}$ , the distribution involves preimages w.r.t.  $\mathbf{A}_i$  for all  $i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})$ , a superset of the ones appearing in  $\text{Hyb}_{b,1}^{(c)}$  and  $\text{Hyb}_{b,2}^{(c)}$  (which will be useful in the proof of Lemma 7). Define also the distribution

$$\mathcal{D}_{2,1}^{(c)} := \left( \begin{array}{l} (\mathbf{B}_i)_{i \in [k] \setminus \mathcal{I}}, (\mathbf{A}_i)_{i \in [k] \setminus \mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ \left( \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P} \mathbf{k}_{\text{uid}} & \mathbf{Q} \mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \right)_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\bar{\mathbf{c}}_i^T)_{i \in [k] \setminus \mathcal{I}} \\ (\mathbf{c}_{i,Q}^T)_{i \in [k] \setminus \mathcal{I}} \\ \tilde{\mathbf{c}}^T \end{array} \right) \quad (10)$$

where all elements are distributed same as in  $\mathcal{D}_{1,1}^{(c)}$ , except that  $(\bar{\mathbf{c}}_i^T)_{i \in [k] \setminus \mathcal{I}}$ ,  $(\bar{\mathbf{c}}_{i,Q}^T)_{i \in [k] \setminus \mathcal{I}}$  and  $\tilde{\mathbf{c}}$  are uniformly random.



Suppose there exists a PPT  $\mathcal{A}$  that distinguishes  $\text{Hyb}_{b,1}^{(c)}$  and  $\text{Hyb}_{b,2}^{(c)}$  with non-negligible probability, then it is easy to verify that there exists a PPT  $\mathcal{B}$  that distinguishes  $\mathcal{D}_{1,1}^{(c)}$  and  $\mathcal{D}_{2,1}^{(c)}$  defined above with non-negligible probability. A detailed reduction is given in Proposition 1.

Now consider a PPT  $\text{Samp}$  which on input  $\lambda$  outputs the following:

$$\begin{aligned} \tilde{\mathbf{A}} &:= (\mathbf{1}_{[k]\setminus\mathcal{I}} \otimes \mathbf{P} \mid \mathbf{I}_{k-|\mathcal{I}} \otimes \mathbf{Q}), \\ \tilde{\mathbf{P}}_i &:= \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix}_{\text{uid} \in \mathcal{U}} \quad \forall \text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\}), \end{aligned}$$

where  $\mathbf{1}_{[k]\setminus\mathcal{I}}$  is the  $(k-|\mathcal{I}|)$ -dimensional all-one vector, and  $\text{aux}$  containing  $(\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u}$  together with all random coins used.

By the  $\text{EvasiveLWE}_{\text{param}_1}$  assumption (c.f. Table 4) w.r.t.  $\text{Samp}$ , there exists a PPT  $\mathcal{E}$  that distinguishes the distributions  $\mathcal{D}_{1,2}^{(c)}$  and  $\mathcal{D}_{2,2}^{(c)}$  with non-negligible probability, where  $\mathcal{D}_{1,2}^{(c)}$  and  $\mathcal{D}_{2,2}^{(c)}$  are defined as follows:

$$\mathcal{D}_{1,2}^{(c)} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{A}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (\mathbf{s}_i^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}, \mathbf{s}_i^{\text{T}}\mathbf{Q}\mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^{\text{T}})_{\text{uid} \in \mathcal{U}, i \in [k]\setminus(\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\mathbf{s}_i^{\text{T}}\bar{\mathbf{A}}_i + \mathbf{e}_i^{\text{T}})_{i \in [k]\setminus\mathcal{I}} \\ (\mathbf{s}_i^{\text{T}}\mathbf{Q} + \mathbf{e}_{i,Q}^{\text{T}})_{i \in [k]\setminus\mathcal{I}} \\ \mathbf{c}^{\text{T}} = \sum_{i \in [k]\setminus\mathcal{I}} \mathbf{s}_i^{\text{T}}\mathbf{P} + \mathbf{e}^{\text{T}} \end{pmatrix} \quad (11)$$

where all terms are distributed as in  $\mathcal{D}_{1,1}^{(c)}$ , additionally  $e_{i^*,\text{uid},P} \leftarrow \chi_{(3)}$  (where we recall  $i^*$  is arbitrary in  $[k] \setminus \mathcal{I}$  defined at the beginning of the proof),  $e_{\text{uid},i,P} \leftarrow \chi_{(2)}$  for all  $i \in [k], i \neq i^*$ , and  $\mathbf{e}_{\text{uid},i,Q} \leftarrow \chi_{(2)}^{m\ell}$ , and

$$\mathcal{D}_{2,2}^{(c)} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{A}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (c_{\text{uid},i,P}, \mathbf{c}_{\text{uid},i,Q}^{\text{T}})_{\text{uid} \in \mathcal{U}, i \in [k]\setminus(\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\bar{\mathbf{c}}_i^{\text{T}})_{i \in [k]\setminus\mathcal{I}} \\ (\mathbf{c}_{i,Q}^{\text{T}})_{i \in [k]\setminus\mathcal{I}} \\ \mathbf{c}^{\text{T}} \end{pmatrix} \quad (12)$$

where  $(c_{\text{uid},i,P}, \mathbf{c}_{\text{uid},i,Q}^{\text{T}})_{\text{uid} \in \mathcal{U}, i \in [k]\setminus(\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})}, (\bar{\mathbf{c}}_i^{\text{T}}, \mathbf{c}_{i,Q}^{\text{T}})_{i \in [k]\setminus\mathcal{I}}, \mathbf{c}$  are all uniformly random.

We observe that the above implies a PPT distinguisher  $\mathcal{G}$  for the following distributions  $\mathcal{D}_{1,3}^{(c)}, \mathcal{D}_{2,3}^{(c)}$ , given which  $\mathcal{D}_{1,2}^{(c)}$  and  $\mathcal{D}_{2,2}^{(c)}$  can be efficiently simulated respectively:

$$\mathcal{D}_{1,3}^{(c)} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{A}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (\mathbf{s}_i^{\text{T}}\mathbf{P}\mathbf{k}_{\text{uid}} + e_{\text{uid},i,P})_{\text{uid} \in \mathcal{U}, i \in [k]\setminus(\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\mathbf{s}_i^{\text{T}}\bar{\mathbf{A}}_i + \mathbf{e}_i^{\text{T}})_{i \in [k]\setminus\mathcal{I}} \\ (\mathbf{s}_i^{\text{T}}\mathbf{Q} + \mathbf{e}_{i,Q}^{\text{T}})_{i \in [k]\setminus\mathcal{I}} \\ \mathbf{c}^{\text{T}} = \sum_{i \in [k]\setminus\mathcal{I}} \mathbf{s}_i^{\text{T}}\mathbf{P} + \mathbf{e}^{\text{T}} \end{pmatrix} \quad (13)$$

$$\mathcal{D}_{2,3}^{(c)} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{A}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (c_{\text{uid},i,P})_{\text{uid} \in \mathcal{U}, i \in [k]\setminus(\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\bar{\mathbf{c}}_i^{\text{T}})_{i \in [k]\setminus\mathcal{I}} \\ (\mathbf{c}_{i,Q}^{\text{T}})_{i \in [k]\setminus\mathcal{I}} \\ \mathbf{c}^{\text{T}} \end{pmatrix} \quad (14)$$



which are almost identical to  $\mathcal{D}_{1,2}^{(c)}$  and  $\mathcal{D}_{2,2}^{(c)}$  respectively, except that  $\mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T$  respectively  $\mathbf{c}_{\text{uid},i,Q}^T$  are omitted. To simulate  $\mathcal{D}_{1,2}^{(c)}$  from  $\mathcal{D}_{1,3}^{(c)}$ , one computes

$$(\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T) \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T = \mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{e}_{i,Q}^T \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T \stackrel{\$}{\approx} \mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T \pmod{q}$$

where the last  $\stackrel{\$}{\approx}$  follows from noise flooding, since

$$\chi_{(2)} \geq \lambda^{\omega(1)} \cdot \lambda \cdot \chi_{(1)} \cdot \chi_{(1)} \cdot n \geq \lambda^{\omega(1)} \cdot \|\mathbf{e}_{i,Q}^T \cdot \mathbf{K}_{\text{uid}}\|.$$

When  $\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T$  is replaced by uniformly random  $\mathbf{c}_{\text{uid},i,Q}^T$ , then the simulation becomes also uniformly random.

Finally, by Lemma 7 the existence of  $\mathcal{G}$  is not possible under the  $\text{LWE}_{n,2m(m+2),q,\chi_{(1)}}$  and  $\text{LWE}_{m,\text{poly}(n),q,\chi_{(2)},\chi_{(1)}}$  assumptions, thus we have a contradiction. The theorem follows.  $\square$

**Proposition 1.** *If there exists a PPT  $\mathcal{A}$  that distinguishes  $\text{Hyb}_{b,1}^{(c)}$  and  $\text{Hyb}_{b,2}^{(c)}$  defined in Theorem 4 with non-negligible probability, then there exists a PPT  $\mathcal{B}$  that distinguishes the distributions  $\mathcal{D}_{1,1}^{(c)}$  and  $\mathcal{D}_{2,1}^{(c)}$  defined in Eq. (9) and Eq. (10) with non-negligible probability.*

*Proof.* Given such a PPT  $\mathcal{A}$ , we construct such a PPT  $\mathcal{B}$ . On input a sample from either  $\mathcal{D}_{1,1}^{(c)}$  or  $\mathcal{D}_{2,1}^{(c)}$  defined in Eq. (9) and Eq. (10) respectively, let  $\mathcal{B}$  proceed as follows:

- Parse  $\mathbf{P}, \mathbf{u}$  from the input sample and let  $\text{pp} := (\mathbf{P}, \mathbf{u})$  be the public parameters.
- To generate the authority public and secret keys:
  - For corrupt authorities  $i \in \mathcal{I}$ , generate  $(\text{apk}_i, \text{ask}_i) \leftarrow \text{AuthSetup}(\text{pp})$ .
  - For honest authorities  $i \in [k] \setminus \mathcal{I}$ , parse  $\mathbf{A}_i, \mathbf{B}_i$  from the input sample and let  $\text{apk}_i = (\mathbf{A}_i, \mathbf{B}_i)$ .
- To answer the authority key queries:
  - For any query  $(\text{uid}, i, \mathbf{x})$  on corrupt  $i \in \mathcal{I}$ , generate query using  $\text{ask}_i$ .
  - For any query  $(\text{uid}, i, \mathbf{x})$  on honest  $i \in [k] \setminus \mathcal{I}$ , let  $\mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P} \mathbf{k}_{\text{uid}} & \mathbf{Q} \mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} & \mathbf{k}_{\text{uid}} \end{pmatrix}$  from input sample be the answer.
- To generate the ciphertext, sample random  $\mathbf{s} \leftarrow_{\$} \mathbb{Z}_q^{nm}$  and random  $\mathbf{s}_i \leftarrow_{\$} \mathbb{Z}_q^n$  for all  $i \in \mathcal{I}$ , and:
  - For  $i \in \mathcal{I}$ , compute  $\mathbf{c}_i^T = (\mathbf{s}_i^T \mid \mathbf{s}^T) \mathbf{A}_i + \mathbf{e}_i^T$  where  $\mathbf{e}_i \leftarrow_{\$} \chi_{(1)}^{2m(m+1)}$ .
  - For  $i \in [k] \setminus \mathcal{I}$ :
    - \* Parse  $\mathbf{A}_i$  and  $\bar{\mathbf{c}}_{i,A}^T$  from the input sample, write  $\mathbf{A}_i = \begin{pmatrix} \bar{\mathbf{A}}_i \\ \underline{\mathbf{A}}_i \end{pmatrix}$  where  $\bar{\mathbf{A}}_i \in \mathbb{Z}_q^{n \times 2m(m+1)}$  and  $\underline{\mathbf{A}}_i \in \mathbb{Z}_q^{nm \times 2m(m+1)}$ .
    - \* Compute  $\mathbf{s}^T \underline{\mathbf{A}}_i$ , set  $\mathbf{c}_i^T = \bar{\mathbf{c}}_{i,A}^T + \mathbf{s}^T \underline{\mathbf{A}}_i$ .
  - Parse  $\mathbf{c}_{i,Q}^T$  for all  $i \in [k] \setminus \mathcal{I}$  from input sample. Compute  $\mathbf{c}_{i,Q}^T = \mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T \pmod{q}$  for all  $i \in \mathcal{I}$  where  $\mathbf{e}_{i,Q}^T \leftarrow_{\$} \chi_{(1)}^n$ . Concatenate to obtain  $\mathbf{c}_0^T = (\mathbf{c}_{1,Q}^T \mid \dots \mid \mathbf{c}_{k,Q}^T)$ .
  - Parse  $\tilde{\mathbf{c}}^T$  from input sample, compute  $\mathbf{c}^T := \tilde{\mathbf{c}}^T + \sum_{i \in \mathcal{I}} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mu_b \mathbf{g}^T$ .
  - Let the ciphertext be  $(\mathbf{c}, \mathbf{c}_1, \dots, \mathbf{c}_k)$ .
- Pass all terms computed above to  $\mathcal{A}$ , then return whatever  $\mathcal{A}$  returns.

It is immediate that the above simulates  $\text{Hyb}_{b,1}^{(c)}$  and  $\text{Hyb}_{b,2}^{(c)}$  respectively perfectly, if the input is respectively  $\mathcal{D}_{1,1}^{(c)}$  and  $\mathcal{D}_{1,2}^{(c)}$ . In more detail, for the ciphertext, if  $\bar{\mathbf{c}}_{i,A}^T = \mathbf{s}_i^T \bar{\mathbf{A}}_i + \mathbf{e}_i^T$  then  $\mathbf{c}_i^T = \mathbf{s}_i^T \bar{\mathbf{A}}_i + \mathbf{e}_i^T + \mathbf{s}^T \bar{\mathbf{A}}_i = (\mathbf{s}_i^T \mid \mathbf{s}^T) \mathbf{A}_i + \mathbf{e}_i^T$ , else if  $\bar{\mathbf{c}}_{i,A}^T$  is uniform then so is  $\mathbf{c}_i^T$ . The claim follows.  $\square$

**Lemma 7.** For the distributions  $\mathcal{D}_{1,3}^{(c)}$  and  $\mathcal{D}_{2,3}^{(c)}$  defined in Eq. (13) and Eq. (14), we have  $\mathcal{D}_{1,3}^{(c)} \stackrel{c}{\approx} \mathcal{D}_{2,3}^{(c)}$  assuming

$$\text{LWE}_{n,2m(m+2),q,\chi(1)} \quad \text{and} \quad \text{LWE}_{m,\text{poly}(n),q,\chi(2),\chi(1)}.$$

*Proof.* Continue with the notation in the proof of Theorem 4, where we have let  $i^* \in [k] \setminus \mathcal{I}$  be an arbitrarily fixed honest authority (which exists because  $[k] \neq \mathcal{I}$ ), and for each  $\text{uid} \in \mathcal{U}$ , we have let  $\tilde{i}_{\text{uid}} \in [k] \setminus \mathcal{I}$  be an honest authority where  $\text{uid}$  is not queried by the adversary (which exists by design of security experiment).

We consider the following sequence of hybrid distributions:

- $\mathcal{D}_{1,3}^{(c)}$  as in Eq. (11).
- $\mathcal{D}_{1,3,1}$ : For each  $\text{uid} \in \mathcal{U}$ , if  $i^* \neq \tilde{i}_{\text{uid}}$ , then do the following:

We swap  $\mathbf{s}_{i^*}^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{i^*,\text{uid},P}$  to

$$\left( \sum_{i \in [k] \setminus \mathcal{I}} \mathbf{s}_i^T \mathbf{P} + \mathbf{e}^T \right) \mathbf{k}_{\text{uid}} - \left( \sum_{i \in [k] \setminus \mathcal{I}: i \neq i^*} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \right) + e_{i^*,\text{uid},P}$$

We have  $\mathcal{D}_{1,3}^{(c)} \stackrel{s}{\approx} \mathcal{D}_{1,3,1}$  by noise flooding, which is due to the equality

$$\mathbf{s}_{i^*}^T \mathbf{P} \mathbf{k}_{\text{uid}} = \left( \sum_{i \in [k] \setminus \mathcal{I}} \mathbf{s}_i^T \mathbf{P} \right) \mathbf{k}_{\text{uid}} - \sum_{i \in [k] \setminus \mathcal{I}: i \neq i^*} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}}.$$

and  $e_{i^*,\text{uid},P} \stackrel{s}{\approx} \mathbf{e}^T \mathbf{k}_{\text{uid}} - \sum_{i \in [k] \setminus \mathcal{I}: i \neq i^*} e_{\text{uid},i,P} + e_{i^*,\text{uid},P}$ , as  $\chi(3) \geq \lambda^{\omega(1)} (\lambda^2 \chi_{(1)}^2) m + \lambda k \chi(2) \geq \lambda^{\omega(1)} \left\| \mathbf{e}^T \mathbf{k}_{\text{uid}} - \sum_{i \in [k] \setminus \mathcal{I}: i \neq i^*} e_{\text{uid},i,P} \right\|$ .

Otherwise, if  $i^* = \tilde{i}_{\text{uid}}$ , then do nothing. The effect of this swap is that, for all  $\text{uid} \in \mathcal{U}$ , the term  $\mathbf{s}_{i^*}^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$  no longer exists in  $\mathcal{D}_{1,3,1}$  (and is instead simulated by the other terms, where the expression includes LWE samples with secret  $\mathbf{s}_{\tilde{i}_{\text{uid}}}$ ).

As a result, the only remaining terms in  $\mathcal{D}_{1,3,1}$  involving  $\mathbf{s}_{i^*}$  are  $\mathbf{s}_{i^*}^T \bar{\mathbf{A}}_{i^*} + \mathbf{e}_{i^*}^T$  and  $\mathbf{s}_{i^*}^T \mathbf{P} + \mathbf{e}_{i^*,P}^T$ , and  $\mathbf{s}_{i^*}^T \mathbf{Q} + \mathbf{e}_{i^*,Q}^T$ .

- $\mathcal{D}_{1,3,2}$ : We swap

$$\mathbf{s}_{i^*}^T \bar{\mathbf{A}}_{i^*} + \mathbf{e}_{i^*}^T, \quad \mathbf{s}_{i^*}^T \mathbf{P} + \mathbf{e}_{i^*,P}^T \quad \text{and} \quad \mathbf{s}_{i^*}^T \mathbf{Q} + \mathbf{e}_{i^*,Q}^T$$

to uniformly random.

We have  $\mathcal{D}_{1,3,1} \stackrel{c}{\approx} \mathcal{D}_{1,3,2}$  by the  $\text{LWE}_{n,2m(m+2),q,\chi(1)}$  assumption. Notice that as a result  $\mathbf{c}$  is also uniformly random.

- $\mathcal{D}_{1,3,3}$ : For all  $\text{uid} \in \mathcal{U}$ , all  $i \in [k] \setminus (\mathcal{I} \cup \{i^*\})$ , we swap

$$\mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \quad \text{to} \quad (\mathbf{s}_i^T \mathbf{P} + \tilde{\mathbf{e}}_{\text{uid},i,P}^T) \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$$

where  $\tilde{\mathbf{e}}_{\text{uid},i,P} \leftarrow \mathfrak{s} \chi_{(1)}^m$ .

We have  $\mathcal{D}_{1,3,2} \stackrel{s}{\approx} \mathcal{D}_{1,3,3}$  by noise flooding, due to  $\tilde{\mathbf{e}}_{\text{uid},i,P}^T \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \stackrel{s}{\approx} e_{\text{uid},i,P}$ . since  $\chi(2) \geq \lambda^{\omega(1)} \lambda^2 \chi_{(1)} \chi_{(1)} m \geq \lambda^{\omega(1)} \left\| \tilde{\mathbf{e}}_{\text{uid},i,P}^T \mathbf{k}_{\text{uid}} \right\|$ .

- $\mathcal{D}_{1,3,4}$ : For all  $\text{uid} \in \mathcal{U}$ , all  $i \in [k] \setminus (\mathcal{I} \cup \{i^*\})$ , we swap

$$(\mathbf{s}_i^T \mathbf{P} + \tilde{\mathbf{e}}_{i,P}^T) \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \quad \text{to} \quad \mathbf{b}_{i,P}^T \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$$

where  $\mathbf{b}_{\text{uid},i,P}^T$  is uniformly random, and we also swap

$$\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T \quad \text{and} \quad \mathbf{s}_i^T \overline{\mathbf{A}}_i + \mathbf{e}_i^T$$

to uniformly random.

We have  $\mathcal{D}_{1,3,3} \stackrel{\text{c}}{\approx} \mathcal{D}_{1,3,4}$  by the  $\text{LWE}_{n,2m(m+2),q,\chi(1)}$  assumption.

- $\mathcal{D}_{1,3,5}$ : For all  $\text{uid} \in \mathcal{U}$ , all  $i \in [k] \setminus (\mathcal{I} \cup \{i^*\})$ , we swap

$$\mathbf{b}_{i,P}^T \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$$

to uniformly random.

We have  $\mathcal{D}_{1,3,4} \stackrel{\text{c}}{\approx} \mathcal{D}_{1,3,5}$  by the (low-norm)  $\text{LWE}_{m,\text{poly}(n),q,\chi(2),\chi(1)}$  assumption.

Observe that  $\mathcal{D}_{1,3,5} \stackrel{\text{c}}{\approx} \mathcal{D}_{2,3}^{(c)}$  as in Eq. (14), the proof is completed.  $\square$

## A.2 Alternative security proof for corruption

In this subsection we provide an alternative security proof of the MA-ABE scheme in case of  $b_{\text{corrupt\_security}} = 1$ , i.e. for all  $\text{uid} \in \mathcal{U}$  queried, there exists an honest authority  $i$  such that a key  $\text{sk}_{\text{uid},i}$  from  $i$  has not been queried. The evasive LWE assumption involved in this alternative proof is slightly weaker than that in Section A.1, although the overall proof is more complicated. For this, we will make use of non-spherical discrete Gaussian distributions and trapdoors for sampling preimages following these distributions. We recall the necessary preliminaries below.

### A.2.1 Non-spherical Gaussians (Extending Sections 3.1 and 3.3).

A symmetric matrix  $\Sigma \in \mathbb{R}^{m \times m}$  is said to be positive semi-definite, if  $\mathbf{x}^T \Sigma \mathbf{x} \geq 0$  for all non-zero  $\mathbf{x} \in \mathbb{R}^m$ . For a positive semi-definite matrix  $\Sigma$ , we denote by  $\mathcal{D}_{\mathbb{Z}^m, \sqrt{\Sigma}}$  the (centered) discrete Gaussian distribution over  $\mathbb{Z}^m$  with parameter  $\sqrt{\Sigma}$ , i.e. the distribution over  $\mathbb{Z}^m$  where for all  $\mathbf{x}$ ,  $\mathcal{D}_{\mathbb{Z}^m, \Sigma}(\mathbf{x}) \propto e^{-\pi \cdot \mathbf{x}^T \Sigma^\dagger \mathbf{x}}$ , where  $\Sigma^\dagger$  is the (Moore-Penrose) pseudoinverse of  $\Sigma$ . With an abuse of notation, we sometimes also denote by  $\sqrt{\Sigma}$  the (centered) discrete Gaussian distribution over  $\mathbb{Z}^m$  with parameter  $\sqrt{\Sigma}$ .

If  $\Sigma = \chi^2 \mathbf{I}_m$ , i.e. diagonal matrix with the same entry  $\chi^2$ , so that  $\mathcal{D}_{\mathbb{Z}^m, \sqrt{\Sigma}}(\mathbf{x}) \propto e^{-\pi \cdot (x_1^2 + \dots + x_m^2) / \chi^2}$ , we write  $\mathcal{D}_{\mathbb{Z}^m, \sqrt{\Sigma}}$  and  $\mathcal{D}_{\mathbb{Z}^m, \chi}$  interchangeably. Analogously, we sometimes denote by  $\chi^m$  the (centered) discrete Gaussian distribution over  $\mathbb{Z}^m$  with parameter  $\chi$ .

Let  $\Sigma \in \mathbb{R}^{h \times h}$  be diagonal matrix with entries  $\chi_1^2, \dots, \chi_h^2$ . There exist PPT algorithms ( $\text{TrapGen}$ ,  $\text{SampPre}$ ), such that for appropriately chosen  $n, q, \{\chi_i\}_{i \in [m]}$  parametrised by  $\lambda$ , with  $\chi_i \geq O(\sqrt{n} \cdot \log q \cdot \log n)$  for all  $i \in [h]$ , the following properties are satisfied [GPV08, MP12, GM18]:

- $(\mathbf{D}, \mathbf{R}) \leftarrow \text{TrapGen}(1^n, 1^h, q)$  generates a matrix  $\mathbf{D} \in \mathbb{Z}_q^{n \times h}$ , where  $h \geq 2n \lceil \log q \rceil$ , and a trapdoor  $\mathbf{R} \in \mathbb{Z}^{h \times n \lceil \log q \rceil}$  such that  $\mathbf{DR} = \mathbf{G} \bmod q$ . The distribution of  $\mathbf{D}$  is statistically close to the uniform distribution over  $\mathbb{Z}_q^{n \times h}$ .
- $\mathbf{u} \leftarrow \text{SampPre}(\mathbf{D}, \mathbf{R}, \mathbf{v}, \sqrt{\Sigma})$  inputs a target vector  $\mathbf{v} \in \mathbb{Z}_q^n$  and a gaussian parameter  $\sqrt{\Sigma}$ , and samples a vector  $\mathbf{u} \in \mathbb{Z}^h$ . For any  $\mathbf{D} \in \mathbb{Z}_q^{n \times h}$ ,  $\mathbf{R} \in \mathbb{Z}_q^{h \times n \lceil \log q \rceil}$  such that

**Table 6:** Selected parameters and shorthands for MA-ABE scheme (Section 6), under alternative security proof in Section A.2.

$h$	$> 2m(m+1)$	Number of columns of $\mathbf{A}_i$
$m_{lc}, m_{rc}$	$m_{lc} \geq 2(n_{tr} + n_{br}) \log q, m_{rc} = h - m_{lc}$	Number of “left columns” and “right columns” of $\mathbf{A}_i$
$n_{tr}, n_{br}$	$n_{tr} = n, n_{br} = mn$	Number of “top rows” and “bottom rows” of $\mathbf{A}_i$
$\chi_{(0)}$	$\geq O(\lambda)$	Parameter of KGen algorithm, Gaussian width of $\mathbf{R}, \mathbf{w}_{uid,i}, \mathbf{Y}_{uid,i}, \mathbf{e}_{i,A}$ in proofs
$\chi_{(1)}$	$\geq \lambda^{\omega(1)} \cdot \chi_{(0)}^2$	Parameter of KGen algorithm, Gaussian width of $\mathbf{u}, \mathbf{k}_{uid}, \mathbf{K}_{uid}, \mathbf{e}, \mathbf{e}_0 = (\mathbf{e}_{i,Q})_i, (\mathbf{e}_i)_{i \in [k]}$ , and of $\mathbf{v}'_{uid,i}, \mathbf{X}'_{uid,i}, \tilde{\mathbf{e}}_{uid,i,P}$ in proofs
$\chi_{(2)}$	$\geq \lambda^{\omega(1)} \cdot \chi_{(1)}^2$	Gaussian width of $\mathbf{e}_{uid,i,B}, \mathbf{e}_{uid,i,P}, \mathbf{e}_{uid,i,Q}$ in proofs
$\chi_{(3)}$	$\geq \lambda^{\omega(1)} \cdot \chi_{(2)} \cdot m^{O(d)}$	Gaussian width of $\mathbf{e}_{i^*,uid,P}$ in proofs
$\mathcal{I}, z$	$z :=  [k] \setminus \mathcal{I} $	Set $\mathcal{I}$ of corrupt authorities in proofs
$\text{param}_2$	$(q, z, n_{tr}, m_{lc}, zn, (z+1)m, \mathcal{S}_2, \chi_{(1)}, (\text{poly}(\lambda), \chi_{(1)}, \psi_i, \chi_{(1)})_{i \in [z]}, \text{where } \psi_{i^*} = \chi_{(3)}, \psi_i = \chi_{(2)}, i \neq i^*$	Evasive LWE parameter

$\mathbf{DR} = \mathbf{G} \bmod q$  and  $5(s_1(\mathbf{R})^2 + 1) \leq \min_i \chi_i^2$  where  $s_1(\mathbf{R})$  is the maximal singular value of  $\mathbf{R}$  (e.g. when  $(\mathbf{D}, \mathbf{R})$  is output of  $\text{TrapGen}(1^n, 1^h, q)$ ), it is guaranteed that  $\mathbf{Du} = \mathbf{v} \bmod q$  and  $\|u_i\| \leq \lambda \chi_i$  for all  $i \in [h]$  with overwhelming probability, where  $u_i$  is the  $i$ -th entry of  $\mathbf{u}$ . Furthermore, for any  $\mathbf{v} \in \mathbb{Z}_q^n$ , the following distributions are statistically close:

$$\left\{ (\mathbf{D}, \mathbf{u}) \mid \begin{array}{l} (\mathbf{D}, \mathbf{R}) \leftarrow \text{TrapGen}(1^n, 1^h, q) \\ \mathbf{u} \leftarrow \text{SampPre}(\mathbf{D}, \mathbf{R}, \mathbf{v}, \sqrt{\Sigma}) \end{array} \right\} \approx \left\{ (\mathbf{D}, \mathbf{u}) \mid \begin{array}{l} (\mathbf{D}, \mathbf{R}) \leftarrow \text{TrapGen}(1^n, 1^h, q) \\ \mathbf{u} \leftarrow \mathfrak{s} \sqrt{\Sigma} : \mathbf{Du} = \mathbf{v} \bmod q \end{array} \right\}.$$

If  $\chi_1 = \dots = \chi_m = \chi$ , we simply write  $\text{SampPre}(\mathbf{D}, \mathbf{R}, \mathbf{v}, \chi)$ .

### A.2.2 Alternative proof.

We will denote  $\mathbf{A}_i = \begin{pmatrix} \mathbf{A}_i^{\top} & \mathbf{A}_i^{\top} \\ \mathbf{A}_i^{\perp} & \mathbf{A}_i^{\perp} \end{pmatrix}$ , where  $\mathbf{A}_i^{\top} \in \mathbb{Z}_q^{n_{tr} \times m_{lc}}$  is the “top left corner” of  $\mathbf{A}_i$ , and analogously for  $\mathbf{A}_i^{\perp} \in \mathbb{Z}_q^{n_{tr} \times m_{rc}}, \mathbf{A}_i^{\perp} \in \mathbb{Z}_q^{n_{br} \times m_{lc}}$  and  $\mathbf{A}_i^{\perp} \in \mathbb{Z}_q^{n_{br} \times m_{rc}}$ . Also, we slightly modify the scheme in Fig. 9:

- In  $\text{AuthSetup}$ , let  $\mathbf{A}_i$  be sampled from  $\text{TrapGen}(1^{n(m+1)}, 1^h, q)$ , where  $h > 2m(m+1)$ .
- Let  $\Sigma \in \mathbb{R}^{(m_{lc}+m_{rc}) \times (m_{lc}+m_{rc})}$  be diagonal matrix where the first  $m_{lc}$  entries are  $\chi_{(1)} = \lambda^{\omega(1)} \chi_{(0)}^2$  and the rest are  $\chi_{(0)}$ , which is the Gaussian parameter input to  $\text{SampPre}$  in the KGen algorithm.

The modified parameters involved in this alternative proof are summarised in Table 6.

*Proof.* (Alternative.) Below write  $\mathcal{I} = \mathcal{I}_{\text{corr}} \subset [k]$  for the set of corrupt authorities. In this continued proof we focus on that Case (2)  $b_{\text{corrupt\_security}} = 1$  happens. That is, for all  $\text{uid} \in \mathcal{U}$  there exists an honest authority  $i \in [k] \setminus \mathcal{I}$  such that a key  $\text{sk}_{\text{uid},i}$  from  $i$  has not been queried.

Fix arbitrary honest authority  $i^* \in [k] \setminus \mathcal{I}$ , which exists since  $[k] \neq \mathcal{I}$ . For each  $\text{uid} \in \mathcal{U}$ , denote by  $\tilde{i}_{\text{uid}}$  an arbitrarily fixed honest authority from whom  $\text{uid}$  has not been queried by the adversary, which exists by design of the security experiment.

We define the following sequence of hybrids:

- $\text{Hyb}_{b,0}^{(c,\text{alt})}$ : This is the real very-selective security experiment for the scheme in Fig. 9, encrypting  $\mu_b$ .

Note that in this hybrid the adversary is given the following:

$$\begin{aligned}
& (\mathbf{B}_i)_{i \in [k]}, (\mathbf{A}_i)_{i \in [k]}, (\text{td}_{\mathbf{A}_i})_{i \in \mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\
& \mathbf{U}_{\text{uid}, i} = \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid}, i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \quad \forall i \in [k], \text{uid} \in \mathcal{U} : i \in \mathcal{I}_{\text{uid}} \\
& \mathbf{c}_i^{\text{T}} = (\mathbf{s}_i^{\text{T}} \mid \mathbf{s}^{\text{T}}) \mathbf{A}_i + \mathbf{e}_i^{\text{T}} \quad \forall i \in [k] \\
& \mathbf{c}_0^{\text{T}} = (\mathbf{s}_1^{\text{T}} \mid \dots \mid \mathbf{s}_k^{\text{T}}) (\mathbf{I}_k \otimes \mathbf{Q}) + \mathbf{e}_0^{\text{T}} \\
& \mathbf{c}^{\text{T}} = \sum_{i \in [k]} \mathbf{s}_i^{\text{T}} \mathbf{P} + \mathbf{s}^{\text{T}} (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mathbf{e}^{\text{T}} + \mu \mathbf{g}^{\text{T}}
\end{aligned}$$

where all terms are sampled according to the distribution as in the scheme. We recall each  $\mathbf{U}_{\text{uid}, i}$  is sampled with  $\text{td}_{\mathbf{A}_i}$ . Relative to the case in the honest model, here the adversary is additionally given  $\text{ask}_i = \text{td}_{\mathbf{A}_i}$  for the corrupt authorities  $i \in \mathcal{I}$ . Write  $\mathbf{c}_0^{\text{T}} = (\mathbf{c}_{1, Q}^{\text{T}} \mid \dots \mid \mathbf{c}_{k, Q}^{\text{T}})$  where  $\mathbf{c}_{i, Q}^{\text{T}} = \mathbf{s}_i^{\text{T}} \mathbf{Q} + \mathbf{e}_{i, Q}^{\text{T}}$ .

- $\text{Hyb}_{b,1}^{(c, \text{alt})}$ : Same as  $\text{Hyb}_{b,0}^{(c, \text{alt})}$ , except that for all  $i \in [k] \setminus \mathcal{I}$ ,  $\mathbf{A}_i$  is sampled uniformly randomly and all corresponding preimages  $\mathbf{U}_{\text{uid}, i}$  are sampled inefficiently. We have  $\text{Hyb}_{b,0}^{(c, \text{alt})} \stackrel{s}{\approx} \text{Hyb}_{b,1}^{(c, \text{alt})}$  by the properties of TrapGen from Section 3.3.
- $\text{Hyb}_{b,2}^{(c, \text{alt})}$ : Same as  $\text{Hyb}_{b,1}^{(c, \text{alt})}$ , except:
  - we sample uniformly random  $\mathbf{c} \leftarrow \mathbb{Z}_q^m$ ,
  - for each  $i \in [k] \setminus \mathcal{I}$ , we sample uniformly random  $\mathbf{c}_i$ , and
  - for each  $i \in [k] \setminus \mathcal{I}$ , we sample the  $i$ -th chunk  $\mathbf{c}_{i, Q}$  in  $\mathbf{c}_0$  uniformly randomly.

We show in the following that  $\text{Hyb}_{b,1}^{(c, \text{alt})} \stackrel{c}{\approx} \text{Hyb}_{b,2}^{(c, \text{alt})}$ . Then, the theorem follows from noting that  $\text{Hyb}_{0,2}^{(c, \text{alt})} \stackrel{p}{\approx} \text{Hyb}_{1,2}^{(c, \text{alt})}$ .

Define the distribution

$$\mathcal{D}_{1,1}^{(c, \text{alt})} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k] \setminus \mathcal{I}}, (\mathbf{A}_i)_{i \in [k] \setminus \mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (\mathbf{A}_i^{-1}(\mathbf{P}\mathbf{k}_{\text{uid}}), \mathbf{A}_i^{-1}(\mathbf{Q}\mathbf{K}_{\text{uid}}))_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\mathbf{c}_{i, A}^{\text{T}} = \mathbf{s}_i^{\text{T}} \mathbf{A}_i + \mathbf{e}_{i, A}^{\text{T}})_{i \in [k] \setminus \mathcal{I}} \\ (\mathbf{c}_{i, Q}^{\text{T}} = \mathbf{s}_i^{\text{T}} \mathbf{Q} + \mathbf{e}_{i, Q}^{\text{T}})_{i \in [k] \setminus \mathcal{I}} \\ \tilde{\mathbf{c}}^{\text{T}} = \sum_{i \in [k] \setminus \mathcal{I}} \mathbf{s}_i^{\text{T}} \mathbf{P} + \mathbf{e}^{\text{T}} \end{pmatrix} \quad (15)$$

where all terms are distributed as in  $\text{Hyb}_{b,1}$ , in particular  $\mathbf{A}_i^{-1}(\mathbf{P}\mathbf{k}_{\text{uid}}), \mathbf{A}_i^{-1}(\mathbf{Q}\mathbf{K}_{\text{uid}})$  are sampled (inefficiently) with Gaussian parameter  $\chi_{(1)}$ , and additionally the noise  $\mathbf{e}_{i, A} \leftarrow \mathcal{X}_{(0)}^{m_{i, c}}$ . Define also the distribution

$$\mathcal{D}_{2,1}^{(c, \text{alt})} := \begin{pmatrix} (\mathbf{B}_i)_{i \in [k] \setminus \mathcal{I}}, (\mathbf{A}_i)_{i \in [k] \setminus \mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (\mathbf{A}_i^{-1}(\mathbf{P}\mathbf{k}_{\text{uid}}), \mathbf{A}_i^{-1}(\mathbf{Q}\mathbf{K}_{\text{uid}}))_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\mathbf{c}_{i, A}^{\text{T}})_{i \in [k] \setminus \mathcal{I}} \\ (\mathbf{c}_{i, Q}^{\text{T}})_{i \in [k] \setminus \mathcal{I}} \\ \tilde{\mathbf{c}}^{\text{T}} \end{pmatrix} \quad (16)$$

where all elements are distributed same as in  $\mathcal{D}_{1,1}$ , except that  $(\mathbf{c}_{i, A}^{\text{T}})_{i \in [k] \setminus \mathcal{I}}, (\mathbf{c}_{i, Q}^{\text{T}})_{i \in [k] \setminus \mathcal{I}}$  and  $\tilde{\mathbf{c}}$  are uniformly random.

Suppose there exists a PPT  $\mathcal{A}$  that distinguishes  $\text{Hyb}_{b,1}^{(c,\text{alt})}$  and  $\text{Hyb}_{b,2}^{(c,\text{alt})}$  with non-negligible probability, then by Lemma 8 there exists a PPT  $\mathcal{B}$  that distinguishes  $\mathcal{D}_{1,1}$  and  $\mathcal{D}_{2,1}$  defined above with non-negligible probability.

Now consider a PPT  $\text{Samp}$  which on input  $\lambda$  outputs the following:

$$\begin{aligned}\tilde{\mathbf{A}} &:= (\mathbf{1}_{[k]\setminus\mathcal{I}} \otimes \mathbf{P} \mid \mathbf{I}_{k-|\mathcal{I}} \otimes \mathbf{Q}), \\ \tilde{\mathbf{P}}_i &:= (\mathbf{P}\mathbf{k}_{\text{uid}} \quad \mathbf{Q}\mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}} \quad \forall \text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\}),\end{aligned}$$

where  $\mathbf{1}_{[k]\setminus\mathcal{I}}$  is  $(k - |\mathcal{I}|)$ -dimensional all-one vector, and  $\text{aux}$  containing  $(\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u}$  together with all random coins used.

By the  $\text{EvasiveLWE}_{\text{param}_2}$  assumption (c.f. Table 6), there exists a PPT  $\mathcal{E}$  that distinguishes the distributions  $\mathcal{D}_{1,2}^{(c,\text{alt})}$  and  $\mathcal{D}_{2,2}^{(c,\text{alt})}$  with non-negligible probability, where  $\mathcal{D}_{1,2}^{(c,\text{alt})}$  and  $\mathcal{D}_{2,2}^{(c,\text{alt})}$  are defined as follows:

$$\mathcal{D}_{1,2}^{(c,\text{alt})} := \left( \begin{array}{l} (\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{A}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (\mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}, \mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T)_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\mathbf{s}_i^T \mathbf{A}_i + \mathbf{e}_{i,A}^T)_{i \in [k]\setminus\mathcal{I}} \\ (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T)_{i \in [k]\setminus\mathcal{I}} \\ \tilde{\mathbf{c}}^T = \sum_{i \in [k]\setminus\mathcal{I}} \mathbf{s}_i^T \mathbf{P} + \mathbf{e}^T \end{array} \right) \quad (17)$$

where all terms are distributed as in  $\mathcal{D}_{1,1}$ , additionally  $e_{i^*,\text{uid},P} \leftarrow \chi_{(3)}$  (where we recall  $i^*$  is arbitrary in  $[k] \setminus \mathcal{I}$  defined at the beginning of the proof), and  $e_{\text{uid},i,P} \leftarrow \chi_{(2)}$ ,  $\mathbf{e}_{\text{uid},i,Q} \leftarrow \chi_{(3)}^n$  for all  $i \in [k], i \neq i^*$ ,

$$\mathcal{D}_{2,2}^{(c,\text{alt})} := \left( \begin{array}{l} (\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{A}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (c_{\text{uid},i,P}, \mathbf{c}_{\text{uid},i,Q}^T)_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\mathbf{c}_{i,A}^T)_{i \in [k]\setminus\mathcal{I}} \\ (\mathbf{c}_{i,Q}^T)_{i \in [k]\setminus\mathcal{I}} \\ \tilde{\mathbf{c}}^T \end{array} \right) \quad (18)$$

where  $(c_{\text{uid},i,P}, \mathbf{c}_{\text{uid},i,Q}^T)_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})}, (\mathbf{c}_{i,A}^T)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{c}_{i,Q}^T)_{i \in [k]\setminus\mathcal{I}}, \tilde{\mathbf{c}}$  are uniformly random.

We observe that the above implies a PPT distinguisher  $\mathcal{G}$  for the following distributions  $\mathcal{D}_{1,3}^{(c,\text{alt})}, \mathcal{D}_{2,3}^{(c,\text{alt})}$ , given which  $\mathcal{D}_{1,2}^{(c,\text{alt})}$  and  $\mathcal{D}_{2,2}^{(c,\text{alt})}$  can be efficiently simulated respectively:

$$\mathcal{D}_{1,3}^{(c,\text{alt})} := \left( \begin{array}{l} (\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{A}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (\mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P})_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\mathbf{s}_i^T \mathbf{A}_i + \mathbf{e}_{i,A}^T)_{i \in [k]\setminus\mathcal{I}} \\ (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T)_{i \in [k]\setminus\mathcal{I}} \\ \tilde{\mathbf{c}}^T = \sum_{i \in [k]\setminus\mathcal{I}} \mathbf{s}_i^T \mathbf{P} + \mathbf{e}^T \end{array} \right) \quad (19)$$

$$\mathcal{D}_{2,3}^{(c,\text{alt})} := \left( \begin{array}{l} (\mathbf{B}_i)_{i \in [k]\setminus\mathcal{I}}, (\mathbf{A}_i)_{i \in [k]\setminus\mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}}, \mathbf{K}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ (c_{\text{uid},i,P})_{\text{uid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{I} \cup \{\tilde{i}_{\text{uid}}\})} \\ (\mathbf{c}_{i,A}^T)_{i \in [k]\setminus\mathcal{I}} \\ (\mathbf{c}_{i,Q}^T)_{i \in [k]\setminus\mathcal{I}} \\ \tilde{\mathbf{c}}^T \end{array} \right) \quad (20)$$

which are almost identical to  $\mathcal{D}_{1,2}^{(c,\text{alt})}$  and  $\mathcal{D}_{2,2}^{(c,\text{alt})}$  respectively, except that  $\mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T$  respectively  $\mathbf{c}_{\text{uid},i,Q}^T$  are omitted. To simulate  $\mathcal{D}_{1,2}^{(c,\text{alt})}$  from  $\mathcal{D}_{1,3}^{(c,\text{alt})}$ , one computes

$$(\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T) \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T = \mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{e}_{i,Q}^T \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T \stackrel{\$}{\approx} \mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{uid}} + \mathbf{e}_{\text{uid},i,Q}^T \pmod{q}$$

where the last  $\stackrel{\$}{\approx}$  follows from noise flooding, since

$$\chi_{(2)} \geq \lambda^{\omega(1)} \cdot \lambda \cdot \chi_{(1)} \cdot \chi_{(1)} \cdot n \geq \lambda^{\omega(1)} \cdot \|\mathbf{e}_{i,Q}^T \cdot \mathbf{K}_{\text{uid}}\|.$$

When  $\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T$  is replaced by uniformly random  $\mathbf{c}_{\text{uid},i,Q}^T$ , then the simulation becomes also uniformly random.

But by Lemma 9 the existence of  $\mathcal{G}$  is not possible<sup>20</sup> under  $\text{LWE}_{n,n+2m,q,\chi_{(1)}}$  and  $\text{LWE}_{m,\text{poly}(n),q,\chi_{(2)},\chi_{(1)}}$ , thus we have a contradiction. The proof is completed.  $\square$

**Lemma 8.** *If there exists a PPT  $\mathcal{A}$  that distinguishes  $\text{Hyb}_{b,1}^{(c,\text{alt})}$  and  $\text{Hyb}_{b,2}^{(c,\text{alt})}$  defined in the proof of Theorem 4 with non-negligible probability, then there exists a PPT  $\mathcal{B}$  that distinguishes the distributions  $\mathcal{D}_{1,1}^{(c,\text{alt})}$  and  $\mathcal{D}_{2,1}^{(c,\text{alt})}$  defined in Eq. (15) and Eq. (16) with non-negligible probability.*

*Proof.* Given such a PPT  $\mathcal{A}$ , we construct such a PPT  $\mathcal{B}$ .

**Reduction.** On input a sample from either  $\mathcal{D}_{1,1}^{(c,\text{alt})}$  or  $\mathcal{D}_{2,1}^{(c,\text{alt})}$  defined in Eq. (15) and Eq. (16) respectively, let  $\mathcal{B}$  proceed as follows:

- Parse  $\mathbf{P}, \mathbf{Q}, \mathbf{u}$  from the input sample, let public parameters be  $\text{pp} := (\mathbf{P}, \mathbf{Q}, \mathbf{u})$ .
- To generate the authority public and secret keys:
  - For corrupt authorities  $i \in \mathcal{I}$ , generate  $(\text{apk}_i, \text{ask}_i) \leftarrow \text{AuthSetup}(\text{pp})$ .
  - For honest authorities  $i \in [k] \setminus \mathcal{I}$ :
    - \* Parse  $\lceil \mathbf{A}_i, \mathbf{B}_i$  from the input sample.
    - \* Sample uniformly random matrix  $\lfloor \mathbf{A}_i \leftarrow \mathbb{Z}_q^{n_{br} \times m_{ic}}$  and a random low-norm matrix  $\mathbf{R} \leftarrow \chi_{(0)}^{m_{ic} \times m_{rc}}$ . Also sample a matrix  $\mathbf{T}_i \in \mathbb{Z}_q^{n_{br} \times m_{rc}}$  with a trapdoor  $\text{td}_{\mathbf{T}_i}$  using  $\text{TrapGen}$ .
    - \* Let

$$\mathbf{A}_i := \begin{pmatrix} \lceil \mathbf{A}_i & \lceil \mathbf{A}_i \\ \lfloor \mathbf{A}_i & \mathbf{A}_i \end{pmatrix} = \begin{pmatrix} \lceil \mathbf{A}_i & \mathbf{0} \\ \lfloor \mathbf{A}_i & \mathbf{T}_i \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{R} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} = \begin{pmatrix} \lceil \mathbf{A}_i & \lceil \mathbf{A}_i \mathbf{R} \\ \lfloor \mathbf{A}_i & \lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i \end{pmatrix} \pmod{q}.$$

- \* Set  $\text{apk}_i := (\mathbf{A}_i, \mathbf{B}_i)$ .

- All key queries for the corrupt authorities  $i \in \mathcal{I}$  are answered as in the scheme, using  $\text{td}_{\mathbf{A}_i}$ . For each honest authority key query  $(\text{uid}, i, \mathbf{x})$  with  $i \in [k] \setminus \mathcal{I}$ :
  - Parse  $\mathbf{v}_{\text{uid},i} := \lceil \mathbf{A}_i^{-1} (\mathbf{P} \mathbf{k}_{\text{uid}})$  and  $\mathbf{X}_{\text{uid},i} := \lceil \mathbf{A}_i^{-1} (\mathbf{Q} \mathbf{K}_{\text{uid}})$  from the input sample.
  - Sample  $\mathbf{w}_{\text{uid},i} := \mathbf{T}_i^{-1} (-\lfloor \mathbf{A}_i \mathbf{v}_{\text{uid},i})$  and  $\mathbf{Y}_{\text{uid},i} := \mathbf{T}_i^{-1} (\hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} - \lfloor \mathbf{A}_i \mathbf{X}_{\text{uid},i})$  using  $\text{td}_{\mathbf{T}_i}$ .
  - Answer with

$$\mathbf{U}_{\text{uid},i} = \begin{pmatrix} \mathbf{I} & -\mathbf{R} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{v}_{\text{uid},i} & \mathbf{X}_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix} = \begin{pmatrix} \mathbf{v}_{\text{uid},i} - \mathbf{R} \mathbf{w}_{\text{uid},i} & \mathbf{X}_{\text{uid},i} - \mathbf{R} \mathbf{Y}_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix}.$$

<sup>20</sup>Lemma 9 is almost identical to Lemma 7, except that  $\bar{\mathbf{A}}_i$  is replaced by  $\lceil \mathbf{A}_i$ . For completeness we provide Lemma 9.

Note that it holds that

$$\begin{pmatrix} \lceil \mathbf{A}_i & \mathbf{A}_i^\top \\ \lfloor \mathbf{A}_i & \mathbf{A}_i \rceil \end{pmatrix} \mathbf{U}_{\text{uid},i} = \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \bmod q.$$

- To generate the ciphertext, sample random  $\mathbf{s} \leftarrow_{\$} \mathbb{Z}_q^{nm}$  and random  $\mathbf{s}_i \leftarrow_{\$} \mathbb{Z}_q^n$  for all  $i \in \mathcal{I}$ , and:
  - For  $i \in \mathcal{I}$ , compute  $\mathbf{c}_i^\top = (\mathbf{s}_i^\top \mid \mathbf{s}^\top) \mathbf{A}_i + \mathbf{e}_{i,A}^\top$  where  $\mathbf{e}_{i,A} \leftarrow_{\$} \chi_{(1)}^{m_{lc} + m_{rc}}$ .
  - For  $i \in [k] \setminus \mathcal{I}$ , parse  $\lceil \mathbf{c}_{i,A}^\top$  from the input sample, and:
    - \* Compute  $\mathbf{f}_0^\top := \lceil \mathbf{c}_{i,A}^\top + \mathbf{s}^\top \lfloor \mathbf{A}_i + \lfloor \mathbf{e}_{i,A}^\top \bmod q$  where  $\lfloor \mathbf{e}_{i,A} \leftarrow_{\$} \chi_{(1)}^{m_{lc}}$ .
    - \* Compute  $\mathbf{f}_1^\top := \lceil \mathbf{c}_{i,A}^\top \mathbf{R} + \mathbf{s}^\top (\lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i) + \mathbf{e}_{i,A}^\top \bmod q$  where  $\mathbf{e}_{i,A} \leftarrow_{\$} \chi_{(1)}^{m_{rc}}$ .
    - \* Let  $\mathbf{c}_i^\top = (\mathbf{f}_0^\top \mid \mathbf{f}_1^\top)$ .
  - Parse  $\mathbf{c}_{i,Q}^\top$  for all  $i \in [k] \setminus \mathcal{I}$  from input. Compute  $\mathbf{c}_{i,Q}^\top = \mathbf{s}_i^\top \mathbf{Q} + \mathbf{e}_{i,Q}^\top \bmod q$  for all  $i \in \mathcal{I}$  where  $\mathbf{e}_{i,Q}^\top \leftarrow_{\$} \chi_{(1)}^m$ . Concatenate to obtain  $\mathbf{c}_0^\top = (\mathbf{c}_{1,Q}^\top \mid \dots \mid \mathbf{c}_{k,Q}^\top)$ .
  - Parse  $\tilde{\mathbf{c}}^\top$  from input sample, compute  $\mathbf{c}^\top := \tilde{\mathbf{c}}^\top + \sum_{i \in \mathcal{I}} \mathbf{s}_i^\top \mathbf{P} + \mathbf{s}^\top (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mu_b \mathbf{g}^\top$ .
  - Let the ciphertext be  $(\mathbf{c}, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_k)$ .
- Pass all terms computed above to  $\mathcal{A}$ , then return whatever  $\mathcal{A}$  returns.

**Analysis.** Below we argue that, if the input to  $\mathcal{B}$  is  $\mathcal{D}_{1,1}^{(c,\text{alt})}$ , then the above simulation is statistically close to  $\text{Hyb}_{b,1}^{(c,\text{alt})}$ ; else if the input is  $\mathcal{D}_{2,1}^{(c,\text{alt})}$ , the simulation is statistically close to  $\text{Hyb}_{b,2}^{(c,\text{alt})}$ .

Simulating  $\text{Hyb}_{b,1}^{(c,\text{alt})}$ : Suppose the input to  $\mathcal{B}$  is  $\mathcal{D}_{1,1}^{(c,\text{alt})}$ , consider the following hybrids:

- $\mathcal{D}'_0$ : The simulation from  $\mathcal{B}$  as described above, that is:

$$\begin{aligned} & (\mathbf{B}_i)_{i \in [k]}, (\mathbf{A}_i)_{i \in \mathcal{I}}, \left( \begin{pmatrix} \lceil \mathbf{A}_i & \lceil \mathbf{A}_i \mathbf{R} \\ \lfloor \mathbf{A}_i & \lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i \end{pmatrix} \bmod q \right)_{i \in [k] \setminus \mathcal{I}}, \\ & (\text{td}_{\mathbf{A}_i})_{i \in \mathcal{I}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{uid}})_{\text{uid} \in \mathcal{U}}, \mathbf{u} \\ \mathbf{U}_{\text{uid},i} &= \mathbf{A}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \quad \forall i \in \mathcal{I}, \text{uid} \in \mathcal{U} : i \in \mathcal{I}_{\text{uid}} \\ \mathbf{U}_{\text{uid},i} &= \begin{pmatrix} \mathbf{v}_{\text{uid},i} - \mathbf{R}\mathbf{w}_{\text{uid},i} & \mathbf{X}_{\text{uid},i} - \mathbf{R}\mathbf{Y}_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix} \bmod q \quad \forall \text{uid} \in \mathcal{U}, i \in \mathcal{I}_{\text{uid}} \cap ([k] \setminus \mathcal{I}) \\ \mathbf{c}_i^\top &= (\mathbf{s}_i^\top \mid \mathbf{s}^\top) \mathbf{A}_i + \mathbf{e}_i^\top \quad \forall i \in \mathcal{I}, \quad \mathbf{c}_i^\top = (\mathbf{f}_0^\top \mid \mathbf{f}_1^\top) \quad \forall i \in [k] \setminus \mathcal{I} \\ \mathbf{c}_0^\top &= (\mathbf{c}_{1,Q}^\top \mid \dots \mid \mathbf{c}_{k,Q}^\top) \\ \mathbf{c}^\top &:= \tilde{\mathbf{c}}^\top + \sum_{i \in \mathcal{I}} \mathbf{s}_i^\top \mathbf{P} + \mathbf{s}^\top (\mathbf{B}_f \mathbf{u} \otimes \mathbf{I}_m) + \mu_b \mathbf{g}^\top \end{aligned}$$

where  $\mathbf{f}_0^\top = \lceil \mathbf{c}_{i,A}^\top + \mathbf{s}^\top \lfloor \mathbf{A}_i + \lfloor \mathbf{e}_{i,A}^\top \bmod q$  and  $\mathbf{f}_1^\top = \lceil \mathbf{c}_{i,A}^\top \mathbf{R} + \mathbf{s}^\top (\lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i) + \mathbf{e}_{i,A}^\top \bmod q$ .

Recall that in this case  $\lceil \mathbf{c}_{i,A}^\top = \mathbf{s}_i^\top \lceil \mathbf{A}_i + \lceil \mathbf{e}_{i,A}^\top \bmod q$  for  $i \in [k] \setminus \mathcal{I}$ .

- $\mathcal{D}'_1$ : We change the query answers for the honest authorities: For all  $i \in [k] \setminus \mathcal{I}$ ,  $\text{uid} \in \mathcal{U}$ , we swap

$$\begin{pmatrix} \mathbf{v}_{\text{uid},i} - \mathbf{R}\mathbf{w}_{\text{uid},i} & \mathbf{X}_{\text{uid},i} - \mathbf{R}\mathbf{Y}_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix} \quad \text{to} \quad \begin{pmatrix} \mathbf{v}'_{\text{uid},i} & \mathbf{X}'_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix}$$



where  $\mathbf{v}'_{\text{uid},i} \leftarrow \chi_{(1)}^{m_{lc}}$  and  $\mathbf{X}'_{\text{uid},i} \leftarrow \chi_{(1)}^{m_{rc} \times m_\ell}$  are Gaussian subject to

$$\mathbf{A}_i \begin{pmatrix} \mathbf{v}'_{\text{uid},i} & \mathbf{X}'_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix} = \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ & \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \bmod q.$$

We recall  $\mathbf{A}_i = \begin{pmatrix} \lceil \mathbf{A}_i & \lceil \mathbf{A}_i \mathbf{R} \\ \lfloor \mathbf{A}_i & \lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i \end{pmatrix} \bmod q$  in the above.

We have  $\mathcal{D}'_0 \stackrel{\approx}{\approx} \mathcal{D}'_1$  by noise flooding, due to

$$\mathbf{v}_{\text{uid},i} - \mathbf{R}\mathbf{w}_{\text{uid},i} \stackrel{\approx}{\approx} \mathbf{v}'_{\text{uid},i} \quad \text{and} \quad \mathbf{X}_{\text{uid},i} - \mathbf{R}\mathbf{Y}_{\text{uid},i} \stackrel{\approx}{\approx} \mathbf{X}'_{\text{uid},i}$$

since  $\chi_{(1)} \geq \lambda^{\omega(1)} \cdot \lambda^2 \cdot \chi_{(0)} \cdot \chi_{(0)} \cdot m_{rc} \geq \lambda^{\omega(1)} \cdot \|\mathbf{R} \cdot \mathbf{w}_{\text{uid},i}\|$  and  $\chi_{(1)} \geq \lambda^{\omega(1)} \cdot \lambda^2 \cdot \chi_{(0)} \cdot \chi_{(0)} \cdot m_{rc} \geq \lambda^{\omega(1)} \cdot \|\mathbf{R} \cdot \mathbf{Y}_{\text{uid},i}\|$  with overwhelming probability.

As a result all query answers are independent of  $\mathbf{R}$ .

- $\mathcal{D}'_2$ : We change the ciphertext component  $\mathbf{c}_i$  for the honest authorities. For all  $\mathbf{c}_i^{\text{T}} = (\mathbf{f}_0^{\text{T}}, \mathbf{f}_1^{\text{T}})$  where  $i \in [k] \setminus \mathcal{I}$ , we swap  $\mathbf{f}_0^{\text{T}}$  from

$$\mathbf{s}_i^{\text{T}\lceil} \mathbf{A}_i + \lceil \mathbf{e}_{i,A}^{\text{T}} + \mathbf{s}_i^{\text{T}} \lfloor \mathbf{A}_i + \lfloor \mathbf{e}_{i,A}^{\text{T}} \quad \text{to} \quad \mathbf{s}_i^{\text{T}\lceil} \mathbf{A}_i + \mathbf{s}_i^{\text{T}} \lfloor \mathbf{A}_i + \lfloor \mathbf{e}_{i,A}^{\text{T}},$$

and we swap  $\mathbf{f}_1^{\text{T}}$  from

$$(\mathbf{s}_i^{\text{T}\lceil} \mathbf{A}_i + \lceil \mathbf{e}_{i,A}^{\text{T}}) \mathbf{R} + \mathbf{s}_i^{\text{T}} (\lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i) + \mathbf{e}_{i,A}^{\text{T}} \quad \text{to} \quad \mathbf{s}_i^{\text{T}\lceil} \mathbf{A}_i \mathbf{R} + \mathbf{s}_i^{\text{T}} (\lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i) + \mathbf{e}_{i,A}^{\text{T}}.$$

We have  $\mathcal{D}'_1 \stackrel{\approx}{\approx} \mathcal{D}'_2$  by noise flooding, due to

$$\lceil \mathbf{e}_{i,A}^{\text{T}} + \lfloor \mathbf{e}_{i,A}^{\text{T}} \stackrel{\approx}{\approx} \lfloor \mathbf{e}_{i,A}^{\text{T}} \quad \text{and} \quad \lceil \mathbf{e}_{i,A}^{\text{T}} \mathbf{R} + \mathbf{e}_{i,A}^{\text{T}} \stackrel{\approx}{\approx} \mathbf{e}_{i,A}^{\text{T}},$$

since  $\chi_{(1)} \geq \lambda^{\omega(1)} \cdot \lambda \cdot \chi_{(0)} \geq \lambda^{\omega(1)} \cdot \|\lceil \mathbf{e}_{i,A}\|$  and  $\chi_{(1)} \geq \lambda^{\omega(1)} \cdot \lambda \cdot \chi_{(0)} \cdot \chi_{(0)} \cdot m_{rc} \geq \lambda^{\omega(1)} \cdot \|\lceil \mathbf{e}_{i,A}^{\text{T}} \mathbf{R}\|$ . As a result we have for  $i \in [k] \setminus \mathcal{I}$

$$\begin{aligned} \mathbf{c}_i^{\text{T}} = (\mathbf{f}_0^{\text{T}} \mid \mathbf{f}_1^{\text{T}}) &= (\mathbf{s}_i^{\text{T}\lceil} \mathbf{A}_i + \mathbf{s}_i^{\text{T}} \lfloor \mathbf{A}_i + \lfloor \mathbf{e}_{i,A}^{\text{T}} \mid \mathbf{s}_i^{\text{T}\lceil} \mathbf{A}_i \mathbf{R} + \mathbf{s}_i^{\text{T}} (\lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i) + \mathbf{e}_{i,A}^{\text{T}}) \\ &= (\mathbf{s}_i^{\text{T}} \mid \mathbf{s}_i^{\text{T}}) \begin{pmatrix} \lceil \mathbf{A}_i & \lceil \mathbf{A}_i \mathbf{R} \\ \lfloor \mathbf{A}_i & \lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i \end{pmatrix} + (\lfloor \mathbf{e}_{i,A}^{\text{T}} \mid \mathbf{e}_{i,A}^{\text{T}}) \\ &= (\mathbf{s}_i^{\text{T}} \mid \mathbf{s}_i^{\text{T}}) \mathbf{A}_i + \mathbf{e}_{i,A}^{\text{T}} \bmod q. \end{aligned}$$

- $\mathcal{D}'_3$ : We change the  $\text{apk}$  for the honest authorities: For all  $i \in [k] \setminus \mathcal{I}$ , we swap  $\text{apk}_i = \begin{pmatrix} \lceil \mathbf{A}_i & \lceil \mathbf{A}_i \mathbf{R} \\ \lfloor \mathbf{A}_i & \lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i \end{pmatrix} \bmod q$  to a uniformly random  $\mathbf{A}_i$ .

We have  $\mathcal{D}'_2 \stackrel{\approx}{\approx} \mathcal{D}'_3$ . This follows from (1)  $\lceil \mathbf{A}_i$  and  $\lfloor \mathbf{A}_i$  are uniformly random, and hence (2)  $\lceil \mathbf{A}_i \mathbf{R} \bmod q$  and  $\lfloor \mathbf{A}_i \mathbf{R} \bmod q$  are statistically close to uniform by Lemma 4, which applies since  $\chi_{(1)} \geq \omega(\sqrt{\log m_{lc}})$  and  $m_{lc} \geq 2(n_{tr} + n_{br}) \log q$ .

Observe  $\mathcal{D}'_3 \stackrel{\text{c,alt}}{\approx} \text{Hyb}_{b,1}^{(\text{c,alt})}$ . Thus we conclude  $\mathcal{B}$  statistically simulates  $\text{Hyb}_{b,1}^{(\text{c,alt})}$ .

Simulating  $\text{Hyb}_{b,2}^{(\text{c,alt})}$ : Suppose the input to  $\mathcal{B}$  is  $\mathcal{D}_{2,1}^{(\text{c,alt})}$ , consider the following hybrids:

- $\mathcal{D}'_0$ : The simulation output by  $\mathcal{B}$  as described. Recall that in this case  $\lceil \mathbf{c}_{i,A}^{\text{T}}$  is uniformly random for  $i \in [k] \setminus \mathcal{I}$ .

- $\mathcal{D}'_1$ : We change the query answers for the honest authorities: For all  $i \in [k] \setminus \mathcal{I}$ ,  $\text{uid} \in \mathcal{U}$ , we swap

$$\begin{pmatrix} \mathbf{v}_{\text{uid},i} - \mathbf{R}\mathbf{w}_{\text{uid},i} & \mathbf{X}_{\text{uid},i} - \mathbf{R}\mathbf{Y}_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix} \quad \text{to} \quad \begin{pmatrix} \mathbf{v}'_{\text{uid},i} & \mathbf{X}'_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix}$$

where  $\mathbf{v}'_{\text{uid},i} \leftarrow \mathcal{X}_{(1)}^{m_{lc}}$  and  $\mathbf{X}'_{\text{uid},i} \leftarrow \mathcal{X}_{(1)}^{m_{rc} \times m_{\ell}}$  are Gaussian subject to

$$\mathbf{A}_i \begin{pmatrix} \mathbf{v}'_{\text{uid},i} & \mathbf{X}'_{\text{uid},i} \\ \mathbf{w}_{\text{uid},i} & \mathbf{Y}_{\text{uid},i} \end{pmatrix} = \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{uid}} & \mathbf{Q}\mathbf{K}_{\text{uid}} \\ \hat{\mathbf{B}}_{\text{uid},i} \otimes \mathbf{k}_{\text{uid}} \end{pmatrix} \pmod{q}.$$

We have  $\mathcal{D}'_0 \stackrel{\mathcal{S}}{\approx} \mathcal{D}'_1$  by the same argument as in the previous case.

- $\mathcal{D}'_2$ : We change  $\text{apk}_i$  and the ciphertext component  $\mathbf{c}_i$  for the honest authorities: For all  $i \in [k] \setminus \mathcal{I}$ , we swap  $\text{apk}_i = \begin{pmatrix} \lceil \mathbf{A}_i & \lceil \mathbf{A}_i \mathbf{R} \\ \lfloor \mathbf{A}_i & \lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i \end{pmatrix}$  and  $\mathbf{c}_i^{\text{T}} = (\lceil \mathbf{c}_{i,A}^{\text{T}} + \mathbf{s}^{\text{T}} \lfloor \mathbf{A}_i + \lfloor \mathbf{e}_{i,A}^{\text{T}} \mid \lceil \mathbf{c}_{i,A}^{\text{T}} \mathbf{R} + \mathbf{s}^{\text{T}} (\lfloor \mathbf{A}_i \mathbf{R} + \mathbf{T}_i) + \mathbf{e}_{i,A}^{\text{T}})$  to uniformly random.

We have  $\mathcal{D}'_1 \stackrel{\mathcal{S}}{\approx} \mathcal{D}'_2$ . This follows from (1)  $\lceil \mathbf{A}_i, \lfloor \mathbf{A}_i$  and  $\lceil \mathbf{c}_{i,A}^{\text{T}}$  are uniformly random, and hence (2)  $\lceil \mathbf{A}_i \mathbf{R} \pmod{q}, \lfloor \mathbf{A}_i \mathbf{R} \pmod{q}$  and  $\lceil \mathbf{c}_{i,A}^{\text{T}} \mathbf{R} \pmod{q}$  are statistically close to uniform by Lemma 4, which applies since  $\chi_{(0)} \geq \omega(\sqrt{\log m_{lc}})$  and  $m_{lc} \geq 2(n_{tr} + n_{br} + 1) \log q$ .

Observe  $\mathcal{D}'_2 \stackrel{\mathcal{P}}{=} \text{Hyb}_{b,2}^{(c,\text{alt})}$ . Thus we conclude  $\mathcal{B}$  statistically simulates  $\text{Hyb}_{b,2}^{(c,\text{alt})}$ . This completes the proof.  $\square$

**Lemma 9.** For the distributions  $\mathcal{D}_{1,3}^{(c,\text{alt})}$  and  $\mathcal{D}_{2,3}^{(c,\text{alt})}$  defined in Eq. (19) and Eq. (20), we have  $\mathcal{D}_{1,3}^{(c,\text{alt})} \stackrel{\mathcal{L}}{\approx} \mathcal{D}_{2,3}^{(c,\text{alt})}$  assuming

$$\text{LWE}_{n,n+2m,q,\chi_{(1)}} \quad \text{and} \quad \text{LWE}_{m,\text{poly}(n),q,\chi_{(2)},\chi_{(1)}}.$$

*Proof.* Continue with the notation in the proof of Theorem 4, where we have let  $i^* \in [k] \setminus \mathcal{I}$  be an arbitrarily fixed honest authority (which exists because  $[k] \neq \mathcal{I}$ ), and for each  $\text{uid} \in \mathcal{U}$ , we have let  $\tilde{i}_{\text{uid}} \in [k] \setminus \mathcal{I}$  be an honest authority where  $\text{uid}$  is not queried by the adversary (which exists by design of security experiment).

We define the following sequence of hybrid distributions:

- $\mathcal{D}_{1,3}^{(c,\text{alt})}$  as in Eq. (17).
- $\mathcal{D}_{1,3,1}$ : For each  $\text{uid} \in \mathcal{U}$ , if  $i^* \neq \tilde{i}_{\text{uid}}$ , then do the following:

We swap  $\mathbf{s}_{i^*}^{\text{T}} \mathbf{P}\mathbf{k}_{\text{uid}} + e_{i^*,\text{uid},P}$  to

$$\left( \sum_{i \in [k] \setminus \mathcal{I}} \mathbf{s}_i^{\text{T}} \mathbf{P} + \mathbf{e}^{\text{T}} \right) \mathbf{k}_{\text{uid}} - \left( \sum_{i \in [k] \setminus \mathcal{I}: i \neq i^*} \mathbf{s}_i^{\text{T}} \mathbf{P}\mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \right) + e_{i^*,\text{uid},P}$$

We have  $\mathcal{D}_{1,3}^{(c,\text{alt})} \stackrel{\mathcal{S}}{\approx} \mathcal{D}_{1,3,1}$  by noise flooding, which is due to the equality

$$\mathbf{s}_{i^*}^{\text{T}} \mathbf{P}\mathbf{k}_{\text{uid}} = \left( \sum_{i \in [k] \setminus \mathcal{I}} \mathbf{s}_i^{\text{T}} \mathbf{P} \right) \mathbf{k}_{\text{uid}} - \sum_{i \in [k] \setminus \mathcal{I}: i \neq i^*} \mathbf{s}_i^{\text{T}} \mathbf{P}\mathbf{k}_{\text{uid}}.$$

and that

$$e_{i^*,\text{uid},P} \stackrel{\mathcal{S}}{\approx} \mathbf{e}^{\text{T}} \mathbf{k}_{\text{uid}} - \sum_{i \in [k] \setminus \mathcal{I}: i \neq i^*} e_{\text{uid},i,P} + e_{i^*,\text{uid},P},$$

since

$$\chi_{(3)} \geq \lambda^{\omega(1)} (\lambda^2 \chi_{(1)}^2 m + \lambda k \chi_{(2)}) \geq \lambda^{\omega(1)} \left\| \mathbf{e}^T \mathbf{k}_{\text{uid}} - \sum_{i \in [k] \setminus \mathcal{I}: i \neq i^*} e_{\text{uid},i,P} \right\|.$$

Notice that in  $\mathcal{D}_{1,3,1}$  the remaining terms involving  $\mathbf{s}_{i^*}$  are  $\mathbf{s}_{i^*}^T \mathbf{A}_{i^*} + \mathbf{e}_{i^*,A}^T$ ,  $\mathbf{s}_{i^*}^T \mathbf{P} + \mathbf{e}_{i^*,P}^T$ , and  $\mathbf{s}_{i^*}^T \mathbf{Q} + \mathbf{e}_{i^*,Q}^T$ .

- $\mathcal{D}_{1,3,2}$ : We swap

$$\mathbf{s}_{i^*}^T \mathbf{A}_{i^*} + \mathbf{e}_{i^*,A}^T, \quad \mathbf{s}_{i^*}^T \mathbf{P} + \mathbf{e}_{i^*,P}^T \quad \text{and} \quad \mathbf{s}_{i^*}^T \mathbf{Q} + \mathbf{e}_{i^*,Q}^T$$

to uniformly random.

We have  $\mathcal{D}_{1,3,1} \stackrel{\text{c}}{\approx} \mathcal{D}_{1,3,2}$  by the  $\text{LWE}_{n,n+2m,q,\chi(1)}$  assumption.

Notice that as a result  $\tilde{\mathbf{c}}$  is also uniformly random.

- $\mathcal{D}_{1,3,3}$ : For all  $\text{uid} \in \mathcal{U}$ , all  $i \in [k] \setminus (\mathcal{I} \cup \{i^*\})$ , we swap

$$\mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \quad \text{to} \quad (\mathbf{s}_i^T \mathbf{P} + \tilde{\mathbf{e}}_{\text{uid},i,P}^T) \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$$

where  $\tilde{\mathbf{e}}_{\text{uid},i,P} \stackrel{\text{c}}{\leftarrow} \chi_{(1)}^m$ .

We have  $\mathcal{D}_{1,3,2} \stackrel{\text{c}}{\approx} \mathcal{D}_{1,3,3}$  by noise flooding, due to  $\tilde{\mathbf{e}}_{\text{uid},i,P}^T \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \stackrel{\text{c}}{\approx} e_{\text{uid},i,P}$  since  $\chi_{(2)} \geq \lambda^{\omega(1)} \lambda^2 \chi_{(1)} \chi_{(1)} m \geq \lambda^{\omega(1)} \|\tilde{\mathbf{e}}_{\text{uid},i,P}^T \mathbf{k}_{\text{uid}}\|$ .

- $\mathcal{D}_{1,3,4}$ : For all  $\text{uid} \in \mathcal{U}$ , all  $i \in [k] \setminus (\mathcal{I} \cup \{i^*\})$ , we swap

$$(\mathbf{s}_i^T \mathbf{P} + \tilde{\mathbf{e}}_{\text{uid},i,P}^T) \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P} \quad \text{to} \quad \mathbf{b}_{\text{uid},i,P}^T \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$$

where  $\mathbf{b}_{\text{uid},i,P}^T$  is uniformly random, and we also swap

$$\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T \quad \text{and} \quad \mathbf{s}_i^T \mathbf{A}_i + \mathbf{e}_{i,A}^T$$

to uniformly random.

We have  $\mathcal{D}_{1,3,3} \stackrel{\text{c}}{\approx} \mathcal{D}_{1,3,4}$  by the  $\text{LWE}_{n,n+2m,q,\chi(1)}$  assumption.

- $\mathcal{D}_{1,3,5}$ : For all  $\text{uid} \in \mathcal{U}$ , all  $i \in [k] \setminus (\mathcal{I} \cup \{i^*\})$ , we swap

$$\mathbf{b}_{\text{uid},i,P}^T \mathbf{k}_{\text{uid}} + e_{\text{uid},i,P}$$

to uniformly random.

We have  $\mathcal{D}_{1,3,4} \stackrel{\text{c}}{\approx} \mathcal{D}_{1,3,5}$  by the (low-norm)  $\text{LWE}_{m,\text{poly}(n),q,\chi(2),\chi(1)}$  assumption.

Observe that  $\mathcal{D}_{1,3,5} \stackrel{\text{c}}{\approx} \mathcal{D}_{2,3}^{(\text{c,alt})}$ , the proof is completed.  $\square$

## B Proofs for MC-ABE

We provide the remaining proofs for the MC-ABE construction. For clarity we also restate the theorem and lemma appeared in the main content.

## B.1 Proof of Lemma 6

**Lemma 6.** *For the distributions  $\mathcal{D}_{1,2}^{(h)}$  and  $\mathcal{D}_{2,2}^{(h)}$  defined in Eq. (7) and Eq. (8), we have  $\mathcal{D}_{1,2}^{(h)} \stackrel{c}{\approx} \mathcal{D}_{2,2}^{(h)}$  assuming*

$$\text{LWE}_{n,2m(m+2),q,\chi_{(0)}} \quad \text{and} \quad \text{TensorLWE}_{n,(k+2)m+1,q,\chi_{(0)},\chi_{(0)},\ell,\mathcal{Q}}.$$

*Proof.* We define the following sequence of hybrid distributions:

- $\mathcal{D}_{1,2}^{(h)}$  as in Eq. (7).
- $\mathcal{D}_{1,2,1}$ : For each  $\text{cid} \in \mathcal{C}$ , we swap  $\mathbf{s}_2^T \mathbf{P} \mathbf{k}_{\text{cid}} + e_{2,\text{cid},P}$  to

$$\begin{aligned} & \left( \sum_{i \in [2,k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{v} \otimes \mathbf{I}_m) + \mathbf{e}^T \right) \mathbf{k}_{\text{cid}} - \sum_{i \in [3,k]} (\mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}} + \mathbf{e}_{\text{cid},i,P}^T) \\ & - \left[ \mathbf{s}^T (\mathbf{A} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid},A}^T \mid \right. \\ & \quad \left. \left( \mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}^*,1} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}^*,\text{cid},1,B}^T \mid \left( \mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid},i,B}^T - \mathbf{e}_{i,Q}^T \mathbf{K}_{\text{cid}} \right)_{i \in [2,k]} \right) \right. \\ & \quad \left. \cdot \mathbf{H}_{\mathbf{B},f^*,\mathbf{x}_{\text{cid}^*,\text{cid}}} \right] \cdot \mathbf{r}_{f^*} \\ & + (\mathbf{0} \mid \mathbf{s}^T (\mathbf{G} \mathbf{r}_{f^*} \otimes \mathbf{k}_{\text{cid}}) + e_{f^*,\text{cid}}) + e_{1,\text{cid},P} \end{aligned}$$

where  $e_{f^*,\text{cid}} \leftarrow \chi_{(0)}$ ,  $\mathbf{x}_{\text{cid}^*,\text{cid}}^T := (\mathbf{x}_{\text{cid}^*,1}^T \mid \mathbf{x}_{\text{cid},2}^T \mid \dots \mid \mathbf{x}_{\text{cid},k}^T)$ ,  $(\mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid},i,B}^T)_{i \in [k]}$  denotes the horizontal concatenation of  $\mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid},i,B}^T$ ,  $f^* \in \mathcal{F}$  is any function such that  $f^*(\mathbf{x}_{\text{cid}^*,\text{cid}}) = 1$ , and  $\mathbf{r}_{f^*} := (\mathbf{A} \mid \mathbf{B}_{f^*})^{-1}(\mathbf{v})$ . Note that in the above we make use of  $\mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}^*,1} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}^*,\text{cid},1,B}^T$ , and for  $i \in [2,k]$ , the term  $\mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}^*,i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}^*,i,B}^T - \mathbf{e}_{i,Q}^T \mathbf{K}_{\text{cid}}$  is obtained from

$$(\mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}^*,i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}^*,i,B}^T) - (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T) \mathbf{K}_{\text{cid}}.$$

We have  $\mathcal{D}_{1,2}^{(h)} \stackrel{s}{\approx} \mathcal{D}_{1,2,1}$  by noise flooding, which is due to the equality

$$\begin{aligned} & \mathbf{s}_2^T \mathbf{P} \mathbf{k}_{\text{cid}} \\ & = \left( \sum_{i \in [2,k]} \mathbf{s}_i^T \mathbf{P} + \mathbf{s}^T (\mathbf{v} \otimes \mathbf{I}_m) \right) \mathbf{k}_{\text{cid}} - \sum_{i \in [3,k]} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}} \\ & \quad - (\mathbf{s}^T (\mathbf{A} \otimes \mathbf{k}_{\text{cid}}) \mid (\mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}}), (\mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}}))_{i \in [2,k]}) \mathbf{H}_{\mathbf{B},f^*,\mathbf{x}_{\text{cid}^*,\text{cid}}}) \mathbf{r}_{f^*} \\ & \quad + (\mathbf{0} \mid \mathbf{s}^T (\mathbf{G} \mathbf{r}_{f^*} \otimes \mathbf{k}_{\text{cid}})) \end{aligned}$$

and that

$$\begin{aligned} e_{2,\text{cid},P} & \stackrel{s}{\approx} \mathbf{e}^T \mathbf{k}_{\text{cid}} - \sum_{i \in [3,k]} e_{\text{cid},i,P} \\ & \quad - (\mathbf{e}_{\text{cid},A}^T \mid (\mathbf{e}_{\text{cid}^*,\text{cid},1,B}^T, (\mathbf{e}_{\text{cid},i,B}^T - \mathbf{e}_{i,Q}^T \mathbf{K}_{\text{cid}})_{i \in [2,k]}) \mathbf{H}_{\mathbf{B},f^*,\mathbf{x}_{\text{cid}^*,\text{cid}}}) \mathbf{r}_{f^*} \\ & \quad + e_{f^*,\text{cid}} + e_{2,\text{cid},P} \end{aligned}$$

because

$$\chi_{(2)} \geq \lambda^{\omega(1)} \cdot \text{poly}(\lambda, m) (\chi_{(0)}^2 + k\chi_{(1)} + \chi_{(1)} \ell m^{O(d)} \sigma)$$

$$\geq \lambda^{\omega(1)} \left\| \mathbf{e}^T \mathbf{k}_{\text{cid}} - \sum_{i \in [3, k]} e_{\text{cid}, i, P} + e_{f^*, \text{cid}} \right. \\ \left. - \left( \mathbf{e}_{\text{cid}, A}^T \mid \left( \mathbf{e}_{\text{cid}^*, \text{cid}, 1, B}^T \mid \left( \mathbf{e}_{\text{cid}, i, B}^T - \mathbf{e}_{i, Q}^T \right)_{i \in [2, k]} \right) \mathbf{H}_{\mathbf{B}, f^*, \mathbf{x}_{\text{cid}^*, \text{cid}}} \right) \mathbf{r}_{f^*} \right\|$$

Notice that the only remaining terms in  $\mathcal{D}_{1,2,1}$  involving  $\mathbf{s}_2$  are  $\mathbf{s}_2^T \overline{\mathbf{C}}_2 + \overline{\mathbf{e}}_{2, C}^T$ ,  $\mathbf{s}_2^T \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}, 2} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}, 2, B}^T$ ,  $\mathbf{s}_2^T \mathbf{Q} + \mathbf{e}_{2, Q}^T$  and  $\mathbf{s}_2^T \mathbf{P} + \mathbf{e}_{2, P}^T$ . Also, looking ahead, to argue the above simulation is pseudorandom, it suffices to argue  $\mathbf{s}^T (\mathbf{G} \mathbf{r}_{f^*} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{f^*, \text{cid}}^T$  is.

- $\mathcal{D}_{1,2,2}$ : For all  $\text{cid} \in \mathcal{C}$ , all  $i \in [2, k]$ , we swap

$$\mathbf{s}_i^T \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}, i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}, i, B}^T \\ \text{to } (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i, Q}^T) \mathbf{K}_{\text{cid}} + \mathbf{s}^T (\hat{\mathbf{B}}_{\text{cid}, i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}, i, B}^T.$$

We have  $\mathcal{D}_{1,2,1} \stackrel{\S}{\approx} \mathcal{D}_{1,2,2}$  by noise flooding, since  $\chi(1) \geq \lambda^{\omega(1)} \cdot \lambda \cdot \chi(0) \cdot \chi(0) \cdot n \geq \lambda^{\omega(1)} \cdot \|\mathbf{e}_{i, Q}^T \cdot \mathbf{K}_{\text{cid}}\|$ . Now in  $\mathcal{D}_{1,2,2}$  the remaining terms involving  $\mathbf{s}_2$  are  $\mathbf{s}_2^T \overline{\mathbf{C}}_2 + \overline{\mathbf{e}}_{2, A}^T$ ,  $\mathbf{s}_2^T \mathbf{Q} + \mathbf{e}_{2, Q}^T$ , and  $\mathbf{s}_2^T \mathbf{P} + \mathbf{e}_{2, P}^T$ .

- $\mathcal{D}_{1,2,3}$ : We swap

$$\mathbf{s}_2^T \overline{\mathbf{C}}_2 + \mathbf{e}_2^T, \quad \mathbf{s}_2^T \mathbf{Q} + \mathbf{e}_{2, Q}^T \quad \text{and} \quad \mathbf{s}_2^T \mathbf{P} + \mathbf{e}^T$$

to uniformly random.

We have  $\mathcal{D}_{1,2,2} \stackrel{\S}{\approx} \mathcal{D}_{1,2,3}$  by the  $\text{LWE}_{n, 2m(m+2), q, \chi(0)}$  assumption.

Notice that as a result  $\mathbf{c}$  is also uniformly random.

- $\mathcal{D}_{1,2,4}$ : For each  $i \in [3, k]$  and all  $\text{cid} \in \mathcal{C}$ , we swap

$$\mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}} + e_{\text{cid}, i, P} \quad \text{to} \quad (\mathbf{s}_i^T \mathbf{P} + \tilde{\mathbf{e}}_{\text{cid}, i, P}^T) \mathbf{k}_{\text{cid}} + e_{\text{cid}, i, P}.$$

where  $\tilde{\mathbf{e}}_{\text{cid}, i, P} \leftarrow_{\S} \chi(0)$ .

We have  $\mathcal{D}_{1,2,3} \stackrel{\S}{\approx} \mathcal{D}_{1,2,4}$  by noise flooding, due to  $\tilde{\mathbf{e}}_{\text{cid}, i, P}^T \mathbf{k}_{\text{cid}} + e_{\text{cid}, i, P} \stackrel{\S}{\approx} +e_{\text{cid}, i, P}$  since  $\chi(1) \geq \lambda^{\omega(1)} \lambda^2 \chi(0) \chi(0) \geq \lambda^{\omega(1)} \|\tilde{\mathbf{e}}_{\text{cid}, i, P}^T \mathbf{k}_{\text{cid}}\|$ .

- $\mathcal{D}_{1,2,5}$ : For each  $i \in [3, k]$  and all  $\text{cid} \in \mathcal{C}$ , we swap

$$(\mathbf{s}_i^T \mathbf{P} + \tilde{\mathbf{e}}_{\text{cid}, i, P}^T) \mathbf{k}_{\text{cid}} + e_{\text{cid}, i, P} \quad \text{to} \quad \mathbf{b}_{\text{cid}, i, P}^T \mathbf{k}_{\text{cid}} + e_{\text{cid}, i, P}$$

where  $\mathbf{b}_{\text{cid}, i, P}^T$  is uniformly random, and we also swap

$$\mathbf{s}_i^T \overline{\mathbf{C}}_i + \mathbf{e}_i^T \quad \text{and} \quad \mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i, Q}^T$$

to uniformly random.

We have  $\mathcal{D}_{1,2,4} \stackrel{\S}{\approx} \mathcal{D}_{1,2,5}$  by the  $\text{LWE}_{n, 2m(m+2), q, \chi(0)}$  assumption.

- $\mathcal{D}_{1,2,6}$ : For all  $\text{cid} \in \mathcal{C}$ , all  $i \in [3, k]$ , we swap

$$\mathbf{b}_{\text{cid}, i, P}^T \mathbf{k}_{\text{cid}} + e_{\text{cid}, i, P}$$

to uniformly random.

We have  $\mathcal{D}_{1,2,5} \stackrel{\S}{\approx} \mathcal{D}_{1,2,6}$  by the (low-norm)  $\text{LWE}_{m, \text{poly}(n), q, \chi(1), \chi(0)}$  assumption.

- $\mathcal{D}_{1,2,7}$ : For all  $\text{cid} \in \mathcal{C}$  and the  $f^*$  picked in  $\mathcal{D}_{1,2,1}$ , we swap the terms

$$\begin{aligned} & \mathbf{s}^\top(\hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid},i,B}^\top \quad \forall i \in [2, k], \quad \mathbf{s}^\top(\hat{\mathbf{B}}_{\text{cid}^*,1} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid}^*,\text{cid},1,B}^\top, \\ & \mathbf{s}^\top(\mathbf{A} \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_{\text{cid},A}^\top, \quad \mathbf{s}^\top(\mathbf{G}\mathbf{r}_{f^*} \otimes \mathbf{k}_{\text{cid}}) + e_{f^*,\text{cid}} \end{aligned}$$

to uniformly random.

Note that  $\mathbf{G}\mathbf{r}_{f^*} \bmod q$  is statistically close to uniformly random. Then, we have  $\mathcal{D}_{1,2,6} \stackrel{\epsilon}{\approx} \mathcal{D}_{1,2,7}$  by the  $\text{TensorLWE}_{n,(k+2)m+1,q,\chi(0),\chi(0),\ell,\mathcal{Q}}$  where the set  $\mathcal{Q}$  contains all queries  $\mathbf{x}_{\text{cid},i}$  from the adversary.

Observe that  $\mathcal{D}_{1,2,7} \stackrel{h}{\approx} \mathcal{D}_{2,2}^{(h)}$  as in Eq. (8), and the proof is completed.  $\square$

## B.2 Continued proof of Theorem 6 (corruption)

**Theorem 6.** *For parameters as in Table 5,  $\Pi_{\text{MC}}$  is IND-CPA-secure without missing ciphertexts (Definition 7) assuming*

$$\begin{aligned} & \text{LWE}_{n,2m(m+2),q,\chi(0)}, & & \text{LWE}_{m,\text{poly}(n),q,\chi(1),\chi(0)}, \\ & \text{TensorLWE}_{n,(k+2)m+1,q,\chi(0),\chi(0),\ell,\mathcal{Q}}, & & \text{EvasiveLWE}_{\text{param}_0} \quad \text{and} \quad \text{EvasiveLWE}_{\text{param}_1} \end{aligned}$$

in the (non-programmable) random oracle model.

*Proof.* (Continued.) Below write  $\mathcal{J} = \mathcal{J}_{\text{corr}} \subset [2, k]$  for the set of corrupt encryptors. In this continued proof we focus on that Case (2)  $b_{\text{corrupt\_security}} = 1$  happens. That is, there exists an honest encryptor  $i \in [2, k] \setminus \mathcal{J}$  such that a ciphertext  $\text{ctx}_{\text{cid},i^*,\mathbf{x}}$  from  $i$  has not been queried.

Fix arbitrary honest encryptor  $i^* \in [k] \setminus \mathcal{J}$ , which exists since  $[k] \neq \mathcal{J}$ . For each  $\text{cid} \in \mathcal{C}$ , denote by  $\hat{i}_{\text{cid}}$  an arbitrarily fixed honest encryptor from whom a ciphertext on  $\text{cid}$  has not been queried by the adversary, which exists by design of the security experiment.

We define the following sequence of hybrids:

- $\text{Hyb}_{b,0}^{(c)}$ : This is the real security experiment for the scheme in Fig. 10, encrypting  $\mu_b$ , and conditioned on that  $b_{\text{corrupt\_security}} = 1$ .

Recall that in this hybrid the adversary is given the following:

$$\begin{aligned} & \mathbf{A}, (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k]}, (\text{td}_{\mathbf{C}_i})_{i \in \mathcal{J}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \mathbf{v} \\ & \mathbf{r}_f = (\mathbf{A} \mid \mathbf{B}_f)^{-1}(\mathbf{v}) \quad \forall f \in \mathcal{F} \\ & \mathbf{U}_{\text{cid},i} = \mathbf{C}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix} \quad \forall \text{cid} \in \mathcal{C}, i \in \mathcal{J}_{\text{cid}} \cap [2, k] \\ & \hat{\mathbf{c}}^\top = \mathbf{s}^\top(\mathbf{A} \otimes \mathbf{k}_{\text{cid}}) + \hat{\mathbf{e}}^\top \\ & \mathbf{c}_1^\top = \mathbf{s}^\top((\mathbf{B} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{k}_{\text{cid}}) + \mathbf{e}_1^\top \\ & \mathbf{c}_i^\top = (\mathbf{s}_i^\top \mid \mathbf{s}^\top)\mathbf{C}_i + \mathbf{e}_i^\top \quad \forall i \in [2, k] \\ & \mathbf{c}_0^\top := (\mathbf{s}_2^\top \mid \dots \mid \mathbf{s}_k^\top)(\mathbf{I}_{k-1} \otimes \mathbf{Q}) + \mathbf{e}_0^\top \\ & \mathbf{c}^\top = \sum_{i \in [2,k]} \mathbf{s}^\top \mathbf{P} + \mathbf{s}^\top(\mathbf{v} \otimes \mathbf{I}_n) + \mathbf{e}^\top + \mu_b \cdot \mathbf{g}^\top \end{aligned}$$

where all terms are sampled according to the distribution as in the scheme. We recall each  $\mathbf{r}_f$  is sampled with  $\text{td}_{\mathbf{A}}$ . Relative to the case in the honest model, here the adversary is additionally given  $\text{ask}_i = \text{td}_{\mathbf{C}_i}$  for the corrupted authorities  $i \in \mathcal{J}$ . Write  $\mathbf{c}_0^\top = (\mathbf{c}_{2,Q}^\top \mid \dots \mid \mathbf{c}_{k,Q}^\top)$  where  $\mathbf{c}_{i,Q}^\top = \mathbf{s}_i^\top \mathbf{Q} + \mathbf{e}_{i,Q}^\top$ .

- $\text{Hyb}_{b,1}^{(c)}$ : Same as  $\text{Hyb}_{b,0}^{(c)}$ , except that for all  $i \in [2, k] \setminus \mathcal{J}$ ,  $\mathbf{C}_i$  is sampled uniformly randomly and all (entries of the) corresponding preimages  $\mathbf{U}_{\text{cid},i}$  are sampled (inefficiently) from the Gaussian distribution with parameter  $\tau$ , subject to

$$\mathbf{C}_i \mathbf{U}_{\text{cid},i} = \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix}.$$

We have  $\text{Hyb}_{b,0}^{(c)} \stackrel{s}{\approx} \text{Hyb}_{b,1}^{(c)}$  by the properties of TrapGen from Section 3.3.

- $\text{Hyb}_{b,2}^{(c)}$ : Same as  $\text{Hyb}_{b,1}^{(c)}$ , except:
  - we sample uniformly random  $\mathbf{c} \leftarrow \mathbb{Z}_q^m$ ,
  - for each  $i \in [2, k] \setminus \mathcal{J}$ , we sample uniformly random  $\mathbf{c}_i$ , and
  - for each  $i \in [2, k] \setminus \mathcal{J}$ , we sample the  $i$ -th chunk  $\mathbf{c}_{i,Q}$  in  $\mathbf{c}_0$  uniformly randomly.

We show in the following that  $\text{Hyb}_{b,1}^{(c)} \stackrel{s}{\approx} \text{Hyb}_{b,2}^{(c)}$ . Then, the theorem follows from noting that  $\text{Hyb}_{0,2}^{(c)} \stackrel{p}{=} \text{Hyb}_{1,2}^{(c)}$ , since in both hybrids the component  $\mathbf{c}$  in the challenge ciphertext is chosen uniformly randomly.

Define the distribution

$$\mathcal{D}_{1,1}^{(c)} := \left( \begin{array}{l} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k] \setminus \mathcal{J}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \\ \left( \mathbf{C}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix} \right)_{\text{cid} \in \mathcal{C}, i \in [2,k] \setminus (\mathcal{J} \cup \{\tilde{i}_{\text{cid}}\})} \\ (\mathbf{s}_i^T \bar{\mathbf{C}}_i + \mathbf{e}_i^T)_{i \in [2,k] \setminus \mathcal{J}} \\ (\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T)_{i \in [2,k] \setminus \mathcal{J}} \\ \mathbf{c}^T = \sum_{i \in [2,k] \setminus \mathcal{J}} \mathbf{s}_i^T \mathbf{P} + \mathbf{e}^T \end{array} \right) \quad (21)$$

where all terms are distributed as in  $\text{Hyb}_{b,1}^{(c)}$ . We note that in the above distribution, the LWE samples  $\mathbf{c}_i$  are w.r.t.  $\bar{\mathbf{C}}_i$ , whereas the preimages are w.r.t. (the full)  $\mathbf{C}_i$ . Define also the distribution

$$\mathcal{D}_{2,1}^{(c)} := \left( \begin{array}{l} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k] \setminus \mathcal{J}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \\ \left( \mathbf{C}_i^{-1} \begin{pmatrix} \mathbf{P}\mathbf{k}_{\text{cid}} & \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{pmatrix} \right)_{\text{cid} \in \mathcal{C}, i \in [2,k] \setminus (\mathcal{J} \cup \{\tilde{i}_{\text{cid}}\})} \\ (\bar{\mathbf{c}}_i^T)_{i \in [2,k] \setminus \mathcal{J}} \\ (\mathbf{c}_{i,Q}^T)_{i \in [2,k] \setminus \mathcal{J}} \\ \mathbf{c}^T \end{array} \right) \quad (22)$$

where all elements are distributed same as in  $\mathcal{D}_{1,1}^{(c)}$ , except that  $(\bar{\mathbf{c}}_i^T)_{i \in [2,k] \setminus \mathcal{J}}$ ,  $(\bar{\mathbf{c}}_{i,Q}^T)_{i \in [2,k] \setminus \mathcal{J}}$  and  $\tilde{\mathbf{c}}$  are uniformly random.<sup>21</sup>

Suppose there exists a PPT  $\mathcal{A}$  that distinguishes  $\text{Hyb}_{b,1}^{(c)}$  and  $\text{Hyb}_{b,2}^{(c)}$  with non-negligible probability, then it is easy to see that<sup>22</sup> there exists a PPT  $\mathcal{B}$  that distinguishes  $\mathcal{D}_{1,1}^{(c)}$  and  $\mathcal{D}_{2,1}^{(c)}$  defined above with non-negligible probability.

<sup>21</sup>The distributions in Eq. (21) and Eq. (22) are respectively the same as those in Eq. (9) and Eq. (10) from the proof of our MA-ABE scheme up to renaming: here having  $\mathbf{C}_i$  in place of  $\mathbf{A}_i$  and running variables  $i \in [2, k] \setminus \mathcal{J}$  in place of  $[k] \setminus \mathcal{J}$ . The rest of the proof, which boils down to showing that the two distributions are computationally close, thus follows analogously. For completeness we nevertheless include the full proof.

<sup>22</sup>The simulation is analogous to Proposition 1 for the proof of our MA-ABE scheme. In addition, the reduction samples  $\mathbf{v}$  and  $(\mathbf{A}, \text{td}_{\mathbf{A}})$  itself, using which it can generate both the authority query answers  $\mathbf{r}_f = (\mathbf{A} \mid \mathbf{B}_f)^{-1}(\mathbf{v})$  and the ciphertext component  $\hat{\mathbf{c}}$ .

Now consider a PPT Samp which on input  $\lambda$  outputs the following:

$$\begin{aligned}\tilde{\mathbf{A}} &:= (\mathbf{1}_{[2,k]\setminus\mathcal{J}} \otimes \mathbf{P} \mid \mathbf{I}_{k-|\mathcal{J}} \otimes \mathbf{Q}), \\ \tilde{\mathbf{P}}_i &:= \left( \begin{array}{c} \mathbf{P}\mathbf{k}_{\text{cid}} \quad \mathbf{Q}\mathbf{K}_{\text{cid}} \\ \hat{\mathbf{B}}_{\text{cid},i} \otimes \mathbf{k}_{\text{cid}} \end{array} \right)_{\text{cid} \in \mathcal{U}} \quad \forall \text{cid} \in \mathcal{U}, i \in [k] \setminus (\mathcal{J} \cup \{\tilde{i}_{\text{cid}}\}),\end{aligned}$$

where  $\mathbf{1}_{[2,k]\setminus\mathcal{J}} \in \{0,1\}^{k-1-|\mathcal{J}|}$  is the all-one vector, and aux containing  $(\mathbf{B}_i)_{i \in [k]}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{U}}$  together with all random coins used.

Then, by the  $\text{EvasiveLWE}_{\text{param}_1}$  assumption (c.f. Table 5), there exists a PPT  $\mathcal{E}$  that distinguishes the distributions  $\mathcal{D}_{1,2}^{(c)}$  and  $\mathcal{D}_{2,2}^{(c)}$  with non-negligible probability, where  $\mathcal{D}_{1,2}^{(c)}$  and  $\mathcal{D}_{2,2}^{(c)}$  are defined as follows:

$$\mathcal{D}_{1,2}^{(c)} := \left( \begin{array}{c} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k]\setminus\mathcal{J}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \\ \left( \mathbf{s}_i^{\text{T}} \mathbf{P} \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P}, \mathbf{s}_i^{\text{T}} \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{e}_{\text{cid},i,Q}^{\text{T}} \right)_{\text{cid} \in \mathcal{C}, i \in [2,k] \setminus (\mathcal{J} \cup \{\tilde{i}_{\text{cid}}\})} \\ \left( \mathbf{s}_i^{\text{T}} \bar{\mathbf{C}}_i + \mathbf{e}_i^{\text{T}} \right)_{i \in [2,k]\setminus\mathcal{J}}, \\ \left( \mathbf{s}_i^{\text{T}} \mathbf{Q} + \mathbf{e}_{i,Q}^{\text{T}} \right)_{i \in [2,k]\setminus\mathcal{J}} \\ \mathbf{c}^{\text{T}} = \sum_{i \in [2,k]\setminus\mathcal{J}} \mathbf{s}_i^{\text{T}} \mathbf{P} + \mathbf{e}^{\text{T}} \end{array} \right) \quad (23)$$

where all terms are distributed as in  $\mathcal{D}_{1,1}$ , additionally  $e_{i^*,\text{cid},P} \leftarrow \chi_{(2)}$  where  $i^*$  is arbitrary in  $[2,k] \setminus \mathcal{J}$  (which exists since  $\mathcal{J} \neq [2,k]$ ), and  $e_{\text{cid},i,P} \leftarrow \chi_{(1)}$ ,  $\mathbf{e}_{\text{cid},i,Q} \leftarrow \chi_{(2)}^n$  for all  $i \in [2,k], i \neq i^*$ .

$$\mathcal{D}_{2,2}^{(c)} := \left( \begin{array}{c} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k]\setminus\mathcal{J}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \\ \left( c_{\text{cid},i,P}, \mathbf{c}_{\text{cid},i,Q}^{\text{T}} \right)_{\text{cid} \in \mathcal{C}, i \in [2,k] \setminus (\mathcal{J} \cup \{\tilde{i}_{\text{cid}}\})} \\ \left( \bar{\mathbf{c}}_i^{\text{T}} \right)_{i \in [2,k]\setminus\mathcal{J}}, \\ \left( \mathbf{c}_{i,Q}^{\text{T}} \right)_{i \in [2,k]\setminus\mathcal{J}} \\ \mathbf{c}^{\text{T}} \end{array} \right) \quad (24)$$

where all  $(c_{\text{cid},i,P}, \mathbf{c}_{\text{cid},i,Q}^{\text{T}})_{\text{cid} \in \mathcal{C}, i \in [2,k] \setminus (\mathcal{J} \cup \{\tilde{i}_{\text{cid}}\})}$ ,  $(\bar{\mathbf{c}}_i^{\text{T}})_{i \in [2,k]\setminus\mathcal{J}}$ ,  $(\mathbf{c}_{i,Q}^{\text{T}})_{i \in [2,k]\setminus\mathcal{J}}$  and  $\mathbf{c}$  are all uniformly random.

We observe that the above implies a PPT distinguisher  $\mathcal{G}$  for the following distributions  $\mathcal{D}_{1,3}^{(c)}, \mathcal{D}_{2,3}^{(c)}$ , given which  $\mathcal{D}_{1,2}^{(c)}$  and  $\mathcal{D}_{2,2}^{(c)}$  can be efficiently simulated respectively:

$$\mathcal{D}_{1,3}^{(c)} := \left( \begin{array}{c} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k]\setminus\mathcal{J}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \\ \left( \mathbf{s}_i^{\text{T}} \mathbf{P} \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P} \right)_{\text{cid} \in \mathcal{C}, i \in [2,k] \setminus (\mathcal{J} \cup \{\tilde{i}_{\text{cid}}\})} \\ \left( \mathbf{s}_i^{\text{T}} \bar{\mathbf{C}}_i + \mathbf{e}_i^{\text{T}} \right)_{i \in [2,k]\setminus\mathcal{J}}, \\ \left( \mathbf{s}_i^{\text{T}} \mathbf{Q} + \mathbf{e}_{i,Q}^{\text{T}} \right)_{i \in [2,k]\setminus\mathcal{J}} \\ \mathbf{c}^{\text{T}} = \sum_{i \in [2,k]\setminus\mathcal{J}} \mathbf{s}_i^{\text{T}} \mathbf{P} + \mathbf{e}^{\text{T}} \end{array} \right) \quad (25)$$

$$\mathcal{D}_{2,3}^{(c)} := \left( \begin{array}{c} (\mathbf{B}_i)_{i \in [k]}, (\mathbf{C}_i)_{i \in [2,k]\setminus\mathcal{J}}, \mathbf{P}, \mathbf{Q}, (\mathbf{k}_{\text{cid}}, \mathbf{K}_{\text{cid}})_{\text{cid} \in \mathcal{C}}, \\ \left( c_{\text{cid},i,P} \right)_{\text{cid} \in \mathcal{C}, i \in [2,k] \setminus (\mathcal{J} \cup \{\tilde{i}_{\text{cid}}\})} \\ \left( \bar{\mathbf{c}}_i^{\text{T}} \right)_{i \in [2,k]\setminus\mathcal{J}}, \\ \left( \mathbf{c}_{i,Q}^{\text{T}} \right)_{i \in [2,k]\setminus\mathcal{J}} \\ \mathbf{c}^{\text{T}} \end{array} \right) \quad (26)$$

which are almost identical to  $\mathcal{D}_{1,2}^{(c)}$  and  $\mathcal{D}_{2,2}^{(c)}$  respectively, except that  $\mathbf{s}_i^{\text{T}} \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{e}_{\text{cid},i,Q}^{\text{T}}$  respectively  $\mathbf{c}_{\text{cid},i,Q}^{\text{T}}$  are omitted. To simulate  $\mathcal{D}_{1,2}^{(c)}$  from  $\mathcal{D}_{1,3}^{(c)}$ , one computes

$$(\mathbf{s}_i^{\text{T}} \mathbf{Q} + \mathbf{e}_{i,Q}^{\text{T}}) \mathbf{K}_{\text{cid}} + \mathbf{e}_{\text{cid},i,Q}^{\text{T}} = \mathbf{s}_i^{\text{T}} \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{e}_{i,Q}^{\text{T}} \mathbf{K}_{\text{cid}} + \mathbf{e}_{\text{cid},i,Q}^{\text{T}} \stackrel{\approx}{\approx} \mathbf{s}_i^{\text{T}} \mathbf{Q} \mathbf{K}_{\text{cid}} + \mathbf{e}_{\text{cid},i,Q}^{\text{T}} \pmod{q}$$



where the last  $\stackrel{\S}{\approx}$  follows from noise flooding, since

$$\chi_{(2)} \geq \lambda^{\omega(1)} \cdot \lambda \cdot \chi_{(0)} \cdot \chi_{(0)} \cdot n \geq \lambda^{\omega(1)} \cdot \|\mathbf{e}_{i^*,Q}^T \cdot \mathbf{K}_{\text{cid}}\|.$$

When  $\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T$  is replaced by uniformly random  $\mathbf{c}_{\text{cid},i,Q}^T$ , then the simulation becomes also uniformly random.

But by Lemma 10 the existence of  $\mathcal{G}$  is not possible under the  $\text{LWE}_{n,2m(m+2),q,\chi_{(0)}}$  and  $\text{LWE}_{m,\text{poly}(n),q,\chi_{(1)},\chi_{(0)}}$  assumptions, thus we have a contradiction. The theorem follows.  $\square$

**Lemma 10.** *For the distributions  $\mathcal{D}_{1,3}^{(c)}$  and  $\mathcal{D}_{2,3}^{(c)}$  defined in Eq. (25) and Eq. (26), we have  $\mathcal{D}_{1,3}^{(c)} \stackrel{\S}{\approx} \mathcal{D}_{2,3}^{(c)}$  assuming*

$$\text{LWE}_{n,2m(m+2),q,\chi_{(0)}} \quad \text{and} \quad \text{LWE}_{m,\text{poly}(n),q,\chi_{(1)},\chi_{(0)}}.$$

*Proof.* Continue with the notation in the proof of Theorem 6, where we have let  $i^* \in [k] \setminus \mathcal{J}$  be an arbitrarily fixed honest encryptor (which exists because  $[k] \neq \mathcal{J}$ ), and for each  $\text{cid} \in \mathcal{C}$ , we have let  $\tilde{i}_{\text{cid}} \in [k] \setminus \mathcal{J}$  be an honest encryptor where  $\text{cid}$  is not queried by the adversary (which exists by design of security experiment).

We define the following sequence of hybrid distributions:

- $\mathcal{D}_{1,3}^{(c)}$  as in Eq. (23).
- $\mathcal{D}_{1,3,1}$ : For each  $\text{cid} \in \mathcal{C}$ , if  $i^* \neq \tilde{i}_{\text{cid}}$ , then do the following:

We swap  $\mathbf{s}_{i^*}^T \mathbf{P} \mathbf{k}_{\text{cid}} + e_{i^*,\text{cid},P}$  to

$$\left( \sum_{i \in [2,k] \setminus \mathcal{J}} \mathbf{s}_i^T \mathbf{P} + \mathbf{e}^T \right) \mathbf{k}_{\text{cid}} - \left( \sum_{i \in [2,k] \setminus \mathcal{J}: i \neq i^*} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P} \right) + e_{i^*,\text{cid},P}.$$

We have  $\mathcal{D}_{1,3}^{(c)} \stackrel{\S}{\approx} \mathcal{D}_{1,3,1}$  by noise flooding, which is due to the equality

$$\mathbf{s}_{i^*}^T \mathbf{P} \mathbf{k}_{\text{cid}} = \left( \sum_{i \in [2,k] \setminus \mathcal{J}} \mathbf{s}_i^T \mathbf{P} \right) \mathbf{k}_{\text{cid}} - \sum_{i \in [2,k] \setminus \mathcal{J}: i \neq i^*} \mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}}.$$

and that

$$e_{i^*,\text{cid},P} \stackrel{\S}{\approx} \mathbf{e}^T \mathbf{k}_{\text{cid}} - \sum_{i \in [2,k] \setminus \mathcal{J}: i \neq i^*} e_{\text{cid},i,P} + e_{i^*,\text{cid},P},$$

since

$$\chi_{(2)} \geq \lambda^{\omega(1)} (\lambda^2 m \chi_{(0)}^2 + k \lambda \chi_{(1)}) \geq \lambda^{\omega(1)} \cdot \left\| \mathbf{e}^T \mathbf{k}_{\text{cid}} - \sum_{i \in [2,k] \setminus \mathcal{J}: i \neq i^*} e_{\text{cid},i,P} \right\|$$

Otherwise, if  $i^* = \tilde{i}_{\text{cid}}$ , then do nothing. The effect of this swap is that, for all  $\text{cid} \in \mathcal{C}$ , the term  $\mathbf{s}_{i^*}^T \mathbf{P} \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P}$  no longer exists in  $\mathcal{D}_{1,3,1}$  (and is instead simulated by the other terms, where the expression includes LWE samples with secret  $\mathbf{s}_{\tilde{i}_{\text{cid}}}$ ).

As a result, the only remaining terms in  $\mathcal{D}_{1,3,1}$  involving  $\mathbf{s}_{i^*}$  are  $\mathbf{s}_{i^*}^T \overline{\mathbf{C}}_{i^*} + \mathbf{e}_{i^*}^T$ ,  $\mathbf{s}_{i^*}^T \mathbf{P} + \mathbf{e}^T$ , and  $\mathbf{s}_{i^*}^T \mathbf{Q} + \mathbf{e}_{i^*,Q}^T$ .

- $\mathcal{D}_{1,3,2}$ : We swap

$$\mathbf{s}_{i^*}^T \overline{\mathbf{C}}_{i^*} + \mathbf{e}_{i^*}^T, \quad \mathbf{s}_{i^*}^T \mathbf{P} + \mathbf{e}_{i^*,P}^T \quad \text{and} \quad \mathbf{s}_{i^*}^T \mathbf{Q} + \mathbf{e}_{i^*,Q}^T$$

to uniformly random.

We have  $\mathcal{D}_{1,3,1} \stackrel{\S}{\approx} \mathcal{D}_{1,3,2}$  by the  $\text{LWE}_{n,2m(m+2),q,\chi_{(0)}}$  assumption. Notice that as a result  $\mathbf{c}$  is also uniformly random.

- $\mathcal{D}_{1,3,3}$ : For all  $\text{cid} \in \mathcal{C}$ , all  $i \in [2, k] \setminus (\mathcal{J} \cup \{i^*\})$ , we swap

$$\mathbf{s}_i^T \mathbf{P} \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P} \quad \text{to} \quad (\mathbf{s}_i^T \mathbf{P} + \tilde{\mathbf{e}}_{\text{cid},i,P}^T) \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P}.$$

where  $\tilde{\mathbf{e}}_{\text{cid},i,P} \leftarrow_{\$} \chi_{(0)}^m$ .

We have  $\mathcal{D}_{1,3,2} \stackrel{\$}{\approx} \mathcal{D}_{1,3,3}$  by noise flooding, since  $\tilde{\mathbf{e}}_{\text{cid},i,P}^T \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P} \stackrel{\$}{\approx} e_{\text{cid},i,P}$ , because  $\chi_{(1)} \geq \lambda^{\omega(1)} \lambda^2 \chi_{(0)} \chi_{(0)} \geq \lambda^{\omega(1)} \|\tilde{\mathbf{e}}_{\text{cid},i,P}^T \mathbf{k}_{\text{cid}}\|$ .

- $\mathcal{D}_{1,3,4}$ : For all  $\text{cid} \in \mathcal{C}$ , all  $i \in [2, k] \setminus (\mathcal{J} \cup \{i^*\})$ , we swap

$$(\mathbf{s}_i^T \mathbf{P} + \tilde{\mathbf{e}}_{\text{cid},i,P}^T) \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P} \quad \text{to} \quad \mathbf{b}_{\text{cid},i,P}^T \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P}$$

where  $\mathbf{b}_{\text{cid},i,P}^T$  is uniformly random, and we also swap

$$\mathbf{s}_i^T \mathbf{Q} + \mathbf{e}_{i,Q}^T \quad \text{and} \quad \mathbf{s}_i^T \overline{\mathbf{C}}_i + \mathbf{e}_i^T$$

to uniformly random.

We have  $\mathcal{D}_{1,3,3} \stackrel{\$}{\approx} \mathcal{D}_{1,3,4}$  by the  $\text{LWE}_{n,2m(m+2),q,\chi_{(0)}}$  assumption.

- $\mathcal{D}_{1,3,5}$ : For all  $\text{cid} \in \mathcal{C}$ , all  $i \in [k] \setminus (\mathcal{J} \cup \{i^*\})$ , we swap

$$\mathbf{b}_{\text{cid},i,P}^T \mathbf{k}_{\text{cid}} + e_{\text{cid},i,P}$$

to uniformly random.

We have  $\mathcal{D}_{1,3,4} \stackrel{\$}{\approx} \mathcal{D}_{1,3,5}$  by the (low-norm)  $\text{LWE}_{m,\text{poly}(n),q,\chi_{(1)},\chi_{(0)}}$  assumption.

Observe that  $\mathcal{D}_{1,3,5} \stackrel{\$}{\approx} \mathcal{D}_{2,3}^{(c)}$  as in Eq. (26), the proof is completed.  $\square$

## C On Stronger Security with Corruption

We discuss why it is difficult to achieve stronger security in presence of corrupt authorities. Consider an adversary who requests a ciphertext for some function  $f$  which is independent of the  $i^*$ -th input. The adversary corrupts authority  $i^*$ , and requests a secret key  $\text{sk}_{\text{uid},i,\mathbf{x}_i}$  for each  $i \neq i^*$  such that  $f(\mathbf{x}_1, \dots, \mathbf{x}_k) = 1$  for any possible  $\mathbf{x}_{i^*}$ . An ideal MA-ABE scheme would have security against the above attack.

Security for the above scenario, however, is difficult to achieve at least with a construction template based on LWE and homomorphic computation techniques. Consider some ciphertext with LWE samples of the form  $\widetilde{\mathbf{s}}^T \mathbf{B}$  where  $\mathbf{B}$  is reserved for policy checking via homomorphic computations. Now since multiple authorities are contributing to such computation, the secret  $\mathbf{s}$  is “shared” across the authorities, and as such information about  $\mathbf{s}$  can be leaked to an adversary via any corrupt authority. The alternative of letting the secret individual to each authority  $i$  sacrifices correctness, since with components of the form  $\widetilde{\mathbf{s}}_i^T \mathbf{B}$ , computing on both  $\mathbf{s}_i$  and  $\mathbf{B}$  results in cross-terms across authorities which cannot be cancelled out (due to non-interactiveness of authorities). On the other hand, any other components independent of policy evaluation is not governed by the condition  $f(\mathbf{x}_1, \dots, \mathbf{x}_k) = 1$ .

For our construction, the strong security mentioned in the beginning cannot be achieved for the same reason. In particular, we observe the following. First, the adversary can learn the LWE secrets  $\mathbf{s}_{i^*}$  and  $\mathbf{s}$  in the challenge ciphertext using the trapdoor of  $\mathbf{A}_{i^*}$ , and compute the masking terms  $\mathbf{s}_{i^*}^T \mathbf{P} \mathbf{k}_{\text{uid}}$  and  $\mathbf{s}^T (\mathbf{B}_f \mathbf{u} \otimes \mathbf{k}_{\text{uid}})$ . Second, the adversary can combine  $\widetilde{\mathbf{s}}_i^T \mathbf{A}_i$  in the challenge ciphertext with the top part of a secret key  $\text{sk}_{\text{uid},i,\mathbf{x}_i}$ , i.e.

$\overline{\mathbf{A}}_i^{-1}(\mathbf{Pk}_{\text{uid}} \mid \mathbf{QK}_{\text{uid}})$ , for any  $\mathbf{x}_i$  to obtain the masking terms  $\underline{\mathbf{s}}_i^T \mathbf{Pk}_{\text{uid}}$  for each  $i \neq i^*$ . Using the above, the adversary can recover  $\underline{\mu} \mathbf{g}^T \mathbf{k}_{\text{uid}}$ , which is short if  $\mu = 0$ .

Due to the above, we settle for the slightly weaker security notion in face of corruption, where we require that for each uid there exists an honest authority from which the adversary has not queried a key for uid. We remark that for any non-monotone function  $f$  which, the attribute  $\mathbf{x}_{i^*}$  of any authority  $i^*$  has influence on the final output of  $f$  regardless of attributes from other authorities  $i \neq i^*$ , security in our weaker model implies the stronger one mentioned above. This is the case for a variety of typical non-monotone functions, such as the parity function, “A and B and not C”, or more generally most low-degree polynomials.

## D Witness Encryption from MI-ABE

**Witness Encryption.** Recall that a witness encryption scheme (WE) for a relation  $R$  consists of an encryption algorithm  $\text{Enc}$  which takes as input a statement  $\psi$  and a message  $m$  and produces a ciphertext  $c$ . Correctness requires that  $\text{Dec}(w, c) = m$  if  $w$  is a witness for  $\psi$  being in the NP language  $\mathcal{L}_R$  induced by  $R$ , i.e.  $R(\psi, w) = 1$ . In turn, security requires that when  $\psi \notin \mathcal{L}_R$ , then  $\text{Enc}(\psi, m)$  and  $\text{Enc}(\psi, 0^{|m|})$  are indistinguishable.

**MI-ABE  $\Rightarrow$  WE.** Brakerski et al. [BJK<sup>+</sup>18] show that MI-ABE implies WE via the following simple construction: Let  $R$  be an NP-relation and assume for simplicity that statement size equals witness size. Given a statement  $\psi$ , the encryptor does the following:

- Spawn an authority and generate a secret key  $\text{sk}_f$  for the function

$$f(X_2, \dots, X_{|\psi|+1}) := 1 \oplus R(\psi, X_2 \mid \dots \mid X_{|\psi|+1}).$$

- Run  $\text{Enc}_1$  (associated to an arbitrary attribute  $x_1$ ) to generate a ciphertext  $\text{ctxt}_1$  encrypting the message  $m$ .
- For  $i \in [2, |\psi| + 1]$ , run  $\text{Enc}_i$  twice to generate  $\text{ctxt}_{i,0}$  and  $\text{ctxt}_{i,1}$  associate to the attributes  $x_i = 0$  and  $x_i = 1$  respectively.
- Output  $(\text{sk}_f, \text{ctxt}_1, (\text{ctxt}_{i,b})_{i \in [2, |\psi|+1], b \in \{0,1\}})$  as a ciphertext.

MI-ABE correctness indeed allows to decrypt when knowing a witness  $w$  using

$$(\text{ctxt}_{i,w_i})_{i \in [k] \times \{0,1\}},$$

since  $f(w_1, \dots, w_k) = 1 \oplus R(\psi, w_1 \mid \dots \mid w_k) = 0$ . In turn, when there is no witness such that  $R(\psi, w) = 1$ , the MI-ABE security requires that ciphertext  $c$  is indistinguishable from an encryption of  $0^{|m|}$ , thus implying both security and correctness of witness encryption.

Given that witness encryption is a very strong cryptographic primitive, the above implication indicates that MI-ABE schemes are very challenging to construct, let alone to prove secure.

**Ciphertext Identity.** Our proof of the AYY MI-ABE scheme [AYY22] in the CID model (cf. Section 5) circumvents the above difficulty by introducing a *ciphertext identifier*. Namely, encryptors give away ciphertexts  $\text{ctxt}_{\text{cid}, i, \mathbf{x}_i}$  for a specific ciphertext identifier cid, and for each cid, an encryptor only gives away a key for a *single* attribute. In this way, the WE construction by Brakerski et al. [BJK<sup>+</sup>18] can no longer be implemented, while the core MI-ABE functionality is retained.