

On Enabling Attribute-Based Encryption to Be Traceable against Traitors

Zhen Liu¹ and Duncan S. Wong²

¹ Shanghai Jiao Tong University, China.

liuzhen@sjtu.edu.cn

² CryptoBLK.

duncanwong@cryptoblk.io

Abstract. Attribute-Based Encryption (ABE) is a versatile one-to-many encryption primitive which enables fine-grained access control over encrypted data. Due to its promising applications in practice, ABE has been attracting much attention in the community and schemes with better security, access policy expressivity, and efficiency have been continuously emerging. On the other hand, due to the nature of ABE, namely, different users may share some common decryption privileges and a malicious user may leak some common decryption privileges for financial gain or other incentives, being able to identify such malicious users (i.e. traitor tracing) is crucial towards the practicality of an ABE system. For some existing ABE schemes with appealing properties (e.g. full security, large universe), the corresponding traceable counterparts have been proposed. However, these works are proceeded case by case, and there are still many appealing ABE schemes not having the traceable counterparts. Furthermore, when any new ABE scheme emerges and we want to apply it in practice, it will take significant workload to investigate and propose its traceable counterpart.

In this paper, we propose a framework to transform existing and (possibly) future ABE schemes to their traceable counterparts in a generic manner. In particular, by specifying some requirements on the structure of the ABE constructions, we propose an ABE template, and show that any ABE scheme satisfying this template can be transformed to a fully collusion-resistant blackbox traceable ABE scheme in a generic manner, at the cost of sublinear overhead, while keeping the appealing properties, such as fine-grained access control on encrypted data, highly expressive access policy, short ciphertext, and so on. We prove the security in the framework all in the standard model, and we present a couple of existing ABE schemes with appealing properties as examples that do satisfy our ABE template.

Keywords: Attribute-Based Encryption, Traitor Tracing, Framework

1 Introduction

Attribute-Based Encryption (ABE), introduced by Sahai and Waters [29], is a versatile one-to-many encryption primitive which enables fine-grained access control over encrypted data. Due to its promising applications in practice, ABE has been attracting much attention in the community and undergoing a significant development. Among the recently proposed ABE schemes [29,13,5,10,12,30,18,27,14,3,19,31,15,28,16,1], progress has been made on the schemes' security, access policy expressivity, and efficiency. For example, Lewko et al. [18] proposed the first *fully secure* ABE schemes, Lewko and Waters [19] proposed a new proof technique for achieving full security for ABE, Attrapadung et al. [3] proposed the first expressive Key-Policy ABE (KP-ABE) with *constant-size ciphertexts*, Rouselakis and Waters [28] proposed the first *large universe* ABE³ schemes which impose no limitations on the attribute sets or the access policies, Waters [31] proposed the first ABE scheme supporting *regular languages* to be the access policy while the previous works support at most boolean formulas, and Attrapadung [1] proposed a series of fully secure ABE schemes which support regular languages, constant size ciphertexts, or large universe.

³ In a large universe ABE scheme, the attribute universe can be exponentially large, any string can be used as an attribute, and attributes do not need to be pre-specified during setup.

As security, access policy expressivity, and efficiency are the three preliminary directions for ABE research, *traitor tracing* is a compulsory requirement for *practical* ABE schemes. In particular, using Ciphertext-Policy ABE (CP-ABE) [13,5] as an example, ciphertext access policies do not have to contain any receivers’ identities, and more commonly, a CP-ABE policy is role-based and attributes are *shared* between multiple users. For example, the user with attributes {Bob, Mathematics, PhD Student} and the user with attributes {Carl, Mathematics, PhD Student} are sharing the attributes {Mathematics, PhD Student} and both of them can decrypt the ciphertext with policy “(Mathematics AND (PhD Student OR Alumni))”. In practice, a malicious user, with attributes shared with multiple other users, might leak a decryption blackbox/device, which is made of the user’s decryption key, for the purpose of financial gain or some other forms of incentives, as the malicious user has little risk of being identified out of all the users who can build a decryption blackbox with identical decryption capability. Being able to identify this malicious user (refer to as ‘traitor’) is crucial towards the practicality of an ABE system.

With a series of work [21,20,22,23,25,24], Liu et al. formalized the problem of traitor tracing for ABE well and proposed the counterparts supporting traitor tracing for some existing appealing ABE schemes. For example, [20,23] add fully collusion-resistant blackbox traceability to the fully secure CP-ABE scheme in [18], and [24] adds fully collusion-resistant blackbox traceability to the large universe CP-ABE scheme in [28]. Note that the schemes in [20,22,23,25,24] achieve fully collusion-resistant blackbox traceability ⁴ at the cost of sublinear (i.e, linear in the square root of the number of users in the system) overhead, which is the most efficient level to date.

While Liu et al. [21,20,22,23,25,24] transformed several existing appealing ABE schemes to their traceable counterparts, there are still many other appealing ABE schemes for which no traceable counterparts are proposed, for example, the fully secure ABE schemes in [1] which support regular languages, large universe, or constant size ciphertexts. Furthermore, we believe that in the future more and newer ABE schemes with better security, expressivity, efficiency and other appealing features will appear, and to be practical, these existing and future ABE schemes also need to be traceable against traitors. Investigating these schemes and proposing the traceable counterparts one by one will be a heavy workload.

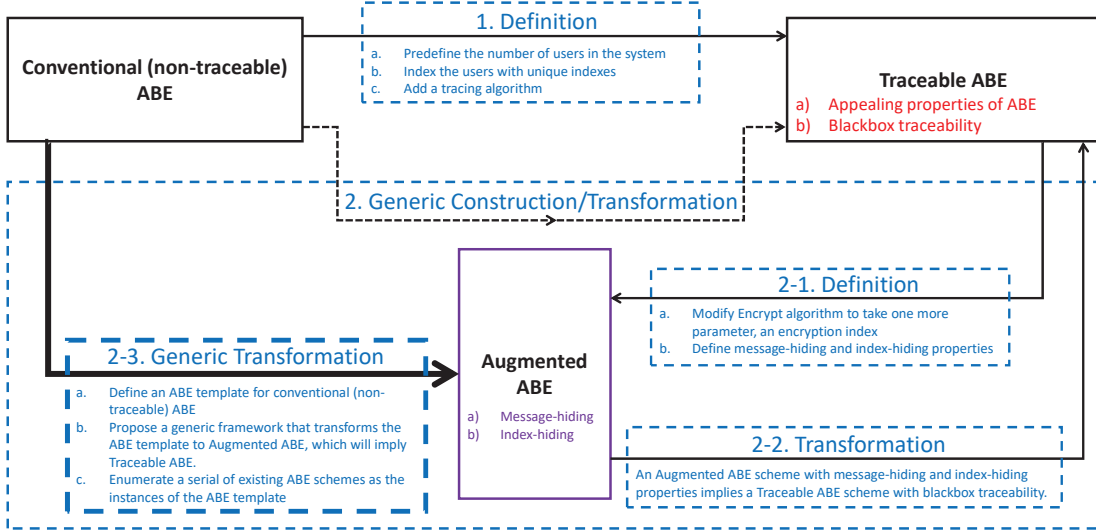
In this paper, we make an attempt to propose a framework to transform existing and future ABE schemes to their traceable counterparts in a generic manner. In particular, by specifying some requirements on the structure of the ABE constructions, we propose an ABE template, and show that any ABE scheme satisfying this template can be transformed to a fully collusion-resistant blackbox traceable ABE scheme in a generic manner, at the cost of sublinear overhead, while keeping the appealing properties of the underlying ABE schemes, such as fine-grained access control on encrypted data, highly expressive access policy, short ciphertext, and so on. The contributions of this framework are two folds:

- For the existing ABE schemes satisfying the template, the traceable counterparts can be given directly by applying the transformation framework. And we indeed show that the appealing ABE schemes in [1], which are fully secure and support regular languages, constant size ciphertexts, or large universe, do satisfy this template. In addition, we also show that the large universe CP-ABE scheme by Rouselakis and Waters [28] also satisfies this template.
- For the existing ABE schemes not satisfying the template and the potential future ABE schemes, this framework provides a ‘target’ which they can try to achieve and then also be transformed to a traceable one.

1.1 Our Results

First, as shown in “1. Definition” of Fig. 1, we define Traceable ABE by extending the definition of Conventional (non-traceable) ABE, i.e., a) predefining the number of users in the system, b) indexing the users with unique indexes, and c) adding a tracing algorithm. As predefining the number of users in the system is a necessary setting for achieving blackbox traceability and does not undermine the capacity of ABE, i.e.

⁴ Fully collusion-resistant traceability means that the number of colluding users in constructing a decryption device is not limited and can be arbitrary.



A conventional (non-traceable) ABE scheme complying with our ABE template can be transformed to a Traceable ABE scheme by the transformation in 2-3 and then 2-2.

Fig. 1. Outline

enabling fine-grained access control on encrypted data, the Traceable ABE has the appealing properties of conventional ABE and additionally supports blackbox traceability. This part is proceeded in Sec. 2.

The aim of this work is to transform existing (even some future) conventional (non-traceable) ABE schemes to traceable counterparts, i.e. proposing a generic framework that enables ABE schemes to be traceable, as shown in “2. Generic Construction/Transformation” of Fig. 1. This aim is achieved by two steps. First, as shown in “2-1 Definition” and “2-2 Transformation” of Fig. 1, we define a simpler primitive called Augmented ABE (or AugABE for short) and show that an Augmented ABE implies a Traceable ABE. This part is proceeded in Sec. 3. Then, as shown in “2-3 Generic Transformation” of Fig. 1, we propose a generic framework to transform Conventional (non-traceable) ABE to Augmented ABE. This part is proceeded in Sec. 4. Thus, for the conventional (non-traceable) ABE schemes that satisfy the proposed ABE template, the “2-3 Generic Transformation” will transform them to Augmented ABE counterparts, then the “2-2 Transformation” will transform those Augmented ABE schemes to corresponding Traceable ABE schemes, which will keep the appealing properties of the corresponding conventional (non-traceable) ABE schemes and additionally support blackbox traceability.

More specifically, in Sec. 2.1, we present a general ABE definition which covers a variety of ABE systems, including CP-ABE, KP-ABE, ABE supporting boolean formula, ABE supporting regular language, etc., and has a potential for supporting blackbox traceability. Namely, we define a ‘functional’ ABE system, which is identical to conventional (non-traceable) ABE, except that each user/decryption key is assigned and identified by a unique index $k \in \{1, \dots, \mathcal{K}\}$ (\mathcal{K} is the number of users in the system). Note that predefining the number of users \mathcal{K} in the system is a necessary setting for achieving blackbox traceability, and in practice this should not incur much concern, and does not undermine the capacity of ABE, i.e. enabling fine-grained access control on encrypted data. In other words, except this necessary setting, the functional ABE has all the appealing properties of conventional ABE, and additionally, as each user/decryption key is uniquely indexed, this functional ABE can support blackbox traceability and is referred to as Traceable ABE, as defined in Sec. 2.2.

In Sec. 3.1, we define Augmented ABE by modifying the definition of Traceable ABE. In particular, Augmented ABE has four algorithms (Setup_A , KeyGen_A , Encrypt_A , Decrypt_A), where the setup, key generation,

and decryption algorithms, i.e., Setup_A , KeyGen_A , and Decrypt_A , are the same as that of the Traceable ABE. The encryption algorithm Encrypt_A takes one more parameter $\bar{k} \in \{1, \dots, \mathcal{K} + 1\}$ than the original one in Traceable ABE, and the decryption criteria in Augmented ABE is changed in such a way that an encrypted message using ciphertext tag Y and encryption index \bar{k} can be recovered using a decryption key $\text{SK}_{k,X}$, which is identified by index $k \in \{1, \dots, \mathcal{K}\}$ and associated with a key tag X , only if $(X \text{ matches } Y) \wedge (k \geq \bar{k})$, where $(X \text{ matches } Y)$ is the standard decryption criteria for conventional ABE and $(k \geq \bar{k})$ is an additional requirement incurred by encryption index \bar{k} . We define the message-hiding and (encryption-) index-hiding properties of Augmented ABE in Sec. 3.1, and in Sec. 3.2 we show that a message-hiding and index-hiding Augmented ABE scheme, say $\Sigma_A = (\text{Setup}_A, \text{KeyGen}_A, \text{Encrypt}_A, \text{Decrypt}_A)$, will imply a secure Traceable ABE scheme $\Sigma = (\text{Setup}_A, \text{KeyGen}_A, \text{Encrypt}, \text{Decrypt}_A)$, where the encryption algorithm Encrypt is derived from Encrypt_A by always setting the encryption index to be 1, and the tracing algorithm Trace is built on Encrypt_A by producing ciphertexts with index $\bar{k} \in \{1, \dots, \mathcal{K}\}$ and feeding these ciphertexts to the decryption blackbox. The message-hiding property of Augmented ABE will guarantee the security of the derived Traceable ABE and the index-hiding property of Augmented ABE will guarantee the traceability of the derived Traceable ABE.

The definitions of Traceable ABE in Sec. 2, the definitions of Augmented ABE in Sec. 3.1, and the reduction of Traceable ABE to Augmented ABE in Sec. 3.2 are similar to previous work in [20,22,23,25,24]. While [20,23,25,24] focus on CP-ABE and [22] focuses on KP-ABE, this paper formalizes the definitions of Traceable ABE and Augmented ABE and the reduction of Traceable ABE to Augmented ABE in a most generic manner, which covers all kinds of ABE, including CP-ABE, KP-ABE, ABE supporting boolean formulas, ABE supporting regular languages, etc. While re-formalizing these preliminaries is a necessary part, the major contribution of this paper lies in the **generic transformation** of Conventional (non-traceable ABE) to Augmented ABE (i.e. the 2-3 part in Fig. 1). In particular,

- We define an ABE template for Conventional (non-traceable) ABE. The template represents a type of ABE construction techniques, so that this template covers not only many existing important ABE schemes with appealing properties, but also some possible ABE schemes in the future, which consider this template and corresponding construction techniques when designed.
- We propose a generic framework that transforms the ABE template to Augmented ABE. This means that all the ABE schemes falling in the template can be transformed to their traceable counterparts, enjoying their original appealing properties and additional fully collusion-resistant blackbox traceability.
 - The overhead for the transformation (i.e. the overhead for the fully collusion-resistant blackbox traceability) is linear in $\sqrt{\mathcal{K}}$, i.e. the resulting Traceable ABE schemes achieve the most efficient level to date for fully collusion-resistant blackbox traceable systems.
 - We prove the message-hiding and index-hiding properties of the resulting Augmented ABE in the standard model. (The outline for the security analysis is given later in Fig. 2.)
- We show some existing appealing ABE schemes, i.e. the ones in [1] which are fully secure and support regular languages, constant size ciphertexts, and large universe, satisfy our ABE template. That is, we can obtain the traceable counterparts for these appealing ABE schemes, by applying our generic transformation framework.
- To cover the appealing ABE schemes in [1], the template, as well as the generic transformation and the proof, are described on composite order groups. To be more general, we show that the template, the transformation, and the proof also work well for the schemes on prime order groups, and present the large universe CP-ABE scheme Rouselakis and Waters [28] as an example.

We do not want to oversell our asymptotic result. Our method/framework considers and works for a subset of pairing-based ABE schemes, namely, those ABE schemes complying with our non-traceable ABE template, rather than ALL the ABE schemes. For example, our framework is not applicable to the lattice-based ABE schemes (e.g. [9]). Actually, as so far there is not known results on lattice-based ABE schemes with traitor tracing.

We would like to view our asymptotic result mainly as a stepping stone towards building practical ABE schemes. In particular, in retrospect, the ABE schemes by Waters [30], Lewko et al. [18], Lewko and Waters [19], Attrapadung [1], and so on, represent one of the main branches of ABE development, as well as a branch

of pairing-based ABE design/construction method, and it is reasonable to believe that new ABE schemes in this branch will be proposed in future. While these ABE schemes have been getting better security, policy expressivity, and/or efficiency, they did not consider or support traitor tracing, and this seriously limits their applicability in practice. Our asymptotic result makes the ABE schemes following this branch to have traitor tracing functionality, while leaving it as future work to further reduce the overhead incurred by traitor tracing functionality and make other types of ABE schemes (e.g. the lattice-based ones) to support traitor tracing.

2 ABE and Blackbox Traceability

In this section, we define a ‘functional’ ABE and its security, which are similar to Conventional (non-traceable) ABE (e.g. [19,28]), except that we explicitly assign and identify users using unique indices. Then we formalize the fully collusion-resistant traceability for this ‘functional’ ABE.

To be as general as possible, in the definitions of this functional ABE, we use the terms ‘ciphertext tag’ and ‘key tag’, rather than ‘access policy’ and ‘attributes’. When the ciphertext tag is an attribute set and the key tag is a Boolean formula, it is a KP-ABE supporting Boolean formula as policy; when ciphertext tag is a Deterministic Finite Automata (DFA) and the key tag is a string, it is a CP-ABE supporting DFA as policy, an so on.

2.1 Attribute-Based Encryption and its Security

Attribute-Based Encryption Syntax. Given integers a and b where $a \leq b$, let $[a, b]$ be the set $\{a, a + 1, \dots, b\}$. Also, we use $[b]$ to denote the set $\{1, 2, \dots, b\}$. Let relation $\Gamma : \mathbb{X} \times \mathbb{Y} \rightarrow \{0, 1\}$ is a predicate function that maps a pair of key tag in a space \mathbb{X} and ciphertext tag in a space \mathbb{Y} to $\{0, 1\}$. An Attribute-Based Encryption (ABE) scheme for predicate Γ consists of following algorithms:

Setup($\lambda, \Gamma, \mathcal{K}$) \rightarrow (PP, MSK). The algorithm takes as input a security parameter λ , a predicate Γ , and the number of users in the system \mathcal{K} , runs in polynomial time in λ , and outputs a public parameter PP and a master secret key MSK.

KeyGen(PP, MSK, X) \rightarrow $\text{SK}_{k,X}$. The algorithm takes as input PP, MSK, and a *key tag* $X \in \mathbb{X}$, and outputs a secret key $\text{SK}_{k,X}$ corresponding to X . The secret key is assigned and identified by a unique index $k \in [\mathcal{K}]$.

Encrypt(PP, M, Y) \rightarrow CT_Y . The algorithm takes as input PP, a message M , and a *ciphertext tag* $Y \in \mathbb{Y}$, and outputs a ciphertext CT_Y . Y is included in CT_Y .

Decrypt(PP, $CT_Y, \text{SK}_{k,X}$) \rightarrow M or \perp . The algorithm takes as input PP, a ciphertext CT_Y , and a secret key $\text{SK}_{k,X}$, and outputs a message M or \perp indicating the failure of decryption.

Correctness. For all $X \in \mathbb{X}$, $Y \in \mathbb{Y}$, and messages M , suppose $(\text{PP}, \text{MSK}) \leftarrow \text{Setup}(\lambda, \Gamma, \mathcal{K})$, $\text{SK}_{k,X} \leftarrow \text{KeyGen}(\text{PP}, \text{MSK}, X)$, $CT_Y \leftarrow \text{Encrypt}(\text{PP}, M, Y)$. If $\Gamma(X, Y) = 1$ then $\text{Decrypt}(\text{PP}, CT_Y, \text{SK}_{k,X}) = M$.

Security. The security of an ABE scheme for predicate Γ is defined using the following message-hiding game, which is a typical semantic security game and is similar to that for conventional ABE [19,28] security.

Game_{MH}. The message-hiding game is defined between a challenger and an adversary \mathcal{A} as follows:

Setup. The challenger runs $\text{Setup}(\lambda, \Gamma, \mathcal{K})$ and gives the public parameter PP to \mathcal{A} .

Phase 1. For $i = 1$ to Q_1 , \mathcal{A} adaptively submits (index, key tag) pair (k_i, X_{k_i}) to ask for secret key for key tag X_{k_i} . For each (k_i, X_{k_i}) pair, the challenger responds with a secret key $\text{SK}_{k_i, X_{k_i}}$, which corresponds to key tag X_{k_i} and has index k_i .

Challenge. \mathcal{A} submits two equal-length messages M_0, M_1 and a ciphertext tag Y^* . The challenger flips a random coin $b \in \{0, 1\}$, and sends $CT_{Y^*} \leftarrow \text{Encrypt}(\text{PP}, M_b, Y^*)$ to \mathcal{A} .

Phase 2. For $i = Q_1 + 1$ to Q , \mathcal{A} adaptively submits (index, key tag) pair (k_i, X_{k_i}) to ask for secret key for key tag X_{k_i} . For each (k_i, X_{k_i}) pair, the challenger responds with a secret key $\text{SK}_{k_i, X_{k_i}}$, which corresponds to key tag X_{k_i} and has index k_i .

Guess. \mathcal{A} outputs a guess $b' \in \{0, 1\}$ for b .

\mathcal{A} wins the game if $b' = b$ under the **restriction** that none of the queried $\{(k_i, X_{k_i})\}_{i=1}^Q$ can satisfy $\Gamma(X_{k_i}, Y^*) = 1$. The advantage of \mathcal{A} is defined as $\text{MHAdv}_{\mathcal{A}} = |\Pr[b' = b] - \frac{1}{2}|$.

Definition 1. A \mathcal{K} -user ABE scheme for predicate Γ is secure if for all probabilistic polynomial time (PPT) adversaries \mathcal{A} , $\text{MHAdv}_{\mathcal{A}}$ is negligible in λ .

We say that a \mathcal{K} -user ABE scheme for predicate Γ is *selectively* secure if we add an **Init** stage before **Setup** where the adversary commits to the challenge ciphertext tag Y^* .

Remark: As pointed out in previous work [20,22,23,25,24], (1) although the KeyGen algorithm is responsible for determining/assigning the index of each user's secret key, to capture the security that an adversary can adaptively choose secret keys to corrupt, the above model allows \mathcal{A} to specify the index when querying for a key, i.e., for $i = 1$ to Q , \mathcal{A} submits pairs of (k_i, X_{k_i}) for secret keys with key tags corresponding to X_{k_i} , and the challenger will assign k_i to be the index of the corresponding secret key, where $Q \leq \mathcal{K}$, $k_i \in [\mathcal{K}]$, and $k_i \neq k_j \forall 1 \leq i \neq j \leq Q$ (this is to ensure that each user/key can be *uniquely* identified by an index). (2) For $k_i \neq k_j$ it does not require $X_{k_i} \neq X_{k_j}$, i.e., different users/keys may have the same key tag.

2.2 Blackbox Traceability

A *ciphertext-tag-specific* decryption blackbox \mathcal{D} is described by a ciphertext tag $Y_{\mathcal{D}}$ and a noticeable probability value ϵ (i.e. $\epsilon = 1/f(\lambda)$ for some polynomial f), and this blackbox \mathcal{D} can decrypt ciphertexts generated under $Y_{\mathcal{D}}$ with probability at least ϵ . Such a blackbox can reflect most practical scenarios, which include the key-like decryption blackbox for sale and decryption blackbox “found in the wild”, which are discussed in [20,23]. In particular, once a blackbox is found being “useful”, i.e. being able to decrypt ciphertexts (regardless of how this is found, for example, an explicit description of the blackbox’s decryption ability is given, or the law enforcement agency finds some clue), we can regard it as a ciphertext-tag-specific decryption blackbox with the corresponding ciphertext tag (which is associated to the ciphertext that it can decrypt).

We now define the tracing algorithm and traceability against ciphertext-tag-specific decryption blackbox.

$\text{Trace}^{\mathcal{D}}(\text{PP}, Y_{\mathcal{D}}, \epsilon) \rightarrow \mathbb{K}_T \subseteq [\mathcal{K}]$. *Trace* is an oracle algorithm that interacts with a ciphertext-tag-specific decryption blackbox \mathcal{D} . By given the public parameter PP , a ciphertext tag $Y_{\mathcal{D}}$, and a probability value ϵ , the algorithm runs in time polynomial in λ and $1/\epsilon$, and outputs an index set $\mathbb{K}_T \subseteq [\mathcal{K}]$ which identifies the set of malicious users. Note that ϵ has to be polynomially related to λ , i.e. $\epsilon = 1/f(\lambda)$ for some polynomial f .

Traceability. The following tracing game captures the notion of **fully collusion-resistant traceability** against ciphertext-tag-specific decryption blackbox. In the game, the adversary targets to build a decryption blackbox \mathcal{D} that can decrypt ciphertexts under some ciphertext tag $Y_{\mathcal{D}}$. The tracing algorithm, on the other side, is designed to extract the index of at least one of the malicious users whose decryption keys have been used for constructing \mathcal{D} .

Game_{TR}. The tracing game is defined between a challenger and an adversary \mathcal{A} as follows:

Setup. The challenger runs $\text{Setup}(\lambda, \Gamma, \mathcal{K})$ and gives the public parameter PP to \mathcal{A} .

Key Query. For $i = 1$ to Q , \mathcal{A} adaptively submits (index, key tag) pair (k_i, X_{k_i}) to ask for secret key for key tag X_{k_i} . For each (k_i, X_{k_i}) pair, the challenger responds with a secret key $\text{SK}_{k_i, X_{k_i}}$, which corresponds to key tag X_{k_i} and has index k_i .

Decryption Blackbox Generation. \mathcal{A} outputs a decryption blackbox \mathcal{D} associated with a ciphertext tag $Y_{\mathcal{D}}$ and a non-negligible probability value ϵ .

Tracing. The challenger runs $\text{Trace}^{\mathcal{D}}(\text{PP}, Y_{\mathcal{D}}, \epsilon)$ to obtain an index set $\mathbb{K}_T \subseteq [\mathcal{K}]$.

Let $\mathbb{K}_{\mathcal{D}} = \{k_i | 1 \leq i \leq Q\}$ be the index set of secret keys corrupted by the adversary. We say that \mathcal{A} wins the game if the following two conditions hold:

1. $\Pr[\mathcal{D}(\text{Encrypt}(\text{PP}, M, Y_{\mathcal{D}})) = M] \geq \epsilon$, where the probability is taken over the random choices of message M and the random coins of \mathcal{D} . A decryption blackbox satisfying this condition is said to be a *useful ciphertext-tag-specific decryption blackbox*.
2. $\mathbb{K}_T = \emptyset$, or $\mathbb{K}_T \not\subseteq \mathbb{K}_{\mathcal{D}}$, or $(\Gamma(X_{k_t}, Y_{\mathcal{D}}) \neq 1 \forall k_t \in \mathbb{K}_T)$.

We denote by $\text{TRAdv}_{\mathcal{A}}$ the probability that \mathcal{A} wins.

Remark: For a useful ciphertext-tag-specific decryption blackbox \mathcal{D} , the traced \mathbb{K}_T must satisfy $(\mathbb{K}_T \neq \emptyset) \wedge (\mathbb{K}_T \subseteq \mathbb{K}_{\mathcal{D}}) \wedge (\exists k_t \in \mathbb{K}_T \text{ s.t. } \Gamma(X_{k_t}, Y_{\mathcal{D}}) = 1)$ for traceability. (1) $(\mathbb{K}_T \neq \emptyset) \wedge (\mathbb{K}_T \subseteq \mathbb{K}_{\mathcal{D}})$ captures the preliminary traceability that the tracing algorithm can extract at least one malicious user and the coalition of malicious users cannot frame any innocent user. (2) $(\exists k_t \in \mathbb{K}_T \text{ s.t. } \Gamma(X_{k_t}, Y_{\mathcal{D}}) = 1)$ captures the *strong traceability* that the tracing algorithm can extract at least one malicious user whose secret key enables \mathcal{D} to have the decryption ability corresponding to $Y_{\mathcal{D}}$. We refer to [17,20] for why strong traceability is desirable.

Note that, as of [7,8,11,17,20], we are modeling a stateless (resettable) decryption blackbox – such a blackbox is just an oracle and maintains no state between activations. Also note that we are modeling public traceability, namely, the **Trace** algorithm does not need any secrets and anyone can perform the tracing.

Definition 2. A \mathcal{K} -user ABE scheme for predicate Γ is traceable against ciphertext-tag-specific decryption blackbox if for all PPT adversaries \mathcal{A} , $\text{TRAdv}_{\mathcal{A}}$ is negligible in λ .

We say that a \mathcal{K} -user ABE scheme for predicate Γ is *selectively* traceable against ciphertext-tag-specific decryption blackbox if we add an **Init** stage before **Setup** where the adversary commits to the ciphertext tag $Y_{\mathcal{D}}$.

3 Augmented Attribute-Based Encryption

As outlined in Sec. 1.1, we now define Augmented ABE (or AugABE for short) from the ABE above and formalize its message-hiding and index-hiding notions, then show that a message-hiding and index-hiding AugABE can be transformed to a secure ABE with blackbox traceability.

3.1 Definitions

An AugABE scheme has four algorithms: $\text{Setup}_{\mathcal{A}}$, $\text{KeyGen}_{\mathcal{A}}$, $\text{Encrypt}_{\mathcal{A}}$, and $\text{Decrypt}_{\mathcal{A}}$. The setup algorithm $\text{Setup}_{\mathcal{A}}$ and key generation algorithm $\text{KeyGen}_{\mathcal{A}}$ are the same as that of ABE, respectively. For the encryption algorithm, it takes one more parameter $\bar{k} \in [\mathcal{K} + 1]$ as input, and is defined as follows.

$\text{Encrypt}_{\mathcal{A}}(\text{PP}, M, Y, \bar{k}) \rightarrow CT_Y$. The algorithm takes as input PP, a message M , a ciphertext tag Y , and an index $\bar{k} \in [\mathcal{K} + 1]$, and outputs a ciphertext CT_Y . Y is included in CT_Y , but the value of \bar{k} is not.

The decryption algorithm $\text{Decrypt}_{\mathcal{A}}$ is also defined in the same way as that of ABE. However, the correctness definition is changed to the following.

Correctness. For all $X \in \mathbb{X}$, $Y \in \mathbb{Y}$, $\bar{k} \in [\mathcal{K} + 1]$, and messages M , suppose $(\text{PP}, \text{MSK}) \leftarrow \text{Setup}_{\mathcal{A}}(\lambda, \Gamma, \mathcal{K})$, $\text{SK}_{k,X} \leftarrow \text{KeyGen}_{\mathcal{A}}(\text{PP}, \text{MSK}, X)$, $CT_Y \leftarrow \text{Encrypt}_{\mathcal{A}}(\text{PP}, M, Y, \bar{k})$. If $(\Gamma(X, Y) = 1) \wedge (k \geq \bar{k})$ then $\text{Decrypt}_{\mathcal{A}}(\text{PP}, CT_Y, \text{SK}_{k,X}) = M$.

Note that during decryption, as long as $\Gamma(X, Y) = 1$, the decryption algorithm outputs a message, but only when $k \geq \bar{k}$, the output message is equal to the correct message, that is, $k \geq \bar{k}$ is an additional condition and if and only if $(\Gamma(X, Y) = 1) \wedge (k \geq \bar{k})$, can $\text{SK}_{k,X}$ correctly decrypt a ciphertext under (Y, \bar{k}) . If we always set $\bar{k} = 1$, the functions of AugABE are identical to that of ABE. In fact, the idea behind transforming an AugABE to a traceable ABE, that we will show shortly, is to construct an AugABE with index-hiding property, and then always sets $\bar{k} = 1$ in normal encryption, while using $\bar{k} \in [\mathcal{K} + 1]$ to generate ciphertexts for tracing.

Security. We define the security of AugABE in three games. The first game is a **message-hiding game** and says that a ciphertext created using index 1 is unreadable to the users whose key tags do not satisfy

the ciphertext tag. The second game is a **message-hiding game** and says that a ciphertext created using index $\mathcal{K} + 1$ is unreadable by anyone. The third game is an **index-hiding game** and captures the intuition that a ciphertext created using index \bar{k} reveals no non-trivial information about \bar{k} .

$\text{Game}_{\text{MH}_1}^{\text{A}}$. The **message-hiding game** $\text{Game}_{\text{MH}_1}^{\text{A}}$ is similar to Game_{MH} except that the **Challenge** phase is

Challenge. \mathcal{A} submits two equal-length messages M_0, M_1 and a ciphertext tag Y^* . The challenger flips a random coin $b \in \{0, 1\}$, and sends $CT_{Y^*} \leftarrow \text{Encrypt}_{\text{A}}(\text{PP}, M_b, Y^*, 1)$ to \mathcal{A} .

\mathcal{A} wins the game if $b' = b$ under the **restriction** that none of the queried $\{(k_i, X_{k_i})\}_{i=1}^Q$ can satisfy $\Gamma(X_{k_i}, Y^*) = 1$. The advantage of \mathcal{A} is defined as $\text{MH}_1^{\text{A}}\text{Adv}_{\mathcal{A}} = |\Pr[b' = b] - \frac{1}{2}|$.

Definition 3. A \mathcal{K} -user Augmented ABE scheme for predicate Γ is Type-I message-hiding if for all PPT adversaries \mathcal{A} the advantage $\text{MH}_1^{\text{A}}\text{Adv}_{\mathcal{A}}$ is negligible in λ .

We say that an Augmented ABE scheme for predicate Γ is *selectively* Type-I message-hiding if we add an **Init** stage before **Setup** where the adversary commits to the challenge ciphertext tag Y^* .

$\text{Game}_{\text{MH}_2}^{\text{A}}$. The **message-hiding game** $\text{Game}_{\text{MH}_2}^{\text{A}}$ is similar to Game_{MH} except that the **Challenge** phase is

Challenge. \mathcal{A} submits two equal-length messages M_0, M_1 and a ciphertext tag Y^* . The challenger flips a random coin $b \in \{0, 1\}$, and sends $CT_{Y^*} \leftarrow \text{Encrypt}_{\text{A}}(\text{PP}, M_b, Y^*, \mathcal{K} + 1)$ to \mathcal{A} .

\mathcal{A} wins the game if $b' = b$. The advantage of \mathcal{A} is defined as $\text{MH}_2^{\text{A}}\text{Adv}_{\mathcal{A}} = |\Pr[b' = b] - \frac{1}{2}|$.

Definition 4. A \mathcal{K} -user Augmented ABE scheme for predicate Γ is Type-II message-hiding if for all PPT adversaries \mathcal{A} the advantage $\text{MH}_2^{\text{A}}\text{Adv}_{\mathcal{A}}$ is negligible in λ .

$\text{Game}_{\text{IH}}^{\text{A}}$. The **index-hiding game** defines that, for any ciphertext tag Y^* , without a secret key $\text{SK}_{\bar{k}, X_{\bar{k}}}$ such that $\Gamma(X_{\bar{k}}, Y^*) = 1$, an adversary cannot distinguish between a ciphertext under (Y^*, \bar{k}) and $(Y^*, \bar{k} + 1)$. The game proceeds as follows:

Setup. The challenger runs $\text{Setup}_{\text{A}}(\lambda, \Gamma, \mathcal{K})$ and gives the public parameter PP to \mathcal{A} .

Key Query. For $i = 1$ to Q , \mathcal{A} adaptively submits (index, key tag) pair (k_i, X_{k_i}) to ask for secret key for key tag X_{k_i} . For each (k_i, X_{k_i}) pair, the challenger responds with a secret key $\text{SK}_{k_i, X_{k_i}}$, which corresponds to key tag X_{k_i} and has index k_i .

Challenge. \mathcal{A} submits a message M and a ciphertext tag pair Y^* . The challenger flips a random coin $b \in \{0, 1\}$, and sends $CT_{Y^*} \leftarrow \text{Encrypt}_{\text{A}}(\text{PP}, M, Y^*, \bar{k} + b)$ to \mathcal{A} .

Guess. \mathcal{A} outputs a guess $b' \in \{0, 1\}$ for b .

\mathcal{A} wins the game if $b' = b$ under the **restriction** that none of the queried pairs $\{(k_i, X_{k_i})\}_{i=1}^Q$ can satisfy $(k_i = \bar{k}) \wedge (\Gamma(X_{k_i}, Y^*) = 1)$. The advantage of \mathcal{A} is defined as $\text{IH}^{\text{A}}\text{Adv}_{\mathcal{A}}[\bar{k}] = |\Pr[b' = b] - \frac{1}{2}|$.

Definition 5. A \mathcal{K} -user Augmented ABE scheme for predicate Γ is index-hiding if for all PPT adversaries \mathcal{A} the advantages $\text{IH}^{\text{A}}\text{Adv}_{\mathcal{A}}[\bar{k}]$ for $\bar{k} = 1, \dots, \mathcal{K}$ are negligible in λ .

We say that an Augmented ABE scheme for predicate Γ is *selectively* index-hiding if we add an **Init** stage before **Setup** where the adversary commits to the challenge ciphertext tag Y^* .

3.2 The Reduction of Traceable ABE to Augmented ABE

Let $\Sigma_{\text{A}} = (\text{Setup}_{\text{A}}, \text{KeyGen}_{\text{A}}, \text{Encrypt}_{\text{A}}, \text{Decrypt}_{\text{A}})$ be an AugABE, define $\text{Encrypt}(\text{PP}, M, Y) = \text{Encrypt}_{\text{A}}(\text{PP}, M, Y, 1)$, then $\Sigma = (\text{Setup}_{\text{A}}, \text{KeyGen}_{\text{A}}, \text{Encrypt}, \text{Decrypt}_{\text{A}})$ is an ABE derived from Σ_{A} . In the following, we show that if Σ_{A} is Type-I message-hiding, then Σ is secure (w.r.t. Def. 1). Furthermore, we propose a tracing algorithm **Trace** for Σ and show that if Σ_{A} is Type-II message-hiding and index-hiding, then Σ (equipped with **Trace**) is traceable (w.r.t. Def. 2).

3.2.1 ABE Security

Theorem 1. *If Σ_A is Type-I message-hiding (resp. selectively Type-I message-hiding), then Σ is secure (resp. selectively secure).*

Proof. The proof is similar to that in [20,23]. Due to the page limitation, we omit the details here.

3.2.2 ABE Traceability

We now propose a tracing algorithm `Trace`, which uses a general tracing method previously used in [6,26,7,8,11,20], and show that equipped with `Trace`, Σ is traceable (w.r.t. Def. 2).

$\text{Trace}^{\mathcal{D}}(\text{PP}, Y_{\mathcal{D}}, \epsilon) \rightarrow \mathbb{K}_T \subseteq [\mathcal{K}]$: Given a ciphertext-tag-specific decryption blackbox \mathcal{D} associated with a ciphertext tag $Y_{\mathcal{D}}$ and probability $\epsilon > 0$, the tracing algorithm works as follows:

1. For $k = 1$ to $\mathcal{K} + 1$, do the following:
 - (a) Repeat the following $8\lambda(N/\epsilon)^2$ times:
 - i. Sample M from the message space at random.
 - ii. Let $CT_{Y_{\mathcal{D}}} \leftarrow \text{Encrypt}_A(\text{PP}, M, Y_{\mathcal{D}}, k)$.
 - iii. Query oracle \mathcal{D} on input $CT_{Y_{\mathcal{D}}}$, and compare the output of \mathcal{D} with M .
 - (b) Let \hat{p}_k be the fraction of times that \mathcal{D} decrypted the ciphertexts correctly.
2. Let \mathbb{K}_T be the set of all $k \in [\mathcal{K}]$ for which $\hat{p}_k - \hat{p}_{k+1} \geq \epsilon/(4\mathcal{K})$. Output \mathbb{K}_T as the index set of the decryption keys of malicious users.

Theorem 2. *If Σ_A is Type-II message-hiding and index-hiding (resp. selectively index-hiding), then Σ is traceable (resp. selectively traceable).*

Proof. The proof is similar to that in [20,23]. Due to the page limitation, we omit the details here.

4 Transform a Non-Traceable ABE to an Augmented ABE

In this section, we first formalize the notation of Pair Encoding Scheme in Sec. 4.1, which is the core components of the conventional (non-traceable) ABE template we propose in Sec. 4.2. Then in Sec. 4.3 we propose the generic transformation from the ABE template to the Augmented ABE and in Sec. 4.4 prove the security of the resulting Augmented ABE.

Note that the ABE template, the transformation, and the proof in this section are described in composite order bilinear groups, but as shown later in Sec. 5, all these also work well in prime order bilinear groups.

4.1 Pair Encoding Scheme: Syntax

The notion of Pair Encoding Scheme here is inspired by the work of Attrapdung [1]. Attrapdung [1] proposed the notion of Pair Encoding Scheme, including syntax and security definitions, and proved the full security of some Functional Encryption schemes based on the security of corresponding Pair Encoding Scheme instantiations. Here we borrow the term of Pair Encoding Scheme, and actually we *only use the syntax* to abstract the *structures* of the non-traceable ABE schemes which we aim to transform to AugABE, while not considering or using the security properties of Pair Encoding Scheme.

A Pair Encoding Scheme for predicate Γ consists of four deterministic algorithms given by $(\text{SysParam}, \text{KeyParam}, \text{CiperParam}, \text{DecPair})$:

- $\text{SysParam}(\Gamma) \rightarrow (d, d_0)$. It takes as input a predicate $\Gamma : \mathbb{X} \times \mathbb{Y} \rightarrow \{0, 1\}$ and outputs two integers d and d_0 . d is used to specify the number of *common variables* in `KeyParam` and `CiperParam`, and $d_0 (\leq d)$ will be used to specify the requirements of the ABE template. For the default notation, let α and $\beta = (\beta_1, \dots, \beta_d)$ denote the list of common variables.

- $\text{KeyParam}(X, N) \rightarrow (\phi = (\phi_0, \phi_1, \dots, \phi_{d_k}), d_\delta)$. It takes as inputs $N \in \mathbb{N}$ and a key tag $X \in \mathbb{X}$, and outputs a sequence of polynomials $\phi = (\phi_0, \phi_1, \dots, \phi_{d_k})$ with coefficients in \mathbb{Z}_N and an integer d_δ that specifies the number of its own variables. Let $\delta = (\delta_1, \dots, \delta_{d_\delta})$ be the variables, we require that each polynomial $\phi_z (0 \leq z \leq d_k)$ is a *linear combination of monomials* $\alpha, \delta_i, \delta_i \beta_j$, where $\alpha, \beta = (\beta_1, \dots, \beta_d)$ are the common variables. For simplicity, we write $\phi(\alpha, \beta, \delta) = (\phi_0(\alpha, \beta, \delta), \phi_1(\alpha, \beta, \delta), \dots, \phi_{d_k}(\alpha, \beta, \delta))$.
- $\text{CiperParam}(Y, N) \rightarrow (\psi = (\psi_1, \dots, \psi_{d_c}), d_\pi)$. It takes as inputs $N \in \mathbb{N}$ and a ciphertext tag $Y \in \mathbb{Y}$, and outputs a sequence of polynomials $\psi = (\psi_1, \dots, \psi_{d_c})$ with coefficients in \mathbb{Z}_N and an integer d_π that specifies the number of its own variables. Let $\pi = (\pi, \pi_1, \dots, \pi_{d_\pi})$ be the variables, we require that each polynomial $\psi_z (1 \leq z \leq d_c)$ is a *linear combination of monomials* $\pi, \pi_i, \pi \beta_j, \pi_i \beta_j$, where $\beta = (\beta_1, \dots, \beta_d)$ are the common variables. For simplicity, we write $\psi(\beta, \pi) = (\psi_1(\beta, \pi), \dots, \psi_{d_c}(\beta, \pi))$.
- $\text{DecPair}(X, Y, N) \rightarrow \mathbf{E}$. It takes as inputs $N \in \mathbb{N}$, a key tag $X \in \mathbb{X}$, and a ciphertext tag $Y \in \mathbb{Y}$, and output $\mathbf{E} \in \mathbb{Z}_N^{(d_k+1) \times (d_c)}$.

Correctness. The correctness requirement is defined as follows.

- First, for any $N \in \mathbb{N}$, $X \in \mathbb{X}$, $Y \in \mathbb{Y}$, let $(\phi = (\phi_0, \phi_1, \dots, \phi_{d_k}), d_\delta) \leftarrow \text{KeyParam}(X, N)$, $(\psi = (\psi_1, \dots, \psi_{d_c}), d_\pi) \leftarrow \text{CiperParam}(Y, N)$, and $\mathbf{E} \leftarrow \text{DecPair}(X, Y, N)$, if $\Gamma(X, Y) = 1$, then for any $\alpha, \beta = (\beta_1, \dots, \beta_d), \delta = (\delta_1, \dots, \delta_{d_\delta}), \pi = (\pi, \pi_1, \dots, \pi_{d_\pi})$, we have $\phi(\alpha, \beta, \delta) \mathbf{E} \psi(\beta, \pi)^T = \alpha \pi$, where the equality holds symbolically. Note that since $\phi(\alpha, \beta, \delta) \mathbf{E} \psi(\beta, \pi)^T = \sum_{i \in [0, d_k], j \in [1, d_c]} E_{i,j} \phi_i \psi_j$, this correctness amounts to check if there is a linear combination of $\phi_i \psi_j$ terms summed up to $\alpha \pi$.
- Second, for p that divides N , if we let $\text{KeyParam}(X, N) \rightarrow (\phi = (\phi_0, \phi_1, \dots, \phi_{d_k}), d_\delta)$ and $\text{KeyParam}(X, p) \rightarrow (\phi' = (\phi'_0, \phi'_1, \dots, \phi'_{d_k}), d_\delta)$, then it holds that $\phi \bmod p = \phi'$. The requirement for CiperParam is similar.

Remark. We mandate that the variables used in KeyParam and those in CiperParam are different except only the common variables α and β . We remark that in the syntax, all variables are only *symbolic*: no probability distributions have been assigned to them yet. (We will assign these in the later ABE template construction). Note that d_δ, d_k , can depend on X and d_π, d_c can depend on Y . We also remark that each polynomial in ϕ, ψ has no constant terms.

4.2 A Template for Non-traceable ABE Constructions

Below, we first review the Composite Order Bilinear Groups and some notations. Then, from a Pair Encoding Scheme, by adding some additional requirements, we define a template for Conventional (non-traceable) ABE constructions, which works on composite order bilinear groups. We would like to point out, as shown later in Sec. 5, the template can be easily changed to one on prime order bilinear groups, and the transformation from the non-traceable ABE template to Augmented ABE, as well as the proof, work well on prime order bilinear groups.

Composite Order Bilinear Groups. Let \mathcal{G} be a group generator, which takes a security parameter λ and outputs $(p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)$ where p_1, p_2, p_3 are distinct primes, \mathbb{G} and \mathbb{G}_T are cyclic groups of order $N = p_1 p_2 p_3$, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ a map such that: (1) (Bilinear) $\forall g, h \in \mathbb{G}, a, b \in \mathbb{Z}_N, e(g^a, h^b) = e(g, h)^{ab}$, (2) (Non-Degenerate) $\exists g \in \mathbb{G}$ such that $e(g, g)$ has order N in \mathbb{G}_T . Assume that group operations in \mathbb{G} and \mathbb{G}_T as well as the bilinear map e are computable in polynomial time with respect to λ . Let $\mathbb{G}_{p_1}, \mathbb{G}_{p_2}$ and \mathbb{G}_{p_3} be the subgroups of order p_1, p_2 and p_3 in \mathbb{G} , respectively. These subgroups are “orthogonal” to each other under the bilinear map e : if $h_i \in \mathbb{G}_{p_i}$ and $h_j \in \mathbb{G}_{p_j}$ for $i \neq j$, then $e(h_i, h_j) = 1$ (the identity element in \mathbb{G}_T).

Notations. For a given vector $\mathbf{v} = (v_1, \dots, v_d) \in \mathbb{Z}_N^d$ and $g \in \mathbb{G}$, by $g^{\mathbf{v}}$ we mean the vector $(g^{v_1}, \dots, g^{v_d}) \in \mathbb{G}^d$. For two vectors $\mathbf{V} = (V_1, \dots, V_d), \mathbf{W} = (W_1, \dots, W_d) \in \mathbb{G}^d$, by $\mathbf{V} \cdot \mathbf{W}$ we mean the vector $(V_1 \cdot W_1, \dots, V_d \cdot W_d) \in \mathbb{G}^d$, i.e. it performs component-wise multiplication. Furthermore, by $e_d(\mathbf{V}, \mathbf{W})$ we mean $\prod_{k=1}^d e(V_k, W_k)$. Particularly, for $\mathbf{v} = (v_1, \dots, v_d), \mathbf{w} = (w_1, \dots, w_d) \in \mathbb{Z}_N^d$, we have $g^{\mathbf{v}} \cdot g^{\mathbf{w}} = g^{\mathbf{v}+\mathbf{w}}$, and $e_d(g^{\mathbf{v}}, g^{\mathbf{w}}) = \prod_{k=1}^d e(g^{v_k}, g^{w_k}) = e(g, g)^{(\mathbf{v} \cdot \mathbf{w})}$, where $(\mathbf{v} \cdot \mathbf{w})$ is the inner product of \mathbf{v} and \mathbf{w} . Sometimes we omit the subscript d of $e_d(\mathbf{V}, \mathbf{W})$. For a vector $\mathbf{V} = (V_1, \dots, V_d) \in \mathbb{G}_d$ and a matrix $\mathbf{A} = (A_{i,j})_{d \times t} \in \mathbb{Z}_N^{d \times t}$, by $\mathbf{V}^{\mathbf{A}}$ we mean $(\prod_{i=1}^n V_i^{A_{i,1}}, \prod_{i=1}^n V_i^{A_{i,2}}, \dots, \prod_{i=1}^n V_i^{A_{i,t}}) \in \mathbb{G}^t$.

Non-traceable ABE template. The template consists of four algorithms as follows:

$\text{Setup}_{\text{NT}}(\lambda, \Gamma) \rightarrow (\text{PP}, \text{MSK})$. Run $(N, p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$. Pick generators $g \in \mathbb{G}_{p_1}$, $X_3 \in \mathbb{G}_{p_3}$. Run $(d, d_0) \leftarrow \text{SysParam}(\Gamma)$, where $1 \leq d_0 \leq d$. Pick random $\beta = (\beta_1, \dots, \beta_d) \in \mathbb{Z}_N^d$. Pick random $\alpha \in \mathbb{Z}_N$. The public parameter is

$$\text{PP} = ((N, \mathbb{G}, \mathbb{G}_T, e), g, g^\beta, X_3, e(g, g)^\alpha).$$

The master secret key is $\text{MSK} = (\alpha)$.

$\text{KeyGen}_{\text{NT}}(\text{PP}, \text{MSK}, X) \rightarrow \text{SK}_X$. Upon input a key tag X , run $(\phi = (\phi_0, \phi_1, \dots, \phi_{d_k}), d_\delta) \leftarrow \text{KeyParam}(X, N)$. Pick random $\delta = (\delta_1, \dots, \delta_{d_\delta}) \in \mathbb{Z}_N^{d_\delta}$, $\mathbf{R} = (R_0, \dots, R_{d_k}) \in \mathbb{G}_{p_3}^{d_k+1}$. Output a secret key SK_X as

$$\text{SK}_X = (X, \mathbf{K} = g^{\phi(\alpha, \beta, \delta)} \cdot \mathbf{R}).$$

To satisfy the template, it is required that for any key tag X and variables $\delta = (\delta_1, \dots, \delta_{d_\delta})$,

1. $d_k \geq d_0$.
2. for $z \in [2, d_k]$, $\phi_z(\alpha, \beta, \delta)$ does not contain α or $\beta_1 \delta_1$. For simplicity, we write them as $\phi_z(\beta, \delta)$, as they do not contain α .
3. $\phi_1(\alpha, \beta, \delta) = \delta_1$, $\phi_0(\alpha, \beta, \delta) = \alpha + \beta_1 \delta_1 + \sum_{\tilde{d}=2}^{d_0} \beta_{\tilde{d}} \phi_{\tilde{d}}(\beta, \delta)$.

That is,⁵

$$\begin{aligned} \text{SK}_X = (X, & (K_0 = g^\alpha g^{\beta_1 \delta_1} \prod_{\tilde{d}=2}^{d_0} g^{\beta_{\tilde{d}} \phi_{\tilde{d}}(\beta, \delta)} R_0, K_1 = g^{\delta_1} \cdot R_1, \\ & K_2 = g^{\phi_2(\beta, \delta)} \cdot R_2, \dots, K_{d_k} = g^{\phi_{d_k}(\beta, \delta)} \cdot R_{d_k})). \end{aligned}$$

$\text{Encrypt}_{\text{NT}}(\text{PP}, M, Y) \rightarrow CT_Y$. Upon input a ciphertext tag Y , run $(\psi = (\psi_1, \dots, \psi_{d_c}), d_\pi) \leftarrow \text{CiperParam}(Y, N)$. Pick random $\pi = (\pi, \pi_1, \dots, \pi_{d_\pi}) \in \mathbb{Z}_N^{d_\pi+1}$. Set $\mathbf{P} = g^{\psi(\beta, \pi)}$. Output a ciphertext CT_Y as

$$CT_Y = (Y, \mathbf{P}, C = M \cdot e(g, g)^{\alpha \pi}).$$

Note that \mathbf{P} can be computed from g^β and π since $\psi(\beta, \pi)$ contains only linear combinations of monomials $\pi, \pi_i, \pi \beta_j, \pi_i \beta_j$.

To satisfy the template, it is required that for any ciphertext tag Y and variables $\pi = (\pi, \pi_1, \dots, \pi_{d_\pi})$,

1. $\psi_1(\beta, \pi) = \pi$.
2. $\psi_2(\beta, \pi) = \beta_2 \pi, \dots, \psi_{d_0}(\beta, \pi) = \beta_{d_0} \pi$.

That is, the first d_0 components of \mathbf{P} are $P_1 = g^\pi, P_2 = g^{\beta_2 \pi}, \dots, P_{d_0} = g^{\beta_{d_0} \pi}$.

$\text{Decrypt}_{\text{NT}}(\text{PP}, CT_Y, \text{SK}_X) \rightarrow M$ or \perp . Obtain X, Y from SK_X, CT_Y . Suppose $\Gamma(X, Y) = 1$ (if $\Gamma(X, Y) \neq 1$, output \perp). Run $\mathbf{E} \leftarrow \text{DecPair}(X, Y, N)$. Compute $e(g, g)^{\alpha \pi} = e(\mathbf{K}^{\mathbf{E}}, \mathbf{P})$, and output $M \leftarrow C / e(g, g)^{\alpha \pi}$.

To satisfy the template, it is required that there are two algorithms DecPair_1 and DecPair_2 such that:

- For any $N \in \mathbb{N}$, $X \in \mathbb{X}$, $Y \in \mathbb{Y}$, let $(\phi = (\phi_0, \phi_1, \dots, \phi_{d_k}), d_\delta) \leftarrow \text{KeyParam}(X, N)$, $(\psi = (\psi_1, \dots, \psi_{d_c}), d_\pi) \leftarrow \text{CiperParam}(Y, N)$, for any variables $\alpha, \beta = (\beta_1, \beta_2, \dots, \beta_d), \delta = (\delta_1, \delta_2, \dots, \delta_{d_\delta}), \pi = (\pi, \pi_1, \dots, \pi_{d_\pi})$, let $\mathbf{E}_1 \leftarrow \text{DecPair}_1(X, Y, N)$, $\mathbf{E}_2 \leftarrow \text{DecPair}_2(X, Y, N)$, if $\Gamma(X, Y) = 1$ we have that $\phi \mathbf{E}_1 \psi^T = \beta_1 \delta_1 \pi$ and $\phi \mathbf{E}_2 \psi^T = \beta_1 \delta_1 \pi + \alpha \pi$.

Note that $e(g, g)^{\alpha \pi}$ can be computed by $e(g, g)^{\alpha \pi} = e(\mathbf{K}^{\mathbf{E}_2}, \mathbf{P}) / e(\mathbf{K}^{\mathbf{E}_1}, \mathbf{P})$.

Later we will show there are a series of ABE schemes with appealing features complying with this template.

⁵ Note that to cover as many ABE schemes as possible, we only specify the *necessary* requirements which we may use in the constructions and proofs of our generic transformation framework. Here we do not require $\phi_{\tilde{d}}(\beta, \delta)$ (for $\tilde{d} = 2$ to d_0) to contain only linear combination of monomials δ_i . Actually, if $\phi_{\tilde{d}}(\beta, \delta)$ contained β_j , K_0 could still be computed, by putting β in MSK.

4.3 Augmented ABE Transformed from Non-traceable ABE

Notations. Suppose that the number of users \mathcal{K} in the system equals to m^2 for some m . In practice, if \mathcal{K} is not a square, we can add some “dummy” users until it pads to the next square. We arrange the users in an $m \times m$ matrix and uniquely assign a tuple (i, j) , where $i, j \in [1, m]$, to each user. A user at position (i, j) of the matrix has index $k = (i - 1) * m + j$. For simplicity, we directly use (i, j) as the index where $(i, j) \geq (\bar{i}, \bar{j})$ means that $((i > \bar{i}) \vee (i = \bar{i} \wedge j \geq \bar{j}))$. The use of pairwise notation (i, j) is purely a notational convenience, as $k = (i - 1) * m + j$ defines a bijection between $\{(i, j) | i, j \in [1, m]\}$ and $[1, \mathcal{K}]$. Given a bilinear group order N , one can randomly choose $r_x, r_y, r_z \in \mathbb{Z}_N$, and set $\chi_1 = (r_x, 0, r_z)$, $\chi_2 = (0, r_y, r_z)$, $\chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$. Let $\text{span}\{\chi_1, \chi_2\} = \{\nu_1 \chi_1 + \nu_2 \chi_2 | \nu_1, \nu_2 \in \mathbb{Z}_N\}$ be the subspace spanned by χ_1 and χ_2 . We can see that χ_3 is orthogonal to the subspace $\text{span}\{\chi_1, \chi_2\}$ and $\mathbb{Z}_N^3 = \text{span}\{\chi_1, \chi_2, \chi_3\} = \{\nu_1 \chi_1 + \nu_2 \chi_2 + \nu_3 \chi_3 | \nu_1, \nu_2, \nu_3 \in \mathbb{Z}_N\}$. For any $\mathbf{v} \in \text{span}\{\chi_1, \chi_2\}$, $(\chi_3 \cdot \mathbf{v}) = 0$, and for random $\mathbf{v} \in \mathbb{Z}_N^3$, $(\chi_3 \cdot \mathbf{v}) \neq 0$ happens with overwhelming probability.

Below we propose our AugABE construction, which is transformed from the Conventional (Non-traceable) ABE template in above Sec. 4.2. Note that the parts written in the box are the same as the Conventional (Non-traceable) ABE template, and we add/modify some additional parts to form our generic AugABE construction.

$\text{Setup}_A(\lambda, \Gamma, \mathcal{K} = m^2) \rightarrow (\text{PP}, \text{MSK})$. Run $(N, p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$. Pick generators $g \in \mathbb{G}_{p_1}$, $X_3 \in \mathbb{G}_{p_3}$. Run $(d, d_0) \leftarrow \text{SysParam}(\Gamma)$, where $1 \leq d_0 \leq d$. Pick random $\beta = (\beta_1, \dots, \beta_d) \in \mathbb{Z}_N^d$.
Pick random $\{\alpha_i, r_i, z_i \in \mathbb{Z}_N\}_{i \in [m]}$, $\{c_j \in \mathbb{Z}_N\}_{j \in [m]}$. The public parameter is

$$\text{PP} = ((N, \mathbb{G}, \mathbb{G}_T, e), g, \mathbf{h} = g^\beta, X_3, \{E_i = e(g, g)^{\alpha_i}, G_i = g^{r_i}, Z_i = g^{z_i}\}_{i \in [m]}, \{H_j = g^{c_j}\}_{j \in [m]}).$$

The master secret key is $\text{MSK} = (\alpha_1, \dots, \alpha_m, r_1, \dots, r_m, c_1, \dots, c_m)$.

A counter $ctr = 0$ is implicitly included in MSK .

$\text{KeyGen}_A(\text{PP}, \text{MSK}, X) \rightarrow \text{SK}_{(i,j),X}$. Upon input a key tag X , run $(\phi = (\phi_0, \phi_1, \dots, \phi_{d_k}), d_\delta) \leftarrow \text{KeyParam}(X, N)$. Pick random $\delta = (\delta_1, \dots, \delta_{d_\delta}) \in \mathbb{Z}_N^{d_\delta}$, $\mathbf{R} = (R_0, \dots, R_{d_k}) \in \mathbb{G}_{p_3}^{d_k+1}$.
Pick random $R'_0 \in \mathbb{G}_{p_3}$. Set $ctr = ctr + 1$ and then compute the corresponding index in the form of (i, j) where $1 \leq i, j \leq m$ and $(i - 1) * m + j = ctr$. Output a secret key $\text{SK}_{(i,j),X}$ as

$$\text{SK}_{(i,j),X} = ((i, j), X, \mathbf{K} = g^{\phi(r_i c_j + \alpha_i, \beta, \delta)} \cdot \mathbf{R}, K'_0 = Z_i^{\delta_1} R'_0),$$

Note the requirements stated in $\text{KeyGen}_{\text{NT}}$, we have

$$\begin{aligned} \text{SK}_{(i,j),X} = ((i, j), X, (K_0 = g^{r_i c_j + \alpha_i} g^{\beta_1 \delta_1} \prod_{\bar{a}=2}^{d_0} g^{\beta_{\bar{a}} \phi_{\bar{a}}(\beta, \delta)} R_0, K_1 = g^{\delta_1} R_1, \\ K_2 = g^{\phi_2(\beta, \delta)} \cdot R_2, \dots, K_{d_k} = g^{\phi_{d_k}(\beta, \delta)} \cdot R_{d_k}), \\ K'_0 = Z_i^{\delta_1} R'_0). \end{aligned}$$

$\text{Encrypt}_A(\text{PP}, M, Y, (\bar{i}, \bar{j})) \rightarrow CT_Y$.

1. Upon input a ciphertext tag Y , run $(\psi = (\psi_1, \dots, \psi_{d_c}), d_\pi) \leftarrow \text{CiperParam}(Y, N)$. Pick random $\pi =$

$(\pi, \pi_1, \dots, \pi_{d_\pi}) \in \mathbb{Z}_N^{d_\pi+1}$. Set $\mathbf{P} = g^{\psi(\beta, \pi)}$.

Note that \mathbf{P} can be computed from g^β and π since $\psi(\beta, \pi)$ contains only linear combinations of monomials $\pi, \pi_i, \pi \beta_j, \pi_i \beta_j$.

2. Pick random

$$\kappa, \tau, s_1, \dots, s_m, t_1, \dots, t_m \in \mathbb{Z}_N,$$

$$\mathbf{v}_c, \mathbf{w}_1, \dots, \mathbf{w}_m \in \mathbb{Z}_N^3.$$

Pick random $r_x, r_y, r_z \in \mathbb{Z}_N$, and set $\chi_1 = (r_x, 0, r_z)$, $\chi_2 = (0, r_y, r_z)$, $\chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$.
Pick random

$$\begin{aligned} \mathbf{v}_i &\in \mathbb{Z}_N^3 \quad \forall i \in \{1, \dots, \bar{i}\}, \\ \mathbf{v}_i &\in \text{span}\{\chi_1, \chi_2\} \quad \forall i \in \{\bar{i} + 1, \dots, m\}. \end{aligned}$$

For each row $i \in [m]$:

– if $i < \bar{i}$: randomly choose $\hat{s}_i \in \mathbb{Z}_p$, and set

$$\begin{aligned} \mathbf{R}_i &= g^{\mathbf{v}_i}, \quad \mathbf{R}'_i = g^{\kappa \mathbf{v}_i}, \quad Q_i = g^{s_i}, \quad Q_{i,1} = (g^{\beta_1})^{s_i} Z_i^{t_i} (g^{\beta_1})^\pi, \\ Q_{i,2} &= (g^{\beta_2})^{s_i}, \dots, Q_{i,d_0} = (g^{\beta_{d_0}})^{s_i}, \\ Q'_i &= g^{t_i}, \quad T_i = E_i^{\hat{s}_i}. \end{aligned}$$

– if $i \geq \bar{i}$: set

$$\begin{aligned} \mathbf{R}_i &= C_i^{s_i \mathbf{v}_i}, \quad \mathbf{R}'_i = C_i^{\kappa s_i \mathbf{v}_i}, \quad Q_i = g^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}, \quad Q_{i,1} = (g^{\beta_1})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)} Z_i^{t_i} (g^{\beta_1})^\pi, \\ Q_{i,2} &= (g^{\beta_2})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}, \dots, Q_{i,d_0} = (g^{\beta_{d_0}})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}, \\ Q'_i &= g^{t_i}, \quad T_i = M \cdot E_i^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}. \end{aligned}$$

For each column $j \in [m]$:

– if $j < \bar{j}$: randomly choose $\mu_j \in \mathbb{Z}_N$, and set $\mathbf{C}_j = H_j^{\tau(\mathbf{v}_c + \mu_j \chi_3)} \cdot g^{\kappa \mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

– if $j \geq \bar{j}$: set $\mathbf{C}_j = H_j^{\tau \mathbf{v}_c} \cdot g^{\kappa \mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

3. Output the ciphertext CT_Y as $CT_Y = \langle Y, \mathbf{P}, (\mathbf{R}_i, \mathbf{R}'_i, Q_i, \{Q_{i,\bar{d}}\}_{\bar{d}=1}^{d_0}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$.

Decrypt_A(PP, CT_Y , $\text{SK}_{(i,j),X}$) $\rightarrow M$ or \perp . Parse CT_Y to $CT_Y = \langle Y, \mathbf{P}, (\mathbf{R}_i, \mathbf{R}'_i, Q_i, \{Q_{i,\bar{d}}\}_{\bar{d}=1}^{d_0}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$ and $\text{SK}_{(i,j),X}$ to $\text{SK}_{(i,j),X} = ((i, j), X, \mathbf{K} = (K_0, \dots, K_{d_k}), K'_0)$. Obtain Y, X from CT_Y , $\text{SK}_{(i,j),X}$. Suppose $\Gamma(X, Y) = 1$ (if $\Gamma(X, Y) \neq 1$, output \perp).

1. Run $\mathbf{E}_1 \leftarrow \text{Pair}_1(X, Y, N)$. Compute $D_P \leftarrow e(\mathbf{K}^{\mathbf{E}_1}, \mathbf{P})$.
2. Compute

$$D_I \leftarrow \frac{e(K_0, Q_i) \cdot e(K'_0, Q'_i)}{e(K_1, Q_{i,1}) \cdot \prod_{\bar{d}=2}^{d_0} e(K_{\bar{d}}, Q_{i,\bar{d}})} \cdot \frac{e_3(\mathbf{R}'_i, \mathbf{C}'_j)}{e_3(\mathbf{R}_i, \mathbf{C}_j)}.$$

3. Computes $M \leftarrow T_i / (D_P \cdot D_I)$ as the output message. Suppose that the ciphertext is generated from message M' and encryption index (\bar{i}, \bar{j}) , it can be verified that only when $(i > \bar{i})$ or $(i = \bar{i} \wedge j \geq \bar{j})$, $M = M'$. This is because for $i > \bar{i}$, we have $(\mathbf{v}_i \cdot \chi_3) = 0$ (since $\mathbf{v}_i \in \text{span}\{\chi_1, \chi_2\}$), and for $i = \bar{i}$, we have that $(\mathbf{v}_i \cdot \chi_3) \neq 0$ happens with overwhelming probability (since \mathbf{v}_i is randomly chosen from \mathbb{Z}_N^3). The **correctness** is referred to Appendix A.

4.4 Augmented ABE Security

Let $\Sigma_{\text{NT}} = (\text{Setup}_{\text{NT}}, \text{KeyGen}_{\text{NT}}, \text{Encrypt}_{\text{NT}}, \text{Decrypt}_{\text{NT}})$ be a non-traceable ABE scheme satisfying the template in Sec. 4.2, and $\Sigma_A = (\text{Setup}_A, \text{KeyGen}_A, \text{Encrypt}_A, \text{Decrypt}_A)$ be an Augmented ABE scheme derived from Σ_{NT} as shown in Sec. 4.3. As shown in Fig. 2, Theorem 3, Theorem 4, and Theorem 5 state that the AugABE proposed above is Type-I message-hiding, Type-II message-hiding, and selectively index-hiding, respectively. Below we prove Theorem 3 and Theorem 4 in a framework manner. For the Theorem 5, we prove it in a framework manner partially, namely, we prove Claim 1 in a framework manner, while proving Lemma 1 case by case for the concrete underlying conventional (non-traceable) ABE schemes, and the proof of Claim 2 will be identical to that of Lemma 1.

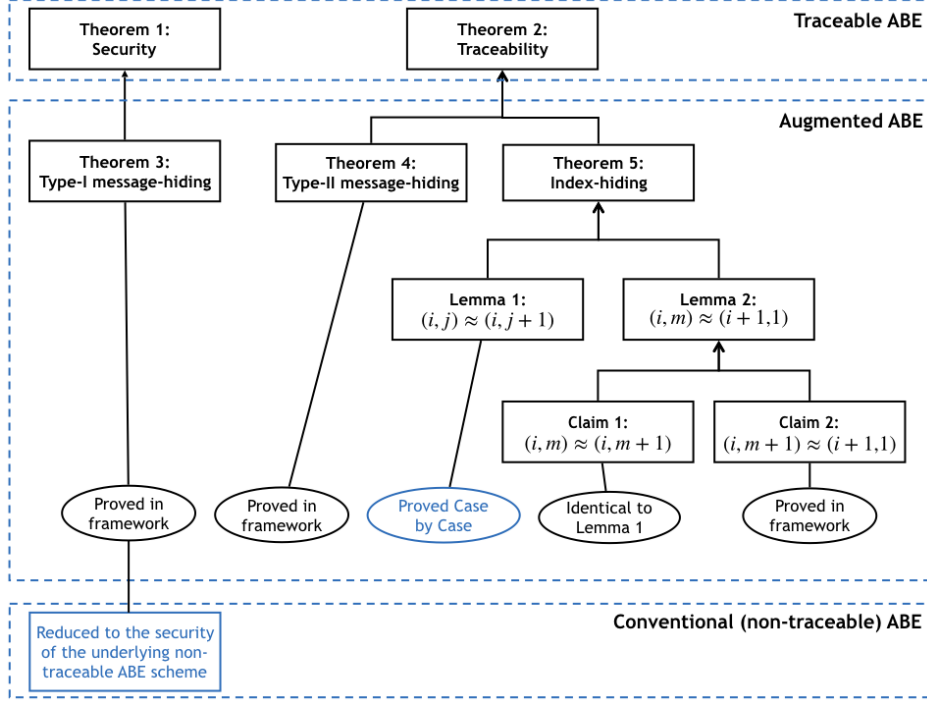


Fig. 2. Outline for Security Analysis

Theorem 3. *If Σ_{NT} is secure (resp. selectively secure), then Σ_{A} is Type-I message-hiding (resp. selectively Type-I message-hiding).*

Proof. Suppose there is a PPT adversary \mathcal{A} that can break Σ_{A} in $\text{Game}_{\text{MH}_1}^{\text{A}}$ with non-negligible advantage $\text{MH}_1^{\text{A}}\text{Adv}_{\mathcal{A}}$, we construct a PPT algorithm \mathcal{B} to break Σ_{NT} with advantage $\text{Adv}_{\mathcal{B}}\Sigma_{\text{NT}}$, which equals to $\text{MH}_1^{\text{A}}\text{Adv}_{\mathcal{A}}$.

Setup. \mathcal{B} receives the public parameter $\text{PP}^{\text{NT}} = ((N, \mathbb{G}, \mathbb{G}_T, e), g, g^{\beta}, X_3, E = e(g, g)^{\alpha})$ from the challenger, where $g \in \mathbb{G}_{p_1}$ and $X_3 \in \mathbb{G}_{p_3}$ are the generators of subgroups \mathbb{G}_{p_1} and \mathbb{G}_{p_3} respectively, $\beta = (\beta_1, \dots, \beta_d) \in \mathbb{Z}_N^d$ (for $(d, d_0) \leftarrow \text{SysParam}(T)$) and $\alpha \in \mathbb{Z}_N$ are randomly chosen. \mathcal{B} picks random $\{\alpha'_i, r_i, z_i \in \mathbb{Z}_N\}_{i \in [m]}$, $\{c_j \in \mathbb{Z}_N\}_{j \in [m]}$, then gives \mathcal{A} the public parameter PP :

$$\text{PP} = ((N, \mathbb{G}, \mathbb{G}_T, e), g, g^{\beta}, X_3, \{E_i = E \cdot e(g, g)^{\alpha'_i}, G_i = g^{r_i}, Z_i = g^{z_i}\}_{i \in [m]}, \{H_j = g^{c_j}\}_{j \in [m]}).$$

Note that \mathcal{B} implicitly chooses $\{\alpha_i \in \mathbb{Z}_N\}_{i \in [m]}$ such that $\{\alpha + \alpha'_i \equiv \alpha_i \pmod{p_1}\}_{i \in [m]}$.

Phase 1. To respond to \mathcal{A} 's query for $((i, j), X_{(i,j)})$, \mathcal{B} submits $X_{(i,j)}$ to the challenger, and receives a secret key

$$\text{SK}_{X_{(i,j)}}^{\text{NT}} = (X_{(i,j)}, (\tilde{K}_0 = g^{\alpha} g^{\beta_1 \delta_1} \prod_{\tilde{a}=2}^{d_0} g^{\beta_{\tilde{a}} \phi_{\tilde{a}}(\beta, \delta)} R_0, \tilde{K}_1 = g^{\delta_1} \cdot R_1, \tilde{K}_2 = g^{\phi_2(\beta, \delta)} \cdot R_2, \dots, \tilde{K}_{d_k} = g^{\phi_{d_k}(\beta, \delta)} \cdot R_{d_k})),$$

where $(\phi = (\phi_0, \phi_1, \dots, \phi_{d_k}), d_{\delta}) \leftarrow \text{KeyParam}(X_{(i,j)}, N)$, $\delta = (\delta_1, \dots, \delta_{d_{\delta}}) \in \mathbb{Z}_N^{d_{\delta}}$, $\mathbf{R} = (R_0, \dots, R_{d_k}) \in \mathbb{G}_{p_3}^{d_k+1}$.

\mathcal{B} picks random $\tilde{R}'_0 \in \mathbb{G}_{p_3}$, then responses \mathcal{A} with a secret key $\text{SK}_{(i,j),X_{(i,j)}}$ as

$$\begin{aligned} \text{SK}_{(i,j),X_{(i,j)}} &= ((i,j), X_{(i,j)}, (K_0 = \tilde{K}_0 \cdot g^{r_i c_j + \alpha'_i}, K_1 = \tilde{K}_1, \\ &K_2 = \tilde{K}_2, \dots, K_{d_k} = \tilde{K}_{d_k}, \\ &K'_0 = \tilde{K}_1^{z_i} \tilde{R}'_0)). \end{aligned}$$

Note that such a secret key has the same distribution as the secret key in the real Augmented ABE scheme, i.e. $\text{SK}_{(i,j),X_{(i,j)}} = ((i,j), X_{(i,j)}, \mathbf{K} = g^{\phi(r_i c_j + \alpha_i, \beta, \delta)} \cdot \mathbf{R}, K'_0 = Z_i^{\sigma_{i,j}} R'_0)$, where $R'_0 = R_1^{z_i} \tilde{R}'_0$.

Challenge. \mathcal{A} submits to \mathcal{B} a ciphertext tag Y^* and two equal length messages M_0, M_1 . \mathcal{B} submits (Y^*, M_0, M_1) to the challenger, and receives the challenge ciphertext in the form of $CT^{\text{NT}} =$

$$\langle Y^*, \tilde{\mathbf{P}} = g^{\psi(\beta, \tilde{\pi})}, \tilde{C} = M \cdot e(g, g)^{\alpha \tilde{\pi}} \rangle,$$

where $(\psi = (\psi_1, \dots, \psi_{d_c}), d_\pi) \leftarrow \text{CiperParam}(Y^*, N)$, $\tilde{\pi} = (\tilde{\pi}, \tilde{\pi}_1, \dots, \tilde{\pi}_{d_\pi}) \in \mathbb{Z}_N^{d_\pi+1}$.

Note that $\psi(\beta, \tilde{\pi})$ contains only linear combinations of monomials $\tilde{\pi}, \tilde{\pi}_i, \tilde{\pi} \beta_j, \tilde{\pi}_i \beta_j$, and the first d_0 components of $\tilde{\mathbf{P}}$ are $\tilde{P}_1 = g^{\tilde{\pi}}, \tilde{P}_2 = g^{\beta_2 \tilde{\pi}}, \dots, \tilde{P}_{d_0} = g^{\beta_{d_0} \tilde{\pi}}$. \mathcal{B} creates a challenge ciphertext for $(\bar{i}, \bar{j}) = (1, 1)$ as follows:

1. \mathcal{B} picks random $\pi' = (\pi', \pi'_1, \dots, \pi'_{d_\pi}) \in \mathbb{Z}_N^{d_\pi+1}$, then sets $\mathbf{P} = g^{\psi(\beta, \pi')} \cdot (\tilde{\mathbf{P}})^{-1}$.

Here $(\tilde{\mathbf{P}})^{-1}$ means $(\tilde{P}_1^{-1}, \dots, \tilde{P}_{d_c}^{-1})$. Note that $\psi(\beta, \tilde{\pi})$ contains only linear combinations of monomials $\tilde{\pi}, \tilde{\pi}_i, \tilde{\pi} \beta_j, \tilde{\pi}_i \beta_j$, we have $(\tilde{\mathbf{P}})^{-1} = g^{\psi(\beta, -\tilde{\pi})}$. Note that $\psi(\beta, \pi')$ contains only linear combinations of monomials $\pi', \pi'_i, \pi' \beta_j, \pi'_i \beta_j$, we have that $\mathbf{P} = g^{\psi(\beta, \pi' - \tilde{\pi})}$.

2. \mathcal{B} picks random

$$\kappa, \tau, s'_1, \dots, s'_m, t_1, \dots, t_m \in \mathbb{Z}_N, \mathbf{v}_c, \mathbf{w}_1, \dots, \mathbf{w}_m \in \mathbb{Z}_N^3.$$

\mathcal{B} picks random $r_x, r_y, r_z \in \mathbb{Z}_N$, and sets $\chi_1 = (r_x, 0, r_z), \chi_2 = (0, r_y, r_z), \chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$. \mathcal{B} picks random $\mathbf{v}_1 \in \mathbb{Z}_N^3$, $\mathbf{v}_i \in \text{span}\{\chi_1, \chi_2\} \forall i \in \{2, \dots, m\}$.

For each row $i \in [m]$: note that $i \geq \bar{i}$ (since $\bar{i} = 1$), \mathcal{B} sets

$$\begin{aligned} \mathbf{R}_i &= G_i^{s'_i \mathbf{v}_i} \cdot \tilde{P}_1^{\frac{r_i}{\tau(\mathbf{v}_i \cdot \mathbf{v}_c)} \mathbf{v}_i}, \quad \mathbf{R}'_i = G_i^{\kappa s'_i \mathbf{v}_i} \cdot \tilde{P}_1^{\frac{r_i \kappa}{\tau(\mathbf{v}_i \cdot \mathbf{v}_c)} \mathbf{v}_i}, \\ Q_i &= g^{\tau s'_i (\mathbf{v}_i \cdot \mathbf{v}_c)} \tilde{P}_1, \quad Q_{i,1} = (g^{\beta_1})^{\tau s'_i (\mathbf{v}_i \cdot \mathbf{v}_c)} Z_i^{t_i} (g^{\beta_1})^{\pi'}, \\ Q_{i,2} &= (g^{\beta_2})^{\tau s'_i (\mathbf{v}_i \cdot \mathbf{v}_c)} \cdot \tilde{P}_2, \quad \dots, \quad Q_{i,d_0} = (g^{\beta_{d_0}})^{\tau s'_i (\mathbf{v}_i \cdot \mathbf{v}_c)} \cdot \tilde{P}_{d_0}, \\ Q'_i &= g^{t_i}, \quad T_i = \tilde{C} \cdot e(g^{\alpha'_i}, \tilde{P}_1) \cdot E_i^{\tau s'_i (\mathbf{v}_i \cdot \mathbf{v}_c)}. \end{aligned}$$

For each column $j \in [m]$: note that $j \geq \bar{j}$ (since $\bar{j} = 1$), \mathcal{B} sets

$$\mathbf{C}_j = H_j^{\tau \mathbf{v}_c} \cdot g^{\kappa \mathbf{w}_j}, \quad \mathbf{C}'_j = g^{\mathbf{w}_j}.$$

3. \mathcal{B} outputs the ciphertext CT_{Y^*} as $CT_{Y^*} = \langle Y^*, \mathbf{P}, (\mathbf{R}_i, \mathbf{R}'_i, Q_i, \{Q_{i,\bar{d}}\}_{\bar{d}=1}^{d_0}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$. Note that this CT_{Y^*} is a well-formed ciphertext for ciphertext tag Y^* and encryption index $(\bar{i}, \bar{j}) = (1, 1)$, with implicitly setting $s_1, \dots, s_m \in \mathbb{Z}_N$ and $\pi = (\pi, \pi_1, \dots, \pi_{d_\pi}) \in \mathbb{Z}_N^{d_\pi+1}$ by

$$s'_i + \frac{\tilde{\pi}}{\tau(\mathbf{v}_i \cdot \mathbf{v}_c)} \equiv s_i \pmod{p_1} \quad \forall i \in \{1, \dots, m\}, \quad \pi' - \tilde{\pi} \equiv \pi \pmod{p_1}.$$

Phase 2. Same with Phase 1.

Guess. \mathcal{A} gives \mathcal{B} a b' . \mathcal{B} gives b' to the challenger.

Note that the distributions of the public parameter, secret keys and challenge ciphertext that \mathcal{B} gives \mathcal{A} are same as the real scheme, we have $\text{Adv}_{\mathcal{B}} \Sigma_{\text{NT}} = \text{MH}_1^{\text{A}} \text{Adv}_{\mathcal{A}}$.

Theorem 4. Σ_A is Type-II message-hiding.

Proof. The argument for message-hiding in $\text{Game}_{\text{MH}_2}^A$ is straightforward since an encryption to index $\mathcal{K} + 1$ (i.e. $(m + 1, 1)$) contains no information about the message. The simulator simply runs Setup_A and KeyGen_A and encrypts M_b under the challenge ciphertext tag Y^* and index $(m + 1, 1)$. Since for all $i = 1$ to m , $T_i = E_i^{\hat{s}_i}$ contains no information about the message, the bit b is perfectly hidden and $\text{MH}^A \text{Adv}_{\mathcal{A}} = 0$.

Now we investigate the Theorem 5 where we prove the index-hiding property. As shown in Fig. 2, Theorem 5 follows Lemma 1 and Lemma 2, and we need to prove Lemma 1 case by case. Here we use ‘Assumption X’ to represent the assumption(s) that Lemma 1 is based on, and we will present the concrete assumptions when we prove Lemma 1 concretely.

Theorem 5. Suppose that the Assumption X, the D3DH, and the DLIN Assumption hold.⁶ Then no PPT adversary can selectively win $\text{Game}_{\text{IH}}^A$ with non-negligible advantage.

Proof. It follows Lemma 1 and Lemma 2 below.

Lemma 1. If the Assumption X hold, then for $\bar{j} < m$, no PPT adversary can selectively distinguish between an encryption to (\bar{i}, \bar{j}) and $(\bar{i}, \bar{j} + 1)$ in $\text{Game}_{\text{IH}}^A$ with non-negligible advantage.

Proof. In $\text{Game}_{\text{IH}}^A$ with index (\bar{i}, \bar{j}) , let Y^* be the challenge ciphertext tag, the restriction is that the adversary \mathcal{A} does not query a secret key for (index, key tag) pair $((i, j), X_{(i,j)})$ such that $((i, j) = (\bar{i}, \bar{j})) \wedge (\Gamma(X_{(i,j)}, Y^*) = 1)$. Under this restriction, there are two ways for \mathcal{A} to take:

Case I: In Key Query phase, \mathcal{A} does not query a secret key with index (\bar{i}, \bar{j}) .

Case II: In Key Query phase, \mathcal{A} queries a secret key with index (\bar{i}, \bar{j}) . Let $X_{(\bar{i}, \bar{j})}$ be the corresponding key tag. The restriction requires that $\Gamma(X_{(\bar{i}, \bar{j})}, Y^*) \neq 1$.

Case I is easy to handle as the adversary does not query a secret key with the challenge index (\bar{i}, \bar{j}) . **Case II** captures the index-hiding requirement in that even if a user has a key with index (\bar{i}, \bar{j}) he cannot distinguish between an encryption to $(Y^*, (\bar{i}, \bar{j}))$ and $(Y^*, (\bar{i}, \bar{j} + 1))$, if the corresponding key tag does not satisfies $\Gamma(X_{(\bar{i}, \bar{j})}, Y^*) = 1$. This is the most challenging part of achieving strong traceability. Actually, this is the only part where we cannot handle in a framework manner, and we have to prove this lemma for different schemes case by case.

Lemma 2. If the Assumption X, the D3DH, and the DLIN Assumption hold, then for $1 \leq \bar{i} \leq m$, no PPT adversary can selectively distinguish between an encryption to (\bar{i}, m) and $(\bar{i} + 1, 1)$ in $\text{Game}_{\text{IH}}^A$ with non-negligible advantage.

Proof. Similar to the proof of Lemma 6.3 in [11], to prove this lemma we define the following hybrid experiment: H_1 : encrypt to $(\bar{i}, \bar{j} = m)$; H_2 : encrypt to $(\bar{i}, \bar{j} = m + 1)$; and H_3 : encrypt to $(\bar{i} + 1, 1)$. This lemma follows Claim 1 and Claim 2 below.

Claim 1. If the Assumption X holds, then no PPT adversary can selectively distinguish between experiment H_1 and H_2 with non-negligible advantage.

Proof. The proof is identical to that for Lemma 1.

Claim 2. If the D3DH and the DLIN hold, then no PPT adversary can distinguish between experiment H_2 and H_3 with non-negligible advantage.

⁶ Here D3DH and DLIN are the abbreviation of the widely accepted Decision 3-Party Diffie Hellman Assumption and Decisional Linear Assumption, respectively. we refer to [11] for the details of these two assumptions.

Proof. The indistinguishability of H_2 and H_3 can be proved using a proof similar to that of Lemma 6.3 in [11], which was used to prove the indistinguishability of similar hybrid experiments for their Augmented Broadcast Encryption (AugBE) scheme. For simplicity, we prove Claim 2 by a reduction from our AugBE scheme to the AugBE scheme in [11].

In particular, Garg et al. [11, Sec. 5.1] proposed an AugBE scheme $\Sigma_{\text{AugBE}} = (\text{Setup}_{\text{AugBE}}, \text{Encrypt}_{\text{AugBE}}, \text{Decrypt}_{\text{AugBE}})$ and proved Σ_{AugBE} is index-hiding. In the proof of index-hiding for Σ_{AugBE} in [11, Lemma 6.3], two hybrid experiments were defined and proven indistinguishable via a sequence of hybrid sub-experiments.

- H_2^{AugBE} : Encrypt to $(\bar{i}, m+1)$, (i.e. H_2 in [11])
- H_3^{AugBE} : Encrypt to $(\bar{i}+1, 1)$, (i.e. H_5 in [11])

By following [11, Lemma 6.3], *if the D3DH and the DLIN hold, no PPT adversary can distinguish between H_2^{AugBE} and H_3^{AugBE} for Σ_{AugBE} with non-negligible advantage.* Suppose there is a PPT adversary \mathcal{A} that can distinguish between H_2 and H_3 for our AugBE scheme with non-negligible advantage. We can construct a PPT algorithm \mathcal{B} to distinguish between H_2^{AugBE} and H_3^{AugBE} for Σ_{AugBE} with non-negligible advantage.

The game of \mathcal{B} distinguishing between H_2^{AugBE} and H_3^{AugBE} is played in the subgroup \mathbb{G}_{p_1} of order p_1 in a composite order group \mathbb{G}_N of order $N = p_1 p_2 p_3$. \mathcal{B} is given the values of p_1 , p_2 and p_3 , and can choose for itself everything in the subgroup \mathbb{G}_{p_3} .

Setup. The challenger gives \mathcal{B} the public key PK^{AugBE} , and due to $(\bar{i}, m+1) \notin \{(i, j) | 1 \leq i, j \leq m\}$, the challenger gives \mathcal{B} all private keys in the set $\{\text{SK}_{(i, j)}^{\text{AugBE}} | 1 \leq i, j \leq m\}$:⁷

$$\begin{aligned} \text{PK}^{\text{AugBE}} &= (g, \{E_i = e(g, g)^{\alpha_i}, G_i = g^{r_i}\}_{i \in [m]}, \{H_j = g^{c_j}, f_j\}_{j \in [m]}), \\ \text{SK}_{(i, j)}^{\text{AugBE}} &= (\tilde{K}_{i, j}, \tilde{K}'_{i, j}, \{\tilde{K}_{i, j, j'}\}_{j' \in [m] \setminus \{j\}}) = (g^{\alpha_i} g^{r_i c_j} f_j^{\sigma_{i, j}}, g^{\sigma_{i, j}}, \{f_{j'}^{\sigma_{i, j}}\}_{j' \in [m] \setminus \{j\}}), \end{aligned}$$

where $g, f_1, \dots, f_m \in \mathbb{G}_{p_1}$, $\{\alpha_i, r_i \in \mathbb{Z}_{p_1}\}_{i \in [m]}$, $\{c_j \in \mathbb{Z}_{p_1}\}_{j \in [m]}$, $\sigma_{i, j} (1 \leq i, j \leq m) \in \mathbb{Z}_{p_1}$ are randomly chosen.

\mathcal{B} picks random $X_3 \in \mathbb{G}_{p_3}$, runs $(d, d_0) \leftarrow \text{SysParam}(\Gamma)$, and picks random $\beta_2, \dots, \beta_d \in \mathbb{Z}_N$. \mathcal{B} picks random $z_1, \dots, z_m \in \mathbb{Z}_N$. Setting $g^\beta = (\prod_{j=1}^m f_j, g^{\beta_2}, \dots, g^{\beta_d})$, \mathcal{B} gives \mathcal{A} the following public parameter PP:

$$\text{PP} = ((N, \mathbb{G}, \mathbb{G}_T, e), g, g^\beta, X_3, \{E_i, G_i, Z_i = g^{z_i}\}_{i \in [m]}, \{H_j\}_{j \in [m]}).$$

Note that \mathcal{B} implicitly picks $\beta_1 \in \mathbb{Z}_N$ such that $g^{\beta_1} = \prod_{j=1}^m f_j$.

Key Query. To respond to \mathcal{A} 's query for $((i, j), X_{(i, j)})$, \mathcal{B} runs $(\phi = (\phi_0, \phi_1, \dots, \phi_{d_k}), d_\delta) \leftarrow \text{KeyParam}(X_{(i, j)}, N)$, picks random $\delta_2, \dots, \delta_{d_\delta} \in \mathbb{Z}_N$, $\mathbf{R} = (R_0, \dots, R_{d_k}) \in \mathbb{G}_{p_3}^{d_k+1}$, and $R'_0 \in \mathbb{G}_{p_3}$. \mathcal{B} outputs a secret key $\text{SK}_{(i, j), X_{(i, j)}}$ as

$$\begin{aligned} \text{SK}_{(i, j), X_{(i, j)}} &= ((i, j), X_{(i, j)}, (K_0 = \tilde{K}_{i, j} \cdot (\prod_{\tilde{j} \in [m] \setminus \{j\}} \tilde{K}_{i, j, \tilde{j}}) \cdot \prod_{\tilde{d}=2}^{d_0} g^{\beta_{\tilde{d}} \phi_{\tilde{d}}(\beta, \delta)} R_0, K_1 = \tilde{K}'_{i, j} \cdot R_1, \\ &K_2 = g^{\phi_2(\beta, \delta)} \cdot R_2, \dots, K_{d_k} = g^{\phi_{d_k}(\beta, \delta)} \cdot R_{d_k}), \\ &K'_0 = (\tilde{K}'_{i, j})^{z_i} \cdot R'_0). \end{aligned}$$

Note that \mathcal{B} implicitly picks $\delta_1 \in \mathbb{Z}_N$ such that $\delta_1 \equiv \sigma_{i, j} \pmod{p_1}$. Note that for any variables $\alpha \in \mathbb{Z}_N$, $\beta = (\beta_1, \dots, \beta_d) \in \mathbb{Z}_N^d$, $\delta = (\delta_1, \dots, \delta_{d_\delta}) \in \mathbb{Z}_N^{d_\delta}$, each $\phi_z(\beta, \delta) (2 \leq z \leq d_k)$ contains only linear combinations of monomials $\delta_i, \delta_i \beta_j$ and does not contain $\beta_1 \delta_1$. Note that \mathcal{B} knows the values of $g^{\delta_1} = g^{\sigma_{i, j}} = \tilde{K}'_{i, j}$, $\delta_2, \dots, \delta_{d_\delta}$ and $g^{\beta_1} = \prod_{j=1}^m f_j, \beta_2, \dots, \beta_d$, \mathcal{B} can calculate the values of $g^{\phi_2(\beta, \delta)}, \dots, g^{\phi_{d_k}(\beta, \delta)}$, and then the values of $g^{\beta_{\tilde{d}} \phi_{\tilde{d}}(\beta, \delta)}$ for $\tilde{d} \in \{2, \dots, d_0\}$. Thus, we know \mathcal{B} can produce the above secret key $\text{SK}_{(i, j), X_{(i, j)}}$.

Challenge. \mathcal{A} submits a message M and a ciphertext tag Y^* . Note that $(\bar{i}, m+1) \notin \{(i, j) | 1 \leq i, j \leq m\}$, \mathcal{B} sets the receiver set to be $J = \{(i, j) | 1 \leq i, j \leq m\}$ and submits (M, J) to the challenger. The challenger gives \mathcal{B} the challenge ciphertext $CT^{\text{AugBE}} = \langle (\tilde{\mathbf{R}}_i, \tilde{\mathbf{R}}'_i, \tilde{Q}_i, \tilde{Q}'_i, \tilde{T}_i)_{i=1}^m, (\tilde{\mathbf{C}}_j, \tilde{\mathbf{C}}'_j)_{j=1}^m, J \rangle$, which is encrypted to $(i^*, j^*) \in \{(\bar{i}, m+1), (\bar{i}+1, 1)\}$ and in the form of

⁷ Note that we slightly changed the variable names in the underlying AugBE scheme to better suit our proof.

1. For each $i \in [m]$:
 - if $i < i^*$: $\tilde{\mathbf{R}}_i = g^{\mathbf{v}_i}$, $\tilde{\mathbf{R}}'_i = g^{\kappa \mathbf{v}_i}$, $\tilde{Q}_i = g^{s_i}$, $\tilde{Q}'_i = (\prod_{j \in J_i} f_j)^{s_i}$, $\tilde{T}_i = E_i^{\hat{s}_i}$.
 - if $i \geq i^*$: $\tilde{\mathbf{R}}_i = G_i^{s_i \mathbf{v}_i}$, $\tilde{\mathbf{R}}'_i = G_i^{\kappa s_i \mathbf{v}_i}$, $\tilde{Q}_i = g^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}$, $\tilde{Q}'_i = (\prod_{j \in J_i} f_j)^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}$, $\tilde{T}_i = M \cdot E_i^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}$.
2. For each $j \in [m]$:
 - if $j < j^*$: $\tilde{\mathbf{C}}_j = H_j^{\tau (\mathbf{v}_c + \mu_j \chi_3)} \cdot g^{\kappa \mathbf{w}_j}$, $\tilde{\mathbf{C}}'_j = g^{\mathbf{w}_j}$.
 - if $j \geq j^*$: $\tilde{\mathbf{C}}_j = H_j^{\tau \mathbf{v}_c} \cdot g^{\kappa \mathbf{w}_j}$, $\tilde{\mathbf{C}}'_j = g^{\mathbf{w}_j}$.

where $\kappa, \tau, s_i (1 \leq i \leq m), \hat{s}_i (1 \leq i < i^*), \mu_j (1 \leq j < j^*) \in \mathbb{Z}_{p_1}$, $\mathbf{v}_c, \mathbf{w}_j (1 \leq j \leq m), \mathbf{v}_i (1 \leq i \leq i^*) \in \mathbb{Z}_{p_1}^3$, and $\mathbf{v}_i (i > i^*) \in \text{span}\{\chi_1, \chi_2\}$ are randomly chosen (where $\chi_1 = (r_x, 0, r_z), \chi_2 = (0, r_y, r_z), \chi_3 = (-r_y r_z, -r_x r_z, r_x r_y)$ are for randomly chosen $r_x, r_y, r_z \in \mathbb{Z}_{p_1}$), and $J_i = \{j | (i, j) \in J\}$.

Note that $J = \{(i, j) | 1 \leq i, j \leq m\}$, we have $J_i = \{1, \dots, m\}$ for all $1 \leq i \leq m$, and then $\tilde{Q}'_i = (\prod_{j \in J_i} f_j)^{s_i} = (g^{\beta_1})^{s_i}$ for $i < i^*$ and $\tilde{Q}'_i = (\prod_{j \in J_i} f_j)^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)} = (g^{\beta_1})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}$ for $i \geq i^*$.

\mathcal{B} runs $(\psi = (\psi_1, \dots, \psi_{d_c}), d_\pi) \leftarrow \text{CiperParam}(Y^*, N)$ and picks random $\pi = (\pi, \pi_1, \dots, \pi_{d_\pi}) \in \mathbb{Z}_N^{d_\pi+1}$, then sets

$$\mathbf{P} = g^{\psi(\beta, \pi)}.$$

Note that \mathbf{P} can be computed from g^β and π since $\psi(\beta, \pi)$ contains only linear combinations of monomials $\pi, \pi_i, \pi \beta_j, \pi_i \beta_j$.

\mathcal{B} picks random $t_1, \dots, t_m \in \mathbb{Z}_N$. \mathcal{B} outputs a challenge ciphertext as $CT_{Y^*} = \langle Y^*, \mathbf{P}, (\mathbf{R}_i, \mathbf{R}'_i, Q_i, \{Q_{i,d}\}_{d=1}^{d_0}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$, where

1. For each $i \in [m]$: $\mathbf{R}_i = \tilde{\mathbf{R}}_i$, $\mathbf{R}'_i = \tilde{\mathbf{R}}'_i$, $Q_i = \tilde{Q}_i$, $Q_{i,1} = \tilde{Q}'_i \cdot Z_i^{t_i} (g^{\beta_1})^\pi$, $Q_{i,2} = Q_i^{\beta_2}, \dots, Q_{i,d_0} = Q_i^{\beta_{d_0}}$, $Q'_i = g^{t_i}$, $T_i = \tilde{T}_i$.
2. For each $j \in [m]$: $\mathbf{C}_j = \tilde{\mathbf{C}}_j$, $\mathbf{C}'_j = \tilde{\mathbf{C}}'_j$.

Guess. \mathcal{A} outputs a guess $b' \in \{0, 1\}$ to \mathcal{B} , then \mathcal{B} outputs this b' to the challenger as its answer to distinguish between H_2^{AugBE} and H_3^{AugBE} for scheme Σ_{AugBE} .

As the exponents are applied only to the elements in the subgroup \mathbb{G}_{p_1} , from the view of \mathcal{A} , the distributions of the public parameter, secret keys and challenge ciphertext that \mathcal{B} gives \mathcal{A} are same as the real scheme. Thus \mathcal{B} 's advantage in distinguishing between H_2^{AugBE} and H_3^{AugBE} for scheme Σ_{AugBE} will be exactly equal to \mathcal{A} 's advantage in distinguishing between H_2 and H_3 for scheme $\Sigma_{\mathcal{A}}$.

5 Extensions to Prime Order Groups

In Sec. 4, the Non-traceable ABE Template, the transformation from Non-traceable ABE Template to Augmented ABE, and the proofs are all presented on composite order bilinear groups. Note that our generic transformation from Non-traceable ABE Template to Augmented ABE and the security proofs for the transformation do not rely on the the composite order bilinear groups, and are only related to the G_{p_1} subgroup. Actually, the only reason we use composite order bilinear groups in Sec. 4 is that some appealing ABE schemes, e.g. the ones in [1], are built on the composite order bilinear groups, and we want our Non-Traceable ABE template to cover these appealing ABE schemes. On the other side, as shown below, it is easy to adjust the Sec. 4 contents to prime order bilinear groups, and the resulting generic framework still works well. Roughly speaking, this can be done by replacing the N with the prime order p_1 and removing all the parts related to p_2, p_3 . Below we list the details.

- In Sec. 4.2, define 'Prime Order Bilinear Groups'. Let \mathcal{G} be a group generator, which takes a security parameter λ and outputs $(p, \mathbb{G}, \mathbb{G}_T, e)$ where p is prime, \mathbb{G} and \mathbb{G}_T are cyclic groups of order p , and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ a map such that: (1) (Bilinear) $\forall g, h \in \mathbb{G}, a, b \in \mathbb{Z}_p, e(g^a, h^b) = e(g, h)^{ab}$, (2) (Non-Degenerate) $\exists g \in \mathbb{G}$ such that $e(g, g)$ has order p in \mathbb{G}_T . Assume that group operations in \mathbb{G} and \mathbb{G}_T as well as the bilinear map e are computable in polynomial time with respect to λ .

- In Sec. 4.2, redefine the Non-Traceable ABE Template by replacing $(N, p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$ with $(p, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$, replacing N with p , replacing p_1 with p , and removing all the parts related to \mathbb{G}_{p_3} :
 - Removing X_3 in Setup_{NT} and PP,
 - Removing $\mathbf{R} = (R_0, \dots, R_{d_k}) \in \mathbb{G}_{p_3}^{d_k+1}$ in $\text{KeyGen}_{\text{NT}}$ and SK_X .
- For Sec. 4.3, similar to Sec. 4.2, modify the transformation from Non-Traceable ABE Template to Augmented ABE by replacing $(N, p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$ with $(p, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$, replacing N with p , replacing p_1 with p , and removing all the parts related to \mathbb{G}_{p_3} :
 - Removing X_3 in Setup_{NT} and PP,
 - Removing $\mathbf{R} = (R_0, \dots, R_{d_k}) \in \mathbb{G}_{p_3}^{d_k+1}$ and $R'_0 \in \mathbb{G}_{p_3}$ in KeyGen_A and $\text{SK}_{(i,j),X}$.
- For Sec. 4.4, modify the proofs according to the above modifications for Sec. 4.2 and Sec. 4.3. In particular, replace N with p , replace p_1 with p , and remove all the parts related to \mathbb{G}_{p_3} .

It is easy to see that with the above modifications, the generic transformation framework on prime order bilinear groups also works well. And Later we also give some instantiations on prime order bilinear groups.

6 Instantiations Satisfying the Non-traceable ABE Template

In this section we show that some existing non-traceable ABE schemes with appealing features satisfy the template in Sec. 4.2, and prove the Lemma 1 (the indistinguishability between an encryption to (\bar{i}, \bar{j}) and $(\bar{i}, \bar{j} + 1)$) for the AugABE constructions from these non-traceable ABE instantiations.

These instantiations include three ABE instantiations on composite order bilinear groups, which were proposed by Attrapadung [1,2], and one ABE instantiation on prime order bilinear groups, which was proposed by Rouselakis and Waters [28].

6.1 Fully Secure Unbounded KP-ABE with Large Universe

Attrapadung [1, Sec. 5.3] proposed a fully secure unbounded KP-ABE scheme with large universe (i.e. the public key size is constant and independent from the size of the attribute universe), here we denote it by $\Sigma_{\text{NT}}^{\text{kpLU}}$. In $\Sigma_{\text{NT}}^{\text{kpLU}}$ the predicate Γ is described by *linear secret sharing scheme (LSSS)* [4], which is used in many ABE schemes (e.g. [13,30,18,19,28]) to express the access policy. Actually, any monotonic boolean formula (resp. monotonic access structure) can be realized by an LSSS [4]. We refer to [19] for more details of LSSS in ABE. Below we review $\Sigma_{\text{NT}}^{\text{kpLU}}$ in terms of Pair Encoding Scheme. Note that we change the variable names in $\Sigma_{\text{NT}}^{\text{kpLU}}$ to better suit our template definitions.

6.1.1 The Pair Encoding Scheme

$\Sigma_{\text{NT}}^{\text{kpLU}}$ complies with our non-traceable ABE template Sec. 4.2, with the following Pair Encoding Scheme.

SysParam. Take as input $\Gamma : \mathbb{X} \times \mathbb{Y} \rightarrow \{0, 1\}$, where the ciphertext tag (here is the attribute set) space $\mathbb{Y} = \{Y \mid Y \subseteq \mathbb{Z}_N\}$ and the key tag space $\mathbb{X} = \{\text{LSSS}(A, \rho) \mid A \text{ is a matrix over } \mathbb{Z}_N \text{ and } \rho \text{ maps each row of } A \text{ to an attribute in } \mathbb{Z}_N \text{ (} \rho \text{ does not need to be injective)}\}$, output $d = 6$ and $d_0 = 2$. Denote $\beta = (\beta_1, \dots, \beta_6)$.

KeyParam. Take in N and key policy $(A, \rho) \in \mathbb{X}$, where A is an $l \times n$ matrix, and $\rho : [1, l] \rightarrow \mathbb{Z}_N$ maps each row of A to an attribute in \mathbb{Z}_N , output $d_\delta = l + n + 1$ and $\phi = (\phi_0, \phi_1, \phi_2, \{\phi_{3,k}, \phi_{4,k}, \phi_{5,k}\}_{k \in [l]})$ with $d_k = 2 + 3l$:

$$\begin{aligned} \phi_0 &= \alpha + \beta_1 \delta_1 + \beta_2 \delta_2, & \phi_1 &= \delta_1, & \phi_2 &= \delta_2, \\ \phi_{3,k} &= A_k \cdot \mathbf{u} + \xi_k \beta_4, & \phi_{4,k} &= \xi_k, & \phi_{5,k} &= \xi_k (\beta_5 + \beta_6 \rho(k)), \end{aligned}$$

where $\delta = (\delta_1, \delta_2, \xi_1, \dots, \xi_l, u_2, \dots, u_n) \in \mathbb{Z}_N^{l+n+1}$ and $\mathbf{u} := (u_1 = \beta_3 \delta_1, u_2, \dots, u_n)$.

CiperParam. Take in N and attribute set $S \subseteq \mathbb{Z}_N$, output $d_\pi = 1 + |S|$ and $\psi = (\psi_1, \psi_2, \psi_3, \psi_4, \{\phi_{5,x}, \phi_{6,x}\}_{x \in S})$ with $d_c = 4 + 2|S|$:

$$\begin{aligned} \psi_1 &= \pi, & \psi_2 &= \beta_2 \pi, & \psi_3 &= \beta_1 \pi + \beta_3 \bar{\pi}, \\ \psi_4 &= \bar{\pi}, & \psi_{5,x} &= \bar{\pi} \beta_4 + \pi_x (\beta_5 + \beta_6 x), & \psi_{6,x} &= \pi_x, \end{aligned}$$

where $\boldsymbol{\pi} = (\pi, \bar{\pi}, \{\pi_x\}_{x \in S}) \in \mathbb{Z}_N^{2+|S|}$.

We can see that the outputs of above (SysParam, KeyParam, CiperParam) satisfies our template requirements:

- **KeyParam:**
 1. $d_k \geq d_0$, where $d_k = 2 + 3l$ and $d_0 = 2$.
 2. Each of $\{\phi_0, \phi_1, \phi_2, \{\phi_{3,k}, \phi_{4,k}, \phi_{5,k}\}_{k \in [l]}\}$ is a linear combination of monomials $\alpha, \delta_i, \delta_i \beta_j$.
 3. $\phi_0 = \alpha + \beta_1 \phi_1 + \beta_2 \phi_2$, $\phi_1 = \delta_1$. None of $\{\phi_2, \{\phi_{3,k}, \phi_{4,k}, \phi_{5,k}\}_{k \in [l]}\}$ contains α or $\beta_1 \delta_1$.
- **CiperParam:**
 1. Each of $\{\psi_1, \psi_2, \psi_3, \psi_4, \{\phi_{5,x}, \phi_{6,x}\}_{x \in S}\}$ is a linear combination of monomials $\pi, \pi_i, \pi \beta_j, \pi_i \beta_j$.
 2. $\psi_1 = \pi, \psi_2 = \beta_2 \pi$.
- **DecPair:** When S satisfies (A, ρ) , let $I = \{k \in [l] \mid \rho(k) \in S\}$, we have reconstruction coefficients $\{\omega_k\}_{k \in I}$ such that $\sum_{k \in I} \omega_k (A_k \cdot \mathbf{u}) = u_1 = \beta_3 \delta_1$. Therefore, we have the following linear combination of the $\phi_i \psi_j$ terms:

$$\phi_1 \psi_3 - \sum_{k \in I} \omega_k (\phi_{3,k} \psi_4 - \phi_{4,k} \psi_{5,\rho(k)} + \phi_{5,k} \psi_{6,\rho(k)}) = \delta_1 (\beta_1 \pi + \beta_3 \bar{\pi}) - \sum_{k \in I} \omega_k ((A_k \cdot \mathbf{u}) \bar{\pi}) = \beta_1 \delta_1 \pi.$$

6.1.2 Security Analysis of the Resulting Augmented ABE

As shown in Sec. 4.4 and Fig. 2, here we only need to handle the BLUE parts in Fig. 2, i.e, (1) state the security of the underlying conventional non-traceable ABE scheme (since the Type-I message hiding property of the AugABE is reduced to it) and (2) prove the Lemma 1.

(1) *The Section 5.3 of [1] shows that their KP-ABE scheme corresponding to the above Pair Encoding Scheme is a fully secure unbounded KP-ABE scheme with large universe.*

(2) The Lemma 1 instantiation here is: *if the Modified $(1, q)$ -EDHE3 Assumption holds, then for $\bar{j} < m$, no PPT adversary can selectively distinguish between an encryption to (\bar{i}, \bar{j}) and $(\bar{i}, \bar{j} + 1)$ in $\text{Game}_{\text{IH}}^{\text{A}}$ with non-negligible advantage, provided that the size of the challenge attribute set is $\leq q$.*

The Modified $(1, q)$ -EDHE3 Assumption is a special case of the Modified (n, t) -EDHE3 Assumption, which we introduce by modifying the (n, t) -EDHE3 Assumption in [2, Definition 6], i.e., giving the adversary one more element $g^{a^n c/z}$. In Appendix B, we prove that Modified (n, t) -EDHE3 Assumption holds in the generic group.

Definition 6. The Modified (n, t) -EDHE3 Assumption *Given a group generator \mathcal{G} , let $(N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, e) \xleftarrow{R} \mathcal{G}(\lambda)$, $g \xleftarrow{R} \mathbb{G}_{p_1}$, $g_2 \xleftarrow{R} \mathbb{G}_{p_2}$, $g_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $a, c, z, d_1, \dots, d_t \xleftarrow{R} \mathbb{Z}_N$. Suppose that an adversary is given*

$$\begin{aligned} D = & ((N, \mathbb{G}, \mathbb{G}_T, e), g, g^a, g^{a^n}, g^c, g^{c/z}, \underline{g^{a^n c/z}} \\ & \forall_{j \in [1, t]} g^{d_j}, \\ & \forall_{j, j' \in [1, t]} \text{ s.t. } j \neq j' g^{a^n c d_j / d_{j'}}, \\ & \forall_{i \in [1, n], j, j' \in [1, t]} \text{ s.t. } j \neq j' g^{a^i d_j / d_{j'}^2}, \\ & \forall_{i \in [1, 2n], j \in [1, t]} g^{a^i c d_j}, \\ & \forall_{i \in [1, 2n], i \neq n+1, j \in [1, t]} g^{a^i c / d_j}, \\ & \forall_{i \in [1, 2n], j, j' \in [1, t]} \text{ s.t. } j \neq j' g^{a^i c d_j / d_{j'}^2}, \\ & \forall_{i \in [1, n+1], j \in [1, t]} g^{a^i / d_j^2}, \\ & \forall_{i \in [n+1, 2n], j, j' \in [1, t]} g^{a^i c^2 d_j / d_{j'}}) \end{aligned}$$

and a target element $T \in \mathbb{G}_{p_1}$. The assumption states that it is hard for any polynomial time adversary to distinguish whether $T = g^{a^{n+1}z}$ or $T \xleftarrow{R} \mathbb{G}_{p_1}$.

The proof of the above Lemma 1 instantiation is given in Appendix C.

6.2 Fully Secure KP-ABE with Short Ciphertexts

Attrapadung [1, Sec. 5.3] proposed a fully secure KP-ABE scheme with short ciphertexts (i.e. ciphertext size is constant and independent from the size of the attribute set associated with the ciphertext), here we denote it by $\Sigma_{\text{NT}}^{\text{kpSC}}$. In $\Sigma_{\text{NT}}^{\text{kpSC}}$ the predicate Γ is also described by LSSS. Below we review $\Sigma_{\text{NT}}^{\text{kpSC}}$ in terms of Pair Encoding Scheme. Note that we change the variable names in $\Sigma_{\text{NT}}^{\text{kpSC}}$ to better suit our template definitions.

6.2.1 The Pair Encoding Scheme

$\Sigma_{\text{NT}}^{\text{kpSC}}$ is a bounded ABE where the maximum size for attribute set associated with the ciphertext is bounded by T , while no further restriction is required. $\Sigma_{\text{NT}}^{\text{kpSC}}$ complies with our non-traceable ABE template Sec. 4.2, with the following Pair Encoding Scheme.

SysParam. Take as input $\Gamma : \mathbb{X} \times \mathbb{Y} \rightarrow \{0, 1\}$, where the ciphertext tag (here is the attribute set) space $\mathbb{Y} = \{Y \mid Y \subseteq \mathbb{Z}_N \wedge |Y| \leq T\}$ and the key tag space $\mathbb{X} = \{\text{LSSS}(A, \rho) \mid A \text{ is a matrix over } \mathbb{Z}_N \text{ and } \rho \text{ maps each row of } A \text{ to an attribute in } \mathbb{Z}_N \text{ (} \rho \text{ does not need to be injective)}\}$, output $d = T + 6$ and $d_0 = 2$. Denote $\beta = (\beta_1, \dots, \beta_4, \theta_0, \theta_1, \dots, \theta_{T+1})$.

KeyParam. Take in N and key policy $(A, \rho) \in \mathbb{X}$, where A is an $l \times n$ matrix, and $\rho : [1, l] \rightarrow \mathbb{Z}_N$ maps each row of A to an attribute in \mathbb{Z}_N , output $d_\delta = l + n + 1$ and $\phi = (\phi_0, \phi_1, \phi_2, \{\phi_{3,k}, \phi_{4,k}, \phi_{5,k,0}, \{\phi_{5,k,t}\}_{t \in [T]}\}_{k \in [l]})$ with $d_k = 2 + l(T + 3)$:

$$\begin{aligned} \phi_0 &= \alpha + \beta_1 \delta_1 + \beta_2 \delta_2, & \phi_1 &= \delta_1, & \phi_2 &= \delta_2, \\ \phi_{3,k} &= A_k \cdot \mathbf{u} + \xi_k \beta_4, & \phi_{4,k} &= \xi_k, \\ \phi_{5,k,0} &= \xi_k \theta_0, & \{\phi_{5,k,t}\}_{t \in [T]} &= \xi_k (\theta_{t+1} - \theta_1 \rho(k)^t), \end{aligned}$$

where $\delta = (\delta_1, \delta_2, \xi_1, \dots, \xi_l, u_2, \dots, u_n) \in \mathbb{Z}_N^{l+n+1}$ and $\mathbf{u} := (u_1 = \beta_3 \delta_1, u_2, \dots, u_n)$.

CiperParam. Take in N and attribute set $S \subseteq \mathbb{Z}_N$ such that $|S| \leq T$, let c_t be the coefficient of z^t in $p(z) := \prod_{x \in S} (z - x)$, output $d_\pi = 2$ and $\psi = (\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6)$ with $d_c = 6$:

$$\begin{aligned} \psi_1 &= \pi, & \psi_2 &= \beta_2 \pi, & \psi_3 &= \beta_1 \pi + \beta_3 \bar{\pi}, \\ \psi_4 &= \bar{\pi}, & \psi_5 &= \bar{\pi} \beta_4 + \hat{\pi} (\theta_0 + \sum_{t=0}^T c_t \theta_{t+1}), & \psi_6 &= \hat{\pi}, \end{aligned}$$

where $\boldsymbol{\pi} = (\pi, \bar{\pi}, \hat{\pi}) \in \mathbb{Z}_N^3$.

We can see that the outputs of above (SysParam, KeyParam, CiperParam) satisfies our template requirements:

- **KeyParam:**
 1. $d_k \geq d_0$, where $d_k = 2 + l(T + 3)$ and $d_0 = 2$.
 2. Each of $\{\phi_0, \phi_1, \phi_2, \{\phi_{3,k}, \phi_{4,k}, \phi_{5,k,0}, \{\phi_{5,k,t}\}_{t \in [T]}\}_{k \in [l]}\}$ is a linear combination of monomials $\alpha, \delta_i, \delta_i \beta_j$.
 3. $\phi_0 = \alpha + \beta_1 \phi_1 + \beta_2 \phi_2, \phi_1 = \delta_1$. None of $\{\phi_2, \{\phi_{3,k}, \phi_{4,k}, \phi_{5,k,0}, \{\phi_{5,k,t}\}_{t \in [T]}\}_{k \in [l]}\}$ contains α or $\beta_1 \delta_1$.
- **CiperParam:**
 1. Each of $\{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6\}$ is a linear combination of monomials $\pi, \pi_i, \pi \beta_j, \pi_i \beta_j$.
 2. $\psi_1 = \pi, \psi_2 = \beta_2 \pi$.
- **DecPair:** When S satisfies (A, ρ) , let $I = \{k \in [l] \mid \rho(k) \in S\}$, we have reconstruction coefficients $\{\omega_k\}_{k \in I}$ such that $\sum_{k \in I} \omega_k (A_k \cdot \mathbf{u}) = u_1 = \beta_3 \delta_1$. Therefore, we have the following linear combination of the $\phi_i \psi_j$ terms:

$$D_P = \phi_1 \psi_3 - \sum_{k \in I} \omega_k (\phi_{3,k} \psi_4 - \phi_{4,k} \psi_5 + (\phi_{5,k,0} + \sum_{t=1}^T c_t \phi_{5,k,t}) \psi_6).$$

Note that

$$(\phi_{5,k,0} + \sum_{t=1}^T c_t \phi_{5,k,t}) \psi_6 = \xi_k (\theta_0 + \sum_{t=1}^T c_t \theta_{t+1} - \theta_1 \sum_{t=1}^T c_t \rho(k)^t) \hat{\pi}$$

$$\begin{aligned}
&= \xi_k \left(\theta_0 + \sum_{t=1}^T c_t \theta_{t+1} - \theta_1 (p(\rho(k)) - c_0) \right) \hat{\pi} \\
&= \xi_k \left(\theta_0 + \sum_{t=1}^T c_t \theta_{t+1} + \theta_1 c_0 \right) \hat{\pi} && \text{since } p(\rho(k)) = 0 \\
&= \xi_k \left(\theta_0 + \sum_{t=0}^T c_t \theta_{t+1} \right) \hat{\pi}.
\end{aligned}$$

We have that

$$\begin{aligned}
D_P &= \phi_1 \psi_3 - \sum_{k \in I} \omega_k \left(\phi_{3,k} \psi_4 - \phi_{4,k} \psi_5 + (\phi_{5,k,0} + \sum_{t=1}^T c_t \phi_{5,k,t}) \psi_6 \right) \\
&= \phi_1 \psi_3 - \sum_{k \in I} \omega_k \left((A_k \cdot \mathbf{u} + \xi_k \beta_4) \bar{\pi} - \xi_k (\bar{\pi} \beta_4 + \hat{\pi} (\theta_0 + \sum_{t=0}^T c_t \theta_{t+1})) + \xi_k \left(\theta_0 + \sum_{t=0}^T c_t \theta_{t+1} \right) \hat{\pi} \right) \\
&= \delta_1 (\beta_1 \pi + \beta_3 \bar{\pi}) - \sum_{k \in I} \omega_k (A_k \cdot \mathbf{u}) \bar{\pi} \\
&= \delta_1 \beta_1 \pi.
\end{aligned}$$

6.2.2 Security Analysis of the Resulting Augmented ABE

As shown in Sec. 4.4 and Fig. 2, here we only need to handle the BLUE parts in Fig. 2, i.e, (1) state the security of the underlying conventional non-traceable ABE scheme (since the Type-I message hiding property of the AugABE is reduced to it) and (2) prove the Lemma 1.

(1) *The Section 5.3 of [1] shows that their KP-ABE scheme corresponding to the above Pair Encoding Scheme is a fully secure KP-ABE scheme with short ciphertexts.*

(2) The Lemma 1 instantiation here is: *if the Modified $(T + 1, 1)$ -EDHE3 Assumption holds, then for $\bar{j} < m$, no PPT adversary can selectively distinguish between an encryption to (\bar{i}, \bar{j}) and $(\bar{i}, \bar{j} + 1)$ in $\text{Game}_{\text{IH}}^{\text{A}}$ with non-negligible advantage, provided that the size of the challenge attribute set is $\leq T$.*

Note that the Modified $(T + 1, 1)$ -EDHE3 Assumption is a special case of the Modified (n, t) -EDHE3 Assumption in Def. 6.

The proof of the above Lemma 1 instantiation is given in Appendix D.

6.3 Fully Secure ABE with Ciphertexts Associated with DFAs

Attrapadung [2, Sec. 8.2] proposed a fully secure ABE scheme for regular languages⁸, with ciphertexts associated with *Deterministic Finite Automata (DFA)*. Here we denote it by $\Sigma_{\text{NT}}^{\text{cpDFA}}$. In $\Sigma_{\text{NT}}^{\text{cpDFA}}$ the predicate Γ is described by DFA. In particular, for a DFA \mathbb{M} and a string \mathbf{u} , $\Gamma(\mathbb{M}, \mathbf{u}) = 1$ if the automata \mathbb{M} accepts the string \mathbf{u} . We refer to [31,1] for more details about DFA-based ABE, here we only give the below brief introduction. A DFA \mathbb{M} is a 5-tuple $(Q, \Lambda, \mathcal{T}, q_0, F)$ in which Q is the set of states $Q = \{q_0, q_1, \dots, q_{n-1}\}$, Λ is the alphabet set, \mathcal{T} is the set of transitions, in which each transition is of the form $(q_x, q_y, \sigma) \in Q \times Q \times \Lambda$, q_0 is the start state, and $F \subseteq Q$ is the set of accepted states. We say that \mathbb{M} accepts a string $\mathbf{u} = (u_1, u_2, \dots, u_l) \in \Lambda^*$ if there exists a sequence of states $\rho_0, \rho_1, \dots, \rho_n \in Q$ such that $\rho_0 = q_0$, for $i = 1$ to l we have $(\rho_{i-1}, \rho_i, u_i) \in \mathcal{T}$, and $\rho_l \in F$. Note that, as shown in [1,2], it is wlog if we consider machines such that $|F| = 1$. Below we review $\Sigma_{\text{NT}}^{\text{cpDFA}}$ in terms of Pair Encoding Scheme. Note that we change the variable names in $\Sigma_{\text{NT}}^{\text{cpDFA}}$ to better suit our template definitions.

⁸ Attrapadung [2] refers to the scheme as a ‘Functional Encryption’ scheme. Note that the scheme in [2] is still in ‘All-Or-Nothing’ style and is covered by our ABE definitions, in this paper we refer to it as an ABE scheme.

6.3.1 The Pair Encoding Scheme

$\Sigma_{\text{NT}}^{\text{cpDFA}}$ complies with our non-traceable ABE template Sec. 4.2, with the following Pair Encoding Scheme.

SysParam. Take as input $\Gamma : \mathbb{X} \times \mathbb{Y} \rightarrow \{0, 1\}$, where the ciphertext tag space $\mathbb{Y} = \{\mathbb{M} \mid \mathbb{M} \text{ is a DFA}\}$ and the key tag space $\mathbb{X} = \{\mathbf{u} \mid \mathbf{u} \in (\mathbb{Z}_N)^*\}$, output $d = 9$ and $d_0 = 2$. Denote $\boldsymbol{\beta} = (\beta_1, \dots, \beta_9)$.

KeyParam. Take in N and a string $\mathbf{u} \in (\mathbb{Z}_N)^*$, let $l = |\mathbf{u}|$, and parse $\mathbf{u} = (u_1, \dots, u_l)$. Output $d_\delta = 3 + l$ and $\boldsymbol{\phi} = (\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_{5,0}, \{\phi_{5,k}, \phi_{6,k}\}_{k \in [1,l]})$ with $d_k = 5 + 2l$:

$$\begin{aligned} \phi_0 &= \alpha + \beta_1 \delta_1 + \beta_2 \delta_2, & \phi_1 &= \delta_1, & \phi_2 &= \delta_2, & \phi_3 &= -\beta_3 \delta_1 + \beta_4 \xi_l, \\ \phi_4 &= \xi_0 \beta_5, & \phi_{5,0} &= \xi_0, & \{\phi_{5,k}, \phi_{6,k}\}_{k \in [1,l]} &= \{\xi_k(\beta_8 + \beta_9 u_k)\}_{k \in [1,l]}, \end{aligned}$$

where $\boldsymbol{\delta} = (\delta_1, \delta_2, \xi_0, \xi_1, \dots, \xi_l) \in \mathbb{Z}_N^{3+l}$.

CiperParam. Take in N and a DFA $\mathbb{M} = (Q, \mathbb{Z}_N, \mathcal{J}, q_0, q_{n-1})$ where $n = |Q|$, let $J = |\mathcal{J}|$, and parse $\mathcal{J} = \{(q_{x_t}, q_{y_t}, \sigma_t) \mid t \in [1, J]\}$. Output $d_\pi = 1 + J + n$ and $\boldsymbol{\psi} = (\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6, \{\psi_{7,t}, \psi_{8,t}, \psi_{9,t}\}_{t \in [1, J]})$ with $d_c = 6 + 3J$:

$$\begin{aligned} \psi_1 &= \pi, & \psi_2 &= \beta_2 \pi, & \psi_3 &= \beta_1 \pi + \beta_3 \bar{\pi}, \\ \psi_4 &= \bar{\pi}, & \psi_5 &= \pi_0, & \psi_6 &= -\nu_0 + \pi_0 \beta_5, \\ \psi_{7,t} &= \pi_t, & \psi_{8,t} &= \nu_{x_t} + \pi_t(\beta_6 + \beta_7 \sigma_t), & \psi_{9,t} &= -\nu_{y_t} + \pi_t(\beta_8 + \beta_9 \sigma_t), \end{aligned}$$

where $\boldsymbol{\pi} = (\pi, \bar{\pi}, \pi_0, \pi_1, \dots, \pi_J, \{\nu_x\}_{q_x \in Q \setminus \{q_{n-1}\}}) \in \mathbb{Z}_N^{2+J+n}$ and $\nu_{n-1} := \beta_4 \bar{\pi}$.

We can see that the outputs of above (SysParam, KeyParam, CiperParam) satisfies our template requirements:

- **KeyParam:**
 1. $d_k \geq d_0$, where $d_k = 5 + 2l$ and $d_0 = 2$.
 2. Each of $\{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_{5,0}, \{\phi_{5,k}, \phi_{6,k}\}_{k \in [1,l]}\}$ is a linear combination of monomials $\alpha, \delta_i, \delta_i \beta_j$.
 3. $\phi_0 = \alpha + \beta_1 \phi_1 + \beta_2 \phi_2$, $\phi_1 = \delta_1$. None of $\{\phi_2, \phi_3, \phi_4, \phi_{5,0}, \{\phi_{5,k}, \phi_{6,k}\}_{k \in [1,l]}\}$ contains α or $\beta_1 \delta_1$.
- **CiperParam:**
 1. Each of $\{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6, \{\psi_{7,t}, \psi_{8,t}, \psi_{9,t}\}_{t \in [1, J]}\}$ is a linear combination of monomials $\pi, \pi_i, \pi \beta_j, \pi_i \beta_j$.
 2. $\psi_1 = \pi, \psi_2 = \beta_2 \pi$.
- **DecPair:** When \mathbb{M} accepts $\mathbf{u} = (u_1, \dots, u_l)$, we have that there is a sequence of states $\rho_0, \rho_1, \dots, \rho_l \in Q$ such that $\rho_0 = q_0$, for $k = 1$ to l we have $(\rho_{k-1}, \rho_k, u_k) \in \mathcal{J}$, and $\rho_l \in F$. Let $(q_{x_{t_k}}, q_{y_{t_k}}, \sigma_{t_k}) = (\rho_{k-1}, \rho_k, u_k)$. Therefore, we have the following linear combination of the $\phi_i \psi_j$ terms:

$$\begin{aligned} & \phi_1 \psi_3 + \phi_3 \psi_4 - \phi_4 \psi_5 + \phi_{5,0} \psi_6 + \sum_{k \in [1, l]} (-\phi_{6,k} \psi_{7,t_k} + \phi_{5,k-1} \psi_{8,t_k} + \phi_{5,k} \psi_{9,t_k}) \\ &= \delta_1 (\beta_1 \pi + \beta_3 \bar{\pi}) + (-\beta_3 \delta_1 + \beta_4 \xi_l) \bar{\pi} - \xi_0 \beta_5 \pi_0 + \xi_0 (-\nu_0 + \pi_0 \beta_5) + (\xi_0 \nu_0 - \xi_l \nu_{n-1}) \\ &= \delta_1 \beta_1 \pi + \beta_4 \xi_l \bar{\pi} - \xi_l \beta_4 \bar{\pi} \\ &= \beta_1 \delta_1 \pi. \end{aligned}$$

Note that for any $k \in [1, l]$ we have

$$\begin{aligned} & -\phi_{6,k} \psi_{7,t_k} + \phi_{5,k-1} \psi_{8,t_k} + \phi_{5,k} \psi_{9,t_k} \\ &= -(\xi_{k-1}(\beta_6 + \beta_7 u_k) + \xi_k(\beta_8 + \beta_9 u_k)) \pi_{t_k} + \xi_{k-1}(\nu_{x_{t_k}} + \pi_{t_k}(\beta_6 + \beta_7 \sigma_{t_k})) + \xi_k(-\nu_{y_{t_k}} + \pi_{t_k}(\beta_8 + \beta_9 \sigma_{t_k})) \\ &= \xi_{k-1} \nu_{x_{t_k}} - \xi_k \nu_{y_{t_k}} \end{aligned}$$

and for any $k \in [1, l-1]$ we have $y_{y_{t_k}} = x_{t_{k+1}}$. Note that $q_{x_{t_1}} = \rho_0 = q_0$ implies $x_{t_1} = 0$ and $q_{x_{t_l}} = \rho_l = q_{n-1}$ implies $x_{t_l} = n-1$. Thus, we have

$$\sum_{k \in [1, l]} (-\phi_{6,k} \psi_{7,t_k} + \phi_{5,k-1} \psi_{8,t_k} + \phi_{5,k} \psi_{9,t_k}) = \xi_0 \nu_{x_{t_1}} - \xi_l \nu_{y_{t_l}} = \xi_0 \nu_0 - \xi_l \nu_{n-1}.$$

6.3.2 Security Analysis of the Resulting Augmented ABE

As shown in Sec. 4.4 and Fig. 2, here we only need to handle the BLUE parts in Fig. 2, i.e., (1) state the security of the underlying conventional non-traceable ABE scheme (since the Type-I message hiding property of the AugABE is reduced to it) and (2) prove the Lemma 1.

(1) *The Section 8.2 of [2] shows that their ABE scheme corresponding to the above Pair Encoding Scheme is a fully secure ABE scheme with Ciphertexts Associated with DFAs.*

(2) The Lemma 1 instantiation here is: *if the Modified (n, J) -EDHE2-Dual assumption holds, then for $\bar{j} < m$, no PPT adversary can selectively distinguish between an encryption to (\bar{i}, \bar{j}) and $(\bar{i}, \bar{j} + 1)$ in $\text{Game}_{\text{IH}}^{\text{A}}$ with non-negligible advantage, provided that the size of the challenge transition set is $\leq J$.*

The Modified (n, J) -EDHE2-Dual Assumption is a special case of the Modified (n, m) -EDHE2-Dual Assumption, which we introduce by modifying the (n, m) -EDHE2-Dual Assumption in [2, Definition 9], i.e., giving the adversary one more element $g^{a^{n-1}bc/z}$. In Appendix B, we prove that Modified (n, m) -EDHE2-Dual Assumption holds in the generic group.

Definition 7. The Modified (n, m) -EDHE2-Dual Assumption *Given a group generator \mathcal{G} , let $(N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, e) \xleftarrow{R} \mathcal{G}(\lambda)$, $g \xleftarrow{R} \mathbb{G}_{p_1}$, $g_2 \xleftarrow{R} \mathbb{G}_{p_2}$, $g_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $a, b, c, z, d_1, \dots, d_m \xleftarrow{R} \mathbb{Z}_N$. Suppose that an adversary is given*

$$D = \left((N, \mathbb{G}, \mathbb{G}_T, e), g, g^a, g^b, g^{b/z}, g^{a^{n-1}bc/z}, g_2, g_3, \right. \\ \forall_{i \in [1, n], j, j' \in [1, m], j \neq j'} g^{a^i/d_j^2}, g^{a^i b/d_j}, g^{d_j}, g^{a^i d_j/d_{j'}^2}, g^{a^i b d_j/d_{j'}}, g^{a^i/d_{j'}^6}, g^{a^i d_j/d_{j'}^6}, \\ \forall_{i \in [0, n-1], j \in [1, m]} g^{a^i c}, g^{a^i b c d_j}, \\ \forall_{i \in [0, n], j \in [1, m]} g^{a^i b c d_j^5}, \\ \forall_{i \in [1, 2n-1], j, j' \in [1, m], j \neq j'} g^{a^i b c d_j/d_{j'}^2}, g^{a^i b c d_j^5/d_{j'}^6}, \\ \forall_{i \in [1, 2n-1], i \neq n, j \in [1, m]} g^{a^i b c/d_j}, \\ \left. \forall_{i \in [1, 2n-1], j, j' \in [1, m]} g^{a^i c/d_j^2}, g^{a^i b^2 c d_j/d_{j'}}, g^{a^i b c d_j/d_{j'}^6}, g^{a^i c/d_{j'}^6}, g^{a^i b c d_j^5/d_{j'}^2}, g^{a^i b^2 c d_j^5/d_{j'}} \right)$$

and a target element $T \in \mathbb{G}_{p_1}$. The assumption states that it is hard for any polynomial time adversary to distinguish whether $T = g^{a^n c z}$ or $T \xleftarrow{R} \mathbb{G}_{p_1}$.

The proof of the above Lemma 1 instantiation is given in Appendix E.

6.4 Large Universe CP-ABE on Prime Order Groups

Rouselakis and Waters [28] proposed a large universe CP-ABE scheme which is on prime order groups and consequently more efficient than those on composite order groups. Here we denote it by $\Sigma_{\text{NT}}^{\text{cpLU}^p}$. In $\Sigma_{\text{NT}}^{\text{cpLU}^p}$ the predicate Γ is described by LSSS. Below we review $\Sigma_{\text{NT}}^{\text{cpLU}^p}$ in terms of Pair Encoding Scheme. Note that we change the variable names in $\Sigma_{\text{NT}}^{\text{cpLU}^p}$ to better suit our template definitions.

6.4.1 The Pair Encoding Scheme

$\Sigma_{\text{NT}}^{\text{cpLU}^p}$ complies with our non-traceable ABE template Sec. 4.2, with the following Pair Encoding Scheme.

SysParam. Take as input $\Gamma : \mathbb{X} \times \mathbb{Y} \rightarrow \{0, 1\}$, where the key tag (here is the attribute set) space $\mathbb{X} = \{X \mid X \subseteq \mathbb{Z}_p\}$ and the ciphertext tag space $\mathbb{Y} = \{\text{LSSS}(A, \rho) \mid A \text{ is a matrix over } \mathbb{Z}_p \text{ and } \rho \text{ maps each row of } A \text{ to an attribute in } \mathbb{Z}_p \text{ (}\rho \text{ does not need to be injective)}\}$, output $d = 4$ and $d_0 = 1$. Denote $\beta = (\beta_1, \dots, \beta_4)$.

KeyParam. Take in p and attribute set $S \subseteq \mathbb{Z}_p$. Output $d_\delta = 1 + |S|$ and $\phi = (\phi_0, \phi_1, \{\phi_{x,2}, \phi_{x,3}\}_{x \in S})$ with $d_k = 1 + 2|S|$:

$$\phi_0 = \alpha + \beta_1 \delta_1, \quad \phi_1 = \delta_1, \quad \{\phi_{x,2} = \theta_x, \quad \phi_{x,3} = (\beta_2 x + \beta_3) \theta_x - \beta_4 \delta_1\}_{x \in S},$$

where $\delta = (\delta_1, \{\theta_x\}_{x \in S}) \in \mathbb{Z}_p^{1+|S|}$.

CiperParam. Take in p and ciphertext policy $(A, \rho) \in \mathbb{Y}$, where A is an $l \times n$ matrix over \mathbb{Z}_p , and $\rho : [1, l] \rightarrow \mathbb{Z}_p$ maps each row of A to an attribute in \mathbb{Z}_p . Output $d_\pi = l + n$ and $\boldsymbol{\psi} = (\psi_1, \{\phi_{k,1}, \psi_{k,2}, \psi_{k,3}\}_{k \in [l]})$ with $d_c = 1 + 3l$:

$$\psi_1 = \pi, \quad \{\psi_{k,1} = \beta_1(A_k \cdot \mathbf{u}) + \beta_4 \xi_k, \quad \psi_{k,2} = -(\beta_2 \rho(k) + \beta_3) \xi_k, \quad \psi_{k,3} = \xi_k\}_{k \in [l]}$$

where $\boldsymbol{\pi} = (\pi, u_2, \dots, u_n, \xi_1, \dots, \xi_l) \in \mathbb{Z}_p^{l+n}$ and $\mathbf{u} := (u_1 = \pi, u_2, \dots, u_n)$.

We can see that the outputs of above (SysParam, KeyParam, CiperParam) satisfies our template requirements:

- **KeyParam:**
 1. $d_k \geq d_0$, where $d_k = 1 + 2|S|$ and $d_0 = 1$.
 2. Each of $\{\phi_0, \phi_1, \{\phi_{x,2}, \phi_{x,3}\}_{x \in S}\}$ is a linear combination of monomials $\alpha, \delta_i, \delta_i \beta_j$.
 3. $\phi_0 = \alpha + \beta_1 \phi_1$, $\phi_1 = \delta_1$. None of $\{\phi_{x,2}, \phi_{x,3}\}_{x \in S}$ contains α or $\beta_1 \delta_1$. Note that $d_0 = 1$.
- **CiperParam:**
 1. Each of $\{\psi_1, \{\psi_{k,1}, \psi_{k,2}, \psi_{k,3}\}_{k \in [l]}\}$ is a linear combination of monomials $\pi, \pi_i, \pi \beta_j, \pi_i \beta_j$.
 2. $\psi_1 = \pi$. Note that $d_0 = 1$, thus there is no requirement on $\psi_{\tilde{d}}$ for $\tilde{d} \geq 2$.
- **DecPair:** When S satisfies (A, ρ) , let $I = \{k \in [l] \mid \rho(k) \in S\}$, we have reconstruction coefficients $\{\omega_k\}_{k \in I}$ such that $\sum_{k \in I} \omega_k (A_k \cdot \mathbf{u}) = u_1 = \pi$. Therefore, we have the following linear combination of the $\phi_i \psi_j$ terms:

$$\sum_{k \in I} \omega_k (\phi_1 \psi_{k,1} + \phi_{\rho(k),2} \psi_{k,2} + \phi_{\rho(k),3} \psi_{k,3}) = \delta_1 \beta_1 \sum_{k \in I} \omega_k ((A_k \cdot \mathbf{u})) = \beta_1 \delta_1 \pi.$$

6.4.2 Security Analysis of the Resulting Augmented ABE

As shown in Sec. 4.4 and Fig. 2, here we only need to handle BLUE parts in Fig. 2, i.e, (1) state the security of the underlying conventional non-traceable ABE scheme (since the Type-I message hiding property of the AugABE is reduced to it) and (2) prove the Lemma 1.

(1) *The Section 4 of [28] shows that their CP-ABE scheme corresponding to the above Pair Encoding Scheme is a selectively secure CP-ABE scheme with large universe.*

(2) The Lemma 1 instantiation here is: *if the Extended Source Group q -parallel BDHE Assumption [24] holds, then for $\bar{j} < m$, no PPT adversary can selectively distinguish between an encryption to (\bar{i}, \bar{j}) and $(\bar{i}, \bar{j} + 1)$ in $\text{Game}_{\text{IH}}^A$ with non-negligible advantage, provided that the challenge LSSS matrix's size $l \times n$ satisfies $l, n \leq q$.*

The proof of the above Lemma 1 instantiation is given in Appendix F.

7 Discussions

Besides the instantiations above in Section 6, some other existing ABE schemes also satisfy our ABE template and can be transferred to Traceable ABE by applying our approach. For example,

1. The Fully Secure ABE for Keys associated with Regular Languages in [1, Sec. 5.2], with $d_0 = 2$.
2. The Fully Secure CP-ABE in [2, Scheme 11], with $d_0 = 1$.
3. The Fully Secure CP-ABE with large universe in [2, Scheme 13], with $d_0 = 1$.
4. The Fully Secure CP-ABE Scheme in [18, Sec. 2], with $d_0 = 1$.
5. The Fully Secure CP-ABE Scheme in [19], with $d_0 = 2$.

We omit the details of these instantiations here.

8 Conclusion

In this work, we proposed a generic framework that can transform conventional (non-traceable) ABE schemes to their traceable counterparts, which remain the appealing properties of the original conventional (non-traceable) ABE and achieve additional fully collusion-resistant blackbox traceability at the cost of sublinear overhead. In particular, we proposed a conventional (non-traceable) ABE template, and proposed a generic transformation from the ABE template to Augmented ABE which implies Traceable ABE. This generic framework implies that any ABE schemes satisfying our ABE template can be transformed to a Traceable ABE in a generic manner. And we showed that some existing appealing ABE schemes do satisfy our ABE template. We proved the security of our transformation framework in the standard model.

References

1. Attrapadung, N.: Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In: EUROCRYPT 2014. pp. 557–577 (2014)
2. Attrapadung, N.: Dual system encryption via doubly selective security: Framework, fully-secure functional encryption for regular languages, and more. IACR Cryptology ePrint Archive 2014, 428 (2014), <http://eprint.iacr.org/2014/428>
3. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Public Key Cryptography. pp. 90–108 (2011)
4. Beimel, A.: Secure Schemes for Secret Sharing and Key Distribution. Ph.D. thesis, Israel Institute of Technology, Technion, Haifa, Israel (1996)
5. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy. pp. 321–334 (2007)
6. Boneh, D., Franklin, M.K.: An efficient public key traitor tracing scheme. In: CRYPTO. pp. 338–353 (1999)
7. Boneh, D., Sahai, A., Waters, B.: Fully collusion resistant traitor tracing with short ciphertexts and private keys. In: EUROCRYPT. pp. 573–592 (2006)
8. Boneh, D., Waters, B.: A fully collusion resistant broadcast, trace, and revoke system. In: ACM Conference on Computer and Communications Security. pp. 211–220 (2006)
9. Boyen, X.: Attribute-based functional encryption on lattices. In: TCC. pp. 122–142 (2013)
10. Cheung, L., Newport, C.C.: Provably secure ciphertext policy ABE. In: ACM Conference on Computer and Communications Security. pp. 456–465 (2007)
11. Garg, S., Kumarasubramanian, A., Sahai, A., Waters, B.: Building efficient fully collusion-resilient traitor tracing and revocation schemes. In: ACM Conference on Computer and Communications Security. pp. 121–130 (2010)
12. Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attribute based encryption. In: ICALP (2). pp. 579–591 (2008)
13. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security. pp. 89–98 (2006)
14. Herranz, J., Laguillaumie, F., Ràfols, C.: Constant size ciphertexts in threshold attribute-based encryption. In: Public Key Cryptography. pp. 19–34 (2010)
15. Hohenberger, S., Waters, B.: Attribute-based encryption with fast decryption. In: Public-Key Cryptography. pp. 162–179 (2013)
16. Hohenberger, S., Waters, B.: Online/offline attribute-based encryption. In: Public-Key Cryptography. pp. 293–310 (2014)
17. Katz, J., Schröder, D.: Tracing insider attacks in the context of predicate encryption schemes. In: ACITA (2011), <https://www.usukita.org/node/1779>
18. Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: EUROCRYPT. pp. 62–91 (2010)
19. Lewko, A.B., Waters, B.: New proof methods for attribute-based encryption: Achieving full security through selective techniques. In: CRYPTO. pp. 180–198 (2012)
20. Liu, Z., Cao, Z., Wong, D.S.: Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay. In: ACM Conference on Computer and Communications Security. pp. 475–486 (2013)
21. Liu, Z., Cao, Z., Wong, D.S.: White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Transactions on Information Forensics and Security 8(1), 76–88 (2013)

22. Liu, Z., Cao, Z., Wong, D.S.: Fully collusion-resistant traceable key-policy attribute-based encryption with sub-linear size ciphertexts. In: Inscript 2014. pp. 403–423 (2014)
23. Liu, Z., Cao, Z., Wong, D.S.: Traceable CP-ABE: how to trace decryption devices found in the wild. IEEE Transactions on Information Forensics and Security 10(1), 55–68 (2015)
24. Liu, Z., Wong, D.S.: Practical ciphertext-policy attribute-based encryption: Traitor tracing, revocation, and large universe. In: ACNS 2015. pp. 127–146 (2015)
25. Liu, Z., Wong, D.S.: Traceable CP-ABE on prime order groups: Fully secure and fully collusion-resistant blackbox traceable. In: ICICS 2015. pp. 109–124 (2015)
26. Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: CRYPTO. pp. 41–62 (2001)
27. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: CRYPTO. pp. 191–208 (2010)
28. Rouselakis, Y., Waters, B.: Practical constructions and new proof methods for large universe attribute-based encryption. In: ACM Conference on Computer and Communications Security. pp. 463–474 (2013)
29. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: EUROCRYPT. pp. 457–473 (2005)
30. Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Public Key Cryptography. pp. 53–70 (2011)
31. Waters, B.: Functional encryption for regular languages. In: CRYPTO. pp. 218–235 (2012)

A Correctness

Correctness. Suppose that the message is M' and the encryption index is (\bar{i}, \bar{j}) . For $i \geq \bar{i}$ we have

$$\begin{aligned} \frac{e(K_0, Q_i) \cdot e(K'_0, Q'_i)}{e(K_1, Q_{i,1}) \cdot \prod_{\bar{d}=2}^{d_0} e(K_{\bar{d}}, Q_{i,\bar{d}})} &= \frac{e(g^{r_i c_j + \alpha_i} g^{\beta_1 \delta_1} \prod_{\bar{d}=2}^{d_0} g^{\beta_{\bar{d}} \phi_{\bar{d}}(\beta, \delta)}, g^{\tau s_i(\mathbf{v}_i \cdot \mathbf{v}_c)}) e(Z_i^{\delta_1}, g^{t_i})}{e(g^{\delta_1}, (g^{\beta_1})^{\tau s_i(\mathbf{v}_i \cdot \mathbf{v}_c)}) Z_i^{t_i} (g^{\beta_1})^\pi) \cdot \prod_{\bar{d}=2}^{d_0} e(g^{\phi_{\bar{d}}(\beta, \delta)}, (g^{\beta_{\bar{d}}})^{\tau s_i(\mathbf{v}_i \cdot \mathbf{v}_c)})} \\ &= \frac{e(g^{r_i c_j + \alpha_i}, g^{\tau s_i(\mathbf{v}_i \cdot \mathbf{v}_c)})}{e(g^{\delta_1}, (g^{\beta_1})^\pi)}. \end{aligned}$$

If $i \geq \bar{i} \wedge j \geq \bar{j}$: we have

$$\frac{e_3(\mathbf{R}'_i, \mathbf{C}'_j)}{e_3(\mathbf{R}_i, \mathbf{C}_j)} = \frac{e_3(G_i^{\kappa s_i \mathbf{v}_i}, g^{\mathbf{w}_j})}{e_3(G_i^{s_i \mathbf{v}_i}, H_j^{\tau(\mathbf{v}_c + \mu_j \mathbf{x}_3)} \cdot g^{\kappa \mathbf{w}_j})} = \frac{1}{e_3(g^{r_i s_i \mathbf{v}_i}, g^{c_j \tau \mathbf{v}_c})} = \frac{1}{e(g, g)^{r_i s_i c_j \tau(\mathbf{v}_i \cdot \mathbf{v}_c)}}.$$

If $i > \bar{i} \wedge j < \bar{j}$: note that for $i > \bar{i}$, we have $(\mathbf{v}_i \cdot \mathbf{x}_3) = 0$ (since $\mathbf{v}_i \in \text{span}\{\mathbf{x}_1, \mathbf{x}_2\}$), then we have

$$\frac{e_3(\mathbf{R}'_i, \mathbf{C}'_j)}{e_3(\mathbf{R}_i, \mathbf{C}_j)} = \frac{e_3(G_i^{\kappa s_i \mathbf{v}_i}, g^{\mathbf{w}_j})}{e_3(G_i^{s_i \mathbf{v}_i}, H_j^{\tau(\mathbf{v}_c + \mu_j \mathbf{x}_3)} \cdot g^{\kappa \mathbf{w}_j})} = \frac{1}{e_3(g^{r_i s_i \mathbf{v}_i}, g^{c_j \tau(\mathbf{v}_c + \mu_j \mathbf{x}_3)})} = \frac{1}{e(g, g)^{r_i s_i c_j \tau(\mathbf{v}_i \cdot \mathbf{v}_c)}}.$$

If $i = \bar{i} \wedge j < \bar{j}$: note that for $i = \bar{i}$, we have that $(\mathbf{v}_i \cdot \mathbf{x}_3) \neq 0$ happens with overwhelming probability (since \mathbf{v}_i is randomly chosen from \mathbb{Z}_N^3), then we have

$$\frac{e_3(\mathbf{R}'_i, \mathbf{C}'_j)}{e_3(\mathbf{R}_i, \mathbf{C}_j)} = \frac{e_3(G_i^{\kappa s_i \mathbf{v}_i}, g^{\mathbf{w}_j})}{e_3(G_i^{s_i \mathbf{v}_i}, H_j^{\tau(\mathbf{v}_c + \mu_j \mathbf{x}_3)} \cdot g^{\kappa \mathbf{w}_j})} = \frac{1}{e_3(g^{r_i s_i \mathbf{v}_i}, g^{c_j \tau(\mathbf{v}_c + \mu_j \mathbf{x}_3)})} = \frac{1}{e(g, g)^{r_i s_i c_j \tau((\mathbf{v}_i \cdot \mathbf{v}_c) + \mu_j (\mathbf{v}_i \cdot \mathbf{x}_3))}}.$$

Note that $D_P = e(\mathbf{K}^{\mathbf{E}_1}, \mathbf{P}) = e(g, g)^{\phi_{\mathbf{E}_1} \psi^T} = e(g, g)^{\beta_1 \sigma_{i,j} \pi}$. Thus from the values of T_i, D_P and D_I , for $M = T_i / (D_P \cdot D_I)$ we have that: (1) if $(i > \bar{i}) \vee (i = \bar{i} \wedge j \geq \bar{j})$, then $M = M'$; (2) if $i = \bar{i} \wedge j < \bar{j}$, then $M = M' \cdot e(g, g)^{\tau s_i r_i c_j \mu_j (\mathbf{v}_i \cdot \mathbf{x}_3)}$; (3) if $i < \bar{i}$, then M has no relation with M' .

B Generic Security of the Assumptions

As the underlying assumptions in this paper are modified versions of the assumptions in [2], in this section we prove the generic security of these assumptions using the proof framework of [2].

Theorem 6. *The Modified (n, m) -EDHE2-Dual assumption is secure in the generic group model.*

Proof. The Modified (n, m) -EDHE2-Dual assumption could be considered as (M, Y) -EDHE assumption [2, Definition 11] where the matrix M and the vector Y are depicted in Table 1, and where we use variables $a, b, c, d_1, \dots, d_m, z$. The first requirement holds since $n, m = O(\text{poly}(\lambda))$. We now prove the second requirement. We denote by $\mathbf{v}_{x,i,j}$ the row of type x with specified i, j in the range if there is any for that type. We also denote by S_x the set of all row indexes of type x ranged in its specified condition.

Type	Terms	Range	a	b	c	d_1	d_2	\dots	d_m	z
1	g		0	0	0	0	0	\dots	0	0
2	g^a		1	0	0	0	0	\dots	0	0
3	g^b		0	1	0	0	0	\dots	0	0
4	$g^{b/z}$		0	1	0	0	0	\dots	0	-1
4 ⁺	$g^{a^{n-1}bc/z}$		$n-1$	1	1	0	0	\dots	0	-1
5	$g^{a^i c}$	$i \in [0, n-1]$	i	0	1	0	0	\dots	0	0
6	g^{d_j}	$j \in [1, m]$	0	0	0			$1_{@j}$		0
7	g^{a^i/d_j^2}	$i \in [1, n], j \in [1, m]$	i	0	0			$-2_{@j}$		0
8	g^{a^i/d_j^6}	$i \in [1, n], j \in [1, m]$	i	0	0			$-6_{@j}$		0
9	$g^{a^i b/d_j}$	$i \in [1, n], j \in [1, m]$	i	1	0			$-1_{@j}$		0
10	$g^{a^i d_j/d_j^2}$	$i \in [1, n], j, j' \in [1, m], j \neq j'$	i	0	0			$1_{@j}, -2_{@j'}$		0
11	$g^{a^i d_j/d_j^6}$	$i \in [1, n], j, j' \in [1, m], j \neq j'$	i	0	0			$1_{@j}, -6_{@j'}$		0
12	$g^{a^i b d_j/d_j'}$	$i \in [1, n], j, j' \in [1, m], j \neq j'$	i	1	0			$1_{@j}, -1_{@j'}$		0
13	$g^{a^i b c d_j}$	$i \in [0, n-1], j \in [1, m]$	i	1	1			$1_{@j}$		0
14	$g^{a^i b c d_j^5}$	$i \in [0, n], j \in [1, m]$	i	1	1			$5_{@j}$		0
15	$g^{a^i b c d_j/d_j^2}$	$i \in [1, 2n-1], j, j' \in [1, m], j \neq j'$	i	1	1			$1_{@j}, -2_{@j'}$		0
16	$g^{a^i b c d_j^5/d_j^6}$	$i \in [1, 2n-1], j, j' \in [1, m], j \neq j'$	i	1	1			$5_{@j}, -6_{@j'}$		0
17	$g^{a^i b c/d_j}$	$i \in [1, 2n-1], i \neq n, j \in [1, m]$	i	1	1			$-1_{@j}$		0
18	$g^{a^i c/d_j^2}$	$i \in [1, 2n-1], j \in [1, m]$	i	0	1			$-2_{@j}$		0
19	$g^{a^i c/d_j^6}$	$i \in [1, 2n-1], j \in [1, m]$	i	0	1			$-6_{@j}$		0
20	$g^{a^i b^2 c d_j/d_j'}$	$i \in [1, 2n-1], j, j' \in [1, m]$	i	2	1			$1_{@j}, -1_{@j'}$		0
21	$g^{a^i b^2 c d_j^5/d_j'}$	$i \in [1, 2n-1], j, j' \in [1, m]$	i	2	1			$5_{@j}, -1_{@j'}$		0
22	$g^{a^i b c d_j/d_j^6}$	$i \in [1, 2n-1], j, j' \in [1, m]$	i	1	1			$1_{@j}, -6_{@j'}$		0
23	$g^{a^i b c d_j^5/d_j^2}$	$i \in [1, 2n-1], j, j' \in [1, m]$	i	1	1			$5_{@j}, -2_{@j'}$		0
*	Target $g^{a^n c z}$		n	0	1	0	0	\dots	0	1

Table 1. The matrix representation of the Modified (n, m) -EDHE2-Dual assumption

We first observe that $2\mathbf{v}_*$ contains 2 in the column z , but for any v, w , $\mathbf{v}_v + \mathbf{v}_w$ contains at most 0 in the z column, hence $2\mathbf{v}_* \neq \mathbf{v}_v + \mathbf{v}_w$ for any v, w . It remains to prove that $\mathbf{v}_* + \mathbf{v}_u \neq \mathbf{v}_v + \mathbf{v}_w$ for any u, v, w . We observe that $\mathbf{v}_* + \mathbf{v}_u$ for $u \notin \{4, 4^+\}$ contains 1 in the column z . Hence by the same reason, $\mathbf{v}_* + \mathbf{v}_u \neq \mathbf{v}_v + \mathbf{v}_w$ for all $u \notin \{4, 4^+\}, v, w$. It remains to prove that $\mathbf{v}_* + \mathbf{v}_4 = (n, 1, 1, 0, \dots, 0) \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w and $\mathbf{v}_* + \mathbf{v}_{4^+} = (2n-1, 1, 2, 0, \dots, 0) \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w . By the proof of the (n, m) -EDHE2-Dual assumption [2, Lemma 46], $\mathbf{v}_* + \mathbf{v}_4 \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w such that $v, w \notin \{4^+\}$. We observe that $\mathbf{v}_v + \mathbf{v}_w$ for $v \in \{4^+\}$

or $w \in \{4^+\}$ contains at most -1 in the z column. Hence $\mathbf{v}_* + \mathbf{v}_4 \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w . Now it remains to prove that $\mathbf{v}_* + \mathbf{v}_{4^+} = (2n-1, 1, 2, 0, \dots, 0) \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w . For a vector X and column q , we denote $[X]_q$ the entry in X at q . We first consider the following five cases.

- $v \in \{4, 4^+\}$ or $w \in \{4, 4^+\}$: $[\mathbf{v}_v + \mathbf{v}_w]_z \leq -1$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_z = 0$.
- $v \in S_{20} \cup S_{21}$ or $w \in S_{20} \cup S_{21}$: $[\mathbf{v}_v + \mathbf{v}_w]_b \geq 2$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_b = 1$.
- $v \in S_8 \cup S_{11} \cup S_{16} \cup S_{19}$ or $w \in S_8 \cup S_{11} \cup S_{16} \cup S_{19}$: $[\mathbf{v}_v + \mathbf{v}_w]_{d_j} \leq -1$ for some j but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_{d_j} = 0$ for all j . This is since $[\mathbf{v}_v]_{d_j} = -6$ for some j and $[\mathbf{v}_w]_{d_j} \leq 5$ for all j .
- $v \in S_{23}$ or $w \in S_{23}$: $[\mathbf{v}_v + \mathbf{v}_w]_{d_j} \neq 0$ for some j but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_{d_j} = 0$ for all j . This is due to the following. WLOG, we assume $v \in S_{23}$ (and w can be any) and write $v = (23, i, j, j')$. We further categorize as:
 - If $j = j'$, $[\mathbf{v}_v]_{d_j} = 3$. But for all j , $[\mathbf{v}_w]_{d_j} \neq -3$.
 - If $j \neq j'$, $([\mathbf{v}_v]_{d_j}, [\mathbf{v}_v]_{d_{j'}}) = (5, -2)$. But for all j, j' , $([\mathbf{v}_w]_{d_j}, [\mathbf{v}_w]_{d_{j'}}) \neq (-5, 2)$.
- $v \in S_{14}$ or $w \in S_{14}$: WLOG, we assume $v \in S_{14}$. We further categorize as:
 - $w \in S_{22}$: $[\mathbf{v}_v + \mathbf{v}_w]_b = 2$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_b = 1$.
 - $w \notin S_{22}$: $[\mathbf{v}_v + \mathbf{v}_w]_{d_j} \neq 0$ for some j but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_{d_j} = 0$ for all j . This is since $[\mathbf{v}_v]_{d_j} = 5$ for some j and $[\mathbf{v}_w]_{d_j} \neq -5$ for all j .

From now, we can assume $v, w \notin \{4, 4^+\} \cup S_8 \cup S_{11} \cup S_{14} \cup S_{16} \cup S_{19} \cup S_{20} \cup S_{21} \cup S_{23}$. We then consider the following case:

- $v \in S_7 \cup S_{10} \cup S_{15} \cup S_{18} \cup S_{22}$ or $w \in S_7 \cup S_{10} \cup S_{15} \cup S_{18} \cup S_{22}$: $[\mathbf{v}_v + \mathbf{v}_w]_{d_j} \leq -1$ for some j but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_{d_j} = 0$ for all j . This is since $[\mathbf{v}_v]_{d_j} \leq -2$ for some j and $[\mathbf{v}_w]_{d_j} \leq 1$ for all j .

From now, we can assume also $v, w \notin S_7 \cup S_{10} \cup S_{15} \cup S_{18} \cup S_{22}$. We further categorize as:

- $v \notin S_5 \cup S_{13} \cup S_{17}$ and $w \notin S_5 \cup S_{13} \cup S_{17}$: $[\mathbf{v}_v + \mathbf{v}_w]_c = 0$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_c = 2$.
- $v \in S_5 \cup S_{13} \cup S_{17}$ and $w \in S_5 \cup S_{13} \cup S_{17}$: we further categorize as:
 - $v \in S_5$ and $w \in S_5$: $[\mathbf{v}_v + \mathbf{v}_w]_b = 0$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_b = 1$.
 - $v \in S_5$ and $w \in S_{13} \cup S_{17}$: $[\mathbf{v}_v + \mathbf{v}_w]_{d_j} \neq 0$ for some j but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_{d_j} = 0$ for all j .
 - $v \in S_{13} \cup S_{17}$ and $w \in S_5$: $[\mathbf{v}_v + \mathbf{v}_w]_{d_j} \neq 0$ for some j but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_{d_j} = 0$ for all j .
 - $v \in S_{13} \cup S_{17}$ and $w \in S_{13} \cup S_{17}$: $[\mathbf{v}_v + \mathbf{v}_w]_b = 2$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_b = 1$.
- $v \in S_5 \cup S_{13} \cup S_{17}$ and $w \notin S_5 \cup S_{13} \cup S_{17}$: $[\mathbf{v}_v + \mathbf{v}_w]_c = 1$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_c = 2$.
- $v \notin S_5 \cup S_{13} \cup S_{17}$ and $w \in S_5 \cup S_{13} \cup S_{17}$: $[\mathbf{v}_v + \mathbf{v}_w]_c = 1$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_c = 2$.

This concludes all cases.

Theorem 7. *The Modified (n, t) -EDHE3 assumption is secure in the generic group model.*

Proof. The Modified (n, t) -EDHE3 assumption could be considered as (M, Y) -EDHE assumption [2, Definition 11] where the matrix M and the vector Y are depicted in Table 2, and where we use variables $a, b, c, d_1, \dots, d_t, z$. The first requirement holds since $n, t = O(\text{poly}(\lambda))$. We now prove the second requirement. We denote by $\mathbf{v}_{x, i, j}$ the row of type x with specified i, j in the range if there is any for that type. We also denote by S_x the set of all row indexes of type x ranged in its specified condition.

We first observe that $2\mathbf{v}_*$ contains 2 in the column z , but for any v, w , $\mathbf{v}_v + \mathbf{v}_w$ contains at most 0 in the z column, hence $2\mathbf{v}_* \neq \mathbf{v}_v + \mathbf{v}_w$ for any v, w . It remains to prove that $\mathbf{v}_* + \mathbf{v}_u \neq \mathbf{v}_v + \mathbf{v}_w$ for any u, v, w . We observe that $\mathbf{v}_* + \mathbf{v}_u$ for $u \notin \{4, 4^+\}$ contains 1 in the column z . Hence by the same reason, $\mathbf{v}_* + \mathbf{v}_u \neq \mathbf{v}_v + \mathbf{v}_w$ for all $u \notin \{4, 4^+\}, v, w$. It remains to prove that $\mathbf{v}_* + \mathbf{v}_4 = (n, 1, 0, \dots, 0) \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w and $\mathbf{v}_* + \mathbf{v}_{4^+} = (2n+1, 1, 0, \dots, 0) \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w . By the proof of the (n, t) -EDHE3 assumption [2, Lemma 47], $\mathbf{v}_* + \mathbf{v}_4 \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w such that $v, w \notin \{4^+\}$. We observe that $\mathbf{v}_v + \mathbf{v}_w$ for $v \in \{4^+\}$ or $w \in \{4^+\}$ contains at most -1 in the z column. Hence $\mathbf{v}_* + \mathbf{v}_4 \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w . Now it remains to prove that $\mathbf{v}_* + \mathbf{v}_{4^+} = (2n+1, 1, 0, \dots, 0) \neq \mathbf{v}_v + \mathbf{v}_w$ for all v, w . For a vector X and column q , we denote $[X]_q$ the entry in X at q . We first consider the following five cases.

- $v \in \{4, 4^+\}$ or $w \in \{4, 4^+\}$: $[\mathbf{v}_v + \mathbf{v}_w]_z \leq -1$ but $[\mathbf{v}_* + \mathbf{v}_{4^+}]_z = 0$.

Type	Terms	Range	a	c	d_1	d_2	\dots	d_t	z
1	g		0	0	0	0	\dots	0	0
2	g^a		1	0	0	0	\dots	0	0
3	g^c		0	1	0	0	\dots	0	0
4	$g^{c/z}$		0	1	0	0	\dots	0	-1
4 ⁺	$g^{a^n c/z}$		n	1	0	0	\dots	0	-1
5	g^{d_j}	$j \in [1, t]$	0	0	$1_{@j}$			0	0
6	g^{a^i/d_j^2}	$i \in [1, n+1], j \in [1, t]$	i	0	$-2_{@j}$			0	0
7	$g^{a^i d_j/d_{j'}^2}$	$i \in [1, n], j, j' \in [1, t], j \neq j'$	i	0	$1_{@j}, -2_{@j'}$			0	0
8	$g^{a^n c d_j/d_{j'}}$	$j, j' \in [1, t], j \neq j'$	n	1	$1_{@j}, -1_{@j'}$			0	0
9	$g^{a^i c d_j}$	$i \in [1, 2n], j \in [1, t]$	i	1	$1_{@j}$			0	0
10	$g^{a^i c/d_j}$	$i \in [1, 2n], i \neq n+1, j \in [1, t]$	i	1	$-1_{@j}$			0	0
11	$g^{a^i c d_j/d_{j'}^2}$	$i \in [1, 2n], j, j' \in [1, t], j \neq j'$	i	1	$1_{@j}, -2_{@j'}$			0	0
12	$g^{a^i c^2 d_j/d_{j'}}$	$i \in [n+1, 2n], j, j' \in [1, t]$	i	2	$1_{@j}, -1_{@j'}$			0	0
13	g^{a^n}		n	0	0	0	\dots	0	0
	Target								
*	$g^{a^{n+1}z}$		$n+1$	0	0	0	\dots	0	1

Table 2. The matrix representation of the Modified (n, t) -EDHE3 assumption

- $v \in S_6 \cup S_7 \cup S_{11}$ or $w \in S_6 \cup S_7 \cup S_{11}$: $[v_v + v_w]_{d_j} \leq -1$ for some j but $[v_* + v_{4+}]_{d_j} = 0$ for all j . This is since $[v_v]_{d_j} = -2$ for some j and $[v_w]_{d_j} \leq 1$ for all j .
- $v \in S_{12}$ or $w \in S_{12}$: $[v_v + v_w]_c \geq 2$ but $[v_* + v_{4+}]_c = 1$.

From now, we can assume $v, w \notin \{4, 4^+\} \cup S_6 \cup S_7 \cup S_{11} \cup S_{12}$. We further categorize as:

- $v \notin \{3\} \cup S_8 \cup S_9 \cup S_{10}$ and $w \notin \{3\} \cup S_8 \cup S_9 \cup S_{10}$: $[v_v + v_w]_c = 0$ but $[v_* + v_{4+}]_c = 1$.
- $v \in \{3\} \cup S_8 \cup S_9 \cup S_{10}$ and $w \in \{3\} \cup S_8 \cup S_9 \cup S_{10}$: $[v_v + v_w]_c = 2$ but $[v_* + v_{4+}]_c = 1$.
- $v \in \{3\} \cup S_8 \cup S_9 \cup S_{10}$ and $w \notin \{3\} \cup S_8 \cup S_9 \cup S_{10}$: we further categorize as:
 - $v \in \{3\}$ and $w \in \{2, 5, 13\}$: $[v_v + v_w]_a \leq n$ but $[v_* + v_{4+}]_a = 2n + 1$.
 - $v \in S_8 \cup S_9 \cup S_{10}$ and $w \in \{2, 13\}$: $[v_v + v_w]_{d_j} \neq 0$ for some j but $[v_* + v_{4+}]_{d_j} = 0$ for all j .
 - $v \in S_8 \cup S_9 \cup S_{10}$ and $w = 5$: $[v_v + v_w]_a \leq 2n$ but $[v_* + v_{4+}]_a = 2n + 1$.
- $v \notin \{3\} \cup S_8 \cup S_9 \cup S_{10}$ and $w \in \{3\} \cup S_8 \cup S_9 \cup S_{10}$: this is the same as the previous case for “ $v \in \{3\} \cup S_8 \cup S_9 \cup S_{10}$ and $w \notin \{3\} \cup S_8 \cup S_9 \cup S_{10}$ ” by exchanging v, w .

This concludes all cases.

C Proof of the Lemma 1 for the Fully Secure Unbounded KP-ABE with Large Universe

To make the proof easy to follow, we present the details of the resulting AugABE scheme first.

C.1 The Resulting Augmented KP-ABE

Setup_A $(\lambda, \Gamma, \mathcal{K} = m^2) \rightarrow (\text{PP}, \text{MSK})$. Run $(N, p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$. Pick generators $g \in \mathbb{G}_{p_1}$, $X_3 \in \mathbb{G}_{p_3}$. Set $d = 6, d_0 = 2$. Pick random $\beta = (\beta_1, \dots, \beta_6) \in \mathbb{Z}_N^6$. Pick random $\{\alpha_i, r_i, z_i \in \mathbb{Z}_N\}_{i \in [m]}$, $\{c_j \in \mathbb{Z}_N\}_{j \in [m]}$. The public parameter is

$$\text{PP} = \left((N, \mathbb{G}, \mathbb{G}_T, e), g, \mathbf{h} = (h_1 = g^{\beta_1}, \dots, h_6 = g^{\beta_6}), X_3, \{E_i = e(g, g)^{\alpha_i}, G_i = g^{r_i}, Z_i = g^{z_i}\}_{i \in [m]}, \{H_j = g^{c_j}\}_{j \in [m]} \right).$$

The master secret key is $\text{MSK} = (\alpha_1, \dots, \alpha_m, r_1, \dots, r_m, c_1, \dots, c_m)$.

A counter $ctr = 0$ is implicitly included in MSK.

$\text{KeyGen}_A(\text{PP}, \text{MSK}, (A, \rho)) \rightarrow \text{SK}_{(i,j),(A,\rho)}$. Set $\text{ctr} = \text{ctr} + 1$ and then compute the corresponding index in the form of (i, j) where $1 \leq i, j \leq m$ and $(i-1) * m + j = \text{ctr}$. Let $l \times n$ be the size of A . Pick random $\delta = (\delta_1, \delta_2, \xi_1, \dots, \xi_l, u_2, \dots, u_n) \in \mathbb{Z}_N^{l+n+1}$, $\mathbf{R} = (R_0, R_1, R_2, \{R_{3,k}, R_{4,k}, R_{5,k}\}_{k \in [l]}) \in \mathbb{G}_{p_3}^{3+3l}$, and $R'_0 \in \mathbb{G}_{p_3}$. Implicitly setting $\mathbf{u} = (u_1 = \beta_3 \delta_1, u_2, \dots, u_n)$, output a secret key $\text{SK}_{(i,j),(A,\rho)}$ as

$$\begin{aligned} \text{SK}_{(i,j),(A,\rho)} &= ((i, j), (A, \rho), \\ &K_0 = g^{r_i c_j + \alpha_i} g^{\beta_1 \delta_1} g^{\beta_2 \delta_2} R_0, \quad K_1 = g^{\delta_1} R_1, \quad K_2 = g^{\delta_2} \cdot R_2, \\ &\{K_{3,k} = g^{A_k \cdot \mathbf{u}} g^{\beta_4 \xi_k} R_{3,k}, \quad K_{4,k} = g^{\xi_k} R_{4,k}, \quad K_{5,k} = (g^{\beta_5} g^{\beta_6 \rho(k)})^{\xi_k} R_{5,k}\}_{k \in [l]}, \\ &K'_0 = Z_i^{\delta_1} R'_0). \end{aligned}$$

Note that $K_{3,k} = g^{A_k \cdot \mathbf{u}} g^{\beta_4 \xi_k} R_{3,k}$ can be computed as $K_{3,k} = (g^{\beta_3})^{A_{k,1} \delta_1} g^{\sum_{t=2}^n A_{k,t} u_t} g^{\beta_4 \xi_k} R_{3,k}$, where $A_k = (A_{k,1}, A_{k,2}, \dots, A_{k,n})$ is the k -th row of A .

$\text{Encrypt}_A(\text{PP}, M, S, (\bar{i}, \bar{j})) \rightarrow CT_S$.

1. Upon input the attribute set $S \subseteq \mathbb{Z}_N$, pick random $\boldsymbol{\pi} = (\pi, \bar{\pi}, \{\pi_x\}_{x \in S}) \in \mathbb{Z}_N^{2+|S|}$. Set

$$\begin{aligned} P_1 &= g^\pi, & P_2 &= g^{\beta_2 \pi}, & P_3 &= g^{\beta_1 \pi} g^{\beta_3 \bar{\pi}}, \\ P_4 &= g^{\bar{\pi}}, & \{P_{5,x}\} &= g^{\beta_4 \bar{\pi}} (g^{\beta_5} g^{\beta_6 x})^{\pi_x}, & P_{6,x} &= g^{\pi_x} \}_{x \in S}. \end{aligned}$$

2. Pick random $\kappa, \tau, s_1, \dots, s_m, t_1, \dots, t_m \in \mathbb{Z}_N$, $\mathbf{v}_c, \mathbf{w}_1, \dots, \mathbf{w}_m \in \mathbb{Z}_N^3$.

Pick random $r_x, r_y, r_z \in \mathbb{Z}_N$, and set $\boldsymbol{\chi}_1 = (r_x, 0, r_z)$, $\boldsymbol{\chi}_2 = (0, r_y, r_z)$, $\boldsymbol{\chi}_3 = \boldsymbol{\chi}_1 \times \boldsymbol{\chi}_2 = (-r_y r_z, -r_x r_z, r_x r_y)$.

Pick random $\mathbf{v}_i \in \mathbb{Z}_N^3 \forall i \in \{1, \dots, \bar{i}\}$, $\mathbf{v}_i \in \text{span}\{\boldsymbol{\chi}_1, \boldsymbol{\chi}_2\} \forall i \in \{\bar{i} + 1, \dots, m\}$.

For each row $i \in [m]$:

– if $i < \bar{i}$: randomly choose $\hat{s}_i \in \mathbb{Z}_N$, and set

$$\mathbf{R}_i = g^{\mathbf{v}_i}, \quad \mathbf{R}'_i = g^{\kappa \mathbf{v}_i}, \quad Q_i = g^{s_i}, \quad Q_{i,1} = (g^{\beta_1})^{s_i} Z_i^{t_i} (g^{\beta_1})^\pi, \quad Q_{i,2} = (g^{\beta_2})^{s_i}, \quad Q'_i = g^{t_i}, \quad T_i = E_i^{\hat{s}_i}.$$

– if $i \geq \bar{i}$: set

$$\begin{aligned} \mathbf{R}_i &= G_i^{s_i \mathbf{v}_i}, \quad \mathbf{R}'_i = G_i^{\kappa s_i \mathbf{v}_i}, \quad Q_i = g^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}, \quad Q_{i,1} = (g^{\beta_1})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)} Z_i^{t_i} (g^{\beta_1})^\pi, \quad Q_{i,2} = (g^{\beta_2})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}, \\ Q'_i &= g^{t_i}, \quad T_i = M \cdot E_i^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}. \end{aligned}$$

For each column $j \in [m]$:

– if $j < \bar{j}$: randomly choose $\mu_j \in \mathbb{Z}_p$, and set $\mathbf{C}_j = H_j^{\tau(\mathbf{v}_c + \mu_j \boldsymbol{\chi}_3)} \cdot g^{\kappa \mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

– if $j \geq \bar{j}$: set $\mathbf{C}_j = H_j^{\tau \mathbf{v}_c} \cdot g^{\kappa \mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

3. Output the ciphertext CT_S as $CT_S = \langle S, (P_1, P_2, P_3, P_4, \{P_{5,x}, P_{6,x}\}_{x \in S}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q_{i,2}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$.

$\text{Decrypt}_A(\text{PP}, CT_S, \text{SK}_{(i,j),(A,\rho)}) \rightarrow M$ or \perp . Parse CT_S to $CT_S = \langle S, (P_1, P_2, P_3, P_4, \{P_{5,x}, P_{6,x}\}_{x \in S}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q_{i,2}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$ and $\text{SK}_{(i,j),(A,\rho)}$ to $\text{SK}_{(i,j),(A,\rho)} = ((i, j), (A, \rho), (K_0, K_1, K_2, \{K_{3,k}, K_{4,k}, K_{5,k}\}_{k \in [l]}, K'_0))$. Suppose S satisfies (A, ρ) (if S does not satisfies (A, ρ) , output \perp).

1. Compute constants $\{\omega_k\}_{\rho(k) \in S}$ such that $\sum_{\rho(k) \in S} \omega_k A_k = (1, 0, \dots, 0)$. Compute

$$D_P \leftarrow e(K_1, P_3) / \prod_{\rho(k) \in S} \left(\frac{e(K_{3,k}, P_4) \cdot e(K_{5,k}, P_{6,\rho(k)})}{e(K_{4,k}, P_{5,\rho(k)})} \right)^{\omega_k}$$

2. Compute

$$D_I \leftarrow \frac{e(K_0, Q_i) \cdot e(K'_0, Q'_i)}{e(K_1, Q_{i,1}) \cdot e(K_2, Q_{i,2})} \cdot \frac{e_3(\mathbf{R}'_i, \mathbf{C}'_j)}{e_3(\mathbf{R}_i, \mathbf{C}_j)}.$$

3. Computes $M \leftarrow T_i / (D_P \cdot D_I)$ as the output message.

C.2 Proof of Lemma 1

Proof. Suppose there exists a polynomial time adversary \mathcal{A} that selectively breaks the index-hiding game with advantage ϵ . We build a PPT algorithm \mathcal{B} to solve a Modified $(1, q)$ -EDHE3 problem instance in a subgroup as follows. \mathcal{B} is given

$$D = \left((N, \mathbb{G}, \mathbb{G}_T, e), g, g^a, g^c, g^{c/z}, g^{ac/z} \text{ (for } g^{ca^n/z} \text{ with } n = 1), g_2, g_3, \right. \\ \left. \begin{array}{l} \forall j \in [q] \quad g^{d_j}, g^{acd_j}, g^{a^2cd_j}, g^{ac/d_j}, g^{a/d_j^2}, g^{a^2/d_j^2}, \\ \forall j, j' \in [q] \text{ s.t. } j \neq j' \quad g^{ad_j/d_{j'}^2}, g^{acd_j/d_{j'}}, g^{acd_j/d_{j'}^2}, g^{a^2cd_j/d_{j'}}, \\ \forall j, j' \in [q] \quad g^{a^2c^2d_j/d_{j'}} \end{array} \right)$$

and T , where $(N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, e) \xleftarrow{R} \mathcal{G}$, $g \xleftarrow{R} \mathbb{G}_{p_1}$, $g_2 \xleftarrow{R} \mathbb{G}_{p_2}$, $g_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $a, c, z, d_1, \dots, d_q \xleftarrow{R} \mathbb{Z}_N$, and T is either equal to g^{a^2z} or is a random element from \mathbb{G}_{p_1} . \mathcal{B} 's goal is to determine $T = g^{a^2z}$ or T is a random element from \mathbb{G}_{p_1} .

Init. \mathcal{A} gives \mathcal{B} the challenge attribute set $S^* = \{a_1^*, \dots, a_{l^*}^*\} \subseteq \mathbb{Z}_N$, where $|S^*| = l^* \leq q$.

Setup. \mathcal{B} randomly chooses $\{\alpha_i \in \mathbb{Z}_N\}_{i \in [m]}$, $\{r_i, z'_i \in \mathbb{Z}_N\}_{i \in [m] \setminus \{\bar{i}\}}$, $r'_i, z_i \in \mathbb{Z}_N$, $\{c'_j \in \mathbb{Z}_N\}_{j \in [m]}$, and $\beta'_1, \beta_2, \beta'_3, \beta'_4, \beta'_5, \beta'_6 \in \mathbb{Z}_N$. \mathcal{B} gives \mathcal{A} the public parameter PP:

$$\left(g, h_1 = (g^a)^{\beta'_1}, h_2 = g^{\beta_2}, h_3 = (g^a)^{\beta'_3}, h_4 = (g^a)^{\beta'_4}, \right. \\ h_5 = g^{\beta'_5} \cdot \left(\prod_{t \in [l^*]} (g^{a/d_t^2})^{-a_t^*} \right) \cdot \left(\prod_{t \in [l^*]} g^{ac/d_t} \right), h_6 = g^{\beta'_6} \cdot \left(\prod_{t \in [l^*]} g^{a/d_t^2} \right), \\ \{E_i = e(g, g)^{\alpha_i}\}_{i \in [m]}, \\ \{G_i = g^{r_i}, Z_i = (g^a)^{z'_i}\}_{i \in [m] \setminus \{\bar{i}\}}, \{H_j = (g^{c/z})^{c'_j}\}_{j \in [m] \setminus \{\bar{j}\}}, G_{\bar{i}} = (g^a)^{r'_i}, Z_{\bar{i}} = g^{z_i}, H_{\bar{j}} = (g^a)^{c'_j} \Big).$$

Note that \mathcal{B} implicitly chooses $r_{\bar{i}}, z_i (i \in [m] \setminus \{\bar{i}\}), c_j (j \in [m]), \beta_1, \beta_3, \beta_4, \beta_5, \beta_6 \in \mathbb{Z}_N$ such that

$$\begin{aligned} ar'_{\bar{i}} &\equiv r_{\bar{i}} \pmod{p_1}, az'_i \equiv z_i \pmod{p_1} \quad \forall i \in [m] \setminus \{\bar{i}\}, \\ ac'_j &\equiv c_j \pmod{p_1}, (c/z)c'_j \equiv c_j \pmod{p_1} \quad \forall j \in [m] \setminus \{\bar{j}\}, \\ a\beta'_1 &\equiv \beta_1 \pmod{p_1}, a\beta'_3 \equiv \beta_3 \pmod{p_1}, a\beta'_4 \equiv \beta_4 \pmod{p_1}, \\ \beta'_5 + \sum_{t \in [l^*]} (-a_t^* a/d_t^2) + \sum_{t \in [l^*]} (ac)/d_t &\equiv \beta_5 \pmod{p_1}, \\ \beta'_6 + \sum_{t \in [l^*]} a/d_t^2 &\equiv \beta_6 \pmod{p_1}. \end{aligned}$$

Query Phase. To respond to \mathcal{A} 's query for $((i, j), (A, \rho))$, let $l \times n$ be the size of A ,

- if $(i, j) \neq (\bar{i}, \bar{j})$: \mathcal{B} picks random $\delta = (\delta_1, \delta_2, \xi_1, \dots, \xi_l, u_2, \dots, u_n) \in \mathbb{Z}_N^{l+n+1}$, $\mathbf{R} = (R_0, R_1, R_2, \{R_{3,k}, R_{4,k}, R_{5,k}\}_{k \in [l]}) \in \mathbb{G}_{p_3}^{3+3l}$, and $R'_0 \in \mathbb{G}_{p_3}$. Implicitly setting $\mathbf{u} = (u_1 = \beta_3 \delta_1, u_2, \dots, u_n)$, \mathcal{B} creates a secret key $\text{SK}_{(i,j),(A,\rho)}$:

$$K_0 = \begin{cases} g^{\alpha_i} (g^{c/z})^{r_i c'_j} \cdot h_1^{\delta_1} h_2^{\delta_2} R_0, & : i \neq \bar{i}, j \neq \bar{j} \\ g^{\alpha_i} (g^{ac/z})^{r'_i c'_j} \cdot h_1^{\delta_1} h_2^{\delta_2} R_0, & : i = \bar{i}, j \neq \bar{j} \\ g^{\alpha_i} (g^a)^{r_i c'_j} \cdot h_1^{\delta_1} h_2^{\delta_2} R_0, & : i \neq \bar{i}, j = \bar{j}. \end{cases} \\ K_1 = g^{\delta_1} R_1, \quad K_2 = g^{\delta_2} \cdot R_2, \quad K'_0 = Z_i^{\delta_1} R'_0, \\ \{K_{3,k} = h_3^{A_{k,1} \delta_1} g^{\sum_{t=2}^n A_{k,t} u_t} h_4^{\xi_k} R_{3,k}, K_{4,k} = g^{\xi_k} R_{4,k}, K_{5,k} = (h_5 h_6^{\rho(k)})^{\xi_k} R_{5,k}\}_{k \in [l]}.$$

- if $(i, j) = (\bar{i}, \bar{j})$: it implies that \mathcal{A} is querying a secret key with the challenge index (\bar{i}, \bar{j}) , and (A, ρ) is not satisfied by S^* . \mathcal{B} first computes a vector $\bar{\mathbf{u}} = (\bar{u}_1, \dots, \bar{u}_n) \in \mathbb{Z}_N^n$ that has first entry equal to 1 (i.e. $\bar{u}_1 = 1$)

and is orthogonal to all of the rows A_k of A such that $\rho(k) \in S^*$ (i.e. $A_k \cdot \bar{\mathbf{u}} = 0 \forall k \in [l]$ s.t. $\rho(k) \in S^*$). Note that such a vector must exist since S^* fails to satisfy (A, ρ) , and it is efficiently computable. \mathcal{B} picks random $\delta'_1, \delta_2, \{\xi_k\}_{k \in [l]}$ s.t. $\rho(k) \in S^*$, $\{\xi'_k\}_{k \in [l]}$ s.t. $\rho(k) \notin S^*$, $u'_2, \dots, u'_n \in \mathbb{Z}_N$, $\mathbf{R} = (R_0, R_1, R_2, \{R_{3,k}, R_{4,k}, R_{5,k}\}_{k \in [l]}) \in \mathbb{G}_{p_3}^{3+3l}$, and $R'_0 \in \mathbb{G}_{p_3}$. Let $\mathbf{u}' = (0, u'_2, \dots, u'_n) \in \mathbb{Z}_N^n$, \mathcal{B} sets the values of $\delta_1 \in \mathbb{Z}_N$, $\mathbf{u} \in \mathbb{Z}_N^n$, $\{\xi_k \in \mathbb{Z}_N\}_{k \in [l]}$ s.t. $\rho(k) \notin S^*$ by implicitly setting

$$\delta'_1 - ar'_i c'_j / \beta'_1 \equiv \delta_1 \pmod{p_1}, \quad \mathbf{u} = \mathbf{u}' + (a\beta'_3) \delta_1 \bar{\mathbf{u}},$$

$$\xi'_k + (a - \sum_{t \in [l^*]} \frac{acd_t}{\rho(k) - a_t^*}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4) \equiv \xi_k \pmod{p} \forall k \in [l] \text{ s.t. } \rho(k) \notin S^*.$$

Note that for $a_t^* \in S^*$ and $\rho(k) \notin S^*$ we have $\rho(k) - a_t^* \neq 0$. \mathcal{B} creates a secret key $\text{SK}_{(\bar{i}, \bar{j}), (A, \rho)}$ as follows:

$$K_0 = g^{\alpha_{\bar{i}}} h_1^{\delta'_1} h_2^{\delta_2} R_0, \quad K_1 = g^{\delta'_1} (g^a)^{-r'_i c'_j / \beta'_1} R_1, \quad K_2 = g^{\delta_2} R_2, \quad K'_0 = (K_1)^{z_{\bar{i}}} R'_0,$$

- for $k \in [l]$ s.t. $\rho(k) \in S^*$,

$$K_{3,k} = g^{(A_k \cdot \mathbf{u})} h_4^{\xi_k} R_{3,k} = g^{(A_k \cdot \mathbf{u}') + a\beta'_3 \delta_1 (A_k \cdot \bar{\mathbf{u}})} h_4^{\xi_k} R_{3,k} = g^{(A_k \cdot \mathbf{u}')} h_4^{\xi_k} R_{3,k},$$

$$K_{4,k} = g^{\xi_k} R_{4,k}, \quad K_{5,k} = (h_5 h_6^{\rho(k)})^{\xi_k} R_{5,k},$$

- for $k \in [l]$ s.t. $\rho(k) \notin S^*$,

$$\begin{aligned} K_{3,k} &= g^{(A_k \cdot \mathbf{u})} h_4^{\xi_k} R_{3,k} \\ &= g^{(A_k \cdot \mathbf{u}')} \cdot g^{a\beta'_3 (\delta'_1 - ar'_i c'_j / \beta'_1) (A_k \cdot \bar{\mathbf{u}})} \\ &\quad \cdot h_4^{\xi'_k} \cdot (g^{a\beta'_4})^{a\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot (g^{a\beta'_4})^{-(\sum_{t \in [l^*]} \frac{acd_t}{\rho(k) - a_t^*}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} R_{3,k} \\ &= g^{(A_k \cdot \mathbf{u}')} \cdot g^{a\beta'_3 \delta'_1 (A_k \cdot \bar{\mathbf{u}})} \cdot h_4^{\xi'_k} \cdot (g^{\sum_{t \in [l^*]} \frac{a^2 cd_t}{\rho(k) - a_t^*}})^{-\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / \beta'_1} R_{3,k} \\ &= g^{(A_k \cdot \mathbf{u}')} \cdot (g^a)^{\beta'_3 \delta'_1 (A_k \cdot \bar{\mathbf{u}})} \cdot h_4^{\xi'_k} \cdot \left(\prod_{t \in [l^*]} (g^{a^2 cd_t})^{\frac{1}{\rho(k) - a_t^*}} \right)^{-\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / \beta'_1} R_{3,k}, \\ K_{4,k} &= g^{\xi_k} R_{4,k} = g^{\xi'_k + (a - \sum_{t \in [l^*]} \frac{acd_t}{\rho(k) - a_t^*}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} R_{4,k} \\ &= g^{\xi'_k} \cdot (g^a)^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \left(\prod_{t \in [l^*]} (g^{acd_t})^{\frac{1}{\rho(k) - a_t^*}} \right)^{-\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} R_{4,k}, \\ K_{5,k} &= (h_5 h_6^{\rho(k)})^{\xi_k} R_{5,k} \\ &= (h_5 h_6^{\rho(k)})^{\xi'_k} \cdot (h_5 h_6^{\rho(k)})^{(a - \sum_{t' \in [l^*]} \frac{acd_{t'}}{\rho(k) - a_{t'}^*}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} R_{5,k} \\ &= (h_5 h_6^{\rho(k)})^{\xi'_k} \\ &\quad \cdot \left(g^{\beta'_5 + \beta'_6 \rho(k)} \cdot \left(\prod_{t \in [l^*]} (g^{a/d_t^2})^{\rho(k) - a_t^*} \right) \cdot \left(\prod_{t \in [l^*]} g^{ac/d_t} \right) \right)^{(a - \sum_{t' \in [l^*]} \frac{acd_{t'}}{\rho(k) - a_{t'}^*}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot R_{5,k} \\ &= (h_5 h_6^{\rho(k)})^{\xi'_k} \cdot (g^{\beta'_5 + \beta'_6 \rho(k)})^{a\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot (g^{\beta'_5 + \beta'_6 \rho(k)})^{-(\sum_{t' \in [l^*]} \frac{acd_{t'}}{\rho(k) - a_{t'}^*}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \\ &\quad \cdot \left(\prod_{t \in [l^*]} (g^{a/d_t^2})^{\rho(k) - a_t^*} \right)^{a\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \left(\prod_{t \in [l^*]} (g^{a/d_t^2})^{\rho(k) - a_t^*} \right)^{-(\sum_{t' \in [l^*]} \frac{acd_{t'}}{\rho(k) - a_{t'}^*}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \\ &\quad \cdot \left(\prod_{t \in [l^*]} g^{ac/d_t} \right)^{a\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \left(\prod_{t \in [l^*]} g^{ac/d_t} \right)^{-(\sum_{t' \in [l^*]} \frac{acd_{t'}}{\rho(k) - a_{t'}^*}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot R_{5,k} \\ &= (h_5 h_6^{\rho(k)})^{\xi'_k} \cdot (g^a)^{(\beta'_5 + \beta'_6 \rho(k)) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \underbrace{\left(\prod_{t' \in [l^*]} (g^{acd_{t'}})^{\frac{1}{\rho(k) - a_{t'}^*}} \right)^{-(\beta'_5 + \beta'_6 \rho(k)) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}}_{\Psi_1} \end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left(\prod_{t \in [l^*]} (g^{a^2/d_t^2})^{\rho(k)-a_t^*} \right)^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \left(\prod_{t \in [l^*]} \prod_{t' \in [l^*]} (g^{a^2 c d_{t'}/d_t^2})^{\frac{\rho(k)-a_t^*}{\rho(k)-a_{t'}^*}} \right)^{-\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}}_{\Psi_2} \\
& \cdot \underbrace{\left(\prod_{t \in [l^*]} g^{a^2 c/d_t} \right)^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \left(\prod_{t \in [l^*]} \prod_{t' \in [l^*]} (g^{a^2 c^2 d_{t'}/d_t})^{\frac{1}{\rho(k)-a_{t'}^*}} \right)^{-\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}}_{\Psi_3} \cdot R_{5,k} \\
= & \Psi_1 \cdot \Psi_2 \cdot \underbrace{\left(\prod_{t \in [l^*]} \prod_{t' \in [l^*] \setminus \{t\}} (g^{a^2 c d_{t'}/d_t^2})^{\frac{\rho(k)-a_t^*}{\rho(k)-a_{t'}^*}} \right)^{-\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}}_{\Psi_4, \text{ for } t' \neq t} \\
& \cdot \underbrace{\left(\prod_{t \in [l^*]} (g^{a^2 c d_t/d_t^2})^{\frac{\rho(k)-a_t^*}{\rho(k)-a_t^*}} \right)^{-\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \left(\prod_{t \in [l^*]} g^{a^2 c/d_t} \right)^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}}_{\text{for } t'=t} \cdot \Psi_3 \cdot R_{5,k} \\
= & \Psi \cdot \Psi_2 \cdot \Psi_4 \cdot \Psi_3 \cdot R_{5,k}.
\end{aligned}$$

Note that \mathcal{B} can calculate the values of $K_0, K_1, K_2, K'_0, \{K_{3,k}, K_{4,k}, K_{5,k}\}_{k \in [l]}$ using the suitable terms of the assumption.

Challenge. \mathcal{A} submits a message M . \mathcal{B} randomly chooses

$$\begin{aligned}
& \tau', s_1, \dots, s_{\bar{i}-1}, s'_{\bar{i}}, s_{\bar{i}+1}, \dots, s_m, t'_1, \dots, t'_{\bar{i}-1}, t_{\bar{i}}, t'_{\bar{i}+1}, \dots, t'_m \in \mathbb{Z}_N, \\
& \mathbf{w}_1, \dots, \mathbf{w}_{\bar{j}-1}, \mathbf{w}'_{\bar{j}}, \dots, \mathbf{w}'_m \in \mathbb{Z}_N^3, \\
& \pi', \bar{\pi}', \pi'_{a_1^*}, \dots, \pi'_{a_l^*} \in \mathbb{Z}_N.
\end{aligned}$$

\mathcal{B} randomly chooses $r_x, r_y, r_z \in \mathbb{Z}_N$, and sets $\chi_1 = (r_x, 0, r_z), \chi_2 = (0, r_y, r_z), \chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$. \mathcal{B} randomly chooses

$$\begin{aligned}
& \mathbf{v}_i \in \mathbb{Z}_p^3 \quad \forall i \in \{1, \dots, \bar{i}-1\}, \\
& \mathbf{v}_i^p \in \text{span}\{\chi_1, \chi_2\}, \quad \mathbf{v}_i^q \in \text{span}\{\chi_3\}, \\
& \mathbf{v}_i \in \text{span}\{\chi_1, \chi_2\} \quad \forall i \in \{\bar{i}+1, \dots, m\}, \\
& \mathbf{v}_c^p \in \text{span}\{\chi_1, \chi_2\}, \quad \mathbf{v}_c^q = \nu_3 \chi_3 \in \text{span}\{\chi_3\}.
\end{aligned}$$

\mathcal{B} sets the value of $\kappa, \tau, s_{\bar{i}}, t_i (i \in [m] \setminus \{\bar{i}\}) \in \mathbb{Z}_N, \mathbf{v}_c, \mathbf{v}_{\bar{i}} \in \mathbb{Z}_N^3, \{\mathbf{w}_j \in \mathbb{Z}_N^3\}_{j=\bar{j}}^m, \pi \in \mathbb{Z}_N, \bar{\pi} \in \mathbb{Z}_N, \{\pi'_{a_i^*} \in \mathbb{Z}_N\}_{t \in [l^*]}$ by implicitly setting

$$\begin{aligned}
& a \equiv \kappa \pmod{p_1}, \quad a z \tau' \equiv \tau \pmod{p_1}, \quad s'_{\bar{i}}/a \equiv s_{\bar{i}} \pmod{p_1}, \\
& t'_i + c \beta'_1 \tau' s'_{\bar{i}} (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i \equiv t_i \pmod{p_1} \quad \forall i \in \{1, \dots, \bar{i}-1\}, \\
& t'_i - a \beta'_1 \tau' s_i (\mathbf{v}_i \cdot \mathbf{v}_c^p) / z'_i + c \beta'_1 \tau' s'_{\bar{i}} (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i \equiv t_i \pmod{p_1} \quad \forall i \in \{\bar{i}+1, \dots, m\}, \\
& \mathbf{v}_c = \frac{1}{z} \mathbf{v}_c^p + \mathbf{v}_c^q, \quad \mathbf{v}_{\bar{i}} = \mathbf{v}_{\bar{i}}^p + \frac{c}{z} \mathbf{v}_{\bar{i}}^q, \\
& \mathbf{w}'_j - a c'_j \tau' \mathbf{v}_c^p \equiv \mathbf{w}_{\bar{j}} \pmod{p_1}, \\
& \mathbf{w}'_j - c c'_j \tau' \mathbf{v}_c^q \equiv \mathbf{w}_j \pmod{p_1} \quad \forall j \in \{\bar{j}+1, \dots, m\}, \\
& \pi' - c \tau' s'_{\bar{i}} (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) \equiv \pi \pmod{p_1}, \quad \bar{\pi}' + c \beta'_1 \tau' s'_{\bar{i}} (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) / \beta'_3 \equiv \bar{\pi} \pmod{p_1}, \\
& \pi'_{a_t^*} - d_t \beta'_1 \beta'_4 \tau' s'_{\bar{i}} (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) / \beta'_3 \equiv \pi_{a_t^*} \pmod{p_1} \quad \forall t \in [l^*].
\end{aligned}$$

It is worth noticing that $\mathbf{v}_{\bar{i}}$ and \mathbf{v}_c are random vectors in \mathbb{Z}_N^3 as required, and $(\mathbf{v}_{\bar{i}} \cdot \mathbf{v}_c) = \frac{1}{z} (\mathbf{v}_{\bar{i}}^p \cdot \mathbf{v}_c^p) + \frac{c}{z} (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q)$, since χ_3 is orthogonal to $\text{span}\{\chi_1, \chi_2\}$ and $\mathbb{Z}_N^3 = \text{span}\{\chi_1, \chi_2, \chi_3\}$.

\mathcal{B} creates a ciphertext $\langle S^*, (P_1, P_2, P_3, P_4, \{P_{5,x}, P_{6,x}\}_{x \in S^*}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q_{i,2}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$ as follows:

1. $P_1 = g^{\pi'} (g^c)^{-\tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}$, $P_2 = (P_1)^{\beta_2}$, $P_3 = h_1^{\pi'} h_3^{\pi'}$, $P_4 = g^{\bar{\pi}'} (g^c)^{\beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}$,
for $t \in [l^*]$,

$$\begin{aligned}
P_{5,a_t^*} &= h_4^{\bar{\pi}'} (h_5 h_6^{a_t^*})^{\pi_{a_t^*}} \\
&= h_4^{\bar{\pi}' + c \beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \cdot (h_5 h_6^{a_t^*})^{\pi_{a_t^*} - d_t \beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= h_4^{\bar{\pi}'} \cdot (g^{a \beta'_4})^{c \beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot (h_5 h_6^{a_t^*})^{\pi_{a_t^*}} \cdot \left(g^{\beta'_5} g^{\beta'_6 a_t^*} \cdot \left(\prod_{t' \in [l^*]} (g^{a/d_{t'}})^{a_t^* - a_{t'}} \right) \cdot \left(\prod_{t' \in [l^*]} g^{ac/d_{t'}} \right) \right)^{-d_t \beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= h_4^{\bar{\pi}'} \cdot (g^{ac})^{\beta'_4 \beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \cdot (h_5 h_6^{a_t^*})^{\pi_{a_t^*}} \cdot (g^{d_t})^{-(\beta'_5 + \beta'_6 a_t^*) \beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{t' \in [l^*]} (g^{ad_t/d_{t'}})^{a_t^* - a_{t'}} \right)^{-\beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \cdot \left(\prod_{t' \in [l^*]} g^{acd_t/d_{t'}} \right)^{-\beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= \underbrace{h_4^{\bar{\pi}'}}_{\Psi_1} \cdot \underbrace{(g^{ac})^{\beta'_4 \beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\Delta} \cdot \underbrace{(h_5 h_6^{a_t^*})^{\pi_{a_t^*}} \cdot (g^{d_t})^{-(\beta'_5 + \beta'_6 a_t^*) \beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\Psi_2} \\
&\quad \cdot \underbrace{\left(\prod_{t' \in [l^*] \setminus \{t\}} (g^{ad_t/d_{t'}})^{a_t^* - a_{t'}} \right)^{-\beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\Psi_3, \text{ for } t' \neq t} \cdot \underbrace{\left((g^{ad_t/d_t})^{a_t^* - a_t} \right)^{-\beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{1, \text{ for } t'=t} \\
&\quad \cdot \underbrace{\left(\prod_{t' \in [l^*] \setminus \{t\}} g^{acd_t/d_{t'}} \right)^{-\beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\Psi_4, \text{ for } t' \neq t} \cdot \underbrace{(g^{acd_t/d_t})^{-\beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\Delta^{-1}, \text{ for } t'=t} \\
&= \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \Psi_4, \\
P_{6,a_t^*} &= g^{\pi_{a_t^*}} = g^{\pi_{a_t^*} - d_t \beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} = g^{\pi_{a_t^*}} (g^{d_t})^{-\beta'_1 \beta'_4 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}.
\end{aligned}$$

Note that the values of Ψ_1, \dots, Ψ_4 can be calculated using the suitable terms of the assumption.

2. For each $i \in [m]$:

– if $i < \bar{i}$: it randomly chooses $\hat{s}_i \in \mathbb{Z}_p$, then sets

$$\begin{aligned}
\mathbf{R}_i &= g^{\mathbf{v}^i}, \quad \mathbf{R}'_i = (g^a)^{\mathbf{v}^i}, \quad Q_i = g^{s_i}, \quad Q_{i,1} = h_1^{s_i} Z_i^{t_i} h_1^{\pi'}, \\
Q_{i,2} &= (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i} (g^c)^{\beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i}, \quad T_i = E_i^{\hat{s}_i}.
\end{aligned}$$

– if $i = \bar{i}$: it sets

$$\begin{aligned}
\mathbf{R}_i &= g^{r'_i s'_i \mathbf{v}_i^p} (g^{c/z})^{r'_i s'_i \mathbf{v}_i^q}, \quad \mathbf{R}'_i = (g^a)^{r'_i s'_i \mathbf{v}_i^p} (g^{ac/z})^{r'_i s'_i \mathbf{v}_i^q}, \quad Q_i = g^{\tau' s'_i (\mathbf{v}_i^p \cdot \mathbf{v}_c^p)} (g^c)^{\tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}, \\
Q_{i,1} &= h_1^{\tau' s'_i (\mathbf{v}_i^p \cdot \mathbf{v}_c^p)} Z_i^{t_i} h_1^{\pi'}, \quad Q_{i,2} = (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i}, \quad T_i = M \cdot e(g^{\alpha_i}, Q_i).
\end{aligned}$$

– if $i > \bar{i}$: it sets

$$\begin{aligned}
\mathbf{R}_i &= g^{r_i s_i \mathbf{v}^i}, \quad \mathbf{R}'_i = (g^a)^{r_i s_i \mathbf{v}^i}, \quad Q_i = (g^a)^{\tau' s_i (\mathbf{v}^i \cdot \mathbf{v}_c^p)}, \quad Q_{i,1} = Z_i^{t_i} h_1^{\pi'}, \\
Q_{i,2} &= (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i} (g^a)^{-\beta'_1 \tau' s_i (\mathbf{v}^i \cdot \mathbf{v}_c^p) / z'_i} (g^c)^{\beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i}, \quad T_i = M \cdot e(g^{\alpha_i}, Q_i).
\end{aligned}$$

3. For each $j \in [m]$:

– if $j < \bar{j}$: it randomly chooses $\mu'_j \in \mathbb{Z}_N$ and implicitly sets the value of μ_j such that $(ac)^{-1} \mu'_j \nu_3 - \nu_3 \equiv \mu_j \pmod{p_1}$, then sets $\mathbf{C}_j = (g^{(ac)/z})^{c'_j \tau' \mathbf{v}_c^p} \cdot g^{c'_j \tau' \mu'_j \mathbf{v}_c^q} \cdot (g^a)^{\mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

- if $j = \bar{j}$: it sets $\mathbf{C}_j = T^{c'_j \tau' v_c^q} \cdot (g^a) \mathbf{w}'_j$, $\mathbf{C}'_j = g \mathbf{w}'_j \cdot (g^a)^{-c'_j \tau' v_c^q}$.
- if $j > \bar{j}$: it sets $\mathbf{C}_j = (g^{(ac)/z})^{c'_j \tau' v_c^q} \cdot (g^a) \mathbf{w}'_j$, $\mathbf{C}'_j = g \mathbf{w}'_j \cdot (g^e)^{-c'_j \tau' v_c^q}$.

If $T = g^{a^2 z}$, then the ciphertext is a well-formed encryption to the index (\bar{i}, \bar{j}) . If T is randomly chosen, say $T = g^r$ for some random $r \in \mathbb{Z}_{p_1}$, the ciphertext is a well-formed encryption to the index $(\bar{i}, \bar{j} + 1)$ with implicitly setting $\mu_{\bar{j}}$ such that $(\frac{r}{a^2 z} - 1) \nu_3 \equiv \mu_{\bar{j}} \pmod{p_1}$.

Guess. \mathcal{A} outputs a guess $b' \in \{0, 1\}$ to \mathcal{B} , then \mathcal{B} outputs this b' to the challenger.

The distributions of the public parameters, private keys and challenge ciphertext are the same as that in the real scheme. \mathcal{B} 's advantage in the Modified $(1, q)$ -EDHE3 game will be exactly equal to \mathcal{A} 's advantage in the selective index-hiding game.

D Proof of the Lemma 1 for the Fully Secure KP-ABE with Short Ciphertexts

To make the proof easy to follow, we present the details of the resulting AugABE scheme first.

D.1 The Resulting Augmented KP-ABE

$\text{Setup}_A(\lambda, \mathcal{U}, N = m^2, T) \rightarrow (\text{PP}, \text{MSK})$. Run $\mathcal{G}(\lambda)$ to get $(N, p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)$. Pick generators $g \in \mathbb{G}_{p_1}$, $X_3 \in \mathbb{G}_{p_3}$. Set $d = T + 6, d_0 = 2$. Pick random $\beta = (\beta_1, \dots, \beta_4, \theta_0, \theta_1, \dots, \theta_{T+1}) \in \mathbb{Z}_N^{T+6}$. Pick random $\{\alpha_i, r_i, z_i \in \mathbb{Z}_N\}_{i \in [m]}$, $\{c_j \in \mathbb{Z}_N\}_{j \in [m]}$. The public parameter is

$$\text{PP} = ((N, \mathbb{G}, \mathbb{G}_T, e), g, h_1 = g^{\beta_1}, \dots, h_4 = g^{\beta_4}, f_0 = g^{\theta_0}, f_1 = g^{\theta_1}, \dots, f_{T+1} = g^{\theta_{T+1}}, X_3, \\ \{E_i = e(g, g)^{\alpha_i}, G_i = g^{r_i}, Z_i = g^{z_i}\}_{i \in [m]}, \{H_j = g^{c_j}\}_{j \in [m]}).$$

The master secret key is $\text{MSK} = (\alpha_1, \dots, \alpha_m, r_1, \dots, r_m, c_1, \dots, c_m)$.

A counter $ctr = 0$ is implicitly included in MSK.

$\text{KeyGen}_A(\text{PP}, \text{MSK}, (A, \rho)) \rightarrow \text{SK}_{(i,j),(A,\rho)}$. Set $ctr = ctr + 1$ and then compute the corresponding index in the form of (i, j) where $1 \leq i, j \leq m$ and $(i-1) * m + j = ctr$. Let $l \times n$ be the size of A . Pick random $\delta = (\delta_1, \delta_2, \xi_1, \dots, \xi_l, u_2, \dots, u_n) \in \mathbb{Z}_N^{l+n+1}$, $\mathbf{R} = (R_0, R_1, R_2, \{R_{3,k}, R_{4,k}, R_{5,k,0}, \{R_{5,k,t}\}_{t \in [T]}\}_{k \in [l]} \in \mathbb{G}_{p_3}^{3+(3+T)l}$, and $R'_0 \in \mathbb{G}_{p_3}$. Implicitly setting $\mathbf{u} = (u_1 = \beta_3 \delta_1, u_2, \dots, u_n)$, output a secret key $\text{SK}_{(i,j),(A,\rho)}$ as

$$\text{SK}_{(i,j),(A,\rho)} = ((i, j), (A, \rho), \\ K_0 = g^{r_i c_j + \alpha_i} h_1^{\delta_1} h_2^{\delta_2} R_0, \quad K_1 = g^{\delta_1} R_1, \quad K_2 = g^{\delta_2} \cdot R_2, \quad K'_0 = Z_i^{\delta_1} R'_0, \\ \{K_{3,k} = g^{A_k \cdot \mathbf{u}} h_4^{\xi_k} R_{3,k}, \quad K_{4,k} = g^{\xi_k} R_{4,k}, \\ K_{5,k,0} = f_0^{\xi_k}, \quad \{K_{5,k,t} = (f_{t+1} f_1^{-\rho(k)t})^{\xi_k} R_{5,k,t}\}_{t \in [T]}\}_{k \in [l]}).$$

Note that $K_{3,k} = g^{A_k \cdot \mathbf{u}} g^{\beta_4 \xi_k} R_{3,k}$ can be computed as

$$K_{3,k} = (g^{\beta_3})^{A_{k,1} \delta_1} g^{\sum_{t=2}^n A_{k,t} u_t} g^{\beta_4 \xi_k} R_{3,k} = h_3^{A_{k,1} \delta_1} g^{\sum_{t=2}^n A_{k,t} u_t} h_4^{\xi_k} R_{3,k}, \text{ where } A_k = (A_{k,1}, A_{k,2}, \dots, A_{k,n})$$

is the k -th row of A .

$\text{Encrypt}_A(\text{PP}, M, S, (\bar{i}, \bar{j})) \rightarrow CT_S$.

1. Upon input the attribute set $S \subseteq \mathbb{Z}_N$, pick random $\pi = (\pi, \bar{\pi}, \hat{\pi}) \in \mathbb{Z}_N^3$. Let c_t be the coefficient of z^t in $p(z) := \prod_{x \in S} (z - x)$. Set

$$P_1 = g^\pi, \quad P_2 = h_2^\pi, \quad P_3 = h_1^\pi h_3^{\bar{\pi}}, \\ P_4 = g^{\bar{\pi}}, \quad P_5 = h_4^{\hat{\pi}} (f_0 \prod_{t=0}^T f_{t+1}^{c_t})^{\hat{\pi}}, \quad P_6 = g^{\hat{\pi}}.$$

2. Pick random

$$\kappa, \tau, s_1, \dots, s_m, t_1, \dots, t_m \in \mathbb{Z}_N,$$

$$\mathbf{v}_c, \mathbf{w}_1, \dots, \mathbf{w}_m \in \mathbb{Z}_N^3.$$

Pick random $r_x, r_y, r_z \in \mathbb{Z}_N$, and set $\chi_1 = (r_x, 0, r_z)$, $\chi_2 = (0, r_y, r_z)$, $\chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$.
Pick random

$$\begin{aligned} \mathbf{v}_i &\in \mathbb{Z}_N^3 \quad \forall i \in \{1, \dots, \bar{i}\}, \\ \mathbf{v}_i &\in \text{span}\{\chi_1, \chi_2\} \quad \forall i \in \{\bar{i} + 1, \dots, m\}. \end{aligned}$$

For each row $i \in [m]$:

– if $i < \bar{i}$: randomly choose $\hat{s}_i \in \mathbb{Z}_p$, and set

$$\begin{aligned} \mathbf{R}_i &= g^{\mathbf{v}_i}, \quad \mathbf{R}'_i = g^{\kappa \mathbf{v}_i}, \quad Q_i = g^{s_i}, \quad Q_{i,1} = (g^{\beta_1})^{s_i} Z_i^{t_i} (g^{\beta_1})^\pi, \quad Q_{i,2} = (g^{\beta_2})^{s_i}, \\ Q'_i &= g^{t_i}, \quad T_i = E_i^{\hat{s}_i}. \end{aligned}$$

– if $i \geq \bar{i}$: set

$$\begin{aligned} \mathbf{R}_i &= G_i^{s_i \mathbf{v}_i}, \quad \mathbf{R}'_i = G_i^{\kappa s_i \mathbf{v}_i}, \quad Q_i = g^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}, \quad Q_{i,1} = (g^{\beta_1})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)} Z_i^{t_i} (g^{\beta_1})^\pi, \\ Q_{i,2} &= (g^{\beta_2})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}, \\ Q'_i &= g^{t_i}, \quad T_i = M \cdot E_i^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}. \end{aligned}$$

For each column $j \in [m]$:

– if $j < \bar{j}$: randomly choose $\mu_j \in \mathbb{Z}_N$, and set $\mathbf{C}_j = H_j^{\tau(\mathbf{v}_c + \mu_j \chi_3)} \cdot g^{\kappa \mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.
– if $j \geq \bar{j}$: set $\mathbf{C}_j = H_j^{\tau \mathbf{v}_c} \cdot g^{\kappa \mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

3. Output the ciphertext $CT_S = \langle S, (P_1, P_2, P_3, P_4, P_5, P_6), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q_{i,2}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$.
Decrypt_A(PP, CT_S , $\text{SK}_{(i,j),(A,\rho)}$) $\rightarrow M$ or \perp . Parse CT_S to $CT_S = \langle S, (P_1, P_2, P_3, P_4, P_5, P_6), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q_{i,2}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$ and $\text{SK}_{(i,j),(A,\rho)}$ to $\text{SK}_{(i,j),(A,\rho)} = ((i, j), (A, \rho), (K_0, K_1, K_2, \{K_{3,k}, K_{4,k}, K_{5,k,0}, \{K_{5,k,t}\}_{t \in [T]}\}_{k \in [l]}, K'_0))$. Suppose S satisfies (A, ρ) (if S does not satisfies (A, ρ) , output \perp).

1. Compute constants $\{\omega_k\}_{\rho(k) \in S}$ such that $\sum_{\rho(k) \in S} \omega_k A_k = (1, 0, \dots, 0)$. Let c_t be the coefficient of z^t in $p(z) := \prod_{x \in S} (z - x)$. Compute

$$\begin{aligned} D_P &\leftarrow e(K_1, P_3) / \prod_{\rho(k) \in S} \left(\frac{e(K_{3,k}, P_4) \cdot e(K_{5,k,0} \prod_{t=1}^T K_{5,k,t}^{c_t}, P_6)}{e(K_{4,k}, P_5)} \right)^{\omega_k} \\ &= e(K_1, P_3) / \prod_{\rho(k) \in S} \left(\frac{e(g^{A_k \cdot \mathbf{u}} h_4^{\xi_k}, g^{\bar{\pi}}) \cdot e((f_0 \prod_{t=0}^T f_{t+1}^{c_t})^{\xi_k}, g^{\bar{\pi}})}{e(g^{\xi_k}, h_4^{\bar{\pi}} (f_0 \prod_{t=0}^T f_{t+1}^{c_t})^{\bar{\pi}})} \right)^{\omega_k} \\ &= e(K_1, P_3) / \prod_{\rho(k) \in S} (e(g^{A_k \cdot \mathbf{u}}, g^{\bar{\pi}}))^{\omega_k} = e(g, g)^{a_1 \delta_1 \pi} e(g, g)^{a_3 \delta_1 \bar{\pi}} / e(g, g)^{a_3 \delta_1 \bar{\pi}} \\ &= e(g, g)^{a_1 \delta_1 \pi}. \end{aligned}$$

Note that D_P can be computed using 4 pairing computations, since $\prod_{\rho(k) \in S} (e(K_{3,k}, P_4))^{\omega_k}$ can be compute by $e(\prod_{\rho(k) \in S} K_{3,k}^{\omega_k}, P_4)$, and the same applies to two parts for P_5 and P_6 .

2. Compute

$$D_I \leftarrow \frac{e(K_0, Q_i) \cdot e(K'_0, Q'_i)}{e(K_1, Q_{i,1}) \cdot e(K_2, Q_{i,2})} \cdot \frac{e_3(\mathbf{R}'_i, \mathbf{C}'_j)}{e_3(\mathbf{R}_i, \mathbf{C}_j)}.$$

3. Computes $M \leftarrow T_i / (D_P \cdot D_I)$ as the output message.

D.2 Proof of Lemma 1

Proof. Suppose there exists a polynomial time adversary \mathcal{A} that selectively breaks the index-hiding game with advantage ϵ . We build a PPT algorithm \mathcal{B} to solve a Modified $(T+1, 1)$ -EDHE3 problem instance in a subgroup as follows. \mathcal{B} is given

$$D = \left((N, \mathbb{G}, \mathbb{G}_T, e), g, g^a, g^c, g^{c/z}, \underline{g^{ca^{T+1}/z} \text{ (for } g^{ca^n/z} \text{ with } n = T+1)}, g^d, \underline{g^{a^{T+1}}}, \right. \\ \left. \begin{array}{l} \forall_{i \in [2(T+1)]} g^{a^i c d}, \\ \forall_{i \in [2(T+1)], i \neq T+2} g^{a^i c/d}, \\ \forall_{i \in [T+2]} g^{a^i/d^2}, \\ \forall_{i \in [T+2, 2(T+1)]} g^{a^i c^2} \end{array} \right)$$

and T , where $(N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, e) \xleftarrow{R} \mathcal{G}$, $g \xleftarrow{R} \mathbb{G}_{p_1}$, $g_2 \xleftarrow{R} \mathbb{G}_{p_2}$, $g_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $a, c, z, d \xleftarrow{R} \mathbb{Z}_N$, and T is either equal to $g^{a^{T+2}z}$ or is a random element from \mathbb{G}_{p_1} . \mathcal{B} 's goal is to determine $T = g^{a^{T+2}z}$ or T is a random element from \mathbb{G}_{p_1} .

Init. \mathcal{A} gives \mathcal{B} the challenge attribute set $S^* = \{a_1^*, \dots, a_{l^*}^*\} \subseteq \mathbb{Z}_N$, where $|S^*| = l^* \leq T$.

Setup. \mathcal{B} randomly chooses $\{\alpha_i \in \mathbb{Z}_N\}_{i \in [m]}$, $\{r_i, z'_i \in \mathbb{Z}_N\}_{i \in [m] \setminus \{\bar{i}\}}$, $r'_i, z_i \in \mathbb{Z}_N$, $\{c'_j \in \mathbb{Z}_N\}_{j \in [m]}$, and $\beta'_1, \beta_2, \beta'_3, \beta'_4, \theta'_0, \theta'_1, \dots, \theta'_{T+1} \in \mathbb{Z}_N$. Let c_t^* be the coefficients of z^t in $p(z) = \prod_{x \in S^*} (z - x)$, \mathcal{B} gives \mathcal{A} the public parameter PP:

$$\left(g, h_1 = (g^{a^{T+1}})^{\beta'_1}, h_2 = g^{\beta_2}, h_3 = (g^{a^{T+1}})^{\beta'_3}, h_4 = (g^{a^{T+1}})^{\beta'_4}, \right. \\ f_0 = g^{\theta'_0} g^{a^{T+1}c/d} \prod_{t=0}^T (g^{a^{t+1}/d^2})^{-c_t^*}, \{f_t = g^{\theta'_t} g^{a^t/d^2}\}_{t=1}^{T+1}, \\ \{E_i = e(g, g)^{\alpha_i}\}_{i \in [m]}, \\ \{G_i = g^{r_i}, Z_i = (g^{a^{T+1}})^{z'_i}\}_{i \in [m] \setminus \{\bar{i}\}}, \{H_j = (g^{c/z})^{c'_j}\}_{j \in [m] \setminus \{\bar{j}\}}, G_{\bar{i}} = (g^{a^{T+1}})^{r'_i}, Z_{\bar{i}} = g^{z_i}, H_{\bar{j}} = (g^a)^{c'_j} \left. \right).$$

Note that \mathcal{B} implicitly chooses $r_{\bar{i}}, z_i (i \in [m] \setminus \{\bar{i}\})$, $c_j (j \in [m])$, $\beta_1, \beta_3, \beta_4, \beta_5, \beta_6 \in \mathbb{Z}_N$ such that

$$\begin{aligned} a^{T+1} r'_{\bar{i}} &\equiv r_{\bar{i}} \pmod{p_1}, \quad a^{T+1} z'_i \equiv z_i \pmod{p_1} \quad \forall i \in [m] \setminus \{\bar{i}\}, \\ a c'_j &\equiv c_j \pmod{p_1}, \quad (c/z) c'_j \equiv c_j \pmod{p_1} \quad \forall j \in [m] \setminus \{\bar{j}\}, \\ a^{T+1} \beta'_1 &\equiv \beta_1 \pmod{p_1}, \quad a^{T+1} \beta'_3 \equiv \beta_3 \pmod{p_1}, \quad a^{T+1} \beta'_4 \equiv \beta_4 \pmod{p_1}, \\ \theta'_0 + a^{T+1} c/d - \sum_{t=0}^T c_t^* (a^{t+1}/d^2) &\equiv \theta_0 \pmod{p_1}, \\ \forall t \in \{1, \dots, T+1\} : \theta'_t + a^t/d^2 &\equiv \theta_t \pmod{p_1}, \end{aligned}$$

Query Phase. To respond to \mathcal{A} 's query for $((i, j), (A, \rho))$, let $l \times n$ be the size of A ,

• if $(i, j) \neq (\bar{i}, \bar{j})$: \mathcal{B} picks random $\delta = (\delta_1, \delta_2, \xi_1, \dots, \xi_l, u_2, \dots, u_n) \in \mathbb{Z}_N^{l+n+1}$, $\mathbf{R} = (R_0, R_1, R_2, \{R_{3,k}, R_{4,k}, R_{5,k,0}, \{R_{5,k,t}\}_{t \in T}\}_{k \in [l]}) \in \mathbb{G}_{p_3}^{3+l(3+T)}$, and $R'_0 \in \mathbb{G}_{p_3}$. Implicitly setting $\mathbf{u} = (u_1 = \beta_3 \delta_1, u_2, \dots, u_n)$, \mathcal{B} creates a secret key $\text{SK}_{(i,j),(A,\rho)}$:

$$K_0 = \begin{cases} g^{\alpha_i} (g^{c/z})^{r_i c'_j} \cdot h_1^{\delta_1} h_2^{\delta_2} R_0, & : i \neq \bar{i}, j \neq \bar{j} \\ g^{\alpha_i} (g^{(a^{T+1}c)/z})^{r'_i c'_j} \cdot h_1^{\delta_1} h_2^{\delta_2} R_0, & : i = \bar{i}, j \neq \bar{j} \\ g^{\alpha_i} (g^a)^{r_i c'_j} \cdot h_1^{\delta_1} h_2^{\delta_2} R_0, & : i \neq \bar{i}, j = \bar{j}. \end{cases} \\ K_1 = g^{\delta_1} R_1, \quad K_2 = g^{\delta_2} \cdot R_2, \quad K'_0 = Z_i^{\delta_1} R'_0, \\ \{K_{3,k} = h_3^{A_{k,1} \delta_1} g^{\sum_{t=2}^n A_{k,t} u_t} h_4^{\xi_k} R_{3,k}, \quad K_{4,k} = g^{\xi_k} R_{4,k},$$

$$K_{5,k,0} = f_0^{\xi_k}, \{K_{5,k,t} = (f_{t+1} f_1^{-\rho(k)^t})^{\xi_k} R_{5,k,t}\}_{t \in [T]}\}_{k \in [l]}.$$

• if $(i, j) = (\bar{i}, \bar{j})$: it implies that \mathcal{A} is querying a secret key with the challenge index (\bar{i}, \bar{j}) , and (A, ρ) is not satisfied by S^* . \mathcal{B} first computes a vector $\bar{\mathbf{u}} = (\bar{u}_1, \dots, \bar{u}_n) \in \mathbb{Z}_N^n$ that has first entry equal to 1 (i.e. $\bar{u}_1 = 1$) and is orthogonal to all of the rows A_k of A such that $\rho(k) \in S^*$ (i.e. $A_k \cdot \bar{\mathbf{u}} = 0 \forall k \in [l]$ s.t. $\rho(k) \in S^*$). Note that such a vector must exist since S^* fails to satisfy (A, ρ) , and it is efficiently computable. \mathcal{B} picks random $\delta'_1, \delta_2, \{\xi_k\}_{k \in [l]}$ s.t. $\rho(k) \in S^*$, $\{\xi'_k\}_{k \in [l]}$ s.t. $\rho(k) \notin S^*$, $u'_2, \dots, u'_n \in \mathbb{Z}_N$, $\mathbf{R} = (R_0, R_1, R_2, \{R_{3,k}, R_{4,k}, R_{5,k,0}, \{R_{5,k,t}\}_{t \in [T]}\}_{k \in [l]}) \in \mathbb{G}_{p_3}^{3+1(3+T)}$, and $R'_0 \in \mathbb{G}_{p_3}$. Let $\mathbf{u}' = (0, u'_2, \dots, u'_n) \in \mathbb{Z}_N^n$, \mathcal{B} sets the values of $\delta_1 \in \mathbb{Z}_N$, $\mathbf{u} \in \mathbb{Z}_N^n$, $\{\xi_k \in \mathbb{Z}_N\}_{k \in [l]}$ s.t. $\rho(k) \notin S^*$ by implicitly setting

$$\delta'_1 - ar'_i c'_j / \beta'_1 \equiv \delta_1 \pmod{p_1}, \quad \mathbf{u} = \mathbf{u}' + (a^{T+1} \beta'_3) \delta_1 \bar{\mathbf{u}},$$

$$\xi'_k + \left(a + \frac{1}{p(\rho(k))} \sum_{t=0}^T \rho(k)^t cda^{T+1-t}\right) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4) \equiv \xi_k \pmod{p_1} \quad \forall k \in [l] \text{ s.t. } \rho(k) \notin S^*.$$

Note that for $\rho(k) \notin S^*$ we have $p(\rho(k)) \neq 0$. \mathcal{B} creates a secret key $\text{SK}_{(\bar{i}, \bar{j}), (A, \rho)}$ as follows:

$$K_0 = g^{\alpha_{\bar{i}}} h_1^{\delta_1} h_2^{\delta_2} R_0, \quad K_1 = g^{\delta'_1} (g^a)^{-r'_i c'_j / \beta'_1} R_1, \quad K_2 = g^{\delta_2} R_2, \quad K'_0 = (K_1)^{z_i} R'_0,$$

• for $k \in [l]$ s.t. $\rho(k) \in S^*$,

$$K_{3,k} = g^{(A_k \cdot \mathbf{u})} h_4^{\xi_k} R_{3,k} = g^{(A_k \cdot \mathbf{u}') + a^{T+1} \beta'_3 \delta_1 (A_k \cdot \bar{\mathbf{u}})} h_4^{\xi_k} R_{3,k} = g^{(A_k \cdot \mathbf{u}')} h_4^{\xi_k} R_{3,k},$$

$$K_{4,k} = g^{\xi_k} R_{4,k}, \quad K_{5,k,0} = f_0^{\xi_k}, \quad \{K_{5,k,t} = (f_{t+1} f_1^{-\rho(k)^t})^{\xi_k} R_{5,k,t}\}_{t \in [T]},$$

• for $k \in [l]$ s.t. $\rho(k) \notin S^*$,

$$\begin{aligned} K_{3,k} &= g^{(A_k \cdot \mathbf{u})} h_4^{\xi_k} R_{3,k} \\ &= g^{(A_k \cdot \mathbf{u}')} \cdot g^{a^{T+1} \beta'_3 (\delta'_1 - ar'_i c'_j / \beta'_1) (A_k \cdot \bar{\mathbf{u}})} \\ &\quad \cdot h_4^{\xi'_k} \cdot (g^{a^{T+1} \beta'_4})^{a \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot (g^{a^{T+1} \beta'_4})^{(\sum_{t=0}^T \frac{a^{T+1-t} c d \rho(k)^t}{p(\rho(k))}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} R_{3,k} \\ &= g^{(A_k \cdot \mathbf{u}')} \cdot g^{a^{T+1} \beta'_3 \delta'_1 (A_k \cdot \bar{\mathbf{u}})} \cdot h_4^{\xi'_k} \cdot (g^{\sum_{t=0}^T \frac{a^{2T+2-t} c d \rho(k)^t}{p(\rho(k))}})^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / \beta'_1} R_{3,k} \\ &= g^{(A_k \cdot \mathbf{u}')} \cdot (g^{a^{T+1}})^{\beta'_3 \delta'_1 (A_k \cdot \bar{\mathbf{u}})} \cdot h_4^{\xi'_k} \cdot \left(\prod_{t=0}^T (g^{a^{2T+2-t} c d})^{\frac{\rho(k)^t}{p(\rho(k))}}\right)^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / \beta'_1} R_{3,k}, \\ K_{4,k} &= g^{\xi_k} R_{4,k} = g^{\xi'_k + \left(a + \frac{1}{p(\rho(k))} \sum_{t=0}^T \rho(k)^t cda^{T+1-t}\right) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} R_{4,k} \\ &= g^{\xi'_k} \cdot (g^a)^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \left(\prod_{t=0}^T (g^{a^{T+1-t} c d})^{\frac{\rho(k)^t}{p(\rho(k))}}\right)^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} R_{4,k}, \\ K_{5,k,0} &= f_0^{\xi_k} R_{5,k,0} \\ &= f_0^{\xi'_k} \cdot (g^{\theta'_0} g^{a^{T+1} c/d} \prod_{i=0}^T (g^{a^{i+1}/d^2})^{-c_i^*})^{a \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \\ &\quad \cdot (g^{\theta'_0} g^{a^{T+1} c/d} \prod_{i=0}^T (g^{a^{i+1}/d^2})^{-c_i^*})^{(\sum_{t=0}^T \frac{a^{T+1-t} c d \rho(k)^t}{p(\rho(k))}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} R_{5,k,0} \\ &= \underbrace{f_0^{\xi'_k} \cdot ((g^a)^{\theta'_0})^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}}_{\Psi_1} \cdot (g^{a^{T+2} c/d})^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \underbrace{\left(\prod_{i=0}^T (g^{a^{i+2}/d^2})^{-c_i^*}\right)^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}}_{\Psi_2} \end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left(\prod_{t=0}^T (g^{a^{T+1-t}cd})^{\frac{\rho(k)^t}{p(\rho(k))}} \right) \theta'_0 \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}_{\Psi_3} \\
& \cdot \underbrace{\left(\prod_{t=0}^T (g^{a^{2T+2-t}c^2})^{\frac{\rho(k)^t}{p(\rho(k))}} \right) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}_{\Psi_4} \\
& \cdot \left(\prod_{t=0}^T \prod_{i=0}^T (g^{a^{T+i+2-t}c/d})^{\frac{-c_i^* \rho(k)^t}{p(\rho(k))}} \right) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4) R_{5,k,0} \\
= & \Psi_1 \cdot (g^{a^{T+2}c/d})^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)} \cdot \Psi_2 \cdot \Psi_3 \cdot \Psi_4 \\
& \cdot \underbrace{\left(\prod_{t=0}^T \prod_{i \in [0, T] \setminus \{t\}} (g^{a^{T+i+2-t}c/d})^{\frac{-c_i^* \rho(k)^t}{p(\rho(k))}} \right) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}_{\Psi_5, \text{ for } i \neq t} \\
& \cdot \underbrace{\left(\prod_{t=0}^T (g^{a^{T+t+2-t}c/d})^{\frac{-c_i^* \rho(k)^t}{p(\rho(k))}} \right) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}_{\text{for } i=t} R_{5,k,0} \\
= & \Psi_1 \cdot \underbrace{(g^{a^{T+2}c/d})^{\beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}}_{\Delta} \cdot \Psi_2 \cdot \Psi_3 \cdot \Psi_4 \cdot \Psi_5 \\
& \cdot \underbrace{\left((g^{a^{T+2}c/d})^{\frac{-\sum_{i=0}^T c_i^* \rho(k)^t}{p(\rho(k))}} \right) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}_{\Delta^{-1}, \text{ since } \sum_{t=0}^T c_t^* \rho(k)^t = p(\rho(k))} R_{5,k,0} \\
= & \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \Psi_4 \cdot \Psi_5 \cdot R_{5,k,0}, \\
K_{5,k,t} = & (f_{t+1} f_1^{-\rho(k)^t})^{\xi_k} R_{5,k,t} \quad \forall t \in [1, T] \\
= & \underbrace{(f_{t+1} f_1^{-\rho(k)^t})^{\xi_k}}_{\Psi_6} \cdot (g^{\theta'_{t+1}} g^{a^{t+1}/d^2} (g^{\theta'_t} g^{a/d^2} - \rho(k)^t)^{\left(a + \frac{1}{p(\rho(k))} \sum_{i=0}^T \rho(k)^i cda^{T+1-i}\right)}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4) R_{5,k,t} \\
= & \Psi_6 \cdot (g^{\theta'_{t+1} - \theta'_t \rho(k)^t} g^{a^{t+1}/d^2} (g^{a/d^2} - \rho(k)^t)^a \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4) \\
& \cdot (g^{\theta'_{t+1} - \theta'_t \rho(k)^t} g^{a^{t+1}/d^2} (g^{a/d^2} - \rho(k)^t)^{\left(\frac{1}{p(\rho(k))} \sum_{i=0}^T \rho(k)^i cda^{T+1-i}\right)}) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4) R_{5,k,t} \\
= & \Psi_6 \cdot \underbrace{\left((g^a)^{\theta'_{t+1} - \theta'_t \rho(k)^t} \cdot g^{a^{t+2}/d^2} \cdot (g^{a^2/d^2} - \rho(k)^t) \right) \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}_{\Psi_7} \\
& \cdot \underbrace{\left(\prod_{i=0}^T (g^{cda^{T+1-i}} \rho(k)^i) \right)^{\frac{\theta'_{t+1} - \theta'_t \rho(k)^t}{p(\rho(k))}} \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4)}_{\Psi_8} \\
& \cdot \left(\prod_{i=0}^T (g^{a^{T+2+t-i}c/d} \rho(k)^i) \right)^{\frac{1}{p(\rho(k))}} \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4) \\
& \cdot \left(\sum_{i=0}^T (g^{a^{T+2-i}c/d} - \rho(k)^i) \right)^{\frac{\rho(k)^t}{p(\rho(k))}} \beta'_3 r'_i c'_j (A_k \cdot \bar{\mathbf{u}}) / (\beta'_1 \beta'_4) R_{5,k,t} \\
= & \Psi_6 \cdot \Psi_7 \cdot \Psi_8
\end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left(\prod_{i \in [0, T] \setminus \{t\}} (g^{a^{T+2+t-i} c/d})^{\rho(k)^i} \right)^{\frac{1}{p(\rho(k))}} \beta_3' r_i' c_j' (A_k \cdot \bar{\mathbf{u}}) / (\beta_1' \beta_4')}_{\Psi_9, \text{ for } i \neq t} \cdot \underbrace{\left((g^{a^{T+2+t-t} c/d})^{\rho(k)^t} \right)^{\frac{1}{p(\rho(k))}} \beta_3' r_i' c_j' (A_k \cdot \bar{\mathbf{u}}) / (\beta_1' \beta_4')}_{\text{for } i=t} \\
& \cdot \underbrace{\left(\sum_{i=1}^T (g^{a^{T+2-i} c/d})^{-\rho(k)^i} \right)^{\frac{\rho(k)^t}{p(\rho(k))}} \beta_3' r_i' c_j' (A_k \cdot \bar{\mathbf{u}}) / (\beta_1' \beta_4')}_{\Psi_{10}, \text{ for } i \neq 0} \cdot \underbrace{\left((g^{a^{T+2-0} c/d})^{-\rho(k)^0} \right)^{\frac{\rho(k)^t}{p(\rho(k))}} \beta_3' r_i' c_j' (A_k \cdot \bar{\mathbf{u}}) / (\beta_1' \beta_4')}_{\text{for } i=0} R_{5,k,t} \\
& = \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \Psi_{10} \cdot R_{5,k,t}.
\end{aligned}$$

Note that \mathcal{B} can calculate the values of $K_0, K_1, K_2, K_0', \{K_{3,k}, K_{4,k}, K_{5,k,0}, \{K_{5,k,t}\}_{t \in [T]}\}_{k \in [l]}$ using the suitable terms of the assumption.

Challenge. \mathcal{A} submits a message M . \mathcal{B} randomly chooses

$$\begin{aligned}
\tau', s_1, \dots, s_{\bar{i}-1}, s_{\bar{i}}, s_{\bar{i}+1}, \dots, s_m, t'_1, \dots, t'_{\bar{i}-1}, t_{\bar{i}}, t'_{\bar{i}+1}, \dots, t'_m & \in \mathbb{Z}_N, \\
\mathbf{w}_1, \dots, \mathbf{w}_{\bar{j}-1}, \mathbf{w}'_{\bar{j}}, \dots, \mathbf{w}'_m & \in \mathbb{Z}_N^3, \\
\pi', \bar{\pi}', \pi'_{a_1^*}, \dots, \pi'_{a_i^*} & \in \mathbb{Z}_N.
\end{aligned}$$

\mathcal{B} randomly chooses $r_x, r_y, r_z \in \mathbb{Z}_N$, and sets $\chi_1 = (r_x, 0, r_z), \chi_2 = (0, r_y, r_z), \chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$. \mathcal{B} randomly chooses

$$\begin{aligned}
\mathbf{v}_i & \in \mathbb{Z}_N^3 \quad \forall i \in \{1, \dots, \bar{i} - 1\}, \\
\mathbf{v}_i^p & \in \text{span}\{\chi_1, \chi_2\}, \quad \mathbf{v}_i^q \in \text{span}\{\chi_3\}, \\
\mathbf{v}_i & \in \text{span}\{\chi_1, \chi_2\} \quad \forall i \in \{\bar{i} + 1, \dots, m\}, \\
\mathbf{v}_c & \in \text{span}\{\chi_1, \chi_2\}, \quad \mathbf{v}_c^q = \nu_3 \chi_3 \in \text{span}\{\chi_3\}.
\end{aligned}$$

\mathcal{B} sets the value of $\kappa, \tau, s_{\bar{i}}, t_i (i \in [m] \setminus \{\bar{i}\}) \in \mathbb{Z}_N, \mathbf{v}_c, \mathbf{v}_{\bar{i}} \in \mathbb{Z}_N^3, \{\mathbf{w}_j \in \mathbb{Z}_N^3\}_{j=\bar{j}}^m, \pi, \bar{\pi}, \hat{\pi}' \in \mathbb{Z}_N$ by implicitly setting

$$\begin{aligned}
a^{T+1} & \equiv \kappa \pmod{p_1}, \quad a^{T+1} z \tau' \equiv \tau \pmod{p_1}, \quad s_{\bar{i}}' / a^{T+1} \equiv s_{\bar{i}} \pmod{p_1}, \\
t'_i + c \beta_1' \tau' s_{\bar{i}}' (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i & \equiv t_i \pmod{p_1} \quad \forall i \in \{1, \dots, \bar{i} - 1\}, \\
t'_i - a^{T+1} \beta_1' \tau' s_i (\mathbf{v}_i \cdot \mathbf{v}_c^p) / z'_i + c \beta_1' \tau' s_{\bar{i}}' (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i & \equiv t_i \pmod{p_1} \quad \forall i \in \{\bar{i} + 1, \dots, m\}, \\
\mathbf{v}_c & = z^{-1} \mathbf{v}_c^p + \mathbf{v}_c^q, \quad \mathbf{v}_{\bar{i}} = \mathbf{v}_{\bar{i}}^p + \frac{c}{z} \mathbf{v}_{\bar{i}}^q, \\
\mathbf{w}'_{\bar{j}} - a c_{\bar{j}}' \tau' \mathbf{v}_c^p & \equiv \mathbf{w}_{\bar{j}} \pmod{p_1}, \\
\mathbf{w}'_{\bar{j}} - c c_{\bar{j}}' \tau' \mathbf{v}_c^q & \equiv \mathbf{w}_{\bar{j}} \pmod{p_1} \quad \forall j \in \{\bar{j} + 1, \dots, m\}, \\
\pi' - c \tau' s_{\bar{i}}' (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) & \equiv \pi \pmod{p_1}, \quad \bar{\pi}' + c \beta_1' \tau' s_{\bar{i}}' (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) / \beta_3' \equiv \bar{\pi} \pmod{p_1}, \\
\hat{\pi}' - d \beta_1' \beta_4' \tau' s_{\bar{i}}' (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) / \beta_3' & \equiv \hat{\pi} \pmod{p_1}.
\end{aligned}$$

It is worth noticing that $\mathbf{v}_{\bar{i}}$ and \mathbf{v}_c are random vectors in \mathbb{Z}_N^3 as required, and $(\mathbf{v}_{\bar{i}} \cdot \mathbf{v}_c) = \frac{1}{z} (\mathbf{v}_{\bar{i}}^p \cdot \mathbf{v}_c^p) + \frac{c}{z} (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q)$, since χ_3 is orthogonal to $\text{span}\{\chi_1, \chi_2\}$ and $\mathbb{Z}_N^3 = \text{span}\{\chi_1, \chi_2, \chi_3\}$.

\mathcal{B} creates a ciphertext $\langle S^*, (P_1, P_2, P_3, P_4, P_5, P_6), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q'_i, Q''_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$ as follows:

$$1. P_1 = g^{\pi'} (g^c)^{-\tau' s_{\bar{i}}' (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q)}, \quad P_2 = (P_1)^{\beta_2}, \quad P_3 = h_1^{\pi'} h_3^{\hat{\pi}'}, \quad P_4 = g^{\bar{\pi}'} (g^c)^{\beta_1' \tau' s_{\bar{i}}' (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) / \beta_3'}$$

$$\begin{aligned}
P_5 & = h_4^{\bar{\pi}'} (f_0 \prod_{t=0}^T f_{t+1}^{c_t^*})^{\hat{\pi}'} \\
& = h_4^{\bar{\pi}' + c \beta_1' \tau' s_{\bar{i}}' (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) / \beta_3'} \cdot (g^{\theta'_0} g^{a^{T+1} c/d} \prod_{t'=0}^T (g^{a^{t'+1}/d^2})^{-c_{t'}^*}) \cdot \prod_{t=0}^T (g^{\theta'_{t+1}} g^{a^{t+1}/d^2})^{c_t^*})^{\hat{\pi}' - d \beta_1' \beta_4' \tau' s_{\bar{i}}' (\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q) / \beta_3'}
\end{aligned}$$

$$\begin{aligned}
&= h_4^{\hat{\pi}'} \cdot (g^{a^{T+1}c/d})^{c\beta_1'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \cdot (g^{\theta'_0} g^{a^{T+1}c/d} \cdot \prod_{t=0}^T (g^{\theta'_{t+1}c_t^*})^{\hat{\pi}' - d\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'}) \\
&= h_4^{\hat{\pi}'} \cdot (g^{a^{T+1}c})^{\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \cdot (g^{\theta'_0} \prod_{t=0}^T g^{\theta'_{t+1}c_t^*})^{\hat{\pi}' - d\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \\
&\quad \cdot (g^{a^{T+1}c/d})^{\hat{\pi}' - d\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \\
&= h_4^{\hat{\pi}'} \cdot (g^{a^{T+1}c})^{\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \cdot (g^{\theta'_0} \prod_{t=0}^T g^{\theta'_{t+1}c_t^*})^{\hat{\pi}'} \cdot ((g^d)^{\theta'_0} \prod_{t=0}^T (g^d)^{\theta'_{t+1}c_t^*})^{-\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \\
&\quad \cdot (g^{a^{T+1}c/d})^{\hat{\pi}'} \cdot (g^{a^{T+1}c})^{-\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \\
&= h_4^{\hat{\pi}'} \cdot (g^{\theta'_0} \prod_{t=0}^T g^{\theta'_{t+1}c_t^*})^{\hat{\pi}'} \cdot ((g^d)^{\theta'_0} \prod_{t=0}^T (g^d)^{\theta'_{t+1}c_t^*})^{-\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \cdot (g^{a^{T+1}c/d})^{\hat{\pi}'} \\
P_6 &= g^{\hat{\pi}'} = g^{\hat{\pi}' - d\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'} \\
&= g^{\hat{\pi}'} (g^d)^{-\beta_1'\beta_4'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/\beta_3'}.
\end{aligned}$$

2. For each $i \in [m]$:

– if $i < \bar{i}$: it randomly chooses $\hat{s}_i \in \mathbb{Z}_p$, then sets

$$\begin{aligned}
\mathbf{R}_i &= g^{\mathbf{v}_i}, \quad \mathbf{R}'_i = (g^{a^{T+1}})^{\mathbf{v}_i}, \quad Q_i = g^{s_i}, \quad Q_{i,1} = h_1^{s_i} Z_i^{t_i} h_1^{\hat{\pi}'}, \\
Q_{i,2} &= (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i} (g^c)^{\beta_1'\tau's'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/z'_i}, \quad T_i = E_i^{\hat{s}_i}.
\end{aligned}$$

– if $i = \bar{i}$: it sets

$$\begin{aligned}
\mathbf{R}_i &= g^{r'_i s'_i \mathbf{v}_i^p} (g^{c/z})^{r'_i s'_i \mathbf{v}_i^q}, \quad \mathbf{R}'_i = (g^{a^{T+1}})^{r'_i s'_i \mathbf{v}_i^p} (g^{a^{T+1}c/z})^{r'_i s'_i \mathbf{v}_i^q}, \quad Q_i = g^{\tau' s'_i (\mathbf{v}_i^p \cdot \mathbf{v}_c^p)} (g^c)^{\tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}, \\
Q_{i,1} &= h_1^{\tau' s'_i (\mathbf{v}_i^p \cdot \mathbf{v}_c^p)} Z_i^{t_i} h_1^{\hat{\pi}'}, \quad Q_{i,2} = (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i}, \quad T_i = M \cdot e(g^{\alpha_i}, Q_i).
\end{aligned}$$

– if $i > \bar{i}$: it sets

$$\begin{aligned}
\mathbf{R}_i &= g^{r_i s_i \mathbf{v}_i}, \quad \mathbf{R}'_i = (g^{a^{T+1}})^{r_i s_i \mathbf{v}_i}, \quad Q_i = (g^{a^{T+1}})^{\tau' s_i (\mathbf{v}_i \cdot \mathbf{v}_c^p)}, \quad Q_{i,1} = Z_i^{t_i} h_1^{\hat{\pi}'}, \\
Q_{i,2} &= (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i} (g^{a^{T+1}})^{-\beta_1'\tau' s_i (\mathbf{v}_i \cdot \mathbf{v}_c^p)/z'_i} (g^c)^{\beta_1'\tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q)/z'_i}, \quad T_i = M \cdot e(g^{\alpha_i}, Q_i).
\end{aligned}$$

3. For each $j \in [m]$:

- if $j < \bar{j}$: it randomly chooses $\mu'_j \in \mathbb{Z}_N$ and implicitly sets the value of μ_j such that $(a^{T+1}c)^{-1} \mu'_j \nu_3 - \nu_3 \equiv \mu_j \pmod{p_1}$, then sets $\mathbf{C}_j = (g^{(a^{T+1}c)/z})^{c'_j \tau' \mathbf{v}_c^p} \cdot g^{c'_j \tau' \mu'_j \mathbf{v}_c^q} \cdot (g^{a^{T+1}})^{\mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.
- if $j = \bar{j}$: it sets $\mathbf{C}_j = T^{c'_j \tau' \mathbf{v}_c^q} \cdot (g^{a^{T+1}})^{\mathbf{w}'_j}$, $\mathbf{C}'_j = g^{\mathbf{w}'_j} \cdot (g^a)^{-c'_j \tau' \mathbf{v}_c^p}$.
- if $j > \bar{j}$: it sets $\mathbf{C}_j = (g^{(a^{T+1}c)/z})^{c'_j \tau' \mathbf{v}_c^p} \cdot (g^{a^{T+1}})^{\mathbf{w}'_j}$, $\mathbf{C}'_j = g^{\mathbf{w}'_j} \cdot (g^c)^{-c'_j \tau' \mathbf{v}_c^q}$.

If $T = g^{a^{T+2}z}$, then the ciphertext is a well-formed encryption to the index (\bar{i}, \bar{j}) . If T is randomly chosen, say $T = g^r$ for some random $r \in \mathbb{Z}_{p_1}$, the ciphertext is a well-formed encryption to the index $(\bar{i}, \bar{j} + 1)$ with implicitly setting $\mu_{\bar{j}}$ such that $(\frac{r}{a^{T+2}z} - 1) \nu_3 \equiv \mu_{\bar{j}} \pmod{p_1}$.

Guess. \mathcal{A} outputs a guess $b' \in \{0, 1\}$ to \mathcal{B} , then \mathcal{B} outputs this b' to the challenger.

The distributions of the public parameters, secret keys and challenge ciphertext are the same as that in the real scheme. \mathcal{B} 's advantage in the Modified $(T+1, 1)$ -EDHE3 game will be exactly equal to \mathcal{A} 's advantage in the selective index-hiding game.

E Proof of the Lemma 1 for the Fully Secure ABE with Ciphertexts Associated with DFAs

To make the proof easy to follow, we present the details of the resulting AugABE scheme first.

E.1 The Resulting Augmented ABE with Ciphertexts Associated with DFAs

$\text{Setup}_A(\lambda, \mathcal{U}, \mathcal{K} = m^2) \rightarrow (\text{PP}, \text{MSK})$. Run $\mathcal{G}(\lambda)$ to get $(N, p_1, p_2, p_3, \mathbb{G}, \mathbb{G}_T, e)$. Pick generators $g \in \mathbb{G}_{p_1}$, $X_3 \in \mathbb{G}_{p_3}$. Set $d = 9, d_0 = 2$. Pick random $\beta = (\beta_1, \dots, \beta_9) \in \mathbb{Z}_N^9$. Pick random $\{\alpha_i, r_i, z_i \in \mathbb{Z}_N\}_{i \in [m]}$, $\{c_j \in \mathbb{Z}_N\}_{j \in [m]}$. The public parameter is

$$\text{PP} = \left((N, \mathbb{G}, \mathbb{G}_T, e), g, \mathbf{h} = (h_1 = g^{\beta_1}, \dots, h_9 = g^{\beta_9}), X_3, \{E_i = e(g, g)^{\alpha_i}, G_i = g^{r_i}, Z_i = g^{z_i}\}_{i \in [m]}, \{H_j = g^{c_j}\}_{j \in [m]} \right).$$

The master secret key is $\text{MSK} = (\alpha_1, \dots, \alpha_m, r_1, \dots, r_m, c_1, \dots, c_m)$.

A counter $ctr = 0$ is implicitly included in MSK .

$\text{KeyGen}_A(\text{PP}, \text{MSK}, \mathbf{u} \in (\mathbb{Z}_N)^*) \rightarrow \text{SK}_{(i,j),\mathbf{u}}$. Set $ctr = ctr + 1$ and compute the corresponding index in the form of (i, j) where $1 \leq i, j \leq m$ and $(i-1) * m + j = ctr$. Let $l = |\mathbf{u}|$, and parse $\mathbf{u} = (u_1, \dots, u_l)$. Pick random $\delta = (\delta_1, \delta_2, \xi_0, \xi_1, \dots, \xi_l) \in \mathbb{Z}_N^{3+l}$, $\mathbf{R} = (R_0, R_1, \dots, R_4, R_{5,0}, \{R_{5,k}, R_{6,k}\}_{k \in [l]}) \in \mathbb{G}_{p_3}^{6+2l}$, and $R'_0 \in \mathbb{G}_{p_3}$. Output a secret key $\text{SK}_{(i,j),\mathbf{u}}$ as

$$\begin{aligned} \text{SK}_{(i,j),\mathbf{u}} &= \left((i, j), \mathbf{u}, \right. \\ &K_0 = g^{r_i c_j + \alpha_i} h_1^{\delta_1} h_2^{\delta_2} \cdot R_0, \quad K_1 = g^{\delta_1} \cdot R_1, \quad K_2 = g^{\delta_2} \cdot R_2, \\ &K_3 = h_3^{-\delta_1} h_4^{\xi_1} \cdot R_3, \quad K_4 = h_5^{\xi_0} \cdot R_4, \quad K_{5,0} = g^{\xi_0} \cdot R_{5,0}, \\ &\{K_{5,k} = g^{\xi_k} \cdot R_{5,k}, \quad K_{6,k} = (h_6 h_7^{u_k})^{\xi_{k-1}} (h_8 h_9^{u_k})^{\xi_k} \cdot R_{6,k}\}_{k \in [l]}, \\ &K'_0 = Z_i^{\delta_1} \cdot R'_0 \left. \right). \end{aligned}$$

$\text{Encrypt}_A(\text{PP}, M, \mathbb{M}, (\bar{i}, \bar{j})) \rightarrow CT_{\mathbb{M}}$.

1. For any DFA $\mathbb{M} = (Q, \mathbb{Z}_N, \mathcal{J}, q_0, F = \{q_{n-1}\})$ where $n = |Q|$, let $J = |\mathcal{J}|$, and parse $\mathcal{J} = \{(q_{x_t}, q_{y_t}, \sigma_t) | t \in [1, J]\}$. Pick random $\pi = (\pi, \bar{\pi}, \pi_0, \pi_1, \dots, \pi_J, \{\nu_x\}_{q_x \in Q \setminus \{q_{n-1}\}}) \in \mathbb{Z}_N^{2+J+n}$ and implicitly set $\nu_{n-1} := \beta_4 \bar{\pi}$. Set

$$\begin{aligned} P_1 &= g^\pi, & P_2 &= g^{\beta_2 \pi}, & P_3 &= g^{\beta_1 \pi} g^{\beta_3 \bar{\pi}}, \\ P_4 &= g^{\bar{\pi}}, & P_5 &= g^{\pi_0}, & P_6 &= g^{-\nu_0} h_5^{\pi_0}, \\ \{P_{7,t} &= g^{\pi_t}, \quad P_{8,t} = g^{\nu_{x_t}} (h_6 h_7^{\sigma_t})^{\pi_t}, \quad P_{9,t} = g^{-\nu_{y_t}} (h_8 h_9^{\sigma_t})^{\pi_t}\}_{t \in [1, J]}. \end{aligned}$$

Note that for $t \in [1, J]$, if $x_t = n-1$, then $P_{8,t}$ is computed as $P_{8,t} = h_4^{\bar{\pi}} (h_6 h_7^{\sigma_t})^{\pi_t}$; if $y_t = n-1$, then $P_{9,t}$ is computed as $P_{9,t} = h_4^{-\bar{\pi}} (h_8 h_9^{\sigma_t})^{\pi_t}$.

2. Pick random

$$\begin{aligned} \kappa, \tau, s_1, \dots, s_m, t_1, \dots, t_m &\in \mathbb{Z}_N, \\ \mathbf{v}_c, \mathbf{w}_1, \dots, \mathbf{w}_m &\in \mathbb{Z}_N^3. \end{aligned}$$

Pick random $r_x, r_y, r_z \in \mathbb{Z}_N$, and set $\chi_1 = (r_x, 0, r_z)$, $\chi_2 = (0, r_y, r_z)$, $\chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$. Pick random

$$\begin{aligned} \mathbf{v}_i &\in \mathbb{Z}_N^3 \quad \forall i \in \{1, \dots, \bar{i}\}, \\ \mathbf{v}_i &\in \text{span}\{\chi_1, \chi_2\} \quad \forall i \in \{\bar{i} + 1, \dots, m\}. \end{aligned}$$

For each row $i \in [m]$:

– if $i < \bar{i}$: randomly choose $\hat{s}_i \in \mathbb{Z}_p$, and set

$$\begin{aligned} \mathbf{R}_i &= g^{v_i}, \quad \mathbf{R}'_i = g^{\kappa v_i}, \quad Q_i = g^{s_i}, \quad Q_{i,1} = (g^{\beta_1})^{s_i} Z_i^{t_i} (g^{\beta_1})^\pi, \quad Q_{i,2} = (g^{\beta_2})^{s_i}, \\ Q'_i &= g^{t_i}, \quad T_i = E_i^{\hat{s}_i}. \end{aligned}$$

– if $i \geq \bar{i}$: set

$$\begin{aligned} \mathbf{R}_i &= G_i^{s_i v_i}, \quad \mathbf{R}'_i = G_i^{\kappa s_i v_i}, \quad Q_i = g^{\tau s_i (v_i \cdot v_c)}, \quad Q_{i,1} = (g^{\beta_1})^{\tau s_i (v_i \cdot v_c)} Z_i^{t_i} (g^{\beta_1})^\pi, \quad Q_{i,2} = (g^{\beta_2})^{\tau s_i (v_i \cdot v_c)}, \\ Q'_i &= g^{t_i}, \quad T_i = M \cdot E_i^{\tau s_i (v_i \cdot v_c)}. \end{aligned}$$

For each column $j \in [m]$:

– if $j < \bar{j}$: randomly choose $\mu_j \in \mathbb{Z}_p$, and set $\mathbf{C}_j = H_j^{\tau(v_c + \mu_j \chi_3)} \cdot g^{\kappa w_j}$, $\mathbf{C}'_j = g^{w_j}$.
– if $j \geq \bar{j}$: set $\mathbf{C}_j = H_j^{\tau v_c} \cdot g^{\kappa w_j}$, $\mathbf{C}'_j = g^{w_j}$.

3. Output the ciphertext $CT_{\mathbb{M}} = \langle \mathbb{M}, (P_1, P_2, P_3, P_4, P_5, P_6, \{P_{7,t}, P_{8,t}, P_{9,t}\}_{t \in [1, J]}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q_{i,2}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$.

Decrypt_A(PP, $CT_{\mathbb{M}}$, $\text{SK}_{(i,j), \mathbf{u}}$) $\rightarrow M$ or \perp . Parse $CT_{\mathbb{M}}$ to $CT_{\mathbb{M}} = \langle \mathbb{M}, (P_1, P_2, P_3, P_4, P_5, P_6, \{P_{7,t}, P_{8,t}, P_{9,t}\}_{t \in [1, J]}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q_{i,2}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$ and $\text{SK}_{(i,j), \mathbf{u}}$ to $\text{SK}_{(i,j), \mathbf{u}} = ((i, j), \mathbf{u}, (K_0, K_1, K_2, K_3, K_4, K_5, 0, \{K_{5,k}, K_{6,k}\}_{k \in [1, l]}, K'_0))$, where $\mathbb{M} = (Q, \mathbb{Z}_N, \mathcal{J}, q_0, F = \{q_{n-1}\})$ with $n = |Q|$, $J = |\mathcal{J}|$, $\mathcal{J} = \{q_{x_t}, q_{y_t}, \sigma_t\}_{t \in [1, J]}$, and $\mathbf{u} = (u_1, \dots, u_l)$. Suppose \mathbb{M} accepts \mathbf{u} (if \mathbb{M} does not accept \mathbf{u} , output \perp).

1. Find a sequence of states $\rho_0, \rho_1, \dots, \rho_l \in Q$ such that $\rho_0 = q_0$, for $k = 1$ to l we have $(\rho_{k-1}, \rho_k, u_k) \in \mathcal{J}$, and $\rho_l \in F$. Let $(q_{x_{t_k}}, q_{y_{t_k}}, \sigma_{t_k}) = (\rho_{k-1}, \rho_k, u_k)$. Compute

$$\begin{aligned} D_T &\leftarrow \prod_{k \in [1, l]} \frac{e(K_{5, k-1}, P_{8, t_k}) \cdot e(K_{5, k}, P_{9, t_k})}{e(K_{6, k}, P_{7, t_k})} \\ &= \prod_{k \in [1, l]} \frac{e(g^{\xi_{k-1}}, g^{\nu_{x_{t_k}}} (h_6 h_7^{\sigma_{t_k}})^{\pi_{t_k}}) \cdot e(g^{\xi_k}, g^{-\nu_{y_{t_k}}} (h_8 h_9^{\sigma_{t_k}})^{\pi_{t_k}})}{e((h_6 h_7^{u_k})^{\xi_{k-1}} (h_8 h_9^{u_k})^{\xi_k}, g^{\pi_{t_k}})} \\ &= \prod_{k \in [1, l]} e(g^{\xi_{k-1}}, g^{\nu_{x_{t_k}}}) \cdot e(g^{\xi_k}, g^{-\nu_{y_{t_k}}}) \quad (\text{since } \sigma_{t_k} = u_k) \\ &= e(g^{\xi_0}, g^{\nu_{x_{t_1}}}) \cdot e(g^{\xi_l}, g^{-\nu_{y_{t_l}}}) \quad (\text{since } y_{t_k} = x_{t_{k+1}} \text{ for } k = 1, \dots, l-1) \\ &= e(g^{\xi_0}, g^{\nu_0}) \cdot e(g^{\xi_l}, g^{-\nu_{n-1}}) \quad (\text{since } x_{t_1} = 0, y_{t_l} = n-1) \\ &= e(g^{\xi_0}, g^{\nu_0}) \cdot e(g^{\xi_l}, h_4^{-\bar{\pi}}). \end{aligned}$$

Compute

$$\begin{aligned} D_P &\leftarrow \frac{e(K_1, P_3) \cdot e(K_3, P_4) \cdot e(K_{5,0}, P_6) \cdot D_T}{e(K_4, P_5)} \\ &= \frac{e(g^{\delta_1}, g^{\beta_1 \pi} g^{\beta_3 \bar{\pi}}) \cdot e(h_3^{-\delta_1} h_4^{\xi_l}, g^{\bar{\pi}}) \cdot e(g^{\xi_0}, g^{-\nu_0} h_5^{\pi_0}) \cdot e(g^{\xi_0}, g^{\nu_0}) \cdot e(g^{\xi_l}, h_4^{-\bar{\pi}})}{e(h_5^{\xi_0}, g^{\pi_0})} \\ &= e(g^{\delta_1}, g^{\beta_1 \pi}). \end{aligned}$$

2. Compute

$$D_I \leftarrow \frac{e(K_0, Q_i) \cdot e(K'_0, Q'_i)}{e(K_1, Q_{i,1}) \cdot e(K_2, Q_{i,2})} \cdot \frac{e_3(\mathbf{R}'_i, \mathbf{C}'_j)}{e_3(\mathbf{R}_i, \mathbf{C}_j)}.$$

3. Computes $M \leftarrow T_i / (D_P \cdot D_I)$ as the output message.

E.2 Proof of Lemma 1

Proof. Suppose there exists a polynomial time adversary \mathcal{A} that selectively breaks the index-hiding game with advantage ϵ . We build a PPT algorithm \mathcal{B} to solve a Modified (n, J) -EDHE2-Dual problem instance in a subgroup as follows. \mathcal{B} is given

$$D = \left((N, \mathbb{G}, \mathbb{G}_T, e), g, g^a, g^b, g^{b/z}, g^{a^{n-1}bc/z}, g_2, g_3, \right. \\ \forall i \in [1, n], j, j' \in [1, J], j \neq j' \quad g^{a^i/d_j^2}, g^{a^i b/d_j}, g^{d_j}, g^{a^i d_j/d_j^2}, g^{a^i b d_j/d_j'}, g^{a^i/d_j^5}, g^{a^i d_j/d_j^6}, \\ \forall i \in [0, n-1], j \in [1, J] \quad g^{a^i c}, g^{a^i b c d_j}, \\ \forall i \in [0, n], j \in [1, J] \quad g^{a^i b c d_j^5}, \\ \forall i \in [1, 2n-1], j, j' \in [1, J], j \neq j' \quad g^{a^i b c d_j/d_j'}, g^{a^i b c d_j^5/d_j^6}, \\ \forall i \in [1, 2n-1], i \neq n, j \in [1, J] \quad g^{a^i b c/d_j}, \\ \left. \forall i \in [1, 2n-1], j, j' \in [1, m] \quad g^{a^i c/d_j^2}, g^{a^i b^2 c d_j/d_j'}, g^{a^i b c d_j/d_j^6}, g^{a^i c/d_j^6}, g^{a^i b c d_j^5/d_j^2}, g^{a^i b^2 c d_j^5/d_j'} \right)$$

and T , where $(N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, e) \xleftarrow{R} \mathcal{G}$, $g \xleftarrow{R} \mathbb{G}_{p_1}$, $g_2 \xleftarrow{R} \mathbb{G}_{p_2}$, $g_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $a, b, c, z, d_1, \dots, d_J \xleftarrow{R} \mathbb{Z}_N$, and T is either equal to $g^{a^n c z}$ or is a random element from \mathbb{G}_{p_1} . \mathcal{B} 's goal is to determine $T = g^{a^n c z}$ or T is a random element from \mathbb{G}_{p_1} .

Init. \mathcal{A} gives \mathcal{B} the challenge DFA $\mathbb{M}^* = \{Q^*, \mathbb{Z}_N, \mathcal{J}^*, q_0, q_{n-1}\}$, where $n = |Q^*|$, let $J = |\mathcal{J}^*|$, and parse $\mathcal{J} = \{(q_{x_1}, q_{y_1}, \sigma_1^*), \dots, (q_{x_J}, q_{y_J}, \sigma_J^*)\}$.

Setup. \mathcal{B} randomly chooses $\{\alpha_i \in \mathbb{Z}_N\}_{i \in [m]}$, $\{r_i, z'_i \in \mathbb{Z}_N\}_{i \in [m] \setminus \{\bar{i}\}}$, $r'_i, z_i \in \mathbb{Z}_N$, $\{c'_j \in \mathbb{Z}_N\}_{j \in [m]}$, and $\beta'_1, \beta_2, \beta'_3, \beta'_4, \beta'_5, \beta'_6, \beta'_7, \beta'_8, \beta'_9 \in \mathbb{Z}_N$. \mathcal{B} gives \mathcal{A} the public parameter PP:

$$\left(g, h_1 = (g^a)^{\beta'_1}, h_2 = g^{\beta_2}, h_3 = (g^a)^{\beta'_3}, h_4 = (g^a)^{\beta'_4}, h_5 = g^{\beta'_5} \cdot g^{a^n b/d_1}, \right. \\ h_6 = g^{\beta'_6} \cdot \left(\prod_{t \in [1, J]} g^{\sigma_t^* a^{n-x_t}/d_t^2} g^{-a^{n-x_t} b/d_t} \right), h_7 = g^{\beta'_7} \cdot \left(\prod_{t \in [1, J]} g^{-a^{n-x_t}/d_t^2} \right), \\ h_8 = g^{\beta'_8} \cdot \left(\prod_{t \in [1, J]} g^{-\sigma_t^* a^{n-y_t}/d_t^6} g^{a^{n-y_t} b/d_t} \right), h_9 = g^{\beta'_9} \cdot \left(\prod_{t \in [1, J]} g^{a^{n-y_t}/d_t^6} \right), \\ \{E_i = e(g, g)^{\alpha_i}\}_{i \in [m]}, \\ \{G_i = g^{r_i}, Z_i = (g^a)^{z'_i}\}_{i \in [m] \setminus \{\bar{i}\}}, \{H_j = (g^{b/z})^{c'_j}\}_{j \in [m] \setminus \{\bar{j}\}}, G_{\bar{i}} = (g^{a^{n-1}c})^{r'_i}, Z_{\bar{i}} = g^{z_i}, H_{\bar{j}} = (g^a)^{c'_j} \Big).$$

Note that \mathcal{B} implicitly chooses $r_{\bar{i}}, z_i (i \in [m] \setminus \{\bar{i}\})$, $c_j (j \in [m])$, $\beta_1, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8, \beta_9 \in \mathbb{Z}_N$ such that

$$a^{n-1} c r'_i \equiv r_{\bar{i}} \pmod{p_1}, a z'_i \equiv z_i \pmod{p_1} \quad \forall i \in [m] \setminus \{\bar{i}\}, \\ a c'_j \equiv c_j \pmod{p_1}, (b/z) c'_j \equiv c_j \pmod{p_1} \quad \forall j \in [m] \setminus \{\bar{j}\}, \\ a \beta'_1 \equiv \beta_1 \pmod{p_1}, a \beta'_3 \equiv \beta_3 \pmod{p_1}, a \beta'_4 \equiv \beta_4 \pmod{p_1}, \beta'_5 + a^n b/d_1 \equiv \beta_5 \pmod{p_1}, \\ \beta'_6 + \sum_{t \in [1, J]} (\sigma_t^* a^{n-x_t}/d_t^2 - a^{n-x_t} b/d_t) \equiv \beta_6 \pmod{p_1}, \beta'_7 + \sum_{t \in [1, J]} (-a^{n-x_t}/d_t^2) \equiv \beta_7 \pmod{p_1}, \\ \beta'_8 + \sum_{t \in [1, J]} (-\sigma_t^* a^{n-y_t}/d_t^6 + a^{n-y_t} b/d_t) \equiv \beta_8 \pmod{p_1}, \beta'_9 + \sum_{t \in [1, J]} (a^{n-y_t}/d_t^6) \equiv \beta_9 \pmod{p_1}.$$

Query Phase. To respond to \mathcal{A} 's query for $((i, j), \mathbf{u})$, let $l = |\mathbf{u}|$, and parse $\mathbf{u} = (u_1, \dots, u_l)$,

• if $(i, j) \neq (\bar{i}, \bar{j})$: \mathcal{B} picks random $\boldsymbol{\delta} = (\delta_1, \delta_2, \xi_0, \xi_1, \dots, \xi_l) \in \mathbb{Z}_N^{3+l}$, $\mathbf{R} = (R_0, R_1, \dots, R_4, R_{5,0}, \{R_{5,k}, R_{6,k}\}_{k \in [l]}) \in \mathbb{G}_{p_3}^{\delta+2l}$, and $R'_0 \in \mathbb{G}_{p_3}$. \mathcal{B} creates a secret key $\text{SK}_{(i,j), \mathbf{u}}$:

$$K_0 = \begin{cases} g^{\alpha_i} (g^{b/z})^{r_i c'_j} \cdot h_1^{\delta_1} h_2^{\delta_2} \cdot R_0, & : i \neq \bar{i}, j \neq \bar{j} \\ g^{\alpha_i} (g^{a^{n-1}bc/z})^{r'_i c_j} \cdot h_1^{\delta_1} h_2^{\delta_2} \cdot R_0, & : i = \bar{i}, j \neq \bar{j} \\ g^{\alpha_i} (g^a)^{r_i c'_j} \cdot h_1^{\delta_1} h_2^{\delta_2} \cdot R_0, & : i \neq \bar{i}, j = \bar{j}. \end{cases}$$

$$\begin{aligned}
K_1 &= g^{\delta_1} \cdot R_1, \quad K_2 = g^{\delta_2} \cdot R_2, \quad K'_0 = Z_i^{\delta_1} \cdot R'_0, \\
K_3 &= h_3^{-\delta_1} h_4^{\xi'_1} \cdot R_3, \quad K_4 = h_5^{\xi_0} \cdot R_4, \quad K_{5,0} = g^{\xi_0} \cdot R_{5,0}, \\
\{K_{5,k} &= g^{\xi_k} \cdot R_{5,k}, \quad K_{6,k} = (h_6 h_7^{u_k})^{\xi_{k-1}} (h_8 h_9^{u_k})^{\xi_k} \cdot R_{6,k}\}_{k \in [1,l]}.
\end{aligned}$$

• if $(i, j) = (\bar{i}, \bar{j})$: it implies that \mathcal{A} is querying a secret key with the challenge index (\bar{i}, \bar{j}) , and \mathbb{M}^* does not accept \mathbf{u} . We denote by \mathbf{u}_k the vector formed by the last $l-k$ symbol of \mathbf{u} . That is $\mathbf{u}_k = (u_{k+1}, \dots, u_l)$. Hence $\mathbf{u}_0 = \mathbf{u}$ and \mathbf{u}_l is the empty string. For $q_i \in \{q_0, \dots, q_{n-1}\} = Q$, let \mathbb{M}_i^* be the same DFA as \mathbb{M}^* except that the start state is set to q_i . Then for each $k \in [0, l]$ we define $U_k = \{i \in [0, n-1] \mid \mathbb{M}_i^* \text{ accepts } \mathbf{u}_k\}$. From this and the query restriction that \mathbb{M}^* does not accept \mathbf{u} , we have $0 \notin U_0$. Due to the WLOG condition, we have $U_l = \{n-1\}$. \mathcal{B} picks random $\delta = (\delta'_1, \delta_2, \xi_0, \xi'_1, \dots, \xi'_l) \in \mathbb{Z}_N^{3+l}$, $\mathbf{R} = (R_0, R_1, \dots, R_4, R_{5,0}, \{R_{5,k}, R_{6,k}\}_{k \in [l]}) \in \mathbb{G}_{p_3}^{6+2l}$, and $R'_0 \in \mathbb{G}_{p_3}$.

\mathcal{B} sets the values of $\delta_1 \in \mathbb{Z}_N$, $\mathbf{u} \in \mathbb{Z}_N^n$, $\{\xi_k \in \mathbb{Z}_N\}_{k \in [l]}$ by implicitly setting

$$\begin{aligned}
\delta_1 &= \delta'_1 - a^{n-1} c r'_i c'_j / \beta'_1, \\
\xi_0 &= \xi'_0 - r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_0} a^i c \right) \left(1 + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_1}} d_t / (\sigma_t^* - u_1) \right) \right), \\
\forall k \in [1, l-1]: \quad \xi_k &= \xi'_k - r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_k} a^i c \right) \left(1 + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_{k+1}}} d_t / (\sigma_t^* - u_{k+1}) \right) \right. \\
&\quad \left. + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_k}} d_t^5 / (\sigma_t^* - u_k) \right) \right), \\
\xi_l &= \xi'_l - r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_l} a^i c \right) \left(1 + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_l}} d_t^5 / (\sigma_t^* - u_l) \right) \right),
\end{aligned}$$

\mathcal{B} creates a secret key $\text{SK}_{(\bar{i}, \bar{j}), \mathbf{u}}$ as follows:

$$\begin{aligned}
K_0 &= g^{\alpha_{\bar{i}}} h_1^{\delta'_1} h_2^{\delta_2} \cdot R_0, \quad K_1 = g^{\delta'_1} (g^{a^{n-1} c})^{-r'_i c'_j / \beta'_1} \cdot R_1, \quad K_2 = g^{\delta_2} \cdot R_2, \quad K'_0 = (K_1)^{z_{\bar{i}}} \cdot R'_0, \\
K_3 &= h_3^{-\delta_1} h_4^{\xi'_1} \cdot R_3 \\
&= h_3^{-\delta_1} h_4^{\xi'_1} \cdot (g^{a \beta'_3})^{a^{n-1} c r'_i c'_j / \beta'_1} \cdot (g^{a \beta'_4})^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_l} a^i c \right) \left(1 + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_l}} d_t^5 / (\sigma_t^* - u_l) \right) \right) \cdot R_3 \\
&= h_3^{-\delta_1} h_4^{\xi'_1} \cdot (g^{a^n c})^{r'_i c'_j \beta'_3 / \beta'_1} \cdot (g^{a \beta'_4})^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} a^{n-1} c \left(1 + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_l}} d_t^5 / (\sigma_t^* - u_l) \right) \right) \cdot R_3 \\
&\quad (\text{since } U_l = \{n-1\}) \\
&= h_3^{-\delta_1} h_4^{\xi'_1} \cdot (g^{a^n c})^{r'_i c'_j \beta'_3 / \beta'_1} \cdot (g^{a^n c})^{-r'_i c'_j \beta'_3 / \beta'_1} \cdot \left(\prod_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_l}} (g^{a^n b c d_t^5})^{1 / (\sigma_t^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / \beta'_1} \cdot R_3 \\
&= h_3^{-\delta_1} h_4^{\xi'_1} \cdot \left(\prod_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_l}} (g^{a^n b c d_t^5})^{1 / (\sigma_t^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / \beta'_1} \cdot R_3, \\
K_4 &= h_5^{\xi_0} \cdot R_4 \\
&= h_5^{\xi_0} \cdot (g^{\beta'_5} \cdot g^{a^n b / d_1})^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_0} a^i c \right) \\
&\quad \cdot (g^{\beta'_5} \cdot g^{a^n b / d_1})^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_0} a^i c \right) \left(\left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_1}} d_t / (\sigma_t^* - u_1) \right) \right) \cdot R_4
\end{aligned}$$

$$\begin{aligned}
&= h_5^{\xi'_0} \cdot \left(\prod_{i \in U_0} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 \beta'_5 / (\beta'_1 \beta'_4)} \cdot \underbrace{\left(\prod_{i \in U_0} g^{a^{n+i} bc/d_1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{note that } 0 \notin U_0} \\
&\cdot \left(\prod_{i \in U_0} \prod_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_1}} (g^{a^i bcd_t})^{1/(\sigma_t^* - u_1)} \right)^{-r'_i c'_j \beta'_3 \beta'_5 / (\beta'_1 \beta'_4)} \\
&\cdot \left(\prod_{i \in U_0} \prod_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_1}} (g^{a^{n+i} b^2 cd_t/d_1})^{1/(\sigma_t^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot R_4
\end{aligned}$$

$$K_{5,0} = g^{\xi'_0} \cdot R_{5,0}$$

$$\begin{aligned}
&= g^{\xi'_0} \cdot g^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_0} a^i c \right)} \cdot g^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_0} a^i c \right) \left(\left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_1}} d_t / (\sigma_t^* - u_1) \right) \right)} \cdot R_{5,0} \\
&= g^{\xi'_0} \cdot \left(\prod_{i \in U_0} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \left(\prod_{i \in U_0} \prod_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_1}} (g^{a^i bcd_t})^{1/(\sigma_t^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot R_{5,0}
\end{aligned}$$

$$K_{5,k} = g^{\xi'_k} \cdot R_{5,k} \quad \text{for } k \in [1, l-1]$$

$$\begin{aligned}
&= g^{\xi'_k - r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_k} a^i c \right)} \left(1 + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_{k+1}}} d_t / (\sigma_t^* - u_{k+1}) \right) + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_k}} d_t^5 / (\sigma_t^* - u_k) \right) \right) \cdot R_{5,k} \\
&= g^{\xi'_k} \cdot \left(\prod_{i \in U_k} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \left(\prod_{i \in U_k} \prod_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_{k+1}}} (g^{a^i bcd_t})^{1/(\sigma_t^* - u_{k+1})} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
&\cdot \left(\prod_{i \in U_k} \prod_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_k}} (g^{a^i bcd_t^5})^{1/(\sigma_t^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot R_{5,k},
\end{aligned}$$

$$K_{5,l} = g^{\xi'_l} \cdot R_{5,l}$$

$$\begin{aligned}
&= g^{\xi'_l - r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_l} a^i c \right)} \left(1 + \left(b \sum_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_l}} d_t^5 / (\sigma_t^* - u_l) \right) \right) \cdot R_{5,l} \\
&= g^{\xi'_l} \cdot \left(\prod_{i \in U_l} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \left(\prod_{i \in U_l} \prod_{\substack{t \in [1, J] \\ \text{s.t. } \sigma_t^* \neq u_l}} (g^{a^i bcd_t^5})^{1/(\sigma_t^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot R_{5,l},
\end{aligned}$$

$$K_{6,1} = (h_6 h_7^{u_1})^{\xi'_0} (h_8 h_9^{u_1})^{\xi'_1} \cdot R_{6,1}$$

$$= \underbrace{(h_6 h_7^{u_1})^{\xi'_0} (h_8 h_9^{u_1})^{\xi'_1}}_{\Psi_1}$$

$$\begin{aligned}
&\cdot \left(g^{\beta'_6 + \beta'_7 u_1} \cdot \left(\prod_{t \in [1, J]} g^{(\sigma_t^* - u_1) a^{n-x_t} / d_t^2} g^{-a^{n-x_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_0} a^i c \right)} \\
&\cdot \left(g^{\beta'_6 + \beta'_7 u_1} \cdot \left(\prod_{t \in [1, J]} g^{(\sigma_t^* - u_1) a^{n-x_t} / d_t^2} g^{-a^{n-x_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_0} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_1}} d_{t'} / (\sigma_{t'}^* - u_1) \right) \right)} \\
&\cdot \left(g^{\beta'_8 + \beta'_9 u_1} \cdot \left(\prod_{t \in [1, J]} g^{-(\sigma_t^* - u_1) a^{n-y_t} / d_t^6} g^{a^{n-y_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4) \left(\sum_{i \in U_1} a^i c \right)}
\end{aligned}$$

$$\begin{aligned}
& \cdot \left(g^{\beta'_8 + \beta'_9 u_1} \cdot \left(\prod_{t \in [1, J]} g^{-(\sigma_t^* - u_1) a^{n-yt} / d_t^6} g^{a^{n-yt} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_1} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_2}} d_{t'} / (\sigma_{t'}^* - u_2) \right) \right) \\
& \cdot \left(g^{\beta'_8 + \beta'_9 u_1} \cdot \left(\prod_{t \in [1, J]} g^{-(\sigma_t^* - u_1) a^{n-yt} / d_t^6} g^{a^{n-yt} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_1} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1}} d_{t'}^5 / (\sigma_{t'}^* - u_1) \right) \right) \cdot R_{6,1} \\
= & \Psi_1 \cdot \underbrace{\left(\prod_{i \in U_0} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 (\beta'_6 + \beta'_7 u_1) / (\beta'_1 \beta'_4)}}_{\Psi_2} \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_0} (g^{a^{n-xt+i} c / d_t^2})^{(\sigma_t^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_3} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_0} (g^{a^{n-xt+i} bc / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \underbrace{\left(\prod_{i \in U_0} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1}} (g^{a^i b c d_{t'}})^{1 / (\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 (\beta'_6 + \beta'_7 u_1) / (\beta'_1 \beta'_4)}}_{\Psi_4} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_0} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1}} (g^{a^{n-xt+i} b c d_{t'} / d_t^2})^{(\sigma_t^* - u_1) / (\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_0} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1}} (g^{a^{n-xt+i} b^2 c d_{t'} / d_t})^{-1 / (\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_5} \\
& \cdot \underbrace{\left(\prod_{i \in U_1} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 (\beta'_8 + \beta'_9 u_1) / (\beta'_1 \beta'_4)}}_{\Psi_6} \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_1} (g^{a^{n-yt+i} c / d_t^6})^{-(\sigma_t^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_7} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_1} (g^{a^{n-yt+i} bc / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \underbrace{\left(\prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_2}} (g^{a^i b c d_{t'}})^{1 / (\sigma_{t'}^* - u_2)} \right)^{-r'_i c'_j \beta'_3 (\beta'_8 + \beta'_9 u_1) / (\beta'_1 \beta'_4)}}_{\Psi_8} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_2}} (g^{a^{n-yt+i} b c d_{t'} / d_t^6})^{-(\sigma_t^* - u_1) / (\sigma_{t'}^* - u_2)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_9} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_2}} (g^{a^{n-yt+i} b^2 c d_{t'} / d_t})^{1 / (\sigma_{t'}^* - u_2)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{10}}
\end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left(\prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} (g^{a^i b c d_{t'}^5})^{1/(\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 (\beta'_8 + \beta'_9 u_1) / (\beta'_1 \beta'_4)}}_{\Psi_{11}} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} (g^{a^{n-y_t+i} b c d_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_1) / (\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} (g^{a^{n-y_t+i} b^2 c d_{t'}^5 / d_t})^{1/(\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{12}} \cdot R_{6,1} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_0} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_4 \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_0} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1}} (g^{a^{n-x_t+i} b c d_{t'} / d_t^2})^{(\sigma_t^* - u_1) / (\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_1} (g^{a^{n-y_t+i} b c / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_8 \cdot \Psi_9 \cdot \Psi_{10} \cdot \Psi_{11} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} (g^{a^{n-y_t+i} b c d_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_1) / (\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_{12} \cdot R_{6,1} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_0} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_4 \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} \prod_{i \in U_0} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1}} (g^{a^{n-x_t+i} b c d_{t'} / d_t^2})^{(\sigma_t^* - u_1) / (\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_1} (g^{a^{n-y_t+i} b c / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_8 \cdot \Psi_9 \cdot \Psi_{10} \cdot \Psi_{11} \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} \prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1}} (g^{a^{n-y_t+i} b c d_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_1) / (\sigma_{t'}^* - u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_{12} \cdot R_{6,1} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} \prod_{i \in U_0} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_0^{-1}, \text{ for } \sigma_t^* \neq u_1} \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_1}} \prod_{i \in U_0} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{for } \sigma_t^* = u_1} \cdot \Psi_4
\end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} \prod_{i \in U_0} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1, t' \neq t}} (g^{a^{n-x_t+i}bcd_{t'}/d_t^2})^{(\sigma_t^*-u_1)/(\sigma_{t'}^*-u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{13}, \text{ for } t' \neq t} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} \prod_{i \in U_0} (g^{a^{n-x_t+i}bcd_t/d_t^2})^{(\sigma_t^*-u_1)/(\sigma_t^*-u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_0, \text{ for } t'=t} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} \prod_{i \in U_1} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_1, \text{ for } \sigma_t^* \neq u_1} \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_1}} \prod_{i \in U_1} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{for } \sigma_t^* = u_1} \\
& \cdot \Psi_8 \cdot \Psi_9 \cdot \Psi_{10} \cdot \Psi_{11} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} \prod_{i \in U_1} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_1, t' \neq t}} (g^{a^{n-y_t+i}bcd_{t'}/d_t^6})^{-(\sigma_t^*-u_1)/(\sigma_{t'}^*-u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{14}, \text{ for } t' \neq t} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_1}} \prod_{i \in U_1} (g^{a^{n-y_t+i}bcd_t^5/d_t^6})^{-(\sigma_t^*-u_1)/(\sigma_t^*-u_1)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_1^{-1}, \text{ for } t'=t} \\
& \cdot \Psi_{12} \cdot R_{6,1} \\
= & \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_1}} \prod_{\substack{i \in U_0 \\ s.t. i \neq x_t}} (g^{a^{n-x_t+i}bc/d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{15}, \text{ for } i \neq x_t} \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_1}} \prod_{\substack{i \in U_0 \\ s.t. i = x_t}} (g^{a^{n-x_t+i}bc/d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{for } i = x_t \text{ (if } x_t \in U_0)} \\
& \cdot \Psi_4 \cdot \Psi_{13} \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_1}} \prod_{\substack{i \in U_1 \\ s.t. i \neq y_t}} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{16}, \text{ for } i \neq y_t} \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_1}} \prod_{\substack{i \in U_1 \\ s.t. i = y_t}} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{for } i = y_t \text{ (if } y_t \in U_1)} \\
& \cdot \Psi_8 \cdot \Psi_9 \cdot \Psi_{10} \cdot \Psi_{11} \cdot \Psi_{14} \cdot \Psi_{12} \cdot R_{6,1} \\
= & \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \Psi_{15} \cdot \Psi_4 \cdot \Psi_{13} \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_{16} \cdot \Psi_8 \cdot \Psi_9 \cdot \Psi_{10} \cdot \Psi_{11} \cdot \Psi_{14} \cdot \Psi_{12} \cdot R_{6,1} \\
& (\text{since for } t \in [1, J] \text{ such that } \sigma_t^* = u_1, \text{ we have } (x_t \in U_0 \wedge y_t \in U_1) \text{ or } (x_t \notin U_0 \wedge y_t \notin U_1).)
\end{aligned}$$

$$\begin{aligned}
K_{6,k} &= (h_6 h_7^{u_k})^{\xi_{k-1}} (h_8 h_9^{u_k})^{\xi_k} \cdot R_{6,k} \quad \text{for } k \in [2, l-1] \\
&= (h_6 h_7^{u_k})^{\xi_{k-1}} (h_8 h_9^{u_k})^{\xi_k} \\
& \cdot \left(g^{\beta'_6 + \beta'_7 u_k} \cdot \left(\prod_{t \in [1, J]} g^{(\sigma_t^* - u_k) a^{n-x_t} / d_t^2} g^{-a^{n-x_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_{k-1}} a^{i c} \right)
\end{aligned}$$

$$\begin{aligned}
& \cdot \left(g^{\beta'_6 + \beta'_7 u_k} \cdot \left(\prod_{t \in [1, J]} g^{(\sigma_t^* - u_k) a^{n-x_t} / d_t^2} g^{-a^{n-x_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_{k-1}} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} d_{t'} / (\sigma_{t'}^* - u_k) \right) \right) \\
& \cdot \left(g^{\beta'_6 + \beta'_7 u_k} \cdot \left(\prod_{t \in [1, J]} g^{(\sigma_t^* - u_k) a^{n-x_t} / d_t^2} g^{-a^{n-x_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_{k-1}} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_{k-1}}} d_{t'}^5 / (\sigma_{t'}^* - u_{k-1}) \right) \right) \\
& \cdot \left(g^{\beta'_8 + \beta'_9 u_k} \cdot \left(\prod_{t \in [1, J]} g^{-(\sigma_t^* - u_k) a^{n-y_t} / d_t^6} g^{a^{n-y_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_k} a^i c \right) \\
& \cdot \left(g^{\beta'_8 + \beta'_9 u_k} \cdot \left(\prod_{t \in [1, J]} g^{-(\sigma_t^* - u_k) a^{n-y_t} / d_t^6} g^{a^{n-y_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_k} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_{k+1}}} d_{t'} / (\sigma_{t'}^* - u_{k+1}) \right) \right) \\
& \cdot \left(g^{\beta'_8 + \beta'_9 u_k} \cdot \left(\prod_{t \in [1, J]} g^{-(\sigma_t^* - u_k) a^{n-y_t} / d_t^6} g^{a^{n-y_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_k} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} d_{t'}^5 / (\sigma_{t'}^* - u_k) \right) \right) \cdot R_{6,k} \\
= & \underbrace{(h_6 h_7^{u_k})^{\xi'_{k-1}} (h_8 h_9^{u_k})^{\xi'_k}}_{\Psi_1} \\
& \cdot \underbrace{\left(\prod_{i \in U_{k-1}} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 (\beta'_6 + \beta'_7 u_k) / (\beta'_1 \beta'_4)}}_{\Psi_2} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i} c / d_t^2})^{(\sigma_t^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_3} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \underbrace{\left(\sum_{i \in U_{k-1}} \sum_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^i b c d_{t'}})^{1 / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 (\beta'_6 + \beta'_7 u_k) / (\beta'_1 \beta'_4)}}_{\Psi_4} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_{k-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^{n-x_t+i} b c d_{t'}} / d_t^2)^{(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_{k-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^{n-x_t+i} b^2 c d_{t'}} / d_t)^{-1 / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_5} \\
& \cdot \underbrace{\left(\prod_{i \in U_{k-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_{k-1}}} (g^{a^i b c d_{t'}^5})^{1 / (\sigma_{t'}^* - u_{k-1})} \right)^{-r'_i c'_j \beta'_3 (\beta'_6 + \beta'_7 u_k) / (\beta'_1 \beta'_4)}}_{\Psi_6}
\end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_{k-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_{k-1}}} (g^{a^{n-x_t+i} bcd_{t'}^5 / d_t^2})^{(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_{k-1})} (g^{a^{n-x_t+i} b^2 cd_{t'}^5 / d_t})^{-1 / (\sigma_{t'}^* - u_{k-1})} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_7} \\
& \cdot \underbrace{\left(\prod_{i \in U_k} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 (\beta'_8 + \beta'_9 u_k) / (\beta'_1 \beta'_4)}}_{\Psi_8} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_k} (g^{a^{n-y_t+i} c / d_t^6})^{-(\sigma_t^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_9} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_k} (g^{a^{n-y_t+i} bc / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{10}} \\
& \cdot \underbrace{\left(\prod_{i \in U_k} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_{k+1}}} (g^{a^i bcd_{t'}})^{1 / (\sigma_{t'}^* - u_{k+1})} \right)^{-r'_i c'_j \beta'_3 (\beta'_8 + \beta'_9 u_k) / (\beta'_1 \beta'_4)}}_{\Psi_{10}} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_k} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_{k+1}}} (g^{a^{n-y_t+i} bcd_{t'} / d_t^6})^{-(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_{k+1})} (g^{a^{n-y_t+i} b^2 cd_{t'} / d_t})^{1 / (\sigma_{t'}^* - u_{k+1})} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{11}} \\
& \cdot \underbrace{\left(\sum_{i \in U_k} \sum_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^i bcd_{t'}^5})^{1 / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 (\beta'_8 + \beta'_9 u_k) / (\beta'_1 \beta'_4)}}_{\Psi_{12}} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_k} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^{n-y_t+i} bcd_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{13}} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_k} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^{n-y_t+i} b^2 cd_{t'}^5 / d_t})^{1 / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{13}} \cdot R_{6,k} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i} bc / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_4 \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_{k-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^{n-x_t+i} bcd_{t'} / d_t^2})^{(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_k} (g^{a^{n-y_t+i} bc / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_{10} \cdot \Psi_{11} \cdot \Psi_{12} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_k} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^{n-y_t+i} bcd_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}
\end{aligned}$$

$$\begin{aligned}
& \cdot \Psi_{13} \cdot R_{6,k} \\
= & \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i}bc/d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i}bc/d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_4 \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_{k-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^{n-x_t+i}bcd_{t'}/d_t^2})^{(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_k} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{i \in U_k} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_{10} \cdot \Psi_{11} \cdot \Psi_{12} \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_k} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k}} (g^{a^{n-y_t+i}bcd_{t'}/d_t^6})^{-(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_{13} \cdot R_{6,k} \\
= & \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i}bc/d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_0^{-1}} \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i}bc/d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_4 \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_{k-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k, t' \neq t}} (g^{a^{n-x_t+i}bcd_{t'}/d_t^2})^{(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{14}, \text{ for } t' \neq t} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i}bcd_t/d_t^2})^{(\sigma_t^* - u_k) / (\sigma_t^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_0, \text{ for } t'=t} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_k} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_1} \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{i \in U_k} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_{10} \cdot \Psi_{11} \cdot \Psi_{12}
\end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_k} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_k, t' \neq t}} (g^{a^{n-y_t+i} b c d_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_k) / (\sigma_{t'}^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{15}, \text{ for } t' \neq t} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_k}} \prod_{i \in U_k} (g^{a^{n-y_t+i} b c d_t^5 / d_t^6})^{-(\sigma_t^* - u_k) / (\sigma_t^* - u_k)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_1^{-1}, \text{ for } t'=t} \\
& \cdot \Psi_{13} \cdot R_{6,k} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{i \in U_{k-1}} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_4 \cdot \Psi_{14} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{i \in U_k} (g^{a^{n-y_t+i} b c / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_{10} \cdot \Psi_{11} \cdot \Psi_{12} \cdot \Psi_{15} \cdot \Psi_{13} \cdot R_{6,k} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{\substack{i \in U_{k-1} \\ s.t. i \neq x_t}} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{16}, \text{ for } i \neq x_t} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{\substack{i \in U_{k-1} \\ s.t. i = x_t}} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{for } i=x_t \text{ (if } x_t \in U_{k-1})} \cdot \Psi_4 \cdot \Psi_{14} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{\substack{i \in U_k \\ i \neq y_t}} (g^{a^{n-y_t+i} b c / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{17}, \text{ for } i \neq y_t} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_k}} \prod_{\substack{i \in U_k \\ i = y_t}} (g^{a^{n-y_t+i} b c / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{for } i=y_t \text{ (if } y_t \in U_k)} \\
& \cdot \Psi_{10} \cdot \Psi_{11} \cdot \Psi_{12} \cdot \Psi_{15} \cdot \Psi_{13} \cdot R_{6,k} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \Psi_{16} \cdot \Psi_4 \cdot \Psi_{14} \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \Psi_{17} \cdot \Psi_{10} \cdot \Psi_{11} \cdot \Psi_{12} \cdot \Psi_{15} \cdot \Psi_{13} \cdot R_{6,k}, \\
& \text{(since for } t \in [1, J] \text{ such that } \sigma_t^* = u_k, \text{ we have } (x_t \in U_{k-1} \wedge y_t \in U_k) \text{ or } (x_t \notin U_{k-1} \wedge y_t \notin U_k).)
\end{aligned}$$

$$\begin{aligned}
K_{6,l} &= (h_6 h_7^{u_l})^{\xi_{l-1}} (h_8 h_9^{u_l})^{\xi_l} \cdot R_{6,l} \\
&= (h_6 h_7^{u_l})^{\xi'_{l-1}} (h_8 h_9^{u_l})^{\xi'_l} \\
& \cdot \left(g^{\beta'_6 + \beta'_7 u_l} \cdot \left(\prod_{t \in [1, J]} g^{(\sigma_t^* - u_l) a^{n-x_t} / d_t^2} g^{-a^{n-x_t} b / d_t} \right) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_{l-1}} a^i c \right)
\end{aligned}$$

$$\begin{aligned}
& \cdot \left(g^{\beta'_6 + \beta'_7 u_i} \cdot \left(\prod_{t \in [1, J]} g^{(\sigma_t^* - u_i) a^{n-x_t} / d_t^2} g^{-a^{n-x_t} b / d_t} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_{l-1}} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_i}} d_{t'} / (\sigma_{t'}^* - u_i) \right) \right) \right) \\
& \cdot \left(g^{\beta'_6 + \beta'_7 u_i} \cdot \left(\prod_{t \in [1, J]} g^{(\sigma_t^* - u_i) a^{n-x_t} / d_t^2} g^{-a^{n-x_t} b / d_t} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_{l-1}} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_{l-1}}} d_{t'}^5 / (\sigma_{t'}^* - u_{l-1}) \right) \right) \right) \\
& \cdot \left(g^{\beta'_8 + \beta'_9 u_i} \cdot \left(\prod_{t \in [1, J]} g^{-(\sigma_t^* - u_i) a^{n-y_t} / d_t^6} g^{a^{n-y_t} b / d_t} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_l} a^i c \right) \right) \\
& \cdot \left(g^{\beta'_8 + \beta'_9 u_i} \cdot \left(\prod_{t \in [1, J]} g^{-(\sigma_t^* - u_i) a^{n-y_t} / d_t^6} g^{a^{n-y_t} b / d_t} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \left(\sum_{i \in U_l} a^i c \right) \left(\left(b \sum_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_i}} d_{t'}^5 / (\sigma_{t'}^* - u_i) \right) \right) \right) \cdot R_{6,l} \\
= & \underbrace{(h_6 h_7^{u_i})^{\xi'_{i-1}} (h_8 h_9^{u_i})^{\xi'_i}}_{\Psi_1} \\
& \cdot \underbrace{\left(\sum_{i \in U_{l-1}} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 (\beta'_6 + \beta'_7 u_i) / (\beta'_1 \beta'_4)}}_{\Psi_2} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_{l-1}} (g^{a^{n-x_t+i} c / d_t^2})^{(\sigma_t^* - u_i)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_{l-1}} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_3} \\
& \cdot \underbrace{\left(\prod_{i \in U_{l-1}} \prod_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_i}} (g^{a^i b c d_{t'}})^{1 / (\sigma_{t'}^* - u_i)} \right)^{-r'_i c'_j \beta'_3 (\beta'_6 + \beta'_7 u_i) / (\beta'_1 \beta'_4)}}_{\Psi_4} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_{l-1}} \prod_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_i}} (g^{a^{n-x_t+i} b c d_{t'}} / d_t^2)^{(\sigma_t^* - u_i) / (\sigma_{t'}^* - u_i)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_5} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_{l-1}} \prod_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_i}} (g^{a^{n-x_t+i} b^2 c d_{t'}} / d_t)^{-1 / (\sigma_{t'}^* - u_i)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_5} \\
& \cdot \underbrace{\left(\prod_{i \in U_{l-1}} \prod_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_{l-1}}} (g^{a^i b c d_{t'}^5})^{1 / (\sigma_{t'}^* - u_{l-1})} \right)^{-r'_i c'_j \beta'_3 (\beta'_6 + \beta'_7 u_i) / (\beta'_1 \beta'_4)}}_{\Psi_6} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_{l-1}} \prod_{\substack{t' \in [1, J] \\ \text{s.t. } \sigma_{t'}^* \neq u_{l-1}}} (g^{a^{n-x_t+i} b c d_{t'}^5} / d_t^2)^{(\sigma_t^* - u_i) / (\sigma_{t'}^* - u_{l-1})} (g^{a^{n-x_t+i} b^2 c d_{t'}^5} / d_t)^{1 / (\sigma_{t'}^* - u_{l-1})} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_7}
\end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left(\prod_{i \in U_l} g^{a^i c} \right)^{-r'_i c'_j \beta'_3 (\beta'_8 + \beta'_9 u_l) / (\beta'_1 \beta'_4)}}_{\Psi_8} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_l} (g^{a^{n-y_t+i} c / d_t^6})^{-(\sigma_t^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_9} \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_l} (g^{a^{n-y_t+i} bc / d_t})^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \right) \\
& \cdot \underbrace{\left(\prod_{i \in U_l} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l}} (g^{a^i bcd_{t'}^5})^{1/(\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 (\beta'_8 + \beta'_9 u_l) / (\beta'_1 \beta'_4)}}_{\Psi_{10}} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_l} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l}} (g^{a^{n-y_t+i} bcd_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_l) / (\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \underbrace{\left(\prod_{t \in [1, J]} \prod_{i \in U_l} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l}} (g^{a^{n-y_t+i} b^2 cd_{t'}^5 / d_t})^{1/(\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{11}} \cdot R_{6,l} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_{l-1}} (g^{a^{n-x_t+i} bc / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_4 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_{l-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l}} (g^{a^{n-x_t+i} bcd_{t'} / d_t^2})^{(\sigma_t^* - u_l) / (\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_l} (g^{a^{n-y_t+i} bc / d_t})^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \right) \\
& \cdot \Psi_{10} \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_l} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l}} (g^{a^{n-y_t+i} bcd_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_l) / (\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_{11} \cdot R_{6,l} \\
& = \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{t \in [1, J]} \prod_{\substack{i \in U_{l-1} \\ s.t. \sigma_t^* \neq u_l}} (g^{a^{n-x_t+i} bc / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{i \in U_{l-1}} (g^{a^{n-x_t+i} bc / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \quad s.t. \sigma_t^* = u_l \\
& \cdot \Psi_4 \cdot \left(\prod_{t \in [1, J]} \prod_{\substack{i \in U_{l-1} \\ s.t. \sigma_t^* \neq u_l}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l}} (g^{a^{n-x_t+i} bcd_{t'} / d_t^2})^{(\sigma_t^* - u_l) / (\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \left(\prod_{t \in [1, J]} \prod_{\substack{i \in U_l \\ s.t. \sigma_t^* \neq u_l}} (g^{a^{n-y_t+i} bc / d_t})^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \right) \\
& \cdot \left(\prod_{t \in [1, J]} \prod_{\substack{i \in U_l \\ s.t. \sigma_t^* = u_l}} (g^{a^{n-y_t+i} bc / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}
\end{aligned}$$

$$\begin{aligned}
& \cdot \Psi_{10} \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_l}} \prod_{i \in U_l} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l}} (g^{a^{n-y_t+i} b c d_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_l) / (\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_{11} \cdot R_{6,l} \\
= & \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_l}} \prod_{i \in U_{l-1}} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_0^{-1}} \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_l}} \prod_{i \in U_{l-1}} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_4 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_l}} \prod_{i \in U_{l-1}} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l, t' \neq t}} (g^{a^{n-x_t+i} b c d_{t'} / d_t^2})^{(\sigma_t^* - u_l) / (\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{12}, \text{ for } t' \neq t} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_l}} \prod_{i \in U_{l-1}} (g^{a^{n-x_t+i} b c d_{t'} / d_t^2})^{(\sigma_t^* - u_l) / (\sigma_t^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_0, \text{ for } t' = t} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_l}} \prod_{i \in U_l} (g^{a^{n-y_t+i} b c / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_1} \\
& \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_l}} \prod_{i \in U_l} (g^{a^{n-y_t+i} b c / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \\
& \cdot \Psi_{10} \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_l}} \prod_{i \in U_l} \prod_{\substack{t' \in [1, J] \\ s.t. \sigma_{t'}^* \neq u_l, t' \neq t}} (g^{a^{n-y_t+i} b c d_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_l) / (\sigma_{t'}^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{13}, \text{ for } t' \neq t} \\
& \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* \neq u_l}} \prod_{i \in U_l} (g^{a^{n-y_t+i} b c d_{t'}^5 / d_t^6})^{-(\sigma_t^* - u_l) / (\sigma_t^* - u_l)} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Delta_1^{-1}, \text{ for } t' = t} \cdot \Psi_{11} \cdot R_{6,l} \\
= & \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_l}} \prod_{i \in U_{l-1}} (g^{a^{n-x_t+i} b c / d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_4 \cdot \Psi_{12} \\
& \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_l}} \prod_{i \in U_l} (g^{a^{n-y_t+i} b c / d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)} \cdot \Psi_{10} \cdot \Psi_{13} \cdot \Psi_{11} \cdot R_{6,l}
\end{aligned}$$

$$\begin{aligned}
&= \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_l}} \prod_{\substack{i \in U_{l-1} \\ i \neq x_t}} (g^{a^{n-x_t+i}bc/d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{14}, \text{ for } i \neq x_t} \\
&\cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_l}} \prod_{\substack{i \in U_{l-1} \\ i = x_t}} (g^{a^{n-x_t+i}bc/d_t})^{-1} \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{for } i = x_t \text{ (if } x_t \in U_{l-1})} \cdot \Psi_4 \cdot \Psi_{12} \\
&\cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_l}} \prod_{\substack{i \in U_l \\ i \neq y_t}} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\Psi_{15}, \text{ for } i \neq y_t} \\
&\cdot \underbrace{\left(\prod_{\substack{t \in [1, J] \\ s.t. \sigma_t^* = u_l}} \prod_{\substack{i \in U_l \\ i = y_t}} (g^{a^{n-y_t+i}bc/d_t}) \right)^{-r'_i c'_j \beta'_3 / (\beta'_1 \beta'_4)}}_{\text{for } i = y_t, \text{ (if } y_t \in U_l)} \cdot \Psi_{10} \cdot \Psi_{13} \cdot \Psi_{11} \cdot R_{6,l} \\
&= \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \Psi_{14} \cdot \Psi_4 \cdot \Psi_{12} \cdot \Psi_5 \cdot \Psi_6 \cdot \Psi_7 \cdot \Psi_8 \cdot \Psi_9 \cdot \Psi_{15} \cdot \Psi_{10} \cdot \Psi_{13} \cdot \Psi_{11} \cdot R_{6,l} \\
&\quad (\text{since for } t \in [1, J] \text{ such that } \sigma_t^* = u_l, \text{ we have } (x_t \in U_{l-1} \wedge y_t \in U_l) \text{ or } (x_t \notin U_{l-1} \wedge y_t \notin U_l).)
\end{aligned}$$

Note that \mathcal{B} can calculate the values of $K_0, K_1, K_2, K'_0, K_3, K_4, K_{5,0}, \{K_{5,k}, K_{6,k}\}_{k \in [l]}$ using the suitable terms of the assumption.

Challenge. \mathcal{A} submits a message M . \mathcal{B} randomly chooses

$$\begin{aligned}
&\tau', s_1, \dots, s_{\bar{i}-1}, s'_{\bar{i}}, s_{\bar{i}+1}, \dots, s_m, t'_1, \dots, t'_{\bar{i}-1}, t'_{\bar{i}}, t'_{\bar{i}+1}, \dots, t'_m \in \mathbb{Z}_N, \\
&\mathbf{w}_1, \dots, \mathbf{w}_{\bar{j}-1}, \mathbf{w}'_{\bar{j}}, \dots, \mathbf{w}'_m \in \mathbb{Z}_N^3, \\
&\pi', \bar{\pi}', \pi'_0, \pi'_1, \dots, \pi'_J \in \mathbb{Z}_N, \{\nu'_x \in \mathbb{Z}_N\}_{q_x \in Q \setminus \{q_{n-1}\}}.
\end{aligned}$$

\mathcal{B} randomly chooses $r_x, r_y, r_z \in \mathbb{Z}_N$, and sets $\chi_1 = (r_x, 0, r_z), \chi_2 = (0, r_y, r_z), \chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$. \mathcal{B} randomly chooses

$$\begin{aligned}
&\mathbf{v}_i \in \mathbb{Z}_N^3 \quad \forall i \in \{1, \dots, \bar{i} - 1\}, \\
&\mathbf{v}_i^p \in \text{span}\{\chi_1, \chi_2\}, \mathbf{v}_i^q \in \text{span}\{\chi_3\}, \\
&\mathbf{v}_i \in \text{span}\{\chi_1, \chi_2\} \quad \forall i \in \{\bar{i} + 1, \dots, m\}, \\
&\mathbf{v}_c^p \in \text{span}\{\chi_1, \chi_2\}, \mathbf{v}_c^q = \nu_3 \chi_3 \in \text{span}\{\chi_3\}.
\end{aligned}$$

\mathcal{B} sets the value of $\kappa, \tau, s_i, t_i (i \in [m] \setminus \{\bar{i}\}) \in \mathbb{Z}_N, \mathbf{v}_c, \mathbf{v}_{\bar{i}} \in \mathbb{Z}_N^3, \{\mathbf{w}_j \in \mathbb{Z}_N^3\}_{j=\bar{j}}^m, \pi, \bar{\pi}, \pi_0, \pi_1, \dots, \pi_J \in \mathbb{Z}_N, \{\nu'_x \in \mathbb{Z}_N\}_{q_x \in Q \setminus \{q_{n-1}\}}$ by implicitly setting

$$\begin{aligned}
&a^{n-1}c \equiv \kappa \pmod{p_1}, \quad a^{n-1}cz\tau' \equiv \tau \pmod{p_1}, \quad s'_i / (a^{n-1}c) \equiv s_{\bar{i}} \pmod{p_1}, \\
&t'_i + b\beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i \equiv t_i \pmod{p_1} \quad \forall i \in \{1, \dots, \bar{i} - 1\}, \\
&t'_i - a^{n-1}c\beta'_1 \tau' s_i (\mathbf{v}_i \cdot \mathbf{v}_c^p) / z'_i + b\beta'_1 \tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i \equiv t_i \pmod{p_1} \quad \forall i \in \{\bar{i} + 1, \dots, m\}, \\
&\mathbf{v}_c = \frac{1}{z} \mathbf{v}_c^p + \mathbf{v}_c^q, \quad \mathbf{v}_{\bar{i}} = \mathbf{v}_{\bar{i}}^p + \frac{b}{z} \mathbf{v}_{\bar{i}}^q, \\
&\mathbf{w}'_{\bar{j}} - ac'_j \tau' \mathbf{v}_c^p \equiv \mathbf{w}_{\bar{j}} \pmod{p_1}, \\
&\mathbf{w}'_j - bc'_j \tau' \mathbf{v}_c^q \equiv \mathbf{w}_j \pmod{p_1} \quad \forall j \in \{\bar{j} + 1, \dots, m\},
\end{aligned}$$

$$\begin{aligned}
\pi' - b\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) &\equiv \pi \pmod{p_1}, \quad \bar{\pi}' + b\beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3 \equiv \bar{\pi} \pmod{p_1}, \\
\pi'_0 + d_1 \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3 &\equiv \pi_0 \pmod{p_1}, \\
\pi'_t + d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3 &\equiv \pi_t \pmod{p_1} \quad \forall t \in [1, J], \\
\nu'_x + a^{n-x} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3 &\equiv \nu_x \pmod{p_1} \quad \forall q_x \in \mathcal{Q} \setminus \{q_{n-1}\}.
\end{aligned}$$

Also, \mathcal{B} implicitly sets $\nu_{n-1} := \beta_4 \bar{\pi} \equiv a\beta'_4(\bar{\pi}' + b\beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3) \pmod{p_1}$.

It is worth noticing that $\mathbf{v}_{\bar{i}}$ and \mathbf{v}_c are random vectors in \mathbb{Z}_N^3 as required, and $(\mathbf{v}_{\bar{i}} \cdot \mathbf{v}_c) = \frac{1}{z}(\mathbf{v}_{\bar{i}}^p \cdot \mathbf{v}_c^p) + \frac{b}{z}(\mathbf{v}_{\bar{i}}^q \cdot \mathbf{v}_c^q)$, since χ_3 is orthogonal to $\text{span}\{\chi_1, \chi_2\}$ and $\mathbb{Z}_N^3 = \text{span}\{\chi_1, \chi_2, \chi_3\}$.

\mathcal{B} creates a ciphertext $\langle \mathbb{M}^*, (P_1, P_2, P_3, P_4, P_5, P_6, \{P_{7,t}, P_{8,t}, P_{9,t}\}_{t \in [J]}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q_{i,2}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$ as follows:

1.

$$\begin{aligned}
P_1 &= g^\pi = g^{\pi'} (g^b)^{-\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}, \quad P_2 = (P_1)^{\beta_2}, \quad P_3 = h_1^\pi h_3^{\bar{\pi}} = h_1^{\pi'} h_3^{\bar{\pi}'}, \\
P_4 &= g^{\bar{\pi}} = g^{\bar{\pi}'} (g^b)^{\beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}, \quad P_5 = g^{\pi_0} = g^{\pi'_0} (g^{d_1})^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}, \\
P_6 &= g^{-\nu_0} h_5^{\pi_0} = g^{-\nu'_0 - a^{n-b} \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \cdot h_5^{\pi'_0} (g^{\beta'_5} \cdot g^{a^{n-b} / d_1})^{d_1 \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= g^{-\nu'_0} h_5^{\pi'_0} (g^{d_1})^{\beta'_5 \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3},
\end{aligned}$$

for $t \in [1, J]$,

$$P_{7,t} = g^{\pi_t} = g^{\pi'_t} \cdot (g^{d_t})^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3},$$

if $x_t = n - 1$,

$$\begin{aligned}
P_{8,t} &= g^{\nu_{x_t}} (h_6 h_7^{\sigma_t^*})^{\pi_t} \\
&= g^{a\beta'_4(\bar{\pi}' + b\beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3)} (h_6 h_7^{\sigma_t^*})^{\pi'_t + d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= (g^a)^{\beta'_4 \bar{\pi}'} g^{a\beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi'_t} (g^{\beta'_6 + \beta'_7 \sigma_t^*})^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\left(\prod_{t' \in [1, J]} g^{\sigma_{t'}^* a^{n-x_{t'}} / d_{t'}} g^{-a^{n-x_{t'}} b / d_{t'}} \right) \cdot \left(\prod_{t' \in [1, J]} g^{-a^{n-x_{t'}} / d_{t'}} \right)^{\sigma_{t'}^*} \right)^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= (g^a)^{\beta'_4 \bar{\pi}'} g^{a\beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi'_t} (g^{d_t})^{(\beta'_6 + \beta'_7 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{t' \in [1, J]} g^{-a^{n-x_{t'}} b / d_{t'}} \right)^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= (g^a)^{\beta'_4 \bar{\pi}'} g^{a\beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi'_t} (g^{d_t})^{(\beta'_6 + \beta'_7 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{t' \in [1, J]} g^{-a^{n-x_{t'}} b d_t / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= (g^a)^{\beta'_4 \bar{\pi}'} g^{a\beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi'_t} (g^{d_t})^{(\beta'_6 + \beta'_7 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \underbrace{\left(\prod_{\substack{t' \in [1, J] \\ t' \neq t}} g^{-a^{n-x_{t'}} b d_t / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t' \neq t} \cdot \underbrace{(g^{-ab})^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t'=t} \\
&= (g^a)^{\beta'_4 \bar{\pi}'} (h_6 h_7^{\sigma_t^*})^{\pi'_t} (g^{d_t})^{(\beta'_6 + \beta'_7 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{\substack{t' \in [1, J] \\ t' \neq t}} g^{a^{n-x_{t'}} b d_t / d_{t'}} \right)^{-\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3},
\end{aligned}$$

if $x_t \neq n-1$,

$$\begin{aligned}
P_{8,t} &= g^{\nu_{x_t}} (h_6 h_7^{\sigma_t^*})^{\pi_t} \\
&= g^{\nu_{x_t}} \cdot g^{a^{n-x_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi_t + d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= g^{\nu_{x_t}} \cdot g^{a^{n-x_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi_t} (g^{\beta'_6 + \beta'_7 \sigma_t^*})^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\left(\prod_{t' \in [1, J]} g^{\sigma_{t'}^* a^{n-x_{t'}} / d_{t'}^2} g^{-a^{n-x_{t'}} b / d_{t'}} \right) \cdot \left(\prod_{t' \in [1, J]} g^{-a^{n-x_{t'}} / d_{t'}^2} \right) \sigma_{t'}^* \right)^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= g^{\nu_{x_t}} \cdot g^{a^{n-x_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi_t} (g^{d_t})^{(\beta'_6 + \beta'_7 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{t' \in [1, J]} g^{-a^{n-x_{t'}} b / d_{t'}} \right)^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= g^{\nu_{x_t}} \cdot g^{a^{n-x_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi_t} (g^{d_t})^{(\beta'_6 + \beta'_7 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{t' \in [1, J]} g^{-a^{n-x_{t'}} b d_{t'} / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= g^{\nu_{x_t}} \cdot g^{a^{n-x_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_6 h_7^{\sigma_t^*})^{\pi_t} (g^{d_t})^{(\beta'_6 + \beta'_7 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{\substack{t' \in [1, J] \\ t' \neq t}} g^{-a^{n-x_{t'}} b d_{t'} / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \cdot \underbrace{(g^{-a^{n-x_t} b})^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t'=t} \\
&= g^{\nu_{x_t}} \cdot \underbrace{(h_6 h_7^{\sigma_t^*})^{\pi_t} (g^{d_t})^{(\beta'_6 + \beta'_7 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t' \neq t} \cdot \left(\prod_{\substack{t' \in [1, J] \\ t' \neq t}} g^{a^{n-x_{t'}} b d_{t'} / d_{t'}} \right)^{-\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3},
\end{aligned}$$

if $y_t = n-1$,

$$\begin{aligned}
P_{9,t} &= g^{-\nu_{y_t}} (h_8 h_9^{\sigma_t^*})^{\pi_t} \\
&= g^{-a \beta'_4 (\pi' + b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3)} (h_8 h_9^{\sigma_t^*})^{\pi_t + d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= (g^a)^{-\beta'_4 \pi'} g^{-a \beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_t^*})^{\pi_t} (g^{\beta'_8 + \beta'_9 \sigma_t^*})^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\left(\prod_{t' \in [1, J]} g^{-\sigma_{t'}^* a^{n-y_{t'}} / d_{t'}^6} g^{a^{n-y_{t'}} b / d_{t'}} \right) \cdot \left(\prod_{t' \in [1, J]} g^{a^{n-y_{t'}} / d_{t'}^6} \right) \sigma_{t'}^* \right)^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= (g^a)^{-\beta'_4 \pi'} g^{-a \beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_t^*})^{\pi_t} (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{t' \in [1, J]} g^{a^{n-y_{t'}} b / d_{t'}} \right)^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= (g^a)^{-\beta'_4 \pi'} g^{-a \beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_t^*})^{\pi_t} (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{t' \in [1, J]} g^{a^{n-y_{t'}} b d_{t'} / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&= (g^a)^{-\beta'_4 \pi'} g^{-a \beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_t^*})^{\pi_t} (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\
&\quad \cdot \left(\prod_{\substack{t' \in [1, J] \\ t' \neq t}} g^{a^{n-y_{t'}} b d_{t'} / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \cdot \underbrace{(g^{ab})^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t'=t} \\
&= \underbrace{(g^a)^{-\beta'_4 \pi'} g^{-a \beta'_4 b \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_t^*})^{\pi_t} (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_t^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t' \neq t} \cdot \underbrace{(g^{ab})^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t'=t}
\end{aligned}$$

$$= (g^a)^{-\beta'_4 \pi'} (h_8 h_9^{\sigma_i^*}) \pi'_i (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_i^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \cdot \left(\prod_{\substack{t' \in [1, J] \\ t' \neq t}} g^{a^{n-y_{t'}} b d_{t'} / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3},$$

if $y_t \neq n - 1$,

$$\begin{aligned} P_{8,t} &= g^{-\nu_{y_t}} (h_8 h_9^{\sigma_i^*}) \pi_t \\ &= g^{-\nu'_{y_t}} \cdot g^{-a^{n-y_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_i^*}) \pi'_t + d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3 \\ &= g^{-\nu'_{y_t}} \cdot g^{-a^{n-y_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_i^*}) \pi'_t (g^{\beta'_8 + \beta'_9 \sigma_i^*})^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\ &\quad \cdot \left(\left(\prod_{t' \in [1, J]} g^{-\sigma_i^* a^{n-y_{t'}} / d_{t'}} g^{a^{n-y_{t'}} b / d_{t'}} \right) \cdot \left(\prod_{t' \in [1, J]} g^{a^{n-y_{t'}} / d_{t'}} \right)^{\sigma_i^*} \right)^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\ &= g^{-\nu'_{y_t}} \cdot g^{-a^{n-y_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_i^*}) \pi'_t (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_i^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\ &\quad \cdot \left(\prod_{t' \in [1, J]} g^{a^{n-y_{t'}} b / d_{t'}} \right)^{d_t \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\ &= g^{-\nu'_{y_t}} \cdot g^{-a^{n-y_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_i^*}) \pi'_t (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_i^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\ &\quad \cdot \left(\prod_{t' \in [1, J]} g^{a^{n-y_{t'}} b d_{t'} / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\ &= g^{-\nu'_{y_t}} \cdot g^{-a^{n-y_t} b \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} (h_8 h_9^{\sigma_i^*}) \pi'_t (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_i^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \\ &\quad \cdot \underbrace{\left(\prod_{\substack{t' \in [1, J] \\ t' \neq t}} g^{a^{n-y_{t'}} b d_{t'} / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t' \neq t} \cdot \underbrace{\left(g^{a^{n-y_t} b} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}}_{\text{for } t'=t} \\ &= g^{-\nu'_{y_t}} \cdot (h_8 h_9^{\sigma_i^*}) \pi'_t (g^{d_t})^{(\beta'_8 + \beta'_9 \sigma_i^*) \beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3} \cdot \left(\prod_{\substack{t' \in [1, J] \\ t' \neq t}} g^{a^{n-y_{t'}} b d_{t'} / d_{t'}} \right)^{\beta'_4 \beta'_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / \beta'_3}. \end{aligned}$$

Note that the values of $(P_1, P_2, P_3, P_4, P_5, P_6, \{P_{7,t}, P_{8,t}, P_{9,t}\}_{t \in [1, J]})$ can be calculated using the suitable terms of the assumption.

2. For each $i \in [m]$:

– if $i < \bar{i}$: it randomly chooses $\hat{s}_i \in \mathbb{Z}_p$, then sets

$$\begin{aligned} \mathbf{R}_i &= g^{\mathbf{v}_i}, \quad \mathbf{R}'_i = (g^{a^{n-1}c})^{\mathbf{v}_i}, \quad Q_i = g^{s_i}, \quad Q_{i,1} = h_1^{s_i} Z_i^{t_i} h_1^{\pi'}, \\ Q_{i,2} &= (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i} (g^b)^{\beta_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i}, \quad T_i = E_i^{\hat{s}_i}. \end{aligned}$$

– if $i = \bar{i}$: it sets

$$\begin{aligned} \mathbf{R}_i &= g^{r'_i s'_i \mathbf{v}_i^p} (g^{b/z})^{r'_i s'_i \mathbf{v}_i^q}, \quad \mathbf{R}'_i = (g^{a^{n-1}c})^{r'_i s'_i \mathbf{v}_i^p} (g^{a^{n-1}bc/z})^{r'_i s'_i \mathbf{v}_i^q}, \quad Q_i = g^{\tau' s'_i(\mathbf{v}_i^p \cdot \mathbf{v}_c^p)} (g^b)^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}, \\ Q_{i,1} &= h_1^{\tau' s'_i(\mathbf{v}_i^p \cdot \mathbf{v}_c^p)} Z_i^{t_i} h_1^{\pi'}, \quad Q_{i,2} = (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i}, \quad T_i = M \cdot e(g^{\alpha_i}, Q_i). \end{aligned}$$

– if $i > \bar{i}$: it sets

$$\begin{aligned} \mathbf{R}_i &= g^{r_i s_i \mathbf{v}_i}, \quad \mathbf{R}'_i = (g^{a^{n-1}c})^{r_i s_i \mathbf{v}_i}, \quad Q_i = (g^{a^{n-1}c})^{\tau' s_i(\mathbf{v}_i \cdot \mathbf{v}_c^p)}, \quad Q_{i,1} = Z_i^{t_i} h_1^{\pi'}, \\ Q_{i,2} &= (Q_i)^{\beta_2}, \quad Q'_i = g^{t_i} (g^{a^{n-1}c})^{-\beta_1 \tau' s_i(\mathbf{v}_i \cdot \mathbf{v}_c^p) / z'_i} (g^b)^{\beta_1 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i}, \quad T_i = M \cdot e(g^{\alpha_i}, Q_i). \end{aligned}$$

3. For each $j \in [m]$:

– if $j < \bar{j}$: it randomly chooses $\mu'_j \in \mathbb{Z}_N$ and implicitly sets the value of μ_j such that $(a^{n-1}bc)^{-1} \mu'_j \nu_3 - \nu_3 \equiv \mu_j \pmod{p_1}$, then sets $\mathbf{C}_j = (g^{a^{n-1}bc/z})^{c'_j \tau' \mathbf{v}_c^p} \cdot g^{c'_j \tau' \mu'_j \mathbf{v}_c^q} \cdot (g^{a^{n-1}c})^{\mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

- if $j = \bar{j}$: it sets $\mathbf{C}_j = T^{c_j' \tau' v_c^q} \cdot (g^{a^{n-1}c}) \mathbf{w}'_j$, $\mathbf{C}'_j = g^{\mathbf{w}'_j} \cdot (g^a)^{-c_j' \tau' v_c^q}$.
- if $j > \bar{j}$: it sets $\mathbf{C}_j = (g^{a^{n-1}bc/z})^{c_j' \tau' v_c^q} \cdot (g^{a^{n-1}c}) \mathbf{w}'_j$, $\mathbf{C}'_j = g^{\mathbf{w}'_j} \cdot (g^b)^{-c_j' \tau' v_c^q}$.

If $T = g^{a^{ncz}}$, then the ciphertext is a well-formed encryption to the index (\bar{i}, \bar{j}) . If T is randomly chosen, say $T = g^r$ for some random $r \in \mathbb{Z}_{p_1}$, the ciphertext is a well-formed encryption to the index $(\bar{i}, \bar{j} + 1)$ with implicitly setting $\mu_{\bar{j}}$ such that $(\frac{r}{a^{ncz}} - 1) \nu_3 \equiv \mu_{\bar{j}} \pmod{p_1}$.

Guess. \mathcal{A} outputs a guess $b' \in \{0, 1\}$ to \mathcal{B} , then \mathcal{B} outputs this b' to the challenger.

The distributions of the public parameters, private keys and challenge ciphertext are the same as that in the real scheme. \mathcal{B} 's advantage in the Modified (n, J) -EDHE2-Dual game will be exactly equal to \mathcal{A} 's advantage in the selective index-hiding game.

F Proof of the Lemma 1 for the Large Universe CP-ABE on Prime Order Groups

To make the proof easy to follow, we present the details of the resulting AugABE scheme first.

F.1 The Resulting Augmented CP-ABE

$\text{Setup}_A(\lambda, \Gamma, \mathcal{K} = m^2) \rightarrow (\text{PP}, \text{MSK})$. Run $(p, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$. Pick a generator $g \in \mathbb{G}$. Set $d = 4, d_0 = 1$. Pick random $\beta = (\beta_1, \dots, \beta_4) \in \mathbb{Z}_p^4$. Pick random $\{\alpha_i, r_i, z_i \in \mathbb{Z}_p\}_{i \in [m]}$, $\{c_j \in \mathbb{Z}_p\}_{j \in [m]}$. The public parameter is

$$\text{PP} = \left((p, \mathbb{G}, \mathbb{G}_T, e), g, \mathbf{h} = (h_1 = g^{\beta_1}, \dots, h_4 = g^{\beta_4}), \{E_i = e(g, g)^{\alpha_i}, G_i = g^{r_i}, Z_i = g^{z_i}\}_{i \in [m]}, \{H_j = g^{c_j}\}_{j \in [m]} \right).$$

The master secret key is $\text{MSK} = (\alpha_1, \dots, \alpha_m, r_1, \dots, r_m, c_1, \dots, c_m)$.

A counter $ctr = 0$ is implicitly included in MSK .

$\text{KeyGen}_A(\text{PP}, \text{MSK}, S \subseteq \mathbb{Z}_p) \rightarrow \text{SK}_{(i,j),S}$. Set $ctr = ctr + 1$ and then compute the corresponding index in the form of (i, j) where $1 \leq i, j \leq m$ and $(i - 1) * m + j = ctr$. Let $l \times n$ be the size of A . Pick random $\delta = (\delta_1, \{\theta_x\}_{x \in S}) \in \mathbb{Z}_p^{1+|S|}$. Output a secret key $\text{SK}_{(i,j),S}$ as

$$\text{SK}_{(i,j),S} = \left((i, j), S, K_0 = g^{r_i c_j + \alpha_i} g^{\beta_1 \delta_1}, K_1 = g^{\delta_1}, \{K_{x,2} = g^{\theta_x}, K_{x,3} = (g^{\beta_2 x} g^{\beta_3})^{\theta_x} (g^{\beta_4})^{-\delta_1}\}_{x \in S}, K'_0 = Z_i^{\delta_1} \right).$$

$\text{Encrypt}_A(\text{PP}, M, (A, \rho), (\bar{i}, \bar{j})) \rightarrow CT_{(A, \rho)}$.

1. Upon input a ciphertext policy $(A, \rho) \in \mathbb{Y}$, where A is an $l \times n$ matrix over \mathbb{Z}_p , and $\rho : [1, l] \rightarrow \mathbb{Z}_p$ maps each row of A to an attribute in \mathbb{Z}_p . Pick random $\pi = (\pi, u_2, \dots, u_n, \xi_1, \dots, \xi_l) \in \mathbb{Z}_p^{l+n}$ and set $\mathbf{u} := (\pi, u_2, \dots, u_n)$. Set

$$P_1 = g^\pi, \quad \{P_{k,1} = g^{\beta_1 (A_k \cdot \mathbf{u})} g^{\beta_4 \xi_k}, P_{k,2} = (g^{\beta_2 \rho(k)} g^{\beta_3})^{-\xi_k}, P_{k,3} = g^{\xi_k}\}_{k \in [l]}.$$

2. Pick random $\kappa, \tau, s_1, \dots, s_m, t_1, \dots, t_m \in \mathbb{Z}_p$, $\mathbf{v}_c, \mathbf{w}_1, \dots, \mathbf{w}_m \in \mathbb{Z}_p^3$.

Pick random $r_x, r_y, r_z \in \mathbb{Z}_p$, and set $\chi_1 = (r_x, 0, r_z), \chi_2 = (0, r_y, r_z), \chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$.

Pick random $\mathbf{v}_i \in \mathbb{Z}_p^3 \forall i \in \{1, \dots, \bar{i}\}$, $\mathbf{v}_i \in \text{span}\{\chi_1, \chi_2\} \forall i \in \{\bar{i} + 1, \dots, m\}$.

For each row $i \in [m]$:

- if $i < \bar{i}$: randomly choose $\hat{s}_i \in \mathbb{Z}_p$, and set

$$\mathbf{R}_i = g^{\mathbf{v}_i}, \mathbf{R}'_i = g^{\kappa \mathbf{v}_i}, Q_i = g^{s_i}, Q_{i,1} = (g^{\beta_1})^{s_i} Z_i^{t_i} (g^{\beta_1})^\pi, Q'_i = g^{t_i}, T_i = E_i^{\hat{s}_i}.$$

– if $i \geq \bar{i}$: set

$$\begin{aligned} \mathbf{R}_i &= G_i^{s_i \mathbf{v}_i}, \quad \mathbf{R}'_i = G_i^{\kappa s_i \mathbf{v}_i}, \quad Q_i = g^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}, \quad Q_{i,1} = (g^{\beta_1})^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)} Z_i^{t_i} (g^{\beta_1})^\pi, \\ Q'_i &= g^{t_i}, \quad T_i = M \cdot E_i^{\tau s_i (\mathbf{v}_i \cdot \mathbf{v}_c)}. \end{aligned}$$

Note that $d_0 = 1$, thus there is only $Q_{i,1}$.

For each column $j \in [m]$:

– if $j < \bar{j}$: randomly choose $\mu_j \in \mathbb{Z}_p$, and set $\mathbf{C}_j = H_j^{\tau(\mathbf{v}_c + \mu_j \chi_3)} \cdot g^{\kappa \mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

– if $j \geq \bar{j}$: set $\mathbf{C}_j = H_j^{\tau \mathbf{v}_c} \cdot g^{\kappa \mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.

3. Output the ciphertext $CT_{(A,\rho)} = \langle (A, \rho), (P_1, \{P_{k,1}, P_{k,2}, P_{k,3}\}_{k \in [l]}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$.

$\text{Decrypt}_A(\text{PP}, CT_{(A,\rho)}, \text{SK}_{(i,j),S}) \rightarrow M$ or \perp . Parse $CT_{(A,\rho)}$ to $CT_{(A,\rho)} = \langle (A, \rho), (P_1, \{P_{k,1}, P_{k,2}, P_{k,3}\}_{k \in [l]}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q'_i, T_i)_{i=1}^m, (\mathbf{C}_j, \mathbf{C}'_j)_{j=1}^m \rangle$ and $\text{SK}_{(i,j),S}$ to $\text{SK}_{(i,j),S} = ((i, j), S, (K_0, K_1, \{K_{x,2}, K_{x,3}\}_{x \in S}, K'_0))$. Suppose S satisfies (A, ρ) (if S does not satisfies (A, ρ) , output \perp).

1. Compute constants $\{\omega_k\}_{\rho(k) \in S}$ such that $\sum_{\rho(k) \in S} \omega_k A_k = (1, 0, \dots, 0)$. Compute

$$D_P \leftarrow \prod_{\rho(k) \in S} (e(K_1, P_{k,1}) \cdot e(K_{\rho(k),2}, P_{k,2}) \cdot e(K_{\rho(k),3}, P_{k,3}))^{\omega_k}$$

2. Compute

$$D_I \leftarrow \frac{e(K_0, Q_i) \cdot e(K'_0, Q'_i)}{e(K_1, Q_{i,1})} \cdot \frac{e_3(\mathbf{R}'_i, \mathbf{C}'_j)}{e_3(\mathbf{R}_i, \mathbf{C}_j)}.$$

3. Computes $M \leftarrow T_i / (D_P \cdot D_I)$ as the output message.

F.2 Proof of Lemma 1

Proof. Suppose there exists a polynomial time adversary \mathcal{A} that selectively breaks the index-hiding game with advantage ϵ . We build a PPT algorithm \mathcal{B} to solve an Extended Source Group q -parallel BDHE problem as follows. \mathcal{B} is given a problem instance as

$$\begin{aligned} D = & ((p, \mathbb{G}, \mathbb{G}_T, e), g, g^d, g^{cd}, g^{da^q}, \\ & g^{a^i}, g^{b_j}, g^{a^i b_j}, g^{a^i/b_j^2}, g^{cdb_j} \quad \forall i, j \in [q], \\ & g^{a^i/b_j} \quad \forall i \in [2q] \setminus \{q+1\}, j \in [q], \\ & g^{a^i b_{j'}/b_j^2} \quad \forall i \in [2q], j, j' \in [q] \text{ s.t. } j' \neq j, \\ & g^{cda^i b_{j'}/b_j}, g^{cda^i b_{j'}/b_j^2} \quad \forall i \in [q], j, j' \in [q] \text{ s.t. } j \neq j') \end{aligned}$$

and T , where $(p, \mathbb{G}, \mathbb{G}_T, e) \xleftarrow{R} \mathcal{G}$, $g \xleftarrow{R} \mathbb{G}$, $a, c, d, b_1, \dots, b_q \xleftarrow{R} \mathbb{Z}_p$, and T is either equal to $g^{ca^{q+1}}$ or is a random element of \mathbb{G} . \mathcal{B} 's goal is to determine $T = g^{ca^{q+1}}$ or T is a random element from \mathbb{G} .

Init. \mathcal{A} gives \mathcal{B} the challenge LSSS matrix (A^*, ρ^*) , where A^* is an $l \times n$ matrix with $l, n \leq q$.

Setup. \mathcal{B} randomly chooses $\{\alpha_i \in \mathbb{Z}_p\}_{i \in [m]}$, $\{r_i, z'_i \in \mathbb{Z}_p\}_{i \in [m] \setminus \{\bar{i}\}}$, $r'_i, z_i \in \mathbb{Z}_p$, $\{c'_j \in \mathbb{Z}_p\}_{j \in [m]}$, and $\beta'_2, \beta'_3, \beta'_4 \in \mathbb{Z}_p$. \mathcal{B} gives \mathcal{A} the public parameter PP :

$$\begin{aligned} & (g, h_1 = g^a, h_2 = g^{\beta_2} \cdot \prod_{k \in [l]} \prod_{t \in [n]} (g^{a^t/b_k^2})^{A_{k,t}^*}, \\ & h_3 = g^{\beta_3} \cdot \prod_{k \in [l]} \prod_{t \in [n]} (g^{a^t/b_k^2})^{-\rho^*(k) A_{k,t}^*}, h_4 = g^{\beta_4} \cdot \prod_{k \in [l]} \prod_{t \in [n]} (g^{a^t/b_k})^{A_{k,t}^*}, \\ & \{E_i = e(g, g)^{\alpha_i}\}_{i \in [m]}, \end{aligned}$$

$$\{G_i = g^{r_i}, Z_i = (g^a)^{z_i}\}_{i \in [m] \setminus \{\bar{i}\}}, \{H_j = (g^d)^{c_j}\}_{j \in [m] \setminus \{\bar{j}\}}, \quad G_{\bar{i}} = (g^{a^q})^{r_{\bar{i}}}, Z_{\bar{i}} = g^{z_{\bar{i}}}, H_{\bar{j}} = (g^a)^{c_{\bar{j}}}.$$

Note that \mathcal{B} implicitly chooses $r_{\bar{i}}, z_i (i \in [m] \setminus \{\bar{i}\}), c_j (j \in [m]), \beta_1, \beta_2, \beta_3, \beta_4 \in \mathbb{Z}_p$ such that

$$\begin{aligned} a^q r_{\bar{i}} &\equiv r_{\bar{i}} \pmod{p}, \quad a z_i \equiv z_i \pmod{p} \quad \forall i \in [m] \setminus \{\bar{i}\}, \\ d c_j &\equiv c_j \pmod{p} \quad \forall j \in [m] \setminus \{\bar{j}\}, \quad a c_{\bar{j}} \equiv c_{\bar{j}} \pmod{p}, \\ a &\equiv \beta_1 \pmod{p}, \quad \beta'_2 + \sum_{k \in [l]} \sum_{t \in [n]} (a^t / b_k^2) (A_{k,t}^*) \equiv \beta_2 \pmod{p}, \\ \beta'_3 + \sum_{k \in [l]} \sum_{t \in [n]} (a^t / b_k^2) (-\rho^*(k) A_{k,t}^*) &\equiv \beta_3 \pmod{p}, \\ \beta'_4 + \sum_{k \in [l]} \sum_{t \in [n]} (a^t / b_k) (A_{k,t}^*) &\equiv \beta_4 \pmod{p}, \end{aligned}$$

Query Phase. To respond to \mathcal{A} 's query for $((i, j), S)$,

- if $(i, j) \neq (\bar{i}, \bar{j})$: \mathcal{B} picks random $\delta = (\delta_1, \{\theta_x\}_{x \in S}) \in \mathbb{Z}_p^{1+|S|}$, then creates a secret key $\text{SK}_{(i,j),S}$:

$$\begin{aligned} K_0 &= \begin{cases} g^{\alpha_i} (g^d)^{r_i c_j} h_1^{\delta_1}, & : i \neq \bar{i}, j \neq \bar{j} \\ g^{\alpha_i} (g^{da^q})^{r_i c_j} h_1^{\delta_1}, & : i = \bar{i}, j \neq \bar{j} \\ g^{\alpha_i} (g^a)^{r_i c_j} h_1^{\delta_1}, & : i \neq \bar{i}, j = \bar{j} \end{cases} \\ K_1 &= g^{\delta_1}, \quad K'_0 = Z_i^{\delta_1}, \\ \{K_{x,2} = g^{\theta_x}, K_{x,3} = (h_2^x h_3)^{\theta_x} h_4^{-\delta_1}\}_{x \in S}. \end{aligned}$$

- if $(i, j) = (\bar{i}, \bar{j})$: it implies that \mathcal{A} is querying a secret key with the challenge index (\bar{i}, \bar{j}) , and S does not satisfy (A^*, ρ^*) . \mathcal{B} first computes a vector $\bar{u} = (\bar{u}_1, \dots, \bar{u}_n) \in \mathbb{Z}_p^n$ that has first entry equal to $-r_{\bar{i}}' c_{\bar{j}}'$ (i.e. $\bar{u}_1 = -r_{\bar{i}}' c_{\bar{j}}'$) and is orthogonal to all of the rows A_k^* of A^* such that $\rho^*(k) \in S$ (i.e. $A_k^* \cdot \bar{u} = 0 \quad \forall k \in [l] \text{ s.t. } \rho^*(k) \in S$). Note that such a vector must exist since S fails to satisfy (A^*, ρ^*) , and it is efficiently computable. Then \mathcal{B} randomly chooses $(\delta'_1, \{\theta'_x\}_{x \in S}) \in \mathbb{Z}_p^{1+|S|}$ and sets the values of δ_1 and $\{\theta_x\}_{x \in S}$ by implicitly setting

$$\delta_1 = \delta'_1 + \sum_{t \in [n]} \bar{u}_t a^{q+1-t}, \quad (1)$$

$$\theta_x = \theta'_x + \delta'_1 \cdot \sum_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} \frac{b_{k'}}{x - \rho^*(k')} + \sum_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} \sum_{t \in [n]} \frac{\bar{u}_t b_{k'} a^{q+1-t}}{x - \rho^*(k')}. \quad (2)$$

Note that for $x \in S$ and $\rho^*(k') \notin S$ we have $x - \rho^*(k') \neq 0$.

\mathcal{B} creates a secret key $\text{SK}_{(\bar{i}, \bar{j}), S}$ as follows:

$$K_0 = g^{\alpha_{\bar{i}}} h_1^{\delta'_1} \left(\prod_{t=2}^n (g^{a^{q+2-t}})^{\bar{u}_t} \right), \quad K_1 = g^{\delta'_1} \prod_{t=1}^n (g^{a^{q+1-t}})^{\bar{u}_t}, \quad K'_0 = (K_1)^{z_{\bar{i}}},$$

For $x \in S$, we have

$$K_{x,2} = g^{\theta_x} = g^{\theta'_x} \cdot \left(\prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} (g^{b_{k'}})^{\delta'_1 / (x - \rho^*(k'))} \right) \cdot \left(\prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} \prod_{t \in [n]} (g^{b_{k'} a^{q+1-t}})^{\bar{u}_t / (x - \rho^*(k'))} \right),$$

Note that for $x \in S$, we have

$$(h_2^x h_3)^{\theta_x} = \underbrace{(h_2^x h_3)^{\theta'_x}}_{\Psi_{1,1}} \cdot (h_2^x h_3)^{\delta'_1 \cdot \sum_{k' \in [l], \rho^*(k') \notin S} \frac{b_{k'}}{x - \rho^*(k')}} \cdot (h_2^x h_3)^{\sum_{k' \in [l], \rho^*(k') \notin S} \sum_{t \in [n]} \frac{\bar{u}_t b_{k'} a^{q+1-t}}{x - \rho^*(k')}}.$$

$$\begin{aligned}
&= \Psi_{1,1} \cdot \left(\prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} (g^{\beta'_2 x + \beta'_3} \prod_{k \in [l]} \prod_{t \in [n]} (g^{a^t/b_k^2})^{(x-\rho^*(k))A_{k,t}^*})^{\frac{\delta'_1 b_{k'}}{x-\rho^*(k')}} \right) \\
&\quad \cdot \left(\prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} \prod_{t' \in [n]} (g^{\beta'_2 x + \beta'_3} \prod_{k \in [l]} \prod_{t \in [n]} (g^{a^t/b_k^2})^{(x-\rho^*(k))A_{k,t}^*})^{\frac{\bar{u}_{t'} b_{k'} a^{q+1-t'}}{x-\rho^*(k')}} \right) \\
&= \Psi_{1,1} \cdot \underbrace{\left(\prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} (g^{b_{k'}})^{\sigma'_1 \cdot (\beta'_2 x + \beta'_3) / (x-\rho^*(k'))} \right)}_{\Psi_{1,2}} \cdot \left(\prod_{k \in [l]} \prod_{t \in [n]} \prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} (g^{a^t b_{k'} / b_k^2})^{\delta'_1 A_{k,t}^* \frac{x-\rho^*(k)}{x-\rho^*(k')}} \right) \\
&\quad \cdot \underbrace{\left(\prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} \prod_{t' \in [n]} (g^{b_{k'} a^{q+1-t'}})^{\bar{u}_{t'} (\beta'_2 x + \beta'_3) / (x-\rho^*(k'))} \right)}_{\Psi_{1,3}} \\
&\quad \cdot \left(\prod_{k \in [l]} \prod_{t \in [n]} \prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} \prod_{t' \in [n]} (g^{a^{q+1-t'+t} b_{k'} / b_k^2})^{A_{k,t}^* \bar{u}_{t'} \frac{x-\rho^*(k)}{x-\rho^*(k')}} \right) \\
&= \Psi_{1,1} \cdot \Psi_{1,2} \cdot \underbrace{\left(\prod_{\substack{k \in [l] \\ \rho^*(k) \in S}} \prod_{t \in [n]} \prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} (g^{a^t b_{k'} / b_k^2})^{\delta'_1 A_{k,t}^* \frac{x-\rho^*(k)}{x-\rho^*(k')}} \right)}_{\Psi_{1,4} \text{ (for } \rho^*(k) \in S)} \\
&\quad \cdot \underbrace{\left(\prod_{\substack{k \in [l] \\ \rho^*(k) \notin S}} \prod_{t \in [n]} \prod_{\substack{k' \in [l] \setminus \{k\} \\ \rho^*(k') \notin S}} (g^{a^t b_{k'} / b_k^2})^{\delta'_1 A_{k,t}^* \frac{x-\rho^*(k)}{x-\rho^*(k')}} \right)}_{\Psi_{1,5} \text{ (for } \rho^*(k) \notin S, k' \neq k)} \cdot \underbrace{\left(\prod_{k \in [l]} \prod_{t \in [n]} (g^{a^t / b_k})^{\delta'_1 A_{k,t}^*} \right)}_{\Psi_{1,6} \text{ (for } \rho^*(k) \notin S, k'=k)} \cdot \Psi_{1,3} \\
&\quad \cdot \underbrace{\left(\prod_{\substack{k \in [l] \\ \rho^*(k) \in S}} \prod_{t \in [n]} \prod_{\substack{k' \in [l] \\ \rho^*(k') \notin S}} \prod_{t' \in [n]} (g^{a^{q+1-t'+t} b_{k'} / b_k^2})^{A_{k,t}^* \bar{u}_{t'} \frac{x-\rho^*(k)}{x-\rho^*(k')}} \right)}_{\Psi_{1,7} \text{ (for } \rho^*(k) \in S)} \\
&\quad \cdot \underbrace{\left(\prod_{\substack{k \in [l] \\ \rho^*(k) \notin S}} \prod_{t \in [n]} \prod_{\substack{k' \in [l] \setminus \{k\} \\ \rho^*(k') \notin S}} \prod_{t' \in [n]} (g^{a^{q+1-t'+t} b_{k'} / b_k^2})^{A_{k,t}^* \bar{u}_{t'} \frac{x-\rho^*(k)}{x-\rho^*(k')}} \right)}_{\Psi_{1,8} \text{ (for } \rho^*(k) \notin S, k' \neq k)} \\
&\quad \cdot \underbrace{\left(\prod_{\substack{k \in [l] \\ \rho^*(k) \notin S}} \prod_{t \in [n]} \prod_{t' \in [n]} (g^{a^{q+1-t'+t} / b_k})^{A_{k,t}^* \bar{u}_{t'}} \right)}_{\text{(for } \rho^*(k) \notin S, k'=k)} \\
&= \underbrace{\Psi_{1,1} \cdot \Psi_{1,2} \cdot \Psi_{1,4} \cdot \Psi_{1,5} \cdot \Psi_{1,6} \cdot \Psi_{1,3} \cdot \Psi_{1,7} \cdot \Psi_{1,8}}_{\Psi_1} \cdot \left(\prod_{\substack{k \in [l] \\ \rho(k) \notin S}} \prod_{t \in [n]} \prod_{t' \in [n]} (g^{a^{q+1-t'+t} / b_k})^{A_{k,t}^* \bar{u}_{t'}} \right),
\end{aligned}$$

$$h_4^{-\delta_1} = h_4^{-\delta'_1} (g^{\beta'_4} \prod_{k \in [l]} \prod_{t \in [n]} (g^{a^t / b_k})^{A_{k,t}^*})^{-\sum_{t' \in [n]} \bar{u}_{t'} a^{q+1-t'}}$$

$$\begin{aligned}
&= h_4^{-\delta'_1} \left(\prod_{t' \in [n]} (g^{a^{q+1}-t'})^{-\beta'_4 \bar{u}_{t'}} \right) \cdot \left(\prod_{k \in [l]} \prod_{t \in [n]} \prod_{t' \in [n]} (g^{a^{q+1}-t'+t}/b_k)^{-A_{k,t}^* \bar{u}_{t'}} \right) \\
&\quad \underbrace{\hspace{10em}}_{\Psi_2} \\
&= \Psi_2 \cdot \left(\prod_{k \in [l]} \prod_{t \in [n]} \prod_{t' \in [n]} (g^{a^{q+1}-t'+t}/b_k)^{-A_{k,t}^* \bar{u}_{t'}} \right),
\end{aligned}$$

where $\Psi_1 = \Psi_{1,1} \cdot \Psi_{1,2} \cdots \Psi_{1,8}$ and Ψ_2 can be calculated using the suitable terms of the assumption. Thus, we have

$$\begin{aligned}
K_{x,3} &= (h_2^x h_3)^{\theta_x} h_4^{-\delta_1} \\
&= \Psi_1 \cdot \Psi_2 \cdot \left(\prod_{\substack{k \in [l] \\ \rho^*(k) \in S}} \prod_{t \in [n]} \prod_{t' \in [n]} (g^{a^{q+1}-t'+t}/b_k)^{-A_{k,t}^* \bar{u}_{t'}} \right) \\
&= \Psi_1 \cdot \Psi_2 \cdot \left(\prod_{\substack{k \in [l] \\ \rho^*(k) \in S}} \prod_{t \in [n]} \prod_{t' \in [n] \setminus \{t\}} (g^{a^{q+1}-t'+t}/b_k)^{-A_{k,t}^* \bar{u}_{t'}} \right) \cdot \left(\prod_{\substack{k \in [l] \\ \rho^*(k) \in S}} \prod_{t \in [n]} (g^{a^{q+1}/b_k})^{-A_{k,t}^* \bar{u}_t} \right) \\
&\quad \underbrace{\hspace{10em}}_{\Psi_3 \text{ (for } t' \neq t)} \quad \underbrace{\hspace{10em}}_{\text{for } t'=t} \\
&= \Psi_1 \cdot \Psi_2 \cdot \Psi_3 \cdot \left(\prod_{\substack{k \in [l] \\ \rho^*(k) \in S}} (g^{a^{q+1}/b_k})^{-A_k^* \bar{\mathbf{u}}} \right) \\
&= \Psi_1 \cdot \Psi_2 \cdot \Psi_3, \quad (\text{since } A_k^* \cdot \bar{\mathbf{u}} = 0 \forall k \in [l] \text{ s.t. } \rho^*(k) \in S)
\end{aligned}$$

Note that Ψ_1 , Ψ_2 and Ψ_3 can be calculated using the suitable terms of the assumption, \mathcal{B} can calculate $K_{x,3}$.

Challenge. \mathcal{A} submits a message M . \mathcal{B} randomly chooses

$$\begin{aligned}
\tau', s_1, \dots, s_{\bar{i}-1}, s'_{\bar{i}}, s_{\bar{i}+1}, \dots, s_m &\in \mathbb{Z}_p, \\
t'_1, \dots, t'_{\bar{i}-1}, t'_{\bar{i}}, t'_{\bar{i}+1}, \dots, t'_m &\in \mathbb{Z}_p, \\
\mathbf{w}_1, \dots, \mathbf{w}_{\bar{j}-1}, \mathbf{w}'_{\bar{j}}, \dots, \mathbf{w}'_m &\in \mathbb{Z}_p^3, \\
\xi'_1, \dots, \xi'_l, \pi' \in \mathbb{Z}_p, \mathbf{u}' = (0, u'_2, \dots, u'_n) &\in \mathbb{Z}_p^n.
\end{aligned}$$

\mathcal{B} randomly chooses $r_x, r_y, r_z \in \mathbb{Z}_p$, and sets $\chi_1 = (r_x, 0, r_z)$, $\chi_2 = (0, r_y, r_z)$, $\chi_3 = \chi_1 \times \chi_2 = (-r_y r_z, -r_x r_z, r_x r_y)$, then randomly chooses

$$\begin{aligned}
\mathbf{v}_i &\in \mathbb{Z}_p^3 \forall i \in \{1, \dots, \bar{i} - 1\}, \\
\mathbf{v}_i^p &\in \text{span}\{\chi_1, \chi_2\}, \mathbf{v}_i^q \in \text{span}\{\chi_3\}, \\
\mathbf{v}_i &\in \text{span}\{\chi_1, \chi_2\} \forall i \in \{\bar{i} + 1, \dots, m\}, \\
\mathbf{v}_c^p &\in \text{span}\{\chi_1, \chi_2\}, \mathbf{v}_c^q = \nu_c \chi_3 \in \text{span}\{\chi_3\}.
\end{aligned}$$

\mathcal{B} sets the values of $\kappa, \tau, s_{\bar{i}}, t_i (i \in [m] \setminus \{\bar{i}\}) \in \mathbb{Z}_p, \mathbf{v}_{\bar{i}}, \mathbf{v}_c, \mathbf{w}_j (j \in \{\bar{j}, \dots, m\}) \in \mathbb{Z}_p^3, \pi \in \mathbb{Z}_p, \mathbf{u} \in \mathbb{Z}_p^n$, and $\{\xi_k \in \mathbb{Z}_p\}_{k \in [l]}$ by implicitly setting

$$\begin{aligned}
a^q &\equiv \kappa \pmod{p}, \quad ca^q \tau' \equiv \tau \pmod{p}, \quad s'_i/a^q \equiv s_{\bar{i}} \pmod{p}, \\
\forall i \in \{1, \dots, \bar{i} - 1\} : \quad t'_i + cd\tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i &\equiv t_i \pmod{p}, \\
\forall i \in \{\bar{i} + 1, \dots, m\} : \quad t'_i - a^q \tau' s_i (\mathbf{v}_i \cdot \mathbf{v}_c^p) / z'_i + cd\tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i &\equiv t_i \pmod{p}, \\
\mathbf{v}_{\bar{i}} &= \mathbf{v}_i^p + d\mathbf{v}_i^q, \quad \mathbf{v}_c = c^{-1} \mathbf{v}_c^p + \mathbf{v}_c^q, \\
\mathbf{w}'_j - ac'_j \tau' \mathbf{v}_c^p &\equiv \mathbf{w}_j \pmod{p}, \\
\forall j \in \{\bar{j} + 1, \dots, m\} : \quad \mathbf{w}'_j - cdc'_j \tau' \mathbf{v}_c^q &\equiv \mathbf{w}_j \pmod{p},
\end{aligned}$$

$$\begin{aligned}\pi' - cd\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) &\equiv \pi \pmod{p}, \quad \mathbf{u} = \pi(1, a, a^2, \dots, a^{n-1}) + \mathbf{u}', \\ \forall k \in [l]: \quad \xi'_k + cdb_k \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) &\equiv \xi_k \pmod{p}.\end{aligned}$$

It is worth noticing that \mathbf{v}_i and \mathbf{v}_c are chosen from \mathbb{Z}_p^3 at random as required, and $(\mathbf{v}_i \cdot \mathbf{v}_c) = \frac{1}{c}(\mathbf{v}_i^p \cdot \mathbf{v}_c^p) + d(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)$, since χ_3 is orthogonal to $\text{span}\{\chi_1, \chi_2\}$ and $\mathbb{Z}_p^3 = \text{span}\{\chi_1, \chi_2, \chi_3\}$. \mathcal{B} creates a ciphertext $\langle (A^*, \rho^*), (P_1, \{P_{k,1}, P_{k,2}, P_{k,3}\}_{k \in [l]}), (\mathbf{R}_i, \mathbf{R}'_i, Q_i, Q_{i,1}, Q'_i, T_i)_{i=1}^m, (C_j, C'_j)_{j=1}^m \rangle$ as follows:

1. $P_1 = g^{\pi'} (g^{cd})^{-\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}$,
For each $k \in [l]$: we have

$$\begin{aligned}P_{k,1} &= (h_1)^{A_k^* \cdot \mathbf{u}} h_4^{\xi_k} = (h_1)^{A_k^* \cdot (1, a, \dots, a^{n-1})} \pi \cdot \underbrace{h_1^{A_k^* \cdot \mathbf{u}'}}_{\Phi_1} \cdot h_4^{\xi'_k} \cdot (g^{\beta'_4} \prod_{k' \in [l]} \prod_{t \in [n]} (g^{a^t/b_{k'}})^{A_{k',t}^*})^{cdb_k \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)} \\ &= \left(\prod_{t \in [n]} (g^{a^t})^{A_{k,t}^*} \right)^{\pi' - cd\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)} \cdot \Phi_1 \cdot \underbrace{(g^{cdb_k})^{\beta'_4 \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}}_{\Phi_2} \cdot \left(\prod_{k' \in [l]} \prod_{t \in [n]} (g^{cda^t b_k/b_{k'}})^{A_{k',t}^*} \right)^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)} \\ &= \underbrace{\left(\prod_{t \in [n]} (g^{a^t})^{A_{k,t}^*} \right)^{\pi'}}_{\Phi_3} \cdot \underbrace{\left(\prod_{t \in [n]} (g^{cda^t})^{A_{k,t}^*} \right)^{-\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}}_{\Delta} \cdot \Phi_1 \cdot \Phi_2 \\ &\quad \cdot \underbrace{\left(\prod_{k' \in [l] \setminus \{k\}} \prod_{t \in [n]} (g^{cda^t b_k/b_{k'}})^{A_{k',t}^*} \right)^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}}_{\Phi_4 \text{ (for } k' \neq k)} \cdot \underbrace{\left(\prod_{t \in [n]} (g^{cda^t})^{A_{k,t}^*} \right)^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}}_{\Delta^{-1} \text{ (for } k'=k)} \\ &= \Phi_3 \cdot \Phi_1 \cdot \Phi_2 \cdot \Phi_4, \\ P_{k,2} &= (h_2^{\rho^*(k)} h_3)^{-\xi_k} \\ &= (h_2^{\rho^*(k)} h_3)^{-\xi'_k} \cdot (g^{\beta'_2 \rho^*(k) + \beta'_3})^{-cdb_k \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)} \cdot \left(\prod_{k' \in [l]} \prod_{t \in [n]} (g^{a^t/b_{k'}})^{(\rho^*(k) - \rho^*(k')) A_{k',t}^*} \right)^{-cdb_k \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)} \\ &= \underbrace{(h_2^{\rho^*(k)} h_3)^{-\xi'_k} \cdot (g^{cdb_k})^{-(\beta'_2 \rho^*(k) + \beta'_3) \tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}}_{\Phi_5} \cdot \left(\prod_{k' \in [l]} \prod_{t \in [n]} (g^{cda^t b_k/b_{k'}^2})^{(\rho^*(k') - \rho^*(k)) A_{k',t}^*} \right)^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)} \\ &= \Phi_5 \cdot \underbrace{\left(\prod_{k' \in [l] \setminus \{k\}} \prod_{t \in [n]} (g^{cda^t b_k/b_{k'}^2})^{(\rho^*(k') - \rho^*(k)) A_{k',t}^*} \right)^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}}_{\Phi_6 \text{ (for } k' \neq k)} \\ &\quad \cdot \underbrace{\left(\prod_{t \in [n]} (g^{cda^t b_k/b_k^2})^{(\rho^*(k) - \rho^*(k)) A_{k,t}^*} \right)^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}}_1 \text{ (for } k'=k) \\ &= \Phi_5 \cdot \Phi_6, \\ P_{k,3} &= g^{\xi_k} = g^{\xi'_k} (g^{cdb_k})^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}.\end{aligned}$$

Note that Φ_1, \dots, Φ_6 can be calculated using the suitable terms of the assumption, \mathcal{B} can calculate $P_{k,1}, P_{k,2}, P_{k,3}$.

2. For each $i \in [m]$:

– if $i < \bar{i}$: randomly chooses $\hat{s}_i \in \mathbb{Z}_p$, and sets

$$\begin{aligned}\mathbf{R}_i &= g^{v_i}, \quad \mathbf{R}'_i = (g^{a^q})^{v_i}, \\ Q_i &= g^{s_i}, \quad Q_{i,1} = (g^a)^{s_i} Z_i^{t'_i} (g^a)^{\pi'}, \quad Q'_i = g^{t'_i} (g^{cd})^{\tau' s'_i(\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i}, \quad T_i = E_i^{\hat{s}_i}.\end{aligned}$$

– if $i = \bar{i}$: sets

$$\begin{aligned} \mathbf{R}_i &= g^{r'_i s'_i \mathbf{v}_i^p} \cdot (g^d)^{r'_i s'_i \mathbf{v}_i^q}, \quad \mathbf{R}'_i = (g^{a^q})^{r'_i s'_i \mathbf{v}_i^p} \cdot (g^{da^q})^{r'_i s'_i \mathbf{v}_i^q}, \\ Q_i &= g^{\tau' s'_i (\mathbf{v}_i^p \cdot \mathbf{v}_c^p)} (g^{cd})^{\tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q)}, \quad Q_{i,1} = (g^a)^{\tau' s'_i (\mathbf{v}_i^p \cdot \mathbf{v}_c^p)} Z_i^{t_i} (g^a)^\pi, \quad Q'_i = g^{t_i}, \\ T_i &= M \cdot e(g^{\alpha_i}, Q_i). \end{aligned}$$

– if $i > \bar{i}$: sets

$$\begin{aligned} \mathbf{R}_i &= g^{r_i s_i \mathbf{v}_i}, \quad \mathbf{R}'_i = (g^{a^q})^{r_i s_i \mathbf{v}_i}, \\ Q_i &= (g^{a^q})^{\tau' s_i (\mathbf{v}_i \cdot \mathbf{v}_c^p)}, \quad Q_{i,1} = Z_i^{t_i} (g^a)^\pi, \quad Q'_i = g^{t_i} (g^{a^q})^{-\tau' s_i (\mathbf{v}_i \cdot \mathbf{v}_c^p) / z'_i} (g^{cd})^{\tau' s'_i (\mathbf{v}_i^q \cdot \mathbf{v}_c^q) / z'_i}, \\ T_i &= M \cdot e(g^{\alpha_i}, Q_i). \end{aligned}$$

3. For each $j \in [m]$:

- if $j < \bar{j}$: randomly chooses $\mu'_j \in \mathbb{Z}_p$ and implicitly sets the value of μ_j such that $(\mu'_j / (cda^q) - 1) \nu_c \equiv \mu_j \pmod{p}$, then sets: $\mathbf{C}_j = (g^{da^q})^{c'_j \tau' \mathbf{v}_c^p} \cdot g^{c'_j \tau' \mu'_j \mathbf{v}_c^q} \cdot (g^{a^q})^{\mathbf{w}_j}$, $\mathbf{C}'_j = g^{\mathbf{w}_j}$.
- if $j = \bar{j}$: sets $\mathbf{C}_j = T^{c'_j \tau' \mathbf{v}_c^q} \cdot (g^{a^q})^{\mathbf{w}'_j}$, $\mathbf{C}'_j = g^{\mathbf{w}'_j} \cdot (g^a)^{-c'_j \tau' \mathbf{v}_c^p}$.
- if $j > \bar{j}$: sets $\mathbf{C}_j = (g^{da^q})^{c'_j \tau' \mathbf{v}_c^p} \cdot (g^{a^q})^{\mathbf{w}'_j}$, $\mathbf{C}'_j = g^{\mathbf{w}'_j} \cdot (g^{cd})^{-c'_j \tau' \mathbf{v}_c^q}$.

If $T = g^{ca^{q+1}}$, the ciphertext is a well-formed encryption to the index (\bar{i}, \bar{j}) . If T is randomly chosen, say $T = g^r$ for some random $r \in \mathbb{Z}_p$, the ciphertext is a well-formed encryption to the index $(\bar{i}, \bar{j} + 1)$ with implicit setting $\mu_{\bar{j}}$ such that $(\frac{r}{ca^{q+1}} - 1) \nu_c \equiv \mu_{\bar{j}} \pmod{p}$.

Guess. \mathcal{A} outputs a guess $b' \in \{0, 1\}$ to \mathcal{B} , then \mathcal{B} outputs this b' to the challenger.

The distributions of the public parameters, private keys and challenge ciphertext are the same as that in the real scheme. \mathcal{B} 's advantage in solving the Extended Source Group q -parallel BDHE problem will be exactly equal to \mathcal{A} 's advantage in the selective index-hiding game.