Attribute based Encryption: Traitor Tracing, Revocation and Fully Security on Prime Order Groups

Xiaoyi Li[1], Kaitai Liang[2], Zhen Liu[1] and Duncan Wong[1]
[1]*Security and Data Sciences, Hong Kong Applied Science and Technology Research Institute, Hong Kong SAR, China*
[2]*School of Computing, Mathematics and Digital Technology, Manchester Metropolitan University, Manchester, U.K.*

Keywords: Traitor Tracing, Revocation, Ciphertext-policy Attribute based Encryption, Prime Order Groups.

Abstract: A Ciphertext-Policy Attribute-Based Encryption (CP-ABE) allows users to specify the access policies without having to know the identities of users. In this paper, we contribute by proposing an ABE scheme which enables revoking corrupted users. Given a key-like blackbox, our system can identify at least one of the users whose key must have been used to construct the blackbox and can revoke the key from the system. This paper extends the work of Liu and Wong to achieve traitor revocability. We construct an Augmented Revocable CP-ABE (AugR-CP-ABE) scheme, and describe its security by message-hiding and index-hiding games. Then we prove that an AugR-CP-ABE scheme with message-hiding and index-hiding properties can be transferred to a secure Revocable CP-ABE with fully collusion-resistant blackbox traceability. In the proof for index-hiding, we divide the adversary's behaviors in two ways and build direct reductions that use adversary to solve the D3DH problem. Our scheme achieves the sub-linear overhead of $O(\sqrt{N})$, where N is the number of users in the system. This scheme is highly expressive and can take any monotonic access structures as ciphertext policies.

1 INTRODUCTION

Attribute-Based Encryption (ABE) system is first introduced by Sahai and Waters (Sahai and Waters, 2005), which is based on users' roles and does not have to know their identities in the system. In an Attribute-Based Encryption (CP-ABE) system, each user possesses a set of attributes and a private key generated based on his/her attributes. The encrypting party will define an *access policy* over role-based/descriptive *attributes* to encrypt a message without having to know the identities of the targeted receivers. As a result, only the user who owns the appropriate attributes which satisfy the access policy are able to decrypt the ciphertext. Among the CP-ABE schemes recently proposed, (Bethencourt et al., 2007; Cheung and Newport, 2007; Goyal et al., 2008; Waters, 2011; Lewko et al., 2010; Okamoto and Takashima, 2010; Herranz et al., 2010; Lewko and Waters, 2012a; Rouselakis and Waters, 2013), progress has been made with regard to the schemes' security, access policy expressivity, and efficiency. While the schemes with practical security and expressivity (i.e. full security against adaptive adversaries in the standard model and high expressivity of supporting any monotone access structures) have been proposed in (Lewko et al., 2010; Okamoto and Takashima, 2010; Lewko and Waters, 2012a), the traceability of traitors which intentionally expose their decryption keys has become an important concern related to the applicability of CP-ABE. Assume in a communication system, the sender wants to assure that only those users who have paid for the service can access the content. This concern can be solved by encrypting the content and only receivers who own the legitimate keys can decrypt the content correctly. If we build such a system with ABE, however, due to the nature of CP-ABE, the attributes (and the corresponding decryption privilege) are generally *shared* by multiple users. As a result, a malicious user, with his attributes shared with multiple other users, might have an intention to leak the corresponding decryption key or some decryption privilege in the form of a decryption blackbox/device in which the decryption key is embedded, for example, for financial gain or for some other incentives, as he only has little risk of getting caught. Recently a handful of traceable CP-ABE schemes have been proposed in (Liu et al., 2013b; Liu et al., 2013a; Deng et al., 2014). In the whitebox traceable CP-ABE schemes,

Li, X., Liang, K., Liu, Z. and Wong, D.
Attribute based Encryption: Traitor Tracing, Revocation and Fully Security on Prime Order Groups.
DOI: 10.5220/0006220203090320
In *Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017)*, pages 281-292
ISBN: 978-989-758-243-1

Table 1: Features and Efficiency Comparison.

	(Liu et al., 2013a)	(Liu and Wong, 2015b)	This Paper
Ciphertext Size	$2l+17\sqrt{N}$	$6l+3+46\sqrt{N}$	$6l+3+46\sqrt{N}$
Private Key Size	$\|S\|+4$	$6\|S\|+12$	$6\|S\|+9+3\sqrt{N}$
Public Key Size	$\|\mathcal{U}\|+3+4\sqrt{N}$	$24\|\mathcal{U}\|+22+14\sqrt{N}$	$24\|\mathcal{U}\|+22+23\sqrt{N}$
Paring in Decryption	$2\|I\|+10$	$6\|I\|+30$	$6\|I\|+30$
On prime Order Groups	$\times$	$\surd$	$\surd$
Revocation	$\times$	$\times$	$\surd$
Order of the Groups	$p_1p_2p_3$	p	p

[1] Let l be the size of an access policy, $|S|$ the size of the attribute set of a private key, $|\mathcal{U}|$ the size of the attribute universe, and $|I|$ the number of attributes in a decryption key that satisfies a ciphertext's access policy.

given a well-formed decryption key as input, a tracing algorithm can find out the malicious user who leaked or sold well-formed decryption keys. Liu et al. (Liu et al., 2013b) proposed such a whitebox traceable CP-ABE scheme that can deter users from these malicious behaviors. As malicious users invent a decryption blackbox/device which keeps the embedded decrypt keys and algorithms hidden, Liu et al.(Liu et al., 2013a) proved that the blackbox traceable CP-ABE scheme supports fully collusion-resistant blackbox traceable in the standard model, where *fully collusion-resistant blackbox traceability* means that the number of colluding users in constructing a decryption blackbox/device is not limited and can be arbitrary. This scheme is fully secure in the standard model and highly expressive (i.e. supporting any monotonic access structures).

It should be observed that a tracing system is not designed to protect the encrypted content. It is used to distinguish the compromised users from other legitimate users, which means the corrupted user/key is still remained in the system and an effective blackbox is likely to be produced with these corrupted keys in the wild market. The exposed compromised users need to leave or be removed from the system to avoid incurring more losses. When any of these happens, the corresponding user keys should be revoked. We added the revocability in the scheme so that we can remove the compromised keys as needed. We focus on achieving direct revocation in traceable CP-ABE system. In a direct revocation mechanism, it does not need any periodic key updates and it does not affect any non-revoked users either. A system-wide revocation list could be made public and revocation could be taken into effect promptly as the revocation list could be updated immediately once a key is revoked. Specifically, we generate Q_i', which is a part of ciphertext, with a non-revoked index list $\bar{R}$. When decrypting, we first recover $\vec{K}_{i,j}$ which has a common item $h\prod_{j'\in\bar{R}_i} h_{j'}$ with Q_i' if they share a consistent revocation list R. Then $\vec{K}_{i,j}$ is used in the following decryption process. To avoid a further loss, the revocation list should be updated timely once corrupted users are found. For the security proof for message-hiding, we re-construct the Semi-functional Keys by replacing h with hh_j, which can realize revocability, and adding the random item $\vec{K}_{i,j,j'}$ accordingly. As a contrast, the random items for Semi-functional Ciphertexts remain the same, which is irrelevant to the revocability. For the security proof for index-hiding, we have two ways for adversary to take and add more sub-cases in **Case II** which make the security proof a non-trivial work. In this paper, We continue our work on prime order groups as an extension for (Liu and Wong, 2015b).

1.1 Our Results

It has been shown (e.g. in (Garg et al., 2010; Lewko, 2012)) that the constructions on composite order groups will result in significant loss of efficiency and the security will rely on some non-standard assumptions (e.g. the Subgroup Decision Assumptions) and an additional assumption that the group order is hard to factor. The previous work in (Liu and Wong, 2015b) achieves better security than the scheme in (Liu et al., 2013a), which is constructed on composite order groups. In this paper, we add the revocability in (Liu and Wong, 2015b) and prove it highly expressive and fully secure in the standard model. On the efficiency aspect, this new scheme achieves the same efficient level as in (Liu and Wong, 2015b), i.e. the overhead for the fully collusion-resistant blackbox traceability is in $O(\sqrt{N})$, where N is the number of users in a system.

Table 1 compares this new scheme with the previous work on blackbox traceable CP-ABE (Liu et al., 2013a) and the traceable CP-ABE on prime order group but without revocability (Liu and Wong, 2015b). We only change the size of keypair as we need add revocation items in the key. Both the cipher-

text and the pairing computation in decryption are kept unchanged. This implies both this new scheme and (Liu and Wong, 2015b) have better security than the scheme in (Liu et al., 2013a), although all of them are fully secure in the standard model and have overhead in $O(\sqrt{N})$.

Related Work. In the literature, several revocation mechanisms have been proposed in the context of CP-ABE. In (Sahai et al., 2012), Sahai et al. proposed an *indirect* revocation mechanism, which requires an authority to periodically broadcast a key update information so that only the non-revoked users can update their keys. In (Attrapadung and Imai, 2009), Attrapadung and Imai proposed a *direct* revocation mechanism, which allows a revocation list to be specified directly during encryption so that the resulting ciphertext cannot be decrypted by any decryption key which is in the revocation list even though the associated attribute set of the key satisfies the ciphertext policy. For ABE scheme, in (Liu et al., 2013a) Liu et al. defined a 'functional' CP-ABE that has the same functionality as the conventional CP-ABE (i.e. having all the appealing properties of the conventional CP-ABE), except that each user is assigned and identified by a unique index, which will enable the traceability of traitors. Furthermore, Liu et al. defined a new primitive called Augmented CP-ABE (AugCP-ABE) and formalized its security using message-hiding and index-hiding games. Then Liu et al. proved that *an AugCP-ABE scheme with message-hiding and index-hiding properties can be directly transferred to a secure CP-ABE with fully collusion-resistant blackbox traceability*. With such a framework, Liu et al. obtained a fully secure and fully collusion-resistant blackbox traceable CP-ABE scheme by constructing an AugCP-ABE scheme with message-hiding and index-hiding properties. In (Liu and Wong, 2015b), Liu et al. obtain a prime order construction and it will be tempting to bring the revocation into (Liu and Wong, 2015b) as a practical enhancement and implementation. In this paper, we leverage the revocation idea from (Liu and Wong, 2015a).

Outline. In this paper, we follow the same framework in (Liu and Wong, 2015b). In particular, in Section 2, we propose a definition for CP-ABE supporting key-like blackbox traceability and direct revocation. In our direct revocation definition, the *Encrypt* algorithm takes a revocation list $R \subseteq \{1,\ldots,N\}$ as an additional input so that a message encrypted under the (revocation list, access policy) pair $(R,\mathbb{A})$ would only allow users whose (index, attribute set) pair (k,S) satisfies $(k \in [N] \setminus R)$ AND (S satisfies $\mathbb{A}$) to decrypt. In Section 3, we revisit the definitions and security models of Augmented Revocable CP-ABE (AugR-CP-ABE for short) from (Liu and Wong, 2015a). We refer to the 'functional' CP-ABE in Section 2 as Revocable CP-ABE (R-CP-ABE for short), then extend the R-CP-ABE to AugR-CP-ABE, which will lastly be transformed to a key-like blackbox *traceable* R-CP-ABE. In Section 4 we propose our AugR-CP-ABE construction on prime order groups and prove that our AugR-CP-ABE construction is message-hiding and index-hiding in the standard model. As a result, we obtain a fully secure and fully collusion-resistant blackbox traceable R-CP-ABE scheme on prime order groups.

To construct the AugR-CP-ABE, we continue our work in (Liu and Wong, 2015b) and leverage the revocation idea from (Liu and Wong, 2015a). In particular, besides achieving the important features for practicality, such as revocation, high expressivity and efficiency, the construction is proved secure and traceable in the standard model.

2 REVOCABILITY AND BLACKBOX TRACEABILITY

We follow the definition in (Liu and Wong, 2015a). Given a positive integer n, our Revocable Ciphertext-Policy Attribute-Based Encryption (R-CP-ABE) system consists of four algorithms:

- $\mathsf{Setup}(\lambda, \mathcal{U}, N) \rightarrow (\mathsf{PP}, \mathsf{MSK})$. The algorithm takes as input a security parameter λ, the attribute universe $\mathcal{U}$, and the number of users N in the system, then runs in polynomial time in λ, and outputs the public parameter PP and a master secret key MSK.
- $\mathsf{KeyGen}(\mathsf{PP}, \mathsf{MSK}, S) \rightarrow \mathsf{SK}_{k,S}$. The algorithm takes as input the public parameter PP, the master secret key MSK, and an attribute set S, and outputs a private decryption key $\mathsf{SK}_{k,S}$, which is assigned and identified by a unique index $k \in [N]$.
- $\mathsf{Encrypt}(\mathsf{PP}, M, R, \mathbb{A}) \rightarrow CT_{R,\mathbb{A}}$. The algorithm takes as input the public parameter PP, a message M, a revocation list $R \subseteq [N]$, and an access policy $\mathbb{A}$ over $\mathcal{U}$, and outputs a ciphertext $CT_{R,\mathbb{A}}$ such that only users whose indices are not revoked by R and attributes satisfy $\mathbb{A}$ can recover M. R and $\mathbb{A}$ are implicitly included in $CT_{R,\mathbb{A}}$.
- $\mathsf{Decrypt}(\mathsf{PP}, CT_{R,\mathbb{A}}, \mathsf{SK}_{k,S}) \rightarrow M$ or $\perp$. The algorithm takes as input the public parameter PP, a ciphertext $CT_{R,\mathbb{A}}$, and a private key $\mathsf{SK}_{k,S}$. If $(k \in [N] \setminus R)$ AND (S satisfies $\mathbb{A}$), the algorithm outputs a message M, otherwise it outputs $\perp$ indicating the failure of decryption.

Correctness. For any attribute set $S \subseteq \mathcal{U}$, index $k \in [N]$, revocation list $R \subseteq [N]$, access policy $\mathbb{A}$ over $\mathcal{U}$, and message M, suppose $(\mathsf{PP}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(\lambda, \mathcal{U}, N)$, $\mathsf{SK}_{k,S} \leftarrow \mathsf{KeyGen}(\mathsf{PP}, \mathsf{MSK}, S)$, $CT_{R,\mathbb{A}} \leftarrow \mathsf{Encrypt}(\mathsf{PP}, M, R, \mathbb{A})$. If $(k \in [N] \setminus R) \wedge (S$ satisfies $\mathbb{A})$, then $\mathsf{Decrypt}(\mathsf{PP}, CT_{R,\mathbb{A}}, \mathsf{SK}_{k,S}) = M$.

Security. Now we define the security of a R-CP-ABE system using a message-hiding game.

$\mathsf{Game}_{\mathsf{MH}}$. The Message-hiding game is defined between a challenger and an adversary $\mathcal{A}$ as follows:

- **Setup.** The challenger runs $\mathsf{Setup}(\lambda, \mathcal{U}, N)$ and gives the public parameter PP to $\mathcal{A}$.
- **Phase 1.** For $i = 1$ to Q_1, $\mathcal{A}$ adaptively submits (index, attribute set) pair (k_i, S_{k_i}), and the challenger responds with $\mathsf{SK}_{k_i,S_{k_i}}$.
- **Challenge.** $\mathcal{A}$ submits two equal-length messages M_0, M_1 and a (revocation list, access policy) pair $(R^*, \mathbb{A}^*)$. The challenger flips a random coin $b \in \{0,1\}$, and sends $CT_{R^*,\mathbb{A}^*} \leftarrow \mathsf{Encrypt}(\mathsf{PP}, M_b, R^*, \mathbb{A}^*)$ to $\mathcal{A}$.
- **Phase 2.** For $i = Q_1+1$ to Q, $\mathcal{A}$ adaptively submits (k_i, S_{k_i}), and the challenger responds with $\mathsf{SK}_{k_i,S_{k_i}}$.
- **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 $\{(k_t, S_{k_t})\}_{i=1}^{Q}$ can satisfy $(k_t \in [N] \setminus R^*)$ AND $(S_{k_t}$ satisfies $\mathbb{A}^*)$. The advantage of $\mathcal{A}$ is defined as $\mathsf{MH}^{\mathsf{A}}\mathsf{Adv}_{\mathcal{A}} = |\Pr[b' = b] - \frac{1}{2}|$.

Definition 1. *An N-user R-CP-ABE system is secure if for all polynomial-time adversaries $\mathcal{A}$ the advantage $\mathsf{MHAdv}_{\mathcal{A}}$ is negligible in λ.*

The message-hiding game is a typical semantic security game and is based on that for conventional CP-ABE (Lewko et al., 2010; Lewko and Waters, 2012a), where the revocation list R is always empty. It is clear that such a CP-ABE system (Lewko et al., 2010; Lewko and Waters, 2012a) has the following properties: fully collusion-resistant security, meaning that several users should not be able to decrypt a message that none of them are individually granted to access, fine-grained access control on encrypted data, and efficient one-to-many encryption.

It is worth noticing that, as pointed in (Liu et al., 2013a), in the definition of the game: (1) the adversary is allowed to specify the index of the private key when it makes key queries for the attribute sets of its choice, i.e., for $t = 1$ to Q, the adversary submits (index, attribute set) pair (k_t, S_{k_t}) to query a private key for attribute set S_{k_t}, where $Q \leq N$, $k_t \in [N]$, and $k_t \neq k_{t'}$ $\forall 1 \leq t \neq t' \leq Q$ (this is to guarantee that each user/key can be *uniquely* identified by an index); and (2) for $k_t \neq k_{t'}$ we do not require $S_{k_t} \neq S_{k_{t'}}$, i.e., different users/keys may have the same attribute set. We remark that these two points apply to the rest of the paper.

2.1 Blackbox Traceability

Now we define the traceability against key-like decryption blackbox. A key-like decryption blackbox $\mathcal{D}$ can be viewed as a probabilistic circuit that takes as input a ciphertext $CT_{R,\mathbb{A}}$ and outputs a message M or $\perp$, and such a decryption blackbox does not need to be perfect, namely, we only require it to be able to decrypt with non-negligible success probability. In particular, a key-like decryption blackbox $\mathcal{D}$ is described by a (revocation list, attribute set) pair $(R_{\mathcal{D}}, S_{\mathcal{D}})$ and a non-negligible probability value ε (i.e. $0 \leq \varepsilon \leq 1$ is polynomially related to λ), and advertised that for any ciphertext generated under the (revocation list, access policy) pair $(R, \mathbb{A})$, if $((S_{\mathcal{D}}$ satisfies $\mathbb{A})$ AND $([N] \setminus R) \cap ([N] \setminus R_D) \neq \emptyset)$ can be satisfied by $S_{\mathcal{D}}$ and $R_{\mathcal{D}}$, this blackbox $\mathcal{D}$ can decrypt the corresponding ciphertext with probability at least ε. Specifically, once a blackbox is found being able to decrypt ciphertext, we can regard it as a key-like decryption blackbox with the corresponding (revocation list, attribute set) pair $(R_{\mathcal{D}}, S_{\mathcal{D}})$, and the ciphertext is related to the pair $(R, \mathbb{A})$ which satisfies $((S_{\mathcal{D}}$ satisfies $\mathbb{A})$ AND $([N] \setminus R) \cap ([N] \setminus R_D) \neq \emptyset)$. If we set the revocation list R and $R_{\mathcal{D}}$ as empty, we can get the same definition for key-like decryption blackbox as shown in (Liu et al., 2013a).

$\mathsf{Trace}^{\mathcal{D}}(\mathsf{PP}, R_{\mathcal{D}}, S_{\mathcal{D}}, \varepsilon) \rightarrow \mathbb{K}_T \subseteq [N]$. *This is an oracle algorithm that interacts with a key-like decryption blackbox $\mathcal{D}$. Given the public parameter* PP*, a revocation list $R_{\mathcal{D}}$, a non-empty attribute set $S_{\mathcal{D}}$, and a probability value (lower-bound) ε, the algorithm runs in time polynomial in λ and $1/\varepsilon$, and outputs an index set $\mathbb{K}_T \subseteq [N]$ which identifies the set of malicious users. Note that ε has to be polynomially related to λ.*

In the following Tracing Game game, the adversary targets to build a decryption blackbox $\mathcal{D}$ that functions as a private decryption key with the pair $(R_{\mathcal{D}}, S_{\mathcal{D}})$ (as the name of key-like decryption blackbox implies) which can decrypt ciphertexts under some (revocation list, access policy) pairs $(R, \mathbb{A})$. It captures the notion of **fully collusion-resistant traceability**. The tracing algorithm in the game is designed to extract the index of at least one of the malicious users whose decryption keys have been used for constructing $\mathcal{D}$.

$\mathsf{Game}_{\mathsf{TR}}$. The Tracing Game is defined between a challenger and an adversary $\mathcal{A}$ as follows:

- **Setup.** The challenger runs $\mathsf{Setup}(\lambda, \mathcal{U}, N)$ and gives the public parameter PP to $\mathcal{A}$.

Key Query. For $i = 1$ to Q, $\mathcal{A}$ adaptively submits (k_i, S_{k_i}), and the challenger responds with $\mathsf{SK}_{k_i,S_{k_i}}$.

(Key-like) Decryption Blackbox Generation. $\mathcal{A}$ outputs a decryption blackbox $\mathcal{D}$ associated with a (revocation list, attribute set) pair $(R_{\mathcal{D}}, S_{\mathcal{D}})$, $S_{\mathcal{D}} \subseteq \mathcal{U}, R_{\mathcal{D}} \subseteq [N]$ and a non-negligible probability (lower-bound) value ε.

Tracing. The challenger runs $\mathsf{Trace}^{\mathcal{D}}(\mathsf{PP}, R_{\mathcal{D}}, S_{\mathcal{D}}, \varepsilon)$ to obtain an index set $\mathbb{K}_T \subseteq [N]$.

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

1. For any (revocation list, access policy) pair $(R, \mathbb{A})$ which satisfied $((S_{\mathcal{D}}$ satisfies $\mathbb{A})$ AND $([N] \setminus R) \cap ([N] \setminus R_D) \neq \emptyset)$, we have
$$\Pr[\mathcal{D}(\mathsf{Encrypt}(\mathsf{PP}, M, R, \mathbb{A})) = M] \geq \varepsilon,$$
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 key-like decryption blackbox*.
2. $\mathbb{K}_T = \emptyset$, or $\mathbb{K}_T \not\subseteq \mathbb{K}_{\mathcal{D}}$, or $\big((k_t \in R_{\mathcal{D}})$ OR $(S_{\mathcal{D}} \not\subseteq S_{k_t}) \; \forall k_t \in \mathbb{K}_T\big)$.

We denote by $\mathsf{TRAdv}_{\mathcal{A}}$ the probability that adversary $\mathcal{A}$ wins this game.

Definition 2. *An N-user Blackbox Traceable CP-ABE system is traceable if for all polynomial-time adversaries $\mathcal{A}$ the advantage $\mathsf{TRAdv}_{\mathcal{A}}$ is negligible in λ.*

3 DEFINITION

3.1 Definitions and Security Models

An Augmented R-CP-ABE (AugR-CP-ABE) system consists of the following four algorithms:

$\mathsf{Setup}_{\mathsf{A}}(\lambda, \mathcal{U}, N) \rightarrow (\mathsf{PP}, \mathsf{MSK})$. The algorithm takes as input a security parameter λ, the attribute universe $\mathcal{U}$, and the number of users N in the system, then runs in polynomial time in λ, and outputs the public parameter PP and a master secret key MSK.

$\mathsf{KeyGen}_{\mathsf{A}}(\mathsf{PP}, \mathsf{MSK}, S) \rightarrow \mathsf{SK}_{k,S}$. The algorithm takes as input PP, MSK, and an attribute set S, and outputs a private key $\mathsf{SK}_{k,S}$, which is assigned and identified by a unique index $k \in [N]$.

$\mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M, R, \mathbb{A}, \overline{k}) \rightarrow CT_{R,\mathbb{A}}$. The algorithm takes as input PP, a message M, a revocation list $R \subseteq [N]$, an access policy $\mathbb{A}$ over $\mathcal{U}$, and an index $k \in [N+1]$, and outputs a ciphertext $CT_{R,\mathbb{A}}$. $\mathbb{A}$ **is included in** $CT_{R,\mathbb{A}}$**, but the value of** k **is not**.

$\mathsf{Decrypt}_{\mathsf{A}}(\mathsf{PP}, CT_{R,\mathbb{A}}, \mathsf{SK}_{k,S}) \rightarrow M$ or $\perp$. The algorithm takes as input PP, a ciphertext $CT_{R,\mathbb{A}}$, and a private key $\mathsf{SK}_{k,S}$. If $(k \in [N] \setminus R)$ AND (S satisfies $\mathbb{A}$), the algorithm outputs a message M, otherwise it outputs $\perp$ indicating the failure of decryption.

Correctness. For any attribute set $S \subseteq \mathcal{U}$, index $k \in [N]$, revocation list $R \subseteq [N]$, access policy $\mathbb{A}$ over $\mathcal{U}$, encryption index $k \in [N+1]$, and message M, suppose $(\mathsf{PP}, \mathsf{MSK}) \leftarrow \mathsf{Setup}_{\mathsf{A}}(\lambda, \mathcal{U}, N)$, $\mathsf{SK}_{k,S} \leftarrow \mathsf{KeyGen}_{\mathsf{A}}(\mathsf{PP}, \mathsf{MSK}, S)$, $CT_{R,\mathbb{A}} \leftarrow \mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M, R, \mathbb{A}, k)$. If $(k \in [N] \setminus R) \wedge (S$ satisfies $\mathbb{A}) \wedge (k \geq k)$ then $\mathsf{Decrypt}_{\mathsf{A}}(\mathsf{PP}, CT_{R,\mathbb{A}}, \mathsf{SK}_{k,S}) = M$.

Security. The security of AugR-CP-ABE is defined by the following three games, where the first two are for message-hiding, and the third one is for the index-hiding property.

In the first two **message-hiding games** between a challenger and an adversary $\mathcal{A}$, $k = 1$ (the first game, $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_1}$) or $k = N+1$ (the second game, $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_{N+1}}$).

Setup. The challenger runs $\mathsf{Setup}_{\mathsf{A}}(\lambda, \mathcal{U}, N)$ and gives the public parameter PP to $\mathcal{A}$.

Phase 1. For $t = 1$ to Q_1, $\mathcal{A}$ adaptively submits (index, attribute set) pair (k_t, S_{k_t}), and the challenger responds with $\mathsf{SK}_{k_t,S_{k_t}}$, which corresponds to attribute set S_{k_t} and is assigned index k_t.

Challenge. $\mathcal{A}$ submits two equal-length messages M_0, M_1 and a (revocation list, access policy) pair $(R^*, \mathbb{A}^*)$. The challenger flips a random coin $b \in \{0,1\}$, and sends $CT_{R^*,\mathbb{A}^*} \leftarrow \mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M_b, R^*, \mathbb{A}^*, k)$ to $\mathcal{A}$.

Phase 2. For $t = Q_1 + 1$ to Q, $\mathcal{A}$ adaptively submits (index, attribute set) pair (k_t, S_{k_t}), and the challenger responds with $\mathsf{SK}_{k_t,S_{k_t}}$, which corresponds to attribute set S_{k_t} and is assigned index k_t.

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

$\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_1}$. In the Challenge phase the challenger sends $CT_{R^*,\mathbb{A}^*} \leftarrow \mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M_b, R^*, \mathbb{A}^*, 1)$ to $\mathcal{A}$. $\mathcal{A}$ wins the game if $b' = b$ under the **restriction** that none of the queried $\{(k_t, S_{k_t})\}_{i=1}^{Q}$ can satisfy $(k \in [N] \setminus R^*)$ AND (S_{k_t} satisfies $\mathbb{A}^*$). The advantage of $\mathcal{A}$ is defined as $\mathsf{MH}^{\mathsf{A}}_1\mathsf{Adv}_{\mathcal{A}} = |\Pr[b' = b] - \frac{1}{2}|$.

$\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_{N+1}}$. In the Challenge phase the challenger sends $CT_{R^*,\mathbb{A}^*} \leftarrow \mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M_b, R^*, \mathbb{A}^*, N+1)$ to $\mathcal{A}$. $\mathcal{A}$ wins the game if $b' = b$. The advantage of $\mathcal{A}$ is defined as $\mathsf{MH}^{\mathsf{A}}_{N+1}\mathsf{Adv}_{\mathcal{A}} = |\Pr[b' = b] - \frac{1}{2}|$.

Definition 3. *A N-user Augmented R-CP-ABE system is message-hiding if for all probabilistic polynomial time (PPT) adversaries $\mathcal{A}$ the advantages $\mathsf{MH}^{\mathsf{A}}_1\mathsf{Adv}_{\mathcal{A}}$ and $\mathsf{MH}^{\mathsf{A}}_{N+1}\mathsf{Adv}_{\mathcal{A}}$ are negligible in λ.*

$\mathsf{Game}^{\mathsf{A}}_{\mathsf{IH}}$. In the third game, **index-hiding game**, for any non-empty attribute set $S^* \subseteq \mathcal{U}$, we define **the strictest access policy** as $\mathbb{A}_{S^*} = \bigwedge_{x \in S^*} x$, and require that an adversary cannot distinguish between an encryption using $(\mathbb{A}_{S^*}, R^*, \bar{k})$ and $(\mathbb{A}_{S^*}, R^*, \bar{k}+1)$ without a private decryption key $\mathsf{SK}_{\bar{k}, S_{\bar{k}}}$ such that $(\bar{k} \in [N] \setminus R^*) \wedge (S_{\bar{k}} \supseteq S^*)$. The game takes as input a parameter $k \in [N]$ which is given to both the challenger and the adversary $\mathcal{A}$. The game proceeds as follows:

Setup. The challenger runs $\mathsf{Setup}_{\mathsf{A}}(\lambda, \mathcal{U}, N)$ and gives the public parameter PP to $\mathcal{A}$.

Key Query. For $t = 1$ to Q, $\mathcal{A}$ adaptively submits (index, attribute set) pair (k_t, S_{k_t}), and the challenger responds with $\mathsf{SK}_{k_t, S_{k_t}}$, which corresponds to attribute set S_{k_t} and is assigned index k_t.

Challenge. $\mathcal{A}$ submits a message M and a (revocation list, access policy) pair $(R^*, \mathbb{A}^*)$. The challenger flips a random coin $b \in \{0,1\}$, and sends $CT_{R^*, \mathbb{A}^*} \leftarrow \mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M, R^*, \mathbb{A}^*, k+b)$ 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 $\{(k_t, S_{k_t})\}_{i=1}^{Q}$ can satisfy $(k_t = \bar{k}) \wedge (k_t \in [N] \setminus R^*) \wedge (S_{k_t}$ satisfies $\mathbb{A}_{S^*})$, i.e. $(k_t = k) \wedge (k_t \in [N] \setminus R^*) \wedge (S_{k_t} \supseteq S^*)$. The advantage of $\mathcal{A}$ is defined as $\mathsf{IH}^{\mathsf{A}}\mathsf{Adv}_{\mathcal{A}}[k] = |\Pr[b' = b] - \frac{1}{2}|$.

Definition 4. *A N-user Augmented R-CP-ABE system is index-hiding if for all PPT adversaries $\mathcal{A}$ the advantages $\mathsf{IH}^{\mathsf{A}}\mathsf{Adv}_{\mathcal{A}}[\bar{k}]$ for $\bar{k} = 1, \ldots, N$ are negligible in λ.*

3.2 The Reduction of Traceable R-CP-ABE to AugR-CP-ABE

We now show that an AugR-CP-ABE with message-hiding and index-hiding implies a secure and traceable R-CP-ABE.

Let $\Sigma_{\mathsf{A}} = (\mathsf{Setup}_{\mathsf{A}}, \mathsf{KeyGen}_{\mathsf{A}}, \mathsf{Encrypt}_{\mathsf{A}}, \mathsf{Decrypt}_{\mathsf{A}})$ be an AugR-CP-ABE with message-hiding and index-hiding, define $\mathsf{Encrypt}(\mathsf{PP}, M, \mathbb{A}) = \mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M, \mathbb{A}, 1)$, then $\Sigma = (\mathsf{Setup}_{\mathsf{A}}, \mathsf{KeyGen}_{\mathsf{A}}, \mathsf{Encrypt}, \mathsf{Decrypt}_{\mathsf{A}})$ is a R-CP-ABE derived from Σ_{A}. In the following, we show that if Σ_{A} is message-hiding and index-hiding, then Σ is secure. Furthermore, we propose a tracing algorithm Trace for Σ and show that if Σ_{A} is message-hiding and index-hiding, then Σ (equipped with Trace) is traceable.

3.2.1 R-CP-ABE Security

Theorem 1. *If Σ_{A} is an AugR-CP-ABE with message-hiding and index-hiding properties, then Σ is a secure and traceable R-CP-ABE.*

Proof. Note that Σ is a special case of Σ_{A} where the encryption algorithm always sets $\bar{k} = 1$. Hence, $\mathsf{Game}_{\mathsf{MH}}$ for Σ is identical to $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_1}$ for Σ_{A}, which implies that $\mathsf{MHAdv}_{\mathcal{A}}$ for Σ in $\mathsf{Game}_{\mathsf{MH}}$ is equal to $\mathsf{MH}_1^{\mathsf{A}}\mathsf{Adv}_{\mathcal{A}}$ for Σ_{A} in $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_1}$, i.e., if Σ_{A} is message-hiding (in $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_1}$), then Σ is secure. □

3.2.2 R-CP-ABE Traceability

Now we show that if Σ_{A} is message-hiding (in $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_{N+1}}$) and index-hiding, Σ is traceable. As shown in (Liu et al., 2013a), with the following Trace algorithm (Liu et al., 2013a), Σ achieves fully collusion-resistant blackbox traceability against key-like decryption blackbox.

$\mathsf{Trace}^{\mathcal{D}}(\mathsf{PP}, R_{\mathcal{D}}, S_{\mathcal{D}}, \varepsilon) \rightarrow \mathbb{K}_T \subseteq [N]$: Given a key-like decryption blackbox $\mathcal{D}$ associated with a non-empty attribute set $S_{\mathcal{D}}$ and probability $\varepsilon > 0$, the tracing algorithm works as follows:

1. For $\bar{k} = 1$ to $N+1$, do the following:
   (a) The algorithm repeats the following $8\lambda(N/\varepsilon)^2$ times:
      i. Sample M from the message space at random.
      ii. Let $CT_{R, \mathbb{A}_{S_{\mathcal{D}}}} \leftarrow \mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M, R, \mathbb{A}_{S_{\mathcal{D}}}, \bar{k})$, where $\mathbb{A}_{S_{\mathcal{D}}}$ is the strictest access policy of $S_{\mathcal{D}}$.
      iii. Query oracle $\mathcal{D}$ on input $CT_{R, \mathbb{A}_{S_{\mathcal{D}}}}$, and compare the output of $\mathcal{D}$ with M.
   (b) Let $\hat{p}_{\bar{k}}^-$ be the fraction of times that $\mathcal{D}$ decrypted the ciphertexts correctly.
2. Let $\mathbb{K}_T$ be the set of all $\bar{k} \in [N]$ for which $\hat{p}_{\bar{k}}^- - \hat{p}_{\bar{k}+1}^- \geq \varepsilon/(4N)$. Then output $\mathbb{K}_T$ as the index set of the private keys of malicious users.

Theorem 2. *If Σ_{A} is message-hiding and index-hiding, then Σ is traceable using the* Trace *algorithm against key-like decryption blackbox.*

Proof. In the proof sketch below, we show that if the key-like decryption blackbox output by the adversary is a useful one then the traced $\mathbb{K}_T$ will satisfy $(\mathbb{K}_T \neq \emptyset) \wedge (\mathbb{K}_T \subseteq \mathbb{K}_{\mathcal{D}}) \wedge \big(\exists k_t \in \mathbb{K}_T \; s.t.(\; k_{k_t} \in [N] \setminus R_{\mathcal{D}}) \wedge (S_{\mathcal{D}} \subseteq S_{k_t})\big)$ with overwhelming probability, which implies that the adversary can win the game $\mathsf{Game}_{\mathsf{TR}}$ only with negligible probability, i.e., $\mathsf{TRAdv}_{\mathcal{A}}$ is negligible.

Let $\mathcal{D}$ be the key-like decryption blackbox output by the adversary, and $(R_{\mathcal{D}}, S_{\mathcal{D}})$ be the (revocation list, attribute set) pair which can be used to describe $\mathcal{D}$. Define

$$p_{\bar{k}}^- = \Pr[\mathcal{D}(\mathsf{Encrypt}_{\mathsf{A}}(\mathsf{PP}, M, R, \mathbb{A}_{S_{\mathcal{D}}}, \bar{k})) = M],$$

where the probability is taken over the random choice of message M and the random coins of $\mathcal{D}$. We have

that $p_1 \geq \varepsilon$ and p_{N+1} is negligible. The former follows the fact that $\mathcal{D}$ is a useful key-like decryption blackbox, and the later follows that Σ_A is message-hiding (in $\mathsf{Game}^{A}_{\mathsf{MH}_{N+1}}$). Then there must exist some $\bar{k} \in [N]$ such that $p_{\bar{k}} - p_{\bar{k}+1} \geq \varepsilon/(2N)$. By the Chernoff bound it follows that with overwhelming probability, $\hat{p}_{\bar{k}} - \hat{p}_{\bar{k}+1} \geq \varepsilon/(4N)$. Hence, we have $\mathbb{K}_T \neq \emptyset$.

For any $k_t \in \mathbb{K}_T$ (i.e., $\hat{p}_{k_t} - \hat{p}_{k_t+1} \geq \frac{\varepsilon}{4N}$), we know, by Chernoff, that with overwhelming probability $p_{k_t} - p_{k_t+1} \geq \varepsilon/(8N)$. Clearly $(k_t \in \mathbb{K}_{\mathcal{D}}) \wedge (k_t \in [N] \setminus R_{\mathcal{D}}) \wedge (S_{\mathcal{D}} \subseteq S_{k_t})$ since otherwise, $\mathcal{D}$ can be directly used to win the index-hiding game for Σ_A. Hence, we have $(\mathbb{K}_T \subseteq \mathbb{K}_{\mathcal{D}}) \wedge \big((k_t \in [N] \setminus R_{\mathcal{D}}) \wedge (S_{\mathcal{D}} \subseteq S_{k_t})\ \forall k_t \in \mathbb{K}_T\big)$. □

4 CONSTRUCTION

Now we construct an AugR-CP-ABE scheme on prime order groups, and prove that this AugR-CP-ABE scheme is message-hiding and index-hiding in the standard model. Combined with the results in Section 3.2, we obtain a R-CP-ABE scheme that is fully collusion-resistant blackbox traceable in the standard model, fully secure in the standard model, and on prime order groups.

4.1 Preliminaries

Before proposing our AugR-CP-ABE construction , we first review some preliminaries.

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 a prime, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order p, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is 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 $\mathbb{G}_T$. We refer to $\mathbb{G}$ as the *source group* and $\mathbb{G}_T$ as the *target group*. We assume that group operations in $\mathbb{G}$ and $\mathbb{G}_T$ as well as the bilinear map e are efficiently computable, and the description of $\mathbb{G}$ and $\mathbb{G}_T$ includes a generator of $\mathbb{G}$ and $\mathbb{G}_T$ respectively.

Complexity Assumptions. We will base the message-hiding property of our AugR-CP-ABE scheme on the Decisional Linear Assumption (DLIN), the Decisional 3-Party Diffie-Hellman Assumption (D3DH) and the Source Group q-Parallel BDHE Assumption, and will base the index-hiding property of our AugR-CP-ABE scheme on the DLIN assumption and the D3DH assumption. Please refer to the full version (Li et al., 2016, Appendix A) for the details of the three assumptions.

Dual Pairing Vector Spaces. Our construction will use dual pairing vector spaces, a tool introduced by Okamoto and Takashima (Okamoto and Takashima, 2008; Okamoto and Takashima, 2009; Okamoto and Takashima, 2010) and developed by Lewko (Lewko, 2012) and Lewko and Waters (Lewko and Waters, 2012b). Please refer to the full version (Li et al., 2016, Appendix A) for the details of the dual pairing vector spaces. As our AugR-CP-ABE construction will use dual pairing vector spaces, the security proof will use a lemma and a Subspace Assumption, which are introduced and proved by Lewko and Waters (Lewko and Waters, 2012b), in the setting of dual pairing vector spaces. Please refer to the full version (Li et al., 2016, Appendix A.1) for the details of this lemma and the Subspace Assumption. Here we would like to stress that *the Subspace Assumption is implied by DLIN assumption*.

To construct our AugR-CP-ABE scheme, we further define a new notation. In particular, for any $\vec{v} = (v_1, \ldots, v_n) \in \mathbb{Z}_p^n$, $\vec{v'} = (v'_1, \ldots, v'_{n'}) \in \mathbb{Z}_p^{n'}$, we define

$$\begin{aligned}(g^{\vec{v}})^{\vec{v'}} &:= ((g^{\vec{v}})^{v'_1}, \ldots, (g^{\vec{v}})^{v'_{n'}}) \\ &= (g^{v'_1 v_1}, \ldots, g^{v'_1 v_n}, \ldots, g^{v'_{n'} v_1}, \ldots, g^{v'_{n'} v_n}) \in \mathbb{G}^{nn'}.\end{aligned}$$

Note that for any $\vec{v}, \vec{w} \in \mathbb{Z}_p^n, \vec{v'}, \vec{w'} \in \mathbb{Z}_p^{n'}$, we have

$$\begin{aligned}e_{nn'}((g^{\vec{v}})^{\vec{v'}}, (g^{\vec{w}})^{\vec{w'}}) &= \prod_{j=1}^{n'} \prod_{i=1}^{n} e(g^{v'_j v_i}, g^{w'_j w_i}) \\ &= \prod_{j=1}^{n'} (\prod_{i=1}^{n} e(g^{v_i}, g^{w_i}))^{v'_j w'_j} \\ &= \big(e_n(g^{\vec{v}}, g^{\vec{w}})\big)^{(\vec{v'} \cdot \vec{w'})} \\ &= \big(e(g,g)^{(\vec{v} \cdot \vec{w})}\big)^{(\vec{v'} \cdot \vec{w'})} \\ &= e(g,g)^{(\vec{v} \cdot \vec{w})(\vec{v'} \cdot \vec{w'})} \\ &= e_{nn'}((g^{\vec{v'}})^{\vec{v}}, (g^{\vec{w'}})^{\vec{w}}).\end{aligned}$$

Linear Secret-Sharing Schemes (LSSS). As in previous work, we use linear secret-sharing schemes (LSSS) to express the access policies. The formal definitions of access structures and LSSS can be found in the full version (Li et al., 2016, Appendix D).

Notations. Suppose the number of users N in the system equals n^2 for some n [1], so we use $[n,n]$ instead of $[N]$ in the following content. We arrange the users in a $n \times n$ matrix and uniquely assign a tuple (i,j) where $1 \leq i, j \leq n$, to each user. A user at position

[1] If the number of users is not a square, we add some "dummy" users to pad to the next square.

(i,j) of the matrix has index $k=(i-1)*n+j$. 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 $k=(i-1)*n+j$ defines a bijection between $\{(i,j)|1\leq i,j\leq n\}$ and $\{1,\ldots,N\}$. We conflate the notation and consider the attribute universe to be $[\mathcal{U}]=\{1,2\ldots,\mathcal{U}\}$, so $\mathcal{U}$ serves both as a description of the attribute universe and as a count of the total number of attributes. Given a bilinear group order p, one can randomly choose $r_x,r_y,r_z\in\mathbb{Z}_p$, and set $\vec{\chi}_1=(r_x,0,r_z)$, $\vec{\chi}_2=(0,r_y,r_z)$, $\vec{\chi}_3=\vec{\chi}_1\times\vec{\chi}_2=(-r_yr_z,-r_xr_z,r_xr_y)$. Let $span\{\vec{\chi}_1,\vec{\chi}_2\}$ be the subspace spanned by $\vec{\chi}_1$ and $\vec{\chi}_2$, i.e. $span\{\vec{\chi}_1,\vec{\chi}_2\}=\{\nu_1\vec{\chi}_1+\nu_2\vec{\chi}_2|\nu_1,\nu_2\in\mathbb{Z}_p\}$. We can see that $\vec{\chi}_3$ is orthogonal to the subspace $span\{\vec{\chi}_1,\vec{\chi}_2\}$ and that $\mathbb{Z}_p^3=span\{\vec{\chi}_1,\vec{\chi}_2,\vec{\chi}_3\}=\{\nu_1\vec{\chi}_1+\nu_2\vec{\chi}_2+\nu_3\vec{\chi}_3|\nu_1,\nu_2,\nu_3\in\mathbb{Z}_p\}$. For any $\vec{v}\in span\{\vec{\chi}_1,\vec{\chi}_2\}$, we have $(\vec{\chi}_3\cdot\vec{v})=0$, and for random $\vec{v}\in\mathbb{Z}_p^3$, $(\vec{\chi}_3\cdot\vec{v})\neq 0$ happens with overwhelming probability.

4.2 AugR-CP-ABE Construction

$\mathsf{Setup}_\mathsf{A}(\lambda,\mathcal{U},N=n^2)\rightarrow(\mathsf{PP},\mathsf{MSK})$. The algorithm chooses a bilinear group $\mathbb{G}$ of order p and two generators $g,h\in\mathbb{G}$. It randomly chooses $\{h_j\in\mathbb{Z}_p\}_{j\in[n]},(\mathbb{B},\mathbb{B}^*),(\mathbb{B}_0,\mathbb{B}_0^*)\in Dual(\mathbb{Z}_p^3,\psi)$ and $(\mathbb{B}_1,\mathbb{B}_1^*),\ldots,(\mathbb{B}_\mathcal{U},\mathbb{B}_\mathcal{U}^*)\in Dual(\mathbb{Z}_p^6,\psi)$. We let $\vec{b}_j,\vec{b}_j^*(1\leq j\leq 3)$ denote the basis vectors belonging to $(\mathbb{B},\mathbb{B}^*)$, $\vec{b}_{0,j},\vec{b}_{0,j}^*(1\leq j\leq 3)$ denote the basis vectors belonging to $(\mathbb{B}_0,\mathbb{B}_0^*)$, and $\vec{b}_{x,j},\vec{b}_{x,j}^*(1\leq j\leq 6)$ denote the basis vectors belonging to $(\mathbb{B}_x,\mathbb{B}_x^*)$ for each $x\in[\mathcal{U}]$. The algorithm also chooses random exponents

$$\alpha_1,\alpha_2\in\mathbb{Z}_p,\ \{r_i,z_i,\ \alpha_{i,1},\alpha_{i,2}\in\mathbb{Z}_p\}_{i\in[n]},\ \{c_{j,1},c_{j,2},\ y_j,h_j\in\mathbb{Z}_p\}_{j\in[n]}.$$

The public parameter PP and the master secret key MSK are set to

$$\begin{aligned}\mathsf{PP}=\Big(&(p,\mathbb{G},\mathbb{G}_T,e),\ g,h,g^{\vec{b}_1},g^{\vec{b}_2},\\&\{h_j\}_{j\in[n]},h^{\vec{b}_1},h^{\vec{b}_2},\ \{h_j^{\vec{b}_1},h_j^{\vec{b}_2}\}_{j\in[n]},\\&h^{\vec{b}_{0,1}},h^{\vec{b}_{0,2}},\ \{h^{\vec{b}_{x,1}},h^{\vec{b}_{x,2}},h^{\vec{b}_{x,3}},h^{\vec{b}_{x,4}}\}_{x\in[\mathcal{U}]},\\&F_1=e(g,h)^{\psi\alpha_1},\ F_2=e(g,h)^{\psi\alpha_2},\\&\{F_{1,j}=e(g,h_j)^{\psi\alpha_1},F_{2,j}=e(g,h_j)^{\psi\alpha_2}\}_{j\in[n]},\\&\{E_{i,1}=e(g,g)^{\psi\alpha_{i,1}},\ E_{i,2}=e(g,g)^{\psi\alpha_{i,2}}\}_{i\in[n]},\\&\{\vec{G}_i=g^{r_i(\vec{b}_1+\vec{b}_2)},\ \vec{Z}_i=g^{z_i(\vec{b}_1+\vec{b}_2)}\}_{i\in[n]},\\&\{\vec{H}_j=g^{c_{j,1}\vec{b}_1^*+c_{j,2}\vec{b}_2^*},\ \vec{Y}_j=\vec{H}_j^{y_j}\}_{j\in[n]}\Big).\end{aligned}$$

$$\begin{aligned}\mathsf{MSK}=\Big(&\vec{b}_1^*,\vec{b}_2^*,\ \vec{b}_{0,1}^*,\vec{b}_{0,2}^*,\ \{\vec{b}_{x,1}^*,\vec{b}_{x,2}^*,\vec{b}_{x,3}^*,\vec{b}_{x,4}^*\}_{x\in[\mathcal{U}]},\\&\alpha_1,\alpha_2,\ \{r_i,z_i,\ \alpha_{i,1},\alpha_{i,2}\}_{i\in[n]},\{c_{j,1},c_{j,2}\}_{j\in[n]}\Big).\end{aligned}$$

In addition, a counter $ctr=0$ is implicitly included in MSK.

$\mathsf{KeyGen}_\mathsf{A}(\mathsf{PP},\mathsf{MSK},S)\rightarrow\mathsf{SK}_{(i,j),S}$. The algorithm first sets $ctr=ctr+1$ and computes the corresponding index in the form of (i,j) where $1\leq i,j\leq n$ and $(i-1)*n+j=ctr$. Then it randomly chooses $\sigma_{i,j,1},\sigma_{i,j,2},\delta_{i,j,1},\delta_{i,j,2}\in\mathbb{Z}_p$, and outputs a private key

$$\begin{aligned}&\mathsf{SK}_{(i,j),S}=\langle\ (i,j),S,\\&\vec{K}_{i,j}=g^{(\alpha_{i,1}+r_ic_{j,1})\vec{b}_1^*+(\alpha_{i,2}+r_ic_{j,2})\vec{b}_2^*}\\&\quad\cdot(hh_j)^{(\sigma_{i,j,1}+\delta_{i,j,1})\vec{b}_1^*+(\sigma_{i,j,2}+\delta_{i,j,2})\vec{b}_2^*},\\&\vec{K}'_{i,j}=g^{(\alpha_1+\sigma_{i,j,1}+\delta_{i,j,1})\vec{b}_1^*+(\alpha_2+\sigma_{i,j,2}+\delta_{i,j,2})\vec{b}_2^*},\\&\vec{K}''_{i,j}=(\vec{K}'_{i,j})^{z_i},\\&\{\vec{K}_{i,j,j'}=h_{j'}^{(\sigma_{i,j,1}+\delta_{i,j,1})\vec{b}_1^*+(\sigma_{i,j,2}+\delta_{i,j,2})\vec{b}_2^*}\}_{j'\in[n]\setminus\{j\}},\\&\vec{K}_{i,j,0}=g^{\delta_{i,j,1}\vec{b}_{0,1}^*+\delta_{i,j,2}\vec{b}_{0,2}^*},\\&\{\vec{K}_{i,j,x}=g^{\sigma_{i,j,1}(\vec{b}_{x,1}^*+\vec{b}_{x,2}^*)+\sigma_{i,j,2}(\vec{b}_{x,3}^*+\vec{b}_{x,4}^*)}\}_{x\in S}\ \rangle.\end{aligned}$$

$\mathsf{Encrypt}_\mathsf{A}(\mathsf{PP},M,R,\mathbb{A}=(A,\rho),(\bar{i},\bar{j}))\rightarrow CT_{R,(A,\rho)}$. $R\subseteq[n,n]$ is a revocation list. A is an $l\times m$ LSSS matrix and ρ maps each row A_k of A to an attribute $\rho(k)\in[\mathcal{U}]$. The encryption is for recipients whose (index, attributes set) pair $\big((i,j),S_{(i,j)}\big)$ satisfy $\big((i,j)\in[n,n]\setminus R\big)\wedge\big(S_{(i,j)}\ satisfies\ (A,\rho)\big)\wedge\big((i,j)\geq(\bar{i},\bar{j})\big)$. Let $\bar{R}=[n,n]\setminus R$ and for $i\in[n],\bar{R}_i=\{j'|(i,j')\in\bar{R}\}$, that is, $\bar{R}$ is the non-revoked index list, and $\bar{R}_i$ is the set of non-revoked column index on the i-th row. The algorithm first chooses random

$$\kappa,\ \tau,\ s_1,\ldots,s_n,\ t_1,\ldots,t_n\in\mathbb{Z}_p,\ \ \vec{v}_c,\ \vec{w}_1,\ldots,\vec{w}_n\in\mathbb{Z}_p^3,\ \ \xi_{1,1},\xi_{1,2},\ldots,\xi_{l,1},\xi_{l,2}\in\mathbb{Z}_p,\ \ \vec{u}_1,\vec{u}_2\in\mathbb{Z}_p^m.$$

It also chooses random $r_x,r_y,r_z\in\mathbb{Z}_p$, and sets $\vec{\chi}_1=(r_x,0,r_z),\vec{\chi}_2=(0,r_y,r_z),\vec{\chi}_3=\vec{\chi}_1\times\vec{\chi}_2=(-r_yr_z,-r_xr_z,r_xr_y)$. Then it randomly chooses

$$\begin{aligned}&\vec{v}_i\in\mathbb{Z}_p^3\ \ for\ i=1,\ldots,\bar{i},\\&\vec{v}_i\in span\{\vec{\chi}_1,\vec{\chi}_2\}\ \ for\ i=\bar{i}+1,\ldots,n.\end{aligned}$$

Let π_1 and π_2 be the first entries of $\vec{u}_1$ and $\vec{u}_2$ respectively. The algorithm creates a ciphertext $\langle R,(A,\rho),\ (\vec{R}_i,\vec{R}'_i,\vec{Q}_i,\vec{Q}'_i,\vec{Q}''_i,T_i)_{i=1}^n,\ (\vec{C}_j,\vec{C}'_j)_{j=1}^n,\ (\vec{P}_k)_{k=0}^l\rangle$ as follows:

1. For each row $i\in[n]$:

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

$$\vec{R}_i = (g^{\vec{b}_1+\vec{b}_2})^{\vec{v}_i},\ \vec{R}'_i = \vec{R}_i^{\kappa},\ \vec{Q}_i = g^{s_i(\vec{b}_1+\vec{b}_2)},$$
$$\vec{Q}'_i = (h\prod_{j'\in\bar{R}_i} h_{j'})^{s_i(\vec{b}_1+\vec{b}_2)}\vec{Z}_i^{t_i}h^{\pi_1\vec{b}_1+\pi_2\vec{b}_2},$$
$$\vec{Q}''_i = g^{t_i(\vec{b}_1+\vec{b}_2)}, T_i = e(g,g)^{\hat{s}_i}.$$

- if $i \geq \bar{i}$: set

$$\vec{R}_i = (\vec{G}_i)^{s_i\vec{v}_i},\ \vec{R}'_i = \vec{R}_i^{\kappa},\ \vec{Q}_i = g^{\tau s_i(\vec{v}_i\cdot\vec{v}_c)(\vec{b}_1+\vec{b}_2)},$$
$$\vec{Q}'_i = (h\prod_{j'\in\bar{R}_i} h_{j'})^{\tau s_i(\vec{v}_i\cdot\vec{v}_c)(\vec{b}_1+\vec{b}_2)}\vec{Z}_i^{t_i}h^{\pi_1\vec{b}_1+\pi_2\vec{b}_2},$$
$$\vec{Q}''_i = g^{t_i(\vec{b}_1+\vec{b}_2)},\ T_i = M\frac{(E_{i,1}E_{i,2})^{\tau s_i(\vec{v}_i\cdot\vec{v}_c)}}{(F_1{}'F_2{}')^{\tau s_i(\vec{v}_i\cdot\vec{v}_c)}F_1^{\pi_1}F_2^{\pi_2}},$$

where $F_1{}' = F_1\prod_{j'\in\bar{R}_i} F_{1,j'}$ and $F_2{}' = F_2\prod_{j'\in\bar{R}_i} F_{2,j'}$ respectively.

2. For each column $j \in [n]$:

- if $j < \bar{j}$: choose random $\mu_j \in \mathbb{Z}_p$, then set

$$\vec{C}_j = (\vec{H}_j)^{\tau(\vec{v}_c+\mu_j\vec{\chi}_3)}(\vec{Y}_j)^{\kappa\vec{w}_j},\ \vec{C}'_j = (\vec{Y}_j)^{\vec{w}_j}.$$

- if $j \geq \bar{j}$: set

$$\vec{C}_j = (\vec{H}_j)^{\tau\vec{v}_c}(\vec{Y}_j)^{\kappa\vec{w}_j},\ \vec{C}'_j = (\vec{Y}_j)^{\vec{w}_j}.$$

3.

$$\vec{P}_0 = h^{\pi_1\vec{b}_{0,1}+\pi_2\vec{b}_{0,2}},$$
$$\{\vec{P}_k = h^{(A_k\cdot\vec{u}_1+\xi_{k,1})\vec{b}_{\rho(k),1}-\xi_{k,1}\vec{b}_{\rho(k),2}}$$
$$\cdot h^{(A_k\cdot\vec{u}_2+\xi_{k,2})\vec{b}_{\rho(k),3}-\xi_{k,2}\vec{b}_{\rho(k),4}}\}_{k\in[l]}.$$

$\mathsf{Decrypt}_{\mathsf{A}}(\mathsf{PP}, CT_{R,(A,\rho)}, \mathsf{SK}_{(i,j),S}) \to M$ or $\perp$.

The algorithm parses $CT_{R,(A,\rho)}$ and $\mathsf{SK}_{(i,j),S}$ to $\langle R, (A,\rho), (\vec{R}_i,\vec{R}'_i,\vec{Q}_i,\vec{Q}'_i,\vec{Q}''_i,T_i)_{i=1}^n, (\vec{C}_j,\vec{C}'_j)_{j=1}^n, (\vec{P}_k)_{k=0}^l\rangle$ and $\langle (i,j), S, \vec{K}_{i,j}, \vec{K}'_{i,j}, \vec{K}''_{i,j}, \{\vec{\vec{K}}_{i,j,j'}\}_{j'\in[n]\setminus\{j\}}, \vec{K}_{i,j,0}, \{\vec{K}_{i,j,x}\}_{x\in S}\rangle$ respectively. If $(i,j) \in R$ or S does not satisfy (A,ρ), the algorithm outputs $\perp$, otherwise it

1. Computes constants $\{\omega_k \in \mathbb{Z}_p | \rho(k) \in S\}$ such that $\sum_{\rho(k)\in S}\omega_k A_k = (1,0,\ldots,0)$, then computes

$$D_P = e_3(\vec{K}_{i,j,0}, \vec{P}_0)\prod_{\rho(k)\in S} e_6(\vec{K}_{i,j,\rho(k)}, \vec{P}_k)^{\omega_k}.$$

2. Since $(i,j) \in \bar{R} (= [n,n]\setminus R)$ implies $j \in \bar{R}_i$, the algorithm can compute

$$\vec{\vec{K}}_{i,j} = \vec{K}_{i,j}\cdot(\prod_{j'\in\bar{R}_i\setminus\{j\}}\vec{\bar{K}}_{i,j,j'})$$
$$= g^{(\alpha_{i,1}+r_ic_{j,1})\vec{b}_1^*+(\alpha_{i,2}+r_ic_{j,2})\vec{b}_2^*}$$
$$\cdot(h\prod_{j'\in\bar{R}_i} h_{j'})^{(\sigma_{i,j,1}+\delta_{i,j,1})\vec{b}_1^*+(\sigma_{i,j,2}+\delta_{i,j,2})\vec{b}_2^*}.$$

Note that if $(i,j) \in R$ (implying $j \notin \bar{R}_i$), the algorithm cannot produce such a $\vec{\vec{K}}_{i,j}$. The algorithm then computes

$$D_I = \frac{e_3(\vec{\vec{K}}_{i,j}, \vec{Q}_i)\cdot e_3(\vec{K}''_{i,j}, \vec{Q}''_i)\cdot e_9(\vec{R}'_i, \vec{C}'_j)}{e_3(\vec{K}'_{i,j}, \vec{Q}'_i)\cdot e_9(\vec{R}_i, \vec{C}_j)}.$$

3. Computes $M = T_i/(D_P\cdot D_I)$ as the output message. Assume the ciphertext is generated from message M' and index $(\bar{i},\bar{j})$, it can be verified that only when $(i > \bar{i})$ or $(i = \bar{i} \wedge j \geq \bar{j})$, $M = M'$ will hold. This follows from the facts that for $i > \bar{i}$, we have $(\vec{v}_i\cdot\vec{\chi}_3) = 0$ (since $\vec{v}_i \in span\{\vec{\chi}_1,\vec{\chi}_2\}$), and for $i = \bar{i}$, we have that $(\vec{v}_i\cdot\vec{\chi}_3) \neq 0$ happens with overwhelming probability (since $\vec{v}_i$ is randomly chosen from $\mathbb{Z}_p^3$). The correctness can be found in the full version (Li et al., 2016, Augmented CP-ABE Definitions).

4.3 Security of The AugR-CP-ABE Construction

The following Theorem 3 and Theorem 4 show that our AugR-CP-ABE construction is message-hiding, and Theorem 5 shows that our AugR-CP-ABE construction is index-hiding.

Theorem 3. *Suppose the DLIN assumption, the D3DH assumption, and the source group q-parallel BDHE assumption hold. Then no PPT adversary can win* $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_1}$ *with non-negligible advantage.*

Proof. We begin by defining our various types of semi-functional keys and ciphertexts. The semi-functional space in the exponent will correspond to the span of $\vec{b}_3, \vec{b}_3^*$, the span of $\vec{b}_{0,3}, \vec{b}_{0,3}^*$ and the span of each $\vec{b}_{x,5}, \vec{b}_{x,6}, \vec{b}_{x,5}^*, \vec{b}_{x,6}^*$.

Semi-functional Keys. To produce a semi-functional key for an attribute set S, one first calls the normal key generation algorithm to produce a normal key consisting of $\vec{K}_{i,j}, \vec{K}'_{i,j}, \vec{K}''_{i,j}, \{\vec{\vec{K}}_{i,j,j'}\}_{j'\in[n]\setminus\{j\}}$, $\vec{K}_{i,j,0}, \{\vec{K}_{i,j,x}\}_{x\in S}$ with index (i,j). One then chooses random value γ. The semi-functional key is

$$\vec{K}_{i,j}(hh_j)^{\gamma\vec{b}_3^*},\ \vec{K}'_{i,j}g^{\gamma\vec{b}_3^*},\ \vec{K}''_{i,j}g^{z_i\gamma\vec{b}_3^*},$$
$$\{\vec{\vec{K}}_{i,j,j'}h_{j'}^{\gamma\vec{b}_3^*}\}_{j'\in[n]\setminus\{j\}},\ \vec{K}_{i,j,0},\ \{\vec{K}_{i,j,x}\}_{x\in S}.$$

Semi-functional Ciphertexts. To produce a semi-functional ciphertext for an LSSS matrix (A,ρ) of size $l\times m$, one first calls the normal encryption algorithm to produce a normal ciphertext consisting of

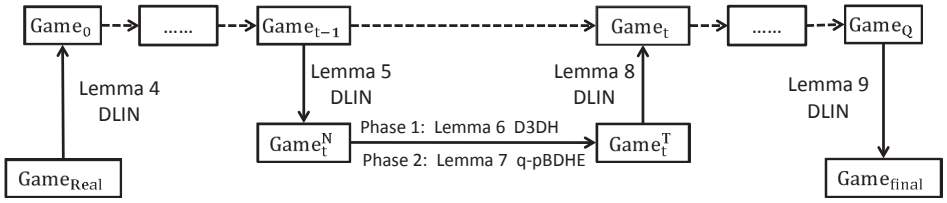

Figure 1: Lemmas 4, 5, 8, and 9 rely on the subspace assumption, which is implied by DLIN assumption, Lemma 6 relies on the D3DH assumption, and Lemma 7 relies on the source group q-parallel BDHE assumption.

$\langle R, (A, \mathrm{p}),\ (\vec{R}_i, \vec{R}'_i, \vec{Q}_i, \vec{Q}'_i, \vec{Q}''_i, T_i)_{i=1}^{n}, (\vec{C}_j, \vec{C}'_j)_{j=1}^{n},$
$(\vec{P}_k)_{k=0}^{l} \rangle$. One then chooses random values $\pi_3, \xi_{k,3} (1 \le k \le l) \in \mathbb{Z}_p$ and a random vector $\vec{u}_3 \in \mathbb{Z}_p^m$ with first entry equal to π_3. The semi-functional ciphertext is:

$$\langle R, (A, \mathrm{p}),\ (\vec{R}_i, \vec{R}'_i, \vec{Q}_i, \vec{Q}'_i h^{\pi_3 \vec{b}_3}, \vec{Q}''_i, T_i)_{i=1}^{n}, (\vec{C}_j, \vec{C}'_j)_{j=1}^{n},$$
$$\vec{P}_0 h^{\pi_3 \vec{b}_{0,3}}, (\vec{P}_k h^{(A_k \cdot \vec{u}_3 + \xi_{k,3}) \vec{b}_{\mathrm{p}(k),5} - \xi_{k,3} \vec{b}_{\mathrm{p}(k),6}})_{k=1}^{l} \rangle.$$

Our proof is obtained via a hybrid argument over a sequence of games: Game_{real}, Game_t and Game_{final}.

The outer structure of our hybrid argument will progress as shown in Figure 1. First, we transition from Game_{real} to Game_0, then to Game_1, next to Game_2, and so on. We ultimately arrive at Game_Q, where the ciphertext and all of the keys given to the attacker are semi-functional. We then transition to Game_{final}, which is defined to be like Game_Q, except that the ciphertext given to the attacker is a semi-functional encryption of a random message. This will complete our proof, since any attacker has a zero advantage in this final game.

The transitions from Game_{real} to Game_0 and from Game_Q to Game_{final} are relatively easy and can be accomplished directly via computational assumptions. The transitions from Game_{t-1} to Game_t require more intricate arguments. For these steps, we will need to treat Phase 1 key requests (before the challenge ciphertext) and Phase 2 key requests (after the challenge ciphertext) differently. We will also need to define two additional types of semi-functional keys:

Nominal Semi-functional Keys. To produce a nominal semi-functional key for an attribute set S, one first calls the normal key generation algorithm to produce a normal key consisting of $\vec{K}_{i,j}, \vec{K}'_{i,j}, \vec{K}''_{i,j}, \{\vec{K}_{i,j,j'}\}_{j' \in [n] \setminus \{j\}}, \vec{K}_{i,j,0}, \{\vec{K}_{i,j,x}\}_{x \in S}$ with index (i, j). One then chooses random values $\sigma_{i,j,3}, \delta_{i,j,3} \in \mathbb{Z}_p$. The nominal semi-functional key is:

$$\vec{K}_{i,j} (hh_j)^{(\sigma_{i,j,3} + \delta_{i,j,3}) \vec{b}^*_3},\ \vec{K}'_{i,j} g^{(\sigma_{i,j,3} + \delta_{i,j,3}) \vec{b}^*_3},$$
$$\vec{K}''_{i,j} g^{z_i (\sigma_{i,j,3} + \delta_{i,j,3}) \vec{b}^*_3},\ \{\vec{K}_{i,j,j'} h_{j'}^{(\sigma_{i,j,3} + \delta_{i,j,3}) \vec{b}^*_3}\}_{j' \in [n] \setminus \{j\}},$$
$$\vec{K}_{i,j,0} g^{\delta_{i,j,3} \vec{b}^*_{0,3}},\ \{\vec{K}_{i,j,x} g^{\sigma_{i,j,3} (\vec{b}^*_{x,5} + \vec{b}^*_{x,6})}\}_{x \in S}.$$

We note that a nominal semi-functional key still correctly decrypts a semi-functional ciphertext.

Temporary Semi-functional Keys. A temporary semi-functional key is similar to a nominal semi-functional key, except that the semi-functional component attached to $\vec{K}'_{i,j}$ will now be randomized (this will prevent correct decryption of a semi-functional ciphertext) and $\vec{K}_{i,j}$, $\vec{K}''_{i,j}$ and $\{\vec{K}_{i,j,j'}\}_{j' \in [n] \setminus \{j\}}$ change accordingly. More formally, to produce a temporary semi-functional key for an attribute set S, one first calls the normal key generation algorithm to produce a normal key consisting of $\vec{K}_{i,j}, \vec{K}'_{i,j}, \vec{K}''_{i,j}, \{\vec{K}_{i,j,j'}\}_{j' \in [n] \setminus \{j\}}, \vec{K}_{i,j,0}, \{\vec{K}_{i,j,x}\}_{x \in S}$ with index (i, j). One then chooses random values $\sigma_{i,j,3}, \delta_{i,j,3}, \gamma \in \mathbb{Z}_p$. The temporary semi-functional key is formed as:

$$\vec{K}_{i,j} (hh_j)^{\gamma \vec{b}^*_3},\ \vec{K}'_{i,j} g^{\gamma \vec{b}^*_3},\ \vec{K}''_{i,j} g^{z_i \gamma \vec{b}^*_3},\ \{\vec{K}_{i,j,j'} h_{j'}^{\gamma \vec{b}^*_3}\}_{j' \in [n] \setminus \{j\}},$$
$$\vec{K}_{i,j,0} g^{\delta_{i,j,3} \vec{b}^*_{0,3}},\ \{\vec{K}_{i,j,x} g^{\sigma_{i,j,3} (\vec{b}^*_{x,5} + \vec{b}^*_{x,6})}\}_{x \in S}.$$

For each t from 1 to Q, we define the additional games: Game_t^N and Game_t^T.

In order to transition from Game_{t-1} to Game_t in our hybrid argument, we will transition first from Game_{t-1} to Game_t^N, then to Game_t^T, and finally to Game_t. The transition from Game_t^N to Game_t^T will require different computational assumptions for Phase 1 and Phase 2 queries (As shown in Figure 1, we use two lemmas based on different assumptions to obtain the transition).

As shown in Figure 1, we use a series of lemmas, i.e. Lemmas 4, 5, 6, 7, 8, and 9, to prove the transitions. The details of these games, lemmas and their proofs can be found in the full version (Li et al., 2016, Appendix C.1).

□

Theorem 4. *No PPT adversary can win* $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_{N+1}}$ *with non-negligible advantage.*

Proof. The argument for security of $\mathsf{Game}^{\mathsf{A}}_{\mathsf{MH}_{N+1}}$ is very straightforward since an encryption to index $N+$

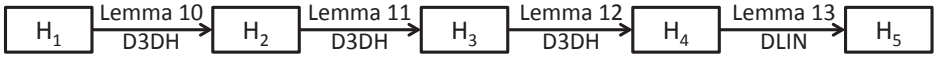

Figure 2: Lemmas 10, 11, and 12 rely on the D3DH assumption, and Lemma 13 relies on the DLIN assumption.

$1 = (n+1,1)$ contains no information about the message. The simulator simply runs actual $\mathsf{Setup}_\mathsf{A}$ and $\mathsf{KeyGen}_\mathsf{A}$ algorithms and encrypts the message M_b by the challenge access policy $\mathbb{A}$ and index $(n+1,1)$. Since for all $i = 1$ to n, the values of T_i contain no information about the message, the bit b is perfectly hidden and $\mathsf{MH}^{\mathsf{A}}_{N+1}\mathsf{Adv}_{\mathcal{A}} = 0$. □

Theorem 5. *Suppose that the D3DH assumption and the DLIN assumption hold. Then no PPT adversary can win* $\mathsf{Game}^{\mathsf{A}}_{\mathsf{IH}}$ *with non-negligible advantage.*

Proof. Theorem 5 follows Lemma 1 and Lemma 2 below. □

Lemma 1. *Suppose that the D3DH assumption holds. Then for* $j < n$ *no PPT adversary can distinguish between an encryption to* $(\bar{i},\bar{j})$ *and* $(\bar{i},\bar{j}+1)$ *in* $\mathsf{Game}^{\mathsf{A}}_{\mathsf{IH}}$ *with non-negligible advantage.*

Proof. In $\mathsf{Game}^{\mathsf{A}}_{\mathsf{IH}}$, the adversary $\mathcal{A}$ will eventually behave in one of two different ways:

Case I: In Key Query phase, $\mathcal{A}$ will not submit $((\bar{i},\bar{j}),S_{(\bar{i},\bar{j})})$ for some attribute set $S_{(\bar{i},\bar{j})}$ to query the corresponding private key. In Challenge phase, $\mathcal{A}$ submits a message M and a non-empty attribute set S^*. There is not any restriction on S^*.

Case II: In Key Query phase, $\mathcal{A}$ will submit $((\bar{i},\bar{j}),S_{(\bar{i},\bar{j})})$ for some attribute set $S_{(\bar{i},\bar{j})}$ to query the corresponding private key. In Challenge phase, $\mathcal{A}$ submits a message M and a non-empty attribute set S^* with the restriction that the corresponding strictest access policy $\mathbb{A}_{S^*}$ is not satisfied by $S_{(\bar{i},\bar{j})}$. **Case II** has the following sub-cases:

1. $(\bar{i},\bar{j}) \notin [n,n] \setminus R^*$, $S_{(\bar{i},\bar{j})}$ satisfies $\mathbb{A}^*$.
2. $(\bar{i},\bar{j}) \notin [n,n] \setminus R^*$, $S_{(\bar{i},\bar{j})}$ does not satisfy $\mathbb{A}^*$.
3. $(\bar{i},\bar{j}) \in [n,n] \setminus R^*$, $S_{(\bar{i},\bar{j})}$ does not satisfy $\mathbb{A}^*$.

We flip a random coin $c \in \{0,1\}$ as our guess on which case that $\mathcal{A}$ is in. In particular, if $c = 0$, we guess that $\mathcal{A}$ is in **Case I**, **Case II.1** or **Case II.2**. In this case, it follows the restriction in the index-hiding game for Augmented Broadcast Encryption (AugBE) in (Garg et al., 2010), where the adversay does not query the key with index $(\bar{i},\bar{j})$ or $(\bar{i},\bar{j})$ is not in the receiver list $[n,n] \setminus R^*$. If $c = 1$, we guess that $\mathcal{A}$ is in **Case I**, **Case II.2** or **Case II.3**. As of the fully secure CP-ABE schemes in (Lewko et al., 2010; Okamoto and Takashima, 2010; Lewko and Waters, 2012a; Lewko and Waters, 2012b; Liu et al., 2013a), we assume that the size of attribute universe (i.e. $|\mathcal{U}|$) is polynomial in the security parameter λ, so that a degradation of $O(1/|\mathcal{U}|)$ in the security reduction is acceptable. The proof details of Lemma 1 can be found in the full version (Li et al., 2016, Appendix C.2). □

Lemma 2. *Suppose the D3DH assumption and the DLIN assumption hold. Then for any* $1 \le \bar{i} \le n$ *no PPT adversary can distinguish between an encryption to* $(\bar{i},n)$ *and* $(\bar{i}+1,1)$ *in* $\mathsf{Game}^{\mathsf{A}}_{\mathsf{IH}}$ *with non-negligible advantage.*

Proof. The proof of this lemma follows from a series of lemmas that establish the indistinguishability of the following games, where "less-than row" implies the corresponding $\vec{v}_i$ is randomly chosen from $\mathbb{Z}_p^3$ and T_i is a random element (i.e. $T_i = e(g,g)^{\hat{s}_i}$), "target row" implies the corresponding $\vec{v}_i$ is randomly chosen from $\mathbb{Z}_p^3$ and T_i is well-formed, and "greater-than row" implies the corresponding $\vec{v}_i$ is randomly chosen from $span\{\vec{\chi}_1,\vec{\chi}_2\}$ and T_i is well-formed.

- H_1: Encrypt to column n, row $\bar{i}$ is the target row, row $\bar{i}+1$ is the greater-than row.
- H_2: Encrypt to column $n+1$, row $\bar{i}$ is the target row, row $\bar{i}+1$ is the greater-than row.
- H_3: Encrypt to column $n+1$, row $\bar{i}$ is the less-than row, row $\bar{i}+1$ is the greater-than row (no target row).
- H_4: Encrypt to column 1, row $\bar{i}$ is the less-than row, row $\bar{i}+1$ is the greater-than row (no target row).
- H_5: Encrypt to column 1, row $\bar{i}$ is the less-than row, row $\bar{i}+1$ is the target row.

It can be observed that game H_1 corresponds to the encryption being done to $(\bar{i},n)$ and game H_5 corresponds to encryption to $(\bar{i}+1,1)$. As shown in Figure 2, we use a series of lemmas, i.e. Lemmas 10, 11, 12, and 13, to prove the indistinguishability of the games H_1 and H_5. The details of these lemmas and their proofs can be found in the full version (Li et al., 2016, Appendix C.3). □

5 CONCLUSION

In this paper, we proposed a new Augmented R-CP-ABE construction on prime order groups, and

proved its message-hiding and index-hiding properties in the standard model. This CP-ABE achieves full security in the standard model on prime order groups. Our contributions are (1) adding the revocation list, and (2) proving its full security with revocability. We follow the proof method in (Liu and Wong, 2015b) for message-hiding, and build two direct reductions for the proof for index-hiding. The scheme is a fully collusion-resistant blackbox traceable R-CP-ABE scheme. It achieves the most efficient level to date, with overhead in $O(\sqrt{N})$ only.

REFERENCES

Attrapadung, N. and Imai, H. (2009). Conjunctive broadcast and attribute-based encryption. In *Pairing*, pages 248–265.

Bethencourt, J., Sahai, A., and Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334.

Cheung, L. and Newport, C. C. (2007). Provably secure ciphertext policy ABE. In *ACM Conference on Computer and Communications Security*, pages 456–465.

Deng, H., Wu, Q., Qin, B., Mao, J., Liu, X., Zhang, L., and Shi, W. (2014). Who is touching my cloud. In *ESORICS, Part I*, pages 362–379.

Garg, S., Kumarasubramanian, A., Sahai, A., and Waters, B. (2010). Building efficient fully collusion-resilient traitor tracing and revocation schemes. In *ACM Conference on Computer and Communications Security*, pages 121–130.

Goyal, V., Jain, A., Pandey, O., and Sahai, A. (2008). Bounded ciphertext policy attribute based encryption. In *ICALP (2)*, pages 579–591.

Herranz, J., Laguillaumie, F., and Ràfols, C. (2010). Constant size ciphertexts in threshold attribute-based encryption. In *Public Key Cryptography*, pages 19–34.

Lewko, A. B. (2012). Tools for simulating features of composite order bilinear groups in the prime order setting. In *EUROCRYPT*, pages 318–335.

Lewko, A. B., Okamoto, T., Sahai, A., Takashima, K., and Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *EUROCRYPT*, pages 62–91.

Lewko, A. B. and Waters, B. (2012a). New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *CRYPTO*, pages 180–198.

Lewko, A. B. and Waters, B. (2012b). New proof methods for attribute-based encryption: Achieving full security through selective techniques. *IACR Cryptology ePrint Archive*, 2012:326.

Li, X., Liang, K., Liu, Z., and Wong, D. S. (2016). Attribute based encryption: Traitor tracing, revocation and fully security on prime order groups. *IACR Cryptology ePrint Archive*, 2016:1140.

Liu, Z., Cao, Z., and Wong, D. S. (2013a). 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*, pages 475–486.

Liu, Z., Cao, Z., and Wong, D. S. (2013b). White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. *IEEE Transactions on Information Forensics and Security*, 8(1):76–88.

Liu, Z. and Wong, D. S. (2015a). Practical ciphertext-policy attribute-based encryption: Traitor tracing, revocation, and large universe. In Malkin, T., Kolesnikov, V., Lewko, A. B., and Polychronakis, M., editors, *Applied Cryptography and Network Security - 13th International Conference, ACNS 2015, New York, NY, USA, June 2-5, 2015, Revised Selected Papers*, volume 9092 of *Lecture Notes in Computer Science*, pages 127–146. Springer.

Liu, Z. and Wong, D. S. (2015b). Traceable CP-ABE on prime order groups: Fully secure and fully collusion-resistant blackbox traceable. In Qing, S., Okamoto, E., Kim, K., and Liu, D., editors, *Information and Communications Security - 17th International Conference, ICICS 2015, Beijing, China, December 9-11, 2015, Revised Selected Papers*, volume 9543 of *Lecture Notes in Computer Science*, pages 109–124. Springer.

Okamoto, T. and Takashima, K. (2008). Homomorphic encryption and signatures from vector decomposition. In *Pairing*, pages 57–74.

Okamoto, T. and Takashima, K. (2009). Hierarchical predicate encryption for inner-products. In *ASIACRYPT*, pages 214–231.

Okamoto, T. and Takashima, K. (2010). Fully secure functional encryption with general relations from the decisional linear assumption. In *CRYPTO*, pages 191–208.

Rouselakis, Y. and Waters, B. (2013). Practical constructions and new proof methods for large universe attribute-based encryption. In *ACM Conference on Computer and Communications Security*, pages 463–474.

Sahai, A., Seyalioglu, H., and Waters, B. (2012). Dynamic credentials and ciphertext delegation for attribute-based encryption. In *CRYPTO*, pages 199–217.

Sahai, A. and Waters, B. (2005). Fuzzy identity-based encryption. In *EUROCRYPT*, pages 457–473.

Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography*, pages 53–70.