Published online 26 August 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1331

RESEARCH ARTICLE

Fully secure bandwidth-efficient anonymous ciphertext-policy attribute-based encryption

Y. Sreenivasa Rao* and Ratna Dutta

Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur-721302, India

ABSTRACT

The functionality of ciphertext-policy attribute-based encryption (CP-ABE) enables the encryptor to encrypt the data for a group of users of his choice by incorporating an access policy over target receivers' attributes into encryption algorithm itself. This makes CP-ABE systems appealing in several applications where complex access control is at prime concern, but incurs high communication and computation overheads which could impede its practical usage. Another limitation of CP-ABE is that the ciphertext includes the access policy explicitly and, hence, anyone who has access to the ciphertext can identify all legitimate recipients of that ciphertext. This is not desirable for certain mission-critical applications such as military operations. In order to alleviate these problems, we add privacy-preserving property efficiently to CP-ABE scheme via concealing the access policy partially. The encryption in our construction exploits monotone access policies over receivers' attributes and makes ciphertext size constant. The construction is fully secure and can achieve recipient anonymity as the ciphertext terms do not leak any information about recipients. The full semantic security with anonymity relies on dual-system encryption technique in composite order bilinear groups. To the best of our knowledge, the proposed scheme is the *first* construction in the anonymous ABE literature with the stated functionality. Copyright © 2015 John Wiley & Sons, Ltd.

KEYWORDS
attribute-based encryption; recipient anonymity; full security; ciphertext-policy; monotone access policy

***Correspondence**
Y. Sreenivasa Rao, Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur-721302, India.
E-mail: y.sreenivasarao2008@gmail.com

1. INTRODUCTION

It is not always possible for the sender to identify the actual recipients of a ciphertext at the time of encryption, especially in large-scale distributed environments such as online social networks and distributed cloud technology. In these situations, the ordinary public key encryption primitives, including identity-based encryption [1] and broadcast encryption [2], fail to provide fine-grained access control over encrypted data storage as they require prior knowledge of all possible recipients during encryption. The enforcement of complex access control policies over receivers' common credentials, referred as *attributes,* without knowing their original identities resolves the problem. Bethencourt *et al.* [3] devised such cryptographic primitive called ciphertext-policy attribute-based encryption (CP-ABE) wherein each user is tagged with a set of descriptive attributes and the ability to decrypt ciphertexts is controlled by access policies specified in terms of target receivers' attributes. Specifically, user secret key is labeled with a set of attributes and ciphertext is associated with an access policy; a secret key that has enough attributes to satisfy the access policy decrypts the ciphertext. Consider a scenario where a sender wants to transmit a message to all chief editors of Wiley journals. The sender needs to acquire all public keys or identities of chief editors to encrypt the message using traditional public key encryption techniques. This task could be prohibitively expensive. But, using CP-ABE, the sender can encrypt the message with the access control policy "wiley AND editor-in-chief" without knowledge of the complete list of receivers in such a way that no one can view the message from Wiley personnel except chief editors.

While CP-ABE is more flexible to ensure fine-grained access control mechanism, it incurs high communication and computation overheads which could impede its practical usage. Thus, it is desirable to have constructions which feature *constant* communication and computation costs for the environments equipped with computational capability constrained devices and bandwidth is the main concern. In an attempt to reduce the size[†] of ciphertext to constant, Emura *et al.* [4] introduced a less expressive CP-ABE using "equality" relation between the decryptor's attribute set and encryption attribute set. Consequently, the decryptor needs to use all its attribute secret keys in decryption. In this case, the access policy is called an n-of-n (or AND gate) policy, and the scheme is more likely an identity-based construction with the natural consideration that the whole user attribute set is its identity. Following [4], various CP-ABE schemes with constant-size ciphertext have been proposed, enforcing t-of-n [5,6], n-of-n [7–9], non-monotone [10], and monotone [11,12] policies.

In most of the CP-ABE schemes, the access policy is tagged along with the ciphertext, because without knowing the structure of the access policy, the decryptor cannot anticipate which keys make decryption succeed. Thus, anyone who has access to the ciphertext can gain the knowledge of possible recipients. This is not desirable in situations where the access policy itself carries sensitive information such as in some military operations. *Hidden policy* CP-ABE schemes are a prime concern in these circumstances, where the access policy is not explicitly embedded in the ciphertext (in this case, the ciphertext is called a *policy hiding ciphertext*). Regarding hidden policy framework, Nishide *et al.* [13] introduced the notion of partially hidden access policy CP-ABE based on prime order bilinear groups. The scheme is proven to be secure in a weaker model, called *selective* security model, where the adversary needs to fix the challenge access policy before seeing the public parameters.

Emura *et al.* [4] reported that their CP-ABE primitive can be treated as policy hiding realization; however, it fails to provide *recipient anonymity* as explained subsequently: given an access policy W_0 and a policy hiding ciphertext CT. If a third party is able to decide whether CT is generated under W_0 or not, then the scheme is said to provide *no* recipient anonymity. The ciphertext in [4] is in the form of $\mathsf{CT} = [W, C = M\Gamma^s, C_1 = g^s, C_2 = (\prod_{w \in W} T_w)^s]$, where W is an access policy (here, it is a set of attributes), M is a message, Γ and g are public parameters, $T_w = g^{t_w}$ is the public parameter of the attribute w, and s is a random exponent sampled by the encryptor. The components C_1, C_2 of a ciphertext CT for attributes form a decision Diffie–Hellman (DDH)-tuple $(g, C_1, \prod_{w \in W} T_w, C_2) = (g, g^s, g^{\sum_{w \in W} t_w}, g^{s \sum_{w \in W} t_w})$ with the attribute public parameters $\{T_w\}_{w \in W}$as$\hat{e}(C_1, \prod_{w \in W} T_w) = \hat{e}(g^s, \prod_{w \in W} T_w) = \hat{e}(g, (\prod_{w \in W} T_w)^s) = \hat{e}(g, C_2)$, where $\hat{e}$ is a bilinear map on prime order group. Hence, it leaks information about ciphertext attributes. To be specific, given an access policy W_0 and a ciphertext $\mathsf{CT}' = [C', C'_1, C'_2]$ (in the case of treating [4] as hidden policy CP-ABE), the adversary can execute the DDH-test, namely, $\hat{e}(C'_1, \prod_{w' \in W_0} T_{w'}) \overset{?}{=} \hat{e}(g, C'_2)$ using the public keys of attributes listed in W_0 and the given ciphertext components. If the test is valid, then CT' is calculated according to W_0, otherwise, CT' is computed according to some other policy. Consequently, the adversary is able to determine whether the ciphertext CT' is created under the given access policy W_0 or not, thus cannot realize recipient anonymity.

The CP-ABE proposed in [7] is policy hiding, but cannot mount to similar DDH-test attacks and thus not recipient anonymous (Section 3.2 for details). Consequently, policy hiding seems to be inadequate to preserve recipient anonymity. To ensure recipient anonymity, it is essential to conceal the access policy used in encryption as well as the ciphertext should not be vulnerable to the mere DDH-test attacks. The CP-ABE primitives [13–17] achieve recipient anonymity, but the size of ciphertext is proportional to the number of attributes used in the ciphertext. To the best of our knowledge, there is no CP-ABE with recipient anonymity that features constant-size ciphertext and full security (i.e., non-selective security) until we, recently, proposed fully secure recipient anonymous CP-ABE [8] with constant-size ciphertext modifying [4] by means of composite order bilinear groups. However, the construction exploits very restricted n-of-n access policy, thereby can be treated as identity-based realization with all these functionality. The aim of this article is to extend expressivity of access policy from n-of-n to monotone policy while attaining the same functionality as that of [8].

1.1. Our contribution

We propose a new CP-ABE scheme with constant-size ciphertext wherein the access policy is partially hidden in the ciphertext. Instead of the actual access policy over receivers' attributes, we append an attribute index set, called *anonymized access policy*, to the ciphertext in order to reconstruct the original access policy during decryption. The actual attribute from the set of possible attributes of each attribute category involved in the ciphertext is made completely hidden. A legitimate user can rebuild the access policy hidden in the ciphertext from the pair of his own attribute set and the anonymized access policy to make decryption successful. However, unauthorized decryptors cannot learn anything about the access policy.

To achieve recipient anonymity, we multiply public parameters and ciphertext terms with another group element. As a result, every outcome of the DDH-test on the public keys and the ciphertext components is randomized by some pairings on the multiplied elements, and thus, the test fails always unconditionally. Consequently, no one can draw the conclusions based on these equally distributed outcomes. This prevents the DDH-test attacks and attains recipient anonymity.

Recently proposed privacy-preserving CP-ABE [7] features constant-size ciphertext and partially policy hiding but does not realize recipient anonymity. The security analysis described in [7] is not appropriate for policy

[†] According to attribute-based cryptography literature, we do not consider the description of the access policy or the attribute set as being part of the ciphertext or secret key, respectively, while measuring its size.

DOI: 10.1002/sec

Table I. Comparison of CP-ABE schemes with *constant-size* ciphertext.

Scheme	Order of bilinear group	Security	Complexity assumption	Access policy	Recipient anonymity
[4]	p	Selective	DBDH	n-of-n	No
[10]	p	Selective	DBDHE	Non-monotone	No
[5]	p	Selective	aMSE-DDH	t-of-n	No
[6]	p	Selective	DBDHE	t-of-n	No
[11]	p	Selective	DBDH	Monotone	No
[7]	p	Selective	DBDHE	n-of-n with wildcards	No
[9]	p	Full	aDBDHE	n-of-n	No
[12]	$p_1p_2p_3$	Full	3 static assumptions	Monotone	No
[8]	$p_1p_2p_3$	Full	4 static assumptions	n-of-n	Yes
Proposed	$p_1p_2p_3$	Full	4 static assumptions	Monotone	Yes

Here p and $p_i, i \in 1, 2, 3$ are prime numbers, (a)DBDH(E), (augmented) decisional bilinear Diffie–Hellman (exponent); aMSE-DDH, augmented multi-sequence of exponents decisional Diffie–Hellman; CP-ABE, ciphertext-policy attribute-based encryption.

hiding CP-ABE schemes due to the fact that policy hiding is not argued formally by means of indistinguishability game. Although the scheme [7] enforces n-of-n with wildcard policies to enable attribute-based access control, it resembles identity-based encryption in the absence of the wildcard attributes like [4]. Our framework exploits flexible monotone access policies during encryption that are more expressive than n-of-n policies.

The attribute-hiding predicate encryption schemes [18,19] yield complete hidden access policy CP-ABE schemes that offer full security. However, they suffer from linear-size ciphertexts. Recently, Doshi and Jinwala [12] proposed fully secure CP-ABE with constant-size ciphertext by making use of composite order bilinear groups. They did not take policy hiding into account, thereby cannot realize recipient anonymity. Unlike [12], we achieve recipient anonymity and full semantic security under four static assumptions [16], whose security proof is based on Water's dual-system framework [20] in composite order bilinear groups. To the best of our knowledge, the proposed scheme is the first construction with the aforementioned functionality. Table I presents the property comparison of our scheme against existing constant-size ciphertext CP-ABE schemes.

1.2. Previous work

Attribute-based encryption schemes. The notion of attribute-based encryption (ABE) is introduced by Sahai and Waters in their seminal paper [21]. Goyal *et al.* [22] later categorized ABE as either key-policy ABE (KP-ABE) or ciphertext-policy ABE (CP-ABE) based on the role of an access policy/structure. KP-ABE is the dual form of CP-ABE. More specifically, in KP-ABE, the access policy is specified in user secret key and ciphertext is labeled with a set of attributes; a secret key can decrypt a ciphertext only if the attributes listed in the ciphertext satisfy the access policy associated with the secret key. Explicit construction for KP-ABE is given in [22] wherein expressive monotone access structures are exploited while the construction of CP-ABE is left open. The first CP-ABE primitive is constructed by Bethencourt *et al.* [3] for the same access structure used in [22]. Thereafter, various KP and CP-ABE realizations [5,19,23–28] are introduced in order to enhance the security as well as the expressivity of the access policy. The same attribute shared by various users in ABE causes *collusion attack,* that is, a group of users cooperatively succeed in decryption while individually fails for the same. The most popular technique to counteract collusion attack is randomization of user secret keys. We use the same technique here.

Selective vs full security. The ABE schemes [4–7,10,11,21–26,28,29] are secure against selective adversary wherein depending on the challenge access policy predefined by the adversary, the simulator programs the public parameters to establish security reduction. This imposes undesirable restrictions on the adversary and weakens the security level as it forbids the selection of adaptive challenge access policy after setup. Lewko *et al.* [19] designed the first fully secure KP and CP-ABE primitives by employing the dual-system encryption methodology introduced by Waters [20] based on composite order bilinear groups.

In this framework, there are two types of decryption keys and ciphertexts called *normal* and *semi-functional*. The normal keys and ciphertexts are used in the original scheme, whereas the semi-functional ones only appeared in the security proof. The normal decryption keys can decrypt normal as well as semi-functional ciphertexts. The semi-functional decryption keys can decrypt normal ciphertexts but cannot decrypt a semi-functional ciphertext. The security proof employs a hybrid argument over a sequence of security games: first, the normal challenge ciphertext is transformed into semi-functional, and then the decryption keys are changed from normal to semi-functional one by one. In the final game, the adversary can obtain only semi-functional decryption keys which are of no use for decrypting the semi-functional ciphertext. Hence, the security can be realized. The schemes presented in [19] exhibit linear-size ciphertexts. The constructions [8,12] are realized constant-size ciphertext with full security by using the dual-system framework on composite order bilinear groups in the ciphertext-policy setting.

1.3. Paper organization

The rest of the paper is organized as follows. The necessary background is reviewed in Section 2. In Section 3, we discuss the attack on recipient anonymity of Zhou *et al.* [7] CP-ABE scheme. Our construction and its security analysis are described in Sections 4 and 5, respectively. The performance of our proposed scheme is analyzed and compared with existing schemes in Section 6. Finally, the paper is concluded in Section 7. In the Appendix, we present the generic security of the complexity assumptions used in security proof of proposed scheme.

2. BACKGROUND

This section is dedicated to exhibit necessary background for further explanation that includes access policy over attributes, composite order bilinear groups, the complexity assumptions used in security reduction, and the CP-ABE system and its security definition.

We use frequently the following notations in the rest of the paper.

$x \overset{\$}{\leftarrow} X$	:	x is randomly selected from the set X
$\mathsf{op} \leftarrow \mathsf{Alg}(\mathsf{ip})$	:	algorithm Alg takes as input ip and outputs op
$f : \mathbb{A} \rightarrow \mathbb{B}$	:	f is a mapping from $\mathbb{A}$ to $\mathbb{B}$
$[m]$	:	$\{1, 2, \ldots, m\}$
$ord(\Delta)$	:	order of Δ

Definition 1 (Access policy). *Let U be the universe of attributes and $\mathcal{P}(U)$ be the collection of all subsets of U. Every non-empty subset W of $\mathcal{P}(U) \backslash \{\emptyset\}$ is called an access structure/policy. The sets in W are called authorized sets, and the sets not in W are called unauthorized sets with respect to W. An access policy W is said to be monotone access policy if every superset of an authorized set is again authorized in W, that is, for any $C \in \mathcal{P}(U)$, with $C \supseteq B$ where $B \in W$ implies $C \in W$. An attribute set L satisfies W if and only if L is an authorized set in W, that is, $L \in W$.*

2.1. Composite order bilinear group

Our construction is based on composite order bilinear groups [30]. Let $\mathcal{G}(\cdot)$ be a composite order group generator. Taking as input the security parameter κ, $\mathcal{G}(\cdot)$ generates $\Sigma = \left(N, \mathbb{G}, \widehat{\mathbb{G}}, e\right)$, where N is a product of three distinct primes p_1, p_2, p_3, that is, $N = p_1 p_2 p_3$, $\mathbb{G}, \widehat{\mathbb{G}}$ are multiplicative cyclic groups with $ord(\mathbb{G}) = ord(\widehat{\mathbb{G}}) = N$ and $e : \mathbb{G} \otimes \mathbb{G} \rightarrow \widehat{\mathbb{G}}$, where $\mathbb{G} \otimes \mathbb{G} = \{(h, k) : h, k \in \mathbb{G}\}$ is a map satisfying the following properties.

- $e(x^a, y^b) = e(x, y)^{ab}$, for all $x, y \in \mathbb{G}$ and $a, b \in \mathbb{Z}_N$,
- there is a $g \in \mathbb{G}$ such that $e(g, g)$ generates entire $\widehat{\mathbb{G}}$,
- the group operations in $\mathbb{G}, \widehat{\mathbb{G}}$ and the bilinear map e are efficiently computable.

Remark 1. The bilinear property $e(x^a, y^b) = e(x, y)^{ab}$ yields the following identities.
(i) $e(u, v) = e(v, u)$, (ii) $e(u_1 u_2, v) = e(u_1, v) \cdot e(u_2, v)$ and (iii) $e(u, v_1 v_2) = e(u, v_1) \cdot e(u, v_2)$, for $u, u_1, u_2, v, v_1, v_2 \in \mathbb{G}$.

Let $\mathbb{G}_{p_i}$ be a subgroup of $\mathbb{G}$ such that $ord(\mathbb{G}_{p_i}) = p_i$ for $i \in \{1, 2, 3\}$. A random element $u \in \mathbb{G}_{p_i}$ can be sampled by choosing a random $\alpha \in \mathbb{Z}_N$ and setting $u = g_i^{\alpha}$, where g_i is a generator of $\mathbb{G}_{p_i}$ and $i \in \{1, 2, 3\}$. We have the following theorem from [19].

Theorem 1 (Orthogonal Property). *$e(u_i, u_j) = \hat{1}$ for any $u_i \in \mathbb{G}_{p_i}, u_j \in \mathbb{G}_{p_j}$ and $i \neq j$. Here, $\hat{1}$ is the identity element in $\widehat{\mathbb{G}}$.*

Proof. Suppose g is a generator of the cyclic group $\mathbb{G}$. Then, because $ord(g) = ord(\mathbb{G}) = N$,

$$\left(g^{\prod_{k\in\{1,2,3\},k\neq i} p_k}\right)^{p_i} = g^{\prod_{k\in\{1,2,3\}} p_k} = g^N = 1$$

where 1 is the identity in $\mathbb{G}$. Hence, $ord\left(g^{\prod_{k\in\{1,2,3\},k\neq i} p_k}\right) = p_i = ord(\mathbb{G}_{p_i})$. Therefore, $g^{\prod_{k\in\{1,2,3\},k\neq i} p_k}$ is a generator of $\mathbb{G}_{p_i}$. Similarly, the element $g^{\prod_{k\in\{1,2,3\},k\neq j} p_k}$ generates the subgroup $\mathbb{G}_{p_j}$.

Therefore, $u_i = \left(g^{\prod_{k\in\{1,2,3\},k\neq i} p_k}\right)^{\alpha}$ and $u_j = \left(g^{\prod_{k\in\{1,2,3\},k\neq j} p_k}\right)^{\beta}$, for some $\alpha, \beta \in \mathbb{Z}_N$. Thus,

$$\begin{aligned} e(u_i, u_j) &= e\left(\left(g^{\prod_{k\in\{1,2,3\},k\neq i} p_k}\right)^{\alpha}, \left(g^{\prod_{k\in\{1,2,3\},k\neq j} p_k}\right)^{\beta}\right) \\ &= e\left(g^{\alpha \prod_{k\in\{1,2,3\},k\neq i,j} p_k}, g^{\beta}\right)^{\prod_{k\in\{1,2,3\}} p_k} \\ &= e\left(g^{\alpha \prod_{k\in\{1,2,3\},k\neq i,j} p_k}, g^{\beta}\right)^{N} = \hat{1} \end{aligned}$$

because $ord(\widehat{\mathbb{G}}) = N$. □

We can write $\mathbb{G} = \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3} = \left\{X_1 X_2 X_3 : X_i \in \mathbb{G}_{p_i}, i \in \{1, 2, 3\}\right\}$. Here, $X_i \in \mathbb{G}_{p_i}$ is referred as the "$\mathbb{G}_{p_i}$ part of $X_1 X_2 X_3$" for $i \in \{1, 2, 3\}$. For $i, j \in \{1, 2, 3\}, i \neq j$, $\mathbb{G}_{p_i} \times \mathbb{G}_{p_j} = \{K_i K_j : K_i \in \mathbb{G}_{p_i}, K_j \in \mathbb{G}_{p_j}\}$.

2.2. Complexity assumptions

We now state the complexity assumptions following [8,15] that are used to prove security of our CP-ABE scheme. These assumptions can be shown to hold in the generic group model under the assumption that finding a non-trivial factor of N is hard, as described in [19] (proof is given in the Appendix). In the following problems, we denote $\Sigma = (N, \mathbb{G}, \widehat{\mathbb{G}}, e)$, where $N = p_1p_2p_3$.

Problem 1. *Consider the following distribution*

$$\triangle_1 = \left\{ (\Sigma, g_1, g_3) : \begin{array}{r} \Sigma \leftarrow \mathcal{G}(\kappa) \\ g_1 \overset{\$}{\leftarrow} \mathbb{G}_{p_1} \\ g_3 \overset{\$}{\leftarrow} \mathbb{G}_{p_3} \end{array} \right\}$$

Given $D = (\Sigma, g_1, g_3) \overset{\$}{\leftarrow} \triangle_1$ and a random element $T \overset{\$}{\leftarrow} \mathbb{G}$, determine whether $T \in \mathbb{G}$ or $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$.
The advantage of a distinguisher $\mathfrak{D}$ in breaking hardness of Problem 1 is defined to be

$$Adv_{\mathfrak{D}}^{\text{Problem 1}} = \big|\Pr[\mathfrak{D}(\mathrm{D}, \mathrm{T}) = 1 | \mathrm{T} \in \mathbb{G}] \\ - \Pr\left[\mathfrak{D}(\mathrm{D}, \mathrm{T}) = 1 | \mathrm{T} \in \mathbb{G}_{\mathrm{p}_1} \times \mathbb{G}_{\mathrm{p}_3}\right]\big|$$

Problem 2. *Consider the following distribution*

$$\triangle_2 = \left\{ (\Sigma, g_1, X_1X_2X_3, Y_1Y_2, g_3) : \begin{array}{r} \Sigma \leftarrow \mathcal{G}(\kappa) \\ g_1, X_1, Y_1 \overset{\$}{\leftarrow} \mathbb{G}_{p_1} \\ X_2, Y_2 \overset{\$}{\leftarrow} \mathbb{G}_{p_2} \\ g_3, X_3 \overset{\$}{\leftarrow} \mathbb{G}_{p_3} \end{array} \right\}$$

Given $D = (\Sigma, g_1, X_1X_2X_3, Y_1Y_2, g_3) \overset{\$}{\leftarrow} \triangle_2$ and a random element $T \overset{\$}{\leftarrow} \mathbb{G}$,
determine whether $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2}$ or $T \in \mathbb{G}_{p_1}$.
The advantage of a distinguisher $\mathfrak{D}$ in breaking hardness of Problem 2 is defined to be

$$Adv_{\mathfrak{D}}^{\text{Problem 2}} = \big|\Pr\left[\mathfrak{D}(\mathrm{D}, \mathrm{T}) = 1 | \mathrm{T} \in \mathbb{G}_{\mathrm{p}_1} \times \mathbb{G}_{\mathrm{p}_2}\right] \\ - \Pr[\mathfrak{D}(\mathrm{D}, \mathrm{T}) = 1 | \mathrm{T} \in \mathbb{G}_{\mathrm{p}_1}]\big|.$$

Problem 3. *Consider the following distribution*

$$\triangle_3 = \left\{ (\Sigma, g_1, g_1^{\alpha}X_2, X_3, g_1^{s}Y_2Y_3, Z_2) : \begin{array}{r} \Sigma \leftarrow \mathcal{G}(\kappa) \\ \alpha, s \overset{\$}{\leftarrow} \mathbb{Z}_N \\ g_1 \overset{\$}{\leftarrow} \mathbb{G}_{p_1} \\ X_2, Y_2, Z_2 \overset{\$}{\leftarrow} \mathbb{G}_{p_2} \\ X_3, Y_3 \overset{\$}{\leftarrow} \mathbb{G}_{p_3} \end{array} \right\}.$$

Given $D = (\Sigma, g_1, g_1^{\alpha}X_2, X_3, g_1^{s}Y_2Y_3, Z_2) \overset{\$}{\leftarrow} \triangle_3$ and a random element $T \overset{\$}{\leftarrow} \widehat{\mathbb{G}}$,
determine whether $T = e(g_1, g_1)^{\alpha s}$ or a random element of $\widehat{\mathbb{G}}$.

The advantage of a distinguisher $\mathfrak{D}$ in breaking hardness of Problem 3 is defined to be

$$Adv_{\mathfrak{D}}^{\text{Problem 3}} = \big|\Pr\left[\mathfrak{D}(\mathrm{D}, \mathrm{T}) = 1 | \mathrm{T} = \mathrm{e}(\mathrm{g}_1, \mathrm{g}_1)^{\alpha s}\right] \\ - \Pr\left[\mathfrak{D}(\mathrm{D}, \mathrm{T}) = 1 | \mathrm{T} \overset{\$}{\leftarrow} \widehat{\mathbb{G}}\right]\big|$$

Problem 4. *Consider the following distribution*

$$\triangle_4 = \left\{ (\Sigma, g_1X_3, g_1^{s}Z_3, g_1X_2, Z_2, g_3) : \begin{array}{r} \Sigma \leftarrow \mathcal{G}(\kappa) \\ s \overset{\$}{\leftarrow} \mathbb{Z}_N \\ g_1 \overset{\$}{\leftarrow} \mathbb{G}_{p_1} \\ X_2, Y_2, Z_2 \overset{\$}{\leftarrow} \mathbb{G}_{p_2} \\ g_3, X_3, Y_3, Z_3 \overset{\$}{\leftarrow} \mathbb{G}_{p_3} \end{array} \right\}$$

Given $D = (\Sigma, g_1X_3, g_1^{s}Z_3, g_1X_2, Z_2, g_3) \overset{\$}{\leftarrow} \triangle_4$ and a random element $T \overset{\$}{\leftarrow} \mathbb{G}$,
determine whether $T = g_1^{s}Y_2Y_3$ or a random element of $\mathbb{G}$.
The advantage of a distinguisher $\mathfrak{D}$ in breaking hardness of Problem 4 is defined to be

$$Adv_{\mathfrak{D}}^{\text{Problem 4}} = \big|\Pr\left[\mathfrak{D}(D, T) = 1 | T = g_1^{s}Y_2Y_3\right] \\ - \Pr\left[\mathfrak{D}(D, T) = 1 | T \overset{\$}{\leftarrow} \mathbb{G}\right]\big|.$$

Definition 2 (Assumption σ). *Let $\sigma \in \{1, 2, 3, 4\}$. The problem σ is said to be $(\mathcal{T}, \epsilon_{\sigma})$-hard relative to $\Sigma = (N = p_1p_2p_3, \mathbb{G}, \widehat{\mathbb{G}}, e) \leftarrow \mathcal{G}(\kappa)$ if for all $\mathcal{T}$-time distinguishers $\mathfrak{D}$, the advantage $Adv_{\mathfrak{D}}^{\text{Problem } \sigma} \leq \epsilon_{\sigma}$.*

2.3. Ciphertext-policy ABE system

The CP-ABE is a set of four algorithms [3] wherein U is a universe of attributes used in the system. A single central authority (CA) manages all the attributes and their public, secret key pairs by executing Setup algorithm. When a user joins the system, the CA first chooses a set of suitable attributes according to her role in the system. Then, CA computes the secret key associated with the selected attribute set by running KeyGen algorithm and returns the output to the user. When encryptor wants to encrypt a message, it formulates an access policy over receivers' attributes that indicates who are eligible to view the message and executes Encrypt algorithm using public parameters along with the access policy and the message to be encrypted; the resulting ciphertext will be transmitted to the system. On receiving the ciphertext, a decryptor who has a secret key associated with an appropriate attribute set that satisfies the access policy used in the encryption process can recover the message correctly by performing Decrypt algorithm. Formally, the four algorithms are as follows:

$\Sigma_{\mathsf{CP\text{-}ABE}} = \{$	κ	: security parameter,	U	: attribute universe
$(\mathsf{PK}, \mathsf{MK}) \leftarrow \mathsf{Setup}(\kappa, U)$,	PK	: public key,	MK	: master secret key
$\mathsf{SK}_L \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MK}, L)$,	L	: set of user attributes,	SK_L	: secret key for L
$\mathsf{CT} \leftarrow \mathsf{Encrypt}(\mathsf{PK}, M, W)$,	M	: message,	W	: access policy
M or $\perp \leftarrow \mathsf{Decrypt}(\mathsf{PK}, \mathsf{CT}, \mathsf{SK_L})\}$	CT	: ciphertext,	$\perp$	: random message

Remark 2. If the encryption process does not embed the access policy explicitly in the ciphertext, the CP-ABE scheme is termed as hidden policy CP-ABE. In this case, the ciphertext is called a *policy hiding ciphertext.* In the partially hidden policy CP-ABE, the encryptor places some "information" of the access policy in the ciphertext that does not disclose the actual attribute information. In this scenario, the ciphertext is called a *partially policy hiding ciphertext.*

2.4. Recipient anonymity

Given a policy hiding ciphertext CT and an access policy W_0, if no adversary is able to determine whether CT is computed under W_0 or not, then the hidden policy CP-ABE scheme is said to provide recipient anonymity.

Note that if CT is the ciphertext of partially hidden policy CP-ABE scheme, then the access policy information included in the ciphertext must be the same for both W_0 and the access policy used to generate CT; otherwise, the adversary might trivially decide whether CT is computed under W_0 or not.

2.5. Full CPA security and anonymity

The security game described subsequently captures both full chosen plaintext attack (CPA) security and recipient anonymity for (partially) hidden policy CP-ABE schemes. This game, referred to as $\mathsf{Game}_{\mathsf{IND\text{-}CPA\text{-}ANON}}$, is equivalent to the standard security notions for full CPA security and anonymity defined in [15,16].

- **Setup.** The challenger obtains $(\mathsf{PK}, \mathsf{MK}) \leftarrow \mathsf{Setup}(\kappa, U)$ and gives public key PK to the adversary $\mathcal{A}$.
- **Key Query Phase 1.** The adversary requests secret keys corresponding to attribute sets $L_1, L_2, \ldots, L_{q_1}$. The challenger returns $\mathsf{SK}_{L_i} \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MK}, L_i)$ to $\mathcal{A}$, for $i \in [q_1]$.
- **Challenge.** The adversary submits two equal length messages M_0, M_1 and two access policies W_0, W_1. These access policies cannot be satisfied by any of the queried attribute sets $L_1, L_2, \ldots, L_{q_1}$ in phase 1. The challenger flips a random coin $\mu \overset{\$}{\leftarrow} \{0, 1\}$ and returns $\mathsf{CT}^* \leftarrow \mathsf{Encrypt}(\mathsf{PK}, M_\mu, W_\mu)$ to adversary $\mathcal{A}$.

  (In the case of partially hidden policy CP-ABE, the access policy information included in the ciphertext must be the same for both W_0 and W_1 in order to ensure that the adversary cannot trivially distinguish the ciphertexts.)
- **Key query phase 2.** The adversary requests secret keys for the attribute sets $L_{q_1+1}, L_{q_1+2}, \ldots, L_q$ with the restriction that none of these satisfies W_0 and W_1. The challenger sends $\mathsf{SK}_{L_i} \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MK}, L_i)$ to $\mathcal{A}$, for $i \in \{q_1 + 1, q_1 + 2, \ldots, q\}$.
- **Guess.** The adversary outputs a guess bit $\mu' \in \{0, 1\}$ and wins the game if $\mu' = \mu$.

The advantage of $\mathcal{A}$ in this game is defined as $Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{IND\text{-}CPA\text{-}ANON}}} = |\Pr[\mu' = \mu] - \frac{1}{2}|$.

Definition 3. *A (partially) hidden policy CP-ABE scheme is said to be fully $(\mathcal{T}, q, \epsilon)$-IND-CPA-ANON secure if for any $\mathcal{T}$-time adversary $\mathcal{A}$ who makes at most q secret key queries during simulation, the advantage $Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{IND\text{-}CPA\text{-}ANON}}} \leq \epsilon$ in the aforementioned game.*

3. ZHOU *ET AL.* [7] CP-ABE SCHEME

In this section, we first present the Zhou *et al.* [7] selectively secure CP-ABE construction and then show how the scheme fails to provide recipient anonymity.

3.1. Review of Zhou *et al.* [7] CP-ABE scheme

The CP-ABE of [7] is described in the following two algorithms Setup and $\mathsf{Encrypt}$ because the other two KeyGen and $\mathsf{Decrypt}$ algorithms are not required for further explanations.

- $\mathsf{Setup}(\kappa, U)$. The CA generates the prime order bilinear group parameters $(p, \mathbb{G}', \widehat{\mathbb{G}}', \hat{e})$ and executes the following steps, where $ord(\mathbb{G}') = ord(\widehat{\mathbb{G}}') = p$, a prime number and $\hat{e} : \mathbb{G}' \otimes \mathbb{G}' \rightarrow \widehat{\mathbb{G}}'$ is a bilinear map.
  - Choose $g \overset{\$}{\leftarrow} \mathbb{G}', \alpha \overset{\$}{\leftarrow} \mathbb{Z}_p$ and set $g_i = g^{(\alpha^i)}, \forall i \in [2K] \setminus \{K + 1\}$, where $K = 3n$ and n is the number of attribute categories in the attribute universe.

- Select $\gamma \xleftarrow{\$} \mathbb{Z}_p$ and set $v = g^{\gamma}$.

The public key is $\mathsf{PK} = \langle p, \hat{e}, g, v, g_1, g_2, \ldots, g_K, g_{K+2}, \ldots, g_{2K}, U\rangle$ and the master secret key is $\mathsf{MK} = \langle \alpha, \gamma \rangle$.

– $\mathsf{Encrypt}(\mathsf{PK}, M, W)$. Let $W = \{w_1, w_2, \ldots, w_n\}$, where $w_i \in [K]$, be an access policy. The encryptor performs as follows to encrypt a message M.

- Select $t \xleftarrow{\$} \mathbb{Z}_p$ and set the one-time symmetric encryption key as $\mathsf{k} = \hat{e}(g_K, g_1)^{nt}$.
- Encrypt the message M using the symmetric key k as $C = \mathsf{Enc}_{\mathsf{k}}(M)$, where Enc is a one-time symmetric encryption scheme.
- Compute $C_1 = g^t$ and $C_2 = (v \prod_{j\in W} g_{K+1-j})^t$.

The ciphertext associated with the access policy W is $\mathsf{CT} = \langle \overline{W}, C, C_1, C_2\rangle$, where $\overline{W}$ is some information of the access policy[‡] W.

3.2. Note on recipient anonymity

Similar to [4] (described in Section 1), Zhou *et al.* [7] CP-ABE construction cannot resist DDH-test attacks because $(g, C_1, v\prod_{j\in W} g_{K+1-j}, C_2)$ becomes DDH-tuple, that is, $\hat{e}(C_1, v\prod_{j\in W} g_{K+1-j}) = \hat{e}(g^t, v\prod_{j\in W} g_{K+1-j}) = \hat{e}(g, (v\prod_{j\in W} g_{K+1-j})^t) = \hat{e}(g, C_2)$. Precisely, on receiving Zhou *et al.* [7] ciphertext $\mathsf{CT} = \langle \overline{W}, C, C_1, C_2\rangle$ and a random access policy W' such that $\overline{W'} = \overline{W}$ (this condition is necessary as the CP-ABE in [7] is partially hidden policy construction), any third party can conduct the DDH-test as

$$\hat{e}\left(C_1, v \prod_{j'\in W'} g_{K+1-j'}\right) \stackrel{?}{=} \hat{e}(g, C_2) \qquad (1)$$

and decides whether $W' = W$ or not based on the DDH-test valid or not, respectively. Therefore, the scheme is trivially vulnerable to DDH-test attacks, thereby not recipient anonymous.

Now, we can see from the following argument that the CP-ABE [7] is not secure against $\mathsf{Game}_{\mathsf{IND\text{-}CPA\text{-}ANON}}$ game presented in Section 2.5. The adversary obtains the challenge ciphertext CT^* of M_μ under W_μ after submitting two equal length messages M_0, M_1 and two access policies W_0, W_1 satisfying $\overline{W_0} = \overline{W_1}$ to the challenger, where $\mu \xleftarrow{\$} \{0,1\}$. The ciphertext is of the form $\mathsf{CT}^* = \langle \overline{W_\mu}, C^*, C_1^*, C_2^*\rangle$. The adversary first guesses $W_\mu = W_0$ and then runs the DDH-test stated in Equation (1), namely,

$$\hat{e}\left(C_1^*, v \prod_{j\in W_0} g_{K+1-j}\right) \stackrel{?}{=} \hat{e}(g, C_2^*)$$

using public parameters $\langle g, v, \{g_{K+1-j}\}_{j\in W_0}\rangle$ and the components $\langle C_1^*, C_2^*\rangle$ of CT^*. If the test passes, $W_\mu = W_0$ and can know that M_0 is the plaintext of CT^*. Otherwise, $W_\mu = W_1$ and can conclude that M_1 is the plaintext of CT^*. This violates the IND-CPA-ANON security of partially policy hiding CP-ABE [7].

4. PROTOCOL

In this section, we first describe an *anonymized* monotone access policy, followed by our proposed recipient anonymous CP-ABE (anonCP-ABE) construction.

4.1. Anonymized monotone access policy

Let $U = \{\mathsf{Att}_1, \mathsf{Att}_2, \ldots, \mathsf{Att}_n\}$ be the universe of attribute categories in the system. Each attribute category Att_i has k_i possible attributes $\{att_{i,1}, att_{i,2}, \ldots, att_{i,k_i}\}$. The attribute $att_{i,j}$ represents the jth attribute of the ith attribute category. Each attribute category Att_i is identified with an index i in the set $[n]$ of indices. When a user u joins the system, it is assigned an attribute set L_u described as $L_u = \langle I_u, \{att_{i,\ell_i} : i \in I_u, \ell_i \in [k_i]\}\rangle$, where $I_u \subset [n]$ is the (attribute) category index list and the user attribute set L_u contains at most one attribute from a category.

An access policy W is represented as $W = \langle I_W, \{att_{i,w_i} : i \in I_W, w_i \in [k_i]\}\rangle$, where $I_W \subset [n]$ is the list of category indices of W that describes the attribute categories involved in the access policy. At most, one attribute is included in the access policy from a category.

Definition 4. *Given a set of attributes $L_u = \langle I_u, \{att_{i,\ell_i} : i \in I_u, \ell_i \in [k_i]\}\rangle$ of a user u and an access policy $W = \langle I_W, \{att_{i,w_i} : i \in I_W, w_i \in [k_i]\}\rangle$, we say that L_u satisfies W, denoted as $L_u \models W$ if and only if $I_u \supseteq I_W$, and for each $i \in I_u \bigcap I_W, \ell_i = w_i$. Otherwise L_u does not satisfy W, denoted as $L_u \not\models W$.*

Definition 5. *An anonymized access policy W_{aap} of an access policy $W = \langle I_W, \{att_{i,w_i} : i \in I_W, w_i \in [k_i]\}\rangle$ is defined as $W_{\mathsf{aap}} = I_W$. In this case, $L_u \models W_{\mathsf{aap}}$ if and only if $I_u \supseteq W_{\mathsf{aap}}$.*

Note that the anonymized access policy W_{aap} reveals only the attribute categories associated with it, but not specific attributes within the categories. Hence, W_{aap} hides fully the attributes listed in original access policy W.

4.2. Our anonCP-ABE construction

Our CP-ABE with recipient anonymity is a set of four algorithms described subsequently.

$\mathsf{Setup}(\kappa, U)$. The CA generates composite order bilinear group parameters $(p_1, p_2, p_3, \mathbb{G}, \widehat{\mathbb{G}}, e)$ by using the group generator algorithm $\mathcal{G}(\cdot)$ with the

[‡] The information $\overline{W}$ of W is embedded in the ciphertext instead of the original access policy W in order to make the actual attribute set hidden completely in the ciphertext, like the scheme we will present here. In this case, the scheme is called partially policy hiding CP-ABE.

input security parameter κ, where p_1, p_2, and p_3 are distinct primes, $\mathbb{G}$ and $\widehat{\mathbb{G}}$ are two multiplicative cyclic groups of same composite order $N = p_1p_2p_3$, and $e : \mathbb{G} \otimes \mathbb{G} \to \widehat{\mathbb{G}}$ is a bilinear map. Let $\mathbb{G}_{p_i}$ be a subgroup of $\mathbb{G}$ generated by g_i of order p_i for $i \in \{1, 3\}$. A random element $\theta \in \mathbb{G}_{p_i}$ can be sampled by choosing a random $\tau \in \mathbb{Z}_N$ and setting $\theta = g_i^{\tau}$, where g_i is a generator of $\mathbb{G}_{p_i}$ and $i \in \{1, 3\}$. Note that the subgroup $\mathbb{G}_{p_2}$ will only be used in security analysis. The CA then carries out the following steps.

- Choose $P \overset{\$}{\leftarrow} \mathbb{G}_{p_1}$ and set $\Gamma = e(g_1, P)$.
- Sample $P_1 \overset{\$}{\leftarrow} \mathbb{G}_{p_1}, R_0, R \overset{\$}{\leftarrow} \mathbb{G}_{p_3}$ and set $A_0 = g_1R_0, A = P_1R$.
- For each attribute $att_{i,j} \in U, i \in [n], j \in [k_i]$, select $a_{i,j} \overset{\$}{\leftarrow} \mathbb{Z}_N, R_{i,j} \overset{\$}{\leftarrow} \mathbb{G}_{p_3}$ and set $A_{i,j} = g_1^{a_{i,j}} R_{i,j}$.

The public key is $\mathsf{PK} = \langle N, e, \Gamma, A_0, A, g_3, \{A_{i,j}\}_{i\in[n], j\in[k_i]}, U\rangle$. The master secret key is $\mathsf{MK} = \langle g_1, P, P_1\rangle$.

$\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MK}, L_u)$. To generate a secret key for user attribute set $L_u = \langle I_u, \{att_{i,\ell_i}\}_{i\in I_u}\rangle$, the CA performs as follows.

- Pick $r \overset{\$}{\leftarrow} \mathbb{Z}_N$ and set $D_1 = PP_1^r, D_2 = g_1^r$.
- For each attribute $att_{i,\ell_i}, i \in I_u$, compute $D_{i,\ell_i} = g_1^{ra_{i,\ell_i}}$.

The secret key associated with L_u is $\mathsf{SK}_{L_u} = \langle L_u, D_1, D_2, \{D_{i,\ell_i}\}_{i\in I_u}\rangle$.

$\mathsf{Encrypt}(\mathsf{PK}, M, W)$. To encrypt a message $M \in \widehat{\mathbb{G}}$ according to the access policy $W = \langle I_W, \{att_{i,w_i}\}_{i\in I_W}\rangle$, where $I_W \subset [n]$, the encryptor executes as described subsequently.

- Sample $s, t \overset{\$}{\leftarrow} \mathbb{Z}_N, R'_0, R', R'' \overset{\$}{\leftarrow} \mathbb{G}_{p_3}$.
- Calculate $C = M\Gamma^s, C_1 = A_0^s R'_0, C_2 = A^s\Big(\prod_{i\in I_W} A_{i,w_i}\Big)^t R', C_3 = A_0^t R''$.
- Set $W_{\mathsf{aap}} = I_W$.

The ciphertext is $\mathsf{CT} = \langle W_{\mathsf{aap}}, C, C_1, C_2, C_3\rangle$. Note that the anonymized access policy W_{aap} is embedded in the ciphertext instead of the original access policy W in order to make the actual attribute set hidden completely in the ciphertext.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{CT}, \mathsf{SK}_{L_u})$. On receiving the ciphertext $\mathsf{CT} = \langle W_{\mathsf{aap}}, C, C_1, C_2, C_3\rangle$, a decryptor u with secret key $\mathsf{SK}_{L_u} = \langle L_u, D_1, D_2, \{D_{i,\ell_i}\}_{i\in I_u}\rangle$ checks whether $L_u \models W_{\mathsf{aap}}$. If not, it aborts the decryption. Otherwise, $I_u \supseteq W_{\mathsf{aap}}$. The decryptor then performs as follows.

- Collect the secret attribute key components $\{D_{i,\ell_i}\}_{i\in W_{\mathsf{aap}}}$ and calculate $D_u = \prod_{i\in W_{\mathsf{aap}}} D_{i,\ell_i}$.
- Compute $M' = \dfrac{C \cdot e(C_2, D_2)}{e(C_1, D_1) \cdot e(C_3, D_u)}$.

The decryptor obtains the correct message $M' = M$ if $\ell_i = w_i, \forall i \in W_{\mathsf{app}}$. Otherwise, M' is a random element.

In the following sections, we use the identities stated in *Remark 1* (given in Section 2.1) and the orthogonal property mentioned in Theorem 1.

4.3. Correctness

In this section, we show that if $L_u \models W_{\mathsf{aap}}$, then the decryption algorithm can correctly recover the message M.

Suppose $I_u \supseteq W_{\mathsf{aap}} = I_W$ and $\ell_i = w_i, \forall i \in W_{\mathsf{app}}$. Then,

$$\begin{aligned}
M' &= \frac{C \cdot e(C_2, D_2)}{e(C_1, D_1) \cdot e(C_3, D_u)} \\
&= \frac{M\Gamma^s \cdot e\left(A^s\left(\prod_{i\in W_{\mathsf{aap}}} A_{i,w_i}\right)^t R', g_1^r\right)}{e\left(A_0^s R'_0, PP_1^r\right) \cdot e\left(A_0^t R'', \prod_{i\in W_{\mathsf{aap}}} D_{i,\ell_i}\right)} \\
&= \frac{M\Gamma^s \cdot e\left((P_1R)^s\left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,w_i}} R_{i,w_i}\right)^t R', g_1^r\right)}{e\left((g_1R_0)^s R'_0, PP_1^r\right) \cdot e\left((g_1R_0)^t R'', \prod_{i\in W_{\mathsf{aap}}} g_1^{ra_{i,\ell_i}}\right)} \\
&= \frac{M\Gamma^s \cdot e\left(P_1^s \cdot \left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,w_i}}\right)^t \cdot R^s\left(\prod_{i\in W_{\mathsf{aap}}} R_{i,w_i}\right)^t R', g_1^r\right)}{e\left(g_1^s \cdot \left(R_0^s R'_0\right), PP_1^r\right) \cdot e\left(g_1^t \cdot (R_0^t R''), \left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}}\right)^r\right)} \\
&= \frac{M\Gamma^s \cdot e\left(P_1^s, g_1^r\right) \cdot e\left(\left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,w_i}}\right)^t, g_1^r\right) \cdot e\left(R^s\left(\prod_{i\in W_{\mathsf{aap}}} R_{i,w_i}\right)^t R', g_1^r\right)}{e\left(g_1^s, PP_1^r\right) \cdot e\left(R_0^s R'_0, PP_1^r\right) \cdot e\left(g_1^t, \left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}}\right)^r\right) \cdot e\left(R_0^t R'', \left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}}\right)^r\right)}
\end{aligned}$$

Because $\ell_i = w_i, \forall i \in W_{\mathsf{app}}$ and hence $a_{i,\ell_i} = a_{i,w_i}, \forall i \in W_{\mathsf{app}}$, we have

$$e\left(\left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,w_i}}\right)^t, g_1^r\right) = e\left(\left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}}\right)^t, g_1^r\right)$$
$$= e\left(\left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}}\right), g_1\right)^{tr} = e\left(g_1, \left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}}\right)\right)^{tr}$$
$$= e\left(g_1^t, \left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}}\right)^r\right)$$

By the orthogonal property of the subgroups $\mathbb{G}_{p_1}$ and $\mathbb{G}_{p_3}$, we have

$$e\left(R^s\left(\prod_{i\in W_{\mathsf{aap}}} R_{i,w_i}\right)^t R', g_1^r\right) = e\left(R_0^s R_0', PP_1^r\right)$$
$$= e\left(R_0^t R'', \left(\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}}\right)^r\right) = \hat{1}$$

because $R^s(\prod_{i\in W_{\mathsf{aap}}} R_{i,w_i})^t R', R_0^s R_0', R_0^t R'' \in \mathbb{G}_{p_3}$ and $g_1^r, PP_1^r, (\prod_{i\in W_{\mathsf{aap}}} g_1^{a_{i,\ell_i}})^r \in \mathbb{G}_{p_1}$.
Thus,

$$M' = \frac{M\Gamma^s \cdot e\left(P_1^s, g_1^r\right)}{e\left(g_1^s, PP_1^r\right)} = \frac{M\Gamma^s \cdot e\left(P_1^s, g_1^r\right)}{e\left(g_1^s, P\right)\cdot e(g_1^s, P_1^r)}$$

Because $e(P_1^s, g_1^r) = e(P_1, g_1)^{sr} = e(g_1, P_1)^{sr} = e(g_1^s, P_1^r)$, we have

$$M' = \frac{M\Gamma^s}{e(g_1^s, P)} = \frac{M\Gamma^s}{e(g_1, P)^s} = \frac{M\Gamma^s}{\Gamma^s} = M$$

4.4. Note on recipient anonymity

We now illustrate the recipient anonymity of our proposed construction. The formal security analysis is provided in the next section.

Suppose an adversary is given an access policy $W' = \langle W'_{\mathsf{aap}} = I_{W'}, \{att_{i,w'_i} : i \in I_{W'}, w'_i \in [k_i]\}\rangle$ and a ciphertext $\mathsf{CT} = \langle W_{\mathsf{aap}}, C, C_1, C_2, C_3\rangle$ such that $W_{\mathsf{aap}} = W'_{\mathsf{aap}}$.

The DDH-like test in this case is

$$e\left(C_3, \prod_{i\in I_{W'}} A_{i,w'_i}\right)\cdot e(C_1, A) \overset{?}{=} e(A_0, C_2) \qquad (2)$$

This can also be represented as

$$\frac{e\left(C_3, \prod_{i\in I_{W'}} A_{i,w'_i}\right)\cdot e(C_1, A)}{e(A_0, C_2)} \overset{?}{=} \hat{1}$$

Suppose the given ciphertext $\mathsf{CT} = \langle W_{\mathsf{aap}}, C, C_1, C_2, C_3\rangle$ is computed under the access policy $W = \langle W_{\mathsf{aap}} = I_W, \{att_{i,w_i} : i \in I_W, w_i \in [k_i]\}\rangle$ (note that W is not known to the adversary). We have $I_{W'} = I_W$. Then

$$\Theta = \frac{e\left(C_3, \prod_{i\in I_{W'}} A_{i,w'_i}\right)\cdot e(C_1, A)}{e(A_0, C_2)}$$
$$= \frac{e\left(A_0^t R'', \prod_{i\in I_{W'}} A_{i,w'_i}\right)\cdot e(A_0^s R_0', A)}{e\left(A_0, A^s(\prod_{i\in I_{W'}} A_{i,w_i})^t R'\right)}$$
$$= \frac{e\left(A_0^t, \prod_{i\in I_{W'}} A_{i,w'_i}\right)\cdot e\left(R'', \prod_{i\in I_{W'}} A_{i,w'_i}\right)\cdot e(A_0^s, A)\cdot e(R_0', A)}{e(A_0, A^s)\cdot e\left(A_0, (\prod_{i\in I_{W'}} A_{i,w_i})^t\right)\cdot e(A_0, R')}$$
$$= \frac{e\left(A_0, \prod_{i\in I_{W'}} A_{i,w'_i}\right)^t\cdot e\left(R'', \prod_{i\in I_{W'}} g_1^{a_{i,w'_i}} R_{i,w'_i}\right)\cdot e(A_0, A)^s\cdot e(R_0', P_1 R)}{e(A_0, A)^s\cdot e\left(A_0, \prod_{i\in I_{W'}} A_{i,w_i}\right)^t\cdot e(g_1 R_0, R')}$$
$$= \frac{e\left(A_0, \prod_{i\in I_{W'}} A_{i,w'_i}\right)^t\cdot e\left(R'', \prod_{i\in I_{W'}} g_1^{a_{i,w'_i}}\right)\cdot e\left(R'', \prod_{i\in I_{W'}} R_{i,w'_i}\right)\cdot e(R_0', P_1)\cdot e(R_0', R)}{e\left(A_0, \prod_{i\in I_{W'}} A_{i,w_i}\right)^t\cdot e(g_1, R')\cdot e(R_0, R')}$$
$$= \frac{e\left(A_0, \prod_{i\in I_{W'}} A_{i,w'_i}\right)^t\cdot e\left(R'', \prod_{i\in I_{W'}} R_{i,w'_i}\right)\cdot e(R_0', R)}{e\left(A_0, \prod_{i\in I_{W'}} A_{i,w_i}\right)^t\cdot e(R_0, R')}$$

because some pairings in both numerator and denominator of Θ become identity in $\widehat{\mathbb{G}}$ due to the orthogonal property. Now, there are two possible cases.

- If $W' = W$, then $w'_i = w_i, \forall i \in I_{W'}$. Hence, $A_{i,w'_i} = A_{i,w_i}, \forall i \in I_{W'}$. Therefore, $e\left(A_0, \prod_{i \in I_{W'}} A_{i,w'_i}\right)^t = e\left(A_0, \prod_{i \in I_{W'}} A_{i,w_i}\right)^t$. In this case,

$$\Theta = \frac{e\left(R'', \prod_{i \in I_{W'}} R_{i,w'_i}\right) \cdot e(R'_0, R)}{e(R_0, R')}$$

- Suppose $W' \neq W$. Then there exists at least one $i' \in I_{W'}$ such that $w'_{i'} \neq w_{i'}$. Without loss of generality, assume that $w'_i = w_i, \forall i \in I_{W'} \setminus \{i'\}$. In this case, $A_{i,w'_i} = A_{i,w_i}, \forall i \in I_{W'} \setminus \{i'\}$. Hence, $e\left(A_0, \prod_{i \in I_{W'} \setminus \{i'\}} A_{i,w'_i}\right)^t = e\left(A_0, \prod_{i \in I_{W'} \setminus \{i'\}} A_{i,w_i}\right)^t$. Therefore,

$$\Theta = \frac{e\left(A_0, \prod_{i \in I_{W'} \setminus \{i'\}} A_{i,w'_i}\right)^t \cdot e\left(A_0, A_{i',w'_{i'}}\right)^t \cdot e\left(R'', \prod_{i \in I_{W'}} R_{i,w'_i}\right) \cdot e(R'_0, R)}{e\left(A_0, \prod_{i \in I_{W'} \setminus \{i'\}} A_{i,w_i}\right)^t \cdot e\left(A_0, A_{i',w_{i'}}\right)^t \cdot e(R_0, R')}$$
$$= \frac{e\left(A_0, A_{i',w'_{i'}}\right)^t \cdot e\left(R'', \prod_{i \in I_{W'}} R_{i,w'_i}\right) \cdot e(R'_0, R)}{e\left(A_0, A_{i',w_{i'}}\right)^t \cdot e(R_0, R')}$$

In both the cases, Θ becomes a random element in $\widehat{\mathbb{G}}$, thereby Equation (2) is never valid. Consequently, no one can determine whether $W' = W$, that is, whether the ciphertext CT is encrypted under the given access policy W' or not. Thus, our construction *preserves* recipient anonymity.

Note that no one can obtain the original access policy of a given ciphertext by performing DDH-like tests with all possible access policies because the tests fail always unconditionally. Hence, even exhaustive DDH-like tests cannot identify the actual access policy used in the ciphertext. Therefore, our construction provides perfect recipient anonymity.

5. PROOF OF SECURITY

We use the dual-system proof analogous to [19] that requires *semi-functional* secret keys and ciphertexts in addition to *normal* secret keys and ciphertexts[§]. Let us provide SF-KeyGen and SF-Encrypt algorithms that create semi-functional secret keys and ciphertexts, respectively. These algorithms use the subgroup $\mathbb{G}_{p_2}$. Let g_2 be a generator of $\mathbb{G}_{p_2}$.

SF-KeyGen. A semi-functional secret key for the user attribute set $L_u = \langle I_u, \{att_{i,\ell_i}\}_{i \in I_u} \rangle$ is generated as follows.

- Generate normal secret key

$$\mathsf{SK}_{L_u} = \left\langle L_u, D_1 = PP_1^r, D_2 = g_1^r, \left\{ D_{i,\ell_i} = g_1^{ra_{i,\ell_i}} \right\}_{i \in I_u} \right\rangle \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MK}, L_u)$$

for L_u, where $D_1, D_2, D_{i,\ell_i} \in \mathbb{G}_{p_1}, \forall i \in I_u$.

- Sample $\gamma_1, \gamma_2, z_{i,\ell_i} \xleftarrow{\$} \mathbb{Z}_N, \forall i \in I_u$.
- Compute

$$D'_1 = D_1 \cdot g_2^{\gamma_1} = PP_1^r \cdot g_2^{\gamma_1} \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2},$$
$$D'_2 = D_2 \cdot g_2^{\gamma_2} = g_1^r \cdot g_2^{\gamma_2} \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2},$$
$$D'_{i,\ell_i} = D_{i,\ell_i} \cdot g_2^{z_{i,\ell_i}} = g_1^{ra_{i,\ell_i}} \cdot g_2^{z_{i,\ell_i}} \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2}, \forall i \in I_u$$

The semi-functional secret key associated with L_u is $\mathsf{SK}'_{L_u} = \langle L_u, D'_1, D'_2, \{D'_{i,\ell_i}\}_{i \in I_u} \rangle$.

SF-Encrypt. Let $W = \langle I_W, \{att_{i,w_i}\}_{i \in I_W} \rangle$ be the access policy for which a semi-functional ciphertext is created as described subsequently.

- Obtain normal ciphertext

$$\mathsf{CT} = \left\langle W_{\mathsf{aap}} = I_W, C_1 = A_0^s R'_0, C_2 = A^s \left(\prod_{i \in I_W} A_{i,w_i} \right)^t R', C_3 = A_0^t R'' \right\rangle \leftarrow \mathsf{Encrypt}(\mathsf{PK}, M, W)$$

for W, where $C \in \widehat{\mathbb{G}}$ and $C_1, C_2, C_3 \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$.

- Select $\delta_1, \delta_2 \xleftarrow{\$} \mathbb{Z}_N$.
- Compute

[§] The secret keys and ciphertexts obtained from KeyGen and Encrypt algorithms, respectively.

$$\begin{aligned} C' &= C = M\Gamma^s \in \widehat{\mathbb{G}}, \\ C'_1 &= C_1 \cdot g_2^{\delta_1} = A_0^s R'_0 \cdot g_2^{\delta_1} \in \mathbb{G}, \\ C'_2 &= C_2 \cdot g_2^{\delta_2} = A^s \left(\prod_{i \in I_W} A_{i,w_i} \right)^t R' \cdot g_2^{\delta_2} \in \mathbb{G}, \\ C'_3 &= C_3 = A_0^t R'' \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3} \end{aligned}$$

The semi-functional ciphertext corresponding to W is $\mathsf{CT}' = \langle W_{\mathsf{aap}}, C', C'_1, C'_2, C'_3 \rangle$.

The normal secret key can decrypt both normal and semi-functional ciphertexts, whereas the semi-functional secret key can only decrypt normal ciphertext. If a legitimate semi-functional secret key tries to decrypt a semi-functional ciphertext, the z_{i,ℓ_i} terms will always be canceled due to the orthogonal property. But, the decryption algorithm computes the message multiplied by an extra term $e(g_2, g_2)^{\delta_2\gamma_2 - \delta_1\gamma_1}$. However, if $\delta_2\gamma_2 = \delta_1\gamma_1$ modulo p_2, the decryption will be succeeded. In this case, the secret key is *nominally* semi-functional.

Theorem 2. *Our anonCP-ABE scheme is fully $(\mathcal{T}, q, \epsilon)$-IND-CPA-ANON secure, assuming that Problem σ is $(\mathcal{T}', \epsilon_\sigma)$-hard for all $\sigma \in \{1, 2, 3, 4\}$, where $\epsilon = \epsilon_1 + q\epsilon_2 + \epsilon_3 + \epsilon_4$ and $\mathcal{T}' = \mathcal{T} + O(n \cdot k') \cdot \mathcal{T}_{exp} + O(q)\cdot \mathcal{T}_{pair}$. Here $k' = max\{q, k_1, k_2, \ldots, k_n\}$, $k_i = |\mathsf{Att}_i|$, $\mathcal{T}_{exp}$ denotes the maximum running time of one exponentiation in $\mathbb{G}$ and $\mathcal{T}_{pair}$ denotes the running time of one pairing computation in $\widehat{\mathbb{G}}$.*

Proof. We prove security of our anonCP-ABE scheme using dual-system encryption framework. Following [16], we employ a hybrid argument over a sequence of security games between a distinguisher $\mathfrak{D}$ and an adversary $\mathcal{A}$. First, the normal challenge ciphertext is transformed into semi-functional and then the decryption keys are changed from normal to semi-functional one by one in the successive games. In the final game, the adversary can obtain only semi-functional decryption keys which are of no use for decrypting the semi-functional ciphertext, and hence, advantage of adversary in this game is 0. In this way, the security can be realized. Let q be the number of adversary's secret decryption key queries during simulation. The sequence of $q + 4$ games are defined as follows.

$\mathsf{Game}_{\mathsf{Real}}$: same as $\mathsf{Game}_{\mathsf{IND\text{-}CPA\text{-}ANON}}$ game wherein all secret keys and challenge ciphertext are normal.

Game_0 : all secret keys are normal, but challenge ciphertext is semi-functional.

$\mathsf{Game}_k (k \in [q])$: challenge ciphertext is semi-functional; the first k secret keys are semi-functional and the rest are normal.

$\mathsf{Game}_{\mathsf{Final}'}$: all secret keys are semi-functional; challenge ciphertext is a semi-functional encryption of a random element in $\widehat{\mathbb{G}}$ that is independent of the two messages provided by the adversary.

$\mathsf{Game}_{\mathsf{Final}}$: same as $\mathsf{Game}_{\mathsf{Final}'}$ except that in challenge ciphertext, C'_2 is chosen at random from$\mathbb{G}$ and hence the challenge ciphertext is independent of the ciphertext-policies submitted by the adversary. Thus, this game information theoretically hides the distinguisher's uniform random choice of one of the two messages as well as one of the two access policies given by $\mathcal{A}$, and hence, $\mathcal{A}$'s advantage in this game is 0.

Let $Adv_{\mathcal{A}}^{\mathsf{Game}_\square}$ be the advantage of $\mathcal{A}$ in $\mathsf{Game}_\square$, where $\square \in \{\mathsf{Real}, 0, 1, \ldots, q, \mathsf{Final}', \mathsf{Final}\}$. We have $Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}} = 0$.

A sequence of the following lemmas provides the following results.

- $|Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Real}}} - Adv_{\mathcal{A}}^{\mathsf{Game}_0}| \leq \epsilon_1$.
- For $k \in [q]$, $|Adv_{\mathcal{A}}^{\mathsf{Game}_{k-1}} - Adv_{\mathcal{A}}^{\mathsf{Game}_k}| \leq \epsilon_2$.
- $|Adv_{\mathcal{A}}^{\mathsf{Game}_q} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}}| \leq \epsilon_3$.
- $|Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}}| \leq \epsilon_4$.

Thus,

$$\begin{aligned} Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{IND\text{-}CPA\text{-}ANON}}} &= \left| Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Real}}} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}} \right| \\ &\leq \left| Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Real}}} - Adv_{\mathcal{A}}^{\mathsf{Game}_0} \right| \\ &\quad + \sum_{k \in [q]} \left| Adv_{\mathcal{A}}^{\mathsf{Game}_{k-1}} - Adv_{\mathcal{A}}^{\mathsf{Game}_k} \right| \\ &\quad + \left| Adv_{\mathcal{A}}^{\mathsf{Game}_q} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}} \right| \\ &\quad + \left| Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}} \right| \\ &\leq \epsilon_1 + q\epsilon_2 + \epsilon_3 + \epsilon_4 = \epsilon \end{aligned}$$

This proves the theorem. □

Lemma 1. $|Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Real}}} - Adv_{\mathcal{A}}^{\mathsf{Game}_0}| \leq \epsilon_1$.

Proof. The distinguisher $\mathfrak{D}$ receives $\langle D = (\Sigma, g_1, g_3), T \rangle$, where either $T \in \mathbb{G}$ or $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$. It then simulates $\mathsf{Game}_{\mathsf{Real}}$ if $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$ and Game_0 if $T \in \mathbb{G}$ and interacts with $\mathcal{A}$ to solve Problem 1 as follows.

Setup. To compute the public key PK, the distinguisher $\mathfrak{D}$ picks $\alpha, b \xleftarrow{\$} \mathbb{Z}_N$ and sets $P = g_1^\alpha, P_1 = g_1^b$ and $\Gamma = e(g_1, g_1)^\alpha$. It then chooses $R_0, R \xleftarrow{\$} \mathbb{G}_{p_3}$ and computes $A_0 = g_1 R_0$ and $A = P_1 R$. For each attribute $att_{i,j} \in U, i \in [n], j \in [k_i]$, sample $a_{i,j} \xleftarrow{\$} \mathbb{Z}_N$, $R_{i,j} \xleftarrow{\$} \mathbb{G}_{p_3}$ and set $A_{i,j} = g_1^{a_{i,j}} R_{i,j}$. The public key

$\mathsf{PK} = \langle N, e, \Gamma, A_0, A, g_3, \{A_{i,j}\}_{i\in[n],j\in[k_i]}, U\rangle$ is given to $\mathcal{A}$ and the master secret key $\mathsf{MK} = \langle g_1, \alpha, b\rangle$ is kept secret.

Key query phase. For both the games, all secret keys are normal. Because $\mathfrak{D}$ has the knowledge of master secret key MK, it can compute normal secret keys in response to $\mathcal{A}$'s secret key queries by running KeyGen algorithm.

Challenge. The adversary $\mathcal{A}$ outputs two equal length messages $M_0, M_1 \in \widehat{\mathbb{G}}$ and two access policies W_0, W_1. Note that the attribute index sets I_{W_0} and I_{W_1} are same in two access policies provided by the adversary. The distinguisher $\mathfrak{D}$ implicitly defines g_1^s to be the $\mathbb{G}_{p_1}$ part of T and selects $t, d, d', d'' \xleftarrow{\$} \mathbb{Z}_N$. It then flips a random coin $\mu \in \{0,1\}$. Let $W_\mu = \langle I_{W_\mu}, \{att_{i,w_i}\}_{i\in I_{W_\mu}}\rangle$, where $I_{W_\mu} \subset [n]$. Now, compute

$$C' = M_\mu \cdot e(g_1^\alpha, T), C_1' = Tg_3^d, C_2' = T^b\left(\prod_{i\in I_{W_\mu}} A_{i,w_i}\right)^t g_3^{d'}, C_3' = A_0^t g_3^{d''}$$

and send the challenge ciphertext $\mathsf{CT}^* = \langle I_{W_\mu}, C', C_1', C_2', C_3'\rangle$ to the adversary.

Guess. The adversary $\mathcal{A}$ outputs its guess $\mu' \in \{0,1\}$.

The distinguisher $\mathfrak{D}$ outputs 1 if $\mu = \mu'$, otherwise it returns 0.

If $T \in \mathbb{G}$, then T can be written as $T = g_1^s g_2^{\delta_1} X_3$, for some $\delta_1 \in \mathbb{Z}_N, X_3 \in \mathbb{G}_{p_3}$. In this case, $C' = M_\mu \cdot e(g_1^\alpha, g_1^s) = M_\mu \Gamma^s$, $C_1' = A_0^s R_0' \cdot g_2^{\delta_1}$, $C_2' = A^s(\prod_{i\in I_{W_\mu}} A_{i,w_i})^t R' \cdot g_2^{b\delta_1}$ and $C_3' = A_0^t R''$, where implicitly set $R_0^s R_0' = X_3 g_3^d, R_1^s R' = X_3^b g_3^{d'}, R'' = g_3^{d''}$ and $\delta_2 = b\delta_1$. For $\rho \in \mathbb{Z}_N$, the values ρ modulo p_i and ρ modulo p_j $(i \neq j)$ are uncorrelated from the Chinese Remainder Theorem. Hence, the challenge ciphertext CT^* is properly distributed semi-functional ciphertext and hence $\mathfrak{D}$ will simulate the game Game_0. Similarly, if $T(= g_1^s X_3) \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$, the challenge ciphertext has the same distribution as in $\mathsf{Game}_{\mathsf{Real}}$. Thus,

$$\begin{aligned} Adv_{\mathfrak{D}}^{\mathsf{Problem\ 1}} &= \big|\mathrm{Pr}[\mathfrak{D}(\mathrm{D},\mathrm{T}) = 1|\mathrm{T} \in \mathbb{G}_{\mathrm{p}_1} \times \mathbb{G}_{\mathrm{p}_3}] \\ &\quad -\mathrm{Pr}[\mathfrak{D}(\mathrm{D},\mathrm{T}) = 1|\mathrm{T} \in \mathbb{G}]\big| \\ &= \big|\Pr[\mu = \mu'|T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}] \\ &\quad -\Pr[\mu = \mu'|T \in \mathbb{G}]\big| \\ &= \left|Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Real}}} - Adv_{\mathcal{A}}^{\mathsf{Game}_0}\right| \end{aligned}$$

Because $Adv_{\mathfrak{D}}^{\mathsf{Problem\ 1}} \le \epsilon_1$, we have $|Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Real}}} - Adv_{\mathcal{A}}^{\mathsf{Game}_0}| \le \epsilon_1$. □

Lemma 2. *For $k \in [q]$, $|Adv_{\mathcal{A}}^{\mathsf{Game}_{k-1}} - Adv_{\mathcal{A}}^{\mathsf{Game}_k}| \le \epsilon_2$*

Proof. We show the distinguisher $\mathfrak{D}$ takes as input $\langle D = (\Sigma, g_1, X_1X_2X_3, Y_1Y_2, g_3), T\rangle$ and interacts with $\mathcal{A}$ to decide whether $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2}$ or $T \in \mathbb{G}_{p_1}$ as follows.

Setup. To compute the public key PK, the distinguisher $\mathfrak{D}$ picks $\alpha, b \xleftarrow{\$} \mathbb{Z}_N$ and sets $P = g_1^\alpha, P_1 = g_1^b$ and $\Gamma = e(g_1, g_1)^\alpha$. It then chooses $R_0, R \xleftarrow{\$} \mathbb{G}_{p_3}$ and computes $A_0 = g_1R_0$ and $A = P_1R$. For each attribute $att_{i,j} \in U, i \in [n], j \in [k_i]$, sample $a_{i,j} \xleftarrow{\$} \mathbb{Z}_N$, $R_{i,j} \xleftarrow{\$} \mathbb{G}_{p_3}$ and set $A_{i,j} = g_1^{a_{i,j}} R_{i,j}$. The public key $\mathsf{PK} = \langle N, e, \Gamma, A_0, A, g_3, \{A_{i,j}\}_{i\in[n],j\in[k_i]}, U\rangle$ is given to $\mathcal{A}$ and the master secret key $\mathsf{MK} = \langle g_1, \alpha, b\rangle$ is kept secret.

Key query phase. For both the games, the first $k-1$ secret keys are semi-functional and the last $q-k$ keys are normal. For Game_{k-1}, the kth secret key is normal, whereas for Game_k, it is semi-functional. So $\mathfrak{D}$ considers three cases to answer secret key queries for user attribute sets $L_u = \langle I_u, \{att_{i,\ell_i}\}_{i\in I_u}\rangle$, where $I_u \subset [n]$.

Case 1: To generate first $k-1$ semi-functional secret keys, $\mathfrak{D}$ samples $\beta \xleftarrow{\$} \mathbb{Z}_N$ and computes

$$D_1' = g_1^\alpha (Y_1Y_2)^{b\beta}, D_2' = (Y_1Y_2)^\beta,$$
$$D_{i,\ell_i} = (Y_1Y_2)^{\beta a_{i,\ell_i}}, \forall i \in I_u.$$

Let $Y_1Y_2 = g_1^{y_1} g_2^{y_2}$, for some $y_1, y_2 \in \mathbb{Z}_N$. Then $D_1' = g_1^\alpha (g_1^b)^{y_1\beta}(g_2)^{y_2b\beta}, D_2' = g_1^{y_1\beta} g_2^{y_2\beta}$. In this case, $D_1' = PP_1^r \cdot g_2^{\gamma_1}, D_2' = g_1^r \cdot g_2^{\gamma_2}$, $D_{i,\ell_i}' = g_1^{ra_{i,\ell_i}} \cdot g_2^{z_{i,\ell_i}}$ by implicitly setting $r = y_1\beta, \gamma_1 = y_2b\beta, \gamma_2 = y_2\beta, z_{i,\ell_i} = \gamma_2 \cdot a_{i,\ell_i}$. Hence, these are properly distributed semi-functional secret keys because of the fact that the values ρ modulo p_i and ρ modulo p_j are uncorrelated for $i \neq j$, by Chinese Remainder Theorem.

Case 2: $\mathfrak{D}$ generates the last $q-k$ normal secret keys by running KeyGen algorithm because $\mathfrak{D}$ has the master secret key MK.

Case 3: To compute kth secret key, $\mathfrak{D}$ uses T and computes

$$D_1' = g_1^\alpha T^b, D_2' = T, D_{i,\ell_i}' = T^{a_{i,\ell_i}}, \forall i \in I_u$$

Suppose $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2}$. Let $T = g_1^r g_2^{\gamma_2}$, for some $r, \gamma_2 \in \mathbb{Z}_N$. Then $D_1' = PP_1^r \cdot g_2^{\gamma_1}, D_2' = g_1^r \cdot g_2^{\gamma_2}$, $D_{i,\ell_i}' = g_1^{ra_{i,\ell_i}} \cdot g_2^{z_{i,\ell_i}}$ with $\gamma_1 = b\gamma_2, z_{i,\ell_i} = \gamma_2 \cdot a_{i,\ell_i}$, and hence, it is a semi-functional secret key. On the other hand, if $T \in \mathbb{G}_{p_1}$, then this is a normal secret key.

Challenge. For both the games, the challenge ciphertext is semi-functional. On receiving two equal length messages $M_0, M_1 \in \widehat{\mathbb{G}}$ and two access policies W_0, W_1 with the same attribute index set $I_{W_0} = I_{W_1}$ from the adversary, the distinguisher $\mathfrak{D}$ implicitly sets g_1^s to be the $\mathbb{G}_{p_1}$ part of $X_1X_2X_3$ and chooses $t, d, d', d'' \stackrel{\$}{\leftarrow} \mathbb{Z}_N$. It then flips a random coin $\mu \in \{0,1\}$. Let $W_\mu = \langle I_{W_\mu}, \{att_{i,w_i}\}_{i \in I_{W_\mu}}\rangle$, where $I_{W_\mu} \subset [n]$. Now, compute

$$C' = M_\mu \cdot e(g_1^\alpha, g_1^s X_2 X_3), C_1' = g_1^s X_2 X_3 g_3^d, C_2' = (g_1^s X_2 X_3)^b \left(\prod_{i \in I_{W_\mu}} A_{i,w_i}\right)^t g_3^{d'}, C_3' = A_0^t g_3^{d''}$$

If $T = g_1^s g_2^{\delta_1} X_3$, for some $\delta_1 \in \mathbb{Z}_N$, then $C' = M_\mu \cdot e(g_1^\alpha, g_1^s) = M_\mu \Gamma^s$, $C_1' = A_0^s R_0' \cdot g_2^{\delta_1}$, $C_2' = A^s \left(\prod_{i \in I_{W_\mu}} A_{i,w_i}\right)^t R' \cdot g_2^{b\delta_1}$ and $C_3' = A_0^t R''$, by implicitly setting $R_0^s R_0' = X_3 g_3^d, R^s R' = X_3^b g_3^{d'}, R'' = g_3^{d''}$ and $\delta_2 = b\delta_1$. The ciphertext $\mathsf{CT}^* = \langle I_{W_\mu}, C', C_1', C_2', C_3'\rangle$ is sent to the adversary $\mathcal{A}$.

Guess. The adversary $\mathcal{A}$ returns its guess $\mu' \in \{0,1\}$.

The distinguisher $\mathfrak{D}$ outputs 1 if $\mu = \mu'$, otherwise, it returns 0.

The kth semi-functional secret key and the semi-functional ciphertext are properly distributed. However, if a legitimate semi-functional secret key attempts to decrypt the semi-functional ciphertext, the correct message will be recovered because of the fact that $\delta_2\gamma_2 - \delta_1\gamma_1 = b\delta_1\gamma_2 - \delta_1 b\gamma_2 = 0$ modulo p_2 and hence the additional term $e(g_2, g_2)^{\delta_2\gamma_2 - \delta_1\gamma_1} = \hat{1}$. But the adversary is *not* issued any secret key capable of decrypting the challenge ciphertext. Therefore, if $T \in \mathbb{G}_{p_1}$, then $\mathfrak{D}$ simulates Game_{k-1} and if $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2}$, then $\mathfrak{D}$ simulates Game_k. Note that $\mathfrak{D}$ can generate the kth secret key as either normal or semi-functional, and hence, if it attempts to decrypt the semi-functional ciphertext, the decryption will be successful unconditionally in both the cases. Consequently, $\mathfrak{D}$ cannot by itself decide whether the kth key is normal or semi-functional by simply decrypting the semi-functional ciphertext. Hence, $\mathfrak{D}$ has to use the output of $\mathcal{A}$ to solve Problem 2. Thus,

$$\begin{aligned} Adv_{\mathfrak{D}}^{\mathsf{Problem\ 2}} &= \big|\Pr[\mathfrak{D}(\mathrm{D},\mathrm{T}) = 1|\mathrm{T} \in \mathbb{G}_{\mathrm{p}_1}] \\ &\quad - \Pr[\mathfrak{D}(D,T) = 1|T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2}]\big| \\ &= \big|\Pr[\mu = \mu'|T \in \mathbb{G}_{p_1}] \\ &\quad - \Pr[\mu = \mu'|T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2}]\big| \\ &= \left|Adv_{\mathcal{A}}^{\mathsf{Game}_{k-1}} - Adv_{\mathcal{A}}^{\mathsf{Game}_k}\right| \end{aligned}$$

Because $Adv_{\mathfrak{D}}^{\mathsf{Problem\ 2}} \leq \epsilon_2$, we have $|Adv_{\mathcal{A}}^{\mathsf{Game}_{k-1}} - Adv_{\mathcal{A}}^{\mathsf{Game}_k}| \leq \epsilon_2$.

□

Lemma 3. $\left|Adv_{\mathcal{A}}^{\mathsf{Game}_q} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}}\right| \leq \epsilon_3$.

Proof. We show $\mathfrak{D}$ takes the challenge $\langle D = (\Sigma, g_1, g_1^\alpha X_2, X_3, g_1^s Y_2 Y_3, Z_2), T\rangle$ of Problem 3 and interacts with $\mathcal{A}$ to decide whether $T = e(g_1, g_1)^{\alpha s}$ or T is a random element of $\widehat{\mathbb{G}}$.

Setup. The distinguisher $\mathfrak{D}$ generates the public key PK as follows: set $\Gamma = e(g_1, g_1^\alpha X_2)$, and choose $b \stackrel{\$}{\leftarrow} \mathbb{Z}_N, R_0, R \stackrel{\$}{\leftarrow} \mathbb{G}_{p_3}$ and set $P_1 = g_1^b, A_0 = g_1 R_0, A = P_1 R$. For each attribute $att_{i,j} \in U, i \in [n], j \in [k_i]$, sample $a_{i,j} \stackrel{\$}{\leftarrow} \mathbb{Z}_N$, $R_{i,j} \stackrel{\$}{\leftarrow} \mathbb{G}_{p_3}$ and set $A_{i,j} = g_1^{a_{i,j}} R_{i,j}$. Now, the distinguisher $\mathfrak{D}$ starts interaction with $\mathcal{A}$ by sending the public key $\mathsf{PK} = \langle N, e, \Gamma, A_0, A, X_3, \{A_{i,j}\}_{i \in [n], j \in [k_i]}, U\rangle$ to the adversary $\mathcal{A}$.

Key query phase. For both the games, all secret keys are semi-functional. So $\mathfrak{D}$ answers secret key queries for user attribute sets $L_u = \langle I_u, \{att_{i,\ell_i}\}_{i \in I_u}\rangle$, where $I_u \subset [n]$, as follows. Sample $r \stackrel{\$}{\leftarrow} \mathbb{Z}_N$ and compute

$$D_1' = g_1^\alpha X_2 \left(g_1^b\right)^r Z_2^r, D_2' = g_1^r Z_2, D_{i,\ell_i}' = g_1^{r \cdot a_{i,\ell_i}} Z_2^{a_{i,\ell_i}}, \forall i \in I_u.$$

Let $X_2 = g_2^x, Z_2 = g_2^{\gamma_2}$, for some $x, \gamma_2 \in \mathbb{Z}_N$. Then, it is easy to check that this is properly distributed semi-functional secret key by implicitly setting $\gamma_1 = x + r\gamma_2$ and $z_{i,\ell_i} = \gamma_2 \cdot a_{i,\ell_i}$.

Challenge. The adversary $\mathcal{A}$ sends $\mathfrak{D}$ two equal length messages $M_0, M_1 \in \widehat{\mathbb{G}}$ and two access policies W_0, W_1 with the same attribute index set $I_{W_0} = I_{W_1}$. The distinguisher picks $t, d, d', d'' \stackrel{\$}{\leftarrow} \mathbb{Z}_N$ and flips a random coin $\mu \in \{0,1\}$. Let $W_\mu = \langle I_{W_\mu}, \{att_{i,w_i}\}_{i \in I_{W_\mu}}\rangle$, where $I_{W_\mu} \subset [n]$. To form challenge ciphertext, $\mathfrak{D}$ sets

$$C' = M_\mu \cdot T, C_1' = g_1^s Y_2 Y_3 g_3^d, C_2' = (g_1^s Y_2 Y_3)^b \left(\prod_{i \in I_{W_\mu}} A_{i,w_i}\right)^t g_3^{d'}, C_3' = A_0^t g_3^{d''}$$

Guess. The adversary $\mathcal{A}$ outputs its guess $\mu' \in \{0,1\}$.

The distinguisher $\mathfrak{D}$ outputs 1 if $\mu = \mu'$, otherwise it returns to 0.

If $T = e(g_1, g_1)^{\alpha s}$, the challenge ciphertext will be a semi-functional encryption of M_μ and therefore $\mathfrak{D}$ simulates Game_q with $\mathcal{A}$. Similarly, if T is a random element of $\widehat{\mathbb{G}}$, the challenge ciphertext will be a semi-functional encryption of a random message, and hence, $\mathfrak{D}$ simulates $\mathsf{Game}_{\mathsf{Final}'}$ with $\mathcal{A}$. Thus,

$$\begin{aligned} Adv_{\mathfrak{D}}^{\mathsf{Problem\ 3}} &= \left|\Pr\left[\mathfrak{D}(D,T)=1|T=e(g_1,g_1)^{\alpha s}\right]\right. \\ &\quad \left.-\Pr\left[\mathrm{\mathfrak{D}(D,T)=1|T} \xleftarrow{\$} \widehat{\mathbb{G}}\right]\right| \\ &= \left|\Pr\left[\mu=\mu'|T=e(g_1,g_1)^{\alpha s}\right]\right. \\ &\quad \left.-\Pr\left[\mu=\mu'|T \xleftarrow{\$} \widehat{\mathbb{G}}\right]\right| \\ &= \left|Adv_{\mathcal{A}}^{\mathsf{Game}_q} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}}\right|. \end{aligned}$$

Because $Adv_{\mathfrak{D}}^{\mathsf{Problem\ 3}} \leq \epsilon_3$, we have $|Adv_{\mathcal{A}}^{\mathsf{Game}_q} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}}| \leq \epsilon_3$. □

Lemma 4. $|Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}}| \leq \epsilon_4$.

Proof. The distinguisher $\mathfrak{D}$ receives the challenge $\langle D = (\Sigma, g_1X_3, g_1^sZ_3, g_1X_2, Z_2, g_3), T\rangle$ of Problem 4, where $T = g_1^sY_2Y_3$ or a random element of $\mathbb{G}$, and depending on the distribution of T, $\mathfrak{D}$ simulates either $\mathsf{Game}_{\mathsf{Final}'}$ or $\mathsf{Game}_{\mathsf{Final}}$ as follows.

Setup. The distinguisher $\mathfrak{D}$ selects $\alpha, b \xleftarrow{\$} \mathbb{Z}_N$ and computes Γ=$e((g_1X_2)^\alpha, g_1X_3), A_0$= $g_1X_3, A = (g_1X_3)^b$, where implicitly sets $P = g_1^\alpha, P_1 = g_1^b$. For each attribute $att_{i,j} \in U, i \in [n], j \in [k_i]$, pick $a_{i,j} \xleftarrow{\$} \mathbb{Z}_N$ and set $A_{i,j} = (g_1X_3)^{a_{i,j}}$. The public key $\mathsf{PK} = \langle N, e, \Gamma, A_0, A, g_3, \{A_{i,j}\}_{i\in[n],j\in[k_i]}, U\rangle$ is sent to $\mathcal{A}$.

Key query phase. All secret keys are semi-functional for both the games. The distinguisher $\mathfrak{D}$ answers secret key queries for user attribute sets L_u= $\langle I_u, \{att_{i,\ell_i}\}_{i\in I_u}\rangle$, where $I_u \subset [n]$, in the following way: choose $r \xleftarrow{\$} \mathbb{Z}_N$ and compute

$$\begin{aligned} D_1' &= (g_1X_2)^\alpha (g_1X_2)^{br}, D_2' = (g_1X_2)^r, D_{i,\ell_i}' \\ &= (g_1X_2)^{r\cdot a_{i,\ell_i}}, \forall i \in I_u \end{aligned}$$

If $X_2 = g_2^x$, for some $x \in \mathbb{Z}_N$, then this is a properly distributed semi-functional secret key with implicit parameters $\gamma_1 = x(\alpha + br), \gamma_2 = xr$ and $z_{i,\ell_i} = \gamma_2 \cdot a_{i,\ell_i}$.

Challenge. The adversary $\mathcal{A}$ outputs two equal length messages $M_0, M_1 \in \widehat{\mathbb{G}}$ along with two access policies W_0, W_1 satisfying $I_{W_0} = I_{W_1}$. To construct the challenge ciphertext, $\mathfrak{D}$ samples $t, d, d', d'' \xleftarrow{\$} \mathbb{Z}_N, \Lambda \xleftarrow{\$} \widehat{\mathbb{G}}$ and flips a random coin $\mu \in \{0,1\}$. Let $W_\mu = \langle I_{W_\mu}, \{att_{i,w_i}\}_{i\in I_{W_\mu}}\rangle$, where $I_{W_\mu} \subset [n]$. It then forms the challenge ciphertext components as

$$\begin{aligned} C' &= \Lambda, C_1' = g_1^sZ_3Z_2g_3^d, C_2' \\ &= T^b\left(\prod_{i\in I_{W_\mu}} A_{i,w_i}\right)^t g_3^{d'}, C_3' = A_0^t g_3^{d''} \end{aligned}$$

Guess. The adversary $\mathcal{A}$ outputs its guess $\mu' \in \{0,1\}$.
The distinguisher $\mathfrak{D}$ outputs 1 if $\mu = \mu'$, otherwise it returns 0.

If $T = g_1^sY_2Y_3$, the challenge ciphertext is a properly distributed semi-functional encryption of a random message in $\widehat{\mathbb{G}}$, and hence, $\mathfrak{D}$ will simulate the game $\mathsf{Game}_{\mathsf{Final}'}$. Similarly, if T is a random element of $\mathbb{G}$, then the challenge ciphertext is a properly distributed semi-functional encryption of a random element of $\widehat{\mathbb{G}}$ with C_2' is random in $\mathbb{G}$ and hence the challenge ciphertext will give no information about μ to the adversary. In this case, $\mathfrak{D}$ simulates the game $\mathsf{Game}_{\mathsf{Final}}$ and $Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}} = 0$. Thus,

$$\begin{aligned} Adv_{\mathfrak{D}}^{\mathsf{Problem\ 4}} &= \left|\Pr\left[\mathfrak{D}(D,T)=1|T=g_1^sY_2Y_3\right]\right. \\ &\quad \left.-\Pr\left[\mathrm{\mathfrak{D}(D,T)=1|T} \xleftarrow{\$} \mathbb{G}\right]\right| \\ &= \left|\Pr\left[\mu=\mu'|T=g_1^sY_2Y_3\right]\right. \\ &\quad \left.-\Pr[\mu=\mu'|T \xleftarrow{\$} \mathbb{G}]\right| \\ &= \left|Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}}\right| \end{aligned}$$

Because $Adv_{\mathfrak{D}}^{\mathsf{Problem\ 4}} \leq \epsilon_4$, we have $|Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}'}} - Adv_{\mathcal{A}}^{\mathsf{Game}_{\mathsf{Final}}}| \leq \epsilon_4$.

□

6. PERFORMANCE ANALYSIS

In this section, we discuss the theoretical and empirical performance of our construction against previous schemes in the area.

The existing fully secure CP-ABE schemes [9,12] with constant-size ciphertext are not recipient anonymous. Although our previous construction [8] achieves recipient anonymity, it uses very restricted n-of-n access policy similar to [9], where n is the number of attribute categories in the attribute universe. Our anonymized monotone access policy W_{aap} with $|W_{\mathsf{aap}}| = \nu$ contains $\mathsf{as} = 1 + \binom{n-\nu}{1} \cdot k + \binom{n-\nu}{2} \cdot k^2 + \cdots + \binom{n-\nu}{n-\nu} \cdot k^{n-\nu}$ authorized sets if $|\mathsf{Att}_i| = k, \forall i \in [n]$. On the other hand, the n-of-n policy contains only one authorized set, that is, $\mathsf{as} = 1$. Even if each attribute category has only one attribute, that is, $k = 1$, then $\mathsf{as} = 2^{n-\nu}$ for our W_{aap} with $|W_{\mathsf{aap}}| = \nu$. Hence, our proposed approach exploits more expressive monotone policy than n-of-n policy. Although the encryption in proposed

Table II. Comparison of communication and computation cost of *fully* secure CP-ABE with *constant-size* ciphertext

Scheme	Group	Secret key size	Ciphertext size	KeyGen cost	Enc. cost	Dec. cost	Access policy	RA
	order			Exp.	Exp.	Pairings		
[9]	p	$2 \cdot \mathcal{B} + \mathcal{Z}$	$2 \cdot \mathcal{B} + 2 \cdot \mathcal{B}'$	4	6	2	n-of-n	No
[8]	$p_1p_2p_3$	$2 \cdot \mathcal{B}_1$	$2 \cdot \mathcal{B}_{1,3} + \widehat{\mathcal{B}}$	2	3	2	n-of-n	Yes
[12]	$p_1p_2p_3$	$O(\rho) \cdot \mathcal{B}_{1,3}$	$2 \cdot \mathcal{B}_1 + \widehat{\mathcal{B}}$	$O(\rho)$	3	2	Monotone	No
anonCP-ABE	$p_1p_2p_3$	$O(\rho) \cdot \mathcal{B}_1$	$3 \cdot \mathcal{B}_{1,3} + \widehat{\mathcal{B}}$	$O(\rho)$	5	3	Monotone	Yes

p, p_1, p_2, p_3, prime numbers; ρ, number of attributes held by user; n, number of attributes in attribute universe; $\mathcal{B}$, size of an element of group of prime order p; $\mathcal{Z}$, size of an element in $\mathbb{Z}_p$; $\mathcal{B}_1$ (or $\mathcal{B}_{1,3}$), size of an element in the group $\mathbb{G}_{p_1}$ (or $\mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$); $\widehat{\mathcal{B}}$ (or $\mathcal{B}'$), size of an element in the group $\widehat{\mathbb{G}}$ of order $N = p_1p_2p_3$ (or p); Exp., number of exponentiations in $\mathbb{G}$ and $\widehat{\mathbb{G}}$; RA, recipient anonymity; CP-ABE, ciphertext-policy attribute-based encryption.

scheme anonCP-ABE discloses partial information (list of involved attribute categories) of the ciphertext access policy, it is perfectly recipient anonymous, meaning that the adversary cannot learn what access policy is exactly used in the encryption. We make use of composite order (product of three primes) bilinear groups like [8,12] to achieve full semantic security as well as recipient anonymity.

Table II summarizes comparison of communication and computation cost of fully secure CP-ABE schemes with constant-size ciphertext. Due to n-of-n policy, the schemes [8,9] attain constant communication and computation cost. The approach in [12] exhibits constant cost during encryption and decryption that enforces monotone policies. But, the complexity of secret key generation grows linearly with the number of attributes. The complexity of the proposed scheme and that of [12] are asymptotically same. In subsequent sections, we present empirical comparison of the proposed construction against [12] in terms of communication and computation cost. In the following figures, we denote the CP-ABE of [12] as DJ.

6.1. Implementation setup

The implementation of both the proposed and the scheme of [12] is performed on Intel Core 2 Quad CPU at 3.01 GHz, 3.17 GB RAM and 32-bit mode Ubuntu 10.04 operating system by means of Ben Lynn's Pairing-Based Cryptography (PBC) library version 0.5.12 available at http://crypto.stanford.edu/pbc/. Following [12], we use the Type A1 curve for the pairing wherein the order of the group $(\mathbb{G}, \widehat{\mathbb{G}})$ is $N = p_1p_2p_3$. We evaluate the performance of both the schemes at 256-bit security level, where the size of each prime p_i is 256 bits long. All the implementation results are averaged to 20 trails.

6.2. Computation cost

The computation cost in Table II includes only more expensive operations exponentiation and pairing. And, the other operations are asymptotically same in number for both the schemes. The time taken for key generation, encryption and decryption for different number of attributes at 256-bit security level are depicted in Figure 1. The performance of each algorithm in both the approaches are as follows.

Key generation. It can be seen that from Figure 1(a), the secret key generation in [12] consumes more time than the proposed scheme. This is due to the fact that [12] uses the subgroup $\mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$ to generate user secret keys. On the other hand, the key generation algorithm in our approach deals only with the subgroup $\mathbb{G}_{p_1}$. Also, Figure 1(a) shows that the time to compute the secret key is proportional to the number of attributes in both the schemes.

Encryption. Our encryption uses five exponentiations, while the same for [12] is three. Thus, the time to generate ciphertext in our construction is more than [12]. We can see this fact from Figure 1(b). However, Figure 1(b) describes that both the schemes achieve constant encryption time.

Decryption. The proposed construction performs one extra pairing, thereby the time to decrypt a ciphertext in our scheme is a little more than that of [12]. However, we can see from Figure 1(c) that the decryption time in both the schemes is independent of the number of required attributes to make decryption successful.

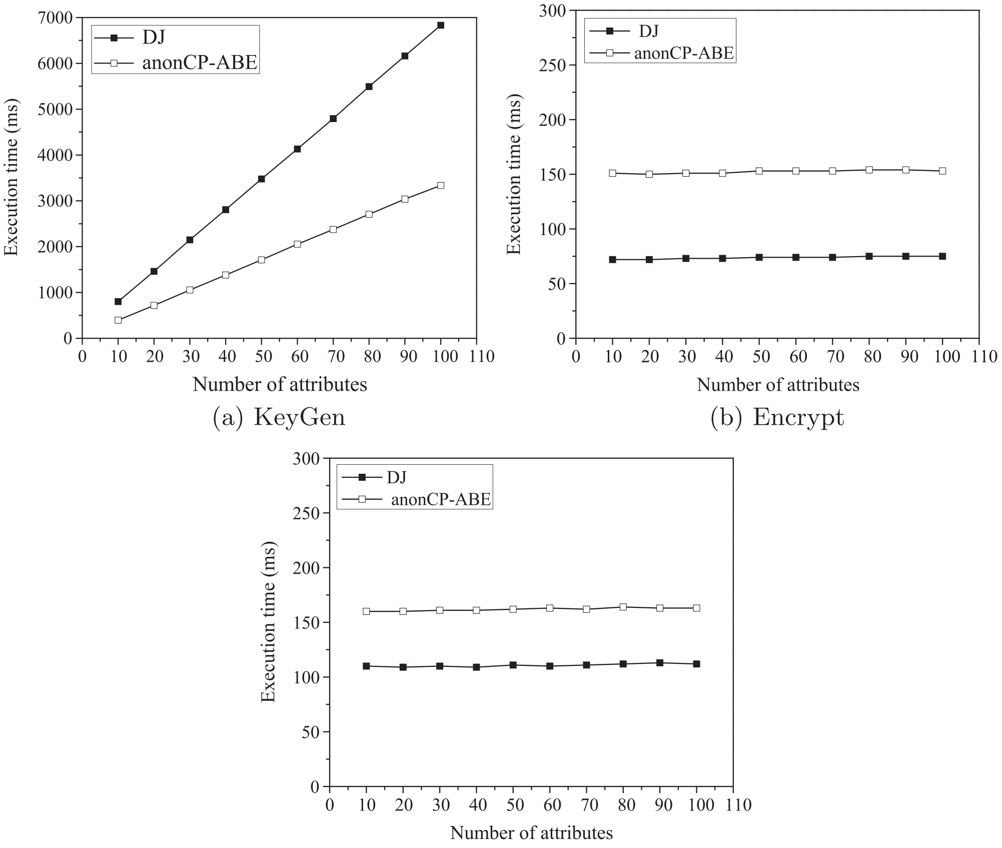
In sum, the construction [12] exhibits efficiency in constant time algorithms Encrypt and Decrypt, while our approach gains significant efficiency in linear time algorithm KeyGen.

6.3. Communication overhead

We measure the communication cost in two aspects: (i) *Secret key size* pertaining to the communication between CA and the user in order to obtain secret key; and (ii) *Ciphertext size* concerning the communication between users via ciphertext. Let us compare the size of secret key and ciphertext of our scheme with [12]. Figure 2 depicts the sizes of secret key and ciphertext for different numbers of attributes at 256-bit security level.

Secret key size. The secret key contains $\rho + 2$ group elements in both the schemes, where ρ is the number of attributes held by user. Consequently, the size of secret key is same in both the constructions, which is clear from Figure 2(a).

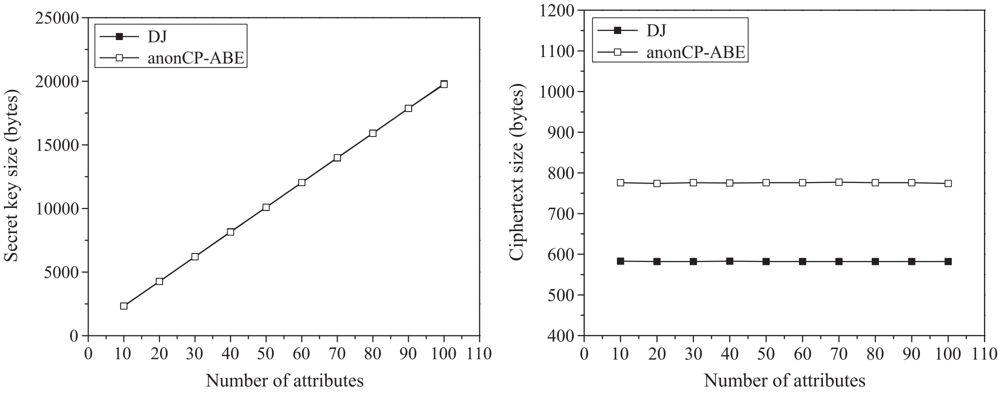
Ciphertext size. Figure 2(b) exhibits that the size of ciphertext in [12] is less than that in our scheme.



(a) KeyGen (b) Encrypt

(c) Decrypt

Figure 1. Comparison of execution time with different number of attributes at 256-bit security level.



(a) Secret key (b) Ciphertext

Figure 2. Comparison of size for different number of attributes at 256-bit security level.

Because our encryption algorithm added one extra group element to the ciphertext when compared with [12]. However, from Figure 2(b), it is justified that the size of ciphertext in both the schemes is constant.

7. CONCLUSION

The recipient anonymity is the critical concern in some circumstances where the receivers' attribute information scales the activity. And, in order to deploy attribute-based access control more efficiently in the circumstances where devices having limited computing power and less communication bandwidth, constant computation and communication overhead ABE realizations are highly desirable. With this end in view, we proposed a constant-size ciphertext CP-ABE that features the following achievements: (i) identity of the recipient is protected via policy hiding and randomize public parameters and ciphertext terms with another group elements in such a way that the DDH-test outcomes are useless to identify the access policy; (ii) fine-grained data access control is enabled by means of flexible anonymized monotone access policies over receivers' attributes; (iii) the amount of computation required for encryption and decryption processes are constant; and (iv) security is argued against adaptive adversary, that is, full security, meaning that the adversary can sample the access policy according to her choice along with plaintexts during challenge phase as opposed to submit at the beginning of simulation. The further direction of this work would be to extend the proposed anonCP-ABE to multi-authority setting wherein several authorities are participated in the secret key generation phase rather than single central authority. Another important direction of investigation would be to construct fully secure anonCP-ABE with constant-size ciphertext that exploits linear secret-sharing scheme-realizable access policy for any boolean formula.

ACKNOWLEDGEMENTS

The authors are thankful to the Editor, Editor-In-Chief and anonymous reviewers for their invaluable suggestions and comments that help us to improve the quality and clarity of this paper.

REFERENCES

1. Waters B. Efficient identity-based encryption without random oracles, *Proceedings of the 24th annual international conference on theory and applications of cryptographic techniques*, EUROCRYPT'05, 2005; 114–127.
2. Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Advances in Cryptology CRYPTO 2005*, vol. 3621, Shoup Victor (ed), Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005; 258–275.
3. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. *IEEE Symposium on Security and privacy (SP '07)*, 2007; 321–334.
4. Emura K, Miyaji A, Nomura A, Omote K, Soshi M. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. *Information security practice and experience, Lecture Notes in Computer Science* 2009; **5451**: 13–23.
5. Attrapadung N, Herranz J, Laguillaumie F, Libert B, de Panafieu E, Rfols C. Attribute-based encryption schemes with constant-size ciphertexts. *Theoretical Computer Science* 2012; **422**(0): 15–38.
6. Ge A, Zhang R, Chen C, Ma C, Zhang Z. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts. *Information security and privacy, Lecture Notes in Computer Science* 2012; **7372**: 336–349.
7. Zhou Z, Huang D, Wang Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. *EEE Transactions on Computers* 2015; **64**(1): 126–138.
8. Rao Y, Dutta R. Recipient anonymous ciphertext-policy attribute based encryption. In *Information systems security, Lecture Notes in Computer Science*, Vol. 8303, Bagchi A, Ray I (eds). Springer Berlin Heidelberg, 2013; 329–344.
9. Ren Y, Wang S, Zhang X, Qian Z. Fully secure ciphertext-policy attribute-based encryption with constant size ciphertext. *2011 Third International Conference on Multimedia Information Networking and Security (MINES)*, 2011; 380–384.
10. Chen C, Zhang Z, Feng D. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. *Provable security, Lecture Notes in Computer Science* 2011; **6980**: 84–101.
11. Han J, Susilo W, Mu Y, Yan J. Attribute-based oblivious access control. *The Computer Journal* 2012; **55** (10): 1202–1215.
12. Doshi N, Jinwala DC. Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption. *Security and Communication Networks* 2014; **7**: 1988–2002.
13. Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures. In *Applied Cryptography and Network Security, Lecture Notes in Computer Science*, Vol. 5037, Bellovin S, Gennaro R, Keromytis A, Yung M (eds). Springer Berlin Heidelberg, 2008; 111–129.
14. Yu S, Ren K, Lou W. Attribute-based content distribution with hidden policy. *4th Workshop on Secure Network Protocols, 2008 (NPsec '08)*, 2008; 39–44.
15. Lai J, Deng R, Li Y. Fully secure ciphertext-policy hiding CP-ABE. In *Information security practice and experience, Lecture Notes in Computer Science*, Vol. 6672, Bao F, Weng J (eds). Springer Berlin Heidelberg, 2011; 24–39.
16. Lai J, Deng RH, Li Y. Expressive CP-ABE with partially hidden access structures. *Proceedings of the 7th acm symposium on information, computer and*

communications security (ASIACCS '12), ACM: New York, NY, USA, 2012; 18–19.

17. Zhang Y, Chen X, Li J, Wong DS, Li H. Anonymous attribute-based encryption supporting efficient decryption test. *Proceedings of the 8th acm sigsac symposium on information, computer and communications security, (ASIA CCS '13)*, ACM: New York, NY, USA, 2013; 511–516.
18. Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *Journal of Cryptology* 2013; **26** (2): 191–224.
19. Lewko A, Okamoto T, Sahai A, Takashima K, Waters B. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. *Advances in cryptology EUROCRYPT 2010, Lecture Notes in Computer Science* 2010; **6110**: 62–91, (full version is Cryptology ePrint report 2010/110).
20. Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In *Advances in Cryptology - CRYPTO 2009, Lecture Notes in Computer Science*, Vol. 5677, Halevi S (ed). Springer Berlin Heidelberg, 2009; 619–636.
21. Sahai A, Waters B. Fuzzy identity-based encryption. *Advances in Cryptology EUROCRYPT 2005, Lecture Notes in Computer Science* 2005; **3494**: 457–473.
22. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security, (CCS '06)*, ACM, 2006; 89–98.
23. Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. *Proceedings of the 14th acm conference on computer and communications security, (CCS '07)*, ACM, 2007; 195–203.
24. Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. *Public Key Cryptography PKC 2011, Lecture Notes in Computer Science* 2011; **6571**: 53–70.
25. Ibraimi L, Tang Q, Hartel P, Jonker W. Efficient and provable secure ciphertext-policy attribute-based encryption schemes, *Proceedings of the 5th International Conference on Information Security Practice and Experience, (ISPEC '09)*, 2009; 1–12.
26. Cheung L, Newport C. Provably secure ciphertext policy ABE. *Proceedings of the 14th ACM conference on computer and communications security (CCS '07)*, ACM, 2007; 456–465.
27. Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption. *Advances in Cryptology CRYPTO 2010, Lecture Notes in Computer Science* 2010; **6223**: 191–208.
28. Rao Y.S, Dutta R. Computationally efficient expressive key-policy attribute based encryption schemes with constant-size ciphertext. In *Information and communications security, Lecture Notes in Computer Science*, Vol. 8233, Qing S, Zhou J, Liu D (eds). Springer International Publishing, 2013; 346–362.
29. Guo F, Mu Y, Susilo W, Wong D, Varadharajan V. CP-ABE with constant-size keys for lightweight devices. *IEEE Transactions on Information Forensics and Security* 2014; **9**(5): 763–771.
30. Boneh D, Goh EJ, Nissim K. Evaluating 2-DNF formulas on ciphertexts. In *Theory of cryptography, Lecture Notes in Computer Science*, Vol. 3378, Kilian J (ed). Springer Berlin Heidelberg, 2005; 325–341.

APPENDIX A: GENERIC SECURITY OF OUR ASSUMPTIONS ON PROBLEMS 1, 2, 3, and 4.

We closely follow [19][¶] to show that Problems 1, 2, 3, and 4 are hard in the generic group model under the assumption that finding a non-trivial factor of N is hard. Let g_1, g_2, and g_3 be generators of the subgroups $\mathbb{G}_{p_1}$, $\mathbb{G}_{p_2}$, and $\mathbb{G}_{p_3}$, respectively. Note that $\mathbb{G} = \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3}, \widehat{\mathbb{G}}$ are cyclic groups of order $N = p_1p_2p_3$ and $e : \mathbb{G} \otimes \mathbb{G} \to \widehat{\mathbb{G}}$ is a bilinear map. Every element $u \in \mathbb{G}$ can be written as $u = g_1^{x_1} g_2^{x_2} g_3^{x_3}$, for some $x_i \in \mathbb{Z}_{p_i}, i \in \{1, 2, 3\}$. For ease of presentation, we denote $u \in \mathbb{G}$ by the tuple (x_1, x_2, x_3). Then, each element $\hat{u} \in \widehat{\mathbb{G}}$ can be expressed as $\hat{u} = e(g_1, g_1)^{\beta_1} e(g_2, g_2)^{\beta_2} e(g_3, g_3)^{\beta_3}$, for some $\beta_i \in \mathbb{Z}_{p_i}, i \in \{1, 2, 3\}$, we denote it as $[\beta_1, \beta_2, \beta_3]$. With this notation, if $u = (x_1, x_2, x_3), v = (y_1, y_2, y_3) \in \mathbb{G}$ and $a \in \mathbb{Z}$, then $u \cdot v = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$, $u^a = (ax_1, ax_2, ax_3)$ and $e(u, v) = [x_1y_1, x_2y_2, x_3y_3]$, where $x_i + y_i, ax_i$ and x_iy_i are done modulo $p_i, i \in \{1, 2, 3\}$.

Random variables are described using formal variables written in capital letters that are each chosen independently and uniformly at random from the appropriate domain. For instance, a random element $X \overset{\$}{\leftarrow} \mathbb{G}$ is described as $X = (X_1, X_2, X_3)$, where $X_i \overset{\$}{\leftarrow} \mathbb{Z}_{p_i}, i \in \{1, 2, 3\}$. Note that a random variable expressed in this way has *degree t* if the maximum degree of any variable is t. Also, the same formal variables are used to show dependencies among elements. For example, $X = (X_1, X_2, X_3)$ and $Y = (X_1, Y_2, Y_3)$ are two random elements of $\mathbb{G}$ having the same $\mathbb{G}_{p_1}$ part.

Definition 6. [18] *Let X and $\{B_i\}$ be random variables over the same group. Then, X is said to be dependent on $\{B_i\}$ if there exists $\gamma_i \in \mathbb{Z}_N$ such that $X = \sum_i \gamma_i B_i$ as formal random variables; otherwise X is said to be independent of $\{B_i\}$.*

[¶] We consider here the full version of [19].

DOI: 10.1002/sec

In order to prove security of our assumptions, we use the following two theorems from [18].

Theorem 3. *let $N = p_1p_2 \dots p_m$ be a product of m distinct primes such that each $p_i > 2^\kappa$. Let $\{B_i\}$ be random variables over $\mathbb{G}$ and let $\{E_i\}, T_0, T_1$ be random variables over $\widehat{\mathbb{G}}$, where the degree of all random variables is at most t. Suppose each of T_0 and T_1 is independent of $\{E_i\} \cup \{e(B_i, B_j)\}$. Then, given any algorithm $\mathcal{A}$ performing at most q group operations and having advantage*

$$Adv_{\mathcal{A}} = \left|Pr\left[b' = b : b' \leftarrow \mathcal{A}(N, \{B_i\}, \{E_i\}, T_b),\ b \xleftarrow{\$} \{0,1\}\right] - \frac{1}{2}\right|$$

in the generic group model, there exists another algorithm that finds a non-trivial factor of N with probability at least $Adv_{\mathcal{A}} - O(q^2t/2^\kappa)$ by executing $\mathcal{A}$ as a subroutine, in time polynomial in κ and the running time of $\mathcal{A}$.

Theorem 4. *let $N = p_1p_2 \dots p_m$ be a product of m distinct primes such that each $p_i > 2^\kappa$. Let $\{B_i\}, T_0, T_1$ be random variables over $\mathbb{G}$ and let $\{E_i\}$ be random variables over $\widehat{\mathbb{G}}$, where degree of all random variables is at most t. Let $J = \{i|e(T_0, B_i) \neq e(T_1, B_i)\}$, where inequality refers to inequality as formal polynomials. Suppose each of T_0 and T_1 is independent of $\{B_i\}$, and furthermore that for all $k \in J$ it holds that $e(T_0, B_k)$ is independent of $\{E_i\} \cup \{e(B_i, B_j)\} \cup \{e(T_0, B_i)\}_{i \neq k}$, and $e(T_1, B_k)$ is independent of $\{E_i\} \cup \{e(B_i, B_j)\} \cup \{e(T_1, B_i)\}_{i \neq k}$. Then, given any algorithm $\mathcal{A}$ performing at most q group operations and having advantage*

$$Adv_{\mathcal{A}} = \left|Pr\left[b' = b : b' \leftarrow \mathcal{A}(N, \{B_i\}, \{E_i\}, T_b),\ b \xleftarrow{\$} \{0,1\}\right] - \frac{1}{2}\right|$$

in the generic group model, there exists another algorithm that finds a non-trivial factor of N with probability at least $Adv_{\mathcal{A}} - O(q^2t/2^\kappa)$ by executing $\mathcal{A}$ as a subroutine, in time polynomial in κ and the running time of $\mathcal{A}$.

We now apply these two theorems for the case $m = 3$, that is, $N = p_1p_2p_3$, to prove our assumptions are secure in generic group model. Note that the group operation is treated as an oracle query to a black box in generic group model. When the two operands are given as the query input, the outcome of applying the group operation to the operands is returned as output of the query. But, how the result can actually be computed is not available externally in the generic group model.

Problem 1. The challenge instance of Problem 1 is $\langle(g_1, g_3), T\rangle$, where $T \in \mathbb{G}$ or $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$. This can be expressed as

$$B_1 = (1,0,0), B_2 = (0,0,1),$$

$$T_0 = (W_1, W_2, W_3), T_1 = (W_1, 0, W_3)$$

Then, $J = \{i|e(T_0, B_i) \neq e(T_1, B_i)\} = \emptyset$ in this case. Because W_1 does not appear in B_1 or B_2, both T_0 and T_1 are independent of $\{B_1, B_2\}$. Thus, from Theorem 4, Problem 1 is generically secure, assuming that finding a non-trivial factor of N is hard. □

Problem 2. The challenge instance of Problem 2 is $\langle(g_1, X_1X_2X_3, Y_1Y_2, g_3), T\rangle$, where $T \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_2}$ or $T \in \mathbb{G}_{p_1}$. This can be expressed as

$$B_1 = (1,0,0), B_2 = (L_1, 1, L_3), B_3 = (K_1, K_2, 0), B_4 = (0,0,1),$$

$$T_0 = (W_1, W_2, 0), T_1 = (W_1, 0, 0)$$

Then $J = \{i|e(T_0, B_i) \neq e(T_1, B_i)\} = \{2, 3\}$. Because W_1 does not appear in $\{B_i\}_{i=1}^4$, both T_0 and T_1 are independent of $\{B_i\}_{i=1}^4$. We have $e(T_0, B_2) = [W_1L_1, W_2, 0]$. We see that $e(T_0, B_2)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_0, B_i)\}_{i \neq 2}$ because it is impossible to obtain W_1L_1 in the first coordinate of a combination of elements of $\{e(B_i, B_j)\} \cup \{e(T_0, B_i)\}_{i \neq 2}$. We have $e(T_1, B_2) = [W_1L_1, 0, 0]$. Because W_1L_1 cannot be the first coordinate of a combination of elements of $\{e(B_i, B_j)\} \cup \{e(T_1, B_i)\}_{i \neq 2}$, so $e(T_1, B_2)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_1, B_i)\}_{i \neq 2}$. We have $e(T_0, B_3) = [W_1K_1, W_2K_2, 0]$ and $e(T_1, B_3) = [W_1K_1, 0, 0]$. Similarly, $e(T_0, B_3)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_0, B_i)\}_{i \neq 3}$ and $e(T_1, B_3)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_1, B_i)\}_{i \neq 3}$ because we cannot obtain W_1K_1 in the first coordinate. Thus, from Theorem 4, Problem 2 is generically secure, assuming that finding a non-trivial factor of N is hard. □

Problem 3. The challenge instance of Problem 3 is $\langle(g_1, g_1^\alpha X_2, X_3, g_1^s Y_2Y_3, Z_2), T\rangle$, where $T = e(g_1, g_1)^{\alpha s}$ or a random element of $\widehat{\mathbb{G}}$. This can be expressed as

$$B_1 = (1,0,0), B_2 = (A, 1, 0), B_3 = (0,0,1), B_4 = (S, K_2, K_3), B_5 = (0, L_2, 0),$$

$$T_0 = [AS, 0, 0], T_1 = [W_1, W_2, W_3]$$

T_0 is independent of $\{e(B_i, B_j)\}$ because the only way to get AS in the first coordinate is to take $e(B_2, B_4) = [AS, K_2, 0]$, but here, K_2 in the second coordinate cannot be canceled. T_1 is independent of $\{e(B_i, B_j)\}$ because W_1, W_2, W_3 do not appear in $\{B_i\}_{i=1}^5$. Thus, from Theorem 3, Problem 3 is generically secure, assuming that finding a non-trivial factor of N is hard. □

Problem 4. The challenge instance of Problem 4 is $\langle(g_1X_3, g_1^sZ_3, g_1X_2, Z_2, g_3), T\rangle$, where $T = g_1^sY_2Y_3$ or a random element of $\mathbb{G}$. This can be expressed as

$$B_1 = (1,0,1), B_2 = (S, 0, L_3),$$
$$B_3 = (1,1,0), B_4 = (0, L_2, 0),$$
$$B_5 = (0,0,K_3),$$

$$T_0 = (S, W_2, W_3), T_1 = (W_1, W_2, W_3)$$

Then $J = \{i|e(T_0, B_i) \neq e(T_1, B_i)\} = \{1, 2, 3\}$. Because W_2 does not appear in $\{B_i\}_{i=1}^5$, both T_0 and T_1 are independent of $\{B_i\}_{i=1}^5$. We have $e(T_0, B_1) = [S, 0, W_3]$ and $e(T_1, B_1) = [W_1, 0, W_3]$. So, we can see that $e(T_0, B_1)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_0, B_i)\}_{i \neq 1}$ and $e(T_1, B_1)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_1, B_i)\}_{i \neq 1}$ because it is impossible to obtain W_3 in the third coordinate. Next, we have $e(T_0, B_2) = [S^2, 0, L_3W_3]$ and $e(T_1, B_2) = [SW_1, 0, L_3W_3]$. It is clear that $e(T_0, B_2)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_0, B_i)\}_{i \neq 2}$ and $e(T_1, B_2)$ is independent of $\left\{e(B_i, B_j)\right\} \cup \{e(T_1, B_i)\}_{i \neq 2}$ because we cannot obtain L_3W_3 in the third coordinate. Finally, we have $e(T_0, B_3) = [S, W_2, 0]$ and $e(T_1, B_3) = [W_1, W_2, 0]$. Similarly, we can say that $e(T_0, B_3)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_0, B_i)\}_{i \neq 3}$ and $e(T_1, B_3)$ is independent of $\{e(B_i, B_j)\} \cup \{e(T_1, B_i)\}_{i \neq 3}$ because it is impossible to obtain W_2 in the second coordinate. Thus, from Theorem 4, Problem 4 is generically secure assuming that finding a non-trivial factor of N is hard.

DOI: 10.1002/sec