Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 08, No. 03, September 2022.

AN ENHANCED APPROACH FOR CP-ABE WITH PROXY RE-ENCRYPTION IN IOT PARADIGM

Nishant Doshi

(Received: 1-Feb.-2022, Revised: 30-Mar.-2022, Accepted: 27-Apr.-2022)

ABSTRACT

In Internet of Things (IoT), encryption is a technique in which plaintext is converted to ciphertext into make it non-recovered by the attacker without secret key. Ciphertext policy attribute-based encryption (CP-ABE) is an encryption technique aimed at multicasting feature; i.e., user can only decrypt the message if the policy of attributes mentioned in the ciphertext is satisfied by the user's secret key attributes. In literature, the authors have improvised the existing technique to enhance the naïve CP-ABE scheme. Recently, in 2021, Wang et al. have proposed the CP-ABE scheme with proxy re-encryption and claimed it to be efficient as compared to its predecessors. However, it follows the variable-length ciphertext in which the size of ciphertext is increased with the number of attributes. Also, it leads to computation overhead on the receiver during decryption which will be performed by the IoT devices. Thus, in this paper, we have proposed on improved scheme to provide the constant-length ciphertext with proxy re-encryption to reduce the computation and communication time. The proposed scheme is secured under Decisional Bilinear Diffie-Hellman (DBDH) problem.

KEYWORDS

Attribute, Multi-authority, Proxy re-encryption, Constant length.

1. INTRODUCTION

In this IoT era, encryption techniques are playing vital role to achieve security and confidentiality. In a conventional symmetric key-based encryption scheme, sender and receiver possess the same key for communication. So, if one of the users compromised, then the entire scheme is compromised. To resolve this problem, [1] proposed the public key or asymmetric key encryption scheme, in which the receiver gives his/her public key to the sender for the encryption of the message, so only the receiver is able to decrypt the message. But, this scheme does not support the efficient multicast because a multicast sender has to encrypt the message a number of times equal to the number of receivers. The other problem is that the sender requires to remember the public key of the receiver. To overcome this problem, in [2] authors propose the Identity-based Encryption (IBE) in which the sender encrypts the message based on the receiver's unique id, like SSN, email id, …etc. But, this scheme also does not support multicast; so in [3], the authors propose the Fuzzy IBE system in which user with id X can only be able to decrypt the ciphertext entitled for X' if and only if $|X - X'| > y$, where y is the initial threshold value.

In research, the idea of IBE is generalized to solve the computation overhead during multicast and is called Attribute-based Encryption (ABE). ABE is classified into two variants; i.e., Key Policy Attribute-based Encryption (KP-ABE) [4] and Ciphertext Policy Attribute-based Encryption (CP-ABE) [5]. As the names suggest, in KP-ABE, policy of attributes is attached with secret key, whereas in CP-ABE, policy of attributes is attached with ciphertext. Indeed, CP-ABE gives more control to the sender in terms of selecting the intended recipients. In this research, we are focusing on the CP-ABE. In [5], the authors have proposed the single authority-based approach in which authority will generate the entire secret key of users.

As the existing approaches deal with single authority, they suffer from issues *viz.* (i) key escrow: authority can regenerate the secret key on behalf of any user (ii) computation overhead on the authority to generate the entire secret key of all system users. To deal with this issue, in [6]–[10], the authors have proposed various approaches based on multi-authority systems. In IoT, this will be helpful to design the decentralized approaches based infrastructure.

All the approaches mentioned so far requires sender to re-encrypt the same message for different policies. This leads to computation overhead which can be mitigated by proxy-based cloud systems. In proxy re-encryption, the proxy will re-encrypt without any knowledge of the secret key of the user. In

N. Doshi is with School of Technology, PANDIT Deendayal Energy Uni., Raisan, India. Email: nishant.doshi@sot.pdpu.ac.in

[11]–[15], the authors have proposed various approaches to deal with proxy-based re-encryption mechanism. In IoT, this will be helpful to reduce the computation overhead on IoT devices.

All the approaches mentioned so far deal with variable-length ciphertext; i.e., length of the ciphertext increases with the number of attributes. This will lead to communication overhead as well as computation overhead on the receiver side. In IoT paradigm, we required energy efficient-approaches as to run on the deployed sensors in the field. To deal with this issue, in [16]–[19], the authors have proposed approaches based on constant-length ciphertext. More details on these approaches are given in the next section.

1.1 Our Contribution

Amidst of the above concerns, research will lead to the need of one system having all features. On the other side, we have schemes to give either of the features as reported in literature [20]–[29]. Thus, in this paper, we propose the collusion-resistant CP-ABE scheme which provides the proxy re-encryption to make our scheme applicable in the scenario where compromised users' leaked decryption keys can be traced and nullified. Our scheme works for the threshold case; i.e., the attributes in the ciphertext must be equal to the subset of user's attributes in his/her secret key. We proposed new protocol to address this problem and show the efficiency compare to the existing protocols. The security of this protocol is based on DBDH assumptions as their predecessors.

1.2 Paper Organization

The rest of the paper is organized as follows. Section 2 deals with a literature review in this field. Section 3 deals with the hardness problems used for the security of the proposed work. Section 4 showcases the proposed work. Section 5 deals with the security and computation analysis. The conclusion and references are presented at the end.

2. LITERATURE REVIEW

In this section, we conduct a literature survey on the various approaches in CP-ABE.

2.1 Multi-authority

The original CP-ABE scheme [5] is dealing with single-authority environment. A single-authority system requires the entire trust on the same authority, so if authority-compromised or behaves maliciously, then the entire system will be compromised. In addition, it deals with computation overhead on authority as to generate the entire secret keys of all system users. To overcome these issues, in [6], the authors firstly propose the idea of multi-authority systems. In a multi-authority system, there is one central authority (CA) and multiple attribute authorities (AAs). As we observed, this scheme requires mutual trust between AAs and the CA must be present to manage the attribute authorities and add new AAs. The CA is able to decrypt any ciphertext, which can harm the system. In [7]–[10], [30]-[31], the authors proposed different approaches to deal with the multi-authority system.

2.2 Proxy Re-encryption (PRE)

It's a technique in which an untrusted proxy server will translate a ciphertext encrypted under Alice's public key to a ciphertext encrypted under bob's public key. This can be useful in email forwarding applications. For PRE, Alice can generate a PRE key, which she can give to proxy, so there is no need to store it at the user side. Proxy can get no information regarding secret of Alice from PRE key. Upon incoming ciphertext, proxy can apply the PRE key to get the required ciphertext. In [32], the authors introduced the notion of PRE. In [33], the authors proposed the bidirectional PRE scheme. In [34], the authors proposed the first unidirectional PRE scheme. In [35], the authors proposed the IBE-PRE scheme which converts ciphertext encrypted under Alice's identity to one encrypted under bob's identity. Their scheme is secure under random Oracle. In [36], the authors proposed the IBE-PRE in standard model. In [37], the authors proposed the first AB-PRE scheme which is bidirectional and based on key policy scheme. In [38], the authors proposed the first CP-ABE-PRE scheme. In [39], the authors proposed the variable-length CP-ABE-PRE scheme. In [40], the authors proposed the constant

ciphertext length for CP-ABE-PRE scheme, but they required the same number of attributes in policy as in secret key. In [11]–[15], the authors have proposed various approaches for improving the existing schemes.

2.3 Ciphertext Length

All the approaches mentioned so far deal with the variable-length ciphertext approach; i.e., length of the ciphertext increases with the number of attributes. This will increase the computation overhead on the receiver due to access amount of operations during decryption. In [41], the authors firstly introduced the concept of constant-length ciphertext using the (t, t) threshold system. As mentioned, it requires the same set of attributes in ciphertext as well as in secret key for successful decryption. This makes the scheme of [41] usable in limited scenarios. In [42], the authors proposed the constant-length ciphertext in threshold ABE based on the dynamic threshold encryption scheme from [43]. In [16]–[19], the authors have proposed various schemes to improve constant-length ciphertext.

Based on our literature survey, we have schemes available for the multi-authority or constant-length ciphertext. However, none of the approach available in research provides all features in a single scheme. In addition, to use a different scheme for each feature can be an overhead on the system users. Thus, in this paper, we have proposed a single scheme to provide all these features.

3. PRELIMINARIES

In this section, we present the preliminaries as well as the hardness problems that will be utilized throughout the paper.

3.1 Bilinear Group

The security of the proposed system is based on the algebraic group called the bilinear groups based on a bilinear map. As we are using bi-linear map function for pairing operations, we have taken Decisional Bilinear Diffie Hellman hardness problem.

Definition 1 (Bilinear map). Consider cyclic multiplicative group G_1, G_2 and G_3 of prime order p and generators g_1, g_2 and g_3, respectively, as well as a deterministic bilinear map function e: $G_1 \times G_2 \rightarrow G_3$ with the following requirements.

- Bi-linearity : For all $x \in G_1, y \in G_2, a, b \in Z_p$, $e\ (x^a, y^b) = e(x, y)^{ab}$.
- Non-degeneracy: $e\ (g_1, g_2) \neq 1$.
- Efficiency: e must be a time-efficient function.

Definition 2 (Discrete Logarithm Problem (DLP)). Find an integer $x \in Z_p$, such that $h = g^x$ whenever such integer exists given two group elements g and h.

Definition 3 (Decisional Bilinear Diffie Hellman (DBDH) Problem). In prime-order group G with generator g, on input $g, g^a, g^b, g^c \in G$, check whether $c = ab$ or not.

3.2 Proposed Construction

The proposed scheme consists of a number of polynomial algorithms as follows.

- **Setup**: It runs by central authority (CA) to generate the private and public parameters of the system.
- $\boldsymbol{AA_i}$ **Setup**: It runs by the respective Attribute Authority (AA) to generate the parameters of authority.
- **KeyGen**: It runs by the CA to generate part of the secret keys of the users. It consists of the following-sub algorithms.
    - **RKGen:** It runs by the user to generate re-encryption key for the proxy servers.
- **RequestAttributeSK:** It runs by AA to give the secret component respective to the attribute in the user's secret key.
- **Encrypt**: It runs by the sender to convert the plaintext into ciphertext based on the access policy. It consists of the following sub-algorithms.
    - **ReEncrypt**: It runs by the proxy server to convert ciphertext from one policy to another policy.

- **Decrypt**: It runs by the receiver to get the plaintext from the ciphertext if the access policy is satisfied; else a random message will be given.

4. THE PROPOSED SCHEME

The proposed scheme(s) consists of the following polynomial algorithms. The schematic diagram of the proposed scheme is given in Figure 1.

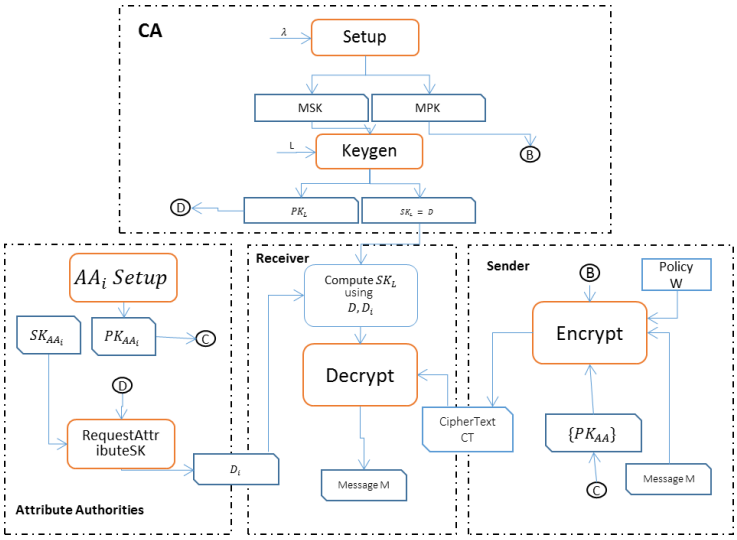

Figure 1. Schematic diagram for the proposed scheme.

Set-up: It executes by the CA as follows.

- Selects a bilinear group G_0 of prime order p with generator g.
- Selects exponents $y, \beta \in_R Z_p$.
- Computes $h = g^{\beta}, Y = e(g,g)^{y}$.
- Computes Master Public Key $MPK = G_0, g, h, Y$.
- Computes Master Secret Key $MSK = (\beta, y)$.

AA_i setup: It runs by AA_i to create parameters for attribute *i*.

- Chooses exponent $\alpha_i \in_R Z_p$.
- Computes Public Parameter $PK_i = g^{\alpha_i}$.
- Computes Secret Parameter $SK_i = \alpha_i$.

Keygen (MSK,u) : It runs by the CA to create the secret key (SK) for user *u*. L denotes the attributes' list. It is exemplified from this algorithm that CA is responsible for the generic parameters, not the attributes of the users. Thus, compromising the CA cannot compromise the system; i.e., the system is secure against key escrow. Also, due to the unique r value in the user's secret key, the proposed scheme is secure against collusion attack.

- Chooses $r \in_R Z_p$.
- Computes secret key $SK_u = g^{(y+r)/\beta}$.
- Computes public key $PK_u = g^r$.
- Sets attribute list $L_u = \emptyset$.

RKGen(MPK,W,W',SK_L) : This algorithm runs by user *u*, consisting of attribute set $AS \subseteq L$ and satisfying access policy *W*. This algorithm gives proxy re-encryption key which can be used to convert ciphertext with access policy *W* into ciphertext with access policy *W'*. Here, $n = |AS| = |W|$; i.e., number of attributes in access policy W.

- Generates $d, g_1 \in_R Z_p$.
- Computes $C = Encrypt\ (MPK, {g_1}^{nd}, W')$.
- Computes $R = D \prod_{v_{i,j} \in AS} (D_{i,j} {g_1}^{d})$.
- $RK_{AS \to W'} = < C, R, g^r >$

RequestAttributeSK(PK_u,u, L_u): This algorithm runs by AA. AA generates exponent $r_i \in_R Z_p$. H denotes hash function with one-way property.

- Computes $D_i = (g^r)^{\alpha_i}$ and $L_u = L_u + i$.
- Sends D_i and L_u to user.

Encrypt(M,W,PK_1,PK_2,…,PK_N): It runs by the sender by taking the list of attributes for policy as well as message M. It follows the steps below:

- Chooses exponent $s \in_R Z_p$.
- Computes $C_1 = M\, Y^s$.
- Computes $C_2 = g^s$.
- Computes $C_3 = (\prod_{t\in W} PK_i)^s = (\prod_{t\in W} g^{\alpha_i})^s$.
- Computes $C_4 = (h)^s = g^{\beta s}$.
- Final ciphertext $CT = \{C_1, C_2, C_3, C_4, W\}$.

As can be seen from the above steps, we have five components only irrespective of the set of attributes in the final ciphertext. This will achieve the constant-length ciphertext approach.

RKEncrypt(CT_W,$RK_{AS\rightarrow W'}$) : It runs by proxy server to convert the CT_W to $CT_{W'}$. There exists the attribute set $AS \subseteq L$ and it satisfies access policy *W*.

- $C' = \frac{C_1\, e(C_2, g^r)}{e(C_3, R)} = \frac{M}{e(g,g_1)^{n\,s\,d\,\beta}}$
- $CT_{W'} = < C', C, C_3 >$

Decrypt(SK,CT) : It runs by the receiver by taking CT as well as SK as input. It returns M if policy is satisfied; else a random message is given. For simplicity, assume $AS \subseteq L$ and $AS = W$. It is divided in two parts based on CT being the original ciphertext of proxy re-encrypted ciphertext.

If **CT** is an original ciphertext, then the user will follows the below:

$$= \frac{C_1 \cdot e(g^r, C_2) \cdot e(C_3, g^r)}{e\left(C_4, g^{\frac{y+r}{\beta}}\right) \cdot e(C_2, (\prod_{t\in AS} g^{\alpha_t})^r)} = \frac{M \cdot e(g,g)^{y\,s} \cdot e(g,g)^{r\,s} \cdot e(g,g)^{r\,s\,p}}{e(g^s, g^{y+r}) \cdot e(g^s, g^{r\,q})} = \frac{M \cdot e(g,g)^{y\,s} \cdot e(g,g)^{r\,s} \cdot e(g,g)^{r\,s\,p}}{e(g,g)^{y\,s} \cdot e(g,g)^{r\,s} \cdot e(g,g)^{r\,s\,q}} = M.$$

Here, $p = \sum_{t\in W} \alpha_t$ and $q \sum_{t\in AS} \alpha_t$.

If **CT** is a re-encrypted ciphertext, then the user will follow the below:

$$g_1{}^{nd} = Decrypt(SK, CT) = \frac{M\, e(C_3, g_1{}^{nd})}{e(g, g_1)^{n\,s\,d\,\beta}} = M.$$

5. ANALYSIS

As we discussed, ABE has actually evolved from IBE. The security of ABE schemes is also typically modeled on the lines of security of the IBE schemes. The scheme that we propose here is inspired by the one in [4], in which the authors first proposed a scheme for ABE. The scheme is described in a setup that involves a security game amongst an attacker and a challenger, along with a simulator.

The simulator generates an initial parameter and gives it to the challenger. Based on this security game, the ABE schemes can broadly be categorized into two categories *viz. selective secure* and *fully secure*. In *selectively* secure schemes, the attacker announces the target policy ahead of the game, so that the simulator can bind the hardness of the problem with the attributes mentioned in the policy. In *fully* secure schemes, the attacker is not required to announce the target policy initially, as there are sequences of games played between the attacker and the challenger. Figure 2 depicts the security game between the challenger (CA+AAs) and the attacker.
As one can see, the attacker announces the target policy before seeing the public parameters, which makes the proposed scheme a selectively secure model.

5.1 Security Analysis

Theorem 1: The proposed scheme is secure under the DBDH assumption for message indistinguishability.
Proof: Assume that the adversary A gains the advantage ϵ in the security game. Therefore, a simulator

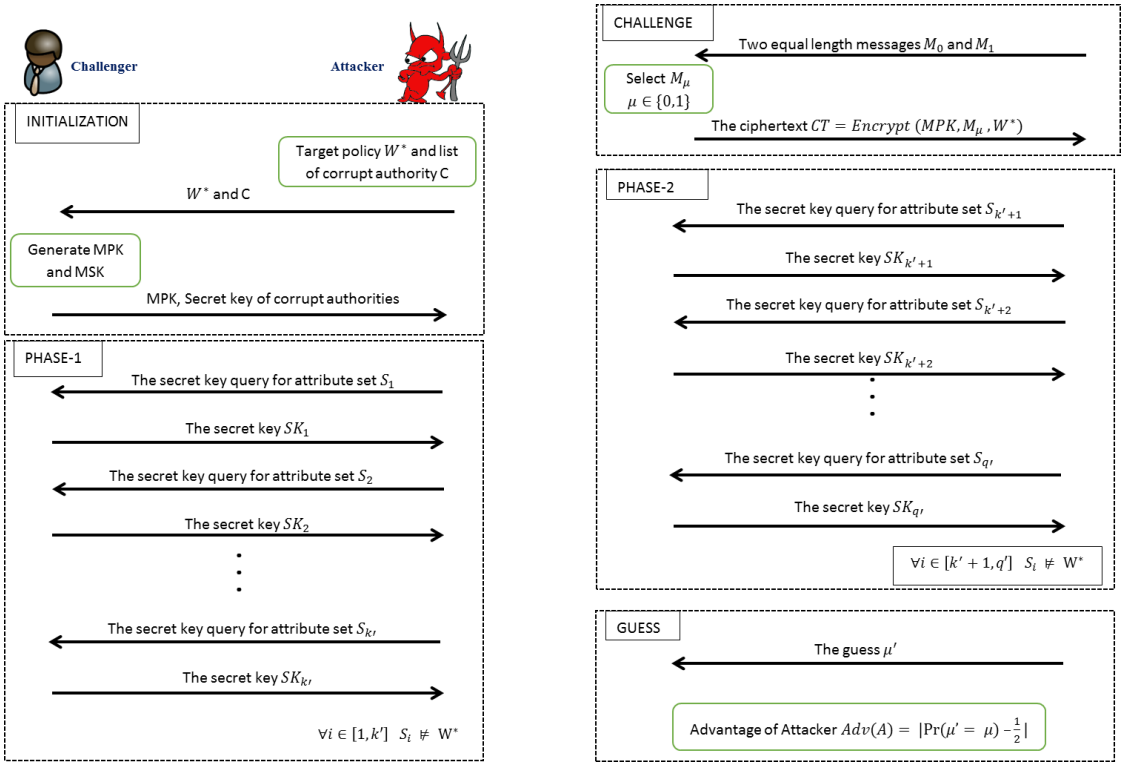

Figure 2. Security game for MA-CP-ABE scheme.

X will be constructed in DBDH assumption with advantage $\frac{\epsilon}{2}(1-\frac{(N')^2}{p})$, where $N' = 2^{n\,n_i}$ represents the number of access structures. The challenger generates $a, b, c, z \in_R Z_p$, $\omega \in_R \{0,1\}$ and g, where g is the generator for group G; so,

$$Z = \begin{cases} e(g,g)^{abc}, & (w=0) \\ e(g,g)^{z}\ , & (w=1) \end{cases}$$

The challenger gives $(g, g^a, g^b, g^c, Z) \in G^4 \times G_1$ to X. Now, A provides target policy $W^* = [W_1^*, W_2^*, \ldots, W_k^*]$ to X. X sets the parameter $Y = e(g^a, g^b) = e(g,g)^{ab}$. For $\alpha'_{i,j}\{i \in [1,n], j \in [1,n_i]\} \in_R Z_p$. X selects secret keys $\alpha_{i,j}\{i \in [1,n], j \in [1,n_i]\}$ and public keys $T_{i,j}\{i \in [1,n], j \in [1,n_i]\}$ as follows:

$$\alpha_{i,j} = \begin{cases} \alpha'_{i,j}, & (v_{i,j} = W_i^*) \\ b\alpha'_{i,j}, & (v_{i,j} \neq W_i^*) \end{cases}$$

$$T_{i,j} = \begin{cases} g^{\alpha'_{i,j}}, & (v_{i,j} = W_i^*) \\ (g^b)^{\alpha'_{i,j}}, & (v_{i,j} \neq W_i^*) \end{cases}$$

X gives $MPK = \left(e, g, h, Y, T_{i,j}\{i \in [1,n], j \in [1,n_i]\}\right)$ to A. X gives the secret parameters of corrupted authorities to A. In **Extract** query L, it requires $v_{i,j} = L_i$ and $v_{i,j} \neq W^*$ because $L \neq W^*$. Thus, X can write $\sum_{v_{i,j} \in L} \alpha_{i,j} = X_1 + bX_2$, where $X_1, X_2 \in Z_p$. Here, X_1 and X_2 showcase the summation of $\alpha'_{i,j}$ values. Thus, X can recalculate X_1 and X_2; it chooses $\beta \in_R Z_p$, calculates $r = \frac{\beta - ua}{X_2}$ and re-computes SK_L as follows:

$SK_L = \{g^{\frac{\beta}{X_2}}(g^a)^{\frac{-u}{X_2}}, \left(g^{ab} g^{\frac{\beta}{X_2}}(g^a)^{\frac{-u}{X_2}}\right)^{1/\beta}, \forall_{v_{i,j} \in L}(g^{\alpha_{i,j}})^{\frac{\beta}{X_2}}((g^a)^{\alpha_{i,j}})^{\frac{-u}{X_2}}\}$.

Therefore, SK_L becomes a correct secret key as follows:

$$\left(g^{ab} g^{\frac{\beta}{X_2}}(g^a)^{\frac{-u}{X_2}}\right)^{1/\beta} = \left((g)^{ab}(g)^{\frac{\beta-ua}{X_2}}\right)^{1/\beta} = g^{(y+r)/\beta}.$$

$g^{\frac{\beta}{X_2}}(g^{a})^{\frac{-u}{X_2}} = g^{\frac{\beta - ua}{X_2}} = g^{r}$ and $(g^{\alpha_{i,j}})^{\frac{\beta}{X_2}}((g^{a})^{\alpha_{i,j}})^{\frac{-u}{X_2}} = (g^{\alpha_{i,j}})^{r} = (T_{i,j})^{r}$.

A will select $AS \subseteq L$ and compute $\prod_{v_{i,j} \in \text{AS}}(T_{i,j})^{r} = g^{r\sum_{v_{i,j} \in \text{AS}} \alpha_{i,j}}$

If $X_2 = 0 \ mod \ p$, then AS ⊆ L with $\sum_{v_{i,j} \in \text{AS}} \alpha_{i,j} = \sum_{v_{i,j} \in \text{W}^*} \alpha_{i,j}$, then X aborts with $\Pr[abort] = \frac{(N')^2}{p}$.

X selects $\mu \in_R \{0,1\}$, calculates $C_1^* = M_\mu Z, C_2^* = g^c, C_3^* = (g^c)^{\sum_{v_{i,j} \in W^*} \alpha_{i,j}}, C_4^* = (g^c)^{\beta}$ and sends $< C_1^*, C_2^*, C_3^*, C_4^*, W^* >$ to A.

Guess: A gives $\mu' \in \{0,1\}$ on μ as guess.

If $\mu' = \mu$, then X sets $\tau' = 0$; else $\tau' = 1$. Appropriate to this, the two cases are as follows:

Case 1: If $\tau = 0$, then $Z = e(g,g)^{abc}$ and ciphertext is valid for M_μ.

$\therefore A$ can output $\mu' = \mu$ with advantage ϵ.

$$\therefore \Pr[\mu' = \mu | \tau = 0 \wedge \overline{abort}] = \frac{1}{2} + \epsilon.$$

$\therefore \Pr[\tau' = \tau | \tau = 0 \wedge \overline{abort}] = \frac{1}{2} + \epsilon$, since X guesses $\tau' = 0$ when $\mu' = \mu$.

Case 2: If $\tau = 1$, the target policy is independent of M_0 and M_1, so that A fails to get μ.

$\therefore A$ can output $\mu' = \mu$ with *NO* knowledge.

$\therefore \Pr[\mu' \neq \mu | \tau = 1 \wedge \overline{abort}] = \frac{1}{2}$.

$\therefore \Pr[\tau' \neq \tau | \tau = 1 \wedge \overline{abort}] = \frac{1}{2}$, since X guesses $\tau' = 1$ when $\mu' \neq \mu$.

From case 1 and case 2, X is having the following advantage in this DBDH game:

$$\Pr[\tau' = \tau] - \frac{1}{2} = \Pr[\tau = 0]\Pr[\tau' = \tau | \tau = 0] + \Pr[\tau = 1]\Pr[\tau' = \tau | \tau = 1] - \frac{1}{2}$$

$$= \frac{1}{2}\Pr[\tau' = \tau | \tau = 0] + \frac{1}{2}\Pr[\tau' = \tau | \tau = 1] - \frac{1}{2} = \frac{1}{2}\{\Pr[\tau' = \tau | \tau = 0] + \Pr[\tau' = \tau | \tau = 1] - 1\}$$

$$= \frac{1}{2}\{\Pr[abort]\Pr[\tau' = \tau | \tau = 0 \wedge abort] + \Pr[\overline{abort}]\Pr[\tau' = \tau | \tau = 0 \wedge \overline{abort}]$$
$$+ \Pr[abort]\Pr[\tau' = \tau | \tau = 1 \wedge abort] + \Pr[\overline{abort}]\Pr[\tau' = \tau | \tau = 1 \wedge \overline{abort}]\}$$

As *"abort"* is not dependent on DBDH challenge, we have:

$\Pr[\tau' = \tau | \tau = 0 \wedge abort] = \Pr[\tau' = \tau | \tau = 1 \wedge abort] = \frac{1}{2}$.

$$= \frac{1}{2}\left\{\frac{(N')^2}{p}\frac{1}{2} + \left(1 - \frac{(N')^2}{p}\right)\left(\frac{1}{2} + \epsilon\right) + \frac{(N')^2}{p}\frac{1}{2} + \left(1 - \frac{(N')^2}{p}\right)\frac{1}{2} - 1\right\}$$

$$= \frac{1}{2}\left\{\left(1 - \frac{(N')^2}{p}\right)\epsilon\right\} = \frac{\epsilon}{2}\left(1 - \frac{(N')^2}{p}\right).$$

5.2 Performance Analysis

In this sub-section, we present the comparative analysis based on the size of various parameters in Table 1 as well as computation time in Table 2. In Table 1, " − " represents that a particular parameter is not required. We assume that each authority is responsible for only one attribute. As one can see from Table 1, the proposed scheme supports a constant-length ciphertext. In addition, from Table 2, one can see that the pairing operations also remain constant due to the *constant-length ciphertext* approach. In Table 3, we give the feature-based comparative analysis for the proposed scheme against existing schemes.

Table 1. Size of parameters for multi-authority ABE schemes.

Scheme	MPK	MSK	SK	CT	Expressiveness of policy
$\boldsymbol{r_1}$=# CT attributes,$\boldsymbol{r_2}$=# SK attributes, $\|\boldsymbol{Z}\|$= Z element bit-length, $\|\boldsymbol{G}\|$= G element bit-length, $\boldsymbol{n}$=# system attributes, $\boldsymbol{n'}$=#*OR* gates in the policy					
[8]	$O(1)\|G\|$	$O(1)\|Z\|$	$O(1)\|G\|$	$O(r_1)\|G\|$	Any threshold gate
[9]	$O(n)\|G\|$	$O(n)\|Z\|$	$O(r_2)\|G\|$	$O(r_1)\|G\|$	AND gate
[10]	$O(1)\|G\|$	−	$O(r_2)\|G\|$	$O(r_1)\|G\|$	Any threshold gate
[30]	$O(1)\|G\|$	$O(1)\|G\|$	$O(r_2)\|G\|$	$O(n')\|G\|$	Any threshold gate
[31]	−	−	$O(n)\|G\|$	$O(r_1)\|G\|$	Any threshold gate
[16]	$O(n)\|G\|$	$O(n)\|Z\|$	$O(r_2)\|G\|$	$O(1)\|G\|$	AND gate
[17]	$O(1)\|G\|$	$O(1)\|G\|$	$O(r_2)\|G\|$	$O(1)\|G\|$	Any threshold gate
[18]	$O(n)\|G\|$	$O(n)\|Z\|$	$O(r_2)\|G\|$	$O(1)\|G\|$	Any threshold gate

[19]	$O(1)\|G\|$	–	$O(r_2)\|G\|$	$O(1)\|G\|$	AND gate
[11]	$O(1)\|G\|$	–	$O(r_2)\|G\|$	$O(r_1)\|G\|$	Any threshold gate
[12]	$O(1)\|G\|$	$O(1)\|G\|$	$O(r_2)\|G\|$	$O(n')\|G\|$	Any threshold gate
[13]	–	–	$O(n)\|G\|$	$O(r_1)\|G\|$	Any threshold gate
[14]	–	–	$O(n)\|G\|$	$O(r_1)\|G\|$	Any threshold gate
[15]	–	–	$O(n)\|G\|$	$O(r_1)\|G\|$	Any threshold gate
Our Work	$O(n)\|G\|$	$O(1)\|Z\|$	$O(r_2)\|G\|$	$O(1)\|G\|$	AND gate

Table 2. Computational comparison for proposed schemes.

Scheme	Encryption	Decryption
$\boldsymbol{T_{Exp}}$= One exponent time, $\boldsymbol{T_{mul}}$= One multiplication time, $\boldsymbol{T_{pairing}}$= One pairing time		
[8]	$O(r_1)T_{Exp} + O(1)T_{Mul}$	$O(r_1)(T_{Exp} + T_{Mul} + T_{Pairing})$
[9]	$O(r_1)(T_{Exp} + T_{Mul} + T_{Pairing})$	$O(r_1)(T_{Exp} + T_{Mul} + T_{Pairing})$
[10]	$O(1)T_{Exp} + O(n)(T_{Mul} + T_{Pairing})$	$O(n)(T_{Mul} + T_{Pairing})$
[30]	$O(n'r_1)T_{Exp} + O(r_1)T_{Mul}$	$O(r_1)T_{Mul} + O(1)T_{Pairing}$
[31]	$O(1)(T_{Exp} + T_{Mul} + T_{Pairing})$	$O(r_1)(T_{Mul} + T_{Pairing})$
[16]	$O(n)(T_{Mul} + T_{Pairing})$	$O(1)(T_{Exp} + T_{Pairing})$
[17]	$O(n)(T_{Mul} + T_{Pairing})$	$O(1)(T_{Exp} + T_{Pairing})$
[18]	$O(n)(T_{Mul} + T_{Pairing})$	$O(1)(T_{Exp} + T_{Pairing})$
[19]	$O(r_1)T_{Exp} + O(1)T_{Mul}$	$O(r_1)(T_{Exp} + T_{Pairing})$
[11]	$O(1)T_{Exp} + O(n)(T_{Mul} + T_{Pairing})$	$O(n)(T_{Mul} + T_{Pairing})$
[12]	$O(n'r_1)T_{Exp} + O(r_1)T_{Mul}$	$O(r_1)T_{Mul} + O(1)T_{Pairing}$
[13]	$O(1)(T_{Exp} + T_{Mul} + T_{Pairing})$	$O(r_1)(T_{Mul} + T_{Pairing})$
[14]	$O(n)(T_{Mul} + T_{Pairing})$	$O(n)(T_{Exp} + T_{Pairing})$
[15]	$O(n)(T_{Mul} + T_{Pairing})$	$O(n)(T_{Exp} + T_{Pairing})$
Our Work	$O(1)T_{Exp} + O(r_1)T_{Mul}$	$O(r_1)T_{Mul} + O(1)T_{Pairing}$

Table 3. Feature-based comparative analysis.

Scheme	Multi-authority	Constant-length Ciphertext	Proxy Re-encryption	Scheme	Multi-authority	Constant-length Ciphertext	Proxy Re-encryption
[8]	✓	✗	✗	[18]	✓	✓	✗
[9]	✓	✗	✗	[19]	✗	✓	✗
[10]	✓	✗	✗	[11]	✗	✗	✓
[30]	✓	✗	✗	[12]	✗	✗	✓
[31]	✓	✗	✗	[13]	✗	✗	✓
[16]	✗	✓	✗	[14]	✗	✗	✓
[17]	✗	✓	✗	[15]	✗	✗	✓
Our scheme					✓	✓	✓

6. Conclusion and Future Work

CP-ABE is the efficient technique for the multicasting feature in the security. However, the basic CP-ABE scheme suffers from various important features like ciphertext length. In research, authors have proposed different schemes for each of the features, but none of the schemes provided all of these features. Thus, in this paper, we have proposed a scheme to provide all-in-one features, which makes the proposed scheme applicable in many scenarios as compared to its predecessors. In the future, one can extend the scheme using proxy-based mechanism to make it suitable for cloud-based environments. One can also extend the proposed scheme for the constant-length secret key to reduce the complexity.

References

[1] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key

Cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

[2] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," Proc. of Workshop on the Theory and Application of Cryptographic Techniques (CRYPTO 1984), vol. 196, pp. 47–53, 1984.

[3] A. Sahai and B. Waters, "Fuzzy Identity-based Encryption," Proc. of the Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques (UROCRYPT 2005), vol. 3494, pp. 457–473, 2005.

[4] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," Proc. of the 13th ACM Conf. on Computer and Communications Security, pp. 89–98, DOI: 10.1145/1180405.1180418, 2006.

[5] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy Attribute-based Encryption," Proc. of the IEEE Symposium on Security and Privacy (SP'07), pp. 321–334, Berkeley, CA, USA, 2007.

[6] M. Chase, "Multi-authority Attribute Based Encryption," Proc. of Theory of Cryptography Conference (TCC 2007), Part of the Lecture Notes in Computer Science Book Series, vol. 4392, pp. 515–534, 2007.

[7] S. Muller, S. Katzenbeisser and C. Eckert, "On Multi-authority Ciphertext-policy Attribute-based Encryption," Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.

[8] N. Gorasia, R. R. Srikanth, N. Doshi and J. Rupareliya, "Improving Security in Multi Authority Attribute Based Encryption with Fast Decryption," Procedia Computer Science, vol. 79, DOI: 10.1016/j.procs.2016.03.080, 2016.

[9] V. Božović, D. Socek, R. Steinwandt and V. I. Villányi, "Multi-authority Attribute-based Encryption with Honest-but-curious Central Authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[10] H. Lin, Z. Cao, X. Liang and J. Shao, "Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority," Proc. of the Int. Conf. on Cryptology in India, pp. 426–436, 2008.

[11] X. Zhang and Y. Yin, "Research on Digital Copyright Management System Based on Blockchain Technology," Proc. of the IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pp. 2093–2097, Chengdu, China, 2019.

[12] Z. Xu, J. Shen, P. Luo and F. Liang, "PVcon: Localizing Hidden Concurrency Errors with Prediction and Verification," IEEE Access, vol. 8, pp. 165373–165386, 2020.

[13] J. Shen, X. Deng and Z. Xu, "Multi-security-level Cloud Storage System Based on Improved Proxy Re-encryption," EURASIP J. on Wireless Communication and Networking, vol. 2019, no. 1, p. 277, 2019.

[14] Z. Xu, J. Shen, F. Liang and Y. Chen, "Fine-grained Access Control Scheme Based on Improved Proxy Re-encryption in Cloud," J. Adv. Comput. Intell. Intell. Informatics, vol. 25, no. 2, pp. 170–176, 2021.

[15] G. Pareek and B. R. Purushothama, "KAPRE: Key-aggregate Proxy Re-encryption for Secure and Flexible Data Sharing in Cloud Storage," J. of Information Security and Applications, vol. 63, p. 103009, 2021.

[16] R. Kothari, N. Choudhary and K. Jain, "CP-ABE Scheme with Decryption Keys of Constant Size Using ECC with Expressive Threshold Access Structure," Proc. of Emerging Trends in Data Driven Computing and Communications, Part of the Studies in Autonomic, Data-driven and Industrial Computing Book Series, Springer, pp. 15–36, 2021.

[17] Z. Zhang, W. Zhang and Z. Qin, "Fully Constant-size CP-ABE with Privacy-preserving Outsourced Decryption for Lightweight Devices in Cloud-assisted IoT," Security and Commun. Networks, vol. 2021, Article ID 6676862, DOI: 10.1155/2021/6676862, 2021.

[18] Z. Zhang and S. Zhou, "A Decentralized Strongly Secure Attribute-based Encryption and Authentication Scheme for Distributed Internet of Mobile Things," Computer Networks, vol. 201, p. 108553, 2021.

[19] W. Yang, R. Wang, Z. Guan, L. Wu, X. Du and M. Guizani, "A Lightweight Attribute Based Encryption Scheme with Constant Size Ciphertext for Internet of Things," Proc. of the IEEE Int. Conf. on Communications (ICC 2020), 2020, pp. 1–6, Dublin, Ireland, 2020.

20] Y. Zhang, J. Li and H. Yan, "Constant Size Ciphertext Distributed CP-ABE Scheme with Privacy Protection and Fully Hiding Access Structure," IEEE Access, vol. 7, pp. 47982–47990, 2019.

[21] S. F. Tan and A. Samsudin, "Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey," Sensors, vol. 21, no. 19, DOI: 10.3390/s21196647, 2021.

[22] C. Ge, Z. Liu, J. Xia and L. Fang, "Revocable Identity-based Broadcast Proxy Re-encryption for Data Sharing in Clouds," IEEE Trans. on Dependable and Secure Comp., vol. 18, no. 3, pp. 1214–1226, 2019.

[23] L. Fang et al., "A Secure and Authenticated Mobile Payment Protocol against off-site Attack Strategy," IEEE Trans. on Dependable and Secure Computing, In Press, DOI: 10.1109/TDSC.2021.3102099, 2021.

[24] C. Ge, W. Susilo, J. Baek et al., "Revocable Attribute-based Encryption with Data Integrity in Clouds," IEEE Trans. on Dependable and Secure Computing, DOI: 10.1109/TDSC.2021.3065999, 2021.

[25] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia and L. Fang, "A Verifiable and Fair Attribute-based Proxy Re-encryption Scheme for Data Sharing in Clouds," IEEE Trans. on Dependable and Secure Computing, In Press, DOI: 10.1109/TDSC.2021.3076580, 2021.

[26] C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski and L. Fang, "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing," IEEE Trans. on Dependable and Secure Computing, vol. 18, no. 6, pp. 2787–2800, 2020.

[27] F. Guo, Y. Mu, W. Susilo, D. S. Wong and V. Varadharajan, "CP-ABE with Constant-size Keys for Lightweight Devices," IEEE Trans. on Inf. Forensics and Security, vol. 9, no. 5, pp. 763–771, 2014.

[28] Y. Chen, L. Song and G. Yang, "Attribute-based Access Control for Multi-authority Systems with Constant Size Ciphertext in Cloud Computing," China Communications, vol. 13, no. 2, pp. 146-162, 2016.
[29] W. Susilo, G. Yang, F. Guo and Q. Huang, "Constant-size Ciphertexts in Threshold Attribute-based Eencryption without Dummy Attributes," Information Sciences, vol. 429, pp. 349–360, 2018.
[30] A. Lewko and B. Waters, "Decentralizing Attribute-based Encryption," Proc. of the Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), vol. 6632, pp. 568–588, 2011.
[31] S. Müller, S. Katzenbeisser and C. Eckert, "Distributed Attribute-based Encryption," Proc. of the Int. Conf. on Information Security and Cryptology (ICISC 2008), vol. 5461, pp. 20–36, 2008.
[32] M. Blaze, G. Bleumer and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," Proc. of the Int. Conf. on the Theory and Applications of Cryptographic Techniques, vol. 1403, pp. 127–144, 1998.
[33] M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol. 80, no. 1, pp. 54–63, 1997.
[34] G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006.
[35] M. Green and G. Ateniese, "Identity-based Proxy Re-encryption," Proc. of the Int. Conf. on Applied Cryptography and Network Security (ACNS 2007), vol. 4521, pp. 288–306, 2007.
[36] T. Matsuo, "Proxy Re-encryption Systems for Identity-based Encryption," Proc. of the International Conference on Pairing-based Cryptography (Pairing 2007), vol. 4575, pp. 247–267, 2007.
[37] S. Guo, Y. Zeng, J. Wei and Q. Xu, "Attribute-based Re-encryption Scheme in the Standard Model," Wuhan Univ. J. Nat. Sci., vol. 13, no. 5, pp. 621–625, 2008.
[38] X. Liang, Z. Cao, H. Lin and J. Shao, "Attribute Based Proxy Re-encryption with Delegating Capabilities," Proc. of the 4th Int. Symp. on Information, Computer and Communications Security, pp. 276–286, 2009.
[39] L. Ibraimi, M. Asim and M. Petković, "An Encryption Scheme for a Secure Policy Updating," Proc. of the Int. Conf. on E-Business and Telecommunications, pp. 304–318, DOI: 10.5220/0002994703990408, 2010.
[40] S. Luo, J. Hu and Z. Chen, "Ciphertext Policy Attribute-based Proxy Re-encryption," Proc. of the Int. Conf. on Information and Communications Security (ICICS 2010), vol. 6476, pp. 401–415, 2010.
[41] K. Emura et al., "A Ciphertext-policy Attribute-based Encryption Scheme with Constant Ciphertext Length," Proc. of the Int. Conf. on Inform. Security Practice and Experience, vol. 5451, pp. 13–23, 2009.
[42] J. Herranz, F. Laguillaumie and C. Ràfols, "Constant Size Ciphertexts in Threshold Attribute-based Encryption," Proc. of the Int. Workshop on Public Key Cryptography (PKC), vol. 6056, pp. 19–34, 2010.
[43] C. Delerablée and D. Pointcheval, "Dynamic Threshold Public-key Encryption," Proc. of the Annual Int. Cryptology Conf., vol. 5157, pp. 317–334, [Online], Available: https://hal.inria.fr/inria-00419154, 2008.

ملخص البحث:

يعدّ التّشفير تقنيةً يتمّ بموجبها تحويل نصٍّ عاديٍ الى نصٍّ مشفّر حتى لا يتمكن المهاجم من استعادة النصّ دون المفتاح السِّرّي. ويُعدّ التّشفير المرتكز على السياسة القائمة على السِّمات إحدى تقنيات التّشفير الموجهة نحو السِّمة التي تتمثل في أنّ المستخدم لا يمكنه فكّ تشفير الرّسالة إلّا إذا تمت تلْبية متطلبات سياسة السِّمات المذكورة في النصّ المشفّر من قِبل سِمات المفتاح السري للمستخدِم. في الدراسات السابقة، إرتجل المؤلفون التّقنية القائمة من أجل تحسين المخطط البسيط لسياسة التّشفير القائم على السِّمات. وحديثاً، في عام 2021، اقترح وانغ وآخرون سياسة التّشفير القائمة على السِّمات باستخدام إعادة التّشفير بالوكالة، وأشاروا الى فعاليتها مقارنةً بالتّقنيات السابقة. إلّا أنّها تتبع النّصّ المشفّر ذا الطّول المتغيّر، الذي يزداد فيه حجم النصّ المشفّر بزيادة عدد السِّمات. كذلك فإنّ تلك التّقنية تقود الى تكاليف تتعلّق بالحوسبة عند المستقبِل خلال فكّ التّشفير الذي يتمّ القيام به عبر أجهزة إنترنت الأشياء.

لذا، اقترحت في هذه الورقة طريقة محسَّنة للحصول على نصّ مشفّرثابت الطّول باستخدام إعادة التّشفير بالوكالة؛ من أجل تقليل وقْت الحوسبة والاتّصال. والجدير بالذّكر أنّ الطّريقة المقترحة تتّسم بالأمان تحت مسألة ديفي هلمان المتعلّقة بالقرارات ثنائية الخطّية.