Fine-Grained Encryption for Search and Rescue Operation on Internet of Things

Depeng Li
Department of Information and Computer Science
University of Hawaii at Manoa
Honolulu, HI, USA
depengli@hawaii.edu

Srinivas Sampalli
Faculty of Computer Science
Dalhousie University
Halifax, NS, Canada
srini@cs.dal.ca

Zeyar Aung
Computing and Information Science
Masdar Institute of Science and Technology
Abu Dhabi, UAE
zaung@masdar.ac.ae

John Williams and Abel Sanchez
Civil Engineering and Engineering Systems Division
Massachusetts Institute of Technology (MIT)
Cambridge, MA, USA
{jrw, doval}@mit.edu

***Abstract* – The search and rescue operation is an increasingly important Internet of Things (IoT) application in which the resource-constrained things play the rescue role. Recently, more and more countries/organizations participate in a rescue task. To make the task more effective, they should share their information with each other but different countries have assorted sharing policies. Our investigation shows that access control systems for current search and rescue operations are either coarse-grained or computationally heavy. It cannot satisfy the rescue operations since those things demand lightweight cryptographic operations and the participating countries require flexible policies to protect their classified data. We propose a fine-grained access control system which is not only secure but also efficient. The practical experiments are conducted and its results demonstrate the lightweight cost in simulation.**

Index Terms* – *Attributed-based encryption, Fine-grained, Internet of Things, Privacy preservation, Search and rescue.

I. INTRODUCTION

The Internet of Things (IoT) is becoming a new paradigm nowadays. In IoT, a variety of smart objects (things) interacts and communicates with the environment by exchanging the information. Its pervasive presence offers the ability to measure the contextual indicators and to facilitate information sharing via the connected networks [1]. IoT is an ideal solution for some applications, one of which is the emergency response service e.g. Search And Rescue (SAR) operations.

The SAR of the missing Malaysia Airline flight MH370 and 239 people on board, for example, had been conducted by more than twenty countries after its loss of connection since March 8, 2014 [2]. The security service, especially confidentiality, is critical for SAR in which fine-grained key management is highly demanded. The reasons are because 1) If being sent in clear text, the classified messages could easily be eavesdropped and gathered by terrorists who can launch the subsequent attacks more precisely by leveraging this critical information. 2) Countries that participate in rescue operations may prohibit sharing with other countries the classified information e.g. satellite imageries, radar maps / beacons, etc. There are similar regulations for personnel who even serve in the same country: some messages obtained by the air force should not be accessed by the civil servant in the government. A message m, for instance, could only be accessed by persons who satisfy the following requirements: *Req =“rank is higher than captain” AND “serve as an air force officer” AND “belongs to Malaysia air force”*. 3) Rescuees e.g. passengers and crews may have some private, sensitive information which should not be disclosed in public.

Although offering the security and especially the confidentiality service, some previous related studies [3], [4], [5], [6], [7] cannot protect the messages in a fine-grained way, or their key managements rely on the public key encryption which consumes heavy computational cost. Some researches [8], [9], [10], [11] are designed for Aeronautical Telecommunications Network (ATN) which facilitate the air-ground and air-air communications. They cannot be utilized in SAR scenarios directly.

In this paper, we aim at proposing a fine-grained encryption scheme for SAR based on the Attribute-Based Encryption (ABE) algorithm [12]. Our contributions are:

- As the best of our knowledge, our paper is the first to focus on the development of fine-grained security protection of SAR missions within IoT in which things are resource-constrained. Detailed experimental results are also provided.
- This paper offers the fine-grained confidentiality service based on ABE [12]. It enables the share of classified rescue information from different countries in a granular way.

II. BACKGROUNDS

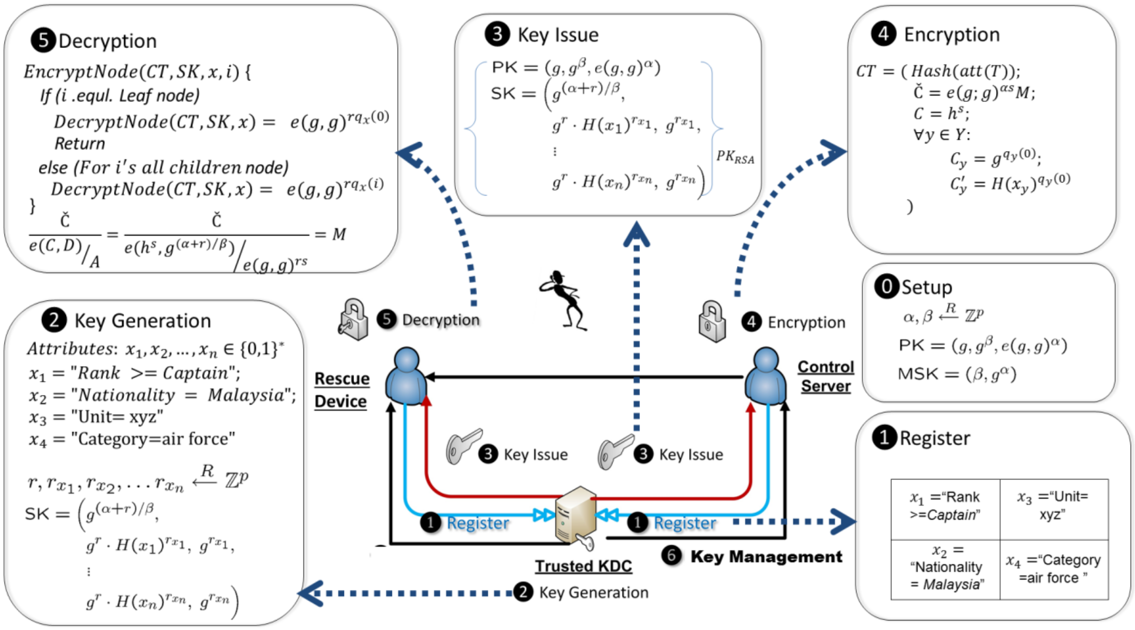
A. *Overview of ATN Networks and its Security Architecture*

A working group at the International Civil Aviation Organization (ICAO) defined the IP-based (IPv6) Aeronautical Telecommunications Network (ATN/IP) which is deployed in ground-ground networks, air-ground access networks and on the airborne (on-board) network itself [8], [9]. In ATNs, the direct computer-to-computer communications improve overall aircraft routing efficiency and minimize the workload of pilots and controllers [10].

In [10], [11], the shared secret-key establishment scheme is proposed to protect ground-air and ground-ground communication. It consists of two phases: 1) hybrid key establishment and 2) utilization of symmetric Message Authentication Code (MAC) to protect the application exchange.

B. Bilinear map

Bilinear map works as the basis of our approach. $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ are a cyclic additive group and a cyclic multiplication group


5 Decryption
$EncryptNode(CT,SK,x,i)$ {
If (i .equl. Leaf node)
$DecryptNode(CT,SK,x) = e(g,g)^{rq_x(0)}$
Return
else (For i's all children node)
$DecryptNode(CT,SK,x) = e(g,g)^{rq_x(i)}$
}
$\frac{Č}{e(C,D)/A} = \frac{Č}{e(h^s, g^{(\alpha+r)/\beta})/e(g,g)^{rs}} = M$
3 Key Issue
$PK = (g, g^{\beta}, e(g,g)^{\alpha})$
$SK = (g^{(\alpha+r)/\beta}, g^r \cdot H(x_1)^{r_{x_1}}, g^{r_{x_1}}, \vdots, g^r \cdot H(x_n)^{r_{x_n}}, g^{r_{x_n}})$
PK_{RSA}
4 Encryption
$CT = (Hash(att(T));$
$Č = e(g;g)^{\alpha s} M;$
$C = h^s;$
$\forall y \in Y:$
$C_y = g^{q_y(0)};$
$C'_y = H(x_y)^{q_y(0)}$
)
0 Setup
$\alpha, \beta \xleftarrow{R} \mathbb{Z}^p$
$PK = (g, g^{\beta}, e(g,g)^{\alpha})$
$MSK = (\beta, g^{\alpha})$
2 Key Generation
$Attributes: x_1, x_2, \ldots, x_n \in \{0,1\}^*$
x_1 = "Rank >= Captain";
x_2 = "Nationality = Malaysia";
x_3 = "Unit= xyz"
x_4 = "Category=air force"
$r, r_{x_1}, r_{x_2}, \ldots r_{x_n} \xleftarrow{R} \mathbb{Z}^p$
$SK = (g^{(\alpha+r)/\beta}, g^r \cdot H(x_1)^{r_{x_1}}, g^{r_{x_1}}, \vdots, g^r \cdot H(x_n)^{r_{x_n}}, g^{r_{x_n}})$
5 Decryption
4 Encryption
Rescue Device
Control Server
3 Key Issue
3 Key Issue
1 Register
1 Register
Trusted KDC
6 Key Management
2 Key Generation
1 Register

x_1 ="Rank >=Captain"	x_3 ="Unit= xyz"
x_2 = "Nationality = Malaysia"	x_4 ="Category =air force "

Figure 1. System Model

generated by P with the same order q, respectively. A mapping $\hat{e}: \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_{\mathbb{T}}$ satisfies the following properties:

- **Bilinear:** for all $u, v \in \mathbb{G}; a, b \in \mathbb{Z}$, we have $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$, where = is an equation;
- **Computable**: there exists an efficient computable algorithm to compute $\hat{e}(u, v), \forall u, v \in \mathbb{G}$;
- **Non-degenerate**: for the generator g of $\mathbb{G}$, q is the order of $\mathbb{G}$, we have $\hat{e}(g, g) \neq 1 \in \mathbb{G}_{\mathbb{T}}$;

C. Attribute-Based Encryption (ABE)

Unlike other schemes at the coarse-grained level which present subscribers the unique private key (e.g. the pairwise key or the group key), ABE [12] is fine-grained and it can establish a specific access control policy on who can decrypt the data. In the ABE system, users are associated with various attributes. The publisher can encrypt the plaintext and the ciphertext can be decrypted by subscribers only when their attributes match the access policy defined by the encryptor. ABE uses the *Access Tree* – an access structure is represented by the tree in which a leaf node is associated with a specific attribute and an intermediate node works as a "AND" or "OR" gate. We say that a set of attributes γ satisfies access tree if the root nodes' gate is true via recursively calculating roots' children nodes. We provide an example in Fig. 1. The details of ABE scheme is described below:

Access Tree – an access structure is represented by the tree in which a leaf node is associated with a specific attribute and an intermediate node works as an "AND" or "OR" gate. We say that a set of attributes γ satisfies access tree $\mathcal{T}$ if the root nodes' gate is true via recursively calculating roots' children nodes.

Setup()→ (PK, MK);
/* *public key PK; master secret key MK;* */

- Randomly selects two credentials

$$\alpha, \beta \xleftarrow{R} \mathbb{Z}_p \,;$$

- Calculates

$$PK = \left\{\mathbb{G};\ g;\ \ h = g^{\beta};\ \ f = g^{1/\beta};\ \ e(g,g)^{\alpha}\right\};$$
$$MK = (\,\beta,\ g^{\alpha}\,)\,;$$

Key Generation $(MK, S) \ \rightarrow SK$
/* MK master key; a set of attributes S; Secret key SK */

- Generate a random $r \xleftarrow{R} \mathbb{Z}_p$.

For each attribute $j \in S$,

- Choose corresponding random $r_j \xleftarrow{R} \mathbb{Z}_p$
- Calculate

$$SK = \{\ \ D = g^{\frac{\alpha+r}{\beta}};$$
$$\{\ \ \forall j \in S:$$
$$D_j = g^r \times H(j)^{r_j};\qquad D'_j = g^{r_j}\}\,;$$
$$\}$$

- For all $i \in \mathcal{T}$ the private keys components are:

$$D_i = g^{q(i)} T(i)^{r_i},$$
$$d_i = g^{r_i},$$
$$where \quad T(i) = g^{x^i} \prod_{j=1}^{n+1} t_j^{\Delta_{j,N}(i)}$$

Encrypt $(PK, M, T) \rightarrow \ \ CT$
/* *public key PK; message M ; tree access structure* $\mathcal{T}$ *Ciphertext CT*/*

- For each node x in the tree $\mathcal{T}$, select a corresponding polynomial q_x; then assign its degree: $d_x = k_x + 1$ where d_x is the degree of polynomial q_x and k_x is the threshold value of a node x.
- Beginning at the root node RT, first assigns $q_R(0) = s$

where $s \in \mathbb{Z}_p$ is a random. Second, randomly selects d_R other points for q_R to complement the definition of the polynomial q_R.

- Process the rest nodes x on the tree T by following the top-down manner: sets $q_x(0) = q_{parent(x)}(index(x))$ where function $parent(x)$ returns node x's parent node and function $index(x)$ returns the ordering number of node x's sibling nodes. Ordering numbers are assigned by x's parent node. Then, randomly selects d_x other points for q_x to complement the definition of the polynomial q_x.
- Ciphertext is output as:

$$CT = \{ \mathcal{T}; \tilde{C} = Me(g,g)^{\alpha s}; C = h^s;$$
$$\{ \ \forall y \in Y:$$
$$C_y = g^{q_y(0)}; C'_y = H(\boldsymbol{att}(y)^{q_y(0)}); \ \};$$
$$\}$$

$where$ function $\boldsymbol{att(x)}$ returns attributes associated with the leaf node;
$H: \{0,1\}^* \rightarrow \mathbb{Z}_p$ is a collision-resistant hash function;

Decrypt (PK, CT, SK) → M

/ Public Key PK: Ciphertext CT ; Private key SK; */*

The $DecryptNode(CT, SK, x)$ function below will be invoked recursively starting at root node RT to verify if the access tree T can be satisfied by S:

- If the node x is a leaf node, set $i = \boldsymbol{att}(x)$;

If $i \notin S$,
$DecryptNode(CT, SK, x) = \perp$
If $i \in S$,
$DecryptNode(CT, SK, x)$

$$= \frac{e(D_i, C_x)}{e(D'_i, C'_x)} = \frac{e\left(g^r \cdot H(i)^{r_i}, g^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})}$$
$$= \frac{e\left(g^r, g^{q_x(0)}\right) \cdot e\left(H(i)^{r_i}, g^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})}$$
$$= e(g,g)^{rq_x(0)}$$

- If the node x is not a leaf node,

For all nodes z which are node x's children nodes, call function $F_z = DecryptNode(CT, SK, z)$. Assign S_x with an arbitrary k_x −sized set of child nodes in such a way that $F_z \neq \perp$. If we cannot find such set, it means that the node cannot be satisfied, and the function returns ⊥.

Otherwise, calculate:

$$F_x = \prod_{z \in S_x} F_z^{\Delta_{i,s'_x(0)}} = \prod_{z \in S_x} \left(e(g,g)^{r \cdot q_z(0)}\right)^{\Delta_{i,s'_x(0)}}$$
$$= \prod_{z \in S_x} \left(e(g,g)^{r \cdot q_{parent(z)(index(x))}}\right)^{\Delta_{i,s'_x(0)}}$$
$$= \prod_{z \in S_x} (e(g,g))^{r \cdot q_x(i) \cdot \Delta_{i,s'_x(0)}} = e(g,g)^{r \cdot q_x(i)}$$

$where\ i = index(z)$ and $S'_x = \{index(z): z \in S_x\}$
and $\Delta_{i,s'_x(0)} = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$

- Decrypt ciphertext

$$\frac{\check{C}}{e(C,D) / A} = \frac{Me(g,g)^{\alpha s}}{e(h^s, g^{(\alpha+r)/\beta}) / e(g,g)^{rs}} = M$$

(where A = DecryptNode(CT,SK,R))

III. Related Works

Let us take a look at previous related studies which focus on the security of SAR or emergence and rescue operations. A. Michalas *et al.* in [3] proposed the SETS protocol to secure the communication between users. Before sharing the emergency information, SETS requires the validation from the certificate authority for each request from any users. Upon the successful authentication, the users can send the information encrypted by public/private keys. In [4], A. A. Bakar *et al.* proposed architecture, part of which concerns access control models. In [5], K. Lorincz *et al.* introduced security architecture for sensor-based emergency response in which the elliptic curve public key system is selected to provide security service. In [6], M. Pužar *et al.* proposed the SKiMPy protocol which uses a symmetric shared key. It designed a new group key management which can keep out unauthorized nodes. In [7], SMOCK key management was proposed to secure communication in mission-critical networks which can be used in emergency response and / or recovery. In SMOCK, a small number of cryptographic keys are pre-stored off-line at individual nodes. To enlarge its scalability, public-private key pairs are combined into the protocol. We find that previous researches relying on the group key or public/private key schemes are not the best choice for SAR. Refer to section IV for discussion.

In addition to the ATN security mechanism [10], [11], a few IP communication protocols were proposed for aeronautical communications. In [8], how different protocols can be used to solve the IP mobility problem within the aeronautical environment is surveyed. In [9], the cyber–physical system security for aeronautical communications is analyzed. How the cyber–physical system integrates into current and future aviation as well as ATN communication system is systemically studied.

IV. Problem Descriptions

A. Notations

Before proceeding, we summarize the notations used in the sequel. In SAR scenarios, we distinguish five roles, the authority, the rescuer, the rescuee, the third-party and the message exchanged among them.

Let A_x (where $x = 1, \dots n$) denote an authority which is an organization that coordinates SAR operations in a given context, such as the governmental organizations or the air force. The Vietnam rescue team, for example, can be denoted as A_i where i is a random number. The set of authorities can be denoted as

$$SAR = \{\mathrm{A}_1, \dots, \mathrm{A}_\mathrm{n}\} \quad (1)$$

$$\textit{where n is the number of authorities}$$

Let $x_{j \cdot A_i}$ (where $j = 1, \dots m_\mathrm{i}$) denote one rescue member belonging to authority A_i in which $|A_i| = m_i$ (means that there are m_i rescue members in authority A_i). As a member of the organization A_i, $x_{j \cdot A_i}$ is asked to provide its services at a scene of a SAR with main goal the successful resolution. The set of members for an authority A_i is denoted as $\{x_{1 \cdot A_i}, x_{2 \cdot A_i}, \dots, x_{j \cdot A_i}, \dots, x_{m_\mathrm{i} \cdot A_i}\}$. $x_{j \cdot A_i}$ can be an aircraft, a ship, a satellite or even a underwater rescue robot which plays the rescuer role on behalf of $\mathrm{A_i}$, an authority. Note that the rescue device is installed at each $x_{j \cdot A_i}$ if any. All rescue members from each rescue authority for a SAR operation, e.g. MH370 rescue mission, can be denoted as

$$SAR = \begin{pmatrix} A_1 \\ \cdot \\ \cdot \\ \cdot \\ A_n \end{pmatrix} = \begin{pmatrix} x_{1 \cdot A_1} & \cdots & x_{m_1 \cdot A_1} \\ \vdots & \ddots & \vdots \\ x_{1 \cdot A_n} & \cdots & x_{m_n \cdot A_n} \end{pmatrix} \quad (2)$$

$$\text{where } \{\ \forall x_{ij} : x_{ij} \in A_i \text{ and } \forall A_i \text{: } A_i \in SAR\}$$

Let y_i denote a rescue which can be a missing airplane / ship, a passenger on board, etc. Other missing issues e.g. the passengers' personal luggage or the debris of the missed plane / ship, for example, also belong to this category.

Let t_i denote the third-parties which do not belong to any authority A_i in the SAR operation but they take their pre-defined commitment. Internet and its routers, for example, are not treated as the rescue members belonging to any authority but they relay and forward packets to their destinations.

Let d_i be the data captured during the SAR operation. Any rescue members, $x_{j \cdot A_i}$, e.g. the aircraft, ship, radar, or satellite take photos, record videos, or measure environmental parameters which can be treated as the d_i, the data.

B. Network Topology for Search and Rescue Operations

During SAR operations, each rescue member, $x_{j \cdot A_i}$, connects with its own authority A_i, directly or indirectly. There should be communication connection between each authority, A_i. Partial data share is desirable depending on each government's regulations which, sometimes, may change. The SAR network connections can be denoted as $M = (\{u_1; \cdots; u_{|M|}\}; L)$ where u_i is a node (e.g. a rescue member $x_{j \cdot A_i}$, a rescue authority A_i, or a third-party intermediate node t_i) and L is the set of communication channels established by two neighbor nodes. So, M can be modeled as $G = (\{v_1; \cdots; v_{|M|}\}, E, W(e))$, a connected and directed graph, where vertex v_i corresponds to node u_i in M, E denotes the set of edges in L and W is the set of weights for all edges. There is an edge in E between a pair of vertices v_i and v_j if nodes u_i and u_j in M enable successful communication directly.

C. Scope, Security Assumption and Adversary Model

Adversary Model*:* like other researches in areas of confidentiality service, we follow the semi-honest adversary model in which each rescue member $x_{j \cdot A_i}$ (e.g. devices on the ship, aircraft, etc.) and third-party intermediate nodes, t_i, obeys ATN network communication mechanism. Meanwhile they are also curious about messages they learn (or share) and have the intension to combine these information if possible. Therefore, any participating rescue member, $x_{j \cdot A_i}$, should relay packets and also intend to uncover others' secret by studying secret messages received.

Scope and Security Assumption: Our solution mainly focuses on the confidentiality service for communication data d_i sent back and forth between rescue member $x_{j \cdot A_i}$ and servers. We assume the availability of PKI [13] deployed in IoT. Other security properties such as integrity and authentication services [14] are also important but beyond this paper's scope. The two ends of communication channels can be vulnerable: there are some attacks against rescue member $x_{j \cdot A_i}$ and the servers can be compromised. However, due to the limited space of this paper, the trustworthiness of server and the physical security of rescue member $x_{j \cdot A_i}$ are out of the scope of this research.

D. Problem Description

When the distress or imminent danger event happens, the authority will be noticed via requests. The official SAR operation is lunched after the request is legitimately proved.

During the SAR operations, each rescue member $x_{j \cdot A_i}$ captures information d_i (e.g. video, audio, photo, alarm, etc.) which may be related with the rescuee y_i. After been preprocessed by the rescue member $x_{j \cdot A_i}$ (this step may pass), d_i is sent back by $x_{j \cdot A_i}$ to its own authority A_i or to other rescue members, $x_{k \cdot A_i}$or the ones in different authorities, $x_{k \cdot A_j}$ where $i \neq j \neq k$. However, d_i, the classified information could be eavesdropped or captured by third-party, t_i. Some countries prohibit sending the classified information in clear text. The confidentiality is mandatory for SAR operations.

Example I:

Terrorists, a third-party t_i, capture the rescue message d_i which is forwarded via wireless communication channels or is sent through the Internet. d_i can be the secret information about airplanes, ships, satellites, radars or public services. After obtaining this critical information, the terrorist redesign their methods/strategies to conduct more dangerous attacks.

Example II:

The SAR video d_i contains rescuee's personal, sensitive information. If d_i is transmitted in the public communication channels, it is possible that the video is captured. It leaks the rescuee's privacy.

The previous related researches deploy cryptographic schemes (e.g. public/private key, group key) to provide the confidentiality service. They are introduced in section II and III. However, they may be unsuitable for SAR operations. Refer to section VII for detailed discussion and analyses.

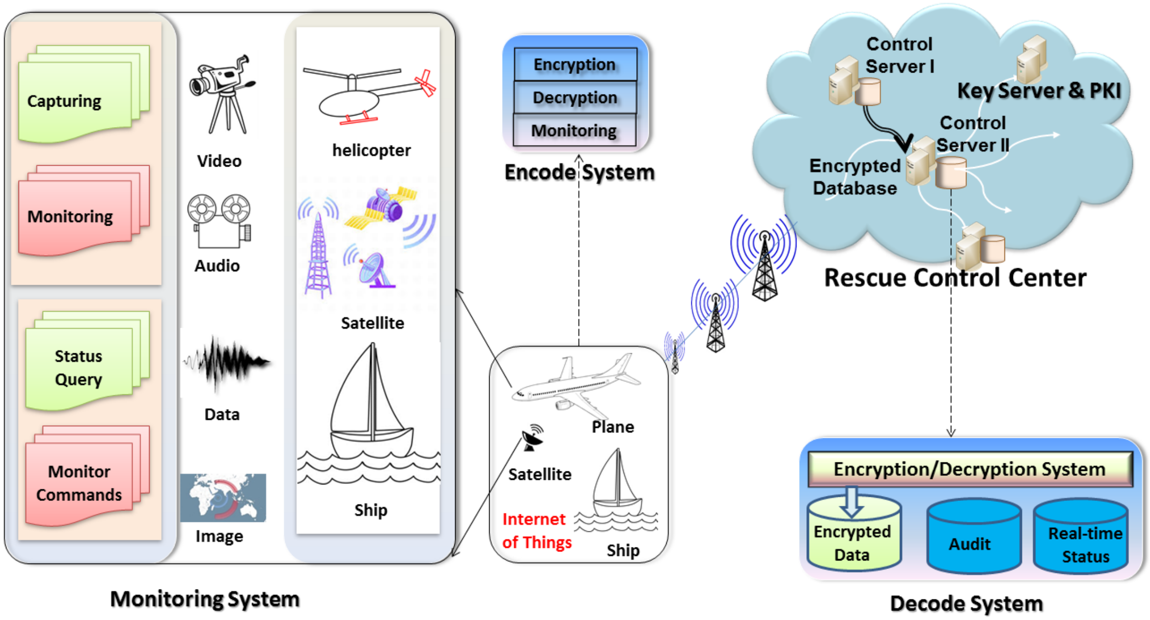


Figure 2. SAR System Architecture

V. SAR System With Confidentiality Service

A. System Overview

The goal of our solution is to prevent rescue information from exposures in an efficient, fine-grained way while satisfying the scalability, time-critical requirements of SAR.

As depicted in Fig. 1, there are three participants in our system: rescue devices (things) installed on rescue members, $x_{j \cdot A_i}$, control servers hosted by each authority, $\mathrm{A_i}$, and trusted KDC hosted by the SAR operation. In our system, both the control server and the KDC are located in the cloud. But they can also be installed in the command center of SAR operations. To protect the crucial rescue messages which are sent from the devices to the control server and vice versa via wireless channels, we adopt an ABE encryption system. The KDC's responsibility is to issue ABE keys to control servers and rescue devices.

In our system, it is crucial that the rescue devices or the control server can efficiently encrypt the rescue information, d_i by a policy written over attributes to accomplish SAR tasks. Other rescue devices and control servers can decrypt ciphertext in an efficient manner if its private key reflects the set of attributes which exactly satisfy the policy specified by the ciphertext.

A detailed view about how our system adopts the ABE cryptography system is illustrated in Fig. 1: at setup ⓿ phase, ABE Public Key (PK) and ABE Master Secret Key (MSK) are generated by the trusted KDC deployed in the cloud or the command center. The next step for every participant (the things e.g. rescue devices) is to register ❶ with their own attribute sets. For example, a rescue device provides attributes: { ***country***: *Malaysia;* ***rescue member type***: *aircraft,* ***ID***: *1234-56;* ***level***: *captain*}. After that, following the successful authorization, the corresponding ABE Secret Key (SK) will be generated ❷ by KDC. Thereafter, every rescue device is issued ❸ its SK and the public key (PK) by KDC in a secure channel (e.g. encrypted by the rescue devices' RSA public keys). The control server receives the public keys (PK) via secured channels. Then, plaintext can be encrypted ❹ by the rescue device with the public keys (PK) and attribute sets. The rescue device multicasts ciphertext to control servers and to other rescue devices, which, in turn, can decrypt ❺ the ciphertext if the reflecting attribute sets match with attributes of the SAR operations.

B. Protocol Design

Our protocol protects classified or sensitive data transferred in SAR operations via integrating the ABE encryption and in conformance with regulations of authorities in SAR operations.

Before the execution of our protocol, some pre-operations should be accomplished: the trusted KDC setups the public key (*PK*) and master key (*MSK*), registers attributes and calculates ABE secret key (*SK*) for all participates, e.g. rescue devices, control servers, etc. Each node is issued *PK* and its own *SK*.

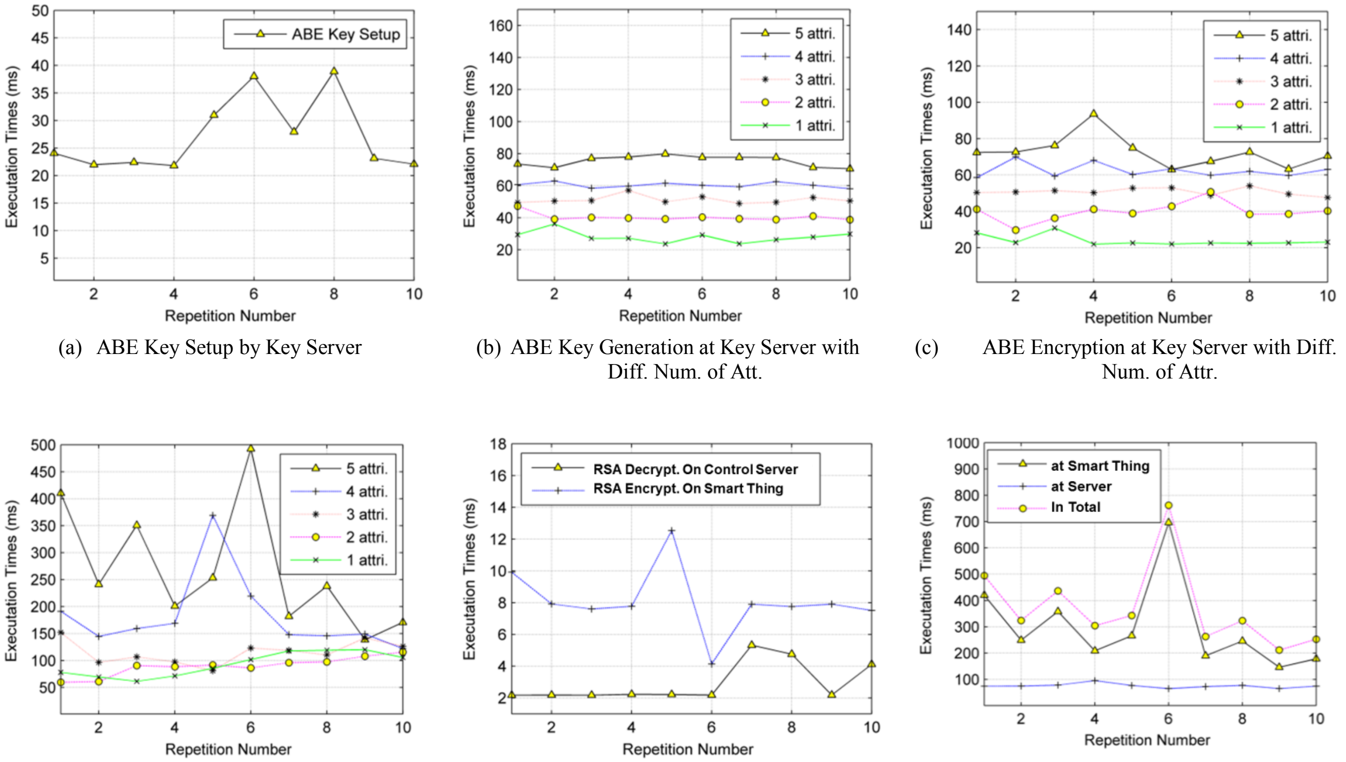
In our protocol, the rescue device (thing), $x_{j \cdot A_i}$ sends to other rescue devices and the control servers the captured data in ciphertext encrypted by the ABE encryption algorithm with public key PK and corresponding attributes ATT_i. Each control server or rescue device decrypts the ciphertext by using its own secret key $SK_{x_{j \cdot A_i}}$ if its own attributes $attr_{x_{j \cdot A_i}}$ matches with ATT_i.

$$x_{j \cdot A_i} \xrightarrow{FWD} x_{k \cdot A_i} \ or\ x_{j \cdot A_t} \ or\ \mathrm{A_i} \ or\ \mathrm{A_t}\text{:}\ Enc\left(d_i, SK_{x_{j \cdot A_i}}; ATT\right);$$

$$x_{k \cdot A_i} \ or\ x_{j \cdot A_t} \ or\ \mathrm{A_i} \ or\ \mathrm{A_t}\text{:}\quad Decryt(Cipher, SK, attr_{x_{j \cdot A_i}});$$

where Enc is the ABE encrypt Alg and Decrypt is decryption

The rescue information transmitted in our protocol requires not only confidentiality but authentication and integrity services. They can be supported by digital signature technology and one-way hash function [13], [14].



(a) ABE Key Setup by Key Server

(b) ABE Key Generation at Key Server with Diff. Num. of Att.

(c) ABE Encryption at Key Server with Diff. Num. of Attr.

(d) ABE Decryption at Smart Things with Diff. Num. Attr.

(e) RSA Public Key Encryption and Decryption

(f) Our protocol at Smart Things, Control Server and In total

Figure 3. Experimental Test Results of ABE Systems.

TABLE I - Performance Evaluation of ABE Components

Component		*Cost of ourABE Scheme*	
		Computation	*Commun.*
ABE Key	*Encry.*	$2E(1+\lvert \mathrm{AT}\rvert)$	$2(1+\lvert \mathrm{AT}\rvert)\lvert g\rvert$
	Decry.	$\leq (2P(1+\lvert \mathrm{AT}\rvert)$ $+E\cdot H\cdot \lvert S\rvert)$	$\lvert M\rvert$

E-Exponentiation; ***P***-Pairing; ***H***-Hashing; $\boldsymbol{g} \in \mathbb{G}$ (cyclic additive group); ***S*** - set of all rescue devices; $|\boldsymbol{S}|$- # of all rescue devices; $|\boldsymbol{M}|$ - Length of plaintext; $|\boldsymbol{AT}|$-# of Leaves in ciphertext Access Tree (AT).

TABLE II
Execution times of Cryptographic Components.

Items	Host	Times (ms)
ABE Setup	Trusted KDC	26.450
RSA Encrypt.	Rescue Device	8.096
RSA Decrypt.	Control Server	2.952

C. *SAR* System Architecture

The SAR operation utilizes a set of policies to protect the security of each participating authority and also to manage the system. An example is that a recuse device forwards classified rescue information to its own authority. If not authorized, personel who even belong to the same authority cannot access it. Meanwhile, rescue information should be partially shared among other authorities to make the rescue task efficient and effective. Therefore, if all rescue members and authorities are labeled with corresponding attributes, e.g. nationality, rank, type, ID number and others, at the key-issuing phase, the task can be easily achieved via sending out rescue information according to given policies. Hence, we require such security mechanisms that demonstrate the flexibility to accommodate the policy. In this subsection, we design and develop the SAR system with confidentiality services by utilizing our protocol as the cornerstone. It is a practical application. The rest will focus on its two fundamental subsystems, (1) Monitoring subsystem, (2) Encode and Decode subsystems, as illustrated in Fig. 2.

***Monitoring Subsystem*:**

The monitoring system captures the rescue data. There are a few formats of data: video, audio, photo, and text. They are generated from different input sources: 1) Aircraft: the helicopter or other airplanes can search the passengers or debris from the air. 2) Ship: ship rescues persons or gathers the issues from the water surface. 3) Submarine: submarine search the wreck. 4) Underwater robot: this kind of robot can also search the wreck. 5) Satellite: satellite provides the imagery. 6) Radar: radar captures the signal. Those entire devices gather the information, encrypt it by ABE algorithm and send it back to the command centre in ciphertext.

***Encode and Decode subsystems*:**

The Encode and Decode system are installed on the control server which is hosted by the command centre of the SAR operation or the cloud. It can decrypt the ciphertext and then encrypt it with other ABE keys and attributes. Meanwhile, the control centre should also validate ciphertext' authorization and verify their authentication, both of which will not be further described due to space limits.

VI. Performance Evaluation

In our application, the performance of *Encode* and *Decode* components at the rescue device and the server ends respectively dominates that of our system. They are of importance. The running time of the *Monitoring* component is not depends on our protocol. The communication roundtrip time from SAR field to the cloud depends on the bandwidth of Internet connection, the cloud performance and the Internet performance. We will not further discuss their performance due to space limits. In this subsection, our emphasis specifically focuses on *Encode* and *Decode* components' performance. We implement them based on Pairing-Based Cryptography (PBC) library [15] built on the GNU Multiple Precision arithmetic (GMP) library [16]: GMP library provides arbitrary precision arithmetic APIs which are invoked by PBC to support pairing-based cryptosystem. In our application, we use the pairing-friendly elliptic curves $E(\mathbb{F}_{2^{379}}): y^2 + y = x^3 + x + 1$ and $E(\mathbb{F}_p): y^2 = x^3 + Ax + B$ with a 512-bit prime. Furthermore, to satisfy the performance requirement, we deploys MNT elliptic curve to implement the ABE system. The control server / KDC and the rescue device in the experiment were both virtual machines hosted by Oracle's VirtualBox installing Ubuntu 11.10. The detailed configuration of KDC / Control Server: Memory-4GB; CPU-2.67GHz; Disk-7.9GB. Here is the rescue devices' configuration: 64MB Memory; 333MHz CPU (the configuration of an ARM Cortex 926EJS processor). It belongs to the high-end smart things.

In Fig. 3, we demonstrate these functions' performance when executing them on a control server and a low-end rescue device. We notice that ABE decryption at a rescue device and ABE encryption at a server executes less than 500*ms* and 100*ms*, respectively when the number of attributes is 5 or less. The overall execution time for our system takes less than 800 *ms* when the number of attributes is 5 or less. Consequently, our system is efficient. In Fig. 3, we illustrate the experimental results when ABE encryption algorithm is executed upon a high-end rescue device with the number of attributes ranging from 1 to 5. Our observation shows that the worst performance (*<= 800 ms*) is achieved when the number of attributes is 5. In [17], similar experiments are designed and conducted.

VII. Security Analysis

A. Discussion of Selection of Cryptographic Schemes

In this subsection, we discuss the advantage and dis-advantages of different cryptographic schemes when applying them to SAR operations.

Pairwise key: The pairwise key scheme demonstrates that its rate of data throughput is high and its key length is relatively short. However, it lacks scalability for multicast communication. Furthermore, it raises complicated key management issues: 1) A number of key pairs should be managed in a large network which results in the mandatory deployment of an unconditionally trusted TTP (Trusted Third Party). 2) It cannot provide scalability when the number of the rescue devices is large. The storage to save pair-key shared with other for each recuse device is huge. Most devices in SAR field are resource limited. It means that they lack of capacity of storage. 3) The frequency to refresh session keys is high – the worst case is that each communication session demands a new session key [13]. Hence, the key management of the pairwise key system requires expensive cost. It is not suitable for SAR operations.

Group Key Scheme: A pre-shared symmetric group key (e.g. [18]) can be used to encrypt / decrypt multicast packets among all group members (e.g. rescue devices). Its advantage is the secure, peer-to-peer data sharing but it is inflexible: to accommodate a policy, a Key Distribution Center (KDC) needs to enumerate all nodes matching the policy and then distribute partial keys / keys to each node in the list via secure channels. Rescue devices need calculate new group key. Expensive overhead in terms of computation and communication incurs at both the server end and the rescue device end. Meanwhile, a new policy introduces more creations of groups which are merely reusable. Therefore, we argue that there are substantial barriers to fully realize it in SAR operations when multi-nation rescues collaborate with each other.

ABE: in the ABE system, users are associated with various attributes. The publisher can encrypt the plaintext and the ciphertext can be decrypted by subscribers only when their attributes match the policy defined by the encryptor. Unlike the pairwise key or the group key, ABE is fine-grained. This satisfies the sharing requirement and follows the access control policies from different countries in SAR operations. However, ABE scheme demands heavy communication cost.

B. Analyses for our system

We critically examine our system based on generic bilinear group model and ABE schemes [12]. We argue that it meets the data confidentiality, namely, distinguishability under Chosen-Plaintext Attack (CPA) and adaptive Chosen-Ciphertext Attacks (CCA) as no efficient adversary with any reasonable probability can break our system. Without direct access to rescue data, attacks mentioned cannot succeed. The full proof is provided in appendix A.

Theorem 1*: Suppose the Decisional Bilinear Diffie-Hellman (D-BDH) assumption holds. There is no polynomial-time adversary $\mathcal{A}$* that *can break semantic security of ABE components in our system by CPA.*

Theorem 2*: Suppose the D-BDH assumption holds. There is no polynomial-time adversary $\mathcal{A}$ that can break semantic security of ABE components in our system by CCA.*

VIII. Conclusion and Future Works

Multinational search and rescue is an increasingly frequent task nowadays. It requests each participating authority sharing the captured data with each other in order to make the rescue as efficient as possible. However, different countries have different regulation prohibiting the share of the classified information. Fine-grained access control mechanism is highly demanded. Meanwhile, RAS operation is also an IoT application which enables the resource-limited rescue device participate on the rescue task. Those things cannot process the heavy cryptographic operations too frequently. This paper provides a fine-grained encryption scheme based on ABE algorithm. It satisfies the requirement aforementioned. The practical simulation results demonstrate that it is sufficient efficient for the SAR fieldwork.

References

[1] R. Rodrigo, J-Y. Zhou, and J. Lopez. "On the features and challenges of security and privacy in distributed Internet of Things." *Computer Networks*, Vol 57(10), PP:2266-2279, 2013.

[2] http:// www.malaysiaairlines.com/my/en/site/dark-site.html, April, 2014.

[3] A. Michalas, M. Bakopoulos, N. Komninos, and N. R. Prasad. Secure & trusted communication in emergency situations. In Proc. of *the 35th IEEE Sarnoff Symposium (SARNOFF)*, 21 - 22 May 2012, Newark, USA.

[4] A. Bakar, R. Ismail, AA. R. Hmad, and J. L. Manan, "Ensuring Data Privacy and Security in MANET: Case in Emergency Rescue Mission" *International Proceedings of Computer Science & Information Technology*, Vol 45. Pp. 165-169. 2012.

[5] K. Lorincz, D. J. Malan, T. R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh and S. Moulton. "Sensor networks for emergency response: challenges and opportunities." *IEEE Pervasive Computing*, Vol. 3, (4), Pp. 16-23, 2004.

[6] M. Pužar, J. Andersson, T. Plagemann, and Y. Roudier. "Skimpy: A simple key management protocol for manets in emergency and rescue operations". In *Security and Privacy in Ad-hoc and Sensor Networks*, pp. 14-26, 2005. Springer Berlin Heidelberg.

[7] W. He, Y. Huang, R. Sathyam, K. Nahrstedt, and W. C. Lee. "SMOCK: a scalable method of cryptographic key management for mission-critical wireless ad-hoc networks". *IEEE Transactions on Information Forensics and Security*, Vol.4(1), Pp:140-150. 2009.

[8] C. Bauer and M. Zitterbart. "A Survey of Protocols to Support IP Mobility in Aeronautical Communications", *IEEE Communications Survey & Tutorial*. VOL. 13(4), pp. 642-657, 2011.

[9] K. Sampigethaya, and R. Poovendran. "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport." *Proceedings of the IEEE*, Vol. 101(8), pp: 1834-1855, August 2013.

[10] M. L. Olive, "Efficient datalink security in a bandwidth-limited mobile environment-an overview of the Aeronautical Telecommunications Network (ATN) security concept". In *20th IEEE Digital Avionics Systems Conference, (DASC 01)*. Vol. 2, pp. 9.E.2-10, 2001.

[11] B. Stephens. "Security architecture for aeronautical networks". In *the 23rd International Conference Digital Avionics Systems Conference (DASC 04)*. Vol. 2, pp. 8.E.2.1-19. October, 2004.

[12] A. Lewko and B. Waters. Decentralizing attribute-based encryption. *In EUROCRYPT'11*, LNCS vol. 6632, pp. 568-588, 2011.

[13] A. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography, CRC Press, 1997.

[14] D. Li, , Z. Aung, J. R. Williams, and A. Sanchez. "Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis". *In Innovative Smart Grid Technologies (ISGT), IEEE PES*, (pp. 1-8). 2012.

[15] B. Lynn. The Stanford Pairing Based Crypto Library. http://crypto.stanford.edu/pbc/, Lasted accessed at April 13, 2013.

[16] http://gmplib.org/, Lasted accessed at Feb. 9, 2014

[17] D. Li, Z. Aung, J. Williams and A. Sanchez. "P3: Privacy preservation protocol for appliance control application". *IEEE SmartGridComm'12*, pp. 294-299, 2012.

[18] D. Li, and S. Sampalli. "An efficient contributory group rekeying scheme based on hash functions for MANETs." *In Network and Parallel Computing Workshops, IFIP Intern. Conf. on*, pp. 191-198. IEEE, 2007.

VIII Appendix

We know that if the ciphertext generated by the ABE scheme, the ciphertext delivered on communication channels of our system can provide data confidentiality service. Thus, in this subsection, we prove that ABE components in our system are secured sufficient.

We first describe the Decisional Bilinear Diffie-Hellman (D-BDH) assumption which is the cornerstone of our protocol's semantic security we are going to prove. Second, we prove the security of ABE components utilized in OUR system.

A. Assumptions

D-BDH Assumption

Let $a, b, c, z \overset{R}{\leftarrow} \mathbb{Z}_P$. There are two tuples: $(A = g^a, B = g^b, C = g^c, \hat{e}(g,g)^{abc})$ as well as $(A = g^a, B = g^b, C = g^c, \hat{e}(g,g)^z)$. The D-BDH assumption is that no probabilistic polynomial-time algorithm $\mathcal{A}$ can distinguish them with more than a negligible advantage. $\mathcal{A}$'s advantage:

$$\boldsymbol{Adv}_{\mathcal{A}} \quad = \quad |\Pr[\mathcal{A}(A,B,C,\hat{e}(g,g)^{abc}) = 0] \\ - \Pr[\mathcal{A}(A,B,C,\hat{e}(g,g)^{z}) = 0]\,|$$

B. Confidentiality service in ABE component of our system

Definition 2 (ABE-CPA) *Let* $\mathcal{P} = (\mathcal{S}, \mathcal{G}, \mathcal{E}, \mathcal{D})$ *be the ABE system in our system which encrypts/decrypts rescue messages* M *in transmission.* $\mathcal{S}$ *stands for ABE Setup,* $\mathcal{G}$ *for ABE key Generation,* $\mathcal{E}$ *for ABE Encryption and* $\mathcal{D}$ *for ABE Decryption. Let* $b \in \{0,1\}$. *Let* $\mathcal{A}$ *denote an adversary which can access the ciphertext, CT.*

We say that ABE-CPA holds the semantic security under chosen plaintext attacks launched by all polynomial time complexity adversaries $\mathcal{A}$ if $\mathcal{A}$'s $\boldsymbol{Adv}^{ABE-CPA-b}_{\mathcal{P},\ \mathcal{A}}(k)$ is negligible. The security model we are going to use follows the experiment listed below:

Experiment $\boldsymbol{Exp}^{ABE-CPA-b}_{\mathcal{PA},\mathcal{A}}(k)$

$$(PK, MSK) \overset{R}{\leftarrow} \mathcal{S}(k);$$

$$SK \overset{R}{\leftarrow} \mathcal{G}(MSK);$$

$$M_0 \overset{R}{\leftarrow} \{0,1\}^*; \qquad M_1 \overset{R}{\leftarrow} \{0,1\}^*;$$

$$CT_b \leftarrow \mathcal{E}(PK, M_b);$$

$$M_b \leftarrow \mathcal{A}(\text{find}, CT_b, M_0, M_1);$$

$$return: \quad g \leftarrow \mathcal{A}(\text{guess}, CT_b)$$

Briefly, there is a security game experiment with the parameter k where k is the bit length. An adversary $\mathcal{A}$ is given a set of public keys which can be used by $\mathcal{A}$ to generate any number of ciphertexts within polynomical bounds. The adversary $\mathcal{A}$ provides the challenger two messages M_0 and M_1. The challenger flips a fair coin $b \in \{0,1\}$ and encrypts M_b. During the experiment, the adversaries $\mathcal{A}$ can query for any private keys but is not allowed to use them for any decryption. At some time points, $\mathcal{A}$ outputs a guess bit $g \in \{0,1\}$. We say that $\mathcal{A}$ wins the game if $g = b$ but fails otherwise. Based on the experiment, the adversary $\mathcal{A}$'s advantages can be defined as:

$$\boldsymbol{Adv}_{\mathcal{P},\ \mathcal{A}}^{ABE-CPA-b}(k) = \Pr[\boldsymbol{Exp}_{\mathcal{P},\ \mathcal{A}}^{ABE-CPA-0}(k) = 0]$$
$$- \Pr[\boldsymbol{Exp}_{\mathcal{P},\ \mathcal{A}}^{ABE-CPA-1}(k) = 0]$$
$$= 2 \cdot \Pr\left[\boldsymbol{Exp}_{\mathcal{P},\ \mathcal{A}}^{ABE-CPA-0}(k) = 0\right] - 1$$

Theorem 1: *Suppose the Decisional Bilinear Diffie-Hellman (D-BDH) assumption holds. There is no polynomial-time adversary $\mathcal{A}$* that *can break semantic security of ABE components in our system by CPA.*

Proof. Suppose we have an adversary $\mathcal{A}$ with negligible advantage $\epsilon = \boldsymbol{Adv}_{\mathcal{P},\ \mathcal{A}}^{ABE-CPA-b}(\cdot)$ which can break ABE components in our system. A simulator $\boldsymbol{\mathcal{B}}$ which plays the Decisional BDH game with advantage ϵ processes in the following way:

Init Let the adversary $\mathcal{A}$ randomly chooses the set of challenge access structure, namely $\mathcal{T}^*$ which will be challenged upon.

Setup The simulator $\boldsymbol{\mathcal{B}}$ first randomly generates two credentials, $\alpha, \beta \overset{R}{\leftarrow} \mathbb{Z}_p$. After then, $\boldsymbol{\mathcal{B}}$ sends adversary $\mathcal{A}$ the following public keys:

$$PK \ = \left\{ \mathbb{G}_0;\ \ g;\ h = g^{\beta};\ f = g^{1/\beta};\ e(g,g)^{\alpha} \right\}$$

We then showcase how the simulator $\boldsymbol{\mathcal{B}}$ programs each node $y \in Y$ where $Y$are set of leaf nodes in the tree $\mathcal{T}^*$:
The simulator $\boldsymbol{\mathcal{B}}$ calculates the following pair, $\{\ C_y = g^{q_y(0)};\ C'_y = H(\boldsymbol{att}(y)^{q_y(0)} where$ $q_y(0)$ is based on $s \overset{R}{\leftarrow} \mathbb{Z}_p$. Note that $\boldsymbol{att}$**()** function returns the attributes which can be any string $\in \{0,1\}^*$.

Phase 1: $\forall i$, a string, the adversary $\mathcal{A}$ evaluates $H(i)$ by randomly generating $t_i \overset{R}{\leftarrow} \mathbb{Z}_p$. The simulator $\boldsymbol{\mathcal{B}}$ provides g^{t_i} in response. For the set s_j of attributes, the adversary $\mathcal{A}$ makes the j'th key generation query. In response, the simulator $\boldsymbol{\mathcal{B}}$ generates $r^{(j)} \overset{R}{\leftarrow} \mathbb{Z}_p$, $G \overset{R}{\leftarrow} \mathbb{Z}_p$ and $\forall i \in s_j$, $r_i^{(j)} \overset{R}{\leftarrow} \mathbb{Z}_p$. Then, the simulator $\boldsymbol{\mathcal{B}}$ calculates:

$$D = g^{\frac{\alpha + r^{(j)}}{\beta} G};$$

$$\text{and} \ \ \forall j \in s_j\text{:}\ \{\ \ D_i = g^{r^{(j)} + t_i r_i^{(j)}};\ \ D'_i = g^{r_i^{(j)}} \}$$

Then, they are sent to adversary $\mathcal{A}$.

Challenge: the adversary $\mathcal{A}$ submits two challenge message M_0 and M_1 and the access tree $\mathcal{T}^*$ to the simulator $\boldsymbol{\mathcal{B}}$**.** The simulator $\boldsymbol{\mathcal{B}}$ needs to computes one of $M_0\hat{e}(g,g)^{G\alpha s}$ and $M_1\hat{e}(g,g)^{G\alpha s}$; where $\alpha, s \overset{R}{\leftarrow} \mathbb{Z}_p$. Here, we consider a modified game where $\tilde{C}$ is calculated by either $\hat{e}(g,g)^{G\alpha s}$ or $\hat{e}(g,g)^{\theta}$ where $\theta \overset{R}{\leftarrow} \mathbb{Z}_p$ Therefore, the adversary $\mathcal{A}$ with advantage ϵ for ABE component in our system can be transformed into a new adversary with the advantage of $\epsilon/2$. To simplify, we will use the modified game from now on. Based on the notions aforementioned, the simulator $\boldsymbol{\mathcal{B}}$ processes the followings: First, $s \overset{R}{\leftarrow} \mathbb{Z}_p$. Then, the linear secret sharing scheme associated with access tree is used to construct share λ_i of s for all relevant attributes i. Third, the simulator $\boldsymbol{\mathcal{B}}$ choses $\theta \overset{R}{\leftarrow} \mathbb{Z}_p$. Fourth, the simulator $\boldsymbol{\mathcal{B}}$ flips a fair coin $\mu \in \{0,1\}$ which is beyond the awareness of adversary $\mathcal{A}$. At last, accomplish the following encryption:

$$\tilde{C} = M_{\mu} e(g,g)^{\theta};\quad C = h^{s};$$
$$\forall i \in Y\text{:}\ \ \{\ C_i = g^{\lambda_i}; C'_i = g^{t_i \lambda_i};\ \};$$

They will be sent to adversary $\mathcal{A}$.

Phase 2: the simulator $\boldsymbol{\mathcal{B}}$ repeats what it did in Phase 1.

Guess: the adversary $\mathcal{A}$ eventually submits a guess b of μ. If $b = \mu$ the simulator $\boldsymbol{\mathcal{B}}$ will output 0 to note that $T = e(g,g)^{\theta}$. If $b \neq \mu$, the simulator $\boldsymbol{\mathcal{B}}$ will output 1 which means that T is evaluated as a random group element of $\mathbb{G}_{\mathbb{T}}$. In case that T is the expected element for which the simulator $\boldsymbol{\mathcal{B}}$ provides a perfect simulation, we can deduce that:

$$P\,r\left[B\ \left(PK, D, D_i, T = e(g,g)^{\theta}\right) = 0\right] = {}^{1}\!/_{2} + Adv_{\mathcal{A}}$$

Otherwise, T is a random group element. It means that the adversary $\mathcal{A}$ cannot correctly decide which message M_{μ} is. Therefore, we have

$$Pr[B\ (PK, D, D_i, T = Random) = 0] = {}^{1}\!/_{2}$$

Consequently, the simulator $\boldsymbol{\mathcal{B}}$ plays the decisional BDH game with non-negligible advantage. ■

Theorem 2: *Suppose the D-BDH assumption holds. There is no polynomial-time adversary $\mathcal{A}$ that can break semantic security of ABE components in our system by CCA.*

Proof: The model utilized in Theorem 1 can easily be extended to prove CCA by allowing random oracle techniques for decryption in Phase 1 and Phase 2. ■