EMA-LAB: efficient multi authorisation level attribute based access control

Nesrine Kaaniche, Sana Belguith, Giovanni Russello

EMA-LAB: Efficient Multi Authorisation Level Attribute Based Access Control

Conference Paper · August 2018

CITATIONS
2

READS
160

3 authors, including:

Sana Belguith
University of Bristol
32 PUBLICATIONS **543** CITATIONS
SEE PROFILE

Giovanni Russello
University of Auckland
143 PUBLICATIONS **2,271** CITATIONS
SEE PROFILE

EMA-LAB: Efficient Multi Authorisation Level Attribute Based Access Control

Nesrine Kaaniche[1], Sana Belguith[2], and Giovanni Russello[2]

[1] SAMOVAR, Telecom SudParis,
University Paris-Saclay, France
[2] The Cyber Security Foundry,
The University of Auckland, New Zealand
nesrine.kaaniche@telecom-sudparis.eu,sbel452@aucklanduni.ac.nz,
g.russello@auckland.ac.nz

Abstract. Recent years have witnessed the trend of increasingly relying on remote and distributed infrastructures. This increases the complexity of access control to data, where access control policies should be flexible and distinguishable among users with different privileges. In this paper, we present EMA-LAB, a novel Multi Authorisation Level Attribute Based Access Control with short ciphertexts size. It relies on the usage of a constant-size threshold attribute based encryption scheme. The EMA-LAB scheme is multifold. First, it ensures a selective access to encrypted data with respect to different security levels. Second, the proposed construction protects the secrecy of enciphered contents against malicious adversaries, even in case of colluding users. Third, EMA-LAB relies on low computation and communication processes, mainly for resource-constrained devices, compared to most closely related schemes.

Keywords: multi-level threshold scheme · attribute based encryption with short ciphertext · access control.

1 Introduction

Nowadays, data sharing is gaining an expanding interest, mainly with the development of remote services and distributed infrastructures. It allows data owners to share their outsourced data among groups of users. However, many security concerns arise, as the outsourced data should be protected from unauthorized access. Thus, fine grained access privileges should be ensured, while preventing malicious access.

The increasing need and complexity of access control to outsourced data lead to the emergence of several encrypted access control schemes. Among these techniques, Attribute based Encryption (ABE) has appeared as a promising cryptographic technique which provides fine grained access control for outsourced data. ABE is used to encrypt data files with respect to an access policy associated with a set of attributes.

However, sharing data contents between different involved actors is often an issue, due to the complexity of access control policies' management. This issue becomes more complex when involved actors do not share the same access privileges to each part of the data file. Hence, different access levels need to be defined to allow authorized users to access different sub-parts of enciphered data. The translation of an access control structure into an equivalent multi-level policy remains the main challenging issue of encrypted access control mechanisms.

To protect some parts of data from unauthorised access, *redaction* techniques are applied to black out or remove these parts. Several redaction techniques have been proposed such as sanitizing schemes for digitally signed document, content extraction algorithms, redactable signatures and sanitizable signatures [1, 11]. These schemes rely on malleable cryptographic primitives such as chameleon hash functions to allow redactors having their own secret key to modify some parts of the originally encrypted or signed data file. Although these techniques allow selective access to some parts of data, they are not efficient with multi-level access privileges.

The multi level access control policies in ABE schemes have been recently explored [12]. In these schemes, data files are encrypted using a multi level access policy where users can access parts of these data w.r.t. their access level. Although these proposals ensure multi level access control, the communication and computation overhead as well as the bandwidth consumption increase exponentially with the number of attributes required in the aggregated access structure.

To save the storage cost of ciphertext and processing overhead of encryption, attribute based encryption schemes with constant ciphertext size have been introduced [2, 7, 9]. In these schemes, the size of the generated ciphertext does not depend on the number of attributes used on the threshold access policies, which presents an interesting feature mainly for resource-constrained devices.

Contributions — In this paper, we propose EMA-LAB, a new multi-threshold attribute based encryption scheme. First, it permits a selective access to enciphered data with respect to different threshold levels. Second, the size of the resulting ciphertext does not depend on the number of attributes involved in the access policy, which makes our scheme more suitable for bandwidth-limited applications. Third, it is proven secure under standard assumptions. Finally, EMA-LAB provides interesting performances compared to most closely related schemes.

Paper organization — the remainder of this paper is organized as follows. First, section 2 clarifies the problem statement and highlights security and functional requirements and section 3 discusses related works. Then, section 4 introduces EMA-LAB system and threat models. Section 5 presents complexity assumptions and mathematical background, and details EMA-LAB concrete construction. The security analysis of EMA-LAB is discussed in section 6. Finally, performances analysis is detailed in section 7 before concluding in section 8.

2 Motivating Scenario

Publish and subscribe (pub/sub) systems have been widely bared to ensure dissemination of data contents from publishers to interested subscribers [14]. Similar to most of existing outsourcing mechanisms, pub/sub systems raise serious security concerns, mainly related to published data access control. It is commonly agreed that emerging encryption techniques are good alternatives to protect data from unauthorised access, namely Attribute Based Encryption (ABE) schemes [3, 5].

Let us consider the following example depicted by Figure 1, where a company subscribing its employees to a finance news service. That is, each publication P is composed of several sub-parts p_i related to k different authorization levels such that each access level corresponds to l sub-parts of data (i.e., $P = \{\{p_i\}_{i\in[1,l]}\}_{l\in[1,k]}$).

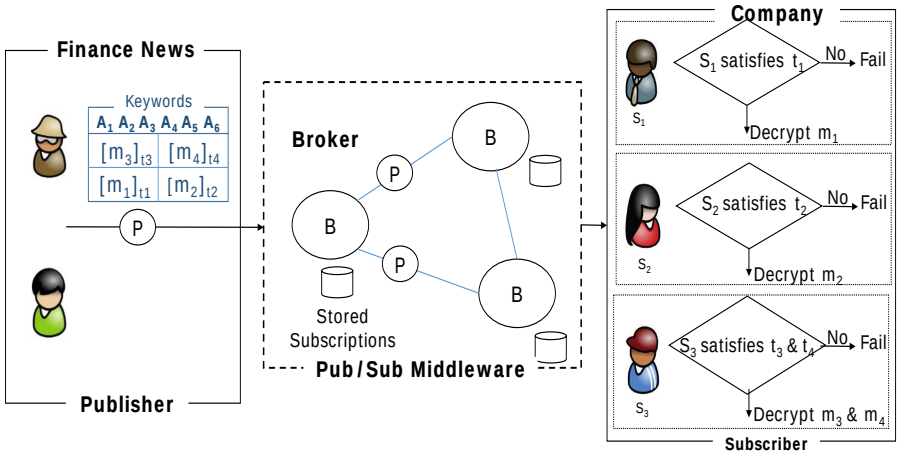

Fig. 1. Publish-Subscribe System Architecture

The subscribed employees can access received publications with respect to their authorisation level. Indeed, an employee who has only two interests can access a small amount of published data while a manager can access more subparts of data contents of the same publication. Obviously, the company's CEO can access the full publication. Thus, a multi level access control is defined as depicted by Figure 1. As mentioned above, publications should be encrypted before forwarding to the pub/sub middleware.

A naive solution [3] is to divide publications into several parts and encrypt them separately with respect to different security levels. However, this solution

[3] Note that the security of publications' keywords and subscribers' interests at the broker side while performing the matching feature is above the scope of this paper.

presents several drawbacks. First, it contradicts the decoupled feature of pub-/sub system as the publisher will be aware of the interests of the subscribers. Second, this solution incurs huge computation and communication overheads due to performing the encryption of the same data content several times, as well as defining several access structures, depending on redundant attributes (i.e., company's employees may share several attributes). Third, it removes the multi authorisation level feature as each subscriber will receive her related publication.

To support all these features with efficiency, we propose to design a multi threshold level ABE scheme. Thus, the proposed scheme EMA-LAB must fulfill the following properties:

- **R1. data confidentiality** – the proposed scheme has to protect the secrecy of encrypted data contents against malicious users, even in case of collusions.
- **R2. multi level access control** – our proposal should ensure flexible security policies among dynamic groups of users with different granted privileges.
- **R3. low processing cost** – the encryption algorithm should have a low computational complexity to minimize the impact of the security on the efficiency of data processing.
- **R4. low communication overhead** – our multi-level encrypted data file should be short-sized as the transmission overhead is important in the emerging infrastructure context.

3 ABE-Related Work

Attribute based Encryption (ABE) schemes are cryptographic primitives ensuring encrypted access control to data. In attribute based encryption schemes, user's private keys and ciphertexts are associated with an access policy or a set of attributes [6]. Thus, a data user is able to decrypt the ciphertext if his private key matches the ciphertext.

Although ABE ensures fine grained and flexible access control, the communication and computation overhead as well as the bandwidth consumption increase exponentially with the number of attributes required in the access policies. To countermeasure this limit, several ABE schemes with short or constant ciphertexts have been proposed [4,7,9]. Herranz et al. [9] have proposed the first constant size threshold attribute based encryption scheme. Indeed, the ciphertext size is constant and does not depend on the number of attributes involved in the threshold access policies. Later, Waters et al. [16] proposed an efficient attribute based encryption scheme with short ciphertext. However, the ciphertext size, the encryption and the decryption times increase linearly with the number of attributes involved in the access structure. Ge et al. [7] have proposed a constant size threshold attribute based encryption scheme. The authors used a different design strategy scheme in order to achieve security against chosen ciphertext attacks (CCA) in the standard model unlike Herranz et al. [9] scheme which is secure against chosen plaintext attacks (CPA). In [17], the authors propose a generic attribute-based data sharing system based on a hybrid mechanism

of CP-ABE and a symmetric encryption scheme. This scheme ensures efficient computation costs as well as reduced ciphertext size.

Although these schemes propose efficient solutions to protect outsourced data from unauthorized access, they are still inefficient with multi-level access policies, where users have to share the same data content with different access rights to distinct parts of the data file.

Wang et al. [15] have proposed an efficient file hierarchy attribute-based encryption scheme in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access structure. Kaaniche et al. [12] have introduced an encryption scheme based on attribute based mechanisms for multi-level access policies. This scheme ensures a selective access to data based on users' granted privileges. Practically, when a party encrypts a data file, she specifies an access structure and a certain number of security levels. Thus, a user is able to decrypt a sub-set of data blocks related to a security level k that users private keys satisfy the sub-set of attributes related to the k-security level.

Table 1. A comparison of ABE schemes.

Schemes	R1	R2	R3	R4
Herranz et al. [9]	✓	×	✓	✓
Waters et al. [16]	✓	×	✓	✓
Ge al. [7]	✓	×	✓	✓
Zhang et al. [17]	✓	×	✓	✓
Wang et al. [15]	✓	✓	×	×
Kaaniche et al. [12]	✓	✓	×	×
EMA-LAB	✓	✓	✓	✓

✓ and × indicate that the requirement is achieved or not, respectively.

The communication and computation overhead as well as the bandwidth consumption in the existing multi level ciphertext policy attribute based encryption [4,12] schemes increase exponentially with the number of attributes required in the multi level access policies. This motivates us to address the problem of constructing a multi level attribute based encryption scheme which introduces a short ciphertext size cost for multi level access control and data confidentiality.

4 Model Description

In this section, we first present the system model of EMA-LAB scheme. Then, we detail the security model.

4.1 System Model

We suppose that the encrypting entity $\mathcal{E}$ chooses a subset S from the attribute universe $\mathbb{U}$ and a set of thresholds $\{t_j\}$ such that $1 \leq t_j \leq l \leq |S|$, and $l \leq |\mathbb{T}|$

(i.e., $\mathbb{T}$ is the threshold universe supported by the system) to define his multi-threshold $(\{t_j\}_{\{1,\cdots,l\}}, S)$ access policy. Then, $\mathcal{U}$ encrypts the message $M \in \mathcal{M}$ (i.e., $\mathcal{M}$ is the message space), where $M = \{m_j\}_{\{1,\cdots,l\}}$ with respect to the policy $(\{t_j\}_{\{1,\cdots,l\}}, S)$.
Our multi-threshold attribute based encryption mechanism consists of four randomized algorithms: `setup`, `keygen`, `encrypt` and `decrypt`, defined as follows:

$\texttt{setup}(\xi) \rightarrow (\texttt{pp}, \texttt{msk})$ – the `setup` algorithm is performed by the central trusted authority. It takes as input a security parameter ξ. The `setup` algorithm outputs the public parameters `pp` and the master secret key `msk`.

$\texttt{encrypt}(\texttt{pp}, (\{t_j\}_{\{1,\cdots,l\}}, S), M) \rightarrow C$ – the encryption algorithm is performed by an encrypting entity $\mathcal{E}$. It takes as inputs the public parameters `pp`, the $(\{t_j\}_{\{1,\cdots,l\}}, S)$ multi level threshold access policy and the message M, defined as a set of sub-messages $M = \{m_j\}_{\{1,\cdots,l\}}$. This algorithm outputs an encrypted message referred to as C.

$\texttt{keygen}(\texttt{pp}, \texttt{msk}, A_{\mathcal{U}}) \rightarrow sk_{\mathcal{U}}$ – this randomized algorithm is executed by the trusted authority to derive the secret keys of the user $\mathcal{U}$ related to his set of attributes $A_{\mathcal{U}}$. Given the public parameters `pp`, the master secret key `msk` and an attribute set $A_{\mathcal{U}} \subset \mathbb{U}$ (i.e., $\mathbb{U}$ is the attribute universe) of the user $\mathcal{U}$. The algorithm outputs the user's secret key $sk_{\mathcal{U}}$ associated to the attribute set $A_{\mathcal{U}}$.

$\texttt{decrypt}(\texttt{pp}, sk_{\mathcal{U}}, A_{\mathcal{U}}, (\{t_j\}_{\{1,\cdots,l\}}, S), C) \rightarrow m_j$ – the decryption algorithm is executed by the user $\mathcal{U}$. It takes as inputs the public parameters `pp`, the user's private key $sk_{\mathcal{U}}$, the access policy $(\{t_j\}_{\{1,\cdots,l\}}, S)$ and the encrypted message C. The algorithm returns the message m_j if the user $\mathcal{U}$ has successfully obtained the secret key related to the t_j required attributes for deciphering the encrypted message, with respect to the threshold t_j. Otherwise, the algorithm outputs a reject symbol $\perp$.

Our EMA-LAB multi-threshold attribute based encryption scheme has to satisfy the **correctness property** defined hereafter as follows.
The correctness property requires that for all security parameter ξ, all attribute universe descriptions $\mathbb{U}$, all threshold universe $\mathbb{T}$, all $(\texttt{pp}, \texttt{msk}) \in \texttt{setup}(\xi)$, all domain entities $\mathcal{E}$, all $A_{\mathcal{E}} \subseteq \mathbb{U}$, all $sk_{\mathcal{E}} \in \texttt{keygen}(\texttt{pp}, \texttt{msk}, A_{\mathcal{E}})$, all $M \in \mathcal{M}$ defined as a set of sub-messages $M = \{m_j\}$, all $(\{t_j\}_{\{1,\cdots,l\}}, S) \in \mathcal{G}$ ($\mathcal{G}$ is the access policy space) and all $C \in \texttt{encrypt}(\texttt{pp}, (\{t_j\}_{\{1,\cdots,l\}}, S), M)$, if the decrypting entity $\mathcal{E}$ has successfully obtained the secret key related to the t_j required attributes for deciphering the encrypted message such that $|A_{\mathcal{E}} \cap S| \geq t_j$, the $\texttt{derypt}(\texttt{pp}, sk_{\mathcal{U}}, A_{\mathcal{E}}, (\{t_j\}_{\{1,\cdots,l\}}, S), C)$ outputs m_j with respected to the satisfied threshold t_j.

4.2 Security Model

For designing a secure multi-threshold attribute based encryption scheme, we consider malicious users (ie; subscribers in our motivating scenario 2), with respect to the indistinguishability property. The indistinguishability property means that if an adversary has some information about the plaintext, he should not learn about the ciphertext. This security notion requires the computational

impossibility to distinguish between two messages chosen by the adversary with a probability greater than a half. Indeed, in ABE schemes, the adversary may lead an attack against the indistinguishability property either on his own or through a collusion attack.

EMA-LAB is said to be indistinguishable against non-adaptive chosen ciphertext attacks if there is no probabilistic polynomial time (PPT) adversary that can win the Exp^{conf} security game with non-negligible advantage. The Exp^{conf} game is formally defined, between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ as follows:

INITIALISATION – $\mathcal{A}$ selects a set of encryption attributes S^* (i.e., S^* corresponds to the set of attributes specified for the general access policy) to be used for encrypting the challenge ciphertext, as a set of threshold values $\{t^*{}_j\}_{\{j\in[1,m]\}}$, where m is the number of threshold values. $\mathcal{A}$ sends $(\{t^*{}_j\}_{\{j\in[1,m]\}}, S^*)$ to $\mathcal{C}$.

SETUP – the challenger $\mathcal{C}$ runs the $\texttt{setup}(\xi)$ algorithm of the encryption scheme and sends the public parameters $\texttt{pp}$ to the adversary $\mathcal{A}$.

DECRYPTION QUERY PHASE – the adversary $\mathcal{A}$ can request, as many times as he wants, the following queries:

- $\texttt{keygen}$ – the adversary $\mathcal{A}$ queries, for each session i, an encryption attribute set $A_{\mathcal{A},i}$ with respect to a threshold $t^*{}_{k,i} \in \{t^*{}_j\}_{\{j\in[1,m]\}}$ where $|A_{\mathcal{A},i} \cap S^*| < t^*{}_{k,i}$. The challenger $\mathcal{C}$ answers by running the $\texttt{keygen}(\texttt{pp}, msk, A_{\mathcal{A},i})$ algorithm and sends the resulting secret key to the adversary $\mathcal{A}$, with respect to the required threshold $t^*{}_{k,i}$. The secret key is referred to as $sk_{\mathcal{A},i}$.
- $\texttt{decrypt}$ – the adversary $\mathcal{A}$ requests the decryption of C with respect to a threshold $t^*{}_{k,i}$, while considering the encryption attribute set $A_{\mathcal{A},i}$. The challenger $\mathcal{C}$ executes the $\texttt{keygen}$ algorithm to generate the secret key $sk_{\mathcal{C},i} = \texttt{keygen}(\texttt{pp}, msk, A_{\mathcal{A},i})$, such that $|A_{\mathcal{A},i} \cap S^*| < t^*{}_{k,i}$. Finally, the challenger $\mathcal{C}$ answers the query by running the $\texttt{decrypt}(\texttt{pp}, sk_{\mathcal{C},i}, A_{\mathcal{C},i}, (t^*{}_{k,i}, S^*), C)$ algorithm that outputs a message m_j or a reject symbol $\perp$.

CHALLENGE PHASE – during the challenge phase, $\mathcal{A}$ picks two equal length cleartexts ${M_0}^*$ and ${M_1}^*$ and a threshold encrypting attribute set (t^*_k, S^*) (i.e; t^*_k has never been queried during the DECRYPTION QUERY PHASE) and sends them to $\mathcal{C}$. This latter chooses a random bit b from $\{0,1\}$ and computes the challenge encrypted message ${C_b}^* = \texttt{encrypt}(\texttt{pp}, (t^*_k, S^*), {M_b}^*)$. Then, the challenger sends ${C_b}^*$ to $\mathcal{A}$.

GUESS – $\mathcal{A}$ tries to guess which message M_i, where $i \in \{0,1\}$ corresponds to the enciphered data ${C_b}^*$. Thus, $\mathcal{A}$ outputs a bit b' of b and wins the game if $b = b'$. The advantage of the adversary $\mathcal{A}$ in the above game is defined as $Adv_{\mathcal{A}}[Exp^{Conf}(1^{\xi})] = |Pr[b = b'] - \frac{1}{2}|$.

5 EMA-LAB: Multi-threshold ABE Scheme

In this paper, we develop a new multi-threshold level attribute based encryption scheme, denoted by EMA-LAB with short ciphertext size. Our proposal is based

on the constant size attribute based encryption proposed by Herranz et al. [9], which has been extended to support multi-level access to data.

5.1 Complexity Assumptions

In our short ciphertext size multi level attribute based encryption construction, we rely on the Computational Diffie Hellman Assumption (CDH) and the augmented multi-sequence of exponents computational Diffie-Hellman ($(\tilde{l},\tilde{m},\tilde{t})$-aMSE-CDH) [2,9]. These assumptions are defined as follows:

Computational Diffie Hellman (CDH) Assumption – Let $\mathbb{G}$ be a group of a prime order p, and g is a generator of $\mathbb{G}$. The CDH problem is, given the tuple of elements (g, g^a, g^b), where $\{a,b\} \xleftarrow{R} \mathbb{Z}_p$, there is no efficient probabilistic algorithm $\mathcal{A}_{CDH}$ that computes g^{ab}.

Bilinear Diffie-Hellman (BDH) Assumption — Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ be an efficiently computable bilinear map. Let $a, b, c \in \mathbb{Z}_p^*$ are random numbers and g be a generator of $\mathbb{G}_1$. No probabilistic polynomial-time algorithm is able to compute $\hat{e}(g,g)^{abc}$ with non-negligible advantage if the tuple $\left\{g, g^a, g^b, g^c\right\}$ is known.

$(\tilde{l},\tilde{m},\tilde{t})$-augmented multi-sequence of exponents computational Diffie-Hellman ($(\tilde{l},\tilde{m},\tilde{t})$-aMSE-CDH) – The $(\tilde{l},\tilde{m},\tilde{t})$-aMSE-CDH problem related to the group pair $(\mathbb{G},\mathbb{G}_{\mathbb{T}})$ is to compute $T = e(g_0,h_0)^{k\cdot f(\gamma)}$. It takes as **input**: the vector $\boldsymbol{x}_{\tilde{l}+\tilde{m}} = (x_1,\cdots,x_{\tilde{l}+\tilde{m}})^\top$ whose components are pairwise distinct elements of $\mathbb{Z}_p$ which define the polynomials f(X) and g(X) as follows:

$$f(X) = \prod_{i=1}^{\tilde{l}}(X+x_i); \qquad g(X) = \prod_{\tilde{l}+1}^{\tilde{l}+\tilde{m}}(X+x_i) \tag{1}$$

where the values x_i are random and pairwise distinct of $\mathbb{Z}_p^*$, and the values:

$$\begin{cases} g_0, g_0^{\gamma}, \cdots, g_0^{\gamma^{\tilde{l}+\tilde{t}-2}}, g_0^{k\cdot\gamma\cdot f(\gamma)} \\ g_0^{\omega\gamma}, \cdots, g_0^{\omega\gamma^{\tilde{l}+\tilde{t}-2}} \\ g_0^{\alpha}, g_0^{\alpha\gamma}, \cdots, g_0^{\alpha\gamma^{\tilde{l}+\tilde{t}}} \\ h_0, h_0^{\gamma}, \cdots, h_0^{\gamma^{\tilde{m}-2}} \\ h_0^{\omega}, h_0^{\omega\gamma}, \cdots, h_0^{\omega\gamma^{\tilde{m}-1}} \\ h_0^{\alpha}, h_0^{\alpha\gamma}, \cdots, h_0^{\alpha\gamma^{2(\tilde{m}-\tilde{t})+3}} \end{cases}$$

Where $k, \alpha, \gamma, \omega$ are unknown random elements of $\mathbb{Z}_p$ and g_0 and h_0 are generators of $\mathbb{G}$. We can solve the problem if we get an **output** $b \in \{0,1\}$ where $b = 1$ if $T = e(g_0,h_0)^{k\cdot f(\gamma)}$ or $b = 0$ when T is a random value from $\mathbb{G}_T$.

5.2 Aggregate Algorithm

Our scheme relies on the aggregate algorithm `aggreg` introduced by Delerablee et al. [9]. Let us consider a list of values $\{g^{\frac{r}{\gamma+x_i}}, x_i\}_{1\leq i\leq n}$, where $r, \gamma \in \mathtt{Z}_p^*$ and

$x_1, \cdots, x_n$ are pairwise different. Then , the algorithm proceeds as follows:

$$\texttt{aggreg}(\{g^{\frac{r}{\gamma+x_i}}, x_i\}_{1\leq i\leq n}) = g^{\frac{r}{\prod_{i=1}^{n}(\gamma+x_i)}}$$

Concretely, the `aggreg` algorithm defines $P_{0,m} = g^{\frac{r}{\gamma+x_m}}$ for each $m \in \{1, \cdots, n\}$. Afterwards, the algorithm computes sequentially $P_{i,m}$ for $i = 1 \cdots n-1$ and $m = i+1, \cdots, n$ using the induction:

$$P_{i,m} = (\frac{P_{i-1,i}}{P_{i-1,m}})^{\frac{1}{x_m - x_i}} \tag{2}$$

Then, we get $P_{i,m} = g^{\frac{r}{(\gamma+x_m)\prod_{k=1}^{i}(\gamma+x_k)}}$ where $1 \leq i \leq m \leq n$. Therefore, since the elements $x_1, \cdots, x_n$ are pairwise different [2] and using the equation 2, we can compute $P_{i,m}$ for $i = 1 \cdots n-1$ and $m = i+1 \cdots n$ such as $P_{n,n-1} = g^{\frac{r}{\prod_{i=1}^{n}(\gamma+x_i)}}$.

5.3 Concrete Construction

EMA-LAB relies on four algorithms defined as follows:

- `setup` – the trusted authority selects a bilinear group $(\hat{e}, p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G})$ of prime order p, such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}$. It selects random generator $g \in \mathbb{G}_1$ and a set of $\mathbb{G}_2$ generators $\{h_j\}_{j=1,\cdots,m}$, such that $m = |\mathbb{T}|$ is the cardinal of the threshold universe $\mathbb{T}$, supported by the system. In addition, it defines an encoding function τ such that $\tau : \mathbb{U} \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$, where $|\mathbb{U}| = n$ and $\mathbb{U}$ is an attribute universe. For each attribute $a \in \mathbb{U}$, the encoded attribute values $\tau(a_i) = x_i$ are pairwise different, where $i \in [1, n]$.
  Then, the `setup` algorithm selects a set $\mathcal{D} = \{d_1, ..., d_{n-1}\}$ consisting of $n-1$ pairwise different elements of $(\mathbb{Z}/p\mathbb{Z})^*$ (i.e., dummy users), which must also be different to the values $\tau(a_i)$, for all $a_i \in \mathbb{U}$. Note that for any integer i lower or equal to $n-1$, we denote as $\mathcal{D}_i$ the set $\{d_1, ..., d_i\}$. Finally, the `setup` algorithm computes u defined as $u = g^{\alpha \cdot \gamma}$ and outputs the global public parameters `pp` as follows:

  $$\texttt{pp} = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}, \hat{e}, u, \{{h_j}^{\alpha\gamma^i}\}_{\{i=0,\cdots,2n-1;j=1,\cdots,m\}}, \mathcal{D}, \tau, \{\hat{e}(g^\alpha, h_j)\}_{\{j=1,\cdots,m\}}\}$$

  We note that the master key of the trusted authority is referred to as $\texttt{msk} = (g, \alpha, \gamma)$ where α, γ are two random values from $(\mathbb{Z}/p\mathbb{Z})^*$.

- `encrypt` – let $(\{t_j\}_{\{j=1,\cdots,l\}}, S)$ be the access policy where $\{t_j\}$ is the set of defined threshold values, l is the cardinal of $\{t_j\}$, $S \subset \mathbb{U}$ is an attribute set of size $s = |S|$ such that for all $j \in [1, l]$, $1 \leq t_j \leq |S|$.
  To encrypt the message M defined as $M = \{m_j\}_{\{j=1,\cdots,l\}}$ with respect to $(\{t_j\}_{\{j=1,\cdots,l\}}, S)$, the encrypting entity $\mathcal{E}$ picks at random $\kappa \in \mathbb{Z}/p\mathbb{Z}$ and generates the ciphertext $C = (C_1, C_{2,j}, C_{3,j})_{\{j=1,\cdots,l\}}$ defined as:

$$\begin{cases} C_1 = g^{-\kappa\alpha\gamma} \\ C_{2,j} = h_j^{\kappa\alpha \prod_{a\in S}(\gamma+\tau(a)) \prod_{d\in D_{n+t_j-1-s}}(\gamma+d)} \\ C_{3,j} = m_j \hat{e}(g^\alpha, h_j)^\kappa = m_j K_j \end{cases}$$

Finally, the encrypting entity outputs the encryption of the message M such that $C = (C_1, C_{2,j}, C_{3,j})_{\{j=1,\cdots,l\}}$.

– `keygen` – for any subset $A_{\mathcal{U}} \subset \mathbb{U}$ of attributes associated with the decrypting user $\mathcal{U}$, the trusted authority chooses a random value $r_{\mathcal{U}} \in (\mathbb{Z}/p\mathbb{Z})^*$ and computes the related secret key as follows:

$$\begin{aligned} sk_{\mathcal{U}} &= (\{g^{\frac{r_{\mathcal{U}}}{\gamma+\tau(a)}}\}_{a\in A_i}, \{h_j^{r_{\mathcal{U}}\gamma^i}\}_{i=0,\cdots,n-2, j=1\cdots m}, \{h_j^{\frac{r_{\mathcal{U}}-1}{\gamma}}\}_{j=1\cdots m}) \\ &= (sk_{\mathcal{U}_1}, sk_{\mathcal{U}_2}, sk_{\mathcal{U}_3}) \end{aligned}$$

– `decrypt` – the decrypting entity $\mathcal{U}$ having a set of attributes $A_{\mathcal{U}}$ where $|A_{\mathcal{U}} \cap S| = t_j$ can decrypt the enciphered message m_j under the access policy $(\{t_j\}_{\{j=1,\cdots,l\}}, S)$, with respect to the t_j threshold level.
For this purpose, for all $a \in A_{\mathcal{U}}$, $\mathcal{U}$ firsts aggregates the required attributes, with respect to t_j satisfied by his certified attributes, such as:

$$A = \texttt{aggreg}(\{g^{\frac{r_{\mathcal{U}}}{\gamma+\tau(a)}}, \tau(a)\}_{a\in A_{\mathcal{U}}}) = g^{\frac{r_{\mathcal{U}}}{\prod_{a\in A_{\mathcal{U}}}(\gamma+\tau(a))}}$$

Afterwards, $\mathcal{U}$ uses the aggregated secret key A and the ciphertext element $C_{2,j}$, related to the satisfied threshold t_j, to compute:

$$\begin{aligned} L_j &= \hat{e}(g^{\frac{r_{\mathcal{U}}}{\prod_{a\in A_{\mathcal{U}}}(\gamma+\tau(a))}}, C_{2,j}) \\ &= \hat{e}(g, h_j)^{r_{\mathcal{U}}\kappa\alpha \prod_{a\in S\setminus A_{\mathcal{U}}}(\gamma+\tau(a)) \prod_{d\in D_{n+t_j-1-s}}(\gamma+d)} \end{aligned} \tag{3}$$

Then, $\mathcal{U}$ defines the polynomial $P_{(A_{\mathcal{U}},t_j,S)}(\gamma)$ such as:

$$P_{(A_{\mathcal{U}},t_j,S)}(\gamma) = \frac{1}{\gamma}\Big(\prod_{a\in S\cup D_{n+t_j-1-s}\setminus A_S}(\gamma+\tau(a)) - \prod_{a\in S\cup D_{n+t_j-1-s}\setminus A_U}\tau(a)\Big) \tag{4}$$

Afterwards, $\mathcal{U}$ uses the aggregated secret key A and the $sk_{\mathcal{U}_2}$ key elements to compute:

$$\begin{aligned} &[\hat{e}(C_1, h_j^{r_{\mathcal{U}}P_{(A_{\mathcal{U}},t_j,S)}(\gamma)}) \cdot L_j]^{\frac{1}{\prod_{a\in S\cup D_{n+t_j-1-s}\setminus A_{\mathcal{U}}}\tau(a)}} \\ &= e(g, h_j)^{\kappa\cdot\alpha\cdot r_{\mathcal{U}}} \end{aligned} \tag{5}$$

Then, from Equation5 and the secret key element the $sk_{\mathcal{U}_3}$, related to t_j, the decrypting entity $\mathcal{U}$ deduces the deciphering key K_j such as:

$$\begin{aligned} K_j &= \hat{e}(C_1, sk_{\mathcal{U}_3}) \cdot \hat{e}(g, h_j)^{\kappa\cdot r_{\mathcal{U}}\cdot\alpha} \\ &= \hat{e}(g, h_j)^{\alpha\cdot\kappa} \end{aligned}$$

Finally, $\mathcal{U}$ recovers the sub-message m_j, with respect to related access level t_j, by computing $m_j = \frac{C_{3,j}}{K_j}$.

6 Security Analysis

To ensure multi-level threshold encryption scheme, our EMA-LAB construction mainly relies on the constant size attribute based encryption scheme proposed by Herranz et al. [9]. As such, the data confidentiality preservation is tightly related to the security of the used attribute based encryption algorithm. Our EMA-LAB scheme is secure against selective non-adaptive chosen ciphertext attacks in the standard model, under the CDH, BDH and $(\tilde{l}, \tilde{m}, \tilde{t})$-aMSE-CDH assumptions, with respect to the Exp^{conf} experiment.

Sketch of proof — As presented in section 4.2, the adversary may lead an attack against the indistinguishability property either on his own or through a collusion attack.

First, the design of our EMA-LAB scheme was motivated by preventing collusion attacks among users. Thus, as our scheme relies on the constant size threshold ABE construction of Herranz et al. [9], it randomizes, in the same way, users' private keys such that they cannot be combined. In fact, each private key element contains a random value $r_{\mathcal{U}}$ related to the user $\mathcal{U}$, which prevents colluding users to override their rights and successfully perform a collusion attack. Consequently, our EMA-LAB mechanism is resistant against collusion attacks.

Second, in order to decrypt a ciphertext with respect to a threshold level ${t^*}_j$, an adversary $\mathcal{A}$ may conduct, on his own, an attack against the indistinguishability property. That is, he must recover $K_j = \hat{e}(g, h_j)^{\kappa\alpha}$, where the secret κ is embedded in the ciphertext. For this purpose, $\mathcal{A}$ has to retrieve the corresponding K_j, based on the related private key associated with ${t^*}_j$.

To prove that our scheme is secure against selective, non-adaptive chosen ciphertext attacks, we first distinguish two different cases, based on the number of defined threshold values during the Initialisation phase of Exp^{conf} experiment, introduced in section 4.2:

Case 0 : we set only one threshold level ${t_j}^*$, such as the public parameter m selected by the adversary is equal to 1. That is, all queried private keys are related to the set of attributes S^* that decrypt ciphertexts, encrypted with respect to ${t_j}^*$, for each session i. This first sub-case simulates a selective CCA-1 security game for [9] scheme.

Case 1 : for this case, the challenger defines different threshold levels, during the Initialisation phase, such as $m > 1$. For each session i, we suppose that $\mathcal{A}$ has access to $C_i = \{C_{k,i}\}_{l \in [1,m^*]}$, where $C_{k,i}$ is an encrypted data block $m_{k,i}$ under a threshold ${t^*}_{k,i}$.

For **Case 0**, one single threshold level is set. Thus, EMA-LAB scheme follows the construction proposed by Attrapadung et al. in [2]. That is, the Setup, Decryption Query Phase and Challenge phases are based on one single threshold level, where the challenge message M_b contains one single data block related to the threshold ${t_j}^*$. The main difference consists in the derivation of

the ciphertext element $C_{3,t_j{}^*}$ corresponding to a pre-defined threshold level $t_j{}^*$, and relying on the public parameter $\hat{e}(g,h_j)^{\alpha}$. Indeed, unlike the [2] scheme relying the `aggreg` algorithm and based on the $(\tilde{l},\tilde{m},\tilde{t})$-aMSE-CDH assumption, in our construction, the generation of ciphertexts depends on different public elements, mainly for $C_{3,t_j{}^*}$. More precisely, the main difference mainly consists in $K_j = \hat{e}(g,h_j)^{\alpha\kappa}$, where $\hat{e}(g,h_j)^{\alpha}$ is a public parameter generated by the challenger $\mathcal{C}$, generated with respect to each different threshold level $t_j{}^*$. As such, similarly to [2], the advantage of the Exp^{conf} adversary is at most equal to advantage of an algorithm resolving the $(\tilde{l},\tilde{m},\tilde{t})$-aMSE-CDH assumption.

For **Case 1**, the INITIALISATION phase is executed similarly as for **Case 0**. In fact, the challenger $\mathcal{C}$ sends the public parameters `pp` defined as:

$$\begin{aligned}\texttt{pp} = \{&\mathbb{G}_1,\mathbb{G}_2,\mathbb{G},\hat{e},u,\{{h_j}^{\alpha\gamma^i}\}_{\{i=0,\cdots,2n-1;j=1,\cdots,m\}},\\ &\mathcal{D},\tau,\{\hat{e}(g^{\alpha},h_j)\}_{\{j=1,\cdots,m\}}\}.\end{aligned}$$

For ease of presentation, we do not show the progress of SETUP and DECRYPTION QUERY PHASE between $\mathcal{C}$ and $\mathcal{A}$, where the outputs of `keygen` and `decrypt` are closely similar to **Case 0**, considering m^* encrypted sub-messages $\{m_i\}_{\{i\in[1,m^*]\}}$ related to m^* threshold levels. During the challenge phase, when $\mathcal{A}$ asks for the encryption of the challenge message with respect to a challenge access structure $(\{t^*{}_j\}_{\{j\in[1,m]\}},S^*)$, $\mathcal{C}$ does the following. $\mathcal{C}$ first chooses a random $\kappa\in\mathbb{Z}/p\mathbb{Z}$ and outputs the encryption of the challenge message such that: for each threshold level t_j, we have $C_j = \hat{e}(g,h_j)^{\kappa\alpha}$. These values are then sent to the adversary. We state that if $\mathcal{A}$ asks for a decryption key for a set of attributes such that $|A_{\mathcal{A}}\cap S^*| > t^*{}_k$, then $\mathcal{C}$ does not issue the key. Similarly, if $\mathcal{A}$ asks for S^*, with respect to any threshold value, such that one of the keys is already issued then the simulation aborts. In the sequel, the advantage of the adversary is at most equal to **Case 0**, due to the randomness of the choice of variable values in the simulation, based on the CDH and BDH assumptions. Indeed, $\mathcal{A}$' view in this simulation is identically distributed for all threshold levels. In fact, the encryptions of data blocks of the challenge message M_b are completely independent, thanks to the use of different $\hat{e}(g,h_j)$ functions. As such, **Case 1** can be considered as m^* random repetitions of **Case 0** simulation, with respect to m^* threshold levels.

As such, we prove that EMA-LAB scheme is secure against selective non-adaptive chosen ciphertext attacks in the standard model, under the CDH, BDH and $(\tilde{l},\tilde{m},\tilde{t})$-aMSE-CDH assumptions, with respect to the Exp^{conf} experiment.

7 Performance Analysis

In most ciphertext policy attribute based encryption schemes, the size of an encrypted data file increases with the number of attributes involved in the access policy used in the encryption phase [2,4]. As detailed in Table 2, in [10] and [13], the ciphertext size increases with the number of attributes defined in the access structure used to encrypt data. Similarly, the encryption and decryption costs

Table 2. Computation and Storage Costs of Multi Level Attribute Based Encryption Schemes

Scheme	Access Policy	Multi-level	Ciphertext Size	$\mathcal{E}$ Computation Overhead	$\mathcal{U}$ Computation Overhead
[12]	Monotone	Yes	$2n + 2m$	$mE + \tau_p + (m + 2n)E_1$	$mE + 2\tau_p$
[15]	Monotone	Yes	$2m + 3n$	$(2n + m)E + (2n + m)E_1$	$(2n + m)\tau_p + (n + m)E$
[13]	Monotone	No	3n+1	$E + (2n + 1)E_1 + \tau_P$	$(2 + n)\tau_P + nE$
[10]	Monotone	No	$2n + 2$	$(2n + 1)E + (3n + 3r)E_1 + \tau_P$	$(n + r)E + 2(n + r)\tau_P$
[9]	Threshold	No	3	$E_1 + E_2 + E$	$(t + 1)E_1 + 3\tau_p + E_2 + E$
EMA-LAB	Threshold	Yes	$2m + 1$	$E_1 + mE_2 + mE$	$(t_j + 1)E_1 + 3\tau_p + E_2 + E$

$\mathcal{E}$ and $\mathcal{U}$ are the encrypting entity and the decrypting user. t, m and n are the size of the threshold, the cardinal of the threshold universe and attribute universe, respectively. E_1, E_2, E represent exponentiation costs in $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, while τ_p is the cost of a pairing operation.

depend on the number of attributes. To countermeasure this limit, attribute based encryption schemes with constant ciphertext size have been introduced. Herranz et al. [9] designed a threshold attribute based encryption scheme where ciphertext size does not depend on the number of attributes. In addition, the encryption overhead is constant while varying the size of the used threshold access predicate. Nevertheless, the aforementioned schemes [9,10,13] do not provide the multi level access feature. In [12, 15], the authors have extended a ciphertext-policy attribute based encryption scheme to ensure multi authorisation level access control to data. Although the practicability of their schemes in several domains, they are lacking for more efficiency especially related to storage and computation costs. Indeed, the ciphertext size and the computation overheads in the encryption and decryption phases increase with both the number of attributes in the access policies and the number of security levels (thresholds). To bring both the practicability and the efficiency features, EMA-LAB introduces a more efficient ABE scheme with short ciphertext. Indeed, as shown by Table 2, our contribution introduces a ciphertext size which only depends on the number of thresholds used in the multi level access policy unlike state of the art multi level ABE schemes which depend on both the number of attributes and the number of thresholds. Similarly, the computation overheads at the encrypting and the decrypting entities sides only depend on the number of thresholds. In other words, the decryption overhead and the ciphertext size are constant for each threshold level.

Several research works have been proposed to evaluate the computation overhead of attribute based encryption schemes [5, 8]. Our ongoing implementation of the EMA-LAB's Proof of Concept (PoC) consists in evaluating the impact of elementary cryptographic operations on different resource-constrained devices as detailed in Table 3. As our EMA-LAB framework relies on the use of bilinear maps as well as mathematical operations in a multiplicative group, we investigate the impacts of these operations (cf. Figure 2) on the performance of different IoT devices, based on the results introduced in [5].

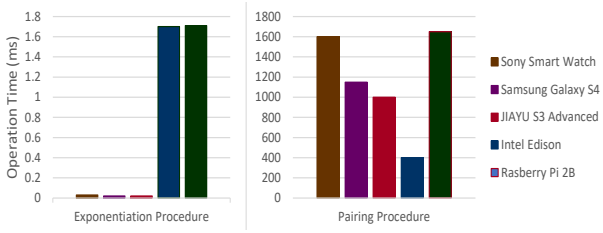

Fig. 2. Elementary functions Computation Costs

In our ongoing implementation, we only consider the computational cost in terms of time in our encryption and decryption algorithms. Indeed, for a single threshold level, the encryption time is constant while varying the number of attributes. Moreover, the decryption overhead increases linearly with the number of attributes in the threshold level. This is due to the aggregation (c.f., Section 5.2) of the decrypting entity's secret keys performed in the decryption phase.

Table 3. Selected Devices [5]

Device	Type	Processor
Sony SmartWatch 3 SWR50	Smart Watch	520 MHz Single-core Cortex-A7
Samsung I9500 Galaxy S4	Smartphone	1.6 GHz Dual-Core Cortex-A15
Jiayu S3 Advanced	Smartphone	1.7 GHz Octa-Core 64bit Cortex A53
Intel Edison	IoT Development Board	500 MHz Dual-Core Intel AtomTM CPU, 100 Mhz MCU
Raspberry Pi 2 model B	IoT Development Board	900 MHz Quad-Core ARM Cortex-A7

8 Conclusion

In this paper, we propose a novel cryptographic mechanism to ensure multi-level access control, based on the use of a constant size threshold attribute based encryption scheme. Our EMA-LAB scheme enables the enciphering user to encrypt the same data content, based on an aggregated set of attributes, and the deciphering entity to decrypt the subsets of data blocks with respect to a threshold t_j, associated with his attributes. Compared to most-closely related schemes, our construction provides interesting computation costs, as it does not depend on the number of involved attributes specified in the aggregated access predicate.

References

1. Ateniese, G., Chou, D.H., de Medeiros, B., Tsudik, G.: Sanitizable Signatures. Springer Berlin Heidelberg (2005)

2. Attrapadung, N., Herranz, J., Laguillaumie, F., Libert, B., De Panafieu, E., Ràfols, C.: Attribute-based encryption schemes with constant-size ciphertexts. Theoretical Computer Science **422**, 15–38 (2012)
3. Belguith, S., Kaaniche, N., Jemai, A., Laurent, M., Attia, R.: Pabac: a privacy preserving attribute based framework for fine grained access control in clouds. In: 13th IEEE International Conference on Security and Cryptography(Secrypt). pp. 133–146 (2016)
4. Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., Attia, R.: Constant-size threshold attribute based signcryption for cloud applications. In: SECRYPT 2017: 14th International Conference on Security and Cryptography. vol. 6, pp. 212–225 (2017)
5. Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., Attia, R.: Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot. Computer Networks **133**, 141–156 (2018)
6. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy. (2007)
7. Ge, A., Zhang, R., Chen, C., Ma, C., Zhang, Z.: Threshold ciphertext policy attribute-based encryption with constant size ciphertexts. In: Australasian Conference on Information Security and Privacy. pp. 336–349. Springer (2012)
8. Guo, L., Zhang, C., Yue, H., Fang, Y.: Psad: A privacy-preserving social-assisted content dissemination scheme in dtns. IEEE Transactions on Mobile Computing **13**(12), 2903–2918 (2014)
9. Herranz, J., Laguillaumie, F., Ràfols, C.: Constant size ciphertexts in threshold attribute-based encryption. In: International Workshop on Public Key Cryptography. pp. 19–34. Springer (2010)
10. Horváth, M.: Attribute-based encryption optimized for cloud computing. In: SOFSEM 2015: Theory and Practice of Computer Science, pp. 566–577. Springer (2015)
11. Johnson, R., Molnar, D., Song, D., Wagner, D.: Homomorphic Signature Schemes, pp. 244–262. Springer Berlin Heidelberg (2002)
12. Kaaniche, N., Laurent, M.: Attribute based encryption for multi-level access control policies. In: SECRYPT 2017: 14th International Conference on Security and Cryptography. vol. 6, pp. 67–78. Scitepress (2017)
13. Li, L., Chen, X., Jiang, H., Li, Z., Li, K.C.: P-cp-abe: Parallelizing ciphertext-policy attribute-based encryption for clouds. In: Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2016 17th IEEE/ACIS International Conference on. pp. 575–580. IEEE (2016)
14. Onica, E., Felber, P., Mercier, H., Rivière, E.: Confidentiality-preserving publish/-subscribe: A survey. ACM Computing Surveys (CSUR) **49**(2), 27 (2016)
15. Wang, S., Zhou, J., Liu, J.K., Yu, J., Chen, J., Xie, W.: An efficient file hierarchy attribute-based encryption scheme in cloud computing. IEEE Transactions on Information Forensics and Security **11**(6), 1265–1277 (2016)
16. Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Public Key Cryptography–PKC 2011, pp. 53–70. Springer (2011)
17. Zhang, Y., Zheng, D., Chen, X., Li, J., Li, H.: Efficient attribute-based data sharing in mobile clouds. Pervasive and Mobile Computing **28**, 135–149 (2016)