INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
G. Öztürk et al., Vol.12, No.3, pp.1-13.
https://doi.org/10.55859/ijiss.1294580

Modified Attribute-Based Authentication for Multi-Agent Systems

Gülnihal Öztürk[1], Ayşe Nurdan Saran[2], Ali Doğanaksoy[3],

[1] Department of Cryptography, Middle East Technical University, Ankara, Turkey
[2] Department of Computer Engineering, Cankaya University, Ankara, Turkey
[3]Department of Mathematics, Middle East Technical University, Ankara, Turkey
Corresponding Author: buz@cankaya.edu.tr

Research Paper Received: 09.05.2023 Revised: 06.09.2023 Accepted: 11.09.2023

Abstract—Attribute-Based Encryption (ABE) is a type of authentication mechanism that validates both the users and their attributes. It is practical for the systems that need authorization according to credentials. In a multi-agent system, specifying an access policy within the user groups is crucial to enable authentic and confidential communication. This paper proposes an attribute-based authentication framework based on elliptic curves to provide privacy in multi-agent systems. In this system, we aim to alleviate the required burden of verification by ensuring that each unit verifies only a small amount of messages. Inspired by Zhang et al. [1], we use ABE for the multi-agent system to authenticate more than one user at a time; our scheme uses elliptic curve groups, unlike Zhang et al. We have thoroughly evaluated the various security attributes and discussed computational overheads for our proposed scheme.

Keywords—attribute-based encryption, authentication, privacy, vehicular ad hoc network

1. Introduction

Entity authentication and key agreement are critical cryptographic challenges in distributed collaborative systems. It is generally convenient for agents to communicate with other representatives in the system using attributes that describe their roles or responsibilities. These attributes are highly desirable if the members dynamically join/leave the system. Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE) are examples of authentication by encryption. In 1984, Shamir [2] proposed the idea of the IBE on a public-key cryptography basis. In the system, there is no pre-distribution of keys among individuals, and it is useful in situations where there are technical restraints in communication between agents. The authorized user should obtain the private-public key pairs generated based on their credentials from the public key generator, PKG. In this way, they cannot deny the encryptions containing their keys. Boneh and Franklin developed a practical identity-based encryption system based on bilinear maps (such as Weil Pairing on elliptic curves) between groups [3]. They formally explained the definition and security model explicitly for such cryptosystems.

In IBE schemes, there is only one attribute that

needs necessarily to be fulfilled to get access to the data; however, in ABE schemes, public/private key pairs are based on each individual's attributes; therefore, if the individuals are in the same attribute group, they may mutually authenticate each other. Firstly, Sahai and Waters [4] proposed the ABE system named Fuzzy Identity-Based Encryption. In the system, users' keys or ciphertexts are linked to attributes. The user can decrypt the encrypted message if the ciphertext attributes match the user's key attributes according to a threshold. However, Sahai, and Waters' system has some limits. Goyal et al. [5] improved this idea by proposing Key-Policy ABE and Ciphertext-Policy ABE in 2006. They separated the concepts in the [4]. Nonetheless, Goyal et al. explained only the Key-Policy ABE in detail. Ciphertext-Policy ABE explicitly studied by Bethencourt, Sahai and Waters [6]. In light of their works, Zhu et al. [7] proposed an attribute-based authentication scheme based on Lagrange Polynomial Interpolation. They aimed to decrease the usage of system resources. However, Yun et al. proved that their scheme is insecure under collusion and impersonation attacks [8].

Besides providing authentication, ABE systems are used to protect privacy in some schemes. In their work, Guo et al. constructed an attribute-based system [9] for the electronic health (eHealth) system. Narayan et al. [10] and, Barua et al. [11] also proposed attribute-based schemes for the eHealth system. All these works focused on patients' privacy protection since patients' concerns increased when electronic health records were used to file their personal information. Another area that needs authentication is vehicular ad hoc networks (VANET). The system arranges communications between vehicles and vehicles to the roadside. Authentication provides security against malicious signals and messages in VANET. There are many studies to provision privacy in vehicular ad hoc networks that use different cryptographic schemes, such as identity-based schemes [12], group signature scheme [13], [14], threshold scheme [15]. They authenticate the messages or signals vehicles receive using certificates, signatures, and group signatures. Huang and Verma [16] proposed the first attribute-based encryption scheme ASPE for VANET. Liu et al. suggested using multiple authorities besides the ABE system [17]. They established a hierarchy between these authorities. In [18], Guo et al. proposed white-box traceability and user revocation for user key abuse in such a system. In 2021, Gan et al. proposed a method that hides attributes in the access policy [19]. Ma et al. proposed attribute-based schemes that use blockchain [20]. The common ground in all these works is privacy, like Zhang et al. scheme [21].

Although the previous works protect data integrity, they do not provide users' privacy. However, we can deduce from recent studies that many application areas need privacy protection. Zhang et al. [1] drew attention to the necessity of privacy in their work and studied a scheme for a multi-agent system as in [22]. They aim to provide privacy, authentication, and confidentiality in this system.

Our main contributions are as follows:

- Inspired by the Zhang et al. scheme, we design an attribute-based authentication system in multi-agent systems, where each agent uses its verifiable attributes to authenticate each other before communication.
- Our attribute-based authentication system can simultaneously provide privacy protection and verifiability of agents' verified attributes.
- We use pairings for bilinear maps and design an ABE on the elliptic curve. We aim to gain the advantage of key size and storage.
- We revoke an agent by deleting the record

from an authentication list, but this operation is done by a trusted third party (group manager). Consequently, revocation becomes a dependent operation.

- Due to the rise in the number of agents, there is an increase in data traffic on the network. We modify attributes set to reduce the number of operations of users and ease of transformation. In other words, when the number of agents is huge in Vanet traffic, reducing the number of operations of users is a challenging task in such a system. In the previous scheme, the receiver should compute a pseudonym with all possible combinations of own credentials until finding the one equal to the pseudonym in ATB-SET. In the proposed scheme, during the decryption of the message, we changed it with a vector. By the way, the receiver computes the pseudonym with its own credentials only one time and compares it with the pseudonym in ATB-SET, which will reduce the network traffic.

2. Preliminaries

2.1. Attribute-based Authentication

Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE) are cryptographic techniques that provide fine-grained access control and user-centric encryption, making them suitable for VANETs. In IBE, encryption keys are generated from a user's identity, such as email address, username, or other identifier. It is primarily designed for one-to-one communication between the sender and receiver; therefore, it is often used in scenarios where one-to-one communication is prevalent. On the other hand, ABE allows access control based on attributes rather than a user's identity. Users are associated with a set of attributes, and access policies are established using these attributes. Encrypted data can be decrypted by users with the necessary attributes that satisfy the policy. It is commonly used in applications like data sharing and cloud storage, where data may need to be selectively shared with users based on various attributes.

2.2. Notations

We use some notations when we explain the schemes. The notations are given in Table 1 to make it easy to understand the schemes.

Table 1.
Notations in ABE Scheme

Parameters:	
q	large prime
G_1	additive cyclic group of prime order q (elliptic curve group in ECDLP in our scheme)
G_2	multiplicative cyclic group of prime order q
g_1	generator of additive group G_1
e	bilinear map from $G_1 \times G_1$ to G_2
s	master key (private key) of the system
pk	public key of the system
GM	group manager in the system,
ID_i	identity of an agent
h_i	pseudonym of the agent who has identity ID_i
d_i	private key of the agent who has identity ID_i
l_m	member list of the group
Atb_i	i_{th} attribute
$Cred_i$	i_{th} credential of Atb_i
l_a	attribute list

Hash functions :
$H : \{0,1\}^* \rightarrow G_1$
$H_2 : G_2 \rightarrow \{0,1\}^n$
$H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{Z}_q^*$
$H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$
$H_5 : G_2 \rightarrow \mathbb{Z}_q^*$

2.3. Bilinear Pairings

Define a map e from $G_1 \times G_1$ to G_2, which satisfies :

Bilinearity: $e(xP, yQ) = e(P, Q)^{xy}$ for all elements P, Q of G_1 and for any $x, y \in \mathbb{Z}_q^*$

Non-degeneracy : $e(P,Q) \neq 1$ for some elements P, Q of G_1
Computable: $e(P,Q)$ is computable for all P, Q of G_1 by an efficient algorithm

Then e is a bilinear map.

2.4. Security Assumptions

Our scheme provides security with some mathematical problems, which are given below.

Elliptic Curve Discrete Logarithm Problem (ECDLP): Let $P, Q \in G_1$. Assume $Q = kP$ for some $k \in \mathbb{Z}_q^*$. Then it is challenging to compute k from P, Q.
Bilinear Diffie-Hellman (BDH) Problem: Let $g_1, ag_1, bg_1, cg_1 \in G_1$. Assume that $a, b, c \in \mathbb{Z}_q^*$ are unknown. Then it is difficult to compute $e(g_1, g_1)^{abc}$.
Decisional Bilinear Diffie-Hellman (DBDH) Problem: Let $g, ag, bg, cg \in G_1$, $a, b, c \in \mathbb{Z}_q^*$, and $\tau \in G_2$. Let q be the order of G_1 and a large prime. Then it is difficult to distinguish the tuples $(g, ag, bg, cg, e(g,g)^{abc})$ and (g, ag, bg, cg, τ).

3. Zhang-Mu-Zhang Scheme

We design an authenticated key agreement protocol based on Zhang et al. [1], an efficient system for bilinear groups. However, their work is based on attribute-based authentication using public-key cryptography; we use elliptic curves, which use smaller key sizes and are more suitable for multi-agent systems. Thus, we briefly introduce the system that fits our scenarios. There are mainly 6 phases in the system Setup, Register, Revoke, IssueAttribute, SendMsg, and RcvMsg.

Setup: The group manager (GM) generates the system parameters and master key.

$$\textit{Params} = (q, G_1, G_2, n, e, g_1, pk, H, H_2, H_3, H_4, H_5, l_m, l_a)$$

Register: Agents with their identity are registered in the system. GM computes the pseudonym $h_i = H(ID_i)$ and the agent's private key $d_i = h_i^s$. Then GM adds the new agent's pseudonym into the member list l_m.
Revoke: GM removes an agent's pseudonym h_i from the member list l_m.
IssueAttribute: GM processes the member's credentials depending on the member's attributes ,and adds the attribute to the list if it is not in the list.
SendMsg: An agent, who wants to encrypt the data, first determines a policy for who can decrypt. A policy is the concatenation of receivers' pseudonyms and chosen attributes. Then the agent with the pseudonym h_i and private key d_i does the following to send a message M :

1 Choose randoms $z \in \{0,1\}^n$ and $\mu \in \mathbb{Z}_q^*$ and compute $r = H_3(z, M)$.
2 Ciphertexts are associated with sets of attributes as

$$C = \{g_1^{\mu}, h_i^r, A, M \oplus H_4(z), \text{ATB-SET}\}$$

where

$$A = z \oplus H_2(e(d_i, h_j^*)^r) \oplus \{\oplus_{k=1}^{l_j} H_2(e(d_i, H(Atb_k^{[j]}))^r)\},$$

$$\text{ATB-SET} = \left\{ l_j + 1, H_5\left(e\left(h_j^* \cdot \prod_{k=1}^{l_j} H(Atb_k^{[j]}), pk\right)^{\mu}\right)\right\}, 1 \leq j \leq l.$$

3 Broadcast C.

RcvMsg: The receiver uses his private key, credentials that match the ciphertext attributes, and *Params* to decrypt the message. The receiver also authenticates the sender in this phase. The agent with pseudonym h_θ, private key d_θ and credentials that match with attributes embedded in the ciphertext does the following to decrypt $C = (X, U, V, W, \text{ATB-SET})$:

1 Check $X, U \in G_1$. If they are not, reject the ciphertext.
2 Check credentials to check whether they match attributes by
- Extract elements of ATB-SET such that $l_r, h_r \in \mathbb{Z}_q^*$ where l_r is the number of necessary credentials, and h_r is the expected result of hash the computation. Therefore, the agent h_θ chooses l_r credentials among all possessions. Until the equality holds, the agent checks all combinations of his credentials and other elements in ATB-SET.
- When the equality holds, the agent finds the credentials $\{Cred_1^{[\theta]}, \ldots, Cred_{l_\theta}^{[\theta]}\}$ that match the attributes.
3 Compute z' and M' with their own credentials determined in the previous step.
4 Compute

$$\begin{aligned} r' &= H_3(z', M') \\ h' &= U^{1/r'} \end{aligned}$$

5 It is expected that h' is an agent's pseudonym. Therefore, check $h' \in l_m$. If it is an element of l_m, the sender is the agent with pseudonym h', and the message is M'. If it is not in l_m, reject the ciphertext.

Verification of the scheme is in [1] .

4. Our Modified Scheme

To provide the same security with smaller key size, storage, and easier information transmission, we modify Zhang et al. [1] by using elliptic curve cryptography. Setup, Register, Revoke and IssueAttribute phases are same as in Zhang et al. while SendMsg, and RcvMsg phases are modified to reduce the receiver's work. We make necessary changes to the choice of the groups for a bilinear map and the operations for the computation of the terms in all phases. In this section, we explain our modified version of the scheme.

Setup: The group manager (GM) generates the system parameters and master key. GM selects a random $s \in \mathbb{Z}_q^*$ as a master key and computes the public key $pk = sg_1$. Then GM publishes the system parameters.

$$Params = (q, G_1, G_2, n, e, g_1, pk, H, H_2, H_3, H_4, H_5, l_m, l_a)$$

The list of members l_m and attributes l_a are empty in this part and controlled by GM as in Zhang et al.

RegisterAgent: Agents with their identity are registered in the system. GM computes the hash of the identity ID_i as pseudonym $h_i = H(ID_i)$ of the agent and multiplies the scalar s with the pseudonym to compute private key $d_i = sh_i$. Then GM gives (h_i, d_i) to the agent ID_i and adds the new agent's pseudonym into the member list l_m by setting $l_m := l_m \cup \{h_i\}$ if $h_i \notin l_m$.

RevokeAgent: GM removes an agent's pseudonym h_i from the member list l_m to revoke agent. GM simply sets $l_m := l_m \setminus \{h_i\}$.

IssueAttribute: Depending on the member's attributes, GM processes the member's credentials. GM computes $Cred_i = sH(Atb_i)$ as the credential of the attribute Atb_i and adds the attribute to the list if it is not in the list earlier by setting $l_a := l_a \cup \{Atb_i\}$.

SendMsg: An agent, who wants to encrypt the data, first determines a policy for who can decrypt. A policy is the concatenation of receivers' pseudonyms and chosen attributes. Then the agent with pseudonym h_i and private key d_i does the following to send a message M with the attribute policy $\vee_{j=1}^{l}[h_j^* \wedge_{k=1}^{l_j} (Atb_k^{[j]})]$:

1 Choose randoms $z \in \{0,1\}^n$ and $\mu \in \mathbb{Z}_q^*$ and compute $r = H_3(z, M)$.
2 Ciphertexts are associated with sets of at-

tributes as

$$C = \{\mu g_1, rh_i, A, M \oplus H_4(z), \text{ATB-SET}\}$$

where

$$A = z \oplus H_2(e(d_i, h_j^*)^r) \oplus \{\oplus_{k=1}^{l_j} H_2(e(d_i, H(Atb_k^{[j]}))^r)\},$$

$$\text{ATB-SET} = \left\{\left(V_j, H_5\left(e\left(h_j^* + \sum_{k=1}^{l_j} v_k H(Atb_k^{[j]}), pk\right)^{\mu}\right)\right)\right\}, 1 \leq j \leq l.$$

In ATB-SET $V_j = (v_1, v_2, \ldots, v_{l_j})$ is a vector for the agent h_j^* where l_j is the number of the agent's all attributes such that

$$v_i = \begin{cases} 1, & \text{if } Atb_i^{[j]} \text{ is required for decryption} \\ 0, & \text{if } Atb_i^{[j]} \text{ is not required for decryption} \end{cases}$$

Setting attributes with this vector differs our scheme from Zhang et al. scheme. ATB-SET includes only the number of necessary credentials and the hash value in their scheme. Because of that, receivers have to try all combinations of their attributes. However, in our scheme receivers get a vector specifying exactly which attributes are required for decryption.

3 Broadcast C.

RcvMsg: The receiver uses his private key, credentials that match the ciphertext attributes, and *Params* to decrypt the messages. The receiver also authenticates the sender in this phase. Unlike Zhang et al., in our scheme attributes are embedded in the ciphertext by using a vector. Therefore in this phase, the agent checks the necessary credentials easier than in Zhang et al..The agent with pseudonym h_θ, private key d_θ and credentials that match with attributes embedded in the ciphertext do the following to decrypt $C = (X, U, V, W, \text{ATB-SET})$:

1 Check $X, U \in G_1$. If they are not, reject the ciphertext.

2 Check credentials to see whether they match attributes by

- Extract the pairs in ATB-SET such that (V_r, h_r) where V_r is the vector for attributes and h_r is the expected result of the hash computation. Therefore, the agents h_θ take the suitable V_r's for their attribute number. In other words, they take the vectors having a size equal to the number of attributes. Check

$$H_5\left(e\left(d_\theta + \sum_{k=1}^{l_r} v_k Cred_k^{[\theta]}, X\right)\right) = h_r$$

where l_r is the number of attributes h_θ has and V_r size.

- When the equality holds, the agent finds which credentials between $\{Cred_1^{[\theta]}, \ldots, Cred_{l_r}^{[\theta]}\}$ match the requested attributes.

- The agent checks the equality for the number of suitable vectors. Even if all vectors are suitable, computation is done once for each vector. The agent does not need to try combinations of wanted number attributes among all of them.

As described in SendMsg phase, receivers know which credentials they use for decryption. For this reason, they do less computation in our scheme than in Zhang et al..

3 Compute

$$z' = V \oplus H_2(e(U, d_\theta)) \oplus \{\oplus_{k=1}^{l_\theta} H_2(e(U, Cred_k^{[\theta]}))\}$$

$$M' = W \oplus H_4(z')$$

4 Compute

$$r' = H_3(z', M')$$
$$h' = (r')^{-1}U,$$

where $(r')^{-1}$ is inverse of r' in modulo q.

5 It is expected that h' is an agent's pseudonym. Therefore, check $h' \in l_m$. If it is an element of l_m, the sender is the agent with pseudonym

h', and the message is M'. If it is not in l_m, reject the ciphertext.

The correctness of the equalities can be proven:

$$\begin{aligned} H_5\left(e\left(d_\theta+\sum_{k=1}^{l_r} v_k Cred_k^{[\theta]}, X\right)\right) &= H_5\left(e\left(sh_\theta+\sum_{k=1}^{l_r} v_k(sH(Atb_k^{[\theta]})), \mu g_1\right)\right) \\ &= H_5\left(e\left(s\left(h_\theta+\sum_{k=1}^{l_r} v_k H(Atb_k^{[\theta]})\right), \mu g_1\right)\right) \\ &= H_5\left(e\left(h_\theta+\sum_{k=1}^{l_r} v_k H(Atb_k^{[\theta]}), g_1\right)^{s\mu}\right) \\ &= H_5\left(e\left(h_\theta+\sum_{k=1}^{l_r} v_k H(Atb_k^{[\theta]}), sg_1\right)^{\mu}\right) \\ &= H_5\left(e\left(h_\theta+\sum_{k=1}^{l_r} v_k H(Atb_k^{[\theta]}), pk\right)^{\mu}\right) \end{aligned}$$

$$\begin{aligned} z' &= V \oplus H_2(e(U,d_\theta)) \oplus \{\oplus_{k=1}^{l_\theta} H_2(e(U, Cred_k^{[\theta]}))\} \\ &= z \oplus H_2(e(d_i,h_\theta)^r) \oplus \{\oplus_{k=1}^{l_\theta} H_2(e(d_i, H(Atb_k^{[\theta]}))^r)\} \\ &\quad \oplus H_2(e(rh_i, sh_\theta)) \oplus \{\oplus_{k=1}^{l_\theta} H_2(e(rh_i, sH(Atb_k^{[\theta]})))\} \\ &= z \oplus H_2(e(h_i,h_\theta)^{sr}) \oplus \{\oplus_{k=1}^{l_\theta} H_2(e(h_i, H(Atb_k^{[\theta]}))^{sr})\} \\ &\quad \oplus H_2(e(h_i,h_\theta)^{sr}) \oplus \{\oplus_{k=1}^{l_\theta} H_2(e(h_i, H(Atb_k^{[\theta]}))^{sr})\} \\ &= z \end{aligned}$$

We summarize the main differences between the two schemes in Table 2

Table 2.
Differences Between ZMZ Scheme and Our Scheme

	Setup
ZMZ Scheme	G_1 additive cyclic group
Our Scheme	G_1 elliptic curve group
	SendMsg
ZMZ Scheme	ATB-SET $= \left\{l_j+1, H_5\left(e\left(h_j^* \cdot \prod_{k=1}^{l_j} H(Atb_k^{[j]}), pk\right)^{\mu}\right)\right\}, 1 \le j \le l.$
Our Scheme	ATB-SET $= \left\{\left(V_j, H_5\left(e\left(h_j^* + \sum_{k=1}^{l_j} v_k H(Atb_k^{[j]}), pk\right)^{\mu}\right)\right)\right\}, 1 \le j \le l.$ *
	RcvMsg
ZMZ Scheme	$H_5\left(e\left(d_\theta \cdot \prod_{k=1}^{l_r} Cred_k^{[\theta]}, X\right)\right) = h_r$ with all l_r, h_r pairs in ATB-SET
Our Scheme	$H_5\left(e\left(d_\theta + \sum_{k=1}^{l_r} v_k Cred_k^{[\theta]}, X\right)\right) = h_r$ with the pair (V_r, h_r) in ATB-SET

* $V_j = (v_1, v_2, \ldots, v_{l_j})$ is a vector for the agent h_j^* that determines the necessary attributes for decryption where l_j is the number of the agent's all attributes

5. Security Analysis

A secure authentication protocol should be able to withstand both passive attacks and active attacks. The following security requirements that may be desirable in such protocols have been identified.This section analyzes the scheme's security according to these attacks. We assume that the adversary knows only the public information: the system parameters $(q, G_1, G_2, n, e, g_1, pk, H, H_2, H_3, H_4, H_5, l_m, l_a)$.

Adaptive Chosen Ciphertext:
Adaptive Chosen Ciphertext is a type of chosen ciphertext attack. An adversary determines some ciphertexts to decrypt and tries to discriminate the target one from the others.
The adversary knows the system parameters except for the master key. She can get some private keys d_i's except the target one. Then she adaptively chooses some ciphertexts C_i's using d_i's and takes the plaintext pairs corresponding to C_i's. These pairs include the message M_i and d_i's pseudonym h_i. The adversary challenges by using knowledge deduced from these. She gives a pseudonym h_S as the sender, a policy POL = $h_R \wedge_k Atb_k$ where h_R is the pseudonym of the receiver and two messages M_0, M_1 that she wants to be challenged. Afterward, ciphertexts are given such as

$$C = \{\mu g_1, rh_S, A, M_i \oplus H_4(z), \text{ATB-SET}\}, i = 0, 1$$

where

$$A = z \oplus H_2(e(d_S, h_R)^r) \oplus \{\oplus_{k=1}^{l_R} H_2(e(d_S, H(Atb_k^{[R]}))^r)\},$$

$$\text{ATB-SET} = \left\{\left(V_R, H_5\left(e\left(h_R + \sum_{k=1}^{l_R} v_k H(Atb_k^{[R]}), pk\right)^{\mu}\right)\right)\right\}.$$

For accurate distinguishing, the adversary has to compute the term z. Since the term z occurs in A and $M \oplus H_4(z)$, the adversary has to compute either a pairing or reverse of hash. Since computing the reverse of a cryptographic hash

function is hard, she cannot compute. she tries to compute the pairing $e(d_S, h_R)^r$. However, computing $e(d_S, h_R)^r$ without knowing d_S and r becomes the bilinear Diffie-Hellman problem. Because

$$\begin{aligned} e(d_S, h_R)^r &= e(sh_S, h_R)^r \\ &= e(sag_1, bg_1)^r \\ &= e(g_1, g_1)^{sabr} \end{aligned}$$

where $h_S = ag_1, h_R = bg_1$ and the adversary knows only g_1, ag_1, bg_1, rag_1, and sg_1.
Hence, the adversary cannot distinguish two ciphertexts accurately.

Key-Compromise Impersonation Resilience:
Key-Compromise Impersonation Resilience is the prevention that an adversary impersonating an agent to communicate with other group members successfully, although the agent's long-term private key is disclosed.
Let the adversary try to impersonate the agent with the pseudonym h_S to convince the agent with the pseudonym h_R. First, she has to compute a valid ciphertext, including h_S's information and h_R's attributes. So, she has to compute

$$C = \{\mu g_1, rh_S, A, M \oplus H_4(z), \text{ATB-SET}\}$$

where

$$A = z \oplus H_2(e(d_S, h_R)^r) \oplus \{\oplus_{k=1}^{l_R} H_2(e(d_S, H(Atb_k^{[R]}))^r)\},$$

$$\text{ATB-SET} = \left\{\left(V_R, H_5\left(e\left(h_R + \textstyle\sum_{k=1}^{l_R} v_k H(Atb_k^{[R]}), pk\right)^{\mu}\right)\right)\right\}$$

Since h_R computes the term z bu using rh_S, she computes

$$H_2(e(rh_S, d_R)) = H_2(e(h_S, sh_R)^r).$$

So, the adversary has to compute

$$e(h_S, sh_R)^r = e(ag_1, bg_1)^{sr} = e(g_1, g_1)^{absr}$$

where $a, b \in \mathbb{Z}_q^*$ for the term A to convince h_R. He knows $g_1, sg_1, rag_1, ag_1, bg_1$. To compute $e(g_1, g_1)^{absr}$ from these terms is the bilinear Diffie-Hellman problem. Thus, the adversary cannot compute the necessary terms in polynomial time.
The other way to compute $e(h_S, sh_R)^r$ is to find s since the adversary knows rh_S and h_R. However, s can be computed from only the term $pk = sg_1$, and it is an elliptic curve discrete logarithm problem. Therefore, the adversary cannot compute s.
Hence, the adversary cannot impersonate h_S to convince h_R.

Probing Resistance:
Probing Resistance is the avoidance of validation of ciphertext without knowledge of the attributes ingrained in it.
The adversary chooses a target sender who has the pseudonym h_S, a policy POL such that $h_{Adv} \in \mathsf{POL}$ where the adversary's pseudonym h_{Adv} and message M. Then ciphertext

$$C = \{\mu g_1, rh_S, A, M \oplus H_4(z), \text{ATB-SET}\}$$

where

$$A = z \oplus H_2(e(d_S, h_{Adv})^r) \oplus \{\oplus_k H_2(e(d_S, H(Atb_k))^r)\},$$

$$\text{ATB-SET} = \{(V, H_5\left(e\left(h_{Adv} + \textstyle\sum_k v_k H(Atb_k), pk\right)^{\mu}\right))\}$$

is given to the adversary without the attributes. Then to verify the ciphertext, she has to compute

$$H_2(e(d_S, h_{Adv})^r) \oplus \{\oplus_k H_2(e(d_S, H(Atb_k)^r))\}$$

She can verify $H_2(e(d_S, h_{Adv})^r)$ by computing $H_2(e(rh_S, d_{Adv}))$. However, she cannot verify $\{\oplus_k H_2(e(d_S, H(Atb_k)^r))\}$. Because

$$\begin{aligned} \oplus_k H_2(e(d_S, H(Atb_k))^r) &= H_2(e(d_S, H(Atb_j))^r) \oplus \{\oplus_k H_2(e(d_S, H(Atb_k))^r)\} \\ &= H_2(e(sh_S, H(Atb_j))^r) \oplus \{\oplus_k H_2(e(d_S, H(Atb_k))^r)\} \\ &= H_2(e(s(ag_1), bg_1)^r) \oplus \{\oplus_k H_2(e(d_S, H(Atb_k))^r)\} \\ &= H_2(e(g_1, g_1)^{sabr}) \oplus \{\oplus_k H_2(e(d_S, H(Atb_k))^r)\} \end{aligned}$$

where $h_S = ag_1, H(Atb_j) = bg_1$. Moreover $e(g_1, g_1)^{sabr}$ cannot be distinguished from $e(g_1, g_1)^{\tau}$ by the adversary for any $\tau \in \mathbb{Z}_q^*$ which gives the same result since it is decisional bilinear Diffie-Hellman problem.

Hence, the adversary can only say whether the ciphertext C is valid or not with knowledge of the attributes.

Indistinguishable to Eavesdroppers:

Indistinguishable to Eavesdroppers is the similarity between valid ciphertext and simulated one. If an adversary is not a participant in communication, he should not be able to distinguish them.

Similar to the probing resistance property, the adversary takes the ciphertext to decide whether it is a simulation or real. Again she does not know the attributes which are used in the ciphertext. Then, she cannot know if the bilinear pairing is valid or has some value since it is a decisional bilinear Diffie-Hellman problem.

Hence, the system provides this property.

Hidden Credentials:

Hidden Credentials are the privacy of the attributes. An adversary cannot know which attributes are embedded into ciphertext.

The adversary chooses a target sender h_S, a policy $\mathsf{POL} = h_R \wedge_k (Atb_k)$ and a message M. According to this information, encryption is done, and ciphertext

$$C = \{\mu g_1, rh_S, A, M \oplus H_4(z), \text{ATB-SET}\}$$

where

$$A = z \oplus H_2(e(d_S, h_R)^r) \oplus \{\oplus_k^{l_R} H_2(e(d_S, H(Atb_k^{[R]}))^r)\},$$

$$\text{ATB-SET} = \left\{\left(V_R, H_5\left(e\left(h_R + \sum_k^{l_R} v_k H(Atb_k^{[R]}), pk\right)^{\mu}\right)\right)\right\}$$

is sent to the adversary.

The adversary tries to extract attributes in ATB-SET. In other words, she tries to say what are Atb_k's. For this she has to analyze $H_5\left(e\left(h_R + \sum_k^{l_R} v_k H(Atb_k^{[R]}), pk\right)^{\mu}\right)$. Let's look at this term

$$\begin{aligned} H_5\left(e\left(h_R + \sum_k^{l_R} v_k H(Atb_k^{[R]}), pk\right)^{\mu}\right) &= H_5\left(e\left(h_R + H(Atb_i^{[R]}) + \sum_k^{l_R} v_k H(Atb_k^{[R]}, pk\right)^{\mu}\right) \\ &= H_5\left(e\left(ag_1 + bg_1 + \sum_k^{l_R} v_k H(Atb_k^{[R]}, sg_1\right)^{\mu}\right) \\ &= H_5\left(e\left(ag_1, \mu sg_1\right) e(bg_1, \mu sg_1) e\left(\sum_k^{l_R} v_k H(Atb_k^{[R]}, \mu sg_1\right)\right)\right) \end{aligned}$$

where $h_R = ag_1, H(Atb_i^{[R]})$.

As we can see, the adversary has to decide $e(bg_1, \mu sg_1)$ is a valid attribute or simulation. However, she cannot determine this since it is a decisional bilinear Diffie-Hellman problem.

Hence, the system provides to hide the credentials.

Forward Secrecy:

Forward Secrecy is the protection of previous session keys, even if users' private keys or current session keys are compromised.

Let the adversary know the private key of the sender and the random keys z and μ . She tries to find the previous randoms from the

$$C = \{\mu g_1, rh_S, A, M \oplus H_4(z), \text{ATB-SET}\}$$

where

$$A = z \oplus H_2(e(d_S, h_R)^r) \oplus \{\oplus_k^{l_R} H_2(e(d_S, H(Atb_k^{[R]}))^r)\},$$

However, z and μ cannot be computed from the elements in the ciphertext without knowing the attributes, even if the private key is known. Also, since both elements are chosen randomly, the random keys of the present ciphertext do not give any advantage in constructing the previous ones.

Hence, the system provides forward secrecy.

Unknown Key Share Resilience:

Unknown Key-Share Resilience assures that the key is shared only with the users who intend to share.

The encrypted message is attached to the receiver's public key and attributes. No one can decrypt the ciphertext without knowing the private key and attributes of the receiver. Besides, the agents' private/public keys are created using their identities. For that reason, they cannot be forged by another person. Therefore, the sender ensures that the ciphertext cannot be open by an adversary who does not have the private key of the pseudonym and the attributes embedded in the ciphertext.
Hence, in other words, the system provides unknown key share resilience.

Besides these attacks, ABE schemes are IND-CPA-secure under the standard model or the random oracle model based on the difficulty of the Bilinear Diffie-Hellman problem and related other problems as mentioned in Rasoli et al. survey [23].

6. Asymptotic Analysis

Selecting the right elliptic curve and algorithm is vital for efficient pairing-based cryptographic protocols in practice, as the pairing computation is the primary performance bottleneck. For a detailed analysis of complexities, the interested reader is referred to [24]. In this section, we compare the performances asymptotically. The comparison is explained by using the following notations.

- T_p = Cost of taking power with the number in $\mathbb{Z}_q^*$,
- T_s = Cost of scalar multiplication of point in G_1,
- T_H = Cost of hash functions,
- T_e = Cost of bilinear maps,
- T_i = Cost of computing inverse in $\mod q$.

In both schemes, GM computes system parameters and agents' registration information. These computations cost $3T_p + 2T_H$ in ZMZ scheme and $3T_s + 2T_H$ in our scheme since one exponentiation (respectively scalar multiplication) is required to compute pk, two exponentiation (respectively scalar multiplication) and two hash operation are required to compute agents' pseudonyms, private keys and credentials in ZMZ scheme (respectively in our scheme).

For the sender's cost, similar computations are done in both schemes. Computing the terms in ciphertext, including one attribute, required $2T_p + 6T_H + 3T_e$ in the ZMZ scheme. First, g_1^{μ} and h_i^r are power operations. Second, the ciphertext includes six hash operations where r includes one hash, $M \oplus H_4(z)$ includes one hash, A includes three hash and ATB-SET includes one hash. The third, three bilinear map operations are done to compute A and ATB-SET. The only difference is using scalar multiplication instead of power operation in our scheme while calculating complexity. Therefore computing the terms in the ciphertext is required $2T_s + 6T_H + 3T_e$ in our scheme.

For the receiver's cost, assume that the receiver has n attributes and has to choose l_r attributes for decryption. In this case, ZMZ scheme requires

$$T_p + \left(4 + \binom{n}{l_r}\right) T_H + \left(2 + \binom{n}{l_r}\right) T_e + T_i$$

on receiver part. Because in the ZMZ scheme, the receiver should compute h_r with all possible combinations of its own credentials until finding the one is equal to h_r in ATB-SET. Therefore, at most $\binom{n}{l_r}$ hash computations can be required. However, in the new scheme, this part is changed with a vector that specifies the required attributes for the decryption of the message. In this way, the receiver computes h_r with its own credentials only one time and compares with h_r in ATB-SET. Therefore while the receiver cost is $\left(4 + \binom{n}{l_r}\right) T_H$ in ZMZ scheme, it is $(4+1)T_H$ in our scheme. Same reason as hash, bilinear map computation decreases to $(2+1)$ in our

scheme while it is $\left(2+\binom{n}{l_r}\right)$ in the ZMZ scheme. Thus, our scheme required $T_s + 5T_H + 3T_e + T_i$ computations for decryption.

Hence, ZMZ scheme requires

$$6T_p + \left(12 + \binom{n}{l_r}\right) T_H + \left(5 + \binom{n}{l_r}\right) T_e + T_i$$

and the new scheme requires

$$6T_s + 13T_H + 6T_e + T_i$$

in total according to the group manager's, the sender's and the receiver's operations. The costs for each user in Table 3 can be seen.

Table 3.
Efficiencies of Attribute-Based Protocols

	ZMZ Scheme	New Scheme
GM	$3T_p + 2T_H$	$3T_s + 2T_H$
Sender	$2T_p + 6T_H + 3T_e$	$2T_s + 6T_H + 3T_e$
Receiver	$T_p + \left(4 + \binom{n}{l_r}\right) T_H + \left(2 + \binom{n}{l_r}\right) T_e + T_i$	$T_s + 5T_H + 3T_e + T_i$
Total	$6T_p + \left(12 + \binom{n}{l_r}\right) T_H + \left(5 + \binom{n}{l_r}\right) T_e + T_i$	$6T_s + 13T_H + 6T_e + T_i$

The bilinear map is the most expensive operation among these operations. Thus, it is crucial to decrease the number of these operations. Embedding the attributes using vectors decreases the computation number in the new scheme. By our modifications, the new scheme requires bilinear map computations less than the ZMZ scheme except for the case that the number of necessary attributes is equal to the number of receiver's attributes. In this case, they both compute an equal number of bilinear maps. In the new scheme, specific pairings can be used with pairing-friendly curves for efficiency, as recommended in Moody et al.'s report [25].

The new scheme also requires the hash function, which maps to a point on an elliptic curve, different than the ZMZ scheme. This hash function can be implemented by using a traditional hash function and multiplying this hash with the generator of G_1. Also, Daniel [26] proposed such hash function ECOH2 in NIST's SHA-3 competition, which can be used for implementation. However, using traditional hash and multiplying this hash with the generator of G_1 can be more efficient than ECOH2. This type of hash function is used in the new scheme three times. Therefore, the new scheme can turn these three hash functions into scalar multiplication. Then it requires $9T_s + 10T_H + 6T_e + T_i$ in total.

Even if the number of scalar multiplication increases, the new scheme uses smaller integers to provide the same level of security as the ZMZ scheme since it is based on ECC. A comparison between scalar multiplication and exponentiation depends on many parameters. When the correct parameters are chosen, scalar multiplication is more efficient than exponentiation, according to Rasoli et al., [23]. Moreover, in the literature, several studies show that ECC coprocessor can speed up an elliptic curve scalar multiplication suitable for low area constraint applications and high-speed applications even considering the power consumption overhead [27], [28], [29]. Hence, according to bilinear map operations, small integer sizes, and the parameters used in construction, the new scheme is more efficient than the ZMZ scheme.

Rasoli et al. give the cost of operations in [23]. The computational cost may be calculated approximately using their results. However, these costs vary depending on the selection of curves and parameters. Youssef El Housni gives benchmarking of pairing-friendly elliptic curves libraries [1]. Also, in [30], the authors compare the computational costs expressed in 10^3 clock cycles for schemes for 100 attributes on many efficient curves.

7. Conclusion

In this study, we presented an attribute-based authentication for multi-agent systems inspired by

1. https://hackmd.io/@gnark/eccbench

Zhang et al. [1]. Their scheme is based on bilinear mapping, which is too expensive. Unlike the previous work, our scheme is based on ECC, and the security is based on ECDLP. ECC fits well for resource-constrained environments with the following features: it requires a smaller key size on the same level of security, its scalar multiplication is faster, and it is easy to transmit and implement. It is an alternative in restricted environments, such as portable and wireless devices, with much smaller area usage (bit size) and low energy consumption than public key encryption systems such as RSA. In this paper, Real-time communication encryption (sending-receiving phases) is based on hash functions and ECC operations; therefore the protocol has lower communication and computation overheads. In addition, controlling the credentials is a heavy burden for the receiver in their work. We simplified this operation and made our scheme practical for the application areas. In all these application areas, the privacy of attributes is an important issue. Thus, we protected the user's personal information (credentials) privacy. Revocation, another crucial issue in these systems, is provided using a list of members. The group manager subtracts pseudonyms from the list, which provides authentication to revoke agents from the system as a trusted third party. Besides, our scheme provides the security properties; adaptive chosen ciphertext, key-compromise impersonation resilience, probing resistance, indistinguishable to eavesdroppers, forward secrecy, and unknown key-share resilience.

References

[1] Q. Zhang, Y. Mu, and M. Zhang, "Attribute-based authentication for multi-agent systems with dynamic groups," *Computer Communications*, vol. 34, pp. 436–446, 2011.

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 47–53.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology — CRYPTO 2001*, J. Kilian, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 213–229.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology – EUROCRYPT 2005*, R. Cramer, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 457–467.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM Conference on Computer and Communications Security*, vol. 89-98, 2006, pp. 89–98.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy (SP '07)*, 2007, pp. 321–334.

[7] S. Zhu, L. Zhan, H. Qiang, D. Fu, W. Sun, and Y. Tang, "A fuzzy attribute-based authentication scheme on the basis of lagrange polynomial interpolation," in *Human Centered Computing*, Q. Zu, B. Hu, N. Gu, and S. Seng, Eds. Springer International Publishing, 2015, pp. 685–692.

[8] J. P. Yun, H. Kim, and D. H. Lee, "An improved fuzzy attribute-based authentication," in *5th International Conference on IT Convergence and Security (ICITCS)*, 2015, pp. 1–5.

[9] L. Guo, C. Zhang, J. Sun, and Y. Fang, "Paas: A privacy-preserving attribute-based authentication system for ehealth networks," in *IEEE 32nd International Conference on Distributed Computing Systems*, 2012, pp. 224–233.

[10] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in *ACM Workshop on Cloud Computing Security Workshop*, 2010, p. 47–52.

[11] M. Barua, X. Liang, R. Lu, and X. Shen, "Peace: An efficient and secure patient-centric access control scheme for ehealth care system," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2011, pp. 970–975.

[12] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *27th Conference on Computer Communications-IEEE INFOCOM 2008*. IEEE, 2008, pp. 246–250.

[13] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking together efficient authentication, revocation, and privacy in vanets," in *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2009, pp. 1–9.

[14] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in vanets," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616–629, 2011.

[15] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for vanets," *IEEE Transactions on vehicular technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[16] D. Huang and M. Verma, "Aspe: attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1526 – 1535, 2009.

[17] X. Liu, Z. Shan, L. Zhang, W. Ye, and R. Yan, "An efficient

message access quality model in vehicular communication networks," *Signal Processing*, vol. 120, pp. 682 – 690, 2016.

[18] Z. Guo, G. Wang, Y. Li, J. Ni, R. Du, and M. Wang, "Accountable attribute-based data-sharing scheme based on blockchain for vehicular ad hoc network," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 7011–7026, 2023.

[19] T. Gan, Y. Liao, Y. Liang, Z. Zhou, and G. Zhang, "Partial policy hiding attribute-based encryption in vehicular fog computing," *Soft Computing*, vol. 25, pp. 10 543–10 559, 2021.

[20] J. Ma, T. Li, J. Cui, Z. Ying, and J. Cheng, "Attribute-based secure announcement sharing among vehicles using blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 873–10 883, 2021.

[21] Q. Zhang, Y. Gan, L. Liu, X. Wang, X. Luo, and Y. Li, "An authenticated asymmetric group key agreement based on attribute encryption," *Journal of Network and Computer Applications*, vol. 123, pp. 1–10, 2018.

[22] M. Wooldridge, *An Introduction to MultiAgent Systems*, 2nd ed. John Wiley & Sons, 2009.

[23] M. Rasori, M. L. Manna, P. Perazzo, and G. Dini, "A survey on attribute-based encryption schemes suitable for the internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8269–8290, 2022.

[24] G. D. Micheli, P. Gaudry, and C. Pierrot, "Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields," Cryptology ePrint Archive, Paper 2020/329, 2020. [Online]. Available: https://eprint.iacr.org/2020/329

[25] D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky, and L. Chen, "Report on pairing-based cryptography," *Journal of research of the National Institute of Standards and Technology*, vol. 120, p. 11, 2015.

[26] M. A. Halcrow and N. Ferguson, "A second pre-image attack against elliptic curve only hash (ecoh)," Cryptology ePrint Archive, Paper 2009/168, 2009. [Online]. Available: https://eprint.iacr.org/2009/168

[27] R. Bilal and M. Rajaram, "High speed and low space complexity fpga based ecc processor," *International Journal of Computer Applications*, vol. 8, no. 3, pp. 5–10, 2008.

[28] A. A.-A. Gutub and S. Arabia, "Remodeling of elliptic curve cryptography scalar multiplication architecture using parallel jacobian coordinate system," *International Journal of Computer Science and Security (IJCSS)*, vol. 4, no. 4, pp. 373–435, 2010.

[29] R. Bilal and M. Rajaram, "Design and implementation of high performance ecc coprocessor," *International Journal of Engineering Science*, vol. 2, no. 11, pp. 6759–6770, 2010.

[30] A. de la Piedra, M. Venema, and G. Alpár, "Abe squared: Accurately benchmarking efficiency of attribute-based encryption," Cryptology ePrint Archive, Paper 2022/038, 2022. [Online]. Available: https://eprint.iacr.org/2022/038