IDENTITY/ATTRIBUTE-BASED AUTHENTICATION PROTOCOLS BASED ON PAIRINGS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

GÜLNİHAL ÖZTÜRK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2020

Approval of the thesis:

IDENTITY/ATTRIBUTE-BASED AUTHENTICATION PROTOCOLS BASED ON PAIRINGS

submitted by **GÜLNİHAL ÖZTÜRK** in partial fulfillment of the requirements for the degree of **Master of Science in Cryptography Department, Middle East Technical University** by,

Prof. Dr. Ömür Uğur
Director, Graduate School of **Applied Mathematics** ________________

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography** ________________

Assoc. Prof. Dr. Ali Doğanaksoy
Supervisor, **Mathematics Department, METU** ________________

Assist. Prof. Dr. Nurdan Saran
Co-supervisor, **Computer Engineering Dept., Çankaya Uni.** ________________

Examining Committee Members:

Assoc. Prof. Dr. Murat Cenk
Cryptography, METU ________________

Assoc. Prof. Dr. Ali Doğanaksoy
Mathematics Department, METU ________________

Assist. Prof. Dr. Nurdan Saran
Computer Engineering Department, Çankaya University ________________

Assoc. Prof. Dr. Fatih Sulak
Mathematics Department, Atılım University ________________

Assoc. Prof. Dr. Oğuz Yayla
Cryptography, METU ________________

Date: ________________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name:	GÜLNİHAL ÖZTÜRK
Signature :	

ABSTRACT

IDENTITY/ATTRIBUTE-BASED AUTHENTICATION PROTOCOLS BASED ON PAIRINGS

Öztürk, Gülnihal
M.S., Department of Cryptography
Supervisor : Assoc. Prof. Dr. Ali Doğanaksoy
Co-Supervisor : Assist. Prof. Dr. Nurdan Saran

September 2020, 40 pages

Authentication is one of the most important goals in cryptography. It provides sharing information with only authorized people and protecting data from being modified. Authentication can be achieved in various ways such as password-based, symmetric-key and public-key. The public-key authentication is the most preferred one among these options. It provides construction of key pairs and verification with based on hard mathematical problems. Public-key authentication is used as a basis for two important ideas: Identity-Based Authentication (IBA) and Attribute-Based Authentication (ABA). The IBA systems are actually specialized public-key encryption systems where the public key is generated using the user identity information. ABA systems, which are the other important idea, are the generalizations of the IBA systems. While IBA systems cover only one attribute about users, ABA systems cover more than one attribute.

In this thesis, identity-based and attribute-based authentication protocols are analyzed, and a new attribute-based authentication protocol is proposed. First, it is given the details and comparison of ID-based authentication protocols Shim, Yuan and Li [37], Tseng 2017 [35] and Tseng 2015 [34], which are based on elliptic curve. Shim, Yuan and Li [37] and Tseng 2017 [35] use pairings for authentication, while Tseng 2015 [34] uses hash functions. Their securities and performances are analyzed. They provide the security properties such as known-key security, forward secrecy, key-compromise impersonation and unknown-key share. They also resist the passive, man-in-the-middle and reveal attacks. The protocols are more efficient than the protocols which are based on public-key by virtue of elliptic curve. Tseng 2015 [34] is the most efficient one among them since it uses only hash functions. Also, the Zhang, Mu and Zhang [41] attribute-based authentication protocol is studied. Then a new protocol, which is inspired by it, is designed. While Zhang et al. [41] is based on public-key, the new protocol is constructed on elliptic curve basis. Moreover, controlling of attributes is simplified. It decreases the number of operations to determine the necessary attributes. In this way, the computational cost is reduced. The new protocol's security analysis is presented and showed that the protocol is resistant to the following attack scenarios; adaptive chosen ciphertext, key-compromise impersonation, probing resistance, indistinguishable to eavesdroppers, forward secrecy and unknown key-share.

Keywords: id-based authentication, attribute-based authentication, pairing-based cryptography

ÖZ

KİMLİK VE ÖZELLİK TABANLI EŞLEME TABANLI KİMLİK DOĞRULAMA PROTOKOLLERİ

Öztürk, Gülnihal

Yüksek Lisans, Kriptografi Bölümü

Tez Yöneticisi : Doç. Dr. Ali Doğanaksoy

Ortak Tez Yöneticisi : Dr. Öğr. Üyesi Nurdan Saran

Eylül 2020, 40 sayfa

Kimlik doğrulama, kriptografideki en önemli hedeflerden biridir. Bilgilerin yalnızca yetkili kişilerle paylaşılmasını ve değiştirilmekten korunmasını sağlar. Kimlik doğrulama; parola tabanlı, simetrik anahtar ve açık anahtar gibi çeşitli yollarla yapılabilir. Açık anahtar kimlik doğrulaması, bu seçenekler arasında en çok tercih edilenidir. Zor matematiksel problemlere dayalı olarak anahtar çiftlerinin oluşturulmasını ve doğrulanmasını sağlar. Açık anahtar kimlik doğrulaması iki önemli fikir için temel olarak kullanılır: Kimlik Tabanlı Kimlik Doğrulama ve Özellik Tabanlı Kimlik Doğrulama. Kimlik tabanlı kimlik doğrulama sistemleri aslında açık anahtarın kullanıcının kimlik bilgileri kullanılarak oluşturulduğu özelleştirilmiş açık anahtar şifreleme sistemleridir. Bir diğer önemli fikir olan özellik tabanlı kimlik doğrulama sistemleri, kimlik tabanlı kimlik doğrulama sistemlerinin genellemeleridir. Kimlik tabanlı sistemler, kullanıcılar hakkında yalnızca bir niteliği kapsarken özellik tabanlı sistemler birden fazla niteliği kapsar.

Bu tezde, kimlik tabanlı ve özellik tabanlı kimlik doğrulama protokolleri incelenmiş ve yeni bir özellik tabanlı kimlik doğrulama protokolü önerilmiştir. İlk olarak, Shim,Yuan ve Li [37], Tseng 2017 [35] ve Tseng 2015 [34]'in eliptik eğriye dayanan kimlik tabanlı kimlik doğrulama protokollerinin ayrıntıları ve karşılaştırması verilmiştir. Shim, Yuan ve Li [37] ve Tseng 2017 [35], kimlik doğrulama için eşleşmeleri kullanırken, Tseng 2015 [34] özet fonksiyonlarını kullanır. Güvenlikleri ve performansları analiz edilmiştir. Bilinen anahtar güvenliği, ileri gizlilik, anahtar-uzlaşma kimliğe bürünme ve bilinmeyen anahtar paylaşımı gibi güvenlik özelliklerini sağlarlar. Ayrıca pasif, ortadaki adam ve açığa çıkarma saldırılarına karşı direnir. Protokoller, eliptik eğri sayesinde açık anahtarlı şifrelemeye dayanan protokollerden daha verimlidir. Tseng 2015 [34], yalnızca özet fonksiyonlarını kullandığı için aralarında en verimli olanıdır. Ayrıca Zhang, Mu ve Zhang [41] özellik tabanlı kimlik doğrulama protokolü de incelenmiştir. Daha sonra ondan esinlenerek yeni bir protokol tasarlanmıştır. Zhang et al. [41] açık anahtara dayalıyken, yeni protokol eliptik eğri temelinde oluşturulmuştur. Ayrıca, özelliklerin kontrolü basitleştirilmiştir. Bu basitleştirme gerekli nitelikleri belirlemek için işlem sayısını azaltır. Bu şekilde hesaplama maliyeti azaltılır. Yeni protokolün güvenlik analizi sunulmuş ve protokolün sıralanan saldırı senaryolarına dirençli olduğu gösterilmiştir; adaptif kapalı metin, anahtar-uzlaşma kimliğe bürünme, deneme direnci, dinleyicinin ayırt edememesi, ileri gizlilik ve bilinmeyen anahtar paylaşımı.

Anahtar Kelimeler: kimlik tabanlı kimlik doğrulama, özellik tabanlı kimlik doğrulama, eşleme tabanlı kriptografi

To my family

ACKNOWLEDGMENTS

First of all, I would like to express my very great appreciation to my thesis supervisor Assoc. Prof. Dr. Ali Doğanaksoy for his guidance, encouragement and valuable advices during preparation of this thesis. I also would like to thank my co-advisor Assist. Prof. Dr. Nurdan Saran for her patient guidance, motivation, suggestions, time and support.

I am very grateful to my family for their endless support and continuous encouragement. I wish to thank them for always believing in me and their love.

I would like to thank my friends İpek Karaman and Gizem Doğru for all their help, sisterhood, and for being there for me and supporting me unconditionally.

I also would like to thank BAMBAM for their friendship, help and entertainment. They have always been there for me to feel good.

I specially thank Tolga Sapmaz for his patience, support and encouragement. He has always been there for me and believed in me.

Lastly, I wish to thank FAME CRYPT and my colleagues for precious supports.

TABLE OF CONTENTS

ABSTRACT vii

ÖZ ix

ACKNOWLEDGMENTS xiii

TABLE OF CONTENTS xv

LIST OF TABLES xix

LIST OF FIGURES xx

LIST OF ABBREVIATIONS xxi

CHAPTERS

1 INTRODUCTION 1

2 PRELIMINARIES 5

2.1 Bilinear Pairings 5

2.2 Mathematical Problems 5

2.3 Security Properties 6

3 IDENTITY-BASED AUTHENTICATION 7

3.1 Notations 7

3.2 Review of Protocols 8

3.2.1 Shim, Yuan and Li's Protocol [37] 9

3.2.2 Tseng, Huang and You's Protocol [35] 10

3.2.3 Tseng, Huang, Tsai and Tseng's Protocol [34] 11

3.3 Security Analysis 13

3.3.1 Known-Key Security 13

3.3.2 Forward Secrecy 14

3.3.3 Key-Compromise Impersonation 15

3.3.4 Unknown Key-Share 16

3.3.5 Passive Attack 16

3.3.6 Man-in-the-middle Attack 16

3.3.7 Reveal Attack 17

3.4 Performance Analysis 19

4 ATTRIBUTE-BASED AUTHENTICATION 21

4.1 Notations 22

4.2 Zhang,Mu and Zhang Scheme [41] 23

4.3 The New Scheme 25

4.4 Security Analysis 27

4.4.1 Adaptive Chosen Ciphertext 28

4.4.2 Key-Compromise Impersonation 28

4.4.3 Probing Resistance 29

4.4.4 Indistinguishable to Eavesdroppers 30

4.4.5 Hidden Credentials 30

4.4.6 Forward Secrecy 31

4.4.7 Unknown Key Share 31

4.5 Computational Overhead 31

4.6 Performance Analysis 32

5 CONCLUSION 35

REFERENCES 37

LIST OF TABLES

Table 3.1 Security Properties of Identity-Based Protocols 18

Table 3.2 Attacks on Identity-Based Protocols 19

Table 3.3 Efficiencies of Identity-Based Protocols 19

Table 4.1 Security Properties of Attribute-Based Protocols 31

Table 4.2 Efficiencies of Attribute-Based Protocols 32

LIST OF FIGURES

Figure 3.1 Shim, Yuan and Li’s Protocol 10

Figure 3.2 Tseng, Huang and You’s Protocol 12

Figure 3.3 Tseng, Huang, Tsai and Tseng’s Protocol 14

LIST OF ABBREVIATIONS

ECC	Elliptic Curve Cryptography
IBE	Identity-Based Encryption
ABE	Attribute-Based Encryption
ID-AKA	Identity-Based Authenticated Key Agreement
ECDLP	Elliptic Curve Discrete Logarithm Problem
BDH	Bilinear Diffie-Hellman Problem
CDH	Computational Diffie-Hellman Problem
DBDH	Decisional Bilinear Diffie-Hellman Problem
SYL	Shim,Yuan and Li's Protocol
THY	Tseng, Huang and You's Protocol
THTT	Tseng, Huang, Tsai and Tseng's Protocol
ZMZ	Zhang, Mu and Zhang's Protocol
KGC	Key Generation Center
GM	Group Manager
eHealth	Electronic Health
VANET	Vehicular Ad Hoc Networks
ECOH2	Elliptic Curve Only Hash 2

CHAPTER 1

INTRODUCTION

Information needs protection in online operations like communications or data storage if it is wanted to share only with the authorized people. Cryptography is the science that aims to provide this protection. It secures the information by attaining confidentially, data integrity, non-repudiation and authentication. Confidentially and data integrity are about protecting the information itself. Non-repudiation and authentication are about ensuring that information is shared with accurate people.

First the information is encrypted for protection from the malicious attacks by using a cryptographic encryption algorithm. Although the encryption algorithm is secure, the information may still be insecure. In other words, the encrypted information can be captured by an adversary with or without the owners' knowledge. However, it can be prevented by ensuring who reach the data. Authentication protocols provide this in cryptography. They protect the information from being corrupted. This information can be the identity that the information comes from, as can be data.

Authentication can be done in various ways such as password-based, symmetric-key, public-key. Password-based authentication is the one way that uses names and passwords matches with these names in the memory. The first idea is proposed by Bellovin and Merritt [2]. This protocol authenticates the users by establishing a common key between them. Steiner et al. [32] improved this idea. They constructed a scheme for three party authentication. Symmetric-key is the other way of the authentication which validates the identities by using symmetric-key techniques. In these systems, a random message is encrypted with a shared secret and then decrypted by authorization with the same secret. In this way authentication is done. Bird et al. [6] constructed such an authentication scheme. Then, it was improved by Janson and Tsudik [22]. Another way of authentication is public-key authentication. In fact, it can be called Diffie-Hellman authentication. Diffie and Hellman [13] proposed the first one in 1976. It accomplishes verification in the key agreement. Their protocol is based on discrete logarithm problem. However, their protocol was vulnerable to man-in-the-middle attack. The attack corrupts the data integrity and causes that the users create different keys from each other. Although it is not secure to use, most of the public-key authentication protocols were built in consideration of their work.

Public-key is the most preferred one among all these works. It is used as a basis in two important ideas: Identity-Based Encryption and Attribute-Based Encryption. The IBE systems are actually specialized public-key encryption systems. They create the public-private key pair based on the users' unique information, identities. In 1984, Shamir [29] proposed the first IBE on 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 key generation center. In this way, they authenticate by their keys. Boneh and Franklin [7] constructed a more practical one by using elliptic curve and pairing as basis. They detailed the IBE construction by dividing into fundamental algorithms. Cocks gave another idea in his identity-based scheme [11] and use quadratic residue for the security of the protocol. Afterward, the idea of identity-based started to use in key agreement protocols. In the same way with the encryption schemes, users' public-private keys are based on their identities. This provides authentication before building the secret key by their identities. Smart [31] first introduced the ID-based authenticated key agreement protocol. Pairing properties contribute to authentication and resistance for some attacks in this scheme. However, Shim [23] proved that the Smart's scheme could not secure the previous secret keys. He proposed a new ID-AKA which has the forward secrecy property in the same work.

The other important idea ABE systems are a generalization of the IBE systems. While identity-based systems cover only one attribute about users, attribute-based systems cover more than one attribute. Many applications need that more than one attribute must be possessed to authorize. Authentication of one attribute at a time costs an enormous amount of time when the number of attributes is high. Nonetheless, Sahai and Waters [28] proposed the attribute-based system, which was named Fuzzy Identity-Based in 2005. The system is encryption that can be decrypted if the attributes match according to a threshold. Yet it has some limits because it links the attributes either key or ciphertext. Goyal et al. worked on this issue. They proposed new concepts, Key-Policy Attribute-Based Encryption and Ciphertext-Policy Attribute-Based Encryption [14], and the system became more practical. Although these studies made some progress, there are still lacks. Bethencourt et al. [3] and Cheung et al. [10] analyzed the ciphertext-policy part that Goyal et al. did not detail. These works focus on one authority. Chase and Melissa [9] expanded the systems to multi-authority. In the light of their works, Zhu et al. [42] 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 the collusion and impersonation attacks [38].

This thesis is a study on identity-based and attribute-based cryptography. Its main contributions are the followings:

- It gives general information about identity-based and attribute-based systems.
- It compares Diffie Hellman authenticated key agreement protocols and explains general

forms of these types of systems.

- The security properties, which are essential in key agreement protocol, are told and analyzed.
- Efficiencies of the constructions are studied. According to applications of the protocols, some ideas are given for this type of systems' structures.
- An attribute-based authentication system is represented. Inspired by this system, a new one is designed.
- Pairings and elliptic curves are used in the new ABE system as a basis.
- A more practical way to transform and control of attribute is suggested. It can decrease the data traffic on the network.

The thesis organization is as follows. In Chapter 2, a summary of mathematical background, which is needed in the studies, is given. It focuses on ID-based authenticated key agreement protocols in Chapter 3. A review and comparison of the protocols are given in this chapter. An attribute-based authentication system is examined in Chapter 4. Firstly review of the system is given, then the original study on the system is explained in the fourth chapter. Finally, the conclusion is made in Chapter 5.

CHAPTER 2

PRELIMINARIES

In this chapter the mathematical background and definition of difficult mathematical problems which is used by the analyzed protocols are explained. Also, the security properties, which are necessary for the authentication protocols, are defined.

2.1 Bilinear Pairings

The protocols, which are studied in this thesis, are constructed by using bilinear pairings on elliptic curves. Bilinear pairings are maps with some properties between algebraic and elliptic curve groups.

Bilinear Pairings:

Suppose G_1 is a cyclic additive group of prime order q, and G_2 is a cyclic multiplicative group of prime order q. P is the generator of G_1. G_1 is a subgroup of additive group of elliptic curve points, and G_2 is a subgroup of multiplicative algebraic group. Define a map e from $G_1 \times G_1$ to G_2 which satisfies :

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

Non-degeneracy : $e(P, P) \neq 1$ for the generator P of G_1

Computable: $e(R, Q)$ is computable for all R, Q of G_1 by an efficient algorithm

Then e is a bilinear map which is named pairing.

2.2 Mathematical Problems

Discrete logarithm problem and Diffie-Hellman problem definitions are given in this part. The protocols provide security with the hardness of these problems. These problems cannot be solved with polynomial-time algorithms using classical computers.

Elliptic Curve Discrete Logarithm Problem : Assume G_1 is additive elliptic curve group. Let $P, Q \in G_1$. Assume $Q = aP$ for some $a \in \mathbb{Z}_q^*$. Then it is difficult to compute a from P, Q.

Computational Diffie-Hellman Problem : Assume G_1 is additive elliptic curve group and P is the generator of G_1. Given $P, aP, bP \in G_1$ for unknown $a, b \in \mathbb{Z}_q^*$ it is difficult to compute abP.

Bilinear Diffie-Hellman Problem: Assume G_1 is additive elliptic curve group and P is the generator of G_1. Let $P, aP, bP, cP \in G_1$. Assume that $a, b, c \in \mathbb{Z}_q^*$ are unknown. Then it is difficult to compute $e(P, P)^{abc}$.

Decisional Bilinear Diffie-Hellman Problem: Assume G_1 is additive elliptic curve group and P is the generator of G_1. Let $P, aP, bP, cP \in G_1$, $a, b, c \in \mathbb{Z}_q^*$, 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 $(P, aP, bP, cP, e(P, P)^{abc})$ and (P, aP, bP, cP, τ).

2.3 Security Properties

The authentication protocols should withstand essential security properties. These main property definitions are given in this section.

Known-Key Security : In each round, a unique key should be generated as independent from the other rounds, and even if other secret keys are compromised, it should not be exposed.

Unknown Key-Share : The users are sure that they establish a key with the users who wanted to establish with.

Adaptive Chosen Ciphertext : It is a type of chosen ciphertext attack such that an adversary tries to discriminate the target one from the ciphertexts determined and examined previously.

Key-Compromise Impersonation : An adversary cannot impersonate an user to communicate others successfully, although the user's secret key is disclosed.

Probing Resistance : The validation of ciphertext cannot be done without the knowledge of the attributes ingrained in it.

Indistinguishable to Eavesdroppers : An adversary should not be able to distinguish valid ciphertext and simulated one if he is not a participant in communication.

Hidden Credentials : It is the privacy of the attributes. An adversary cannot know which attributes are embedded in ciphertext.

Forward Secrecy : It is the protection of previous session keys, even if the secret keys of users are compromised.

CHAPTER 3

IDENTITY-BASED AUTHENTICATION

The identity-based systems are the systems that create secret keys by using users' identities. The first one of these systems is proposed by Shamir [29]. After the idea is proposed, Boneh and Franklin [7] worked on and detailed this concept. Later many studies are done in this area. Smart's [31] ID-AKA protocol is one of them. His scheme claimed that long-term private key secures the previous session keys. However, the incorrectness of this claim is proven by Shim [23]. He constructed a new ID-AKA protocol based on pairing, but his protocol does not provide resistance to man-in-the-middle attack. Yuan and Li [37] modified Shim's protocol and proposed their ID-AKA protocol. They solved its problem. Meanwhile, Islam, Biswas [21] and He et al. [12] studied protocols for mobile users. They proposed ID-AKA based on elliptic curve. Afterward, Tseng 2017 [35] and Tseng 2015 [34] created their ID-AKA for mobile users. The protocol in [35] is based on elliptic curve, while the protocol in [34] is based on pairing.

In this chapter, Shim-Yuan-Li's protocol [37], Tseng 2017 protocol [35] and Tseng 2015 protocol [34] are compared. First, the reviews of the protocols are given, and then analysis of the security and efficiency according to their performance test results are explained.

3.1 Notations

In Chapter 3, the protocols are explained with the same notations, which are given below.

- G_1 is additive cyclic group with prime order p,
- G_2 is multiplicative cyclic group with prime order p,
- e is a bilinear map from $G_1 \times G_1$ to G_2,
- P is generator of additive group G_1,
- s is master key of system $s \in \mathbb{Z}_p^*$,
- P_{pub} is public key of system,

- S_{ID} is private key of the user with identity ID,
- H_1, H_2, H_3, H_4 are hash functions from $\{0,1\}^*$ to G_1,
- f_1, f_2, f_3, f_4 are hash functions from $\{0,1\}^*$ to $\{0,1\}^n$ where n is a fixed length and $2^n < p$,
- H is key derivation function,
- ID is identity of any participant,
- A is identity of Alice,
- B is identity of Bob.

Since Tseng 2017 [35] and Tseng 2015 [34] protocols are for the mobile environment, they occur between client and server. For keeping terminology the same, Alice and Bob are used instead of client and server, respectively.

3.2 Review of Protocols

In this section, the protocols are given in details. There are setup,key extract and authenticated key agreement phases in these protocols. Since the algorithms setup phases are similar, we examine them together.

Setup

The Key Generation Center selects

- Additive group G_1,
- Multiplicative group G_2,
- Bilinear map e,
- Generator P,
- Hash functions $H_1, H_2 : \{0,1\}^* \to G_1$,
- Hash functions $f_1, f_2, f_3, f_4 : \{0,1\}^* \to \{0,1\}^n$,
- Master key of system $s \in \mathbb{Z}_p^*$ and
- Key derivation function H.

In the Shim, Yuan and Li's protocol, KGC computes public key of the system $P_{pub} = sP$ and publishes $< G_1, G_2, e, P, P_{pub}, H_1, H >$.

In the Tseng, Huang and You's protocol, KGC computes public key of the system $P_{pub} = sP$ and publishes $< G_1, P, P_{pub}, f_1, f_2, f_3, f_4 >$.

In the Tseng,Huang,Tsai and Tseng's protocol, KGC computes public key of the system $P_{pub} = sP$ and publishes $< G_1, G_2, e, P, P_{pub}, H_1, H_2, f_1, f_2, f_3, f_4 >$.

3.2.1 Shim, Yuan and Li's Protocol [37]

Key Extract

KGC computes the public key of a user as

$$Q_{ID} = H_1(ID)$$

and the private key as

$$S_{ID} = sQ_{ID}.$$

Authenticated Key Agreement

1. Alice chooses a random number $a \in \mathbb{Z}_p^*$, computes $T_A = aP$ and sends T_A to Bob.
2. Bob chooses a random number $b \in \mathbb{Z}_p^*$, computes $T_B = bP$ and sends T_B to Alice.
3. After taking T_B, Alice computes $sk_A = aT_B$ and the shared secret
$$K_{AB} = e(aP_{pub} + S_B, T_B + Q_B).$$
4. Similarly, after taking T_A, Bob computes $sk_B = bT_A$ and the shared secret
$$K_{BA} = e(T_A + Q_A, bP_{pub} + S_B).$$
5. Then they have the same shared secret
$$\begin{aligned} K_{AB} &= K_{BA} \\ &= e(P,P)^{abs} e(P,Q_B)^{as} e(Q_A,P)^{bs} e(Q_A,Q_B)^{s} \end{aligned}$$
and compute the session key as
$$H(A, B, sk_A, K_{AB})$$
and
$$H(A, B, sk_B, K_{BA}).$$

The diagram of the scheme can be seen in figure 3.1.

Alice		**Bob**
$a \in \mathbb{Z}_p^*$		$b \in \mathbb{Z}_p^*$
$T_A = aP$		$T_B = bP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$sk_A = aT_B$		$sk_B = aT_A$
$K_{AB} = e(aP_{pub} + S_B, T_B + Q_B)$		$K_{BA} = e(T_A + Q_A, bP_{pub} + S_B)$
$H(A, B, sk_A, K_{AB} = K_{BA})$		$H(A, B, sk_B, K_{AB} = K_{BA})$

Figure 3.1: Shim, Yuan and Li's Protocol

3.2.2 Tseng, Huang and You's Protocol [35]

Key Extract

The KGC chooses a random number $l \in \mathbb{Z}_p^*$ for a user with identity ID. Then KGC computes

$$\begin{aligned} Q_{ID} &= lP, \\ h_{ID} &= f_1(ID, Q_{ID}), \\ R_{ID} &= l + h_{ID}s \end{aligned}$$

and gives to a user the private key pair as

$$S_{ID} = (R_{ID}, Q_{ID}).$$

The user can verify the private key pair by controlling if the equality

$$R_{ID}P = Q_{ID} + h_{ID}P_{pub}$$

holds or not.

Authenticated Key Agreement

1. Alice chooses a random number $a \in \mathbb{Z}_p^*$, computes $T_A = aP$ and sends A, Q_A, T_A to Bob.

2. Bob takes A, Q_A, T_A, chooses a random number $b \in \mathbb{Z}_p^*$ and computes

$$\begin{aligned} T_B &= bP, \\ h_A &= f_1(A, Q_A), \\ sk_B &= (b + R_B)(T_A + Q_A + h_AP_{pub}) \oplus bT_A, \\ Auth_B &= f_2(A, B, T_A, T_B, sk_B) \end{aligned}$$

   and sends $Q_B, T_B, Auth_B$ to Alice.

3. Alice takes $Q_B, T_B, Auth_B$ and computes

$$\begin{aligned} h_B &= f_1(B, Q_B), \\ sk_A &= (a + R_A)(T_B + Q_B + h_B P_{pub}) \oplus aT_B. \end{aligned}$$

   Then she checks if

$$Auth_B = f_2(A, B, T_A, T_B, sk_A)$$

   holds or not. If the equality holds, Bob is authenticated.

   Alice continues by computing

$$Auth_A = f_3(A, B, T_A, T_B, sk_A, Auth_B)$$

   and sends $Auth_A$ to Bob.

4. Bob takes $Auth_A$ and checks if

$$Auth_A = f_3(A, B, T_A, T_B, sk_B, Auth_B)$$

   holds or not. If the equality holds, Alice is authenticated.

5. Then they both compute the session key as

$$f_4(A, B, T_A, T_B, sk_A, Auth_B, Auth_A)$$

   and

$$f_4(A, B, T_A, T_B, sk_B, Auth_B, Auth_A).$$

The diagram of the scheme can be seen in figure 3.2.

3.2.3 Tseng, Huang, Tsai and Tseng's Protocol [34]

Key Extract

The KGC chooses a random number $l \in \mathbb{Z}_p^*$ for a user with identity ID, then computes

$$\begin{aligned} Q_{ID,1} &= lP, \\ h_{ID} &= f_1(ID, Q_{ID,1}), \\ R_{ID,1} &= l + h_{ID}s, \\ Q_{ID,2} &= H_1(ID), \\ R_{ID,2} &= sQ_{ID,2} \end{aligned}$$

and gives to user the private key tuple as

$$S_{ID} = (R_{ID,1}, R_{ID,2}, Q_{ID,1}).$$

Authenticated Key Agreement

Alice		**Bob**
$a \in \mathbb{Z}_p^*$		$b \in \mathbb{Z}_p^*$
$T_A = aP$	$\xrightarrow{A,T_A,Q_A}$	$T_B = bP$
		$h_A = f_1(A, Q_A)$
		$sk_B = (b+R_B)(T_A+Q_A+h_AP_{pub}) \oplus bT_A$
	$\xleftarrow{T_B,Q_B,Auth_B}$	$Auth_B = f_2(A, B, T_A, T_B, sk_B)$
$h_B = f_1(B, Q_B)$		
$sk_A = (a + R_A)(T_B + Q_B + h_BP_{pub}) \oplus aT_B$		
$Auth_B = f_2(A, B, T_A, T_B, sk_A)$		
$Auth_A = f_3(A, B, T_A, T_B, sk_A, Auth_B)$	$\xrightarrow{Auth_A}$	
		$Auth_A = f_3(A, B, T_A, T_B, sk_B, Auth_B)$
$f_4(A, B, T_A, T_B, sk_A, Auth_B, Auth_A)$		$f_4(A, B, T_A, T_B, sk_B, Auth_B, Auth_A)$

Figure 3.2: Tseng, Huang and You's Protocol

1. Alice chooses a random number $a \in \mathbb{Z}_p^*$ and make offline computations

$$\begin{aligned} T_{A,1} &= aP, \\ T_{A,2} &= aQ_{A,2}, \\ W &= H_2(T_{A,1}, T_{A,2}), \\ V &= (a + R_{A,1})W + R_{A,2}. \end{aligned}$$

   Then she sends $A, Q_{A,2}, T_{A,1}, T_{A,2}, V$ to Bob.

2. Bob takes $A, Q_{A,2}, T_{A,1}, T_{A,2}, V$ and computes

$$\begin{aligned} W &= H_2(T_{A,1}, T_{A,2}), \\ h_A &= f_1(A, Q_{A,1}), \\ Q_{A,2} &= H_1(A). \end{aligned}$$

   Then he checks if

$$e(P, V) = e(T_{A,1} + Q_{A,1}, W)e(P_{pub}, h_AW + Q_{A,2})$$

   holds or not. If the equality holds, Bob authenticates Alice and starts communication. Then, Bob chooses a nonce N, computes

$$\begin{aligned} sk_B &= sT_{A,2}, \\ Auth_B &= f_2(A, T_{A,1}, T_{A,2}, V, N, sk_B) \end{aligned}$$

   and sends $N, Auth_B$ to Alice.

3. Alice takes $N, Auth_B$ and computes

   $$sk_A = aR_{A,2}.$$

   Then she checks if

   $$Auth_B = f_2(A, T_{A,1}, T_{A,2}, V, N, sk_A)$$

   holds or not. If the equality holds, Alice authenticates Bob. Alice continues by computing

   $$Auth_A = f_3(A, T_{A,1}, T_{A,2}, V, N, sk_A, Auth_B)$$

   and sends $Auth_A$ to Bob.

4. Bob takes $Auth_A$ and checks if

   $$Auth_A = f_3(A, T_{A,1}, T_{A,2}, V, N, sk_B, Auth_B)$$

   holds or not. If the equality holds, Bob authenticates Alice for one more time.

5. Then they both compute the session key as

   $$f_4(A, T_{A,1}, T_{A,2}, V, N, sk_A, Auth_B, Auth_A)$$

   and

   $$f_4(A, T_{A,1}, T_{A,2}, V, N, sk_B, Auth_B, Auth_A).$$

The diagram of the scheme can be seen in figure 3.3.

3.3 Security Analysis

In this section, the security of the protocols is analyzed.

3.3.1 Known-Key Security

SYL : Known-key security is satisfied since, in each round, separate ephemeral private keys a and b are chosen. The adversary must compute abP for each session independently of other session keys. However, it is Computational Diffie-Hellman problem.

THY : Known-key security is satisfied since, in each round, separate ephemeral private keys a and b are chosen. The adversary must compute abP for each session to find sk_A or sk_B independently of other session keys.However, it is Computational Diffie-Hellman problem.

THTT : Known-key security is satisfied by the same way in THY.

Alice		**Bob**
$a \in \mathbb{Z}_p^*$ $T_{A,1} = aP$ $T_{A,2} = aQ_{A,2}$ $W = H_2(T_{A,1}, T_{A,2})$ $V = (a + R_{A,1})W + R_{A,2}$		
	$\xrightarrow{A,Q_{A,2},T_{A,1},T_{A,2},V}$	
		$W = H_2(T_{A,1}, T_{A,2})$ $h_A = f_1(A, Q_{A,1})$ $Q_{A,2} = H_1(A)$ $e(P, V) = e(T_{A,1} + Q_{A,1}, W)e(P_{pub}, h_A W + Q_{A,2})$ a nonce N $sk_B = sT_{A,2}$ $Auth_B = f_2(A, T_{A,1}, T_{A,2}, V, N, sk_B)$
	$\xleftarrow{N,Auth_B}$	
$sk_A = aR_{A,2}$ $Auth_B = f_2(A, T_{A,1}, T_{A,2}, V, N, sk_A)$ $Auth_A = f_3(A, T_{A,1}, T_{A,2}, V, N, sk_A, Auth_B)$		
	$\xrightarrow{Auth_A}$	
		$Auth_A = f_3(A, T_{A,1}, T_{A,2}, V, N, sk_B, Auth_B)$
$f_4(A, T_{A,1}, T_{A,2}, V, N, sk_A, Auth_B, Auth_A)$		$f_4(A, T_{A,1}, T_{A,2}, V, N, sk_B, Auth_B, Auth_A)$

Figure 3.3: Tseng, Huang, Tsai and Tseng's Protocol

3.3.2 Forward Secrecy

SYL : Even the secret keys S_A and S_B are known, the adversary must calculate abP from $T_A = aP$ and $T_B = bP$. However, it is Computational Diffie-Hellman problem. Therefore, the previous session keys cannot be constructed.

THY : Even the secret keys (R_A, Q_A) and (R_B, Q_B) are known, the adversary must calculate abP from $T_A = aP$ and $T_B = bP$ to compute sk_A or sk_B. However, it is Computational Diffie-Hellman problem. Therefore, the previous session keys cannot be constructed.

THTT : Even the secret keys S_A and S_B are known, the adversary must calculate sk_A or sk_B. Nonetheless, this calculation needs to compute $asH_1(ID)$ from $T_{A,2} = aH_1(ID)$ and $R_{A,2} = sH_1(ID)$. However, it is Computational Diffie-Hellman problem. Therefore, the previous session keys cannot be constructed.

3.3.3 Key-Compromise Impersonation

SYL :

1. Adversary knows Alice's private key S_A.
2. He chooses $b \in \mathbb{Z}_p^*$ and sends to Alice.
3. He takes $T_A = aP$ from Alice.
4. He must compute

$$K_{AB} = e(P,P)^{abs} e(P,Q_B)^{as} e(Q_A,P)^{bs} e(Q_A,Q_B)^s.$$

He cannot compute K_{AB} since he cannot compute $e(P,Q_B)^{as}$. Because, a or S_B must be known to compute $e(P,Q_B)^{as}$. However, when $T_A = aP$, $P_{pub} = sP$ are known, to compute asP is Computational Diffie-Hellman problem. Hence, he cannot impersonate Bob. He cannot impersonate Alice when he knows Bob's private key S_B because of the same reason.

THY :

1. Adversary knows Alice's private key (R_A, Q_B).
2. He gets A, Q_A, T_A from Alice.
3. He chooses $b \in \mathbb{Z}_p^*$ and computes T_B, h_A.
4. He must compute

$$sk_B = (b + R_B)(T_A + Q_A + h_A P_{pub}) \oplus bT_A.$$

sk_B cannot be computed since R_B is not known. Hence, he cannot impersonate Bob. Also, he cannot impersonate Alice when he knows Bob's private key (R_B, Q_B) because of the same reason.

THTT :

1. Adversary knows Alice's private key $(R_{A,1}, R_{A,2}, Q_{A,1})$.
2. He gets $Q_{A,2}, A, T_{A,1}, T_{A,2}, V$ from Alice.
3. He computes $W, h_A, Q_{A,2}$.
4. He checks
$$e(P,V) = e(T_{A,1} + Q_{A,1}, W) e(P_{pub}, h_A W + Q_{A,2}).$$
5. He chooses a nonce N.

6. He must compute $sk_B = sT_{A,2}$ next.

$sk_B = sT_{A,2}$ cannot be computed since s is not known. Another way to compute $saQ_{A,2}$ is using $T_{A,2} = aQ_{A,2}$ and $R_{A,2} = sQ_{A,2}$. However, it is Computational Diffie-Hellman problem. Hence, he cannot impersonate Bob. He cannot impersonate Alice when he knows Bob's private key $(R_{B,1}, R_{B,2}, Q_{B,1})$ since he needs to know Alice's private key to compute $V = (a + R_{A,1})W + R_{A,2}$.

3.3.4 Unknown Key-Share

Unknown key-share is provided by using the user's ID or hash of the user's ID as session keys in the protocols.

3.3.5 Passive Attack

SYL : The adversary can take T_A and T_B, since these terms transport over the insecure channel, but still abP must be computed from these. In other words, the adversary must solve Computational Diffie-Hellman problem even with the master key. Hence, the protocol resists passive attack.

THY : The adversary can take A, Q_A, T_A, Q_B, T_B, $Auth_A$ and $Auth_B$ over the insecure channel, but still abP must be computed from these to get sk_A or sk_B. In other words, the adversary must solve Computational Diffie-Hellman problem even with the master key. Hence, the protocol resists passive attack.

THTT : The adversary can take A, $Q_{A,2}$, $T_{A,1}$, $T_{A,2}$, V, N, $Auth_A$ and $Auth_B$ over the insecure channel, but still $asQ_{A,2}$ must be computed from these. For this purpose, a or s must be known. a cannot be computed from aP or $aQ_{A,2}$ by the adversary since it is a Diffie-Hellman problem, but if the master key s is taken, then sk_B and the session key can be computed. However, the master key cannot be taken from the network. Hence, the protocol resists passive attack.

3.3.6 Man-in-the-middle Attack

Man-in-the-middle attack is analyzed in two ways. First way is replacing the terms which include ephemeral keys with the ones computed with the adversary's own choice ephemeral keys. Second way is replacing the terms with the ones as in the attack on the Shim's protocol [23].

SYL : If $T_A = aP$ is changed with $a'P$, and $T_B = bP$ is changed with $b'P$, then sk_A and sk_B can be corrupted by adversary. However, result of this K_{AB} or K_{BA} is corrupted and needs $e(Q_A, Q_B)^s$ to be computed. The adversary cannot find $e(Q_A, Q_B)^s$ without knowing S_A, S_B or s itself.

If $T_A = aP$ is changed with $a'P - Q_B$, then $b(a'P - Q_B)$ must be computed without knowing b. To find b from bP is Diffie-Hellman problem. Hence, the protocol resists against man-in-the-middle attack.

THY : If $T_A = aP$ is changed with $a'P$ and $T_B = bP$ is changed with $b'P$, then sk_A and sk_B can be get corrupted by adversary. However, still true sk_A needs $a + R_A$ to be computed, and true sk_B needs $b + R_B$ to be computed. The adversary cannot find $a + R_A$ or $b + R_B$ without knowing a, R_A, b or R_B.

If $T_A = aP$ is changed with $a'P - Q_B$, then $b(a'P - Q_B)$ must be computed without knowing b and $b + R_B$. To find b from bP is Diffie-Hellman problem and R_B is the private key of Bob. Hence, the protocol resists against man-in-the-middle attack.

THTT : If $T_{A,2} = aQ_{A,2}$ is changed with $a'Q_{A,2}$, then sk_B can be get corrupted. However, corrupted sk_B needs s, which is the master key to be computed. Also, sk_A is computed by Alice without corrupted information. Thus, even adversary corrupts the sk_B, he cannot compute the same session key with Alice. Hence, the protocol resists against man-in-the-middle attack.

3.3.7 Reveal Attack

SYL :

1. Adversary intercepts $T_A = aP$ from Alice. He chooses a random number $v \in \mathbb{Z}$. Then, to impersonate Alice, he sends avP to Bob.

2. Adversary intercepts $T_B = bP$ from Bob. Then to impersonate Bob, he sends bvP to Alice.

3. Alice computes the variable from session key

$$\begin{aligned} K_{AB} &= e(aP_{pub} + S_A, T_B + Q_B) \\ &= e(P, P)^{abvs} e(P, Q_B)^{as} e(Q_A, P)^{bvs} e(Q_A, Q_B)^s. \end{aligned}$$

   Similarly, Bob computes the variable from session key

$$\begin{aligned} K_{BA} &= e(T_A + Q_A, bP_{pub} + S_B) \\ &= e(P, P)^{abvs} e(P, Q_B)^{avs} e(Q_A, P)^{bs} e(Q_A, Q_B)^s. \end{aligned}$$

   These variables are different when they should be equal since there is an interruption by the adversary.

4. Two different session keys are formed with Alice and Bob. Therefore, when the adversary asks to reveal the session key with Alice, he gets only that session key, but he cannot know Bob's.

Hence, the protocol resists against reveal attack.

THY :

1. Adversary intercepts $T_A = aP$ from Alice. He chooses a random number $v \in \mathbb{Z}$. Then, to impersonate Alice, he sends avP to Bob.
2. Adversary intercepts $T_B = bP$ from Bob. Then to impersonate Bob, he sends bvP to Alice.
3. Alice computes session key with $T_A = aP$ and $T_B = bvP$. However, Bob computes session key with $T_A = avP$ and $T_B = bP$. To have same session key, these variables must be equal but they are different because of the interruption of adversary.
4. Two different session keys are formed with Alice and Bob. Therefore, when adversary asks to reveal session key with Alice, he gets only that session key but he cannot know Bob's.

Hence, the protocol resists against reveal attack.

THTT : In this protocol, adversary can intercept messages from Alice.

1. Adversary intercepts messages from Alice. He chooses a random number $v \in \mathbb{Z}$. Then to impersonate Alice, he sends avP or $avQ_{A,2}$ or both to Bob instead of originals.
2. Alice computes the session key with $T_{A,1}$ and $T_{A,2}$. However, Bob computes the session key with avP and $avQ_{A,2}$. To have same session key, these variables must be equal but they are different because of the interruption of adversary.
3. Two different session keys are formed with Alice and Bob. Therefore, when adversary asks the oracle to reveal session key with Alice, he gets only that session key but he cannot know Bob's.

Hence, the protocol resists against reveal attack.

As analyzed above, the protocols provide all the given security properties 3.1.

Table 3.1: Security Properties of Identity-Based Protocols

	Known-Key Security	Forward Secrecy	Key-Compromise Impersonation	Unknown Key-Share
SYL	✓	✓	✓	✓
THY	✓	✓	✓	✓
THTT	✓	✓	✓	✓

Also, they resist against the passive, man-in-the-middle and reveal attacks 3.2.

Table 3.2: Attacks on Identity-Based Protocols

	Passive Attack	Man-in-the-middle Attack	Reveal Attack
SYL	resist	resist	resist
THY	resist	resist	resist
THTT	resist	resist	resist

3.4 Performance Analysis

The performances are compared according to the analyses in the original works. The following notations are used to compare the performances

- T_m = Cost of a scalar multiplication of point in G_1,
- T_e = Cost of a biliniear pairing,
- T_H = Cost of a hash function map to point in G_1.

When looking at the authenticated key agreement phase of the protocols, totally SYL requires $2T_e + 6T_m$ according to [37], THY requires $8T_m$ (according to [35] and THTT requires $3T_e + 6T_m + 3T_H$ according to [34]. The costs can be seen for each user in the table 3.3.

Table 3.3: Efficiencies of Identity-Based Protocols

	SYL	THY	THTT
Computational cost of Alice	$T_e + 3T_m$	$4T_m$	$4T_m + T_H$
Computational cost of Bob	$T_e + 3T_m$	$4T_m$	$3T_e + 2T_m + 2T_H$
Used public key	Pairing-based	ECC Based	Pairing-based
Total	$2T_e + 6T_m$	$8T_m$	$3T_e + 6T_m + 3T_h$

ECC : Elliptic Curve Cryptography

According to Yuan and Li, bilinear pairing is an expensive operation. Also, Tseng et al. said that a hash function, which maps to a point in G_1, can be implemented as a scalar multiplication in G_1 in the article published in 2016. Therefore, it can also be assumed that T_m and T_H are equal. Thus, it can be said that SYL requires $2T_e + 6T_m$ and THTT requires $3T_e + 9T_m$. Hence, in the lights of these arguments from the original articles, it can be concluded that THY is more efficient than the others since no bilinear pairing operations is used, and SYL is more efficient than THTT since it requires less bilinear pairing and multiplication operation.

CHAPTER 4

ATTRIBUTE-BASED AUTHENTICATION

The attribute-based systems are the systems that include the users' attributes in secret keys. ABE systems cover more than one attribute at once as different than the IBE systems. Sahai and Waters [28] are the ones who found this idea first. They named this idea as fuzzy identity-based. After them, Goyal et al. [14], Bethencourt et al. [3], Cheung et al. [10] and Chase and Melissa [9] worked on the idea to improve the system. As a result of these improvements, more areas of usage revealed. Some of these areas need privacy protection besides authentication, which can be provided by the ABE systems. The eHealth systems are one of those systems. The patients' concerns increased when electronic health records file their personal information. Guo et al. [15], Narayan et al. [26] and Barua et al. [1] focused on users' privacy protection, and they proposed attribute-based schemes which provide privacy for the eHealth system. Another area that needs authentication is vehicular ad hoc networks (VANET). It is the system that arranges communications between vehicles and vehicles to the roadside. Authentication provides security against malicious signals and messages in VANET. There are so many studies in that area [27, 20, 39, 33, 30, 18, 8]. They authenticate the messages or signals that vehicles received using methods like certificates, signature, and group signature. Huang and Verma proposed the first attribute-based encryption scheme ASPE [19] for VANET. Liu et al. [24] added a new idea together with the ABE system. They constructed their system by hierarchising multiple authorities. The common ground in all these works is privacy, like Zhang et al. scheme [40].

Although the preliminary works protect the data integrity, they do not provide the privacy of users. However, recent studies show that many application areas need privacy protection. Zhang et al. [41] drew attention to the necessity of privacy in their work and have studied a scheme for a multi-agent system [36]. They aim to provide privacy, authentication and confidentiality in this system.

In this chapter, the working principle of Zhang et al. scheme [41] is explained. Then, a new design, which is inspired by this scheme, is given in detail. Lastly, the security of the new design is analyzed.

4.1 Notations

In Chapter 4, the notations which are given below are used to explain the protocols.

- q is a large prime,
- G_1 is an additive cyclic group of prime order q,
- G_2 is a multiplicative cyclic group of prime order q,
- g_1 is the generator of additive group G_1,
- e is a bilinear map from $G_1 \times G_1$ to G_2,
- s is master key (private key) of the system,
- pk is the public key of the system,
- GM is a group manager in the system,
- ID_i is the identity of an agent,
- h_i is the pseudonym of the agent who has identity ID_i,
- d_i is the private key of the agent who has identity ID_i,
- l_m is member list of the group,
- Atb_i is the i_{th} attribute,
- $Cred_i$ is the i_{th} credential of Atb_i,
- l_a is attribute list,
- H, H_2, H_3, H_4, H_5 are cryptographic hash functions such that
  $H : \{0,1\}^* \to G_1$,
  $H_2 : G_2 \to \{0,1\}^n$,
  $H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^*$,
  $H_4 : \{0,1\}^n \to \{0,1\}^n$,
  $H_5 : G_2 \to \mathbb{Z}_q^*$.

Now, in the next two sections, it will be continued with the review of the schemes. In order to be understood more clearly, the schemes can be thought over an example. To illustrate, these systems can be used for thesis access. Let a group is constructed by all academic members in the system. The attributes in the system are issued as titles (professor, associate professor, student, . . .), schools, faculties, departments and countries. A student who wants to share her thesis sets some limits for the people who can reach her thesis. She encrypts her thesis by using attributes. For instance, if she wants to share her thesis with professors in Cryptography Department of Institute of Applied Mathematics at METU, she embeds professor, cryptography, applied mathematics and METU attributes into the ciphertext. When she broadcasts the ciphertext, a group member, who is not a professor in Cryptography Department of Institute of Applied Mathematics at METU, cannot decrypt the encrypted message and access her thesis.

4.2 Zhang,Mu and Zhang Scheme [41]

The new attribute-based authentication scheme is constructed on ZMZ [41] scheme basis. Thus, it is given a brief introduction to the system that fits the scenarios. There are mainly 6 phases on the system Setup, Register, Revoke, IssueAttribute, SendMsg and RcvMsg.

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 $pk = g_1^s$. Then GM publishes the system parameters

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

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

Register: An agent is registered in the system with his/her identity. GM computes the hash of the identity ID_i as pseudonym $h_i = H(ID_i)$ of the agent and takes the pseudonym's s-th power to compute private key $d_i = h_i^s$. Then GM gives (h_i, d_i) to the agent and adds the new agent's pseudonym into the member list l_m by setting $l_m := l_m \cup \{h_i\}$ if $h_i \notin l_m$.

Revoke: 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 credentials of the member. GM computes $Cred_i = H(Atb_i)^s$ as a 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 followings 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 attributes as

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

where

$$\begin{aligned} A &= z \oplus H_2(e(d_i, h_j^*)^r) \oplus \{\oplus_{k=1}^{l_j} H_2(e(d_i, H(Atb_k^{[j]}))^r)\}, \\ \text{ATB-SET} &= \left\{ l_j + 1, H_5\left(e\left(h_j^* \cdot \prod_{k=1}^{l_j} H(Atb_k^{[j]}), pk\right)^{\mu}\right)\right\}, 1 \le j \le l. \end{aligned}$$

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 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 the computation. Therefore, the agent h_θ chooses l_r credentials $\{Cred_1^{[\theta]}, \ldots, Cred_{l_r}^{[\theta]}\}$ among all possessions. Check

   $$H_5\left(e\left(d_\theta \cdot \prod_{k=1}^{l_r} Cred_k^{[\theta]}, X\right)\right) = h_r.$$

   Until the equality holds, the agent checks 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

   $$\begin{aligned} z' &= V \oplus H_2(e(U, d_\theta)) \oplus \{\oplus_{k=1}^{l_\theta} H_2(e(U, Cred_k^{[\theta]}))\}, \\ M' &= W \oplus H_4(z'). \end{aligned}$$

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.

4.3 The New Scheme

In this section, a new attribute-based authentication protocol, which is designed based on ZMZ [41]and an efficient system for bilinear groups, is explained. Although their work is based on attribute-based authentication using public-key cryptography, in this scheme, it is used elliptic curves, which use smaller key sizes and more suitable for multi-agent systems. It is made necessary changes to the choice of the groups for a bilinear map and the operations for computation the terms. Further, the sending way of the required attributes is changed to reduce the work of the receiver. It contributes the followings:

- It can simultaneously provide the privacy protection and verifiability of agents' verified attributes.
- It uses pairings for bilinear maps and is designed on elliptic curve. The aim is to gain the advantage of key size and storage.
- Revocation of an agent is done by deleting the record from an authentication list, but a trusted third party (group manager) do it. 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. It is also modified attributes set to reduce the number of operations of users and for ease of transformation.

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

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

The list of members l_m and attributes l_a are the same as in Zhang et al.

RegisterAgent: An agent is registered in the system with his/her identity. 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 attributes of the member, GM processes the credentials of the member. 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 the pseudonym h_i and private key d_i does the followings 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 attributes as

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

   where

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

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

   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

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

3. Broadcast C.

RcvMsg: The receiver uses his private key, credentials which match the ciphertext attributes and *Params* to decrypt the messages. 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 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 whether they are 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 agent h_θ takes the suitable V_r's for his/her attribute number. In other words, s/he takes the vectors having the 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 one time for each vector. The agent does not need to try combinations of wanted number attributes among all of them.

3. Compute

$$\begin{aligned} z' &= V \oplus H_2(e(U, d_\theta)) \oplus \{\oplus_{k=1}^{l_\theta} H_2(e(U, Cred_k^{[\theta]}))\}, \\ M' &= W \oplus H_4(z'). \end{aligned}$$

4. Compute

$$\begin{aligned} r' &= H_3(z', M'), \\ h' &= (r')^{-1}U \quad \text{, where } (r')^{-1} \text{ is inverse of } r' \text{ in modulo } q. \end{aligned}$$

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.

The correctness of the equalities can be proven:

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

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

4.4 Security Analysis

In this section, the scheme's security is analyzed according to properties given in section 2.3. It is assumed that the adversary knows only the public information: the system parameters $(q, G_1, G_2, n, e, g_1, pk, H, H_2, H_3, H_4, H_5, l_m, l_a)$.

4.4.1 Adaptive Chosen Ciphertext

The adversary knows the system parameters except for the master key. He can get some private keys d_i's except the target one. Then he 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 the pseudonym h_i. The adversary challenges by using knowledge deduced from these. He gives a pseudonym h_S as the sender, a policy $\mathsf{POL} = h_R \wedge_k Atb_k$ where h_R is the pseudonym of the receiver and two messages M_0, M_1 that he 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

$$\begin{aligned} A &= z \oplus H_2(e(d_S, h_R)^r) \oplus \{\oplus_{k=1}^{l_R} H_2(e(d_S, H(Atb_k^{[R]}))^r)\}, \\ \text{ATB-SET} &= \left\{\left(V_R, H_5\left(e\left(h_R + \sum_{k=1}^{l_R} v_k H(Atb_k^{[R]}), pk\right)^{\mu}\right)\right)\right\}. \end{aligned}$$

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, he cannot compute. He 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

$$\begin{aligned} e(d_S, h_R)^r &= e(sh_S, h_R)^r \qquad h_S = ag_1, h_R = bg_1 \\ &= e(sag_1, bg_1)^r \\ &= e(g_1, g_1)^{sabr} \end{aligned}$$

and the adversary knows only g_1,ag_1,bg_1,rag_1 and sg_1.

Hence, the adversary cannot distinguish two ciphertexts accurately.

4.4.2 Key-Compromise Impersonation

Let the adversary tries to impersonate the agent who has the pseudonym h_S to convince the agent who has the pseudonym h_R. First of all, he has to compute a valid ciphertext, which includes h_S's information and h_R's attributes. So, he has to compute

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

where

$$\begin{aligned} A &= z \oplus H_2(e(d_S, h_R)^r) \oplus \{\oplus_{k=1}^{l_R} H_2(e(d_S, H(Atb_k^{[R]}))^r)\}, \\ \text{ATB-SET} &= \left\{\left(V_R, H_5\left(e\left(h_R + \sum_{k=1}^{l_R} v_k H(Atb_k^{[R]}), pk\right)^{\mu}\right)\right)\right\}. \end{aligned}$$

Since h_R computes the term z bu using rh_S, he 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.

4.4.3 Probing Resistance

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

$$\begin{aligned} A &= z \oplus H_2(e(d_S, h_{Adv})^r) \oplus \{\oplus_k H_2(e(d_S, H(Atb_k))^r)\}, \\ \text{ATB-SET} &= \left\{ \left(V, H_5 \left(e \left(h_{Adv} + \sum_k v_k H(Atb_k), pk \right)^{\mu} \right) \right) \right\}. \end{aligned}$$

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

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

He can verify $H_2(e(d_S, h_{Adv})^r)$ by computing $H_2(e(rh_S, d_{Adv}))$. However, he 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 $h_S = ag_1, H(Atb_j) = bg_1$,
and $e(g_1, g_1)^{sabr}$ 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 cannot say the ciphertext C is valid or not without knowledge of the attributes.

4.4.4 Indistinguishable to Eavesdroppers

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

4.4.5 Hidden Credentials

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

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

where

$$\begin{aligned} A &= z \oplus H_2(e(d_S, h_R)^r) \oplus \{\oplus_k^{l_R} H_2(e(d_S, H(Atb_k^{[R]}))^r)\}, \\ \text{ATB-SET} &= \left\{\left(V_R, H_5\left(e\left(h_R + \sum_k^{l_R} v_k H(Atb_k^{[R]}), pk\right)^{\mu}\right)\right)\right\}. \end{aligned}$$

is sent to the adversary.

The adversary tries to extract attributes in ATB-SET. In other words, he tries to say what are Atb_k's. For this he 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

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

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

As it can be seen, the adversary has to decide $e(bg_1, \mu sg_1)$ is a valid attribute or simulation. However, he cannot determine this since it is decisional bilinear Diffie-Hellman problem. Hence, the system provides to hide the credentials.

4.4.6 Forward Secrecy

Let the adversary know the private key of the sender and the random keys z and μ . He 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 of the elements are chosen randomly, the present ciphertext's random keys do not give any advantage to construct the previous ones. Hence, the system provides forward secrecy.

4.4.7 Unknown Key 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 by using their identities. For that reason, they cannot be forged by another person. Therefore, the sender ensures that the ciphertext cannot be open 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.

As analyzed above, the protocols provide all the given security properties 4.1.

Table 4.1: Security Properties of Attribute-Based Protocols

	ZMZ Scheme	New Scheme
Adaptive Chosen Ciphertext	✓	✓
Key-Compromise Impersonation	✓	✓
Probing Resistance	✓	✓
Indistinguishable to Eavesdroppers	✓	✓
Hidden Credentials	✓	✓
Forward Secrecy	Unanalyzed	✓
Unknown Key-Share	Unanalyzed	✓

4.5 Computational Overhead

Computational overhead can be defined as any combination of computing time, memory, bandwidth, or alternative resources required to perform a specific task. ECC is widely used in constrained environments. It is used as an alternative in restricted environments such as portable and wireless devices, with much smaller area usage (bit size) and low energy consumption compared to public-key encryption systems such as RSA. In this chapter, Real-time communication encryption (sending-receiving phases) is based on hash functions and ECC operations; therefore the protocol has lower communication and computation overheads. Moreover, in the literature, there are several studies that show 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 [4, 16, 5].

4.6 Performance Analysis

The performances are compared theoretically. The comparison is explained according to previous works which use similar operations. The following notations are used

- 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 $\mod q$.

First, assume that the receiver has n attributes and has to choose l_r attributes among them for decryption. In this case, 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 totally according to the group manager's, the sender's and the receiver's operations. The costs can be seen for each user in the table 4.2.

Table 4.2: Efficiencies of Attribute-Based Protocols

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

ECC : Elliptic Curve Cryptography

As it is mentioned in section 3.4, the bilinear map is the most expensive operation among these operations. The ZMZ scheme requires bilinear map computations more than the new 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 it is recommended in Moody et al.'s report [25].The new scheme also requires the hash function, which maps to a point on 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, according to Tseng et al. [35]. Also, Daniel [17] proposed such hash function ECOH2 in NIST's SHA-3 competition, which can be used for implementation. However, ECOH2 can be inefficient, according to Tseng et al.'s suggestion. For this reason, it is continued with Tseng et al.'s advice. This type of hash function is used in the new scheme for three times. Therefore, these three hash functions can be turned into scalar multiplication in the new scheme. Then it requires $9T_s + 10T_H + 6T_e + T_i$ in totally. Even if the number of scalar multiplication increases, the new scheme uses smaller size integers to provide the same level of security with the ZMZ scheme since it is based on ECC. Hence, the new scheme is more efficient than the ZMZ scheme according to bilinear map operations and small integer sizes.

CHAPTER 5

CONCLUSION

Authentication is always important for information security. It is used for ensuring whom the data is shared with, and also it can protect data integrity. There are several authentication protocols in the literature. They can be based on password, symmetric-key or public-key. Among these, public-key based protocols are the most preferred ones. For this reason, there are many works on that basis.

This thesis is a study about authentication protocols based on public-key cryptography. It includes how they work, their security properties and explanation about their efficiencies.

The thesis starts by giving the mathematical background about these protocols in Chapter 2. Then it examines the authentication protocols into two parts.

First, in Chapter 3, the ID-based key agreements, which are the ones proposed by Yuan-Li and Tseng et al. are compared. First, how the protocols works are explained, then their security and efficiency analyses are made. The security of the protocols is based on Diffie-Hellman problems, pairing construction and hash functions. They are secure against man-in-the-middle, passive and reveal attack and provide known-key security, forward secrecy, key-compromise impersonation and unknown key-share properties. The pairing construction and hash functions are also helped to make the protocols more efficient. Although efficiencies are improved according to public-key protocols, SYL and THTT are still not too fast since they use the bilinear pairing. However, THY is the fastest among all of them since it uses only scalar multiplications.

Second, a new attribute-based authentication for multi-agent systems inspired by ZMZ [41] is presented in Chapter 4. Their scheme is based on bilinear mapping, which is too expensive. Differing from the previous work, the new 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; it is easy to transmit and implement. Also, controlling the credentials is a heavy burden for the receiver in their work. This operation is simplified and made the new scheme practical for the application areas. In all these application areas, the privacy of attributes is an important issue. Thus, it is protected the privacy of the users' personal information (credentials). Revocation, which is another crucial issue in these systems, is provided by using a list for members. The group manager subtracts pseudonyms from the list, which provides authentication to revoke agents from the system as a trusted third party. Besides, the new scheme provides the security properties; adaptive chosen ciphertext, key-compromise impersonation resilience, probing resistance, indistinguishable to eavesdroppers, forward secrecy and unknown key-share resilience.

In conclusion, the authentication protocols, which are told in the thesis, are based on elliptic curve cryptography. ECC provides efficiency, less storage necessity and the same security level as public-key cryptography. They secure the protocol by using Diffie-Hellman problems; ECDLP, BDH, CDH and DBDH. For this reason, the protocols fit to implement in many applications like eHealth, VANET.

REFERENCES

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

[2] S. M. Bellovin and M. Merritt, Encrypted key exchange: password-based protocols secure against dictionary attacks, in *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 72–84, 1992.

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

[4] R. Bilal and M. Rajaram, High speed and low space complexity fpga based ecc processor, International Journal of Computer Applications, 8(3), pp. 5–10, 2008.

[5] R. Bilal and M. Rajaram, Design and implementation of high performance ecc coprocessor, International Journal of Engineering Science, 2(11), pp. 6759–6770, 2010.

[6] R. Bird, I. Gopal, A. Herzberg, P. A. Janson, S. Kutten, R. Molva, and M. Yung, Systematic design of a family of attack-resistant authentication protocols, IEEE Journal on Selected Areas in Communications, 11(5), pp. 679–693, 1993.

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

[8] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, Efficient and robust pseudonymous authentication in vanet, in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pp. 19–28, 2007.

[9] M. Chase, Multi-authority attribute based encryption, in *Theory of cryptography conference*, pp. 515–534, Springer, 2007.

[10] L. Cheung and C. Newport, Provably secure ciphertext policy abe, in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 456–465, 2007.

[11] C. Cocks, An identity based encryption scheme based on quadratic residues, in *IMA international conference on cryptography and coding*, pp. 360–363, Springer, 2001.

[12] H. Debiao, C. Jianhua, and H. Jin, An id-based client authentication with key agreement protocol for mobile client–server environment on ecc with provable security, Information Fusion, 13(3), pp. 223 – 230, 2012, ISSN 1566-2535.

[13] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Information Theory, 22, pp. 644–654, 1976.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, Proceedings of the ACM Conference on Computer and Communications Security, 89-98, pp. 89–98, 01 2006.

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

[16] 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), 4(4), pp. 373–435, 2010.

[17] M. Halcrow and N. Ferguson, A second pre-image attack against elliptic curve only hash (ecoh)., IACR Cryptol. ePrint Arch., 2009, p. 168, 2009.

[18] 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, 29(3), pp. 616–629, 2011.

[19] D. Huang and M. Verma, Aspe: attribute-based secure policy enforcement in vehicular ad hoc networks, Ad Hoc Networks, 7(8), pp. 1526 – 1535, 2009, ISSN 1570-8705, privacy and Security in Wireless Sensor and Ad Hoc Networks.

[20] J. P. Hubaux, S. Capkun, and Jun Luo, The security and privacy of smart vehicles, IEEE Security Privacy, 2(3), pp. 49–55, 2004.

[21] S. H. Islam and G. P. Biswas, A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Journal of Systems and Software, 84, pp. 1892–1898, 2011.

[22] P. A. Janson and G. Tsudik, Secure and minimal protocols for authenticated key distribution, Computer Communications, 18, pp. 645–653, 1995.

[23] Kyungah Shim, Efficient id-based authenticated key agreement protocol based on weil pairing, Electronics Letters, 39(8), pp. 653–654, 2003.

[24] X. Liu, Z. Shan, L. Zhang, W. Ye, and R. Yan, An efficient message access quality model in vehicular communication networks, Signal Processing, 120, pp. 682 – 690, 2016, ISSN 0165-1684.

[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, 120, p. 11, 2015.

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

[27] M. Raya and J.-P. Hubaux, Securing vehicular ad hoc networks, Journal of computer security, 15(1), pp. 39–68, 2007.

[28] A. Sahai and B. Waters, Fuzzy identity-based encryption, in R. Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, pp. 457–473, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, ISBN 978-3-540-32055-5.

[29] A. Shamir, Identity-based cryptosystems and signature schemes, in *CRYPTO*, 1984.

[30] J. Shao, X. Lin, R. Lu, and C. Zuo, A threshold anonymous authentication protocol for vanets, IEEE Transactions on vehicular technology, 65(3), pp. 1711–1720, 2015.

[31] N. P. Smart, Identity-based authenticated key agreement protocol based on weil pairing, Electronics Letters, 38(13), pp. 630–632, 2002.

[32] M. Steiner, G. Tsudik, and M. Waidner, Refinement and extension of encrypted key exchange, ACM SIGOPS Operating Systems Review, 29(3), pp. 22–30, 1995.

[33] A. Studer, E. Shi, F. Bai, and A. Perrig, Tacking together efficient authentication, revocation, and privacy in vanets, in *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 1–9, IEEE, 2009.

[34] Y.-M. Tseng, S.-S. Huang, T.-T. Tsai, and L. Tseng, A novel id-based authentication and key exchange protocol resistant to ephemeral-secret-leakage attacks for mobile devices, IJDSN, 11, pp. 898716:1–898716:12, 2015.

[35] Y.-M. Tseng, S.-S. Huang, and M.-L. You, Strongly secure id-based authenticated key agreement protocol for mobile multi-server environments, International Journal of Communication Systems, 30(11), p. e3251, 2017, e3251 IJCS-16-0586.R1.

[36] M. Wooldridge, *An Introduction to MultiAgent Systems*, pp. –348, John Wiley & Sons, 06 2002, ISBN 047149691X.

[37] Q. Yuan and S. Li, A new efficient id-based authenticated key agreement protocol, IACR Cryptology ePrint Archive, 2005, p. 309, 2005.

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

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

[40] 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, 123, pp. 1–10, 2018.

[41] Q. Zhang, Y. Mu, and M. Zhang, Attribute-based authentication for multi-agent systems with dynamic groups, Computer Communications, 34, pp. 436–446, 03 2011.

[42] 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 Q. Zu, B. Hu, N. Gu, and S. Seng, editors, *Human Centered Computing*, pp. 685–692, Springer International Publishing, 2015.