A Survey and Comparing RFID Authentication Protocols Based on Elliptic Curve Cryptography

Negin Dinarvand[1], Hamid Barati[2]
1- Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.
Email: dinarvand@iaud.ac.ir
2- Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.
Email: hbarati@iaud.ac.ir

Received: October 2015 Revised: October 2015 Accepted: November 2015

ABSTRACT:
Security and privacy are inherent problems in RFID systems communication. Many different ways and methods were presented to overcome these problems among which encryption, authentication and hardware techniques can be pointed out. Authentication protocols based on elliptic curve cryptography (ECC) is one of the methods used in authentication protocols in order to improve the security and privacy of RFID systems. This study aims at examining and comparing protocols that utilize this method in establishing security.

KEYWORDS: RFID, Elliptic Curve Cryptography, Security, Authentication.

1. INTRODUCTION

Radio Frequency Identification (RFID) is a wireless technology that uses radio signals to detect the tags attached to objects. An RFID system generally consists of three basic components [1]:

- Tag
- Reader
- Back-end server

In a RFID system, multiple tagged objects are allowed to be scanned simultaneously in a non-contact manner. Thus, the tags can be a best alternative to barcodes that need to be scanned separately [2]. In general, RFID communication process can be described as follows: The relationship between the tag reader and the server is assumed to be secure. RFID tag reader sends a request to access RFID tag and returns a response to the final server. After the identification on the server, the server returns RFID tag information to the reader [3].

RFID is a novel technology that can be used in many fields, including military, health, food safety, textile, construction, feedback control, building management, transport, and aviation fields, etc.

The major concern about RFID systems is security and privacy of data, through which the allowable tag and reader are only required to be able to access the exchanged data so that the unallowable tag readers cannot access the information on the tags, nor can the fake tags send bogus information to the readers.

Different protocols have been introduced to RFID systems for authentication, some of which take benefits of the elliptic curve cryptography method to secure communication in the RFID system. In chapter 2 of this article, the security of RFID systems will be discussed. The elliptic curve cryptography model will be described in chapter 3 and a comparative study of the recent RFID protocols based on elliptic curve cryptography will be explained in chapter 4.

2. SECURITY IN RFID SYSTEMS

2.1. Requirements

Due to the fact of wireless communication between the tag and the reader in RFID systems, the most fundamental problems are the privacy and security of such systems. A reliable communication system must guarantee the transfer of confidential information, as well as its integrity and availability. The messages that are exchanged between the tag and reader are subject to many security threats. The characteristics of RFID systems and specific software environment in these systems have led to unique security needs as well. Mutual authentication is a most important process to secure communications in RFID systems. The research conducted with the purpose of securing communications in RFID has shown that authentication protocols in these systems must meet the security requirements such as mutual authentication, confidentiality, anonymity, availability, forward security, scalability, and attack resistance to be a robust and effective model for authentication on RFID [4].

2.2. Threats

In their communications, RFID systems face a lot of

security threats, including physical attacks, spoofing, eavesdropping and skimming, tack cloning, Denial of Service (DOS), Clandestine Tracking, and replay attacks. The security threats in RFID systems, such as those mentioned above lead to the provision of solutions such as authentication protocols for dealing with threats and keeping their privacy and security.

3. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography system was first introduced by Koblitz and then developed by Miller in 1985 to design a public-key cryptography system, which will soon become as an integral part of modern cryptographic systems [5]. Elliptic Curve Cryptography (ECC) is briefly introduced as follows:

An elliptic curve E is defined over a field Fp by equation (1):

$E = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (1)

where $a_1, a_2, a_3, a_4, a_6 \in F_p$ and $\Delta \neq 0$, while Δ is E discriminate. The above equation is called Weierstrass equation. The condition $\Delta \neq 0$ ensures that the elliptic curve is smooth, i.e. there is no point on the curve that has two or more distinct tangent. Also, in the elliptic curve equation, there is a single element shown as *O* that is called a point at infinity. The law of tangent and chord is used to add two points and get a third point on the elliptic curve. With this addition, the set of points is shown as $E(F_p)$, while forming a commutative group *G*, in which *O* is an identifier and *P* is its generator. An elliptic curve is widely used for making primary geometric shapes for cryptography, including encryption functions, signature design, cryptography protocols, etc. [6].

The group G operation is defined as follows:

- $P = (x, y)$ is an element of the group, thus, $-P = (x, -y)$ and $P + (-P) = O$.
- If P and Q are two distinct elements and $P \neq -Q$, then, $P + Q$ will be defined as follows:

First, a line is drawn to pass through these two points. The line intersects the curve at a point shown as $-R$ and thus $P + Q = R$.

- If the group element is $P\ (x, 0)$, then, $P + P = O$. Otherwise, a tangent is drawn passing through the point P and the point that intersects the curve is called –R. Thus:
  $P + P = 2P = R$
  (2)

In addition, for Group *G*, there is a base point *P* that is called the generator or first root to produce group *G*. So that $G = \{P, 2P, 3P, \ldots, (n-1)\ P, nP = O\}$, where n is the size of *G* [7].

4. RFID AUTHENTICATION PROTOCOLS BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

In this section, several RFID authentication protocols are described that use elliptic curve cryptography as a way to maintain their security and privacy in RFID.

4.1. An Efficient Mutual Authentication RFID Scheme Based on Elliptic Curve Cryptography

In the security model [2], there are two roles: the server or reader and the tag. The term "server" is used as a server or a reader. We assume that the relationship between the tag and the server is insecure. The model presented in [2] has two phases: the setup phase and authentication phase. The notations used to describe this model are shown in Table 1.

Table 1. Notations used in [2]

Notation	Describe
G	A group of order q on an elliptic curve
P	A primitive element of *G*
X_i	Tag's identifier is a random chosen point in *G*
y	Server's private key
Y	Server's public key where *Y(= yP)*
r, k	Two random numbers in *Zq*
h	A one-way hash function

Setup phase: In this phase, the server generates a random number $y \in Zq$ as the private key and calculates $Y = yP$ as its public key. Moreover, it selects a random point $X \in G$ as the ith tag identifier and then stores each tag identifier and the relevant information including tag name, generation number, etc. in its database. Finally, the server stores $\{X_i, Y, P\}$ into each tag memory.

Authentication phase: The server performs a broadcast to a random point when a set of tags are queried. Within the query signal range, each tag implements the authentication protocol according to Fig. **1** as follows.

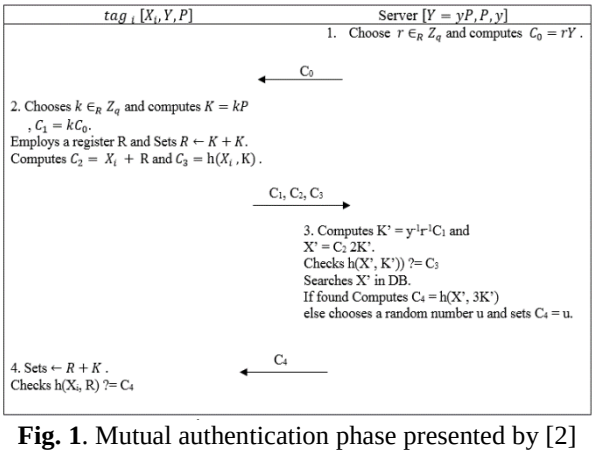

Fig. 1. Mutual authentication phase presented by [2]

By the security analysis presented in this protocol, it is found that this protocol resists physical attacks, replay attacks, man-in-the-middle attack, and spoofing in addition to mutual authentication and privacy maintenance.

4.2. Cryptanalysis and Improvement of an Efficient Mutual Authentication RFID Scheme Based on Elliptic Curve Cryptography

In [6], after reviewing the protocol introduced by [2] and expressing its security weaknesses, including lack of keeping tag privacy, lack of maintaining forward privacy, and poor mutual authentication, Sabzinejad Farash has provided an improvement on this protocol. Similarly, the mentioned protocol includes the two phases of setup and authentication. The setup phase is carried out in the same way as the protocol introduced by [2] and the authentication phase includes 4 steps displayed in Fig. **2**.

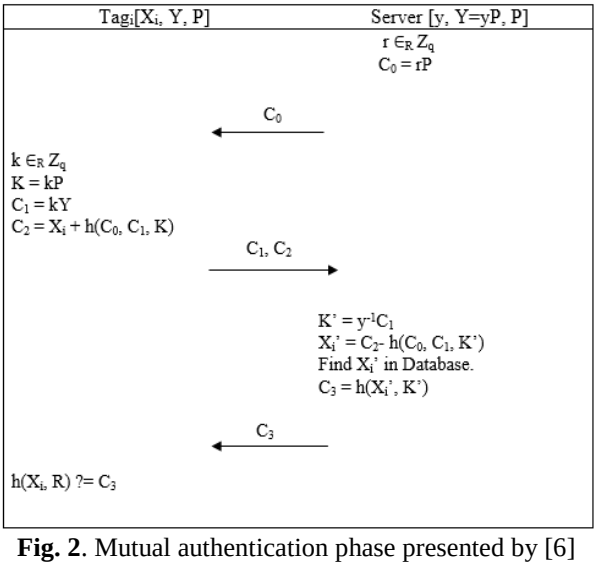

Fig. 2. Mutual authentication phase presented by [6]

The studies of security have shown that following an improvement of the authentication protocol introduced in [2], the security problems of the mentioned protocol will be removed, thus maintaining the privacy and supporting mutual authentication so well as well as resisting replay attacks, man-in-the-middle attack, and spoofing attack.

4.3. An Efficient RFID Authentication Protocol to Enhance Patient Medication Safety Using Elliptic Curve Cryptography

Furthermore, the protocol presented in [8] has provided an improvement for protocol [2]. This protocol also includes the two phases of setup and authentication phase. The setup phase is as the protocol provided by [2] and the authentication phase is exhibited in Fig. **3**.

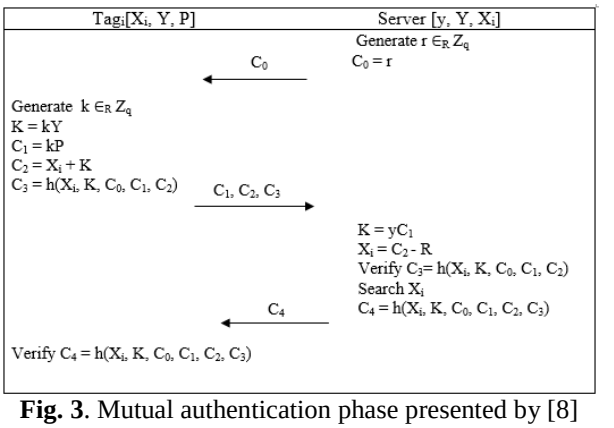

Fig. 3. Mutual authentication phase presented by [8]

This protocol maintains the privacy of tag information. A mutual authentication would further detect tag anonymity and resist backward and forward tracking attack, spoofing attack, tag cloning attack, replay attack, Denial of Service (DoS) attack, modification attack, de-synchronization attack, and man-in-the-middle attack.

4.4. Lightweight ECC Based RFID Authentication Integrated with an ID Verifier Transfer Protocol

In [9], a lightweight authentication protocol has been introduced using elliptic curve cryptography. The signs used in this protocol are described in Table 2.

Table 2. Notations used in [9]

Notation	Describe
n,q	two large prime numbers
F(q)	a finite field, where *q* represents the size of the finite field.
(a,b)	two parameters of an elliptic curve E, which is defined by the equation $y^2 = x^3 + ax + b$ over the finite field F(q).
P	a generator point with order n of the elliptic curve E
x_S	the private key of the server
P_S	the public key of the server, where $P_S = x_S P$
X_T	the ID-verifier of the tag

Setup phase: The server chooses a random number $x_S \in Z_n^*$ to computes $P_S = x_S P$. Also, it selects a random point X_T on the elliptic curve E for each tag. Then the server stores the verification identifier for the tag X_T and the domain parameters in the tag memory. Additionally, it maintains x_S as the private key and stores X_T within its own database.

Authentication phase: the authentication phase is displayed in Fig. **4**. The server and the tag identify each other through some steps as follows.

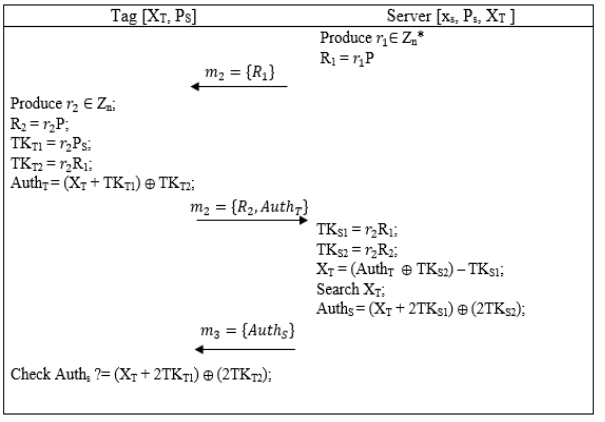

Fig. 4. Mutual authentication phase presented by [9]

In the security analysis of this protocol, it has been shown that a mutual authentication takes place between the server and the tag. Also, the tag verification identifier will remain anonymous besides providing anonymity, availability, forward security, and scalability and resisting replay attack, server spoofing attack, denial of service (DoS) attack, location tracking attack, and tag cloning attack.

4.5. A Secure ECC-Based RFID Authentication Scheme Using Hybrid Protocols

In [10], a mutual authentication model has been proposed that includes two basic phases: the setup phase and authentication phase.

Setup phase: In this phase, the server generates the system's parameters in a way that it chooses a random number $x_S \in Z_n^*$ as its private key and calculates $P_S = x_S P$. Furthermore, it selects $X_T \in Z_n$ as the private key for each tag and sets $Z_T = X_T P$ as the public key for a tag's ID-verifier.

The server would then store the verification identifier of the tag X_T and the system parameters within the tag memory. It also keeps x_S as the private key and stores X_T into its own database. Then, it stores the value $\{Z_T, X_T\}$ for each tag in its database. In addition, the amount of $\{Z_T, X_T\}$ and the system's parameters are stored into each tag memory. The system's parameters are presented in Table 3.

Table 3. Notations used in [10]

Notation	Describe
P_S	the public key of the server, where $P_S = x_S P$.
P	Base point in $E(Z_p)$, whose order is n.
x_S	Server private key.
Z_T	The tag's public key as ID-verifier
X_T	Private key

Authentication phase: the authentication phase of this scheme is illustrated in Fig. 5.

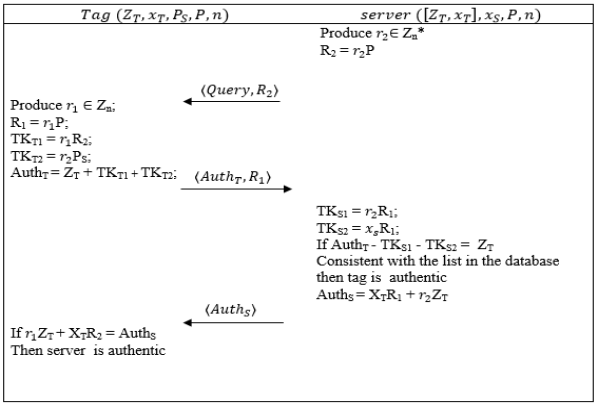

Fig. 5. Mutual authentication phase presented by [10]

The security studies reveal this protocol supports the mutual authentication between the tag and server, privacy of the ID-verifier, anonymity, availability, forward security, and scalability. It also resists the replay attack, tag masquerade attack, server spoofing attack, DoS attack, location tracking attack, and tag cloning attack.

5. ACKNOWLEDGMENT

Data security and privacy is very important when data transmission in RFID systems occurs via radio waves. Authentication protocols are of the main ways of maintaining tag security and privacy suggested by different researchers. The authentication protocols studied in this paper have adopted different methods to deal with the attacks and maintain security and privacy in RFID systems. Elliptic curve cryptography has been used via various procedures in the mentioned RFID authentication protocols. Each of the proposed protocols has a specific ability to deal with the problems of security and privacy. Hence, an integrated approach is required to cope with all the attacks and security problems within RFID systems.

REFERENCES

[1] S. Abughazalah, K. Markantonakis, and K. Mayes, **"Secure Improved Cloud-Based RFID Authentication Protocol,"** *Springer, International Publishing Switzerland,* 2015.

[2] J.S. Chou, **"An Efficient Mutual Authentication RFID Scheme Based on Elliptic Curve Cryptography,"** *Springer, journal of supercomputing, New York,* 2014, pp. 75-94.

[3] I. Syamsuddin, T. Dillon, E. Chang and S. Han, **"A Survey of RFID Authentication Protocols Based on Hash-Chain Method,"** *Third 2008 International Conference on Convergence and Hybrid Information Technology, IEEE,* 2008.

[4] D. He and S. Zeadally, **"An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography,"** *IEEE Internet of Things Journal,* Vol. 2, No.1, February 2015.

[5] X. YIN, Z. LIU, H. J. LEE, **"An Efficient and Secured Data Storage Scheme in Cloud Computing Using ECC-based PKI,"** *Advanced Communication Technology (ICACT), 2014 16th International Conference*, february 2014, pp. 523-527.

[6] M. Sabzinejad Farash, "Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography," *Springer, Journal of Supercomputing, New York*, 2014.

[7] Y. Chen and J. S. Chou, **"ECC-based untraceable authentication for large-scale active-tag RFID systems"**, *Springer, Electronic Commerce Research*, Vol. 15, No. 1, 2015, pp. 97-120.

[8] Z. Zhang and Q. Qi**, "An Efficient RFID Authentication Protocol to Enhance Patient Medication Safety Using Elliptic Curve Cryptography,"** *Springer, Journal of Medical Systems*, 2014, pp. 38-47.

[9] Z. D. He, N. Kumar, N. Chilamkurti and J. H. Lee, **"Lightweight ECC Based RFID Authentication Integrated with an ID Verifier Transfer Protocol",** *Springer, Journal of Medical Systems*, 2014.

[10] Y. P. Liao and C. M. Hsiao, **"A Secure ECC-Based RFID Authentication Scheme Using Hybrid Protocols,"** *Springer, Advances in Intelligent Systems & Applications, SIST 21*, 2013, pp. 1–13.