International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

# A Survey Paper On Elliptic Curve Cryptography

**Himja Agrawal[1], Prof.P.R.Badadapure[2]**

*[1]ME student ,Dept. of E&TC ,Imperial College of Engineering& Research, Pune, Maharashtra , India*
*[2]Associate Professor, Dept. of E&TC, Imperial College of Engineering &Research ,Pune ,Maharashtra ,India*

---

**Abstract** – *Advanced Development in information and communication technologies, there are so many things that gives facility to deal with these technology using internet. For providing proper identification we using RFID (Radio-frequency identification)system. Radio-frequency identification (RFID) is the most important wireless communication technologies used in the Internet of Things as it can store sensitive data, used for wireless communication with other objects, and identify/track particular object automatically. To provide better security and performance to RFID authentication scheme, Elliptic Curve Cryptography is going to be used.*

*Elliptical curve cryptography (ECC) is based on a public key cryptosystem based system that is on elliptic curve theory. Elliptic Curve Cryptography can be used to create smaller, faster, and more efficient cryptographic keys. ECC authentication scheme is more suited for wireless communications, like mobile phones and smart cards, personal information like financial transaction or some secret medical reports, confidential data where main consideration is to provide secure data.*

*Elliptic curve cryptography (ECC) system is for provide suitable authentication RFID system because it can provide similar security level but using a smaller key size and has low computational system requirements. The low processing associated with ECC authentication scheme is to make suitable for use with RFID tags because they have consuming limited computing power.*

*In this paper we present a survey paper on ECC based RFID authentication scheme that is suitable for many applications where security is main concern.*

***Key Words***: **Authentication schemes, Elliptic curve cryptography(ECC),Radio frequency identification(RFID), RSA (Rivest, Shamir and Adleman)**

## 1.INTRODUCTION

Today's advanced technology of internet brings revolution or convenient system for users. This advance technologies are applied to many applications like healthcare or medical area, provide security in people information personally or financially, provide interactions among different types of devices, like smart vehicles management, for patients medical sensors, monitoring CCD cameras, advanced technology based home appliances, smart city, home automation, smart grid, traffic management, RTO offices etc. For that purpose we need a unique identification system for each task.

Radio Frequency Identification (RFID) systems are becoming popular due to their vast applications like supply chains, inventory, tolling, baggage management, access control, medical, financial etc. By use these technology not only improve our lives but they also cause of privacy risk. In many applications privacy is neglected, but due to security reason of RFIDs the issue has to be taken. However, providing additional security to the system is always comes with price and the scarceness of resources on a tag makes conventional privacy-preserving protocols.

Radio-frequency identification (RFID) is a wireless communication technology that is useful for precisely identifying objects. RFID technology uses the radio-frequency waves to transfer identifying information between tagged objects and readers without line of sight (LOS), providing a automatic identification system.

RFID technology attracts a lot of attention in recent years because of it large convergence of lower cost and the increased capabilities of RFID keys. But when RFID scheme is used the data is in open space so there are possibility to hack the data. It doesn't provide proper security to your data that is either your personnel or financial or for that system dealing with security. So the main requirement for this RFID is small computational capacity system that have strong authentication and good performance.

RFID attract a lot of attention from users only in recent years because of the large convergence in low cost and the increased capabilities, provide of RFID tags. Currently, RFID is emerging as an important technology that is cause for revolution in a wide range of applications that include supply-chain management, retail sales, anti counterfeiting, and healthcare.

RFID is most important and popular technology that is used in Internet of things because it can store any kind of data, wireless communication with different system, identifying and track object properly and automatically.

When we compared RFID with traditional barcode system it can be applied for rough surfaces also, it has read write capability, does not require Line of Sight(LOS) and it can read many tags simultaneously

All the above benefits make RFID a superior technology than traditional systems. RFID system can be used in many applications. For example in the healthcare environment[1], RFID technology is being used within IoT and common applications like location tracking of medical assets newborn and patient identification , tracking of medical treatment and validation patient location and procedure

management at a wellness center , and surgical process management

Mutual authentication in RFID systems is a strong requirement that must be met to ensure secure communication between RFID tags and the server. The RFID authentication scheme should be efficient and secure against various attacks through hackers.

## 2 CLASSIFICATION OF RFID AUTHENTICATION SCHEME

RFID authentication scheme have been used for many applications. According to cryptographic primitives used in various schemes, RFID scheme can be classified in two types

(1)Non Public-key cryptosystem(NPKC) based schemes

(2)Public key cryptosystem(PKC)-based scheme

The NPKC based RFID authentication scheme have no complex operation is needed so it gives better performance. In this scheme simple logic gate operations, symmetric encryption technique ,cyclic redundancy codes are used. So this type or schemes have been proposed for normal practical applications like book management ,verification, road traffic administration etc where security of data is not so much concern.

PKC based scheme are necessary where security of data is main concern. Because that attributes cannot be implemented by NPKC based scheme. Development in micro electric technology many complex algorithm have been implemented on RFID chips.

In many schemes ECC authentication system is more suitable for system because it can provide same security but using shorter key size and low computational requirement so it limit the computing power. In PK algorithms it uses a mechanism where large number of participants share keys in complex information system. Compare to RSA (Rivest, Shamir and Adleman) or other schemes,ECC is using shorter key length.

To authenticate RFID is the most important steps to set up a secure communication in RFID system. We are using different authentication scheme for this purpose. Because RFID tags and readers are exposed in many kind of security threats.

## 3 SECURITY REQUIREMENTS

RFID security requirements are fulfilled when they satisfied following requirements to make efficient authentication scheme.

1. Mutual authentication:
   In mutual authentication among the RFID Tag and RFID reader should be fixed before starting any session. In system we assume that our communication channel between server and tag is secured only mutual authentication is required.
2. Confidentiality:
   It is essential to provide security to secret information such as identity, passwords financial transaction when it is transmitted through communication channel. The information can be hacked during transmission so it must be encrypted before transmission.
3. Anonymity:
   RFID authentication should provide anonymity that means it traces the owner's activity ,its location and privacy if the tag's identity is known, so the tag should be encrypted.
4. Availability:
   The authentication process for RFID should be executed during the life cycle period of Tag. When the information is executed the authentication scheme should give a update the secret information. If this is fail to synchronization of any update then authentication scheme will become invalid.
5. Forward security:
   It is very necessary to provide forward security to authentication scheme. Because in many authentication scheme you can track the past location of the tag. This would be very serious for owner's privacy and security.
6. Scalability:
   To provide the authentication to RFID Tag the system has to find the records from the data base. If the computational work on algorithm increases the number of tags increases so no longer the system will remain scalable
7. Attack resistance:
   To provide guaranteed authentication scheme this scheme should be secure against various attacks like man in the middle attack, reply attack, modification attack, server spoofing attack etc.

For providing secure authentication scheme which fulfill above requirements

## 4 ELLIPTICAL CURVE CRYPTOGRAPHY

Cryptography is a electronic technique that is used to protect valuable data over transmission. Mainly cryptography is science to provide security to information. To protect our data by using different authentication scheme is the main objective of cryptography. when authentication of data is main consider that should be less cost than the value of original information.

Two main terms that is used for the cryptography technique are Encryption and Decryption.

Encryption technique is used to send confidential data over communication .The process of encryption require two things (1) an encryption algorithm and (2) key.

Encryption is happened at the sender side. Encrypted algorithm is made to make information unreadable by all intended receivers.

Encrypt (plaintext, key) = cipher text

Decrypt (cipher text, key) = plaintext

Decryption is the reverse process of encryption. It is technique to convert the encrypted data to its original data that is now readable.Decryption technique need separate Decryption algorithm and a key. Encryption and Decryption algorithm are same.

Elliptical curve cryptography (ECC) is a (PKC) public key encryption technique based on elliptic curve theory that can be used to create faster in speed, smaller in size, and more efficient Cryptographic keys to provide authentication scheme to RFID system.ECC is PKC based crypto system like RSA (Rivest-Shamir-Adleman) but it different from RSA because of its quicker evolving capacity and it provide attractive and alternative way to researchers to create cryptographic algorithm according to their requirement that means how much security they want to provide to the system.

Previous research shows that the security level that is provided by RSA,using ECC that same security can be provided but using smaller key size. Research shows that using RSA algorithm that same security level can be achieved using 1024 bits key size but using ECC require only 160 bits key size.ECC algorithm can be implemented on compact size of RFID tags. So ECC authentication scheme is well suited for wireless communications, like mobile phones and smart cards. ECC point of multiplication operation is found to be computationally more efficient than RSA using fast and effective computational time. There are two types of attacks from which we have to provide security to the system

**Active Attack**: Attacker can send old or manipulated messages or it can be deleted

**Passive Attack**: In case of passive attacks, the attacker can interleave and make statistics about the communication. The detection of these attacks is difficult, so the goal is to prevent them. In case of active attacks the attacker can send old/manipulated messages and delete messages.

## 5. BLOCK DIAGRAM

The basic architecture shown in figure.1 for an RFID authentication scheme includes three main parts:

(1)The RFID tag

(2)The RFID reader

(3)The server.

We have to achieve authentication between the tag and the server, some of the secret data that are transmitted are already predefined between tag and the reader when the system is firstly set up. Data transmitted through communication channel between RFID tag and the RFID reader is not secure because their exchange of data is through wirelessly so anybody intercept data easily. So to prevent data proper authentication scheme is needed between RFID tag reader and RFID server.

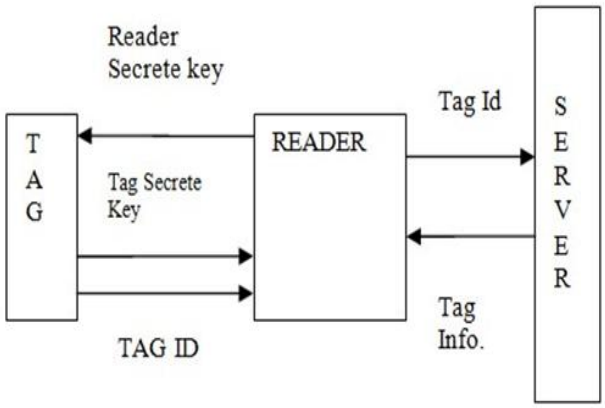


Fig 1. Block Diagram for RFID Authentication Scheme

### 5.1 RFID tag

RFID tag is microchip based technology, an antenna which is used to transmit data and hardware which has cryptographic operations. It stores secrete data that is going to use in authentication. RFID tag is used for communication with RFID reader.

Usually, computing capacity of the RFID tag's and used memory storage are very limited. Based on that RFID tags could be divided into three types:

(1)Passive tag

This type of RFID tag gets power through wireless signals from the reader

(2) Semi active tag

This semi active tag is equipped with a small battery and semi active tag gets power from it. The passive and the semi active tags both type of RFID tag use backscatter modulation to send messages.

(3)Active tag

The active type of RFID tag is equipped with a small battery and a radio transceiver. So that they can communicate directly with the reader.

### 5.2 RFID reader

An RFID reader is like composed of a radio transmitter, a radio receiver, a control unit, and a memory unit. The motive of an RFID reader is to enable the communication between RFID tag and the RFID server for exchange of messages between each other and achieve predefine mutual authentication. RFID reader's computing capacity is higher as compared to the RFID tag.

### 5.3 Server

A server is a trusted entity. To achieve the mutual authentication, Server stores all the identification information of RFID tag in its database when the system is set up. Using the stored identification information the server

determine the validity of tag. Computing capability and memory capacity of server are very high.

## 6. CRYPTOGRAPHY ALGORITHM

There are so many ways to do the classification of Cryptography Algorithm. This categorization are based on different number of keys that is used for encryption and description.

Based on that keys there are three types of algorithm used for Cryptography.

4.1 Secret key cryptography (SKC)

In this type of algorithm it uses Single key for both side Encryption and Decryption. That means Single key is used for encoding the message that is going to be transmitted and the same key is used for decode the received message. This is also called Symmetric key Cryptography.

Plain text —K→ Cipher text —K→ Plain text

4.2 Public key Cryptography (PKC)

In this type of algorithm one key is used for Encryption and another key is used for Decryption. One key is used for encode the message and second key is used for decode the method. There are no symmetry in keys so this method is also called Asymmetric key cryptography.

Plain text —K1→ Cipher text —K2→ Plain text

4.3 Hash Functions

In this algorithm Mathematical transformation is used for Encryption the information and Decryption the information. We represent our Elliptic Curve based authentication protocol, that is used to protects against the well-known attacks by hackers (security risks like eavesdropping, Man-in-the-Middle attack, reply attack etc ) in communication medium.

The basic goal of our protocol is to provide the strong authentication scheme in the RFID system. In defining this system we should consider so many factors that is recommended for achieve goal and the environment of the system where it will going to use.

The main requirement for computational capacity system are strong authentication and good and fast performance.

When any system that operates of the air interface or which uses radio signals for transmit and receive signals is cause of many security risks when defining any kind of authentication scheme it is necessary to know that who is the other user or how to prevent unauthorized access.

The main arithmetic computation of ECC is an operation denoted as point multiplication

When you define a protocol it is divided into two types one is fixed access control and randomized access control. In randomized access control common secret key is used for whole system wide or not. They could not satisfy some basic operation. In fixed access control a RFID tag replies a fixed message to the reader so that they can be designed area and memory.

## 7. PROPOSED ALGORITHM

In this algorithm two parties one sender and another receiver share a secret key. They exchange some public information. They have to be agreed on some domain parameters. They calculate their public information and their private key to calculate the secret data.. At both of the end they have private key and public key. The information that is going to transmit is multiplied with transmitter side secret key. The newly formed multiplied information is received at receiver end, which is multiplied with receiver's secret key. Third Party doesn't have access to calculate the shared information between transmitter and receiver from the available information.

**Step1**:

Consider an elliptic curve whose equation is $Y^2 = X^3 + AX + B$ which is also known as WeiestraB Equation.

**Step2**:

We have to find the coordinates for the above equation:
{(x1,y1),(x2,y2),(x3,y3)…… ∞}

**Step3**:

Generate the generation points that are the multiple of the coordinates on the Elliptic curve lying on the curve Example:2G,3G,4G…so on.

**Step4**:

Encryption

**Step5**:

Both end have key pair private key and public key .Let (p1,Qa)is private key-public key pair at one side suppose A.(p2,Qb) is the private public key pair of another side B.

**Step6**:

At side A, X=p1*Qb

**Step7**:

At side B, Y=p2*Qa

**Step8**:

p1*Qb*p2=p2*Qa*p1 Therefore We know information is X=Y,where Qa,Qb is the common generation point so p1*G*p2=p2*G*p1

**Step9**:

Secret shared is x

THE END

## 8. CONCLUSION

Elliptic curve Cryptography authentication scheme offers considerably greater data security for a given key size. If the key size is smaller it is also possible to implement for a given level of security so that it consume less power and less heat production. The smaller key size makes faster cryptographic operations, running on smaller chip and on more compact software.

So for data security ECC is the great choice for following reason:

1. ECC provide great security of given key size
2. By using smaller keys it make more compact implementation, fast cryptographic operations.
3. Less heat production and less power consumption

4. In ECC, there are efficient and compact hardware implementation

5. It is practically impossible to find private key so it is not possible for third party to obtain the secret.

**REFERENCES**

[1] Debiao He and Sherali 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

[2] R. Weinstein, "RFID: A technical overview and its application to the enterprise," *IEEE IT Prof.*, vol. 7, no. 3, pp. 27–33, May/Jun. 2005.

[3] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco ,"RFID technology for IoT-based personal healthcare in smart spaces,"*IEEE Internet Things J.*, vol. 1, no. 2, pp. 144–152, Apr. 2014.

[4] C. Lai *et al.*, "CPAL: A conditional privacy-preserving authentication with access likability for roaming service," *IEEE Internet Things J.* ,vol . 1, no. 1, pp. 46–57, Feb. 2014

[5] G. Godor and S. Imre, "Elliptic curve cryptography based authentication protocol for low-cost RFID tags," in *Proc. IEEE Int. Conf. RFID-Technol. Appl.*, 2011

[6] Y. Lee, L. Batina, and I. Verbauwhede, "Untraceable RFID authentication protocols: Revision of EC-RAC," in *Proc. IEEE Int. Conf. RFID*, 2009

[7] Q. Sheng, X. Li, and S. Zeadally, "Enabling next-generation RFID applications: Solutions and challenges," *IEEE Comput.*, vol. 41, no. 9, pp. 21–28, Sep. 2008.

[8] L. Batina *et al.*, "Public-key cryptography for RFID-Tags," in *Proc. IEEE Int. Workshop Pervasive Comput. Commun. Secur .*, 2007, pp. 217–222.

[9] Y. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol, "in *Proc. IEEE Int. Conf. RFID*, 2008, pp. 97–104.

[10] M. Burmester, B. Medeiros and R. Motta. Robust, anonymous RFID authentication with constant key-lookup. Cryptology ePrint Archive: listing for 2007 (2007/402), 2007.

[11] R. Weinstein, "RFID: A technical overview and its application to the enterprise," *IEEE IT Prof.*, vol. 7, no. 3, pp. 27–33, May/Jun. 2005.

[12] G. Gaubatz, J. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks, "in *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOMW'05)*, 2005, pp. 146–150.

[13] Kristin Lauter,Microsoft Corporation,2004, "The Advantage of Elliptic Curve Cryptography For Wireless Security",IEEE Wireless Communications

[14] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, "Software Implementation of Elliptic Curve Cryptography over Binary Fields", 2000