Indian Journal of Science and Technology, Vol 9(42), DOI: 10.17485/ijst/2016/v9i42/104589, November 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

# Secure Elliptic Curve Cryptography based RFID Authentication Schemes for Internet of Things

**R. Bagavath Sri* and S. Karthikeyan**

Sathyabama University, Chennai - 600119, Tamil Nadu, India;
Bagavathsriraghu007@gmail.com, karthijoy1@gmail.com

## Abstract

In medical field, patients generally need highly equipped systems because of their inability to access emergency systems. In such situation, high level of security must be ensured to prevent fatal medical errors. RFID technology is generally used in the medical environment. Applications of elliptic curve algorithm are considered and several cryptography modules are analyzed. Heavy weight schemes are considered to be highly secure. Security drawbacks have been analyzed in Godor and Imre scheme in terms of maximum delay and running time and improved encryption and decryption scheme has been proposed. The proposed algorithm has been simulated in Xilinx 14.5 ISE and worst case slack, running time and frequency has been analyzed.

**Keywords:** Desynchronisation Attacks, DOS Attacks, Elliptic Curve Cryptography, IoT, RFID Technology, Server Spoofing Attacks

## 1. Introduction

With the increased life standard of people in various parts of the world, there is a hike in life expectancy of people. But still people suffer from many disabilities due to several reasons and treating them has become a biggest challenge in the medical world. Generally disabilities are genetically transmitted or due to injuries from accidents. The injured parts are mostly not recovered and loss of certain body parts result in serious psychological issues. Several computers have been developed to provide comfort for disabled people. For ease of treatment, people with disabilities are made more accessible to computers. The patient's health condition must be the only focus at any situation. In healthcare environment, it is necessary to deal with several kinds of patients under different situations. Hence medication error and fault in patient medical data would be a fatal issue. RFID technology is generally used in personal healthcare for collection of data. It provides low cost, less energy consuming and disposable sensors for data collection. It can be used as a part of the IoT physical layer for monitoring patient's health and provide remote assistance. RFID can be used to collect information regarding temperature, humidity etc. about the patient's living environment. Open challenges are present in this field where the gathered information is prone to serious security attacks. Hence we design an efficient RFID authentication scheme based on Elliptic Curve Cryptography to avoid these security threats.

## 2. IoT for Healthcare Environment

The major challenge faced by the communication systems is the ability of devices from various locations to exchange data. This is defined as interoperability. Several standards define specifications and procedures to ensure the level of interoperability between the devices. This is given by the huge success of Wi-Fi operated devices. It is mainly implemented in Laptops, Tablets and smart phones because of high level of interoperability. It can be used to connect up to 250 devices. It generally operates in ISM 2.4 GHz band. The output of Wi-Fi has high power which allows for full home coverage[1]. Thus Wi-Fi can be the most possible

*Author for correspondence

wireless internet connectivity technology technique till date. Though its high power and complexity is a barrier to IoT, new silicon based devices reduce these problems and enable Wi-Fi in integrating with the IoT environment. In healthcare environment, IoT provides remote monitoring, ambulance telemetry, hospital assets tracking and maintenance prediction. The main challenges faced by IoT are:

- Complex sensing environment.
- Necessity of security.
- Cloud connection.
- Power consumption.
- Multi connection services.

## 3. Typical RFID Authentication System Architecture

The RFID system architecture includes RFID tag, RFID reader and backend server shown in Figure 1. The channel is insecure between tag and reader because of wireless exchange of data and adversary could attack the channel.

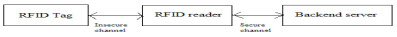


**Figure 1.** RFID System architecture.

:

The channel is secure between reader and server since a secret key is preshared between them when the system is setup initially.

RFID tag consists of microchip, antenna and hardware for cryptography purpose. It stores secret data for authentication. The main drawback is that it has limited storage. There are three types of RFID tags.

Passive tag**:** Wireless signals from the reader provide power[2].

Semiactive tag**:** Battery supplies power for operation.

Active tag: It consists of a battery and transceiver. It can communicate directly with the reader.

RFID reader**:** It consists of transceiver, memory and control unit. It provides mutual authentication when the data is exchanged between tag and server.

Backend server**:** It stores RFID tag's ID information and checks the validity thereby the system achieves mutual authentication.

Power is of high concern in RFID design approach. It is considered for transferring power from reader to tag. It involves magnetic induction and electromagnetic induction. It is associated with RF antenna. Another feature for RFID tag is memory revolution. It should contain more information than a simple ID with additional read only or read write memory through which reader can interact with. Read only memory contain secret product details which is available when needed and not read every time a tag is requested. It is used to recover data in online base. Read write memory size is very small. Though RFID system has a high risk of insecurity, it can be made useful by proper encryption and decryption schemes through cryptography.

## 4. Purpose of Elliptic Curve Cryptography Algorithm

RFID authentication schemes are classified into Non Public Key Cryptosystem schemes and Public Key Cryptosystem schemes. NPKC based schemes have high performance[3] since no complex operations are required. But it remains insecure. PKC based systems are necessary for secure communication since NPKC systems cannot satisfy several security attributes. Some complex PKC algorithms[4] can be implemented in RFID chips. Still Elliptic Curve Cryptography appears to be more suitable due to high security level with shorter key size. The low computation and processing overhead makes it possible for RFID tags with low computation power. ECC algorithm with 164 bit key size has security level similar to 1024 bit key size of RSA algorithm. It can be proposed for practical applications. There are three categories of ECC based RFID authentication schemes based on the type of operations. Heavyweight schemes involve complex public key encryption schemes and digital signature operations. Middleweight schemes require elliptic curve and hash function operations. Lightweight schemes need only elliptic curve operations[5].

Plain text is the original form of the message that sender wants to send to recipient. Cipher text is the encrypted form of the original message which can be transmitted in an insecure channel such as Internet. The sender and recipient use the same secret key for the encryption and decryption function. Therefore, it is called symmetric key cryptography shown in Figure 2.

Consider the equation of elliptic curve, p be the point on the curve and n be maximum limit as shown in Figure 3.

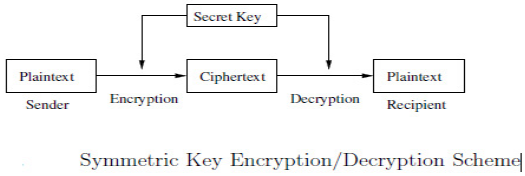


**Figure 2.** Symmetric key encryption and decryption scheme.

ECC involves key generation, encryption and decryption. It generates public key and private key. The sender will encrypt message with receiver's public key[6]. The receiver decrypts the private key of sender. Elliptic curve key pair generation require domain parameters (p, E, P, n). Compute Q = dP where Q = public key, d = private key. It ranges from 1 to (n-1).

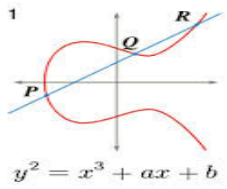


**Figure 3.** Example of elliptic curve equation $y^2 = x^3 + ax + b$.

## 4.1 Basic ElGamal Elliptic Curve Encryption

It has the domain parameters (p, E, P, n) and plaintext M. Two cipher texts will be generated. T1 = RP and T2 = M+RQ. T1 and T2 are generated.

## 4.2 Basic ElGamal Elliptic Curve Decryption

It has private key d and cipher texts T1 and T2. Compute M = T1-dT2 = (M+RQ)-d(RP). Since Q = dP, message M is extracted. It could not satisfy most of the security requirements and it involves complex modular inversion operations.

## 4.3 Improved ECC based RFID Authentication Scheme in Proposed Hardware

It consists of Elliptic Curve domain parameters (p, E, Q, n). Compute y = xP where P = point on the curve, x = private key and y = public key. x ranges from 1 to (n-1). Improved encryption and decryption scheme is shown in Figures 4a and b.

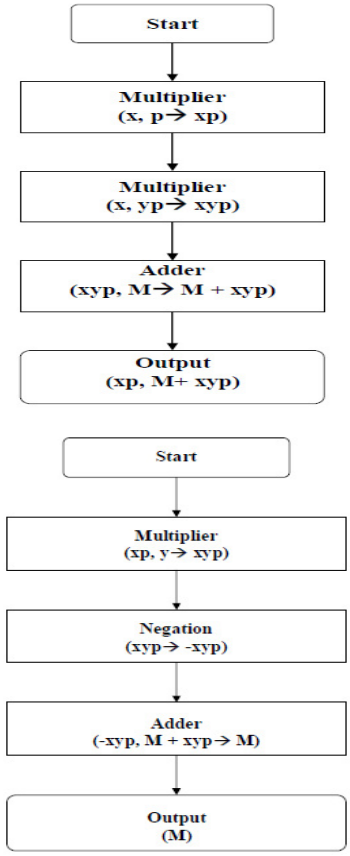


**Figure 4.** Flowchart for (a) encryption and (b) decryption.

## 4.4 Improved Encryption Algorithm

Server chooses the random number xεZn and computes $P_s$ = xP. For each tag, private key is multiplied with public key value yp and finds xyp. This value is added with the message to find E = M + xyp. The server stores ($P_s$, E).

## 4.5 Improved Decryption Algorithm

The server takes the value $P_s$ and public key to find xyp. Message is decrypted by subtracting the value of xyp from the received message. It is added with the value of E to obtain the original message M. Elliptic curve cryptosystem architecture includes:

- Point (scalar) multiplication.
- Point doubling.
- Point addition.
- Finite field arithmetic.

### 4.6 Point Addition

The point addition module is given in Figure 5 where x1, x2, z1, z2 are input data, P and Q are point on the curve, x and y are private and public keys. Bit wise xor operations produce encrypted output z3 after squaring. This involves the addition of two points P and Q in an elliptic curve of equation E to obtain R = P+Q. Join P and Q using line L. On solving the equations of L and E, three solutions are obtained. L intersects E at a third point –R. On negating –R, R is obtained just opposite to it. Join R and –R gives P+Q.

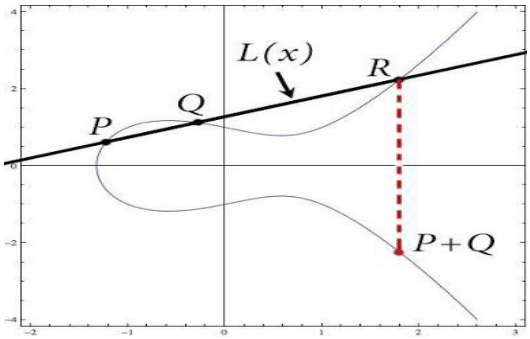


**Figure 5.** Point addition on elliptic curve.

### 4.7 Point Doubling

When P = Q in point addition then R = 2P. To add a point P to it, a tangent line to curve can be drawn at P. If yP is not zero, then the tangent line intersects the curve at another point –R. It is reflected to R as shown in Figure 6.

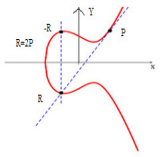

**Figure 6.** Point doubling on elliptic curve.

### 4.8 Point Multiplication

X and y are input data and k is the encrypted input. Point addition and doubling can be done with two multiplications and one field inversion. But inversion is more expensive than field multiplication.

### 4.9 Finite Field Arithmetic

It consists of multiplication, squaring, inversion and addition with finite number of elements. Field $F^{2n}$ or GF ($2^n$) has a binary nature. Hence have hardware implementations.

## 5. Security Proof

### 5.1 Security against DoS and Server Spoofing Attack

DoS attack makes a server unavailable for authenticated user. It is achieved by crashing a server or flooding server with fake requests. In the improved scheme, private key x is preshared between the tag and server which rejects all the unwanted requests from unknown users and only M corresponding to stored tag's identity is taken after the tag's identity is verified by the server. Server spoofing attack is a case when the server is unable to identify the tag and server identity. But in the improved scheme we are storing the identity in the server when the system is setup initially. So it is secure against server spoofing attack.

Adder (M, xyp) = M + xyp

Inversion (xyp) = -xyp, output = M+xyp-xyp = M

### 5.2 Security against Modification and Desynchronisation Attack

Modification attack might change the address of the message and routed to a wrong location. Only the tag's identity is first authenticated by the server before message M reaches the server. If the tag's identity is authenticated by the server, the message will be read which secures against modification attack. Using bitwise operations are proved to be secure against desynchronisation attacks.

## 6. Conclusion

RFID technology has gained much importance in IoT in healthcare environment. Our improved ECC based RFID scheme proves to be secured against DoS, desynchronisation, modification and server spoofing attacks. It can be effectively implemented for IoT for further advancements

in medical field which would also improve the standard of patient's treatment. This also has a great impact on global economy when security issues are satisfied. In this way, medical data can be collected from several hospitals in a city through Internet. This data collection will be useful in getting health condition of patients under different treatments which would reduce fatal medical errors and overall determination of health condition of patients in the particular region will be stored which will be useful for future researches on Internet of Things.

## 7. Acknowledgements

The authors wish to thank all anonymous reviewers for their valuable comments.

## 8. References

1. Najera P. Real-time location and inpatient care systems based on passive RFID. Journal of Networkand Computer Application. 2011; 34(3):980–9.
2. Wang C. Lightweight RFID authentication protocol based on elliptic curve cryptography. Journal of Computers. 2013; 8(11):2880–7.
3. Wang S. Analysis and construction of efficient RFID authentication protocol with backward privacy. Advances in Wireless Sensor Networks. Berlin,Germany: Springer-Verlag. 2014; 334:458–66.
4. Kaya SV, Savaş E, Levi A, Ercetin O. Public key cryptography based privacy preserving multi-context RFID infrastructure. Ad Hoc Networks. 2009; 7(1):136–52.
5. Batina L. Public-key cryptography for RFID-tags. Proceeding of IEEE International Workshop Pervasive Compuer Communication Security; White Planis, NY. 2007. p. 217–22.
6. Amendo S. RFID technology for IoT based personal healthcare in smart spaces. IEEE Internet of Things. 2014; 1(2):144–52.