© 2018 IJSRSET | Volume 4 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
National Conference on Advanced Research Trends in Information and
ting Technologies (NCARTICT-2018), Department of IT, L. D. College of Engineering,
Ahmedabad, Gujarat, India In association with
International Journal of Scientific Research in Science, Engineering and Technology

# A Survey of Authentication of RFID Devices Using Elliptic Curve Cryptography

**Suthar Monali, Prof Alka J Patel**
*[1]ME , IT Department, LDCE, Ahmedabad, Gujarat, India
[2]Assistant professor , IT Department, LDCE, Ahmedabad, Gujarat, India

## ABSTRACT

RFID is a wireless technology for automatic identification and data capture and it's the core technology to implement the internet of things. Because of that, the security issue of RFID is becoming more important. In past , simple mathematical and logical method, hash based schemas and simple PKI schemas are introduce RFID authentication . In this paper I illustrate about the possible security attack on RFID and three different authentication algorithm of RFID based on ECC and I also describe about why ECC is the best method among them .

**Keywords:** RFID, Reader, Tag, Backend Sever , Authentication , Security , ECC.

## I. INTRODUCTION

RFID system is composed of tags, readers, backend sever, and antennas. RFID tags are available in affordable charges, wireless devices which can be communicate with RFID readers [1].RFID architecture shown in below figure which consist tag, reader and back-end server. Tag consist EPC (electronic product code) which store details about tag. Reader is responsible for reading and writing tag information. Back end sever will save all data about tag which are in one group .Communication in RFID network will start on reader broadcast message or query. Communication between tag-reader and reader-server is in insecure channel.

In this paper we first analyse security attack possible on RFID in section II, we discuss RFID device performance measurement in section III, three authentication method or protocol discussed in section IV.

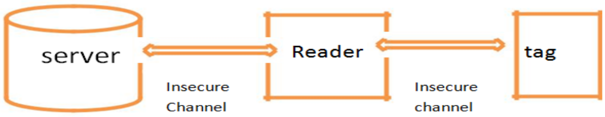

**Figure 1.** RFID architecture

### Security Attck On Rfid

**Denial of Service (DOS) :** In both of wireless and wired communication, there are Denial of Service (DOS) . Once attackers control a large number of fake readers and tags, they can make the data connection to abuse computational resources, and even use up the resources and network bandwidth.[1]

**Eavesdropping:** The communication channel between the tag and the reader can be eavesdropped, because the radio frequency channel is not secure communication channel .[2]

**User privacy:** The attacker can monitor the tag using the tag identifier in order to know the user's behaviour, when the user identity is linked to a certain tag. Also, the attacker can trace the user location with the tag identifier, when the output of the tag such as the tag identifier is unchangeable.[2]

**Replay attack:** The attacker obtains messages between the tag and the reader by eavesdropping and reuses the message in order to impersonate a legitimate tag or a legitimate reader.[2]

**Spoofing attack :** The attacker impersonates a reader, sends a query to a tag, and then obtains the response of the tag. When the legitimate reader queries the tag, the attacker will send the obtained response to reader in order to impersonate the tag.[2]

**Cloning attack:** An attacker can build a cloned tag which will be interpreted by the reader as the legitimate tag, due to the fact that most tags are not tamper-proof.[2]

**Performance**

RFID schemes cannot use computationally intensive cryptographic algorithms for privacy and security because tight tag cost requirements make tag-side resources (such as processing power and storage) scarce .[3]

- Capacity minimisation: The volume of data stored in a tag should be minimised because of the limited size of tag memory

- Computation minimization: Tag-side computations should be minimized because of the very limited power available to a tag.

- Communication compression: The volume of data that each tag can transmit per second is limited by the bandwidth available for RFID tags [3]

- Scalability: The server should be able to handle growing amounts of work in a large tag population. It should be able to identify multiple tags using the same radio channel [3] Performing an exhaustive search to identify individual tags could be difficult when the tag population is large [3].

## II. LITERATURAL SURVEY

Authenticity can be achieved by a secure protocol running between RFID tag and reader [4]. To achieve authentication public key cryptography (PKC), non-public key cryptography (NPKC), hash function, hash with random number, simple bitwise operation, AES, HMAC schema can be used. The suitability of PKC for RFID is an open research problem due to the limitation in tag cost, gate area and power consumption. Among PKC algorithms, ECC based algorithms would be the best choice for RFID system due to their small size key and efficient computation. So, ECC is very attractive for small devices like RFID with limited computational capacity, memory and low bandwidth network. In this paper we will discuss three ECC based RFID authentication algorithms.

### a) A secure ECC based RFID authentication protocol with ID verifier

This paper[Liao's schema] proposes an ECC based mutual authentication algorithm that satsfies the essiential requirements in RFID system [2].

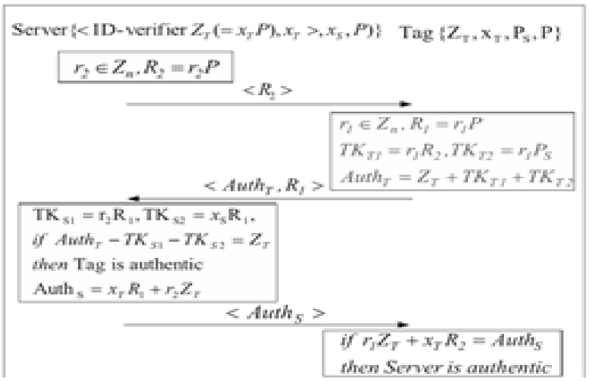
Server {< ID-verifier $Z_T(=x_TP), x_T>, x_S, P$)}
Tag {$Z_T, x_T, P_S, P$}
$r_2 \in Z_n, R_2 = r_2P$
$<R_2>$
$r_1 \in Z_n, R_1 = r_1P$
$TK_{T1} = r_1R_2, TK_{T2} = r_1P_S$
$Auth_T = Z_T + TK_{T1} + TK_{T2}$
$< Auth_T, R_1 >$
$TK_{S1} = r_2R_1, TK_{S2} = x_SR_1,$
if $Auth_T - TK_{S1} - TK_{S2} = Z_T$
then Tag is authentic
$Auth_S = x_TR_1 + r_2Z_T$
$< Auth_S >$
if $r_1Z_T + x_TR_2 = Auth_S$
then Server is authentic

**Figure 2.** Liao's schema

In this algorithm tag believes that the ID verifier Zt is securely transmitted to the server and vice versa. This algorithm provide Mutual authentication, confidentiality, forward security, scalability. This algorithm resisting replay attack, tag masquerade attack, server spoofing attack, location attack, cloning attack [2].To implement this schema successfully a powerful server device needed [2]. There are also some other schema [3-6] which are more efficient then this schema in tag computational time [2].

### b) Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography

This paper is improved version of Chou's protocol [7] based on ECC which is failed to provide mutual authentication and cloning attack. [8]

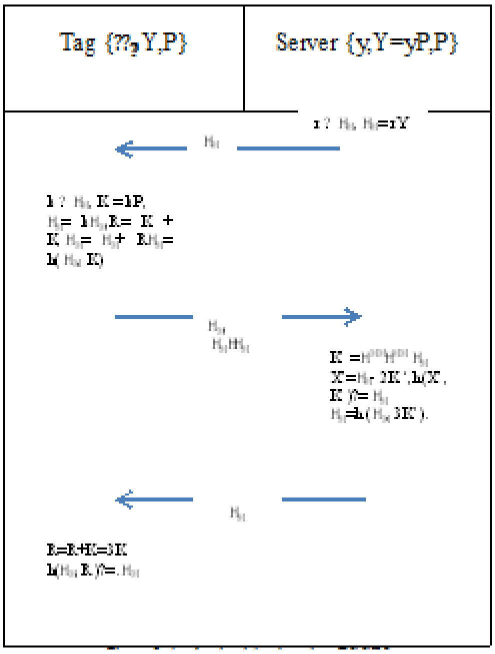

**Figure 3.** chou's algorithm based on ECC[9]

Weaknesses of Chou's schema: Lack of tag privacy, forward privacy and mutual authentication. Farash introduces improved version of Chou's algorithm to achieve mutual authentication and tag privacy [figure 4]. Farash's schema has proof against mutual authentication, tag privacy. Computational cost of Frash's schema is same as Chou's schema [8].The total computation of schema is very high. To improve this some pre computing technique should use [8].

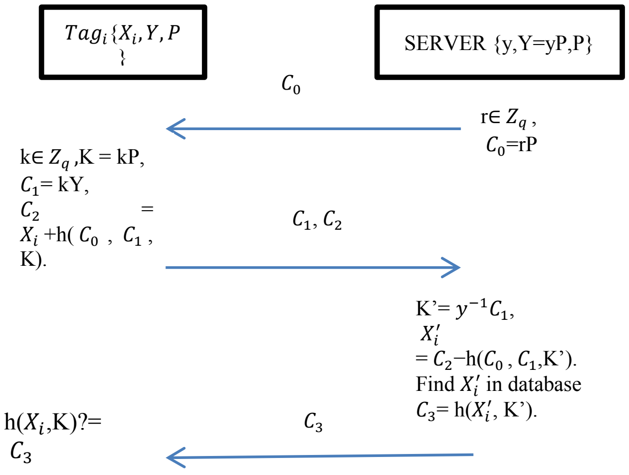

Figure 4 Farash's authentication

**c) Elliptic Curve Cryptography Based Mutual Authentication Protocol for Low Computational Capacity RFID Systems - Performance Analysis by Simulations**

In this paper no reader communication is only happen between back end server and tag. In this group key is use to perform authentication instead of individual key [9].

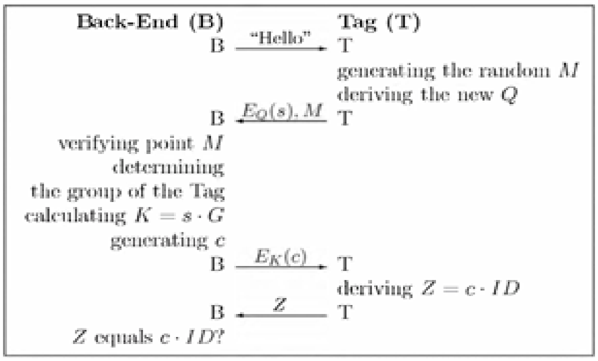

**Figure 5.** Godor's schema[9]

While in use of 160 bit elliptic curve might be very big and required high computational capacity and strong back-end sever[9] .This paper have implementation in OMNET ++.

Godor's schema is acceptable for every attack except DOS . This schema also prove that computational time for 112 bit and 160 bit are almost near.

## III. COMPARISON

| Attacks | Liao's | Farash's | Godor's |
|---|---|---|---|
| Mutual authentication | Yes | Yes | Yes |
| Scalability | - | - | - |
| DOS | - | - | No |
| Cloning | - | - | - |
| Server spoofing | - | - | - |
| Replay | - | Yes | - |

| Comparison factor | Liao's | Farash's | Godor's |
|---|---|---|---|
| Computational time | .32 sec | Not measured | .1006(160bit) |

## IV. CONCLUSION AND FUTURE WORK

In the conclusion three of them are ECC based authentication schema; all are proved more efficient against simple PKI, simple HASH, AES and RSA. All three have much computational time to perform authentication and all three needed high capacity back-end sever. So in future some pre-computational method can implement with ECC.

## V. REFERENCES

[1]. Xiao Nie, Xiong Zhong "Security In the Internet of Things Based on RFID: Issues and Current Countermeasures" Proceedings of the Published by Atlantis Press, Paris, France.

[2]. Yi-Pin Liao , Chih-Ming Hsiao "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol " Department of computer science and information engineering , St.John's university,Taipei,ROC (2013), published by ELSEVIER, http://dx.doi.org/10.1016/j.adhoc.2013.02.004

[3]. C.P. Schnorr," Efficient identification and signatures for smart cards", in: Gilles Brassard (Ed.), Advances in Cryptology – CRYPTO'89, Lecture Notes in Computer Science, 435, Springer-Verlag, 1989, pp. 239–252.

[4]. T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes", in: E.F. Brickell (Ed.), Advances in Cryptology – CRYPTO'92, Lecture Notes in Computer Science, 740, Springer-Verlag, 1992, pp. 31–53.

[5]. Y.K. Lee, L. Batina, I. Verbauwhede, "EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID Authentication Protocol", IEEE International Conference on RFID, 2008, pp. 97–104.

[6]. Xinglei Zhang, Linsen Li, Yue Wu, Quanhai Zhang, "An ECDLP-Based Randomized Key RFID Authentication Protocol", 2011 International Conference on Network Computing and Information Security.

[7]. ChouJS(2013)" An efficient mutual authentication RFID scheme based on elliptic curve cryptography" .J Supercomput. doi:10.1007/s11227-013-1073-x

[8]. Mohammad Sabzinejad Farash " Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptograph" published by Springer Science+Business Media New York 2014, DOI: 10.1007/s11227-014-1272-0

[9]. sGy6z6 Godor, Norbert Giczi, Sandor Imre Dr."Elliptic Curve Cryptography Based Mutual Authentication Protocol for Low Computational Capacity RFID Systems -Performance Analysis by Simulations", Department of Telecommunications, Budapest University of Technology and Economics Magyar Tud6sok korutja 2., Budapest, Hungary H-ll17, 978-1-4244-5849-3/10/$26.00 2010 IEEE