ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

AN ANALYSIS OF AUTHENTICATION SCHEMES FOR INTERNET OF THINGS

Manoj Kumar S
[*] M.tech student, Dept of ISE BMS College of Engineering Bangalore-India

ABSTRACT

Advances in communication and information technologies have led to the emergence of Internet of Things (IoT). Internet of Things (IoT) has emerged as one of the most powerful communication paradigms of the 21st century. The radio-frequency identification (RFID) technology is one of the technologies of IoT deployments. To satisfy the security requirements of RFID technology in IoT, many RFID authentication schemes have been proposed. Recently, elliptic curve cryptography (ECC)-based RFID authentication schemes have attracted a lot of attention. In this paper, we discuss the security requirements of RFID authentication schemes, and present a review of ECC-based RFID authentication schemes in terms of performance and security.

KEYWORDS: Authentication, elliptic curve cryptography (ECC), performance, radio-frequency identification (RFID), security, Internet of Things (IoT).

INTRODUCTION

The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. [4]In the IoT environment, all objects in our daily life become part of the Internet because of their communication and computing capabilities (including microcontrollers, transceivers for digital communication, suitable protocol stacks) that allow them to communicate with other objects [5]. IoT extends the concept of the Internet and makes it more pervasive. In the IoT environment, the seamless interactions among different types of devices, such as vehicles, medical sensors, monitoring cameras, home appliances, etc., have led to the emergence of many applications such as smart city, home automation, smart grid, traffic management. IoT involves many kinds of cheap sensors (wearable, implanted, and environmental).

Radio-frequency identification (RFID) is one of the most important technologies used in the IoT as it can store sensitive data, wireless communication with other objects, and identify/track objects automatically [6]. Compared to the traditional barcode, RFID could be applied to objects with rough surfaces, can provide both read/write capability, requires no line-of-sight contact with RFID readers, and can read many RFID tags simultaneously. All these benefits make RFID a superior technology compared to the traditional barcode system.

According to cryptographic primitives used in those schemes, RFID authentication schemes can be broadly classified into nonpublic-key cryptosystem (NPKC)-based schemes and public-key cryptosystem (PKC)-based schemes. The NPKC-based RFID authentication schemes have better performance because no complex operations are needed. In contrast to PKC algorithms, the elliptic curve cryptography (ECC) system is more suitable for RFID system because it can provide similar security level but with a shorter key size [7] and has low computational requirements. The low processing overhead associated with ECC makes it suitable for use with RFID tags because they have limited computing power The ECC algorithms have been implemented on very compact RFID chips.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

ARCHITECTURE AND SECURITY REQUIREMENTS OF RFID AUTHENTICATION

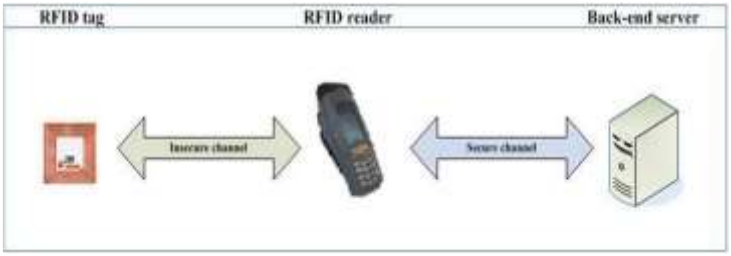

FIG 1.Architecture of an RFID authentication scheme

System Architecture

The basic architecture (shown in Fig. 1) for an RFID authentication scheme includes three entities: the RFID tag, the RFID reader, and the server. To achieve authentication between the tag and the server, some secret data are preshared between them when the system is set up. The communication channel between the RFID tag and the RFID reader is not secure because they exchange data wirelessly and an adversary could intercept the data easily. The communication channel between the RFID read and the server is secure because a secure channel is established between them through a preshared secret key and some security mechanism.

1) RFID tag: A tag is composed of a microchip, an antenna, and a dedicated hardware for cryptographic operations. It can store secret data for authentication and it communicates with the RFID reader. Usually, the RFID tag's computing capacity and memory storage are very limited.
2) RFID reader: An RFID reader is composed of a radio transmitter, a radio receiver, a control unit, and a memory unit. The main function of an RFID reader is to enable the RFID tag and the server to exchange messages between each other and achieve mutual authentication. The RFID reader's computing capacity is higher compared to that of the RFID tag.
3) Server: A server is a trusted entity. To achieve the goal of mutual authentication, it stores all the RFID tag's identification information in its database when the system is set up. Using the stored identification information, the server could determine the validity of the tag. The server's computing capability and memory capacity are high.

Security Requirements for RFID Communication

RFID authentication is one of the most important steps to ensure secure communication in the RFID system. However, messages transmitted between the RFID tag and the RFID reader are exposed to many kinds of security threats. The following security requirements that must be satisfied to ensure secure RFID communications in addition to a robust and efficient authentication scheme in place.

1) Mutual authentication: It is essential that mutual authentication among the RFID tag, the RFID reader, and the server should be achieved before a session starts. Mutual authentication between the RFID tag and the server is required.
2) Confidentiality: It is essential that the secret information stored in the RFID tag cannot be retrieved by the adversary when it is transmitted through the communication channels. The adversary could impersonate the tag to the server if access to the secret information is possible. The information must be encrypted before transmission.
3) Anonymity: It is essential that an RFID authentication scheme should provide anonymity. The adversary will violate the owner's privacy and trace his/her action if the tag's identity becomes known.
4) Availability: It is essential that the authentication process of an RFID authentication scheme be executed during the lifecycle of the RFID tag. To provide anonymity, the RFID tag and the server in most of RFID authentication schemes update the secret information shared between them when the authentication scheme is executed.
5) Forward security: It is essential that an RFID authentication scheme provides forward security. In many RFID authentication schemes, the adversary could trace back the past location of the tag if the secret information from the RFID tag is successfully retrieved by the adversary.

6) Scalability: It is essential that an RFID authentication scheme should be scalable. To authenticate the RFID tag, the server in the RFID system has to find the matching record from its database. If the computational workload of the searching algorithm increases significantly as the number of RFID tags increases, the system will not scale.
7) Attack resistance: To guarantee secure communication within the RFID system, the RFID authentication process should be secure against various attacks including the replay attack, the tag masquerade attack, the server spoofing attack, the man-in-the-middle attack, the tag cloning attack, and the modification attack.

REVIEW OF SOME ECC-BASED RFID AUTHENTICATION SCHEMES

We classify several ECC-based RFID authentication schemes into three broad categories based on the type of operations they use. These three categories include heavyweight, middleweight, and lightweight schemes. Heavyweight schemes [2],often involve very complex operations such as public-key encryption operations and digital signature operations. For the middleweight schemes [3], [14],[16], both elliptic curve operations and hash function operations are needed. Finally, for lightweight schemes [1],[9], [11], [12], [10], only elliptic curve operations are needed. In this section, we review several ECC-based RFID authentication schemes based on these three categories. We use the following notations (shown in Table I) in the rest of the paper.

Table 1. Notations

Notation	Description
$F(q)$	Finite field
n	Large prime number
$E(F(q))$	Elliptic curve defined by the equation
P	Point on $E(F(q))$ with order n
G	Group generated by the point P
(y,Y)	Private/public key pair of the server, where $Y = yP$
(x_i,X_i)	Secret information of the tag, where $X_i = x_iP, i = 1,2$
$h(\cdot)$	Secure hash function mapping $\{0,1\}^*$ to Z_n

Heavyweight Schemes

Godor and Imre [2] proposed an ECC-based RFID scheme using a simplified version of ElGamal scheme and Elliptic Curve Digital Signature Algorithm (ECDSA), the use of a Public-Key Infrastructure (PKI) is assumed in their scheme. In the initialization phase, the server generates system parameters params = $\{F(q),E(F(q)), n, P, Y\}$ and stores $(M,X1)$ and $(x1, Y)$ in its database and the tag's memory separately.

Step 1) Server → Tag: The server uses its private key y to compute a signature σS of the random number rR generated by the reader and sends the message $\{rR, \sigma S\}$ to the tag through the reader.

Step 2) Tag → Server: After the tag receives the message $\{rR, \sigma S\}$, it uses the server's public key Y to check the validity of σ. If it is not valid, the tag terminates the session; otherwise, the tag generates a random number rT and computes $T = rTP$, $M\_ = M \oplus x(rT\,Y)$, and a signature σT, where M is the message about tag's identity and $x(rT\,Y)$ denotes the x-coordinate of the point $rT\,Y$. Finally, the tag sends the message $\{T,M\_, \sigma T\}$ to the server through the reader.

Step 3) Server: After the server receives the message $\{T,M\_, \sigma T\}$, it uses the private key to compute $M = M\_ \oplus x(yT)$ and looks up the tag's public key $X1$ according to M. If no tuple $(M,X1)$ exists in its database, the server terminates the session; otherwise, the server uses $X1$ to check the validity of the signature σT. If it is not valid, the server rejects the session; otherwise, the tag is authenticated.

By using both the ElGamal scheme and the ECDSA, Godor and Imre's scheme could satisfy most security requirements proposed in Section 2. However, both of the two operations are quite complex. For example, the verification algorithm in the ECDSA needs at least two elliptic curve point multiplications. Besides the hardware needed for elliptic curve point operations, additional hardware is needed to support the two algorithms. Therefore, the

performance of their scheme is not suitable for practical applications and their scheme cannot be applied to cheap RFID tags. In addition, Godor and Imre's scheme cannot withstand the replay attack because the tag cannot check the freeness of the received message *{rR, σS}*. Therefore, their scheme is not suitable for practical applications.

Middleweight Schemes

Both of the public-key encryption operation and the digital signature operation are complex operations. To improve performance, several ECC-based RFID schemes combining hash function operations have been proposed. Wang *et al.* [3] proposed an ECC-based RFID authentication scheme using hash function operations to get backward privacy. In the initialization phase of their scheme, the server generates system parameters params = *{F(q),E(F(q)),n, P, Y }* and stores ($X1$) and ($x1$, Y) in its database and the tag's memory respectively. The following steps are executed between the tag and the server to achieve mutual authentication.

Step 1) Tag → Server: The tag generates a random number $r1$, computes $T1 = r1P$, and sends the message *{T1}* to the server.

Step 2) Server → Tag: Upon receiving *{T1}*, the server generates a random number *rs* and sends it to the tag.

Step 3) Tag → Server: Upon receiving *{rs}*, the tag computes $T2 = r1Y$, $v = r1 + x1h(T2, rs)$ and sends the message *{v}* to the server.

Step 4) Server: Upon receiving *{v}*, the server checks whether there is a tuple ($X1$) such that the equation $vP = T1 + h(yT1, rs)X1$ holds. If there is no such tuple, the server rejects the session; otherwise, the tag is authenticated.

If the number of tags in Wang *et al.*'s scheme is *N*, the back-end server has to check about *N*/2 equations to verify the validity of the tags on average. Therefore, the computational workload of the searching algorithm increases significantly with an increase in the number of tags making this scheme not scalable and not suitable for practical applications. Besides, the tag in Wang *et al.*'s scheme cannot authenticate the backend server because it receives only a random number sent by the back-end server. Therefore, Zhang *et al.*'s schemes cannot provide mutual authentication.

Lightweight Schemes

Although middleweight schemes described earlier have better performance than the heavyweight schemes, a specific hardware is still needed in the tag to support the hash function operation. Therefore, ECC-based RFID authentication schemes which only require elliptic curve operations have better performance compared with heavyweight and middleweight schemes and are more suitable for practical applications. Lee *et al.* [1] proposed an ECC-based RFID authentication scheme that requires only elliptic curve operations. In the initialization phase, the server generates system parameters params = *{F(q),E(F(q)), n, P, Y }* and stores ($x1$,$X1$,$X2$) and ($x1$, $x2$, Y) in its database and the tag's memory separately. Then, the server authenticates the tag through the following steps.

Step 1) Server → Tag: The server generates a random number *rs* and sends the message *{rs}* to the tag.

Step 2) Tag → Server: Upon receiving the tag, the tag generates a random number *rt* and computes $T1 = rtP$,$T2 = (rs + x1)P$, and $v = rtx1 + rsx2$. Then, the tag sends the message *{T1, T2, v}* to the server.

Step 3) Server: Upon receiving the message $M1$, the server computes $x1P = y{-}1T2 - T1$ and performs a lookup in its database for the tuple ($x1$,$X1$,$X2$). Then, the server checks whether the equation $r{-}1\ s\ (vP - x1T1) = X2$ holds.

Although Lee *et al.* [36] claimed that their scheme could withstand various attacks, Bringer *et al.* [37] found that their scheme cannot withstand the tracking attack and the tag impersonation attack.

PERFORMANCE AND SECURITY EVALUATION

In this section, we compare the performance and security aspects of the ECC-based RFID authentication schemes discussed earlier. By evaluating them in terms of the security requirements listed in Section 2 and comparing their communication costs, we could determine whether an ECC-based RFID authentication scheme is suitable for practical applications. It is well known that the tag's computing capability and memory are very limited. Therefore, the

communication cost, and the storage requirements are important characteristics for practical applications. To achieve the same security level as the RSA algorithm with 1024 bits key size, an elliptic curve defined over the finite field $F(2^{163})$ is used in many implementations.

Analysis of Communication Cost

We use an elliptic curve defined over the finite field $F(2^{163})$ in our comparisons. We need 42 bytes and 21 bytes to store a point on the elliptic curve and an element of the field, respectively. In addition, we assume that the output of the hash function and the length of identifier are 20 bytes and 4 bytes, respectively. Table 2 shows the detailed communication cost of various ECC-based RFID authentication schemes. From the table, we can deduce that the communication costs of Sandhya and Rangaswamy's scheme [11] and Martinez *et al.*'s scheme [12] are the least. Besides, the communication cost of Chen *et al.*'s scheme [13] is the highest.

Analysis of Security Requirements of ECC-Based Authentication Schemes

Security is the most important aspect of an RFID authentication scheme. The security requirements of related ECC-based RFID authentication schemes are discussed in this section. Let SR1, SR2, SR3, SR4, SR5, SR6, an SR7 denote mutual authentication, confidentiality, anonymity, availability, forward security, scalability, and attack resistance, respectively. The results of the comparison are shown in Table 3. Based on the analysis shown in Table IV, we found that the most of the recently proposed ECC-based RFID authentication schemes cannot satisfy all security requirements (in particular mutual authentication) we

Scheme	From tag to server	From server to tag	Total communicational cost
Sandhya et al.'s scheme[11]	*25*	*42*	*67*
Martinez et al.'s scheme[12]	*25*	*42*	*67*
Wang et al.'s scheme[3]	*63*	*21*	*84*
Lee et al.'s scheme[1]	*21*	*105*	*126*
Godor et al.'s scheme[2]	*63*	*63*	*126*
Zhang et al.'s scheme[15]	*124*	*41*	*165*
Farash's scheme[16]	*124*	*62*	*186*
Zhao's scheme[14]	*126*	*84*	*210*
Chen et al.'s scheme[13]	*189*	*42*	*231*

Table 2.Comparison of Communication Cost

have identified earlier with the exception of Zhao's scheme [14], Zhang and Qi's scheme [15] and Farash's scheme [16] which satisfy all seven security requirements.

CONCLUSION

RFID authentication is one of the most critical security services for IoT implementations. We have presented an in-depth survey of recently proposed ECC-based RFID authentication schemes. We identified some of the security requirements that an RFID authentication scheme should satisfy. We have conducted an analysis of the communication costs associated with past proposed ECC-based RFID schemes, which meet some or all of these requirements. We found that only three recently proposed ECC-based RFID authentication schemes are able to satisfy all the security

requirements. With recent advances in modern cryptography, it is well known that we must be able to prove that a cryptographic scheme is provably secure using a security model. However, none of the ECC-based RFID schemes reviewed in this work proposed a suitable security model for RFID systems to demonstrate that these proposed schemes are provably secure. Most of them are still vulnerable to different types of malicious attacks. To ensure secure communication (using ECC-based techniques) in

Scheme	SR1	SR2	SR3	SR4	SR5	SR6	SR7
Lee et al.'s scheme[1]	NO	YES	YES	YES	NO	YES	NO
Sandhya et al.'s scheme[11]	YES	YES	YES	NO	NO	YES	NO
Martinez et al.'s scheme[12]	YES	YES	YES	YES	NO	YES	YES
Godor et al.'s scheme[2]	NO	YES	YES	YES	YES	YES	YES
Wang et al.'s scheme[3]	NO	YES	YES	YES	YES	NO	NO
Zhao's scheme[14]	YES	YES	YES	YES	YES	YES	YES
Zhang et al.'s scheme[15]	YES	YES	YES	YES	YES	YES	YES
Farash's scheme[16]	YES	YES	YES	YES	YES	YES	YES

Table 3.Comparison of Security Requirements

RFID system, it is necessary to construct a suitable security model for ECC-based RFID schemes first. Then, we need to design ECC-based RFID authentication schemes, which are provably secure in the security model.

REFERENCES

[1] 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.
[2] 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, pp. 386–393.
[3] S. Wang, S. Liu, and D. Chen, "Analysis and construction of efficient RFID authentication protocol with backward privacy," in Advances in Wireless Sensor Networks. Berlin, Germany: Springer-Verlag, 2014, pp. 458–466.
[4] whatis.com
[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.
[6] 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.
[7] M. Hutter, M. Feldhofer, and T. Plos, "An ECDSA processor for RFID authentication," in Proc. Radio Freq. Identif. Secur. Privacy Issues,2010, pp. 189–202.
[8] S. Chatterjee, A. K. Das, and J. K. Sing, "An enhanced access control scheme in wireless sensor networks," Ad Hoc Sens. Wireless Netw., vol. 21, no. 1–2, pp. 121–149, 2014.
[9] Y. Lee, L. Batina, and I. Verbauwhede, "Untraceable RFID authentication protocols: Revision of EC-RAC," in Proc. IEEE Int. Conf. RFID, 2009, pp. 178–185.
[10] Y. Lee, L. Batina, D. Singelee, and I. Verbauwhede, "Low-cost untraceable authentication protocols for RFID," in Proc. 3rd ACM Conf. Wireless Netw. Secur. (WiSec'10), 2010, pp. 55–64.
[11] M. Sandhya and T. Rangaswamy, "A combined approach of elliptic curve and zero knowledge based forward secure protocol," World Acad. Sci. Eng. Technol., vol. 56, pp. 847–852, 2009.
[12] S. Martinez, M. Valls, and C. Roig, "A secure elliptic curve-based RFID protocol," J. Comput. Sci. Technol., vol. 24, no. 2, pp. 309–318, 2009.
[13] Y. Chen, J. Chou, and C. Lin, "A novel RFID authentication protocol based on elliptic curve cryptosystem," Cryptology ePrint Archive, Report, 2011/381, 2011

[14] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," J. Med. Syst., vol. 38, no. 5,2014, doi: 10.1007/s10916-014-0046-9.
[15] Z. Zhang and Q. Qi, "An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography,"J. Med. Syst., vol. 38, no. 5, 2014, doi: 10.1007/s10916-014-0047-8.
[16] M. Farash, "Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography," J. Supercomput., 2014, doi: 10.1007/s11227-014-1272–0.