An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography

Debiao He and Sherali Zeadally

***Abstract*—Advances in information and communication technologies have led to the emergence of Internet of Things (IoT). In the healthcare environment, the use of IoT technologies brings convenience to physicians and patients as they can be applied to various medical areas (such as constant real-time monitoring, patient information management, medical emergency management, blood information management, and health management). The radio-frequency identification (RFID) technology is one of the core technologies of IoT deployments in the healthcare environment. To satisfy the various security requirements of RFID technology in IoT, many RFID authentication schemes have been proposed in the past decade. Recently, elliptic curve cryptography (ECC)-based RFID authentication schemes have attracted a lot of attention and have been used in the healthcare environment. In this paper, we discuss the security requirements of RFID authentication schemes, and in particular, we present a review of ECC-based RFID authentication schemes in terms of performance and security. Although most of them cannot satisfy all security requirements and have satisfactory performance, we found that there are three recently proposed ECC-based authentication schemes suitable for the healthcare environment in terms of their performance and security.**

***Index Terms*—Authentication, elliptic curve cryptography (ECC), Internet of Things (IoT), performance, radio-frequency identification (RFID), security.**

I. Introduction

THE LAST few decades have witnessed a steady increase in life expectancy in many parts of the world leading to a sharp rise in the number of elderly people. A recent report from the United Nations [1] predicted that there will be 2 billion (22% of the world population) older people by 2050. In addition, research indicates that about 89% of elderly people are likely to live independently. However, medical research surveys found that about 80% of elderly people older than 65 suffer from at least one chronic disease [2] causing many elderly people to have difficulty in taking care of themselves. Providing a decent quality of life for elderly people has become a serious social challenge at the moment. The rapid proliferation of information and communication technologies is enabling innovative healthcare solutions and tools that show promise in addressing the aforementioned challenge.

Internet of Things (IoT) has emerged as one of the most powerful communication paradigms of the 21st century. 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 [3]. 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, etc. [4]. In the healthcare area, IoT involves many kinds of cheap sensors (wearable, implanted, and environmental) that enable elderly people to enjoy medical healthcare anywhere, any time. They not only bring convenience to medical workers but also improve elderly people's quality of life greatly.

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 [2]. RFID technology was first used in the Identify Friend or Foe (IFF) aircraft system during World War II. 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 [5]. In the healthcare environment, RFID technology is being used within IoT and common applications including location tracking of medical assets [4], [5], newborn and patient identification [6], medical treatment tracking and validation [7], patient location and procedure management at a wellness center [8], and surgical process management [9]. Fig. 1 demonstrates a typical healthcare system using RFID technology [9]. The system could provide the above services and all of doctors, nurses, and patients could benefit from it.

Manuscript received July 07, 2014; revised September 14, 2014; accepted September 19, 2014. Date of publication September 23, 2014; date of current version February 04, 2015. This work was supported by the National Natural Science Foundation of China (NSFC) under Grant 61370224 and Grant 61472074.

D. He is with the School of Mathematics and Statistics, Wuhan University, Wuhan, 430072, China (e-mail: hedebiao@163.com).

S. Zeadally is with the College of Communication and Information, University of Kentucky, Lexington, KY 40506 USA (e-mail: szeadally@uky.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JIOT.2014.2360121

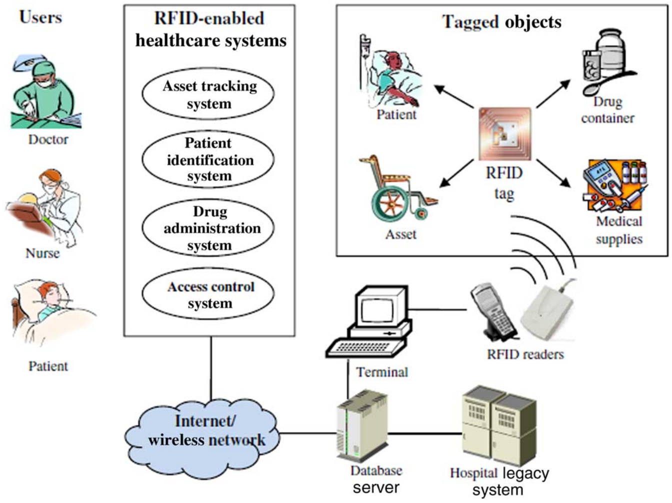

Fig. 1. Typical RFID-based healthcare system [9].

The rapid deployment of RFID technologies in the healthcare environment also means that we need to ensure the reliable and secure access and management of sensitive healthcare information as it is delivered over RFID systems connected to the IoT infrastructure. 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. In the past decade, many RFID authentication schemes have been proposed for a wide range of applications. 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. Therefore, many NPKC-based RFID authentication schemes, such as NP cyclic redundancy code (CRC) checksum-based schemes [10]–[13], simple bit-wise operations (such as XOR, AND, and OR)-based schemes [14], [15], one-way hash functions-based schemes [16]–[21], and symmetric encryption algorithms-based schemes [22], have been proposed for various practical applications such as goods management, books management, identity verification, public security, road traffic administration, and electronic healthcare. Recently, the authors in [23] demonstrated that the PKC-based RFID authentication schemes are necessary for secure communication in RFID systems because many security attributes cannot be implemented by NPKC-based schemes. With the development of microelectronic technology, some complex PKC algorithms have been directly implemented into RFID chips [24]–[27]. 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 [28] 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. Recent research results [29], [30] have demonstrated that the ECC algorithm with 160 bits key size has the same security level as the RSA algorithm with 1024 bits key size. The ECC algorithms have been implemented on very compact RFID chips. Based on these implementations, many ECC-based RFID authentication schemes [31]–[61] have been proposed for practical applications. In particular, Zhao [59] and Zhang and Qi [60] proposed two efficient ECC-based RFID authentication schemes that can be applied to the healthcare environment. Experimental results show that these ECC-based RFID authentication schemes are suitable for enhancing security in the healthcare environment.

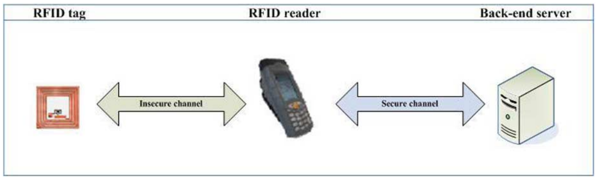

Fig. 2. Architecture for an RFID authentication scheme.

Several papers about surveys of ECC have been published [62]–[64]. However, they only present reviews about past implementations and security of ECC. In this paper, we present an in-depth survey and analysis of recently proposed ECC-based RFID authentication schemes particularly suited for the healthcare environment. We compare their security and performance. We identify approaches (using performance and security criteria) that are most suitable for healthcare applications. Section II presents the overall system architecture and the security requirements of RFID authentication. Section III presents a detailed analysis of recently proposed ECC-based RFID authentication schemes. Section IV presents an analysis of the performance and security of those schemes. Finally, Section V concludes this paper.

II. System Architecture and Security Requirements of RFID Authentication

A. System Architecture

The basic architecture (shown in Fig. 2) 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. RFID tags could be divided into three types: passive tag, semiactive tag, and active tag [65]. The passive tag gets power through wireless signals from the reader. The semiactive tag is equipped with a small battery and gets power from it. The passive and the semiactive tags use

backscatter modulation to send messages. The active tag is equipped with a small battery and a radio transceiver. It can communicate directly with the reader.

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. Usually, 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. Usually, the server's computing capability and memory capacity are high.

B. 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. Previous research efforts on RFID security have identified the following security requirements that must be satisfied to ensure secure RFID communications in addition to a robust and efficient authentication scheme in place [57], [60], [61], [66], [67].

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. In our system architecture, the communication channel between the RFID reader and the server is secure. In this case, only mutual authentication between the RFID tag and the server is required.

2) *Confidentiality*: It is essential that the secret information (such as identity and password) 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. The tag's identity must be encrypted as part of the mutual authentication process.

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. If an adversary destroys the synchronization of the update, the authentication scheme will be invalid.

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. This will seriously violate the owner's privacy.

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.

III. Review of Several Novel ECC-Based RFID Authentication Schemes

Wolkerstorfer [31] introduced the concept of ECC-based RFID authentication scheme in 2005. However, he did not propose any specific authentication scheme. Tuyls and Batina [32] adopted Schnorr's identification protocol [33] and proposed the first ECC-based RFID authentication scheme in 2006. Later, Batina *et al.* [34] adopted Okamoto's identification protocol [35] and proposed another ECC-based RFID authentication scheme in 2007. However, Lee *et al.* [36] pointed out that both Tuyls and Batina's scheme [32] and Batina *et al.*'s scheme [34] cannot provide anonymity. To enhance security and ensure anonymity, Lee *et al.* [36] proposed a provably secure ECC-based RFID authentication scheme. However, Bringer *et al.* [37] found that Lee *et al.*'s scheme cannot withstand tracking attack (the adversary could track the tag's action) and the tag impersonation attack (where the adversary can impersonate the tag to the server). To withstand those two attacks, Bringer *et al.* [37] proposed a new RFID authentication scheme called randomized Schnorr scheme. Later, Lee *et al.* [38] also proposed an ECC-based RFID authentication scheme to withstand the tracking attack and the tag impersonation attack against their previous schemes [36]. However, Deursen and Radomirovi [39] pointed out that all of Lee *et al.*'s schemes [38] cannot withstand the man-in-the-middle attack and the tracking attack. Deursen and Radomirovic [48] pointed out that Lee *et al.*'s schemes were vulnerable to the man-in-the-middle attack. Sandhya and Rangaswamy [40] and Martinez *et al.* [41] proposed two other authentication schemes using the zero-knowledge proof and ECC. Zero-knowledge proof is a method by which one party can prove to another party that a given statement is true, without conveying any information apart from the fact that the statement is indeed true. Later, Lv *et al.* [42] pointed out that Martinez *et al.*'s scheme is vulnerable to the tracking attack.

To overcome weaknesses in their previous schemes, Lee *et al.* [43] proposed three improved ECC-based RFID schemes. Later, Fan *et al.* [44] pointed out that all the three schemes [43] were not secure against man-in-the-middle attack. Subsequently, Lee *et al.* [45] analyze the privacy challenges in RFID systems and proposed three ECC-based RFID authentication schemes to withstand Fan *et al.*'s attacks. Lv *et al.* [46] also pointed out that Lee *et al.*'s three authentication schemes [45] were vulnerable to impersonation attacks and proposed countermeasures to enhance its security. Later, Lee *et al.* [47] analyzed the risk of tracking attacks in RFID systems and proposed two ECC-based RFID authentication schemes to offer privacy protection. Unfortunately, Deursen and Radomirovic [48] pointed out that Lee *et al.*'s schemes [47] were still vulnerable to the man-in-the-middle attack.

Based on Lee *et al.*'s schemes [36], [38], Zhang *et al.* [49] proposed two improved ECC-based RFID authentication schemes to withstand attacks against those two schemes. However, Babaheidarian *et al.* [50] found that Zhang *et al.*'s schemes [49] were vulnerable to the impersonation attack. Later, Godor and Imre [51] proposed a new ECC-based RFID authentication scheme based on ElGamal's algorithm. Chen *et al.* [52] also proposed a new ECC-based RFID authentication scheme. However, Chen *et al.*'s scheme is vulnerable to the replay attack. Later, Batina *et al.* [53] proposed the hierarchical ECC-based RFID authentication. In their scheme, an RFID tag can tune its identification process to the type of reader it is communicating with and only a subset of readers can learn the identity of a particular tag, while others can only acquire information on the group to which the tag belongs [53]. However, the RFID authentication scheme of Batina *et al.* is vulnerable to the server impersonation attack. To achieve backward privacy (where backward privacy means that the adversary cannot track the tag's previous action when the adversary gets the secret information stored in it), Wang *et al.* [54] also proposed a new ECC-based RFID authentication scheme.

To improve performance, Liu *et al.* [55] proposed an efficient ECC-based RFID authentication. However, the computational cost of their scheme is high. Later, Liao and Hsiao [56], [57] proposed a new efficient ECC-based RFID authentication. However, Zhao *et al.* [58] pointed out that Liao and Hsiao's scheme suffered from the key compromise problem, i.e., the adversary could get secret information stored in the tag. Zhao [58] also proposed an improved scheme to overcome such a weakness. Chou [59] proposed an ECC-based RFID authentication scheme using ECC and a one-way hash function. Unfortunately, Zhang and Qi [60] pointed out that Chou's scheme suffers from the key compromise problem, where key compromise means that the adversary could get the secret information stored in the tag. They also proposed an improved scheme to solve the key compromise problem in Chou's scheme [59]. Farash [61] also pointed out that Chou's scheme was vulnerable to the impersonation attack and proposed an improved scheme to withstand such attacks.

As described earlier, several ECC-based RFID authentication schemes have been proposed for different applications recently. Some of these schemes use only elliptic curve operations. In contrast, other schemes involve additional cryptographic operations such as hash function operations and public-key cryptography operations. Due to several constraints, such as tag cost, gate area, and power consumption, the smaller the number of operations involved the better the scheme is.

TABLE I
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 $X_i = x_i P, i = 1,2$
$h(\cdot)$	Secure hash function mapping $\{0,1\}^*$ to Z_n

To support the execution of more operations, an increase in the tag cost, gate area, and power consumption is incurred. 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 [51], [52], [54] often involve very complex operations such as public-key encryption operations and digital signature operations. For the middleweight schemes [55], [59]–[61], both elliptic curve operations and hash function operations are needed. Finally, for lightweight schemes [36]–[38], [40], [41], [43], [45], [47], [49], [53], [56]–[58], 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.

A. Heavyweight Schemes

Godor and Imre [51] 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 $\mathrm{params} = \{F(q), E(F(q)), n, P, Y\}$ and stores (M, X_1) and (x_1, 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 σ_S of the random number r_R generated by the reader and sends the message $\{r_R, \sigma_S\}$ to the tag through the reader.

Step 2) Tag → Server: After the tag receives the message $\{r_R, \sigma_S\}$, 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 r_T and computes $T = r_T P$, $M' = M \oplus x(r_T Y)$, and a signature σ_T, where M is the message about tag's identity and $x(r_T Y)$ denotes the x-coordinate of the point $r_T Y$. 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 X_1 according to M. If no tuple (M, X_1) exists in its database, the server terminates the session; otherwise, the server uses X_1 to check the validity of the signature σ_T. 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 II. 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 $\{r_R, \sigma_S\}$. Therefore, their scheme is not suitable for practical applications.

Liu *et al.* [54] also proposed an ECC-based RFID authentication by using ElGamal scheme. Compared to Godor and Imre's scheme, Liu *et al.*'s scheme has better performance because the ECDSA is not used in it. In the initialization phase, the server generates the system parameters $\mathrm{params} = \{F(q), E(F(q)), n, P\}$, stores (id, X_1) and (id, x_1, X_1) in its database and the tag's memory separately, where id is the tag's unique identity.

Step 1) Tag $\rightarrow$ Server: The tag sends its identity id to the server.

Step 2) Server $\rightarrow$ Tag: After receiving the tag's identity id, the server looks up its database for the tuple (id, X_1). If there is no such tuple, the server aborts the session; otherwise, the server generates three random numbers n_1, n_2, n_3 and computes $(c_1, c_2) = n_3 X_1$, $\gamma_1 = c_1 n_1$, $\gamma_2 = c_2 n_2$, $\gamma_3 = n_3 P$, and $A = (id + n_1 + n_2) \oplus X_1$. Then, the server sends the message $\{\gamma_1, \gamma_2, \gamma_3, A\}$ to the tag.

Step 3) Tag $\rightarrow$ Server: Upon receiving the message $\{\gamma_1, \gamma_2, \gamma_3, A\}$, the tag computes $(c_1, c_2) = x_1 \gamma_3$, $n_1 = c_1^{-1} \gamma_1$, and $n_2 = c_2^{-1} \gamma_2$ and checks whether the equation $A = (id + n_1 + n_2) \oplus X_1$ holds. If it does not hold, the tag rejects the session; otherwise, the tag computes $B = (n_1 \oplus n_2) + id$ and sends the message $\{B\}$ to the back-end server.

Step 4) Server: Upon receiving $\{B\}$, the back-end server checks whether the equation $B = (n_1 \oplus n_2) + id$ holds. If it does not hold, the back-end server rejects the session; otherwise, the tag is authenticated.

In Liu *et al.*'s scheme, the tag's identity is transmitted in plaintext format. Their scheme cannot provide anonymity, and the adversary can track the tag's action by observing its identity. Therefore, their scheme cannot withstand the tracing attack. Besides, several complex modular inversion operations are needed in their scheme leading to low performance. As a result, the scheme is not suitable for practical applications and it cannot be applied to cheap RFID tags.

B. 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.* [55] 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 $\mathrm{params} = \{F(q), E(F(q)), n, P, Y\}$ and stores (X_1) and (x_1, 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 $\rightarrow$ Server: The tag generates a random number r_1, computes $T_1 = r_1 P$, and sends the message $\{T_1\}$ to the server.

Step 2) Server $\rightarrow$ Tag: Upon receiving $\{T_1\}$, the server generates a random number r_s and sends it to the tag.

Step 3) Tag $\rightarrow$ Server: Upon receiving $\{r_s\}$, the tag computes $T_2 = r_1 Y$, $v = r_1 + x_1 h(T_2, r_s)$ and sends the message $\{v\}$ to the server.

Step 4) Server: Upon receiving $\{v\}$, the server checks whether there is a tuple (X_1) such that the equation $vP = T_1 + h(yT_1, r_s) X_1$ 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 back-end server because it receives only a random number sent by the back-end server. Therefore, Zhang *et al.*'s schemes cannot provide mutual authentication.

Chou [59] proposed a new ECC-based RFID scheme using hash function operations to overcome the problems in Wang *et al.*'s scheme. In the initialization phase, the server generates the system parameters $\mathrm{params} = \{F(q), E(F(q)), n, P, Y\}$ and stores (X_1) and (X_1, Y) in its database and the tag's memory.

Step 1) Server $\rightarrow$ Tag: The server selects a random number r_s, computes $T_s = r_s Y$ and sends the message $\{T_{s1}\}$ to the tag.

Step 2) Tag $\rightarrow$ Server: Upon receiving $\{T_{s1}\}$, the tag generates a random number r_t, computes $R_t = r_t P$, $T_{t1} = r_t T_{s1}$, $T_{t2} = X_1 + 2R_t$, and $T_{t3} = h(X_1, R_t)$. The tag then sends the message $\{T_{t1}, T_{t2}, T_{t3}\}$ to the server.

Step 3) Server $\rightarrow$ Tag: Upon receiving $\{T_{t1}, T_{t2}, T_{t3}\}$, the server computes $R_t = y^{-1} r_s^{-1} T_{t1}$, $X_1 = T_{t2} - 2R_t$, and checks whether the equation $T_{t3} = h(X_1, K)$ holds. If it does not hold, the server rejects the session; otherwise, it checks whether X_1 is in its database. If it is not, the server rejects the session;

otherwise, the server computes $T_{s2} = h(X_1, 3R_t)$ and sends the message $\{T_{s2}\}$ to the tag.

Step 4) Tag: Upon receiving $\{T_{s2}\}$, the tag checks whether the equation $T_{s2} = h(X_1, 3R_t)$ holds. If it does not hold, the tag terminates the session; otherwise, the server is authenticated.

Although Chou [59] claimed that their scheme could withstand various attacks, Zhang and Qi [60] pointed out that Chou's scheme is still vulnerable to impersonation attacks and cannot provide forward security. The adversary selects a random number r_A, computes $T_A = r_A Y$ and sends the message $\{T_{A1}\}$ to the tag. Upon receiving $\{T_{A1}\}$, the tag generates a random number r_t, computes $R_t = r_t P$, $T_{t1} = r_t T_{A1}$, $T_{t2} = X_1 + 2R_t$, $T_{t3} = h(X_1, R_t)$, and sends $\{T_{t1}, T_{t2}, T_{t3}\}$ to the adversary. The adversary could get the tag's private information by computing $X_1 = T_{t2} - 2r_A^{-1} T_{t1}$. With the secure information X_1, the adversary could impersonate the tag to the server. Therefore, Chou's scheme is still vulnerable to tag impersonation attacks.

Once the adversary gets the secure information X_1 stored in the tag, the adversary could determine whether the intercepted message $\{T_{t1}, T_{t2}, T_{t3}\}$ was sent by the same tag. The tag computes $R_t = 2^{-1}(T_{t2} - X_1)$ and checks whether the equation $T_{t3} = h(X_1, R_t)$ holds. If it holds, the adversary could confirm that the message $\{T_{t1}, T_{t2}, T_{t3}\}$ was sent by the same tag. Therefore, Chou's scheme cannot provide forward security.

Zhang and Qi [60] also proposed an improved ECC-based RFID authentication scheme using hash function operations to solve security weaknesses in Chou's scheme [59]. In their scheme, public-key encryption is used to enhance security and improve performance. The initialization phase of their scheme is the same as that of Chou's scheme. The various steps of the authentication phase are as follows.

Step 1) Server → Tag: The server selects a random number r_s and sends it to the tag.

Step 2) Tag → Server: Upon receiving r_s, the tag generates a random number r_t, computes $R_{t1} = r_t Y$, $T_{t1} = r_t P$, $T_{t2} = X_1 + R_{t1}$, and $T_{t3} = h(X_1, R_t, r_s, T_{t1}, T_{t2})$. The tag then sends $\{T_{t1}, T_{t2}, T_{t3}\}$ to the server.

Step 3) Server → Tag: Upon receiving $\{T_{t1}, T_{t2}, T_{t3}\}$, the server computes $R_t = yT_{t1}$, $X_1 = T_{t2} - R_t$, and checks whether the equation $T_{t3} = h(X_1, R_{t1}, r_s, T_{t1}, T_{t2})$ holds. If it does not hold, the server rejects the session; otherwise, it checks whether X_1 is in its database. If it is not in its database, the server rejects the session; otherwise, the server computes $T_{s2} = h(X_1, R_{t1}, r_s, T_{t1}, T_{t2}, T_{t3})$ and sends the message $\{T_{s2}\}$ to the tag.

Step 4) Tag: Upon receiving $\{T_{s2}\}$, the tag checks whether the equation $T_{s2} = h(X_1, R_{t1}, r_s, T_{t1}, T_{t2}, T_{t3})$ holds. If it does not hold, the tag terminates the session; otherwise, the server is authenticated.

In Zhang and Qi's scheme, the server's public key Y is used to protect the tag's secret information X_1 by computing $T_{t2} = X_1 + R_{t1}$, where $R_{t1} = r_t Y$, $T_{t1} = r_t P$, and $T_{t3} = h(X_1, R_{t1}, r_s, T_{t1}, T_{t2})$. Upon receiving the message $\{T_{t1}, T_{t2}, T_{t3}\}$, the adversary has to compute $R_{t1} = r_t yP$ from $T_{t1} = r_t P$ and $Y = yP$ to get X_1. Then, the adversary has to solve the elliptic curve Diffie–Hellman problem. Therefore, Zhang and Qi's scheme could withstand the impersonation attack possible in Chou's scheme.

Suppose the adversary could extract the secret information X_1 stored in the tag and intercept the message $\{r_s\}$, $\{T_{t1}, T_{t2}, T_{t3}\}$, and $\{T_{s2}\}$ transmitted between the server and the tag, where $R_{t1} = r_t Y$, $T_{t1} = r_t P$, $T_{t2} = X_1 + R_{t1}$, $T_{t3} = h(X_1, R_t, r_s, T_{t1}, T_{t2})$, and $T_{s2} = h(X_1, R_{t1}, r_s, T_{t1}, T_{t2}, T_{t3})$. If the adversary wants to check whether the message is transmitted by the tag, the adversary has to compute $R_{t1} = r_t yP$ from $T_{t1} = r_t P$ and $Y = yP$. Therefore, with Zhang and Qi's scheme, an adversary has to solve the elliptic curve Diffie–Hellman problem and the scheme could provide forward security.

C. 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.* [36] proposed an ECC-based RFID authentication scheme that requires only elliptic curve operations. In the initialization phase, the server generates system parameters $\mathrm{params} = \{F(q), E(F(q)), n, P, Y\}$ and stores (x_1, X_1, X_2) and (x_1, x_2, 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 r_s and sends the message $\{r_s\}$ to the tag.

Step 2) Tag → Server: Upon receiving the tag, the tag generates a random number r_t and computes $T_1 = r_t P$, $T_2 = (r_s + x_1)P$, and $v = r_t x_1 + r_s x_2$. Then, the tag sends the message $\{T_1, T_2, v\}$ to the server.

Step 3) Server: Upon receiving the message M_1, the server computes $x_1 P = y^{-1} T_2 - T_1$ and performs a lookup in its database for the tuple (x_1, X_1, X_2). Then, the server checks whether the equation $r_s^{-1}(vP - x_1 T_1) = X_2$ 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.

Suppose that the adversary could intercept two transcripts T_1^i, T_1^i, v^i sent by the same tag, where $i = 1, 2$. Then, the adversary could compute $x_1^{-1}P = (r_s^1 v^2 - r_s^2 v^1)^{-1}(r_s^1 T_1^2 - r_s^2 T_1^1)$. For every tag, the corresponding value $x_1^{-1}P$ is constant because one component x_1 of its secret information is constant. Therefore, the adversary could track the tag by checking $x_1^{-1}P$ and Lee *et al.*'s scheme cannot withstand the tracking attack.

Suppose that the adversary could get three transcripts: r_s^i, T_1^i, T_1^i, v^i for $i = 1, 2, 3$. The adversary computes $A = (r_s^1 v^2 - r_s^2 v^1)$, $B = (r_s^1 v^3 - r_s^3 v^1)$, and $x_1 Y = (Br_s^1 - Br_s^2 + Ar_s^1 - Ar_s^3)(Br_s^1 T_2^2 - Br_s^2 T_2^1 + Ar_s^1 T_2^3 - Ar_s^2 T_2^1)$. Upon receiving the message r_s from the server, the adversary generates a random number β, computes $\lambda = \beta(r_s^1)^{-1}$, $T_1 = T_1^1$, $T_2 = \lambda(T_2^1 - x_1 Y) + x_1 Y$, and $v = \lambda v^1$. At last, the adversary sends the message $\{T_1, T_2, v\}$ to the server. Due to above equations, we can get that the equation $r_s^{-1}(vP - x_1 T_1) = X_2$ holds. Then, the message can pass the server's verification. Therefore, the adversary can successfully impersonate the tag and as a result Lee *et al.*'s scheme cannot withstand the impersonation attack.

We found that the tag in Lee *et al.*'s scheme cannot authenticate the server because the server just sends a random number to it. Therefore, Lee *et al.*'s scheme cannot provide mutual authentication and is vulnerable to the reply attack. After Lee *et al.*'s pioneering work, many lightweight ECC-based RFID authentication schemes [36]–[38], [40], [41], [43], [45], [47], [49], [53] have been proposed to enhance security or improve performance. However, most of them cannot provide mutual authentication and cannot withstand the reply attack.

Liao and Hsiao [56], [57] proposed a lightweight ECC-based RFID scheme to achieve mutual authentication. In the initialization phase, the server generates system parameters $\text{params} = \{F(q), E(F(q)), n, P, Y\}$ and stores (x_1, X_1) and (X_1, Y) in its database and the tag's memory. The following steps are executed between the tag and the server to achieve mutual authentication between them.

Step 1) $\text{Server} \rightarrow \text{Tag}$: The server generates a random number r_s, computes $T_s = r_s P$, and sends the message $\{T_s\}$ to the tag.

Step 2) $\text{Tag} \rightarrow \text{Server}$: Upon receiving $\{T_s\}$, the tag generates a random number r_t and computes $R_t = r_t P$. The tag also computes $T_{t1} = r_t T_s$, $T_{t2} = r_t Y$, and $\text{Auth}_t = X_1 + T_{t1} + T_{t2}$. Then the tag sends the message $\{\text{Auth}_t, R_t\}$ to the server.

Step 3) $\text{Server} \rightarrow \text{Tag}$: Upon receiving $\{\text{Auth}_t, R_t\}$, the server computes $T_{s1} = r_s R_t$, $T_{t1} = yR_t$, and $X_1 = \text{Auth}_t - T_{t1} - T_{t2}$. The server checks whether X_1 is in its database. If it is not, the server rejects the session; otherwise, the server finds the corresponding x_1, computes $\text{Auth}_S = x_1 R_t + r_S X_1$ and sends the message $\{\text{Auth}_S\}$ to the tag.

Step 4) Tag: Upon receiving $\{\text{Auth}_S\}$, the tag checks whether the equation $\text{Auth}_S = r_x X_1 + x_1 T_s$ holds. If it does not hold, the tag terminates the session; otherwise, the server is authenticated.

Although Liao and Hsiao claimed that their scheme could withstand various attacks, Zhao [59] pointed out that their scheme cannot withstand the impersonation attack because the adversary could get the tag's secret information through the following steps. First, the adversary generates a random number r_s, computes $T_s = r_s P - Y$ and sends the message $\{T_s\}$ to the tag. Upon receiving $\{T_s\}$, the tag generates a random number r_t and computes $R_t = r_t P$. $T_{t1} = r_t T_s = r_t(r_s P - Y)$, $T_{t2} = r_t Y$, and $\text{Auth}_t = X_1 + T_{t1} + T_{t2} = X_1 + r_t r_s P$. Then, the tag sends the message $\{\text{Auth}_t, R_t\}$ to the server. Upon receiving $\{\text{Auth}_t, R_t\}$, the adversary computes $X_1 = \text{Auth}_t + r_s R_t$. After getting the tag's secret information X_1, the adversary could impersonate the tag to the server. Therefore, Chou's scheme is vulnerable to impersonation attacks.

The reason that Liao and Hsiao's scheme cannot withstand the impersonation attack is because the authentication message Auth_t is a linear combination of X_1, T_{t1}, and T_{t2}. To withstand the above attack, we just need to break the linear relation among X_1, T_{t1}, and T_{t2}.

Zhao [59] proposed an improved scheme of Liao *et al.*'s scheme. To achieve such goal, Zhao [59] modifies the computation of T_{t1} and T_{t2}. In Zhao's scheme, the tag computes $T_{t1} = x(R_t) \cdot r_t T_s$ and $T_{t2} = y(R_t) \cdot r_t Y$, where $x(R_t)$ and $y(R_t)$ denote x-coordinate and y-coordinate of R_t, respectively. With such a simple modification, the linear relation among X_1, T_{t1}, and T_{t2} is totally destroyed.

Suppose the adversary generates a random number r_s, computes $T_s = r_s P - Y$ and sends the message $\{T_s\}$ to the tag. Upon receiving $\{T_s\}$, the tag generates a random number r_t and computes $R_t = r_t P$. The tag also computes $T_{t1} = x(R_t) \cdot r_t T_s$, $T_{t2} = y(R_t) \cdot r_t Y$, and $X_1 = \text{Auth}_t - T_{t1} - T_{t2}$. Then the tag sends the message $\{\text{Auth}_t, R_t\}$ to the server. After receiving $\{\text{Auth}_t, R_t\}$, the adversary cannot get the tag's secret information X_1 because the adversary has to solve the elliptic curve Diffie–Hellman problem. Therefore, Zhao *et al.*'s scheme could withstand the impersonation attack that is possible in Liao and Hsiao's scheme [56], [57].

IV. 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 II and comparing their communication and computation 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 computation cost, 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. We also used such an elliptic curve to discuss the computation cost, communication cost, and security requirements of the various schemes, we have selected to review.

A. Analysis of Computation Cost

Let T_{mul}, T_{inv}, T_{eca}, T_{ecm}, and T_h denote the running time of a modular multiplication operation, a modular inversion operation, an elliptic curve point addition operation, an elliptic curve point multiplication operation, and a hash function operation respectively. For fair comparisons of the computational cost,

TABLE II
COMPARISON OF COMPUTATIONAL COST

Scheme	Tag side computational cost	Server side computational cost	Total computational cost
Lee *et al.*'s server proof scheme [38]	$1 T_{ecm} \approx 1200 T_{mul}$	$1 T_{ecm} \approx 1200 T_{mul}$	$2 T_{ecm} \approx 2400 T_{mul}$
Sandhya *et al.*'s scheme [40]	$2 T_{ecm} \approx 2400 T_{mul}$	$1 T_{mul} +1 T_{eca} +1 T_{ecm} \approx 1206 T_{mul}$	$1 T_{mul} +1 T_{eca} +3 T_{ecm} \approx 3606 T_{mul}$
Liu *et al.*'s scheme [54]	$3 T_{mul} +2 T_{inv} +1 T_{ecm} \approx 1212 T_{mul}$	$2 T_{mul} +2 T_{ecm} \approx 2402 T_{mul}$	$5 T_{mul} +2 T_{inv} +3 T_{ecm} \approx 3614 T_{mul}$
Zhang *et al.*'s Improved Schnorr scheme [48]	$1 T_{mul} +1 T_{ecm} \approx 1201 T_{mul}$	$3 T_{ecm} \approx 3600 T_{mul}$	$1 T_{mul} +4 T_{ecm} \approx 4801 T_{mul}$
Wang *et al.*'s scheme [55]	$2 T_{mul} +2 T_{ecm} +1 T_{h} \approx 2402 T_{mul}$	$1 T_{eca} +2 T_{ecm} +1 T_{h} \approx 2402 T_{mul}$	$2 T_{mul} +1 T_{eca} +4 T_{ecm} +2 T_{h} \approx 4804 T_{mul}$
Lee *et al.*'s EC-RAC1 scheme [45]	$1 T_{mul} +2 T_{ecm} \approx 2401 T_{mul}$	$2 T_{inv} +1 T_{eca} +2 T_{ecm} \approx 2411 T_{mul}$	$1 T_{mul} +2 T_{inv} +1 T_{eca} +4 T_{ecm} \approx 4812 T_{mul}$
Chou's scheme [58]	$3 T_{mul} +2 T_{ecm} +2 T_{h} \approx 2404 T_{mul}$	$1 T_{mul} +2 T_{inv} +2 T_{ecm} +2 T_{h} \approx 2408 T_{mul}$	$4 T_{mul} +2 T_{inv} +4 T_{ecm} +4 T_{h} \approx 4812 T_{mul}$
Farash's scheme [61]	$3 T_{mul} +2 T_{ecm} +2 T_{h} \approx 2404 T_{mul}$	$1 T_{mul} +2 T_{inv} +2 T_{ecm} +2 T_{h} \approx 2408 T_{mul}$	$4 T_{mul} +2 T_{inv} +4 T_{ecm} +4 T_{h} \approx 4812 T_{mul}$
Lee *et al.*'s tag password transfer scheme [38]	$2 T_{mul} +2 T_{ecm} \approx 2402 T_{mul}$	$2 T_{inv} +1 T_{eca} +2 T_{ecm} \approx 2411 T_{mul}$	$2 T_{mul} +2 T_{inv} +1 T_{eca} +4 T_{ecm} \approx 4813 T_{mul}$
Lee *et al.*'s tag identity transfer scheme [38]	$2 T_{mul} +2 T_{ecm} \approx 2402 T_{mul}$	$2 T_{inv} +1 T_{eca} +2 T_{ecm} \approx 2411 T_{mul}$	$2 T_{mul} +2 T_{inv} +1 T_{eca} +4 T_{ecm} \approx 4813 T_{mul}$
Zhang and Qi's scheme [60]	$1 T_{eca} +2 T_{ecm} +2 T_{h} \approx 2406 T_{mul}$	$1 T_{eca} +2 T_{ecm} +2 T_{h} \approx 2406 T_{mul}$	$2 T_{eca} +4 T_{ecm} +4 T_{h} \approx 4816 T_{mul}$
Martinez *et al.*'s scheme [41]	$3 T_{ecm} \approx 3600 T_{mul}$	$1 T_{mul} +2 T_{ecm} \approx 2401 T_{mul}$	$1 T_{mul} +5 T_{ecm} \approx 6001 T_{mul}$
Bringer *et al.*'s scheme [37]	$1 T_{mul} +2 T_{ecm} \approx 2401 T_{mul}$	$2 T_{inv} +2 T_{eca} +3 T_{ecm} \approx 3616 T_{mul}$	$1 T_{mul}\ 2 T_{inv} +2 T_{eca} +5 T_{ecm} \approx 6017 T_{mul}$
Lee *et al.*'s tag password transfer scheme [47]	$2 T_{mul} +2 T_{ecm} \approx 2402 T_{mul}$	$1 T_{mul} +3 T_{inv} +1 T_{eca} +3 T_{ecm} \approx 3615 T_{mul}$	$3 T_{mul} +3 T_{inv} +1 T_{eca} +5 T_{ecm} \approx 6017 T_{mul}$
Lee *et al.*'s tag identity transfer scheme [43]	$1 T_{mul} +3 T_{ecm} \approx 3601 T_{mul}$	$2 T_{inv} +1 T_{eca} +3 T_{ecm} \approx 3611 T_{mul}$	$1 T_{mul} +2 T_{inv} +1 T_{eca} +6 T_{ecm} \approx 7212 T_{mul}$
Lee *et al.*'s tag password transfer scheme [43]	$1 T_{mul} +3 T_{ecm} \approx 3601 T_{mul}$	$2 T_{inv} +1 T_{eca} +3 T_{ecm} \approx 3611 T_{mul}$	$1 T_{mul} +2 T_{inv} +1 T_{eca} +6 T_{ecm} \approx 7212 T_{mul}$
Lee *et al.*'s scheme [36]	$2 T_{mul} +2 T_{ecm} \approx 2402 T_{mul}$	$2 T_{inv} +1 T_{eca} +4 T_{ecm} \approx 4811 T_{mul}$	$2 T_{mul}\ 2 T_{inv} +1 T_{eca} +6 T_{ecm} \approx 7213 T_{mul}$
Chen *et al.*'s scheme [52]	$2 T_{mul} +2 T_{inv} +1 T_{eca} +4 T_{ecm} +5 T_{h} \approx 4815 T_{mul}$	$2 T_{inv} +1 T_{eca} +2 T_{ecm} +3 T_{h} \approx 2412 T_{mul}$	$2 T_{mul} +4 T_{inv} +2 T_{eca} +6 T_{ecm} +8 T_{h} \approx 7227 T_{mul}$
Lee *et al.*'s EC-RAC2 scheme [45]	$3 T_{mul} +3 T_{ecm} \approx 3603 T_{mul}$	$4 T_{inv} +2 T_{eca} +5 T_{ecm} \approx 6022 T_{mul}$	$3 T_{mul} +4 T_{inv} +2 T_{eca} +8 T_{ecm} \approx 9605 T_{mul}$
Zhang *et al.*'s Improved EC-RAC scheme [48]	$2 T_{mul} +2 T_{ecm} \approx 2402 T_{mul}$	$2 T_{inv} +2 T_{eca} +6 T_{ecm} \approx 7216 T_{mul}$	$2 T_{mul} +2 T_{inv} +2 T_{eca} +8 T_{ecm} \approx 9618 T_{mul}$
Lee *et al.*'s EC-RAC3 scheme [45]	$3 T_{mul} +4 T_{ecm} \approx 4803 T_{mul}$	$4 T_{inv} +2 T_{eca} +5 T_{ecm} \approx 6022 T_{mul}$	$3 T_{mul} +4 T_{inv} +2 T_{eca} +9 T_{ecm} \approx 10825 T_{mul}$
Lee *et al.*'s tag identity and password transfer scheme [47]	$3 T_{mul} +4 T_{ecm}$	$1 T_{mul} +4 T_{inv} +2 T_{eca}$	$4 T_{mul} +4 T_{inv} +2 T_{eca}$
	$\approx 4804 T_{mul}$	$+5 T_{ecm} \approx 6023 T_{mul}$	$+9 T_{ecm} \approx 10827 T_{mul}$
Godor and Imre's scheme [51]	$2 T_{mul} +5 T_{ecm} \approx 6002 T_{mul}$	$2 T_{mul} +5 T_{ecm} \approx 6002 T_{mul}$	$4 T_{mul} +10 T_{ecm} \approx 12004 T_{mul}$
Batina *et al.* [53]	$1 T_{mul} +3 T_{ecm} \approx 3601 T_{mul}$	$2 T_{inv} +3 T_{eca} +7 T_{ecm} \approx 8421 T_{mul}$	$1 T_{mul} +2 T_{inv} +3 T_{eca} +10 T_{ecm} \approx 12022 T_{mul}$
Liao *et al.*'s scheme [56], [57]	$3 T_{eca} +5 T_{ecm} \approx 6015 T_{mul}$	$3 T_{eca} +5 T_{ecm} \approx 6015 T_{mul}$	$6 T_{eca} +10 T_{ecm} \approx 12023 T_{mul}$
Zhao's scheme [59]	$2 T_{mul} +3 T_{eca} +5 T_{ecm} \approx 6017 T_{mul}$	$2 T_{mul} +3 T_{eca} +5 T_{ecm} \approx 6017 T_{mul}$	$4 T_{mul} +6 T_{eca} +10 T_{ecm} \approx 12034 T_{mul}$
Lee *et al.*'s tag identity and password transfer scheme [43]	$4 T_{mul} +4 T_{ecm} \approx 4804 T_{mul}$	$1 T_{mul} +4 T_{inv} +2 T_{eca} +6 T_{ecm} \approx 7223 T_{mul}$	$5 T_{mul} +4 T_{inv} +2 T_{eca} +10 T_{ecm} \approx 12037 T_{mul}$

TABLE III
COMPARISON OF COMMUNICATION COST

Scheme	From tag to server	From server to tag	Total communication cost
Sandhya *et al.*'s scheme [40]	25	42	67
Martinez *et al.*'s scheme [41]	25	42	67
Lee *et al.*'s server proof scheme [38]	42	42	84
Wang *et al.*'s scheme [55]	63	21	84
Lee *et al.*'s tag identity transfer scheme [38]	84	21	105
Lee *et al.*'s tag password transfer scheme [38]	84	21	105
Lee *et al.*'s tag identity transfer scheme [43]	84	21	105
Lee *et al.*'s tag password transfer scheme [43]	84	21	105
Lee *et al.*'s EC-RAC1 scheme [45]	84	21	105
Lee *et al.*'s tag password transfer scheme [47]	84	21	105
Lee *et al.*'s scheme [36]	21	105	126
Bringer *et al.*'s scheme [37]	105	21	126
Zhang *et al.*'s Improved Schnorr scheme [48]	84	21	126
Godor and Imre's scheme [51]	63	63	126
Lee *et al.*'s EC-RAC2 scheme [45]	126	21	147
Zhang *et al.*'s Improved EC-RAC scheme [48]	126	21	147
Liu *et al.*'s scheme [54]	29	126	155
Zhang and Qi's scheme [60]	124	41	165
Batina *et al.* [53]	147	21	168
Chou's scheme [58]	124	62	186
Farash's scheme [61]	124	62	186
Lee *et al.*'s tag identity & password transfer scheme [43]	168	21	189
Lee *et al.*'s EC-RAC3 scheme [45]	168	21	189
Lee *et al.*'s tag identity & password transfer scheme [47]	168	21	189
Liao *et al.*'s scheme [56], [57]	126	84	210
Zhao's scheme [59]	126	84	210
Chen *et al.*'s scheme [52]	189	42	231

TABLE IV
COMPARISON OF SECURITY REQUIREMENTS

Scheme	SR1	SR2	SR3	SR4	SR5	SR6	SR7
Lee *et al.*'s scheme [36]	No	Yes	Yes	Yes	No	Yes	No
Bringer *et al.*'s scheme [37]	No	Yes	Yes	Yes	No	Yes	No
Lee *et al.*'s tag identity transfer scheme [38]	No	Yes	Yes	Yes	No	Yes	No
Lee *et al.*'s tag password transfer scheme [38]	No	Yes	Yes	Yes	No	Yes	No
Lee *et al.*'s server proof scheme [38]	No	Yes	Yes	Yes	No	Yes	No
Sandhya *et al.*'s scheme [40]	Yes	Yes	Yes	No	No	Yes	No
Martinez *et al.*'s scheme [41]	Yes	Yes	Yes	Yes	No	Yes	Yes
Lee *et al.*'s tag identity transfer scheme [43]	No	Yes	Yes	Yes	Yes	Yes	No
Lee *et al.*'s tag password transfer scheme [43]	No	Yes	Yes	Yes	Yes	Yes	No
Lee *et al.*'s tag identity & password transfer scheme [43]	No	Yes	Yes	Yes	Yes	Yes	No
Lee *et al.*'s EC-RAC1 scheme [45]	No	Yes	Yes	Yes	Yes	Yes	No
Lee *et al.*'s EC-RAC2 scheme [45]	No	Yes	Yes	Yes	Yes	Yes	No
Lee *et al.*'s EC-RAC3 scheme [45]	No	Yes	Yes	Yes	Yes	Yes	No
Lee *et al.*'s tag password transfer scheme [47]	No	Yes	Yes	Yes	Yes	Yes	No
Lee *et al.*'s tag identity & password transfer scheme [47]	No	Yes	Yes	Yes	Yes	Yes	No
Zhang *et al.*'s Improved EC-RAC scheme [48]	Yes	Yes	Yes	Yes	Yes	Yes	No
Zhang *et al.*'s Improved Schnorr scheme [48]	No	Yes	Yes	Yes	Yes	Yes	No
Godor and Imre's scheme [51]	No	Yes	Yes	Yes	Yes	Yes	Yes
Chen *et al.*'s scheme [52]	No	Yes	Yes	Yes	Yes	Yes	No
Batina *et al.* [53]	No	Yes	Yes	Yes	Yes	Yes	No
Liu *et al.*'s scheme [54]	Yes	Yes	No	Yes	Yes	Yes	No
Wang *et al.*'s scheme [55]	No	Yes	Yes	Yes	Yes	No	No
Liao *et al.*'s scheme [56], [57]	No	Yes	Yes	Yes	Yes	Yes	No
Chou's scheme [58]	No	Yes	Yes	Yes	Yes	Yes	No
Zhao's scheme [59]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Zhang and Qi's scheme [60]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Farash's scheme [61]	Yes	Yes	Yes	Yes	Yes	Yes	Yes

the running time of different operations are measured according to that of a modular multiplication operation. According to Chatterjee *et al.*'s work [68], we have $T_{\mathrm{inv}} \approx 3T_{\mathrm{mul}}$, $T_{\mathrm{eca}} \approx 5T_{\mathrm{mul}}$, $T_{\mathrm{ecm}} \approx 1200T_{\mathrm{mul}}$, and $T_h \approx 0.36T_{\mathrm{mul}}$.

The detailed computation cost comparisons of related ECC-based RFID authentication schemes are given in Table II. From the results shown in the table, we found that the computation cost on both the tag side and server side of Lee *et al.*'s server proof scheme [38] is the lowest. Furthermore, the total computation cost of Lee *et al.*'s tag identity and password transfer scheme [43] is the highest.

B. 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 III 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 [40] and Martinez *et al.*'s scheme [41] are the least. Besides, the communication cost of Chen *et al.*'s scheme [52] is the highest.

C. 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 IV.

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 have identified earlier with the exception of Zhao's scheme [59], Zhang and Qi's scheme [60] and Farash's scheme [61] which satisfy all seven security requirements.

V. Conclusion

RFID authentication is one of the most critical security services for IoT implementations in the healthcare environment. 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 computation and 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 [59]–[61] are able to satisfy all the security requirements. We have identified and they have acceptable computation and communication costs making them suitable for use in IoT applications deployed in the healthcare environment.

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 an 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.

Acknowledgment

The authors are grateful to the anonymous reviewers for their valuable comments, which helped us to improve the quality and presentation of this paper.

References

[1] UN, "World Population Aging 2013," 2013, pp. 8–10.
[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] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.
[4] P. Najera, J. Lopez, and R. Roman, "Real-time location and inpatient care systems based on passive RFID," *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 980–989, 2011.
[5] D. Ranasinghe, Q. Sheng, and S. Zeadally, *Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks.* New York, NY, USA: Springer, 2010.
[6] Y. Hung, "The study of adopting RFID technology in medical institute with the perspectives of cost benefit," Ph.D. dissertation, Dept. Comput. Sci. Inform. Eng., Fu Jen Catholic Univ., New Taipei City, Taiwan, 2011.
[7] J. Katz and R. Rice, "Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology," *Int. J. Med. Informat.*, vol. 78, no. 2, pp. 104–114, 2009.
[8] J. Leu, "The benefit analysis of RFID use in the health management center—The experience in Shin Kong Wu Ho-Su Memorial Hospital," M.A. thesis, College of Management, National Taiwan Univ., Taipei City, Taiwan, 2010.
[9] W. Yao, C. Chu, and Z. Li, "The adoption and implementation of RFID technologies in healthcare: A literature review," *J. Med. Syst.*, vol. 36, no. 6, pp. 3507–3525, 2012.
[10] H. Chien and C. Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," *Comput. Stand. Interfaces*, vol. 29, no. 2, pp. 254–259, 2007.
[11] D. Duc, J. Park, H. Lee, and K. Kim, "Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning," in *Proc. Symp. Cryptogr. Inf. Secur.*, 2006, pp. 97–107.
[12] A. Juels, "Strengthening EPC tag against cloning," in *Proc. ACM Workshop Wireless Secur. (WiSe'05)*, 2005, pp. 67–76.
[13] T. Yeh, Y. Wanga, T. Kuo, and S. Wang, "Securing RFID systems conforming to EPC class 1 generation 2 standard," *Exp. Syst. Appl.*, vol. 37, no. 12, pp. 7678–7683, 2010.
[14] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," in *Proc. 2nd Workshop RFID Secur.*, 2006, pp. 27–36.
[15] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "EMAP: An efficient mutual authentication protocol for low-cost RFID tags," in *Proc. OTM Federated Conf. Workshop: IS Workshop*, 2006, pp. 352–361.

[16] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Proc. Int. Conf. Secur. Pervasive Comput.*, 2003, pp. 454–469.

[17] H. Chien, "Secure access control schemes for RFID systems with anonymity," in *Proc. Int. Workshop Future Mobile Ubiquitous Inf. Technol. (FMUIT '06)*, 2006, pp. 96–99.

[18] J. Lim, H. Oh, and S. Kim, "A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection," in *Proc. 4th Int. Conf. Inf. Secur. Pract. Exper. (ISPEC)*, 2008, pp. 278–289.

[19] A. Liu and A. Bailey, "A privacy and authentication protocol for passive RFID tags," *Comput. Commun.*, vol. 32, no. 7, pp. 1194–1199, 2009.

[20] S. Kang, D. Lee, and I. Lee, "A study on secure RFID mutual authentication scheme in pervasive," *Comput. Commun.*, vol. 31, no. 18, pp. 4248–4254, 2008.

[21] J. Cho, S. Yeo, and S. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Comput. Commun.*, vol. 34, no. 3, pp. 391–397, 2011.

[22] A. Juels, D. Molner, and D. Wagner, "Security and privacy issues in Epassports," in *Proc. 1st Int. Conf. Secur. Privacy Emerg. Areas Commun. Netw. (Secure Comm'05)*, 2005, pp. 74–88.

[23] M. Burmester, B. Medeiros, and R. Motta, "Robust, anonymous RFID authentication with constant key-lookup," *Cryptology ePrint Archive*: Report: 207/402, 2007.

[24] 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.

[25] S. Kaya, E. Savas, A. Levi, and O. Ercetin, "Public key cryptography based privacy preserving multi-context RFID infrastructure," *Ad Hoc Netw.*, vol. 7, no. 1, pp. 136–152, 2009.

[26] F. Furbass and J. Wolkerstorfer, "ECC processor with low die size for RFID applications," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS'07)*, 2007, pp. 1835–1838.

[27] Y. Lee, K. Sakiyama, and L. Batina, "Elliptic-curve-based security processor for RFID," *IEEE Trans. Comput.*, vol. 57, no. 11, pp. 1514–1527, 2008.

[28] 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.

[29] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 1, pp. 203–209, 1987.

[30] A. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[31] J. Wolkerstorfer, "Is elliptic-curve cryptography suitable to secure RFID tags?," in *Proc. Workshop RFID Light-Weight Cryptogr.*, 2005, pp. 11–20.

[32] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Proc. Topics Cryptol.(CT-RSA)*, 2006, pp. 115–131.

[33] C. Schnorr, "Efficient identification and signatures for smart cards," in *Proc. Adv. Cryptol.(CRYPTO'89)*, 1989, pp. 239–252.

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

[35] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," in *Proc. Adv. Cryptol.(CRYPTO'92)*, 1992, pp. 31–53.

[36] 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.

[37] J. Bringer, H. Chabanne, and T. Icart, "Cryptanalysis of EC-RAC, a RFID identification protocol," in *Proc. 7th Int. Conf. Cryptol. Netw. Secur. (CNS'08)*, 2008, pp. 149–161.

[38] 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.

[39] T. Deursen and S. Radomirovic, "Untraceable RFID protocols are not trivially composable: Attacks on the revision of EC-RAC," *Cryptology ePrint Archive*, Report, 2009/332, 2009.

[40] 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.

[41] 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.

[42] C. Lv, H. Li, J. Ma, and B. Niu, "Vulnerability analysis of elliptic curve-based RFID protocol," *China Commun.*, vol. 8, no. 4, pp. 153–158, 2011.

[43] 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.

[44] J. Fan, J. Hermans, and F. Vercauteren, "On the claimed privacy of EC-RAC III," *Radio Freq. Identif. Secur. Privacy Issues*, 2010, pp. 66–74.

[45] Y. Lee, L. Batina, and I. Verbauwhede, "Privacy challenges in RFID systems," in *Proc. Internet Things*, 2010, pp. 397–407.

[46] C. Lv, H. Li, and J. Ma, "Vulnerability analysis of elliptic curve cryptography-based RFID authentication protocols," *Trans. Emerg. Telecommun. Technol.*, vol. 23, no. 7, pp. 618–624, 2012.

[47] Y. Lee, L. Batina, and D. Singelee, "Wide–weak privacy–preserving RFID authentication protocols," in *Proc. Mobile Lightweight Wireless Syst.*, 2010, pp. 254–267.

[48] T. Deursen and S. Radomirovic, "EC-RAC: Enriching a capacious RFID attack collection," in *Proc. Radio Freq. Identif. Secur. Privacy Issues*, 2010, pp. 75–90.

[49] X. Zhang, J. Li, and Y. Wu, "An ECDLP-based randomized key RFID authentication protocol," in *Proc. Int. Conf. Netw. Comput. Inf. Secur. (NCIS)*, 2011, pp. 146–149.

[50] P. Babaheidarian, M. Delavar, and J. Mohajeri, "On the security of an ECC based RFID authentication protocol," in *Proc. 9th Int. ISC Conf. Inf. Secur. Cryptol. (ISCISC)*, 2012, pp. 111–114.

[51] 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.

[52] Y. Chen, J. Chou, and C. Lin, "A novel RFID authentication protocol based on elliptic curve cryptosystem," *Cryptology ePrint Archive*, Report, 2011/381, 2011.

[53] L. Batina, S. Seys, and D. Singeee, "Hierarchical ECC-based RFID authentication protocol," in *Proc. RFID Secur. Privacy*, 2012, pp. 183–201.

[54] Y. Liu, X. Qin, and C. Wang, "A lightweight RFID authentication protocol based on elliptic curve cryptography," *J. Comput.*, vol. 8, no. 11, pp. 2880–2887, 2013.

[55] 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.

[56] Y. Liao and C. Hsiao, "A secure ECC-based RFID authentication scheme using hybrid protocols," in *Advances in Intelligent Systems and Applications*. Berlin, Germany: Springer-Verlag, 2013, pp. 1–13.

[57] Y. Liao and C. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," *Ad Hoc Netw.*, vol. 18, pp. 133–146, 2014.

[58] J. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *J. Supercomput.*, vol. 70, no. 1, pp. 75–94, 2014.

[59] 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.

[60] 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.

[61] 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.

[62] G. Dormale and J. Quisquater, "High-speed hardware implementations of elliptic curve cryptography: A survey," *J. Syst. Archit.*, vol. 53, no. 2, pp. 72–84, 2007.

[63] T. Eisenbarth, S. Kumar, and C. Paar, "A survey of lightweight-cryptography implementations," *IEEE Des. Test Comput.*, vol. 24, no. 6, pp. 522–533, 2007.

[64] S. Kalra and S. Sood, "Elliptic curve cryptography: Survey and its security applications," in *Proc. Int. Conf. Adv. Comput. Artif. Intell.*, 2011, pp. 102–106.

[65] 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.

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

[67] 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.

[68] 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.

Debiao He received the Ph.D. degree in applied mathematics from the School of Mathematics and Statistics, Wuhan University, Wuhan, China, in 2009.

He is currently a Lecturer with Wuhan University. His research interests include cryptography and information security, in particular, cryptographic protocols.

Sherali Zeadally received the Bachelor's degree in computer science from the University of Cambridge, Cambridge, U.K., and the Doctorate degree in computer science from the University of Buckingham, Buckingham, U.K.

He is an Associate Professor with the College of Communication and Information, University of Kentucky, Lexington, KY, USA.

Dr. Zeadally is a Fellow of the British Computer Society and the Institution of Engineering Technology, Stevenage, U.K.