Hindawi
Journal of Sensors
Volume 2017, Article ID 2367312, 10 pages
https://doi.org/10.1155/2017/2367312

Research Article

An Advanced Encryption Standard Powered Mutual Authentication Protocol Based on Elliptic Curve Cryptography for RFID, Proven on WISP

Alaauldin Ibrahim and Gökhan Dalkılıç

Computer Engineering Department, Dokuz Eylul University, 35160 Izmir, Turkey

Correspondence should be addressed to Alaauldin Ibrahim; devletaladdin@gmail.com

Received 8 February 2017; Revised 29 June 2017; Accepted 26 July 2017; Published 31 August 2017

Academic Editor: Eduard Llobet

Information in patients' medical histories is subject to various security and privacy concerns. Meanwhile, any modification or error in a patient's medical data may cause serious or even fatal harm. To protect and transfer this valuable and sensitive information in a secure manner, radio-frequency identification (RFID) technology has been widely adopted in healthcare systems and is being deployed in many hospitals. In this paper, we propose a mutual authentication protocol for RFID tags based on elliptic curve cryptography and advanced encryption standard. Unlike existing authentication protocols, which only send the tag ID securely, the proposed protocol could also send the valuable data stored in the tag in an encrypted pattern. The proposed protocol is not simply a theoretical construct; it has been coded and tested on an experimental RFID tag. The proposed scheme achieves mutual authentication in just two steps and satisfies all the essential security requirements of RFID-based healthcare systems.

1. Introduction

Radio-frequency identification (RFID) technology is one of the most promising advances in pervasive infrastructures that allow the contactless identification of tagged objects and people. RFID systems are composed of a tag, reader, and back-end database server. The reader is used to query the tag identity, which is forwarded to the back-end server.

The data in RFID systems can be read, without line of sight, through nonconducting materials such as cardboard or paper at a rate of hundreds of tags per second and at a distance of several meters. Tags have read/write memory capability, can store data, and are relatively insensitive to adverse conditions (dust, chemicals, and physical damage). Besides replacing optical barcode systems, the above advantages make RFID tags applicable in various scenarios, including access control, environmental sensing, livestock and automobile identification, inventory control, and theft detection. RFID technology is widely used in healthcare environments, where it has been applied to newborn and patient identification [1], tracking medical assets [2], medical treatment tracking and validation [3], surgical process management [4], and patient location and procedure management [5].

The legacy systems in hospitals could be integrated with middleware to provide a lot of smart services, such as drug administration, patient identification, and asset tracking. However, hospitals are open and unsecure environments in which radio waves are used for connections. An eavesdropper could read, modify, or even clone the data stored in patients' tags. Thus, security and privacy are major concerns for the use of RFID systems in healthcare environments. The US Food and Drug Administration (FDA) declared that "Hospira and an independent researcher confirmed that Hospira's Symbiq Infusion System could be accessed remotely through a hospital's network. This could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or underinfusion of critical patient therapies" [6]. In future, the FDA may warn about other devices or even RFID-based healthcare systems. For instance, if the blood groups or laboratory test results were modified on the RFID tags attached to blood bags [7], patients could suffer fatal harm. To prevent and eliminate these potential hazards,

Figure 1: Front and back sides of WISP5.

strict and rigid mutual authentication protocols must be exploited between the tag and the reader using the latest cryptographic technologies.

Protocols conforming to the EPC Class 1 Generation 2 standard increasingly become inadequate, and there is a demand for stronger protocols. Furthermore, the development of integrated circuit techniques means that RFID tags could support the complicated operations of private and public key cryptography. In this paper, using the last revision of the Wireless Identification and Sensing Platform (WISP5) (Figure 1) [8], we propose a mutual authentication protocol based on elliptic curve cryptography (ECC) and advanced encryption standard (AES) algorithms. WISP5 is an EPC Class 1 Generation 2 UHF passive RFID tag that is embedded with AES and sensors and includes a fully programmable 16-bit microcontroller (MSP430 16 Mhz CPU, 64 KB nonvolatile memory, 66 KB RAM [9]). Integrating passive RFID with sensing technologies is widely applicable in many productive sectors.

For instance, some application scenarios of the healthcare systems, as WISP, have built-in sensors; they can easily send temperature of WISP tagged blood bag to the system. Checking whether the box that contains glass tubes having specimens taken from the patients in the laboratory has been fallen or not or measuring the ambient temperature can be achieved via a WISP tagged to the box. Moreover, there are many valuable devices in the hospital and some of these devices are portable. It is possible to get information about the place of the WISP tagged devices and it can be easily determined whether a WISP tagged device has been moved or not. In the above scenarios, if the authentication is provided, we can trust that the tags are the legitimate tags. WISP5 is passively powered, obtaining power from the reader rather than a battery. Hence, this is essentially a maintenance-free system.

Compared with public key algorithms such as RSA, ECC-based systems are smaller and faster and consume less power (Table 1). Thus, the elliptic curve Diffie–Hellman scheme (ECDH) is used to produce the secret key that will encrypt the tag ID and data. The elliptic curve digital signature algorithm (ECDSA) is used to prevent man-in-the-middle attacks [10] and to achieve mutual authentication between the tag and the reader.

Table 1: Comparable key sizes in terms of computational effort for cryptanalysis [11].

RSA-based asymmetric scheme (modulus size in bits)	ECC-based asymmetric scheme (size of n in bits)
512	112
1024	160
2048	224
3072	256
7680	384
15360	512

2. Related Work

Many ECC-based authentication schemes have been proposed to satisfy the security constraints of RFID tags. Tuyls and Batina [12] used the Schnorr identification protocol to develop an ECC-based RFID identification scheme. This scheme claimed to be resistant against tag counterfeiting. However, Lee et al. [13] showed that this scheme is vulnerable to location tracking attacks, does not achieve forward security and mutual authentication, and lacks scalability. Based on Okamoto's authentication protocol, Batina et al. [14] proposed an ECC-based RFID authentication protocol that they claimed could avoid active attacks. Lee et al. [13] mentioned that Batina et al.'s protocol is vulnerable to location tracking attacks and has scalability and forward secrecy issues. Lee et al. [13] claimed to solve all the issues mentioned above, but later studies [15, 16] showed that Lee et al.'s scheme is vulnerable to tracking and forgery attacks and does not provide mutual authentication. In 2010, Lee et al. [17] proposed an ECC-based RFID authentication scheme to address the existing tracking problems [12, 14]. Only tag-to-reader authentication has been considered, rather than reader-to-tag authentication. In 2011, Zhang et al. [18] proposed an ECC-based randomized key scheme that improved previous schemes. Although secure against some relevant attacks, this approach still does not perform mutual authentication.

In 2014, Liao and Hsiao [19] proposed a secure ECC-based RFID authentication scheme with an ID-verifier transfer protocol to achieve mutual authentication. However, the weaknesses of this approach were detailed in three separate studies. First, Moosavi et al. [20] mentioned that the tag identification of Liao and Hsiao's scheme lacks efficiency in terms of the tag's computation time and its memory requirements. Second, He et al. [21] proposed a lightweight ECC-based RFID authentication integrated with an ID-verifier transfer protocol and pointed out that their proposal performs better than that of Liao and Hsiao in terms of computational cost and storage requirements. Third, Zhao [22] showed that Liao and Hsiao's method enabled an adversary to obtain the private key stored in the tag. Chou [23] proposed a new RFID authentication protocol using ECC and claimed that it could resist various attacks. Later, Zhang and Qi [24] pointed out that Chou's protocol [23] suffers problems with tag information privacy, backward traceability, and forward traceability.

In 2015, Jin et al. [25] proposed a secure RFID mutual authentication protocol for healthcare environments using ECC and claimed that their proposal could withstand various attacks while outperforming the protocols detailed

in [21, 22, 24]. In the same year, Lee and Chien [26] proposed an ECC-based RFID authentication protocol for e-health and reported that He et al.'s protocol [21] is vulnerable to active tracking attacks. In 2016, Farash et al. [27] proved that both Zhao's [22] and Zhang and Qi's [24] schemes do not provide forward privacy. Recently, in 2017, Benssalah et al. [28] proposed a secure RFID authentication protocol based on elliptic curve signature with message recovery (ECMR) suitable for m-Health environments and claimed that their proposal can achieve many security requirements, withstands the well-known attacks, and performs better compared to the well-known authentication protocols in the literature, but not applied and tested on RFID tag hardware.

In this point, wireless body area networks (WBAN) authentication protocols are worth mentioning. In 2013, Li et al. [29] proposed the first ECC-based WBAN authentication protocol. However, because of the limited resource of wearable devices, the scheme was unsuitable. To improve the performance, in 2014 Liu et al. [30] proposed two certificateless anonymous authentication protocols. However, Zhao [31] mentioned that protocols of Liu et al. [30] are vulnerable to stolen-verifier attacks and proposed an enhanced scheme. Meanwhile, Xiong [32] pointed that protocols of Liu et al. [30] are lack of forward secrecy and scalability and proposed a scalable and anonymous certificateless remote authentication protocol. In 2015, He and Zeadally [33] showed that Zhao's protocol [31] cannot provide privacy and proposed authentication protocol beyond WBAN for an ambient assisted living system that authenticates the user to the local server, but the authentication between local server and body sensors was not considered. In 2016, He et al. [34] pointed out that the schemes of Liu et al. [30] suffer from impersonation attack and they proposed an anonymous authentication scheme for WBAN. In the same year, Liu et al. [35] presented a 1-round anonymous authentication protocol. However, in 2017 Li et al. [36] pointed that scheme of Liu et al. [35] is vulnerable to impersonation, stolen-verifier, and denial-of-service attacks and proposed an enhanced 1-round authentication protocol with user anonymity. Later in the same year, Li et al. [37] mentioned that the above-reviewed authentication protocols for WBAN either present no revocation procedure to revoke the user's privilege or lack anonymity. Moreover, they proposed anonymous mutual authentication and key agreement scheme for wearable sensors in WBAN.

3. Contributions and Paper Organization

Unlike other existing schemes, the proposed scheme sends tag's ID and the valuable stored data in the tag securely (encrypted by AES), while existing protocols are trying to send only the tag's ID. The schemes that realize the mutual authentication are achieved at least in 3 steps, while in our work the mutual authentication is realized in only 2 steps. The proposed scheme is tested and realized on real devices. Unlike Jin et al.'s study [25] where precomputing method is used, the private and public keys are not static, but they are refreshing after each communication that strengthens the security and makes the keys untraceable and unpredictable. Moreover, contributions can be summarized as follows:

(i) ECDH is used to produce the secret key that will be used in AES to encrypt both tag's ID and the valuable data stored in the tag.

(ii) ECDSA is used to prevent man-in-the-middle attack that ECDH suffers from, to realize the mutual authentication.

(iii) AES embedded in WISP5 is used to encrypt both tag's ID and tag's valuable data.

(iv) ECC almost is not applicable on resource constrained systems. So, the tiny ECC [38] has been used in this scheme.

(v) Shamir's trick optimization is used to compute $(u_1G + u_2R')$ that is used in ECDSA verification. Direct implementation requires two scalar multiplications and a point addition, but with Shamir's trick, the cost is close to one scalar multiplication [39].

(vi) The efficiency of point multiplication has been increased by using Montgomery's ladder with co-Z coordinates [40].

The remainder of this paper is organized as follows. An RFID mutual authentication protocol has been proposed in Section 4, where Section 4.1 discusses the protocol. The security analysis has been given in Section 4.2, performance analysis in Section 4.3, and security and performance comparison in Section 4.4. Finally, conclusion and future works are explained in Section 5.

4. Proposed Protocol

WISP5 built-in random number generator has been used as the random number generator of our proposed protocol. We assume that communication between the reader and the back-end database server is secure, and the communication between the tag and the reader is not secure. The reader is fully equipped and connected directly to a power supply. The proposed scheme uses the WISP5, Impinj Speedway reader, MSP-FET430UIF debugging tool, WISP5 programming adapter, Code Composer Studio, and PC.

4.1. Discussion. The scheme has two participants: the trusted tag and the trusted reader, which is connected to the back-end database server (Figure 2). Our protocol consists of two phases: setup phase and authentication phase. The notation used in this protocol is as follows:

(i) Domain parameters of prime field (F_p) elliptic curve $(E : y^2 = x^3 + ax + b \bmod p)$ are

p: big prime number defined for finite field F_p,
a, b: defining the elliptic curve $E(F_p)$,
G: generator point,
n: order of G (order of the curve),
h: cofactor $= \#E(F_p)/n$, where $\#E(F_p)$ is number of points on elliptic curve $E(F_p)$,

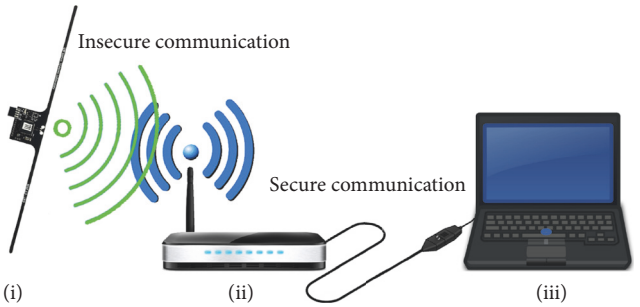

Figure 2: Our study's scheme (WISP5 (i), reader (ii), and back-end database server (iii)).

(ii) K_{TR}: the produced secret key by ECDH key exchange that will be used in AES to encrypt/decrypt tag ID and the sent/received data,

(iii) t, T: private and public keys (at the same time considered as a message during signing T in ECDSA) of a tag used in ECDH key exchange to produce secret key K_{TR},

(iv) t', T': private and public keys of the tag used in ECDSA,

(v) (h, g): signature pair of T (the tag's public key),

(vi) r, R: private and public key (at the same time considered as a message during signing R in ECDSA) of a reader used in ECDH key exchange to produce secret key K_{TR},

(vii) (z, s): signature pair of R (the reader's public key),

(viii) r', R': private and public keys of the reader used in ECDSA,

(ix) ID_i: ID of the ith tag,

(x) k: a random integer used during R (the reader's public key) signing in ECDSA,

(xi) l: a random integer used during T (the tag's public key) signing in ECDSA.

Setup Phase. In this phase, both the reader and tag agree on a curve with elliptic curve domain parameters p, a, b, G, n, and h. Elliptic curve secp160r1, recommended by NIST, is used for the domain parameter values [41].

(1) All tags' identifiers (IDi) are stored in the back-end-database server.

(2) The tag selects an integer t' at random as its private key for ECDSA, where $1 \leq t' \leq n - 1$, and computes its public key T' that will be used in ECDSA, where $T' = t'G$. Then, the public key T' of the tag is stored in the back-end-database server.

(3) The reader selects an integer r' at random as its private key for ECDSA, where $1 \leq r' \leq n - 1$, and computes its public key R' that will be used in ECDSA, where $R' = r'G$. Then, the public key R' of the reader is set on all the tags manually.

Authentication Phase. At the end of this phase, the public keys R and T are produced, R and T are signed and verified, and R and T are exchanged. The secret key K_{TR} is produced and mutual authentication is achieved in two steps as follows:

(1) The reader picks an integer random number r as its private key used in ECDH, where $1 \leq r \leq n - 1$, and computes its public key R (at the same time considered as a message for ECDSA) that will be used in ECDH, where $R = rG$.

(2) Before starting ECDH key exchange and sending R to the tag, the reader signs R using ECDSA as follows:

(a) $e = \mathrm{Hash}(R)$, where the hashing algorithm is SHA-3 (256).
(b) Select a random integer k $[1, n - 1]$.
(c) Calculate $z = x_1 \bmod n$, where $(x_1, y_1) = kG$. If $z = 0$, go to (b).
(d) Calculate $s = k^{-1}(e + r'z) \bmod n$. If $s = 0$, go to (b).
(e) Signature pair is (z, s).

(3) The reader sends R and its signature pair (z, s) to the tag.

(4) Once the tag receives R and its signature (z, s), it verifies R as follows:

(a) Check whether z and s are integers in the range $[1, n - 1]$. If not, the signature is invalid and the session is rejected.
(b) $e = \mathrm{Hash}(R)$, where the hash algorithm is SHA-3 (256).
(c) Calculate $w = s^{-1} \bmod n$.
(d) Calculate $u_1 = ew \bmod n$ and $u_2 = zw \bmod n$.
(e) Calculate $(x_1, y_1) = u_1G + u_2R'$.
(f) The reader is authenticated if $x_1 = z \bmod n$; otherwise, the tag rejects the session.

(5) If the reader is authenticated, the tag picks a random integer t as its private key used in ECDH, where $1 \leq t \leq n - 1$, and computes its corresponding public key $T = tG$.

(6) Before starting ECDH key exchange and sending T to the reader, the tag signs T using ECDSA as follows:

(a) $e = \mathrm{Hash}(T)$, where the hashing algorithm is SHA-3 (256).
(b) Select a random integer l $[1, n - 1]$
(c) Calculate $g = x_2 \bmod n$, where $(x_2, y_2) = lG$. If $g = 0$, go to (b).
(d) Calculate $h = l^{-1}(e + t'g) \bmod n$. If $h = 0$, go to (b).
(e) Signature pair is (g, h).

(7) The tag computes the secret key $K_{TR} = tR = t(rG) = trG$.

(8) The tag encrypts its ID using AES: $C = \mathrm{AES}_{K_{TR}}(\mathrm{ID})$.

(9) The tag sends its public key T and its signature pair (g, h) and C to the reader.

(10) Once the reader receives T and its signature (g, h), it verifies T as follows:

(a) Check whether g and h are integers in the range $[1, n-1]$. If not, the signature is invalid and the session is rejected.

(b) $e = \text{Hash}(T)$, where the hash algorithm is SHA-3 (256).

(c) Calculate $i = h^{-1} \bmod n$.

(d) Calculate $j_1 = ei \bmod n$ and $j_2 = gi \bmod n$.

(e) Calculate $(x_2, y_2) = j_1 G + j_2 T'$.

(f) $x_2 = g \bmod n$; otherwise, the reader rejects the session.

(11) The reader computes the secret key $K_{TR} = rT = r(tG) = rtG$.

(12) To get the tag ID, the reader decrypts AES by $\text{ID} = \text{AES}^{-1}_{K_{TR}}(C)$.

(13) The server will compare the ID with ID_i from its database. If $x_2 = g \bmod n$ *and* $\text{ID} = \text{ID}_i$, the tag is authenticated; otherwise, it is not and reader rejects the session.

As shown in Table 2, the mutual authentication has been achieved in only two steps. If sensing properties of WISP wanted to be exploited, data related to the sensors' readings can be sent with the tag ID.

4.2. Security Analysis. Our proposed protocol is resistant to the known attacks detailed in Table 2. This section analyzes the security of our proposed protocol.

Mutual Authentication. Using the signature pair (z, s) and the reader's public key used in ECDSA (R'), the tag can verify the signed public key (R), herewith the reader can be authenticated. Tag authentication passes through two stages: stage one, using the signature pair (g, h) and the tag's public key used in ECDSA (T'), the reader can verify the signed public key (T) and hence authenticate the tag; stage two, since (1) the unique IDs of all tags are stored formerly in the back-end-database server, (2) the tag IDs are sent in an AES encrypted form, (3) each session uses a different secret key K_{TR}, (4) the reader could decrypt AES and gets the ID, (5) the received ID matches the stored ID_i, and the reader authenticates the tag. Hence, the proposed protocol provides mutual authentication.

Tracking Attack, Traceability, Location, and Information Privacy. Because the ID and confidential information on the tag are encrypted by AES using K_{TR}, an attacker has to break AES or obtain K_{TR} to access the ID or confidential information, which is computationally infeasible. Moreover, K_{TR} is dynamic, meaning that, after each session, a new and different key is produced. Accordingly, the tag cannot be tracked, and the attacker cannot obtain the location and private information stored in the tag. Hence, it cannot be traced.

Desynchronization Attack, Denial-of-Service (DoS) Attack, and Availability. In the proposed scheme, neither the tag ID nor any critical data that can cause desynchronization is updated after each execution. Therefore, the proposed protocol can withstand desynchronization attacks, and both the tag and reader remain synchronized and available to communicate. Thus, DoS attacks can be withstood and availability is maintained.

Tag Anonymity. An adversary who intercepts R, z, s, T, g, h, and C between the reader and the tag and attempts to obtain the tag ID cannot get the session key K_{TR}, because this is computationally infeasible under the Diffie–Hellman problem and the elliptic curve discrete logarithm problem (ECDLP). Thus, the proposed protocol protects tag anonymity.

Eavesdropping and Man-in-the-Middle. Even if an adversary eavesdrops messages transmitted between the reader and the tag, the data are useless without the private keys (t and r). When trying to obtain t, r, or any valuable information, the attacker faces the computational Diffie–Hellman problem and ECDLP. Any modification on the messages will be detected, because R and T are signed by private keys r' and t' respectively, and the received ID is compared with the stored ID_i. Thus, the proposed protocol is resistant to eavesdropping and man-in-the-middle attacks.

Tag Impersonation and Reader Spoofing Attacks. To impersonate a tag, an attacker must produce K_{TR} or break AES, which is computationally infeasible under the Diffie–Hellman problem and ECDLP. As the public key of the tag (T) is signed by the private key t' and verified by the public key T' *of the tag,* an attacker cannot impersonate the tag. Similarly, attackers cannot spoof the reader, because this would require the signature pair (z, s) and to produce K_{TR}, all of which are unattainable without knowing t and r. Thus, the proposed protocol can overcome tag impersonation and reader spoofing attacks.

Cloning Attacks. To clone a tag, attackers must obtain the ID of the tag they wish to clone. Obtaining the tag ID requires the computation of K_{TR}, which is computationally infeasible under the Diffie–Hellman problem and ECDLP or the breaking of AES. Hence, the proposed protocol is resistant to cloning attacks.

Full Disclosure Attacks. The sent messages R, z, s, T, g, h, and C do not disclose any secrets. Hence, even if an adversary could intercept these messages, it would be unable to progress without the random private keys t and r. Furthermore, any attempt to calculate t and r will encounter the computational Diffie–Hellman problem and ECDLP or AES. Thus, the scheme resists full disclosure attacks.

Replay Attacks. Intercepting R, z, and s and replaying them to the tag will not produce K_{TR} from the previous session, because the tag chooses a new private key that is used to form the new session key K_{TR}. Similarly, replaying T, g, h, and C from the previous session will not cause the reader to produce K_{TR} from the previous session.

Confidentiality. As the tag ID is transmitted as ciphertext, and K_{TR} changes for every session, an attacker cannot achieve

Table 2: Proposed scheme.

Tag	Reader
Setup phase(i) Both reader and tag agree on a curve, on elliptic curve domain parameters p, a, b, G, n, and h(ii) (R') is set manually on all the tags (iii) Pick t' randomly as the private key; then the public key will be $T' = t'G$	*Setup phase* (i) Both reader and tag agree on a curve, on elliptic curve domain parameters p, a, b, G, n, and h(ii) Pick r' randomly as the private key; then the public key will be $R' = r'G$
Authentication phase	Authentication phase (1) Computing public key R: Pick r randomly as private key; then $R = rG$ (2) Signing R: (a) $e = \text{Hash}(R)$ (b) Select k randomly (c) $z = x_1 \bmod n$; if $z = 0$, go to (b) (d) $s = k^{-1}(e + r'z) \bmod n$; if $s = 0$, go to (b) (e) Signature pair is (z, s)
	(3) Send R, z, s ←
(4) Verifying R: (a) Check if z and s are integers in range $[1, n-1]$. If not, the signature is invalid and rejects the session (b) $e = \text{Hash}(R)$ (c) $w = s^{-1} \bmod n$ (d) $u_1 = ew \bmod n$ and $u_2 = zw \bmod n$ (e) $(x_1, y_1) = u_1G + u_2R'$ (f) If $x_1 = z \bmod n$, reader is authenticated; otherwise, it is not and rejects the session (5) In case of authentication, pick t as private key and compute public key $T = tG$ (6) Signing T: (a) $e = \text{Hash}(T)$ (b) Select l randomly (c) $g = x_2 \bmod n$; if $g = 0$, go to (b) (d) $h = l^{-1}(e + t'g) \bmod n$; if $h = 0$, go to (b) (e) Signature pair is (g, h) (7) $K_{TR} = tR = t(rG) = trG$ (8) $C = \text{AES}_{K_{TR}}(\text{ID})$	
	(9) Send T, g, h, C →
	(10) Verifying T: (a) Check if g and h are integers in the range $[1, n-1]$. If not, the signature is invalid and rejects the session (b) $e = \text{Hash}(T)$ (c) $i = h^{-1} \bmod n$ (d) $j_1 = ei \bmod n$ and $j_2 = gi \bmod n$ (e) $(x_2, y_2) = j_1G + j_2T'$ (f) If $x_2 \neq g \bmod n$, then the reader rejects the session (11) $K_{TR} = rT = r(tG) = rtG$ (12) $\text{ID} = \text{AES}^{-1}_{K_{TR}}(C)$ (13) If $x_2 = g \bmod n$ and $\text{ID} = \text{ID}_i$, the tag is authenticated; otherwise, it is not and rejects the session

Table 3: Communication cost.

Communication	Cost (bit)
Reader-tag	640
Tag-reader	768
Total	1408

any progress. Thus, unauthorized users cannot obtain the tag ID or other valuable information without computing K_{TR} or breaking of AES.

Integrity, Modification Attack, and Unforgeability. Since ECDSA is used by reader, modifications to the signature pair (z, s) will be detected by the tag and any modifications to T, g, and h will cause the verification to fail and cause wrong K_{TR} and accordingly wrong ID. Hence, the proposed protocol provides integrity, rejects any modifications, and provides unforgeability.

Forward/Backward Security. An adversary cannot compromise the previous/current confidential information, because the transferred messages R, z, s, T, g, h, and C change after each execution according to the random private keys t and r. Adversaries cannot obtain the tag ID, because it is sent as ciphertext with a different K_{TR} in each session.

4.3. Performance Analysis. The performance of the proposed method is analyzed in terms of code size, communication cost, and tag response time (the reader is assumed to be fully equipped). The results are obtained based on the secp160r1 curve. A total of 29450 (code) and 3296 (data) bytes are written to the tag FLASH/FRAM, and RAM usage is 1595 bytes. The communication cost (Table 3) from reader-to-tag involves transmitting the 320-bit reader public key and 320-bit reader signature (=640 bits), and the communication cost from tag-to-reader involves transmitting the 320-bit tag public key, 320-bit tag signature, and 128-bit encrypted tag ID (=768 bits). Unlike the proposal in [25], which used the pairing-based cryptography library with an embedding degree of 2 on an Intel Pentium(R) Dual-Core processor with 2.69 GHz and 2048 MB of RAM, and the proposal in [21], which assumed a hardware platform of a Pentium-IV 3 GHz processor with 512 MB memory and Windows XP [42], our proposed protocol is realized on a passive tag with a 16 MHz MSP430, 64 KB nonvolatile memory, and 66 KB RAM. As shown in Table 4, computing K_{TR} requires 1.4578926250 s (=23,326,282 CPU cycles/16 MHz). However, adopting the same system used by Jin et al. [25], computing K_{TR} would require 0.00867148 s (=23,326,282 CPU cycles/2.69 GHz). Previous ECC-based protocols have been adopted under simulation scenarios, whereas the proposed protocol has been realized on a real device.

Although the proposed scheme uses the tiny ECC [38] and has AES embedded in the WISP5 platform, its heaviness is apparent from the results. However, taking the algorithms used in the proposed protocol, the results reported by Marin et al. [43] indicate that each point addition and point doubling on MSP430 require 22,981.05 and 25,743.13 CPU cycles, respectively. Marin et al. [44] found that producing a signature tiny ECC requires 19308 bytes ROM and 1510 bytes RAM, generating a signature requires 2 s, and verifying the signature requires 2.43 s. Considering these facts, our results are reasonable. Indeed, some enhancements have been achieved. In worst case, according to Moore's law [45], using the same codes, the response times may decrease to half within maximum two years.

Table 4: Response times.

Operation	Resp. time (s)	Resp. time (CPU cycles)	Resp. time adopting system used in [25] (s)
Generating 16-bit RNG	0.0001356875	2171	0.0000008070
Hashing R	0.0185743125	297,189	0.0000001104
Verification of R	1.8052265625	28,883,625	0.0107374070
Generating t	0.0121121250	193,794	0.0000720423
Computing T	1.4709932500	23,535,892	0.0087494022
Signing T	1.6268456250	26,029,530	0.0096764452
Computing K_{TR}	1.4578926250	23,326,282	0.0086714802
Encrypting tag ID (AES)	0.0000471875	755	0.0000002806

4.4. Security and Performance Comparison. In this section, a performance and functionality comparison is made between the proposed and some related ECC-based RFID authentication schemes. Table 5 shows the communication cost of our proposed and related schemes. Although our proposal achieves mutual authentication in just two steps, its communication cost is less than study [23] and very close to the other compared schemes. In terms of security services and attacks, Table 6 lists the security comparisons among our proposed scheme and other ECC-based schemes. It is visible that our protocol has additional security features than the related schemes and withstands the common attacks and satisfies the essential security requirements of RFID-based healthcare systems which make it more suitable than other healthcare related protocols in the field of healthcare systems.

5. Conclusion and Future Works

Following the FDA's declaration, efficient and rigid mutual authentication protocols are needed between the tag and the reader to prevent and eliminate potential hazards related to healthcare environments. Accordingly, this paper has proposed a stable and powerful mutual authentication protocol applied on WISP5. Both symmetric and asymmetric algorithms have been exploited. The protocol has been coded and tested, and its security has been thoroughly analyzed. The code size, RAM usage, and response time of the scheme are clearly not optimal. However, considering that MSP430 is being used with the SHA3, ECDH, and ECDSA algorithms, this is to be expected. ECC includes numerous time-consuming point multiplications. The cost of these operations could be reduced using methods to increase the

Table 5: Performance comparison.

Communication cost	Liao and Hsiao [19]	Zhao [22]	Chou [23]	Zhang and Qi [24]	Our study
Number of steps	3	3	3	3	2
Bytes	168	168	184	160	176

Table 6: Security comparison (√: provide, X: do not provide, and —: not mentioned).

Security services and attacks	Liao and Hsiao [19]	Zhao [22]	Chou [23]	Zhang and Qi [24]	Our study
Mutual authentication	X	√	X	√	√
Tracking attack	X	—	—	—	√
Traceability	X	—	X	—	√
Location privacy	X	√	X	—	√
Information privacy	X	—	X	√	√
Desynchronization attack	—	—	—	√	√
Denial-of-service (DoS) attack	√	√	√	√	√
Availability	√	√	—	—	√
Tag anonymity	√	X	—	√	√
Eavesdropping	—	—	—	—	√
Man-in-the-middle	—	—	X	√	√
Impersonation attack	X	√	X	√	√
Reader spoofing attack	X	√	—	√	√
Cloning attacks	√	√	—	—	√
Full disclosure attacks	—	—	—	—	√
Replay attacks	√	√	√	√	√
Confidentiality	√	—	—	—	√
Integrity	—	—	—	—	√
Modification attack	—	—	—	√	√
Unforgeability attack	—	—	—	—	√
Forward security	X	X	X	X	√
Backward security	X	X	X	X	√

efficiency of point multiplication. Regardless, the proposed protocol, which achieves mutual authentication in only two steps, withstands almost all common attacks and satisfies the essential security requirements of RFID-based healthcare systems.

Reducing the code size and decreasing the tag response time will be considered in future work. Additionally, as most studies on WISP have involved only a single unit, we will intend to use the sensing features of WISP5 to integrate multiple WISPs, thus enabling the exploration of a new battery-free form of wireless sensor networking in the field of healthcare systems.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Y. K. Hung, "The study of adopting RFID technology in medical institute with the perspectives of cost benefit," in *Proceedings of the International Medical Informatics Symposium in Taiwan*, 2007.

[2] P. Najera, J. Lopez, and R. Roman, "Real-time location and inpatient care systems based on passive RFID," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 980–989, 2011.

[3] J. E. Katz and R. E. Rice, "Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology," *International Journal of Medical Informatics*, vol. 78, no. 2, pp. 104–114, 2009.

[4] C. Yu, C. Chen, P. Liao, and Y. Lee, "RFID-based operation room and medicare system for patient safety enhancementa case study of keelung branch," *J Inf Manag*, vol. 15, pp. 97–122, 2008.

[5] J. G. Leu, *The benefit analysis of RFID use in the health management centerThe experience in*, Shin Kong Wu Ho-Su Memorial Hospital. National Taiwan University, 2010.

[6] http://www.fda.gov/MedicalDevices/.

[7] *Blood bags with RFID chips (2010 picturesphotonews/2010/pn201005.php. Accessed*, vol. 23, com/press/en/presspicture/, 2015, http://www.siemens.

[8] WISP5 Wiki, "Welcome to the WISP 5 Wiki!," http://wisp5.wikispaces.com/WISP+Home, 2015.

[9] T. Instruments, "MSP430FR59xx Mixed Signal Microcontroller Datasheet," *Accessed*, vol. 08, 2015, http://www.ti.com/lit/ds/slas704e/slas704e.pdf.

[10] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic curves in cryptography*, vol. 265 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 2000.

[11] H. Tipton and M. KrauseBoca Raton, *Information Security Management Handbook, Four Volume Set*, Auerbach Publications, 2000.

[12] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Topics in cryptology—CT-RSA 2006*, vol. 3860 of *Lecture Notes in Comput. Sci.*, pp. 115–131, Springer, Berlin, 2006.

[13] Y. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol," in *Proceedings of the IEEE International Conference on RFID*, pp. 97–104, Las Vegas, Nev, USA, April 2008.

[14] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2007*, pp. 217–222, March 2007.

[15] T. Van Deursen and S. Radomirovic, *Attacks on RFID Protocols*, IACR Cryptology ePrint Archive, 2009.

[16] J. Bringer, H. Chabanne, and T. Icart, "Cryptanalysis of EC-RAC, a RFID identification protocol," in *Cryptology and Network Security: 7th International Conference, CANS 2008, Hong-Kong, China, December 2–4, 2008. Proceedings*, vol. 5339 of *Lecture Notes in Computer Science*, pp. 149–161, Springer, Berlin, Germany, 2008.

[17] Y. K. Lee, L. Batina, D. Singelee, B. Preneel, and I. Verbauwhede, "Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware," in *Towards Hardware-Intrinsic Security*, Information Security and Cryptography, pp. 237–257, Springer Berlin Heidelberg, Berlin, Germany, 2010.

[18] X. Zhang, L. Li, Y. Wu, and Q. Zhang, "An ECDLP-based randomized key RFID authentication protocol," in *Proceedings of the 2011 International Conference on Network Computing and Information Security, NCIS 2011*, pp. 146–149, May 2011.

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

[20] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "An elliptic curve-based mutual authentication scheme for RFID implant systems," *Procedia Computer Science*, vol. 32, pp. 198–206, 2014.

[21] D. He, N. Kumar, and N. Chilamkurti, "Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol," *Journal of Medical Systems*, vol. 38, article 116, 2014.

[22] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 38, no. 5, pp. 1–7, 2014.

[23] J.-S. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *Journal of Supercomputing*, vol. 70, no. 1, pp. 75–94, 2014.

[24] Z. Zhang and Q. Qi, "An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography," *Journal of Medical Systems*, vol. 38, no. 5, pp. 1–7, 2014.

[25] C. Jin, C. Xu, X. Zhang, and J. Zhao, "A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography," *Journal of Medical Systems*, vol. 39, no. 3, pp. 1–8, 2015.

[26] C. Lee and H. Chien, "An Elliptic Curve Cryptography-Based RFID Authentication Securing E-Health System," *International Journal of Distributed Sensor Networks*, vol. 11, no. 12, p. 642425, 2015.

[27] M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, "A Provably Secure RFID Authentication Protocol Based on Elliptic Curve for Healthcare Environments," *Journal of Medical Systems*, vol. 40, no. 7, article no. 165, 2016.

[28] M. Benssalah, M. Djeddou, and K. Drouiche, "A provably secure RFID authentication protocol based on elliptic curve signature with message recovery suitable for m-Health environments," *Transactions on Emerging Telecommunications Technologies*, p. e3166, 2017.

[29] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Transactions on Sensor Networks*, vol. 9, no. 2, article no. 18, 2013.

[30] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2014.

[31] Z. Zhao, "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 38, article 13, 7 pages, 2014.

[32] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2327–2339, 2014.

[33] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 71–77, 2015.

[34] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016.

[35] J. W. Liu, L. Zhang, and R. Sun, "1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks," *Sensors (Switzerland)*, vol. 16, no. 5, article no. 728, 2016.

[36] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, and K. Raymond Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Computers & Electrical Engineering*, 2017.

[37] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, 2017.

[38] A. Liu and P. Ning, "TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks," in *Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN '08)*, pp. 245–256, St. Louis, Mo, USA, April 2008.

[39] D. Hankerson, S. Vanstone, and A. J. Menezes, *Guide to Elliptic Curve Cryptography*, Springer, New York, NY, USA, 2004.

[40] M. Rivain, "Fast and Regular Algorithms for Scalar Multiplication over Elliptic Curves," in *Rivain M (2011) Fast and Regular Algorithms for Scalar Multiplication over Elliptic Curves. IACR Cryptology ePrint Archive*, p. 338, IACR Cryptology ePrint Archive, 2011.

[41] D. Brown, "SEC 2: Recommended Elliptic Curve Domain Parameters," *Certicom Research. Accessed*, vol. 8, 2010, http://www.secg.org/SEC2-Ver-1.0.pdf.

[42] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences. An International Journal*, vol. 180, no. 15, pp. 2895–2903, 2010.

[43] L. Marin, A. Jara, and A. Skarmeta Gomez, "Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier," *Mathematical and Computer Modelling*, vol. 58, no. 5-6, pp. 1155–1174, 2013.

[44] L. Marin, A. J. Jara, and A. F. G. Skarmeta, "Shifting primes: Extension of pseudo-mersenne primes to optimize ECC for MSP430-based future internet of things devices," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6908, pp. 205–219, 2011.

[45] Moore, "Moore's Law," http://www.mooreslaw.org/, 2017.