Hindawi
Journal of Sensors
Volume 2022, Article ID 7516010, 6 pages
https://doi.org/10.1155/2022/7516010

Research Article

An Improved Security Authentication Protocol for Lightweight RFID Based on ECC

Guo-heng Wei, Yan-lin Qin, and Wei Fu

Information Security Department, Naval University of Engineering, Wuhan, 430033 Hubei, China

Correspondence should be addressed to Yan-lin Qin; qinyanlincool@163.com

Received 17 September 2021; Accepted 13 January 2022; Published 8 February 2022

Academic Editor: Chao Wang

The security, privacy, and operation efficiency of radio frequency identification (RFID) must be fully measured in practical use. A few RFID authentication schemes based on elliptic curve cryptography (ECC) have been proposed, but most of them cannot resist the existing attacks. The scheme presented by Qian et al. could not resist impersonation attack according to our security analysis. Then, we propose a novel lightweight RFID authentication scheme, which is proved that it can resist server spoofing attack, tag masquerade attack, and provide other security properties of a RFID authentication scheme. Comparisons of computation and communication cost demonstrate that the proposed scheme is more suitable for the resource-constrained RFID authentication.

1. Introduction

Radio frequency identification (RFID) is a noncontact automatic identification technology, and the basic principle is to use the transmission characteristics of the RF signal space coupling (inductive or electromagnetic coupling) or reflection to achieve automatic identification of the object. An RFID system usually consists of tags, readers, and a backend server [1]. In recent years, radio frequency identification technology has developed rapidly and been widely used in various fields. However, due to the openness of the channel between the tag and the reader, the security and privacy problems it faces have become increasingly prominent. In particular, the processing capacity, storage space, and energy supply of tag chips are very limited, and many mature security schemes cannot be applied to RFID. Hence, higher security level, lightweight, and efficient RFID authentication scheme has become the new research goal.

At present, several lightweight RFID authentication schemes using cryptography have been successively proposed. These schemes can be roughly divided into the following categories: the schemes using simple bitwise logic operation, the schemes based on hash function, the schemes based on symmetric cryptosystem (AES and others), and the schemes based on public key cryptosystem. Among them, lightweight authentication scheme using simple bitwise logic operations satisfies the properties of low calculation amount, low power consumption, and small chip area, but the security cannot be well guaranteed. At the same time, the authentication scheme using only the hash function and the symmetric cryptographic algorithms has also been proved to be unable to fully meet the security requirements of RFID authentication [2]. Therefore, scholars have carried out research on lightweight authentication schemes based on public key cryptography. In this paper, we propose an improved RFID authentication scheme based on the security analysis of the scheme proposed by Qian et al. [3], analyze the security of the improved scheme, and compare its performance with the existing similar schemes. The security and efficiency comparison results show that the proposed scheme is more secure and has superior computing performance.

2. Related Work

In recent years, the public key cryptosystem has been introduced into the RFID authentication schemes. Chen et al. [4] proposed the RFID authentication scheme based on the quadratic residues for the first time, but Cao et al. [5]found that it could not resist tag impersonation and desynchronization attacks [5]. Yeh et al. [6] further proved that the scheme in [4] could not provide location privacy and resistance to replay attacks and proposed an improved scheme.

Compared with public key cryptosystem based on quadratic residues [7] and other public key cryptosystems (such as RSA and ElGamal), elliptic curve public key cryptography (ECC) requires a much shorter key length while providing the same security strength, so it is especially suitable for environments with limited computing resources and storage space. Lee et al. [8] proposed an ECC-based RFID authentication scheme—EC-RAC—which proved to be unable to resist impersonation attacks and location tracking attacks [9]. Aiming at the security problems in the EC-RAC scheme [10], Zhang et al. [11] proposed a randomized key RFID authentication scheme based on the elliptic curve discrete logarithm problem and proposed an improved scheme for the classic Schnorr authentication scheme at the same time. Babaheidarian et al. [12] pointed out that both of the two improved schemes proposed in [11] have security problems: the improved scheme for EC-RAC has the risk of tag impersonation attack and cannot provide mutual authentication between the server and the tag; the improved scheme for the classic Schnorr authentication scheme is difficult to resist location tracking attack and desynchronization attack. Liao and Hsiao [13] proposed an ECC-based RFID authentication scheme, which does not need to update the data in the server and tag memory and has high computational efficiency. However, Peeters and Hermans [14] proved that there is a server counterfeiting attack, and the attacker can obtain the identity authentication factor of the tag by insertion attack, so it is also difficult to resist the tag impersonation attack. He et al. [15] improved the authentication scheme in [13], but Wei et al. [16] found that the improved scheme [15]could not resist the server impersonation attack. This paper focuses on the analysis to another ECC-based authentication scheme proposed by Qian et al. [3] recently. Through analysis, we found that the scheme still has loopholes for attacks such as server impersonation and tag impersonation.

3. Security Analysis of the RFID Authentication Scheme Proposed by Qian et al.

3.1. The Authentication Scheme Proposed by Qian et al. Qian et al. proposed an ECC-based RFID authentication scheme in [3]. The detailed steps of this scheme are shown in Figure 1.

3.2. Attacks against the Scheme

(i) Server impersonation attack

Assuming that the attacker can obtain the tag's internal ID information, he can impersonate database and reader to interact with the tag and can pass the tag's authentication.

The specific attack steps are as follows:

(a) Attacker→tag: The attacker generates a random number R' and sends $M_1' = \{R', \text{Query}\}$ to the tag

(b) Tag→fake reader: Upon receiving query and R', the tag computes $M_2' = \{M(ID) + tP_s + R', P_t + R'\}$ and sends it to the fake reader

(c) Fake reader→fake database: The fake reader sends $\{M_2', R'\}$ to the fake database

(d) Fake database→tag: The fake database generates a random number k', calculates $K' = k'G$ and $M_4' = \{H(ID) \bigoplus K_x', (K_x' + R') \bigoplus H(ID)\}$, and sends M_4' to the tag

(e) Tag: Upon receiving M_4', the tag checks that $(M_4'^{(1)} \bigoplus H(ID) + R_x') \bigoplus M_4'^{(2)} = H(ID)$ holds

Therefore, the tag believes that the attacker is a legitimate database, and the successful attack proves that the scheme is unable to resist server impersonation attacks.

(ii) Tag impersonation attack

Supposing that after the attacker intercepting message M_2 that the tag sent to the reader, he can calculate $M(ID) + tP_s = M_0 - R$ and then can impersonate the tag to interact with the reader and database and pass the reader's authentication.

The specific steps are as follows:

(1) Attacker→reader: When the attacker receives query and random number R', he calculates $M_2' = \{M_0 - R + R', P_t + R'\} = \{M_0', P_t + R'\}$ and sends M_2' to the reader

(2) Reader→server: The reader sends $M_3' = \{M_2', R'\}$ to the server

(3) Server: The server computes $M(ID) = M_0' - R' - nP_t = M_0 - R - nP_t = (M(ID) + tP_s) - nP_t$ and compares $M(ID)$ with $M(ID')$ stored locally and finds that it is consistent, so it verifies the fake tag.

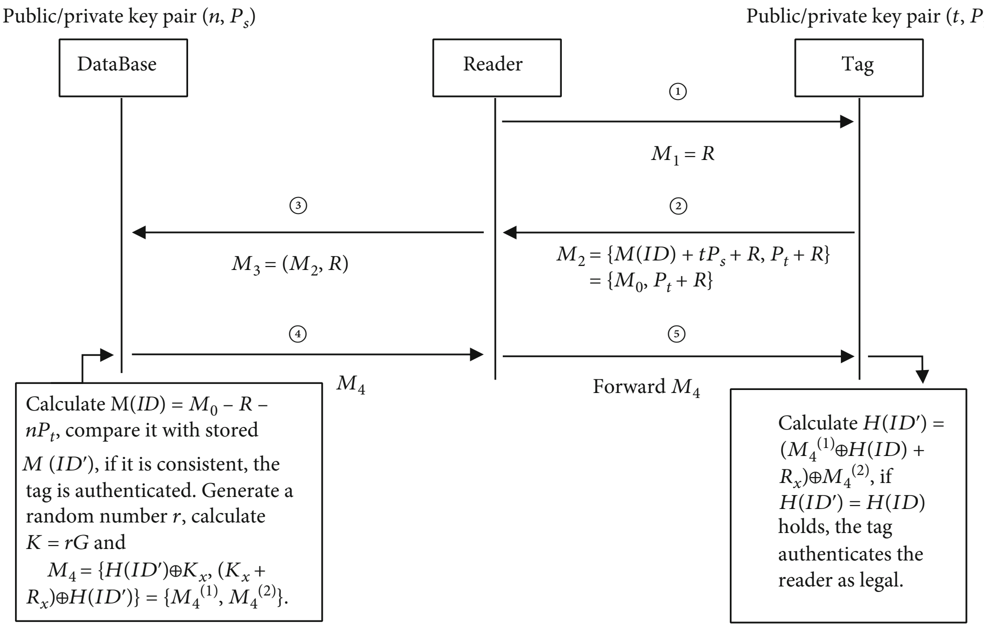
Therefore, the database is made to consider the attacker to be a legitimate tag, and the attack is successful, which proves that the scheme is unable to resist the tag impersonation attack.

At the same time, since the authentication scheme of Qian et al. is difficult to resist server and tag impersonation attacks, it is easy to prove that it cannot resist location tracking attacks nor does it satisfy anonymity and forward security.

4. The Improved Scheme

To resist the above server and tag impersonation attacks, the authentication scheme proposed by Qian et al. has been modified. The detailed process is as follows:

4.1. System Parameter Setting


Public/private key pair (n, P_s)
Public/private key pair (t, P_t)
DataBase
Reader
Tag
①
$M_1 = R$
③
②
$M_3 = (M_2, R)$
$M_2 = \{M(ID) + tP_s + R, P_t + R\}$
$= \{M_0, P_t + R\}$
④
⑤
M_4
Forward M_4

Calculate $M(ID) = M_0 - R - nP_t$, compare it with stored $M\ (ID')$, if it is consistent, the tag is authenticated. Generate a random number r, calculate $K = rG$ and $M_4 = \{H(ID') \oplus K_x, (K_x + R_x) \oplus H(ID')\} = \{M_4^{(1)}, M_4^{(2)}\}$.

Calculate $H(ID') = (M_4^{(1)} \oplus H(ID) + R_x) \oplus M_4^{(2)}$, if $H(ID') = H(ID)$ holds, the tag authenticates the reader as legal.

Figure 1: ECC-based RFID authentication scheme proposed by Qian et al.

Table 1: Comparison of computational overhead of the scheme in this paper and the existing schemes.

	Qian et al.'s scheme [3]	Lee et al.'s scheme [8]	Zhang et al.'s scheme I [11]	Zhang et al.'s scheme II [11]	He et al.'s scheme [15]	Wei et al.'s scheme [16]	Our scheme
Server	3SM+2TA	4SM+2TA	5SM+3TA	3SM+2TA	3SM+4TA	4SM+1TA	4SM +1TA
Tag	1SM+3TA	2SM	2SM	1SM	3SM+4TA	5SM+1TA	4SM +1TA

Table 2: Comparison of communication overhead of the scheme in this paper and the existing schemes.

	Qian et al.'s scheme [3]	Lee et al.'s scheme [8]	Zhang et al.'s scheme I [11]	Zhang et al.'s scheme II [11]	He et al.'s scheme [15]	Wei et al.'s scheme [16]	Our scheme
Server	640 bits	160 bits	160 bits	160 bits	640 bits	640 bits	640 bits
Tag	640 bits	800 bits	960 bits	640 bits	640 bits	960 bits	640 bits

(1) Generate a large prime number q, and $F(q)$ is a finite field, where q represents the number of elements in the finite field.

(2) Choose a safe elliptic curve $y^2 = x^3 + ax + b$, where $a, b \in F(q)$. Select the points on the elliptic curve to form an additive cyclic group $(P, +)$ with order t, and G is a generator of P. The reader, database, and each tag store the elliptic curve parameters $\{q, a, b, G, t\}$ locally.

(3) The server selects $n \in Z_t^*$ as its private key and computes $P_s = nG$ as its public key and selects a random value ID as the identity information of each tag and encodes it as a point on the elliptic curve, denoted as $M(ID)$. The server saves $M(ID)$ and stores its public key P_s together with $M(ID)$ in the memory of the tag.

(4) Select a secure hash function: $H : (P,+) \longrightarrow \{0, 1\}^*$

4.2. The Authentication Process

(1) Reader→tag: The reader generates a random number r_1, computes $R_1 = r_1 G$, and sends $M_1 = \{R_1, \text{Query}\}$ to the tag

(2) Tag→reader: Upon receiving M_1, the tag generates a random number r_2, computes $R_2 = r_2 G$ and $M_2 = H(M(ID) + r_2 P_s) \bigoplus H(r_2 R_1)$, and sends $\{M_2, R_2\}$ to the reader

(3) Reader→database: Upon receiving $\{M_2, R_2\}$, the reader sends $M_3 = \{M_2, R_2, r_1\}$ to the database

(4) Database→reader: Upon receiving M_3, the database uses stored tag identity information ID' to vertify whether $H(M(ID') + nR_2) \bigoplus M_2 = H(r_1 R_2)$ holds. If so, it will compute $M_4 = nR_2$ and send M_4 to the reader

Table 3: Comparison of security performance of the scheme in this paper and the existing schemes.

	Qian et al.'s scheme [3]	Lee et al.'s scheme [8]	Zhang et al.'s scheme I [11]	Zhang et al.'s scheme II [11]	He et al.'s scheme [15]	Wei et al.'s scheme [16]	Our scheme
Mutual authentication	×	×	×	×	×	√	√
Confidentiality of authentication factor	√	√	√	×	√	√	√
Anonymity	×	×	√	×	√	√	√
Practicability	√	√	×	×	√	√	√
Perfect forward security	×	√	√	√	√	√	√
Scalability	√	√	×	×	√	√	√
Resistance to replay attack	√	√	√	√	√	√	√
Resistance to tag impersonation attack	×	×	×	√	√	√	√
Resistance to server impersonation attack	×	×	×	×	×	√	√
Resistance to DoS attack	√	√	×	×	√	√	√
Resistance to location tracking attack	×	×	√	×	√	√	√

√ means providing; × means not providing.

(5) Reader→tag: The reader forwards M_4 to the tag

(6) Tag: Upon receiving M_4, the tag checks whether $M_4 = r_2 P_s$ holds, and if so, the reader and database are authenticated.

5. Security Analysis of the Improved Scheme

(i) Resistance to server impersonation

Assume that the attacker can obtain the tag's internal information $M(ID)$ and uses reader and database impersonation attacks.

(a) Attacker→tag: The attack impersonates the reader to generate a random number r_1', calculates $R_1' = r_1' G$, and sends R_1' to the tag

(b) Tag→fake reader (attacker): Upon receiving R_1', the tag generates a random number r_2', computes $M_2' = H(M(ID) + r_2' P_s) \bigoplus H(r_2' R_1')$, and sends $\{M_2', R_2'\}$ to the fake reader (the attacker)

(c) Fake reader→fake database (attacker): The fake reader sends $M_3' = \{M_2', R_2', r_1'\}$ to the fake database (the attacker)

(d) Fake database: The fake database must forge $M_4' = nR_2'$ to pass the authentication of the tag. Because of the unidirectionality of the hash function, the attacker cannot recover out $M_4' = nR_2' = r_2' P_s$ even though he obtains the $M(ID)$ and uses M_2', R_2', r_1' to calculate $H(M(ID) + r_2' P_s) = M_2' \bigoplus H(r_2' R_1')$. Meanwhile, the attacker cannot obtain the database's private key n or the random number r_2' generated by the tag, so it is unable for him to forge M_4'

(ii) Resistance to tag impersonation

(a) The attacker impersonates the tag to attack: Upon receiving the message $M_1' = \{R_1', \text{Query}\}$ of the reader, the fake tag selects a random number r_2' and calculates $R_2' = r_2' G$. However, it is unable to recover the tag's legal $M(ID)$, so the attack fails because he cannot generate legal authentication information $M_2' = H(M(ID) + r_2' P_s) \bigoplus H(r_2' R_1')$

(b) Assuming that the attacker takes an active attack: The attacker selects a random number r_1', calculates $R_1' = r_1' G$, and sends R_1' to the tag. Upon receiving R_1', the tag generates a random number r_2', computes $R_2' = r_2$ $'G$ and $M_2' = H(M(ID) + r_2' P_s) \bigoplus H(r_2' R_1')$, and sends $\{M_2', R_2'\}$ to the reader. After the attacker intercepts $\{M_2', R_2'\}$, he can calculate $H(r_1' R_2') \bigoplus M_2' = H(M(ID) + r_2' P_s)$, but cannot obtain tag's $M(ID)$ because of the unidirectionality of the hash function

(iii) Resistance to replay attack

In replay attack, the attacker can intercept the reader's past authentication information $M_4 = nR_2 = r_2 P_s$ sent to the tag and resend it to the tag. Upon receiving the replay information, the tag can compute $M_4' = r_2' P_s$ using its current one-time random number r_2'. $M_4 \neq M_4'$, and it can be determined that M_4 is a replay information. The attacker can also intercept the tag's past authentication information $\{M_2, R_2\}$ sent to reader and send it to the reader. Upon receiving $\{M_2, R_2\}$, the reader combines it with the random number r_1' (it currently generates to get $M_3' = \{M_2, R_2, r_1'\}$) and forward M_3' to the database. Upon receiving M_3', the database checks that $H(M(ID') + nR_2) \bigoplus M_2 \neq H(r_1' R_2)$ to identify replay attack.

(iv) Forward security

Forward security ensures that attacker cannot associate the past interaction information with tag's identity. Assume that the attacker can obtain tag's identity information $M(ID)$ and intercept the past interaction information $M_1 = \{R_1, \text{Query}\}$, $\{M_2, R_2\}$, and M_4, among them $R_1 = r_1 G$, $R_2 = r_2 G$, and $M_2 = H(M(ID) + r_2 P_s) \bigoplus H(r_2 R_1)$. Without obtaining one-time random numbers r_1 and r_2 and database's private key n, the attacker cannot confirm the intercept information M_1, $\{M_2, R_2\}$, and M_4 is related to the tag's identity $M(ID)$ that he knows.

(v) Mutual authentication

The attacker can eavesdrop on the information passed between the reader and tag to get the message $M_2 = H(M(ID) + r_2 P_s) \bigoplus H(r_2 R_1)$. Due to the unidirectionality of hash function, he cannot get $M(ID)$, so he cannot generate the legitimate information that can pass authentication. At the same time, the database can use stored ID' to check whether $H(M(ID') + nR_2) \bigoplus M_2 = H(r_1 R_2)$ holds to authenticate the tag. In addition, in the authentication process of the tag to reader, the tag authenticates reader by verifying whether $M_4 = r_2 P_s$ is true. If the attacker does not have private key n of the legitimate database or the one-time random number r_2, it is difficult to calculate M_4 and unable to pass the authentication of the tag.

(vi) Confidentiality of the identity information $M(ID)$

In the improved scheme in this paper, the $M(ID)$ information of the tag is only contained in M_2. Due to the unidirectionality of hash function, the attacker cannot intercept the previous interaction information between the reader and tag to obtain the tag's legitimate $M(ID)$. Similar to the antitag impersonation attack analysis mentioned above, the attacker is also difficult to obtain the tag's $M(ID)$ through active attack.

(vii) Resistance to location tracking attack

We assume that the attacker has mastered the tag's $M(ID)$ and intercepted the interaction information M_1, M_2, R_2. Since the attacker cannot obtain the database's private key n, the reader's random number r_1, and the tag's random number r_2, so it is impossible to use $H(M(ID) + nR_2) \bigoplus M_2 = H(r_1 R_2)$ to associate the intercepted interaction information with a specific tag. Therefore, the improved scheme can resist location tracking attack.

(viii) Anonymity

Anonymity of the scheme requires that the attacker cannot associate the interaction information with tag's identity. According to the previous analysis, it is difficult for an attacker to recover the tag's $M(ID)$ from the interaction information between the reader and tag, and each interaction uses different random numbers r_1 and r_2, so the attacker cannot associate the interaction information with tag's specific identity, which ensures the anonymity.

(ix) Resistance to denial-of-service (DOS) attack

From the above analysis of the confidentiality of the tag's $M(ID)$, it can be seen that the tag's $M(ID)$ can be well protected, and it is difficult for an attacker to obtain the tag's $M(ID)$ from the interaction information between the reader and the tag. Therefore, the authentication scheme in this paper does not need to update tag's $M(ID)$, which can effectively resist DOS attack.

6. Efficiency and Security Performance Comparisons

We compared the computing efficiency, communication overhead, and security of the improved authentication scheme with similar schemes. For the convenience of comparison, the scalar dot product operation on the elliptic curve is denoted as SM and the point addition operation as TA. At the same time, assume that all schemes use the elliptic curve with a key length of 160 bits, and the data length of a point on the elliptic curve is 320 bits. Table 1 shows the comparison of computational overhead between the schemes in References [3, 8, 11, 15, 16] and the schemes in this paper, among which scheme I in [11] refers to the improvement of EC-RAC scheme, and scheme II in [11] refers to the improved scheme of Schnorr authentication scheme.

The communication overhead refers to the length of the authentication information transmitted by the server and the tag during the execution of the authentication scheme. Table 2 gives the comparison of communication overhead between the schemes in [3, 8, 11, 15, 16] and the improved schemes. Only the length of communication data between the server (or reader) and the tag is considered here, and data interactions between the server and reader are ignored.

It can be seen from Table 2 that the length of data transmitted by the tag and server in the scheme in this paper is basically equal to that in the schemes in [3, 15]. Table 3 shows the comparison of security performance between the proposed scheme and the existing schemes.

Through the above analysis, the scheme proposed in this paper is basically the same as the original scheme in terms of computational and communication overhead, which can satisfy the practical application of low-cost tags, but compared with other typical schemes with similar structure, this scheme has a superior security advantage, which can fully meet various security requirements such as mutual authentication and privacy protection in the RFID authentication process.

7. Conclusion

This paper analyzes the security performance of the improved scheme proposed by Qian et al. and proves that it is difficult to resist server and tag impersonation and thus cannot realize the mutual authentication between the server and the tag. On this basis, we improved the scheme proposed by Qian et al. Security analysis and efficiency comparison show that compared with similar schemes, the proposed scheme has higher security while ensuring high computing performance and can fully meet the security requirements of mutual authentication and privacy protection in the RFID authentication process.

Data Availability

The experimental data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] C. Roberts, "Radio frequency identification (RFID)," *Journal of Computer Security*, vol. 25, no. 1, pp. 18–26, 2006.

[2] M. Burmester, B. Medeiros, and R. Motta, *Anonymous RFID Authentication with Constant Key-Lookup*, ACM, 2007, Cryptology ePrint Archive: Listing for 2007 (2007/402).

[3] Q. Qian, Y.-L. Jia, and R. Zhang, "A lightweight RFID security scheme based on elliptic curve cryptography," *International Journal of Network Security*, vol. 18, no. 2, pp. 354–361, 2016.

[4] Y. Chen, J. S. Chou, and H. M. Sun, "A novel mutual authentication scheme based on quadratic residues for RFID systems," *Computer Networks*, vol. 52, no. 12, pp. 2373–2380, 2008.

[5] T. Cao, P. Shen, and E. Bertino, "Cryptanalysis of some RFID authentication protocols," *The Journal of Communication*, vol. 3, no. 7, pp. 20–27, 2008.

[6] T. C. Yeh, C. H. Wu, and Y. M. Tseng, "Improvement of the RFID authentication scheme based on quadratic residues," *Computer Communications*, vol. 34, no. 3, pp. 337–341, 2011.

[7] R. Doss, S. Sundaresan, and W. Zhou, "A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems," *Ad Hoc Networks*, vol. 11, no. 1, pp. 383–396, 2013.

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

[9] T. Van Deursen and S. Radomirovic, *Attacks on RFID Schemes [EB/OL]*, ACM, 2008, Cryptology ePrint Archive, Report 2008/310, 2008. http://eprint.iacr.org/.

[10] J. Bringer, H. Chabanne, and T. Icart, "Cryptanalysis of EC-RAC, a RFID identification scheme," in *CANS, volume 5339 of Lecture Notes in Computer Science*, pp. 149–161, Springer, 2008.

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

[12] P. Babaheidarian, M. Delavar, and J. Mohajeri, "On the security of an ECC based RFID authentication scheme," in *2012 9th International ISC Conference on Information Security and Cryptology*, Tabriz, 2012.

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

[14] R. Peeters and J. Hermans, *Attack on Liao and Hsiao's Secure ECC Based RFID Authentication Scheme Integrated with ID-Verifier Transfer Scheme [EB/OL]*, ACM, 2013, Cryptology ePrint Archive, Report 2013/399, http://eprint.iacr.org/.

[15] D. He, N. Kumar, N. Chilamkurti, and J.-H. Lee, "Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol," *Journal of Medical Systems*, vol. 38, no. 10, pp. 116–118, 2014.

[16] W. Guoheng, Q. Yanlin, and Z. Huanguo, "Security authentication scheme for lightweight radio frequency identification based on ECC," *Journal Huazhong University of Science and Technology (Natural Science Edition)*, vol. 46, no. 1, 2018.