Tripartite Authentication Protocol RFID/NFC Based on ECC

Yong-Shuang Wei and Jian-hua Chen
(Corresponding author: Yong-Shuang Wei)

Department of Mathematics and Statistics, Wuhan University
No. 299, Bayi Road, Wuchang 430072, Wuhan, China
(Email: yongshuang_wei@163.com)

(Received Mar. 9, 2019; Revised and Accepted Sept. 6, 2019; First Online Nov. 10, 2019)

Abstract

An RFID security three-party mutual authentication protocol based on elliptic curve cryptography (ECC) is designed in this paper. The proposed protocol not only satisfies most of basic characteristics of RFID system, such as mutual authentication, confidentiality, anonymity and others, but also resists tracking attack, denial of service attack, spoofing attack, *etc.* Being different from other RFID authentication protocols, our protocol is based on the assumption that the communication between reader and background is unsafe, so that tag, reader and background can mutually authenticate each other. In addition, the protocol provides a public secret co-negotiating key for the three participants to read and modify data in subsequent communication. According to the design of the protocol, it can apply to NFC system, which is evolved from the integration of RFID technology and interoperability technology. We further analyze the security of the protocol through the Burrows-Abadi-Needham logic (BAN-logic), which shows that the protocol can achieve mutual authentication and key agreement, as well as agree with RFID and NFC system.

Keywords: BAN Logic; ECC; Key Negotiation; RFID/NFC; Tripartite Authentication

1 Introduction

Radio Frequency Identification (RFID) is an emerging automatic identification technology developed in the 1980s. RFID technology uses a radio frequency signal to send and receive contactless information to authentication, through spatial coupling, that is alternating or electromagnetic field [18]. As the core supporting technology of the Internet of Things (IoT), RFID technology is widely used in logistics, transportation, medicine and industrial manufacturing, *etc.* And a complete RFID system consists of a reader, an electronic tag and a background sever.

Near Field Communication (NFC) technology, as a wireless peer-to-peer communication technology in the IoT, which is evolved from the integration of contactless RFID and interoperability technology, has made a good figure in the electronic payment and smart media. Compared with an RFID system, the slight difference is that an NFC device must be able to be a reader as well as a tag, and the connection between the background and the reader uses a wireless connection, thus we can treat an NFC device as a special RFID system [5, 8, 10].

With the rapid development and widespread application of RFID/NFC technology, the security and privacy issues of RFID/NFC systems have become increasingly prominent. It is currently the most effective method to protect the security and privacy of RFID systems by designing a high security authentication protocol with Public Key Cryptosystem (PKC). Under the premise of the same security in PKC, the elliptic curve cryptosystem (ECC) has become the preferred cryptosystem of RFID authentication protocol, due to its short key length, fast calculation speed and small occupied bandwidth [16, 22–26].

2 Related Work

In studies of RFID authentication protocol based on ECC, most of them focus on the security and efficiency. We briefly review these concerned works from two aspects: The basic security and the efficiency of security defense their protocol provide, and the goal of our proposed protocol.

2.1 Previous Research

As we all know, the RFID security authentication protocol based on ECC has become a hot spot. In 2007, Batina *et al.* [4] discussed the feasibility of an identification protocol based on ECC of the RFID tag, but the confidentiality of the tag's public key is not guaranteed, while the attacker can still obtain its public key, then the tag is tracked. In 2008, Lee *et al.* [12] proposed an ECC-based RFID authentication protocol, while the protocol

isn't resistant to spoofing and tracking attacks. In 2014, Moosavi *et al.* [15] gave a RFID authentication protocol relying on ECC and D-Quark lightweight ash, claiming that its solution is suitable for providing secure and resource-limited RFID implant system, but the required calculation time is not optimized when the tag still needs to calculate elliptic curve multiplication. In 2015, the ECC-based RFID protocol conceived by Ryu *et al.* [17] had a relatively good performance, however it couldn't provide the most basic mutual authentication. In 2016, Kang [9] analyzed and proposed an improved ECC-based RFID Grouping-proof authentication protocol to solve the problem existing grouping-proof protocols such as low grouping-proof efficiency, vulnerability to spoofing attack, tracking attack and other security threats. But it still can't prevent the illegal tag interference with reader authentication and the tag spoofing attack. In 2018, Zhang *et al.* [28] proposed an RFID mutual authentication protocol based on ECC, when thoroughgoing analysis shows that the interactive information C does not contain the information of the random point R_R of the reader, can't resist replay attack on the reader. In 2018, Chen *et al.* [6] proposed a multi-channels constructing method to build protocol model for formal analysis, then used it to verify RFID three-party authentication protocol based on NTRU cryptosystem, the result shows that an attack exists in this protocol. In 2019, Aghili *et al.* [1] shows that the protocol proposed by Fan *et al.* is vulnerable to secret disclosure and reader impersonation attacks. Moreover, they improved it to a protocol that is resistant to the attacks presented in the paper and the other known attacks in the context of RFID authentication.

2.2 Our Target

Through a large amount of literature analysis, we can know that almost all RFID authentication protocols are based on the assumption that the communication between the reader and the background is secure. We can only say that the back-end wired communication is more secure than the front-end over-the-air wireless transmission, but the system still faces the security problems that are common in traditional computer networks, which has a great impact on the security of the authentication protocol. Thus it's unreasonable to assume it's secure [16]. The protocol proposed in our paper negates this assumption. In addition, the difference between the NFC system and the RFID system is analyzed. This paper aims to design a security tripartite mutual authentication protocol based on ECC that is universal to RFID/NFC, which will be more practical.

3 The RFID/NFC Protocol Based on ECC

We introduce our tripartite authentication protocol RFID/NFC based on ECC in this section firstly. Then the two phases' details of our protocol: initialization and authentication, are described as follow.

3.1 Protocol Description

We propose a security RFID/NFC tripartite authentication protocol based on ECC, with good security and anti-attack capabilities. Our paper doesn't support the assumption that the connection of the background and the reader is a wired connection so that the channel between them is safe. Therefore, the protocol proposed in the paper can also be applicable to NFC, which the communication between reader and background is insecure, and has better practicability.

3.2 Initialization Phase

Definition of the relevant symbols in the protocol are explained in Table 1.

Table 1: Summary of symbols in our protocol

Symbol	Symbol's Description
P	Base point on the elliptic curve
R_S, R_P	Private and public key of Reader
T_S, T_P	Private and public key of Tag
r_R, r_T	Random number
AR, AT	Authentication information
VR, VT, VB	Verification information
K_T, K_R, K_B	Co-negotiating secret key

In the initialization phase, the reader randomly selects a number R_S as its private key and calculates its public key $R_P = [R_S]P$ accordingly. While the tag does the same thing, randomly selects a random number T_S as its private key, and calculates its corresponding public key $T_P = [T_S]P$. We specify the public key of the tag as its unique identifier in our protocol. The background server stores the public and private keys of both the reader and the tag. Each tag stores its own public and private key information and the public key of the reader, while the reader only stores its own public and private key information for RFID system, plus the public key of tag for NFC system.

3.3 Authentication Phase

As shown in Figure 1, the specific mutual authentication process among the tag, the reader, and the background is as follows:

Step 1: The reader chooses a random integer number r_R that belongs to Z_q, and calculates the point $R_R = [r_R]P$ on the elliptic curve, then sends an query and R_R to the tag.

Step 2: The tag also selects a random integer r_T in Z_q, calculating the corresponding point $R_T = [r_T]P$ on

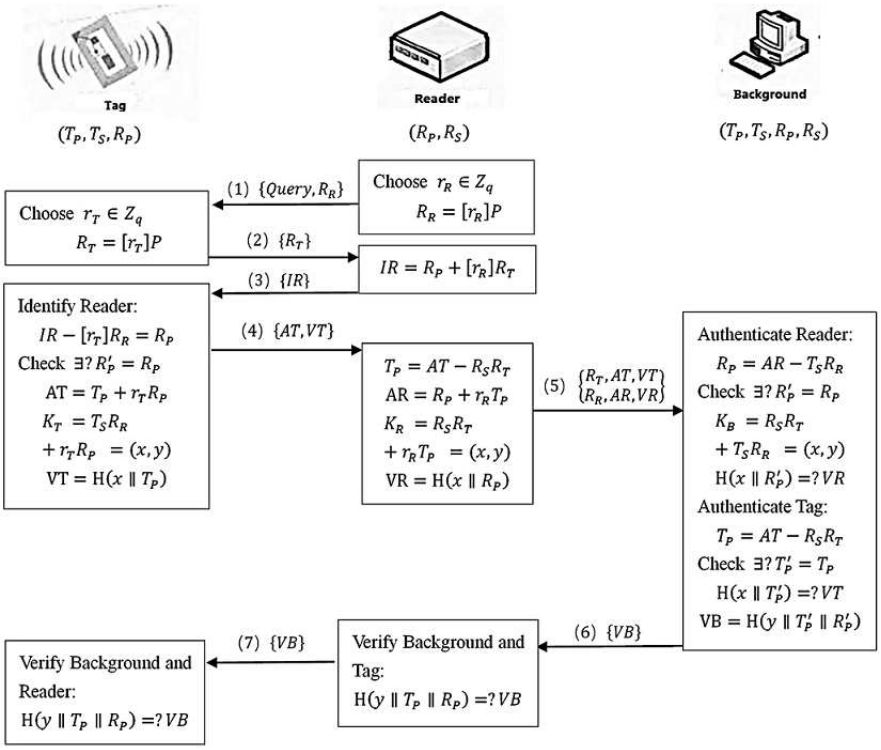

Figure 1: ECC-based RFID/NFC authentication protocol

the elliptic curve. Then it sends R_T to respond the reader.

Step 3: The reader calculates the $IR = R_P + [r_R]R_T$ and sends it, so that the tag identify the reader.

Step 4: The tag identify the reader by counting $R_P = IR - [r_R]R_T$, and it searches whether there is a R'_P equal to R_P. If established, the tag thinks the reader is legal and calculates the Authentication variable $AT = T_P + r_T R_P$ of the tag. What's more, it is possible to calculate the co-negotiating secret key $K_T = T_S R_R + r_T R_P = (x, y)$, and finally calculates the tag verification amount $VT = H(x \| T_P)$for background verification. Then sends AT, VT to the reader.

Step 5: The reader calculates $T_P = AT - R_S R_T$ from the received AT, and counts its authentication variable $AR = R_P + r_R T_P$, co-negotiating secret key $K_R = R_S R_T + r_R T_P = (x, y)$, and the verification variable $VR = H(x \| R_P)$ for the background authenticate the reader. Then the associated amount of the tag and the reader R_T, AT, VT, R_R, AR, VR are passed to the background server.

Step 6: After receiving the message transmitted by the reader, the background server first verifies the legitimacy of the reader by calculating the $R_P = AR - T_S R_R$, and then retrieves whether it's the same as the stored R'_P or not. If it exists, the background calculates the co-negotiating secret key $K_B = R_S R_T + T_S R_R = (x, y)$, and $H(x \| R'_P)$ to check whether it is equal to VR or not. After the reader passing the verification, the background verifies whether the information of tag collected by the reader is legal, calculating the $T_P = AT - R_S R_T$, and retrieves whether there is corresponding T'_P in the repository. Based on it, the background calculates $H(x \| T'_P)$ and judges whether it is equal to VT. Finally, the background calculates its authentication variable $VB = H(y \| T'_P \| R'_P)$ for the reader and the tag to authenticate the legitimacy of the background server, and sends it to the reader.

Step 7: The reader verifies the background server and the tag, when calculated $H(y \| T_P \| R_P)$ and judged whether it is equal to the received VB. And it sends VB to the tag.

Step 8: Lastly, based on the information that the tag receives, the tag verifies the legitimacy of the reader and the background by calculating whether $H(y \| T_P \| R_P)$ is equal to VB. The mutual authentication among the tag, the reader and the background is accomplished, and K_T, K_R, K_B are the same, as a session key is used for subsequent communication.

4 Security Analysis

A safe RFID/NFC system should be able to provide mutual authentication, confidentiality, anonymity, forward security, scalability. As well as resist tracking attack, denial of service attack, spoofing attack, and replay

attack, *etc.* [11,20,27,30] Besides, considering the practicality of RFID/NFC, it should also be able to provide a co-negotiating secret key for subsequent communication. The security performance and scalability of the protocol in our paper has been greatly improved, satisfying the basic security requirements as mentioned above.

4.1 Qualitative Analysis

We give qualitative analysis of our protocol from nine aspects:

- **Mutual authentication:** The tag verifies the reader by judging $R_P^{'} = R_P$ to preliminarily certificate; then it uses K_T to authenticate the background and the reader further with VB.

  To the reader, it also authenticates the background with VB, K_R. Furthermore, VB from the background contains the legal public key T_P of the tag, and the reader can confirm the validity of the tag through the background ulteriorly.

  When received the information, the background retrieves whether there is $R_P^{'} = R_P$, to initially determine that the reader is legal; then uses K_B, VB to authenticate the reader. In the same way, the certification of the tag in the background can be obtained. As a result, the protocol completes the mutual authentication of the three parties.

- **Confidentiality:** In the process of authentication, the public key T_P of the tag is used as its unique identifier, which is calculated by $T_P = AT - R_S R_T$. The public key of the reader is also calculated by $R_P = IR - [r_R]R_T$. Both of them don't transmitted on the channel. Even if the attacker intercepts the interactive information $R_R, R_T, AR, AT, VR, VT, VB$ on the wireless channel, due to the discrete logarithm problem of elliptic curve and the randomness and unipolarity of the Hash function which are unable to be solved based on today's computer calculation, either T_P or R_P is not derived. This ensures the confidentiality of the tag identity and the reader's public key.

- **Anonymity:** As we know, neither the public key of the tag T_P nor the reader R_P is transmitted over the channel directly. Due to the security of the elliptic curve cryptosystem, the attacker can't calculate the corresponding private key and the identity of the parties from the interaction information. So the protocol can provide anonymity of the tag, the reader and the background.

- **Forward security:** Assuming that the attacker can attack on the maximum degree, which gets the public key T_P, R_P and all the interaction information $\{R_R, R_T, AR, AT, VR, VT, VB\}$, the attacker still can't calculate the random number r_R, r_T through these, let alone T_S, R_S. Thus it is impossible to bind the obtained interactive information with the specific tag or the reader, and the protocol has good forward security.

- **Scalability:** For RFID system, the reader doesn't need to store the unique identifier T_P of the tag by calculating it, therefore, a large memory reduction can be achieved for a large number of tags. Similarly, if the memory requires high memory, the tag do the same thing to calculate R_P instead of storing it [19]. But it does in NFC system. In addition, since the public key are used as the unique identifier, the identity validity period can be added to the identity identifier, when the identity is invalid, it can no longer participate in encryption and decryption and authentication, which makes the protocol more practical.

- **Resist tracking attack:** According to the confidentiality, the attacker can't get T_P, R_P. The reader and the tag will generate new random numbers in each new session, hence the interaction information is also fresh at each time. Unpredictable changes in the session make it impossible for the attacker to track the tag or the reader.

- **Resist denial of service attack (DoS attack):** The guarantee of anonymity enables T_P and R_P to be effectively protected, and the private keys of them don't need to be updated, as a result, the shared secret information doesn't need to be updated synchronously among the tag, the reader and the background. In consequence, the protocol can resist denial of service attack.

- **Resist spoofing attack:** If the attacker wants to impersonate a legitimate tag to deceive the reader, it needs to forge a legitimate authentication message R_T, AT, VT, since there is no legal tag identity T_P and T_S, and K_T. The attacker can't generate valid authentication messages AT, VT, so that it can't deceive the background. In case that the attacker wants to impersonate a legitimate reader to spoof the tag, it is necessary to forge a legitimate authentication message AR, VR, but it can't calculate T_P, and K_R. At this point, the attacker is even more impossible to spoof the background.

  Assume that the attacker wants to impersonate the background spoofing the tag and the reader, it's necessary to forge a legitimate authentication message VB. Because there is no legal T_P, R_P, and K_B, the attacker can't generate a valid VB. The protocol is resistant to spoofing attack.

- **Resist replay attack:** Suppose the attacker replays the tag by intercepting the interactive information R_R and AR, VR. While the tag generates a new random number r_T in each session, and it can pass the verification $H(y \| T_P \| R_P) = ?VB$ to determine

whether it is attacked. It's Similar to the reader. For this reason, the protocol resists replay attack.

4.2 Formal Analysis

The formal analysis method is a standardized method, judging whether the authentication protocol itself meets the security objectives, and whether there are security vulnerabilities. It is divided into a structural method based on reasoning, an attack-based structural method and a theorem-based proof method. Burrows-Abadi-Needham (BAN) logic [3, 21] is an industry-recognized milestone in the formal analysis for security authentication protocols. BAN-based logic is widely used in the field of authentication protocol analysis. In this subsection, we adopt the widely-accepted BAN logic to demonstrate that the proposed authentication protocol guarantees mutual authentication and secure session key establishment between the communicating parties.

4.2.1 Basic Terms of BAN Logic

We explain the important notations of BAN logic in Table 2.

Table 2: Notations of BAN logic

Notation	Notation's Description
$P \models X$	P trusts the statement X
$P \lhd X$	P sees X
$P \mid\sim X$	P once said X
$P \Rightarrow X$	P can rule X
$P \overset{SK}{\leftrightarrow} Q$	P and Q share the secret key SK to communicate between each other
$\overset{K}{\longrightarrow} P$	K is the public key of P
$P \overset{X}{\rightleftharpoons} Q$	X is secret information between P and Q
$\#(X)$	X is fresh
$\{X\}_K$	Ciphertext obtained by encrypting X with key K
(X, Y)	X or Y is one part of (X,Y)

Next, the inference rules of BAN logic are shown.

Rule 1: Message-meaning Rule:

$$\frac{P \models P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \models Q \mid\sim X}$$

Rule 2: Jurisdiction Rule:

$$\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$$

Rule 3: Nonce-verification Rule:

$$\frac{P \models \#(X), P \models Q \mid\sim X}{P \models Q \models X}$$

Rule 4: Belief Rule:

$$\frac{P \models X, P \models Y}{P \models (X, Y)}$$

Rule 5: Freshness Rule:

$$\frac{P \models \#(X)}{P \models \#(X, Y)}$$

Rule 6: Message-sink Rule:

$$\frac{P \models P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \lhd X} \qquad \frac{P \lhd (X, Y)}{P \lhd X}$$

Rule 7: Hash Rule:

$$\frac{P \models Q \mid\sim H(X), P \lhd X}{P \models Q \mid\sim X}$$

4.2.2 BAN Logic Analysis of Protocol

There are three participants in our protocol, include T(tag), (R)reader, and B(background).In the protocol for RFID system, T stores the public key of R; for NFC system, R, which is also as tag now, stores the public key of T, which is as the reader at the same time. The background holds the public and private keys of both T and R, while there is no assumption that communication between R and B is safe. We use BAN logic to formally analyze the protocol in following part, which is mainly divided into message idealization, initialization hypothesis, security goal and certification process.

- **Message Idealization:**

$$T \lhd \{R_R, \{R_P\}_{R_P}, H(y \| T_P' \| R_P')\} \quad (1)$$

$$R \lhd \{T_R, \{T_P, r_T\}_{T_P}, H(x \| T_P), H(y \| T_P' \| R_P')\} \quad (2)$$

$$B \lhd \{R_T, \{T_P, r_T\}_{T_P}, H(x \| T_P), R_R, \{R_P, r_R\}_{R_P}, H(x \| R_P)\}$$

- **Initialization Hypothesis:**
  H_1: **Validity of the keys**

$$T \models T \overset{R_P}{\longleftrightarrow} R \quad (3)$$

$$R \models R \overset{T_P}{\longleftrightarrow} T \quad (4)$$

$$T \models T \overset{T_P'}{\longleftrightarrow} B$$

$$B \models B \overset{T_P}{\longleftrightarrow} T$$

$$R \models R \overset{R_P'}{\longleftrightarrow} B$$

$$B \models B \overset{R_P}{\longleftrightarrow} R$$

H_2: **Authority of the subjects**

$$T \models R|\Rightarrow R_P \quad (5)$$
$$R \models T|\Rightarrow T_P \quad (6)$$
$$T \models B|\Rightarrow T_P^{'}$$
$$B \models T|\Rightarrow T_P$$
$$R \models B|\Rightarrow R_P^{'}$$
$$B \models R|\Rightarrow R_P$$

H_3: **Freshness of random numbers**

$$T \models \#(R_R) \quad (7)$$
$$R \models \#(R_T) \quad (8)$$

- **Security Goal:**
There are two main goal to achieve, where we first to authenticate the tag, reader and background to each other, then show that they agree on a session key.

G_1: **Primary goal**

$$T \models T \overset{K_T}{\longleftrightarrow} R$$
$$R \models R \overset{K_R}{\longleftrightarrow} T$$
$$R \models R \overset{K_R}{\longleftrightarrow} B$$
$$B \models B \overset{K_B}{\longleftrightarrow} R$$

where $K_T = K_R = K_B$.

G_2: **Secondary goal**

$$T \models R|\equiv T \overset{K_T}{\longleftrightarrow} R$$
$$R \models T|\equiv R \overset{K_R}{\longleftrightarrow} T$$
$$R \models B|\equiv R \overset{K_R}{\longleftrightarrow} B$$
$$B \models R|\equiv B \overset{K_B}{\longleftrightarrow} R$$

- **Certification Process:**
Proof of G_1:
From Equations (1), (3), and Rule 1: $\frac{P|\equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P|\equiv Q|\sim X}$. We have

$$T|\equiv R|\sim (R_R, \{R_P\}_{R_P}, H(y\|T_P^{'}\|R_P^{'})) \quad (9)$$

From Equation (7) and Rule 5: $\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$. Derive

$$T|\equiv \#(R_R, \{R_P\}_{R_P}, H(y\|T_P^{'}\|R_P^{'})) \quad (10)$$

From Equations (9), (10), and Rule 3: $\frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$. With

$$T|\equiv R|\equiv (R_R, \{R_P\}_{R_P}, H(y\|T_P^{'}\|R_P^{'})) \quad (11)$$

From Equation (11) and Rules 3, 5. We can get

$$T|\equiv R|\equiv (R_P, H(y\|T_P^{'}\|R_P^{'}))$$
$$T|\equiv R|\equiv \#(R_P, H(y\|T_P^{'}\|R_P^{'}))$$

From Equations (5) and (6), there is

$$T|\equiv T \overset{K_T}{\longleftrightarrow} R,\ T|\equiv \#(K_T) \quad (12)$$

From Equations (2), (4), and Rule 1, have

$$R|\equiv T|\sim \{R_T, \{T_P, r_T\}_{T_P}, H(x\|T_P), H(y\|T_P^{'}\|R_P^{'})\} \quad (13)$$

From Equations (13) and (8), get

$$R|\equiv T|\equiv R \overset{K_R}{\longleftrightarrow} T \quad (14)$$

From Equations (14) and (6), we know

$$R|\equiv R \overset{K_R}{\longleftrightarrow} T$$

One part of G_1 is certified, proof of the rest can be obtained by analogy.

Proof of G_2
From Equation (1) and Rule 6: $\frac{P \lhd (X,Y)}{P \lhd X}$. we have

$$T \lhd H(y\|T_P^{'}\|R_P^{'}) \quad (15)$$

From Equations (12), (15), and Rule 1, with

$$T|\equiv R|\sim K_T \quad (16)$$

From Equations (12) and (16) again, we final get

$$T \models R|\equiv T \overset{K_T}{\longleftrightarrow} R$$
$$R \models T|\equiv R \overset{K_R}{\longleftrightarrow} T$$

The similar to the other part of G_2.

4.2.3 Conclusion of Formal Analysis

In summary, the BAN logic formal analysis method proves that the proposed protocol can achieve the expected goal, and also shows that the protocol is safe and reliable in theory.

5 Performance Analysis

In this section, we analyze the performance of the improved protocol from two aspects: The practical advantage and the security comparison with other protocol.

5.1 Practical Advantage

The existing ECC-based security authentication protocol of RFID face the threat brought by the traditional computer network even the traditional computer network communication. So the assumption that the communication between reader and background is secure, which is obviously unreasonable. The protocol in our paper abandons this hypothesis and makes it more scientific.

Beyond that the protocol negotiates the secret key $K_T = K_R = K_B$ in the authentication process, which facilitates subsequent communication between each other. Based on this, the tag can support the reading and writing function, so that information of the target can be updated at any time in real life. This is also not available in many current RFID protocols. All of these improvements makes the tag can be used as a reader as well, so our protocol can be applied to NFC systems, which is more practical.

5.2 Security Comparison

We have shown the security analysis of our protocol above, now we compare our protocol to the latest related protocols in terms of security [2].

Table 2 shows the security comparison of our protocol to Zhang *et al.*'s protocol [29], Liao *et al.*'s protocol [13], Liu *et al.*'s protocol [14] from the necessary security of RFID system, where "$\surd$" means satisfy, "$\times$" means not satisfy.

Table 3: Security properties comparison

Requirements	[29]	[13]	[14]	Our
Mutual authentication	$\times$	$\surd$	$\surd$	$\surd$
Confidentiality	$\surd$	$\surd$	$\times$	$\surd$
Anonymity	$\surd$	$\surd$	$\surd$	$\surd$
Forward security	$\surd$	$\surd$	$\surd$	$\surd$
Scalability	$\times$	$\times$	$\times$	$\surd$
Tracking attack	$\surd$	$\surd$	$\surd$	$\surd$
DoS attack	$\times$	$\surd$	$\times$	$\surd$
Spoofing attack	$\surd$	$\surd$	$\surd$	$\surd$
Replay attack	$\surd$	$\surd$	$\surd$	$\surd$
Mobile environment	$\times$	$\times$	$\times$	$\surd$

As illustrated in Table 3, Zhang *et al.*'s protocol only satisfies one-way authentication from the reader to the tag. Our protocol not only satisfies the two-way authentication of the tag and the reader, but also contents the mutual authentication among the tag, the reader and the background. Liu *et al.*'s protocol doesn't meet the basic confidentiality, and our protocol can solve this problem well. Both Zhang *et al.*'s protocol and Liu *et al.*'s protocol are not resistant to denial of service attack. Instead, our protocol is resistant to multiple attacks including denial of service attack. In addition, all of them have no scalability, which is necessary to the large-scale application of RFID in the IoT, while the tag that our protocol can satisfy and has good scalability. Relatively speaking, our protocol is also applicable to NFC, so only it can be applied to smart device environments such as mobile phones.

6 Conclution

A security tripartite authentication protocol based on ECC of RFID/NFC system is designed in our paper. Since we assume that the communication between reader and background is insecure, tag, reader and background can achieve mutual authentication, which is more scientific and reasonable. Apart from this, they negotiate a secret co-negotiating key for subsequent communication. We through qualitative analysis the basic security of the protocol, and the result show that our protocol can provide mutual authentication, confidentiality, anonymity,etc. As well as resist tracking attack, denial of service attack, spoofing attack, *etc.* Then we further formal analyze the security and aim of our protocol by the BAN logic, while result of the analysis indicated that our protocol achieves the goals that tripartite authentication and key agreement. Compare our protocol to the latest related protocols in security, we can know that our protocol has greater security and better availability. Besides, the protocol, where uses the public key as the identity of tag or reader can provide and add more information to it. To sum up, it can not only solve the problem effectively, which current and potential security issues faced by current RFID systems, but also be applied to NFC systems.

References

[1] S. F. Aghili and H. Mala, "Security analysis of an ultra-lightweight RFID authentication protocol for m-commerce," *International Journal of Communication Systems*, vol. 32, no. 3, pp. e3837, 2019.

[2] P. Alexander, R. Baashirah, and A. Abuzneid, "Comparison and feasibility of various RFID authentication methods using ECC," *Sensors*, vol. 18, no. 9, pp. 2902, 2018.

[3] A. Arfaoui, A. Kribeche, and S. M. Senouci, "Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications," *Computer Networks*, vol. 159, pp. 23–36, 2019.

[4] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*, pp. 217–222, 2007.

[5] S. Bojjagani and V. N. Sastry, "A secure end-to-end proximity NFC-based mobile payment protocol," *Computer Standards & Interfaces*, pp. 103348, 2019.

[6] J. Chen, M. Xiao, K. Yang, W. Li, and X. Zhong, "Formal analysis and verification for three-party authentication protocol of RFID," in *National Conference of Theoretical Computer Science*, pp. 46–60, 2018.

[7] Y. L. Chi, C. H. Chen, I. C. Lin, M. S. Hwang, "The secure transaction protocol in NFC card emulation mode," *International Journal of Network Security*, vol. 17, no. 4, pp. 431–438, 2015.

[8] T. H. Feng, M. S. Hwang, and L. W. Syu, "An authentication protocol for lightweight NFC mobile sensors payment," *Informatica*, vol. 27, no. 4, pp. 723–732, 2016.

[9] K. Hong-yan, "Analysis and improvement of ECC-based grouping-proof protocol for RFID," *International Journal of Control and Automation*, vol. 9, no. 7, pp. 343–352, 2016.

[10] W. Huo, Q. Dong, and Y. Chen, "ECC-based RFID/NFC mutual authentication protocol," in *The 2nd International Workshop on Materials Engineering and Computer Sciences*, 2015. DOI: 10.2991/iwmecs-15.2015.31.

[11] M. Khalid, U. Mujahid, and N. ul I. Muhammad, "Ultralightweight RFID authentication protocols for low-cost passive RFID tags," *Security and Communication Networks*, vol. 2019, pp. 25, 2019.

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

[13] 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.

[14] G. Liu, H. Zhang, F. Kong, and L. Zhang, "A novel authentication management RFID protocol based on elliptic curve cryptography," *Wireless Personal Communications*, vol. 101, no. 3, pp. 1445–1455, 2018.

[15] 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.

[16] Y. Pan, Z. Shan, Q. Dai, and F. Yue, "CPK-ECC based mutual authentication protocol for large-scale RFID system," *Journal on Communications*, vol. 38, no. 8, pp. 165–171, 2017.

[17] E. K. Ryu, D. S. Kim, and K. Y. Yoo, "On elliptic curve based untraceable RFID authentication protocols," in *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, pp. 147–153, 2015.

[18] H. Shen, J. Shen, M. K. Khan, and J. H. Lee, "Efficient RFID authentication using elliptic curve cryptography for the internet of things," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5253–5266, 2017.

[19] X. Tan, M. Dong, C. Wu, K. Ota, J. Wang, and D. W. Engels, "An energy-efficient ECC processor of UHF RFID tag for banknote anti-counterfeiting," *IEEE Access*, vol. 5, pp. 3044–3054, 2016.

[20] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1085–1102, 2017.

[21] L. Tingyuan, L. Xiaodong, Q. Zhiguang, and Z. Xuanfang, "An improved security protocol formal analysis with ban logic," in *International Conference on Electronic Commerce and Business Intelligence*, pp. 102–105, 2009.

[22] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[23] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An authentication protocol for low-cost RFID tags", *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223, 2011.

[24] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An improved authentication protocol for mobile agent device in RFID," *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508–520, 2012.

[25] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "Security analysis of an enhanced mobile agent device for RFID privacy protection," *IETE Technical Review*, vol. 32, no. 3, pp. 183–187, 2015.

[26] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.

[27] G. Xu, Y. Ren, Y. Han, X. Li, and Z. Feng, "Privacy protection method based on two-factor authentication protocol in frid systems," *IEICE Transactions on Information and Systems*, vol. 99, no. 8, pp. 2019–2026, 2016.

[28] X. Zhang and Y. Guo, "Research on RFID system security authentication protocol based on elliptic curve cryptography," *Net Information Security*, vol. 18, no. 10, pp. 51–61, 2018.

[29] X. Zhang, L. Li, Y. Wu, and Q. Zhang, "An ECDLP-based randomized key RFID authentication protocol," in *International Conference on Network Computing and Information Security*, vol. 2, pp. 146–149, 2011.

[30] L. Zheng, Y. Xue, L. Zhang, and R. Zhang, "Mutual authentication protocol for RFID based on ECC," in *IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 2, pp. 320–323, 2017.

Biography

Yong-Shuang Wei, is currently a Master student in the Department of Mathematics and Statistics at Wuhan University, China. She holds a Bachelor of Science degree in Applied Mathematics at Chongqing University, China. Her main research interests are cryptography and information security, especially elliptic curve cryptography.

Jian-Hua Chen, is a Professor in the Department of Applied Mathematics at Wuhan University, Hubei, China. He is the Director of the Information Security Research Center, and the main designer of the SM2 Signature Algorithm for ISO/IEC International Standards. His research interests include number theory and information security, elliptic curve cryptography.