PAPER Special Section on Security, Privacy and Anonymity of Internet of Things

A Secure RFID Application Revocation Scheme for IoT*

Kai FAN[†a)], **Zhao DU**[†b)], **Yuanyuan GONG**[†c)], **Yue WANG**[††d)], ***Nonmembers***, **Tongjiang YAN**[†††e)], ***Member***, **Hui LI**[†f)], ***and*** **Yintang YANG**[††††g)], ***Nonmembers***

SUMMARY Radio Frequency Identification (RFID) plays a crucial role in IoT development. With the extensive use of RFID, the fact that a single RFID tag integrates multiple applications has become a mainstream. To facilitate users to use the multi-application RFID tag and revoke some applications in the tag securely and efficiently, a secure RFID application revocation scheme is proposed in this paper. In the scheme, each response for the challenge between tag and reader is different, and a group has the feature of many tags. Even if the group index number and corresponding group are revealed, a specific tag does not be precisely found and tracked. Users are anonymous completely. The scheme also allows users to set the validity period for an application or some applications. If the application contains the validity period and expires, the server will remove the validity period and revoke the application automatically in the tag when the RFID tag accesses server again. The proposed scheme cannot only be used in multi-application RFID tag but also be used in one-application RFID tag. Furthermore, compared with other existing schemes, the scheme provides a higher level of security and has an advantage of performance. Our scheme has the ability of mutual authentication and Anti-replay by adding a random number r_2, and it is easy to against synchronization attack. Security proof is given in our paper and performance advantage are mainly reflected in the following points such as forward security, synchronization, storage complexity, computational complexity, etc. Finally, the proposed scheme can be used in multi-application RFID tag to promote the development of the IoT.

key words: *RFID, authentication, revocation, security, IoT*

1. Introduction

IoT [1] is a large network which consists of various information sensing devices and the Internet. RFID, as an automatic identification and data capture technology, RFID has been one of the core technologies in IoT and it is also listed as one of the ten most significant technologies in the 21st century [2]. Compared with the traditional two-dimensional codes, bar codes, magnetic cards and IC cards, RFID has many advantages such as having no contact with other something, remote reading, long life and easy operation, etc.

With the extensive use of RFID technology, many security and privacy issues frequently appear. To solve this problem, scholars have proposed many different RFID security authentication schemes such as Hash-lock protocol [3], random Hash-lock protocol [4], Hash-chain protocol [5], lightweight and ultralightweight RFID mutual authentication protocol [6], the change of ID protocol based on hash algorithm [7], David's digital library protocol [8], distributed challenge-response authentication protocol [9] and LD authentication protocol [10], etc. However, neither do these schemes achieve a high level of security to resist a variety of attacks, nor do these protocols take into account the efficiency. More mature encryption algorithms and authentication mechanisms are not well applied directly to RFID system because of the limitation of low-cost RFID tag. Therefore, considering the advantages of simple and fast Hash function, research on RFID security authentication scheme based on Hash function has become a hot research field in recent years.

Because of the wide use of RFID technology, the fact that a single RFID tag integrates multiple applications has become a main stream. This way can facilitate users to use the multi-application RFID tag and revoke some applications in the tag securely and efficiently. For example, in the campus, a card can be used for school shopping, dining, medical services, access control, and borrowing books from the library, etc. If a particular application is no longer used, the application will be revoked timely in the corresponding server.

Manuscript received November 29, 2015.
Manuscript revised April 14, 2016.
Manuscript publicized May 31, 2016.

[†]The authors are with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China.
[††]The author is with the School of Information Engineering, Xi'an University, Xi'an, China.
[†††]The author is with with the College of Science, China University of Petroleum, Qingdao, China.
[††††]The author is with Key Lab. of Minist. of Educ. for Wide Band-Gap Semicon. Materials and Devices, Xidian University, Xi'an, China.

*This paper is supported by the National Natural Science Foundation of China (No. 61303216, No. 61272457, No. U1401251, and No. 61373172), the National High Technology Research and Development Program of China (863 Program) (No. 2012AA013102), the China Postdoctoral Science Foundation funded project (No.2013M542328), and National 111 Program of China B16037 and B08038, and the Xian Science and Technology Plan funded project (CXY1352WL30). Part of the work entitled "RFID secure application revocation for IoT in 5G" was presented at the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, Finland, 20–22 August, 2015.

a) E-mail: kfan@mail.xidian.edu.cn
b) E-mail: duzhao_study@foxmail.com
c) E-mail: gyy890922@qq.com
d) E-mail: kelly8266no1@sina.com
e) E-mail: yantoji@163.com
f) E-mail: lihui@mail.xidian.edu.cn
g) E-mail: ytyang@xidian.edu.cn

DOI: 10.1587/transinf.2015INP0008

However, there are few researches on the revocable problem in the RFID secure authentication scheme and recently only revocable RFID security authentication protocol, called RSEL [11], involves the issue. Although there are some novel protocols proposed in recent years in the campus example application deletion, but most of them are functional innovation, so it is easy to ignore the security issues. Our proposed scheme not only can easily revoke tag applications, but also ensure absolute security.

To overcome the computational complexity and revocable issue, the novel scheme [12] was proposed which preserves privacy of a biometric user. The presented scheme is a cost-effective solution. Besides, the scheme minimizes the system complexity with simple operations. The last but not least, the security in the scheme is unsatisfactory. A new revocable secret handshake scheme [13] with backward unlinkability is presented that allow the members of a certain organization can anonymously authenticate each other. Besides, scheme achieves the impersonator resistance against Group Authority (GA). The revocation is obtained in the new scheme, as well as the unlinkability and the traceability. Moreover, the anonymity of revoked members is improved so that the past transcripts of revoked members remain private, i.e. Even this, it is vulnerable to synchronization attacks and the scalability is bad. In group signature schemes, a signature is anonymous for a verifier, while only a designated Privacy Manager (PM) can identify the signer. This identification is used for tracing a dishonest anonymous signer in case of an illegal act using the signature. T Nakanishi and N Funabiki proposed a short anonymously revocable group signature scheme [14] to resist violating signers' anonymity, the membership of the dishonest signer can be anonymously revoked for excluding the signer without the help of any PM. Compared to the simple adoption of the Brickell-Li DDH-based revoking approach to supersingular curves, the length of our signature is reduced to about from 30% to 60%. Modern power systems have been faced with a rising appeal for the upgrade to a highly intelligent generation of electricity networks known as the smart grid. Thus, security for the smart grid has emerged as an important issue. Recently, Hur proposed an attribute based data sharing for smart grid [15] which unfortunately is vulnerable to the denial of service (DoS) attack. This system maintains basic service to support monitoring, but during an emergency, visits to the service will scale up enormously, which means MDSE must support a rapid scaling up of service capacity in a short time [16]. Moreover, it does not support the user revocation property and the grid system manager cannot prevent the revoked user of having access to the shared data in the storage center. In order to solve these weaknesses, an efficient revocable data sharing scheme [17] which is immune against DoS attack was proposed. However, computational complexity is not very ideal, so it is not reasonable to apply in low performance system. Recently there is a new performance evaluation scheme, it is not just a single evaluation from quality of service, but from QoE. Quality-of-Experience (QoE) is a new concept related to but differs from Quality-of-Service (QoS) perception. QoE is a subjective measure of a customer's experiences with a service focuses on the entire service experience, and is a more holistic evaluation [18], [19].

The main idea of RSEL protocol is that the value of validity period of each tag is stored in the back-end data management system, then setting an appropriate value of validity period of tag and the corresponding list of tag identity, and only when the validity period of the tag ends, the tag application is considered to be revoked. But the scheme is only used in one-application RFID tag, and provides a certain degree of anonymity. Therefore, a strong anonymous, low-complexity, and revocable RFID secure authentication scheme which facilitates users to use the multi-application RFID tag and revokes some applications in the tag securely and efficiently is urgently desired.

In this paper, we propose a secure RFID application revocation scheme. The scheme adopts the hash function and a random number to generate the corresponding module through using a typical challenge-response mechanism. The proposed scheme which reduces storage complexity and provides a higher level of security, in the meantime ensures less computational complexity in tag and communication complexity of the entire protocol. Furthermore, this scheme which has wide development prospect not only can be used in multi-application RFID tag, but also be used in one-application RFID tag.

The rest of this paper is organized as follows. In Sect. 2, some related works are provided. In Sect. 3, the security achievements of the secure RFID application revocation scheme are provided. In Sect. 4, the secure RFID application revocation scheme is proposed. Security Proof with BAN logic is provided in Sect. 5. The analysis and evaluation of the secure RFID application revocation scheme are given in Sect. 6. Finally, concluding remarks are provided.

2. Related Works

In this section, RSEL authentication protocol will be discussed. Firstly, it is assumed that there are many RFID system tags, each tag integrates m applications. RSEL protocol is divided into two sub-processes: the initialization process and the mutual authentication process. The entire protocol authentication process is also considered to be a tag legitimate identity authentication because of the RSEL protocol used in one-application RFID tag.

2.1 Initialization Process

In RSEL protocol, all entities will firstly complete the memory initialization. It is assumed that output length of hash operation is L.

Tags: each tag stores (ID_i, K_i), $K_i = H(ID_i)$, K_i represents the private key of the i-th tag, and ID_i represents the i-th tag identity.

Severs: Server will create the corresponding tag record $(K_i^{now}, K_i^{old}, ID_i, V_i)$for each tag, K_i^{now} is initialized to $H(ID_i)$, K_i^{old} is initialized to empty. K_i of server-side and tag-side will perform the appropriate update operation after the each session ends successfully.

The explanations of symbols are as follows:

V_i: validity period of the i-th tag application, called the maximum lifetime.

r_1,r_2,T: random number and timestamp are generated separately by the reader and the tag.

IDS_{group}: group index of tag.

$K_{i,j}^{now}$: for the application j, use of private key of i-th tag in the current session.

$K_{i,j}^{old}$: for the application j, use of private key of i-th tag in the last successful session.

E: a status bit string of length L which is appointed by legitimate tag and server. When E equals *str1*, the application is only certified. When E equals *str2*, the application is revoked.

2.2 Mutual Authentication Process

The authentication process of RSEL protocol is shown in Fig. 1.

1) The reader generates a timestamp r_1 and sends the *query* and r_1 to the tag. The system initiates a new authentication session.
2) After the tag receives the *query* and r_1, it generates a timestamp r_2 and calculates $H(ID_i||r_1||r_2||K_i)$. Then the tag sends r_2, K_i and $H(ID_i||r_1||r_2||K_i)$ to the reader to response to the query.
3) After the reader receives the information from the tag, it sends r_1, r_2, K_i and $H(ID_i||r_1||r_2||K_i)$to the sever.
4) The sever searches whether $K_i = K_i^{old}$ or $K_i = K_i^{now}$. If any equation is equal and $r_2 \leq V_i$, the sever calculates $H'(ID_i||r_1||r_2||K_i)$ using the corresponding ID_i and judge whether $H'(ID_i||r_1||r_2||K_i)$ equals $H(ID_i||r_1||r_2||K_i)$. If these two values are equal, the authentication is successful, and the database considers that the tag is legal.
   If K_i cannot be found, sever considers that tag is not legal. If $K_i = K_i^{old}$ or $K_i = K_i^{now}$, and $r_2 > V_i$, the sever ignores this message, and it considers that the tag is expired. Then the sever deletes the corresponding tag records to revoke the application in the tag. If $K_i = K_i^{old}$ or $K_i = K_i^{now}$, and $r_2 < V_i$, but $H'(ID_i||r_1||r_2||K_i)$ is not equal to $H(ID_i||r_1||r_2||K_i)$, the sever ignores this message, and it considers that the tag is not legal.
5) Sever calculates $H(ID_i||r_2)$ and sends it to the tag through the reader.
6) According to the ID_i stored and the r_2 generated, tag calculates $H'(ID_i||r_2)$ and then compares the resulting value with the value received. When these two values are equal, the tag determines legitimate identity of sever and updates the value of K_i according to the formula: $K_i \leftarrow H(ID_i||r_1)$. Otherwise, the tag ignores this message, and it considers that the process of authentication session fails

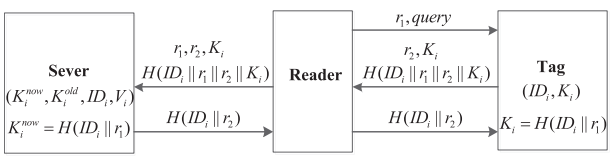

Fig. 1 The RSEL authentication protocol

3. The Security Achievements of the RFID Secure Application Revocation Scheme

1) The scheme which ensures the truth of identity information of communicating parties uses mutual authentication way to achieve authentication between tag and server.
2) This scheme uses Hash function or private key separately to achieve hash or encryption processing of information transmission in the authentication process. Even if attackers gain these data through eavesdropping or intercepting, they cannot get any useful information. Therefore, the scheme improves the confidentiality.
3) Each response for the challenge between tag and reader is different, so attackers are not capable of successfully tracking a specific tag. Furthermore, even if attackers get the group index number and corresponding group, they cannot precisely find a specific tag. This scheme achieves the tag anonymity.
4) The attacker cannot obtain private information of legitimate tag and the current state flag information which is appointed secretly by legal tag and server. Therefore, they cannot construct correct message authentication information to counterfeit a legitimate tag to achieve the server legitimate authentication. Similarly attackers cannot construct the value of correct message authentication information to counterfeit a legitimate server to achieve the tag legitimate authentication.
5) The fact that information exchange in the course of each session are function values of random numbers and these random numbers will independently generate guarantees that the interactive data has no direct relation with the previous data. Therefore, attackers cannot retransmit legal communication data to complete legitimate authentication in the previous session. This scheme improves the ability to effectively resist replay attack.
6) This scheme implements application revocation function through deleting the corresponding application records on the server-side. Even if attackers get some secret information about the application which is successfully revoked, they cannot also complete legal identity authentication of server which has no corresponding records. Therefore, this scheme can improve security on the basis of revocation.

4. Secure RFID Application Revocation Scheme

In this section, we will propose the secure RFID application revocation scheme.

The authentication protocol of the secure RFID application revocation scheme is shown in Fig. 2. The scheme uses the hash function and a random number through using a typical challenge-response mechanism. Specific steps of the scheme are as follows:

1) Setting the initialization of RFID system.

a) i-th tag contains a pseudo-random number generator and a Hash function $H : \{0,1\}^* \rightarrow \{0,1\}^L$, and stores own identity identifier ID_i, the group index IDS and the set of private key of application in the tag $(K_{i,1}, K_{i,2}, \cdots, K_{i,j}, \cdots, K_{i,m})$. Pseudo-random number generator generates a random number or timestamp required in the authentication process. $\{0,1\}^*$ represents a bit string which has arbitrary length. $\{0,1\}^L$ represents a bit string which has L length. $K_{i,j}$ is initialized to $H(ID_i \oplus r_{i,j})$. $r_{i,j}$ is a random number of the j-th application in the i-th tag in the initialization phase, $j = 1, 2, \cdots, m$. T is timestamp and users can use T to set the validity period of the application in the tag. M represents maximum number of applications which can be integrated by i-th tag.

b) Reader in RFID system contains a pseudo-random number generator which generates a random number required in the authentication process.

c) Server in the RFID network holds a Hash function and databases. The database stores a group of corresponding application records which are established by each legitimate tag. Server firstly establish a tag record (IDS, ID_i) for the i-th legitimate tag, then it establishes a group of corresponding application records for the m applications in the i-th tag: $((K_{i,1}^{old}, K_{i,1}^{now}), (K_{i,2}^{old}, K_{i,2}^{now}), \cdots\cdots, (K_{i,m}^{old}, K_{i,m}^{now}))$.

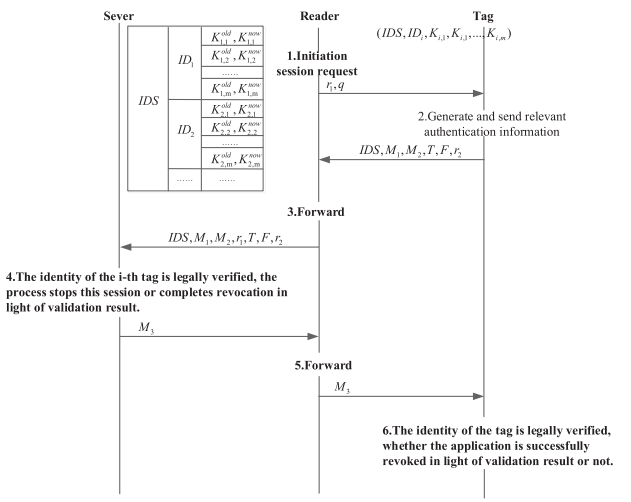

Fig. 2 The RFID secure application revocation scheme

$K_{i,j}^{old}$ is initialized to empty, $K_{i,j}^{now}$ is initialized to $H(ID_i \oplus r_{i,j})$.

2) Reader initiates a session request to the i-th tag in the RFID network. The initialization process is that reader generates authentication request q, and the pseudo-random number generator generates first random number r_1. This process initiates new session through sending r_1 and q to the i-th tag in the RFID network.

3) The i-th tag generates relevant certification information.

a) Tag will generate new timestamp T after the emphi-th tag receives authentication request q.

b) According to the identity identifier ID_i, the private key $K_{i,j}$ and the first random number r_1 of the tag, we can calculate the value of the first hash authentication information: $M_1 = H(ID_i \| r_1 \| T)$, and the value-ofthe second hash authentication information: $M_2 = H(K_{i,j} \| r_1 \| T)$, $K_{i,j}$ is the private key value of the j-th application in the i-th tag.

c) The i-th tag generates the current value of the status flag information E, and calculates the value of XOR authentication information: $F = E \oplus K_{i,j}$, E is a status bit string which is appointed by legitimate tag and server, and its length is L. When E equals $str1$, the application is revoked. When E equals $str2$, the application is only certified.

d) i-th tag sends its own group index IDS, timestamp T, value of first hash authentication information M_1, value of second hash authentication information M_2 and value of the XOR authentication information F to corresponding reader through RF signal.

4) After reader receives group index IDS, timestamp T, the value of first hash authentication information M_1, the value of second hash authentication information M_2 and the value of the XOR authentication information F, reader in the RFID network forwards these data and r_1 immediately to the appropriate server via a wired communication network.

5) The server completes the legitimate identity authentication of the i-th tag in the RFID network.

a) Server determines the group of the tag in light of the tag group index received in RFID network.

b) Server finds tag records to meet the requirement $H'(ID_i \| r_1 \| T \| r_2) = M_1$ in the group. If the server finds corresponding message record, it will determine legitimate tag identity and obtain the tag identity identifier. Otherwise, the server considers that the tag is illegal and stops this session immediately.

c) In the RFID network, server finds the value of previous key $K_{i,j}^{old}$ or the value of current $keyK_{i,j}^{now}$ in the tag application records in light of tag identity identifier ID_i and these values meet the requirement $H'(K_{i,j} \| r_1 \| T \| r_2) = M_2$. If the server finds corresponding key, the fact indicates that the tag could support the application in the past. According to the value of key $K_{i,j}$ found and the value of the XOR authentication information F received, we can obtain the value of

the comparable status flag information: $E' = F \oplus K_{i,j}$. Otherwise, the tag cannot integrate the application, and sever stops this session immediately.

d) Server finds whether the user sets the validity period for an application or some applications according to timestamp T. If T contains the validity period, server will store the validity period, and then compare the current date with validity period automatically when the RFID tag accesses server again. Otherwise, the scheme ignores this step. If the application expires, the server will remove the validity period and revoke the application automatically in the tag. Otherwise, the server still saves the validity period.

e) When the value of the comparable status flag information E' equals $str1$, the server deletes this application record in the tag application records, and calculates the value of the third Hash authentication information $M_3 = H(ID_i \| K_{i,j} \| r_1 \| T \| r_2)$in light of the key value $K_{i,j}$ found.

f) The server sends the value of the third hash authentication information M_3 to the appropriate reader in RFID network.

6) Reader forwards the value of the third hash authentication information received M_3 to the i-th tag through RF signal.

7) The i-th tag completes legitimate identity verification of the server in RFID network.

a) According to timestamp T generated, first random number r_1, tag identity identifier ID_i and the private key of the j-th application $K_{i,j}$, the process calculates the value of the third comparable authentication information $M_3' = H(ID_i \| K_{i,j} \| r_1 \| T \| r_2)$ after the i-th tag receives the value of the third authentication information.

b) When the value of the third comparable authentication information M_3' equals M_3, server is considered to have legitimate identity. Otherwise, the process immediately stops this session.

c) According to step 3, when the current value of the status flag information E equals $str1$, the application is successfully revoked. Otherwise, the session achieves only the process of normal certification, but it does not complete application revocation operation.

5. Security Proof with BAN Logic

The core security assurance of the proposed protocol is the secure mutual authentication, which means the following security aims should be achieved:

- Security Aim 1: $Sever$ needs to make sure the received message $(IDS, M1, M2, r_1, T, F, r_2)$ is exactly the one sent by Tag_i. This means that we need to achieve:
  $Server \equiv Tag_i \sim (IDS, M1, M2, r_1, T, F, r_2)$ and
  $Server \equiv Tag_i \equiv (IDS, M1, M2, r_1, T, F, r_2)$

- Security Aim 2: Tag_i needs to make sure the received message $M3$ is exactly the one sent by $Server$, which means the following formulas need to be achieved:
  $Tag_i \equiv Server \sim M3$ and
  $Tag_i \equiv Server \equiv M3$

5.1 Security Assumption

According to the given protocol, and the $Server$ and $Reader$ are connected securely, the following conditions can be achieved.

$AS1 : Server \equiv \text{Server} \overset{r_{ij}}{\rightleftharpoons} \text{Tag}_i$
$AS2 : Tag_i \equiv \text{Server} \overset{r_{ij}}{\rightleftharpoons} \text{Tag}_i$
$AS3 : Reader \Longrightarrow (r_1)$
$AS4 : Reader \equiv \#(r_1)$
$AS5 : Server \equiv \#(r_1)$
$AS6 : Tag_i \Longrightarrow (r_2)$
$AS7 : Tag_i \equiv \#(r_2)$

5.2 Security Analysis

According to the protocol $k_{ij} = H(ID_i \oplus r_{ij})$, together with the assumptions $AS1$ and $AS2$, we can deduce $Server \equiv \text{Server} \overset{k_{ij}}{\rightleftharpoons} \text{Tag}_i$ and $Tag_i \equiv \text{Server} \overset{k_{ij}}{\rightleftharpoons} \text{Tag}_i$. Because the in this protocol, the $Server$ will receive the message $(IDS, M1, M2, r_1, T, F, r_2)$ forwarded from the $Reader$, where $M2 = H(k_{ij} \| r_1 \| T \| r_2)$. As we have achieved k_{ij} as a secret between $Server$ and Tag_i, we can take k_{ij} as the secret key to protect messages. So we can simply write the received message of $Server$ as $\langle IDS, M1, M2, r_1, T1, F, r_2 \rangle_{k_{ij}}$, and we have:$Server \triangleleft \langle IDS, M1, M2, r_1, T1, F, r_2 \rangle_{k_{ij}}$. For the reason of "message-meaning rule" of BAN: $\frac{P \equiv Q \overset{Y}{\rightleftharpoons} P, P \triangleleft \langle X \rangle_Y}{P \equiv (Q \sim X)}$, we can deduce $Server \equiv Tag_i \sim (IDS, M1, M2, r_1, T1, F, r_2)$.

From the assumption $AS5 : Server \equiv \#(r_1)$, and the BAN rule of $\frac{P \equiv \#(X)}{P \equiv \#(X,Y)}$, we know $Server \equiv \#(IDS, M1, M2, r_1, T1, F, r_2)$. Because we have achieved $Server \equiv Tag_i \sim (IDS, M1, M2, r_1, T1, F, r_2)$, together with the "nonce-verification" rule $\frac{P \equiv (\#(X)), P \equiv (Q \sim X)}{P \equiv (Q \equiv X)}$, we will achieve:

$Server \equiv Tag_i \equiv (IDS, M1, M2, r_1, T, F, r_2)$, and the first security aim of the given protocol is achieved.

For the same reason, we can also deduce $Tag_i \equiv Server \sim M3$ and $Tag_i \equiv Server \equiv M3$, the second of security aim is also achieved, and the security of mutual authentication of the proposed protocol has been proved.

6. Performance Analysis of the RFID Secure Application Revocation Scheme

In this section, we will analyze the performance of the secure application revocation scheme. Compared with other schemes, the scheme is evaluated mainly from the performance of the security and complexity.

6.1 Security Analysis

Proposed scheme has a competence of resisting common attacks effectively in RFID system and takes advantage of the anonymity of the group to provide tag anonymity.

1) The proposed scheme can ensure the identity legitimacy of the tag through message M_1, and then use message M_2 to authenticate application legitimacy in legitimate tag. Tag ensures the identity legitimacy of sever through message M_3. Therefore, the proposed scheme uses mutual authentication way to achieve authentication between tag and server.
2) In the proposed scheme, information exchange uses hash function to achieve encryption processing. Even if attackers gain these data through eavesdropping or intercepting, they cannot get any useful information. Therefore, the scheme improves the confidentiality.
3) Each response for the challenge between tag and reader is different, so attackers are not capable of tracking a specific tag successfully. Furthermore, even if attackers get the group index number *IDS* and corresponding group, they cannot precisely find a specific tag because of the feature of many tags in the group. This scheme achieves the tag anonymity.
4) The attacker cannot obtain private information of legitimate tag(ID, $K_{i,j}$)and the current state flag information E which is appointed secretly by legal tag and server. Therefore, they cannot construct correct message M_1, M_2 and F to counterfeit a legitimate tag to achieve the server legitimate authentication. Similarly attackers cannot construct correct message M_3 to counterfeit a legitimate server to achieve the tag legitimate authentication.
5) The fact that information exchange in the course of each session are function values of r_1, T and r_1, T will independently generate guarantees that the interactive data has no direct relation with the previous data.The fact that each state flag information E is uncertain makes F different in the course of each session.Therefore, attackers cannot retransmit legal communication data to complete legitimate authentication in the previous session. This scheme improves the ability to effectively resist replay attack.
6) After every successful session, the tag and sever should update their key and use different r_1, T in each update.
7) In a normal session, if the attacker intercepts the last message which is forwarded by the reader, the tag will not authenticate server successfully. The fact that the server completes update operation and the tag remains previous state makes the tag and server lose synchronization. If $K_{i,j}$ is stored by $K_{i,j}^{old}$ in the server in the previous session, the scheme will achieve authentication between tags and sever successfully through $K_{i,j}^{old}$ next authentication.
8) When a single RFID tag integrates multiple applications, user no longer wants to use anapplication after a period of time. The sever can automatically revoke the application in the tag according to the validity period which is set by user, and user also uses the proposed scheme to revoke the application. Furthermore, even if attackers get some secret information about the application which is successfully revoked, they cannot also complete legal identity authentication of server which has no corresponding records. Therefore, this scheme can improve security on the basis of revocation.

Comparison between the proposed RFID secure scheme and other existing authentication schemes based on Hash function in terms of security is shown in Table 1. "$\surd$ "means satisfaction, "$\times$" means to dissatisfy, "$-$" indicates that the scheme does not relate to the problem. "# " indicates that the scheme can be used in one-application RFID tag, but they cannot be used in multi-application RFID tag.

From Table 1, Random Hash-lock protocol and Hash-chain protocol cannot resist counterfeiting and replay attack, and cannot guarantee complete anonymity. Furthermore, Hash-chain protocol cannot completemutual authentication. Although the ESLRAS protocol [20] proposed can resist most attacks in the literature, they cannot guarantee complete anonymity of tag. However, complete anonymity is one of the most significant prerequisites in the communication security. RSEL protocol proposed firstly which is application revocation scheme can be used in one-application RFID tag, but it cannot also achieve complete anonymity. The scheme proposed is an RFID secure application revocation scheme. It can achieve complete anonymity and facilitate users to use the multi-application RFID tag and revoke some applications in the tag securely and efficiently.

6.2 Complexity Analysis

In this section, we list the comparative analysis between the proposed scheme and the revocable RSEL protocol in terms of performance. It is assumed firstly that information length of each scheme is L. In light of the storage complexity, computational complexity and communication complexity, we analyze these two schemes.

1) Storage Complexity
   First, it is assumed that RFID system only has a tag. To achieve application revocation in the RSEL protocol, the tag storage space requires *2L* and the corresponding server storage space needs *4L*. If the users achieve the secure revocation of m applications, the system will add another *(m-1)* tags and establish the corresponding tag records on the server-side. Therefore, the tag storage space requires *2mL* and the corresponding server storage space needs *4mL*.
   However, if we use secure application revocation scheme proposed, the scheme will make users use the multi-application RFID tag and revoke some applications in the tag. The tag storage space only requires *(m+2)L* and the corresponding server storage space

Table 1 Functionality and security comparison of revocable schemes

Secure Authentic-at ion scheme	Mutual Authen-tication	Confi denti ality	Com-plete Anon-ymity	Anti-cou-nterfeiting	Anti-re play	Forward Security	Synchro nization	Revoc ability
Random Hash-lock protocol [4]	√	√	×	×	×	√	-	×
Hash-chain protocol [5]	×	√	×	×	×	√	–	×
ESLRAS [20]	√	√	×	√	√	√	√	×
RSEL [11]	√	√	×	√	√	√	√	#
Proposed scheme	√	√	√	√	√	√	√	√

Table 2 Storage complexity comparison of revocable schemes

Authentication scheme	Server-side	Reader-side	Tag-side
RSEL	$2mL$	0	$4mL$
Proposed scheme	$(m+2)L$	0	$(2m+2)L$

Table 3 Computational complexity comparison of revocable schemes

Authentication scheme	Server-side	Reader-side	Tag-side
RSEL	$3T_H$	T_R	$3T_HT_R$
Proposed scheme	$(p+2m+1)T_H, \oplus$	T_R	$4T_H, T_R, \oplus$

needs *(2m+2)L* in the scheme proposed. Due to $m \geq 2$, the proposed scheme has less storage complexity, and it can greatly save storage space with the increase number of applications in the tag. Therefore, the proposed scheme can greatly reduce input costs. Table 2 shows storage complexity comparison of revocable schemes.

2) Computational Complexity

To facilitate the comparison between RSEL protocol and the proposed scheme in terms of computing complexity, we use T_H to be on behalf of a Hash function, T_R is on behalf of pseudo-random number or timestamp, $\bigoplus$ is on behalf of XOR operation. It is assumed that each group contains $p(p \geq 1)$ tags in the proposed secure scheme. The tags perform four times Hash operations, a random number generation and a XOR operation. The server in the corresponding group needs firstly up to p times Hash operations to complete the tag certification. Then the server achieves traverse computing in the m tag application records to find the appropriate application records. This process needs up to $2m$ times Hash operations. Furthermore, the server also requires a XOR operation and makes another Hash operations complete the update operation. Therefore, server needs to perform $(p+2m+1)$ times Hash operations.

From Table 3, computational complexity of the proposed scheme on the server-side has relation with the number of m application in each tag and the number of p tags in the group, and then p and m can be set according to the actual application scenario of the scheme and the requirement for efficiency. Compared with the RSEL protocol, in terms of computational complexity on the tag-side, the proposed scheme only adds a Hash operation and a XOR operation to make users use the multi-application RFID tag and revoke some applications in the tag conveniently.

3) Communication Complexity

The proposed scheme mainly achieves application revocation and is used in multi-application RFID tag. Therefore, to make users use the multi-application RFID tag and revoke some applications in the tag conveniently, the proposed scheme leads to communication complexity increase.

Table 4 Communication complexity comparison of revocable schemes

Authentication scheme	Number of interactions	Total traffic
RSEL	*3*	*6L*
Proposed scheme	*3*	*8L*

From Table 4, the proposed revocable secure authentication scheme do not increase the number of interactions, but the total traffic transmitted relatively increases a littlein the channel.To adapt to the new application scenarios, the proposedscheme needs to complete more interactive authentication information in the channel to lead to the total transmitted information increase. However, in the scenario, the scheme can bring great convenience to users, provide a higher level of security, and expand the application scale of the RFID systems.

A certain application can be easily revoked in our proposed scheme, and it can also be a good solution to solve the security and privacy issues of RFID. By comparing it with the other schemes, it shows that our proposed protocol can not only improve the function of revocation, but also has the advantage of high level of security and high in performance. In addition, our proposed protocol can not only be used in the single card application, so it is a valuable job with a very high practical.

7. Conclusions

A secure application revocation scheme in multi-application RFID tag is proposed in this paper. The scheme can achieve completely anonymity and facilitate users to use the multi-application RFID tag and revoke some applications securely and efficiently according to the users' actual requirements. Compared with other existing schemes, the proposed scheme provides a higher level of security and has an advantage of performance in terms of

complexity. Because server stores both old private key and new private key, when session with new private key fails, the corresponding old private key will be used, so synchronization attack is easy to resist.Finally, the proposed scheme can be used in multi-application RFID tag to promote the development of the IoT.

References

[1] H. Ning and B. Wang, RFID major projects and the state Internet of Things, Mechanical Industry Press, 2008.
[2] A. Juels, "RFID security and privacy: A research survey," IEEE J. Sel. Areas Commun., vol.24, no.2, pp.381–394, 2006.
[3] S.E. Sarma, S.A. Weis, and D.W. Engels, "RFID systems and security and privacy implications," Proc. 2002 Cryptographic Hardware and Embedded Systems-CHES, pp.454–469, 2003.
[4] S.A. Weis, "Security and privacy in radio-frequency identification devices," Massachusetts Institute of Technology, 2003.
[5] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain based forward-secure privacy protection scheme for low-cost RFID," Proc. 2004 SCIS, pp.719–724, 2004.
[6] K. Fan, Y.Y. Gong, Ch. Liang, H. Li, and Y.T. Yang, Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G, Security and Communication Networks, Published online in Wiley Online Library (wileyonlinelibrary.com), 2015. DOI: 10.1002/sec.1314
[7] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," Proc. 2004 PCCW, pp.149–153, 2004.
[8] D. Molnar and D. Wagner, "Privacy and security in library RFID: issues, practices, and architectures," Proc. 2004 CCS, pp.210–219, 2004.
[9] X. Gao, Z. Xiang, H. Wang, J. Shen, J. Huang, and S. Song, "An approach to security and privacy of RFID system for supply chain," Proc. 2004 E-Commerce Technology for Dynamic E-Business, pp.164–168, 2004.
[10] Y. Li and X. Ding, "Protecting RFID communications in supply chains," Proc. 2007 ICCS, pp.234–241, 2007.
[11] K. Fan, J. Li, H. Li, X.H. Liang, X.M. Shen, and Y.T. Yang, "RSEL: Revocable secure efficient lightweight RFID authentication scheme," Concurrency and Computation: Practice and Experience, vol.26, no.5, pp.1084–1096, 2014.
[12] M.K. Khan, K. Alghathbar, and J. Zhang, Privacy-preserving and tokenless chaotic revocable face authentication scheme, Telecommunication Systems, vol.47, no.3-4, pp.227–234, 2011.
[13] H.-Y. Lin, "RPCAE: a novel revocable proxy convertible authenticated encryption scheme, International Journal of Information Security, vol.14, no.5, pp.431–441, 2015.
[14] T. Nakanishi and N. Funabiki, "A short anonymously revocable group signature scheme from decision linear assumption," Proc. 2008 ASIACCS, pp.337–340, 2008.
[15] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol.24, no.11, pp.2171–2180, 2013.
[16] M. Dong, H. Li, K. Ota, L.T. Yang, and H. Zhu, "Multicloud-based evacuation services for emergency management," IEEE Cloud Computing, vol.1, no.4, pp.50–59, 2014.
[17] M. Bayat, H.R. Arkian, and M.R. Aref, "A revocable attribute based data sharing scheme resilient to DoS attacks in smart grid," Wireless Networks, vol.21, no.3, pp.871–881, 2015.
[18] M. Dong, T. Kimata, K. Sugiura, and K. Zettsu, "Quality-of-experience (QoE) in emerging mobile social networks," IEICE Trans. Inf. & Syst., vol.E97-D, no.10, pp.2606–2612, 2014.
[19] M. Dong, X. Liu, Zh. Qian, A. Liu, and T. Wang, "QoE-ensured price competition model for emerging mobile networks," IEEE Wireless Commun., vol.22, no.4, pp.50–57, 2015.
[20] K. Fan, J. Li, H. Li, X. Liang, X. Shen, and Y. Yang, "ESLRAS: a lightweight RFID authentication scheme with high efficiency and strong security for internet of things," Proce. 2012 INCoS, pp.323–328, 2012.

Kai Fan was born in 1978 in Shaanxi Province of China. In 2002, 2005, and 2007, he received his B. S. degree in telecommunications engineering, M. S. degree in cryptography, and Ph. D. degree in telecommunications and information system from Xidian University respectively. He is now an associate professor of Xidian University. His research interests include IoT security, cloud security, network and information security.

Zhao Du was born in 1990 in Shaanxi Province of China. He received his B. S. degree in communication engineering from Shaanxi University of Technology in 2013. He is studying for M.S. degree in Xidian University from 2013. His research interests include IoT security, network and information security.

Yuanyuan Gong was born in 1989 in Henan Province of China. She received her M. S. degree in telecommunications and information system from Xidian University in 2015. Her research interests include IoT security, network and information security.

Yue Wang was born in 1982 in Shaanxi Province of China. In 2004, and 2007, she received his B. S. degree in telecommunications engineering and M. S. degree in telecommunications and information system from Xidian University respectively. She is now an engineering of Xi'an University. Her research interests include wireless communication, wireless network security.

Tongjiang Yan was born in 1973 in Shandong Province of China. In 1999, he received the M.S. degree in mathematics from the Northeast Normal University, Lanzhou, China. In 2007, he received the Ph.D. degree in Xidian University. He is now a professor of China University of Petroleum. His research interests include cryptography and algebra.

Hui Li was born in 1968 in Shaanxi Province of China. In 1990, he received his B. S. degree in radio electronics from Fudan University. In 1993, and 1998, he received his M. S. degree and Ph. D. degree in telecommunications and information system from Xidian University respectively. He is now a professor of Xidian University. His research interests include network and information security.

Yintang Yang was born in 1962 in Hebei Province of China. He received his Ph. D. degree in semiconductor from Xidian University. He is now a professor of Xidian University. His research interests include semiconductor materials and devices, network and information security.