Lightweight RFID Protocol for Medical Privacy Protection in IoT

Kai Fan, *Member, IEEE*, Wei Jiang, Hui Li, *Member, IEEE*, and Yintang Yang, *Member, IEEE*

***Abstract*—Traditional medical privacy data is at serious risk of disclosure, and many related cases have occurred over the years. For example, personal medical privacy data can be easily leaked to insurance companies, which not only compromises the privacy of individuals, but also hinders the healthy development of the medical industry. With the continuous improvement of cloud computing and big data technologies, the Internet of Things technology has been rapidly developed. RFID is one of the core technologies of the Internet of things. The application of RFID system to the medical system can effectively solve this problem of medical privacy. RFID tags in the system can collect useful information and conduct data exchange and processing with back-end server through the reader. The whole process of information interaction is mainly in the form of cipher text. In the context of the Internet of Things, the article presents a lightweight RFID medical privacy protection scheme. The scheme ensures security privacy of the collected data via secure authentication. The security analysis and evaluation about the scheme indicate that the protocol can effectively prevent the risk of medical privacy data being easily leaked.**

***Index Terms*—Internet of Things, Lightweight, Security and Privacy, RFID, Authentication**

I. INTRODUCTION

TODAY, the privacy of individuals has become the legal provisions in many countries, and more and more people begin to concentrate on their medical privacy data. However, medical privacy faces the big challenge. Medical privacy is an extremely important part of personal privacy information, the security of which is a vital asset to people. In the traditional way, most medical behaviors are mainly related to the hospitals and clinics, and people's medical privacy information is often stored in the database of these organizations without "desensitization processing". There is a wide range of risks to the security of these privacy data, which might be used for academic research without desensitizing, or be uploaded to third-party websites, or be obtained by some other agencies (e.g. insurers, cosmetic surgery hospitals) through some unrecognized channels, which can seriously damage the people's privacy and seriously affect their physical and mental health and property safety. Further, researches show that people's life expectancy is becoming longer with the improvement of living standard [1]. Much more medical privacy data will be generated during this process, and it will bring certain challenges to the medical diagnostic industry. Therefore, more advanced means are needed to protect the medical privacy of people and to bring convenience to this industry as well.

With the rapid development of big data and cloud computing technologies, Internet of Things (IoT) technology has been beginning to approach people's daily lives gradually. IoT, just as its name implies, means "everything is connected to the internet". In this context, a large number of objects are expected to connect to the internet, such as smart phones, vehicles, sensors, wearable devices [2]. Facing the issues of the security protection of medical privacy, the technology of wearable devices and sensor can solve the people's concern to some extent. Meanwhile it provides a new effective solution for doctor's diagnosis, enabling people to enjoy better medical care anytime and anywhere [3]. Social science research shows that IoT technology is another wave of information industry after the era of personal computer (PC) network and mobile internet [4-6].

IoT is a complex system, containing many important technologies, and Radio Frequency Identification (RFID) is one of the core technologies in IoT architecture [7]. Classic RFID system is composed of three parts, including RFID tag, reader and server. Among the system, tag is responsible for collecting information and doing some simple processing, the server is used to process the data and store them, and the reader can identify the tag, and play a role of an intermediary for communicating between tag and server. RFID is a non-contact identification technology, with the feature of automatic identification, high storage capacity, portability and security [8, 9], because of which it can be applied in medical scenes friendly. In medical system, RFID tags can be attached to the surface of an object or implanted into it, and collect its information. For patients, the tag can collect physical health data, and communicate and interact with the server. It makes remote real-time monitoring and telemedicine become a reality, providing new technical support for wireless body area networks (WBAN) [10] and mobile health networks (MHN) [11]. Due to these features, the doctor or family members

This work is supported by the National Key R&D Program of China (No. 2017YFB0802300), the National Natural Science Foundation of China (No. 61772403 and No. U1401251), Natural Science Basic Research Plan in Shaanxi Province of China (No. 2017JM6004) and National 111 Program of China B16037 and B08038.

Kai Fan, Wei Jiang and Hui Li are with State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071 China (e-mail: kfan@mail.xidian.edu.cn, 2450855261@qq.com, lihui@mail.xidian.edu.cn)

Yintang Yang is with Key Lab. of the Minist. of Educ. for Wide Band-Gap Semiconductor Materials and Devices, Xidian University, Xi'an, 710071 China (e-mail: ytyang@xidian.edu.cn)

authorized by the patient can monitor the user's physical health data (e.g. body temperature, heart rate, blood pressure) through the RFID system [12]. Along with the advantages of medical RFID system is security issue [2]. As it is known, personal physical healthy information is closely related to individual privacy. The attackers today begin to infiltrate the cyber world, and they steal or falsify the patients' medical privacy data, and undermine the system's normal workflow, leading to the serious result of the disclosure of medical privacy data. Therefore, security has become one of the key issues to be addressed for RFID applied in medical system safely.

To solve this problem, we present a new lightweight RFID mutual authentication scheme used in medical context. Based on Tian's protocol [13], the proposed scheme consumes less computing resources and meet the security requirements of anonymity, replay attack resistance, synchronization, forward security and mutual authentication as well as non-denial of service. This scheme will bring the efficiency of the current medical system, and more importantly, it can protect the patient's data privacy security.

The remainder of this paper is structured as follows: In the section II, we introduce some application background of RFID technologies in the IoT environment, and present the application of RFID technology in the medical system. In the third section, a RFID privacy protection protocol based on the medical environment is proposed and details about its workflow are given too. In the fourth part, the security analysis and performance analysis comparison with some other schemes about this scheme are given, and meanwhile the logic feasibility of this scheme is proved by BAN logic rules. Finally, the fifth part summarizes the full work, and gives out some work in the future about the scheme.

II. Related work

A. RFID technology in IoT

IoT was put forward in 1999 by Massachusetts Institute of Technology, which established the Auto-ID center and proposed the basic idea of "everything can be connected through the network" [14]. In the environment, all the objects are connected with Internet to allow systems trigger the corresponding event automatically. IoT is a new concept that innovates the traditional cognition that separates the physical infrastructures as well as IT infrastructures. However, in the era of IoT, physical infrastructures and IT infrastructures can be combined to be a kind of unified infrastructures very well. In this sense, more fields of infrastructure can blend in IoT, including economic management, production operation, social management and personal lives [15].

The architecture of IoT is showed in Fig.1 [16], including collection control layer (e.g. terminal nodes, or some sensors), access layer, support network, application control layer and users [17, 18]. In this frame, the valid user can get access to information collected by the terminal nodes through the middle layers. As agreed protocols for data exchange and information communication, IoT connects all items and network with information sensing devices, offering a new interactive mode for the communication between people and objects [19].

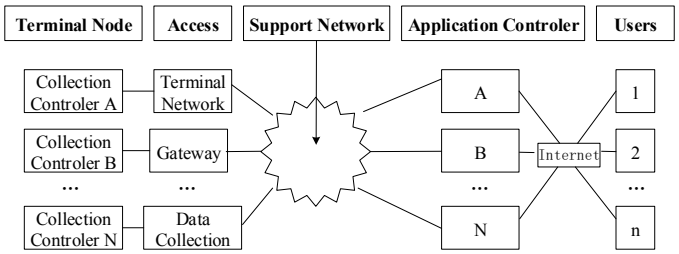

Fig. 1. Architecture of IoT

As a core technology of IoT, RFID was firstly used to identify friends or enemies (IFF) aircraft systems during the Second World War. It is a kind of contactless automatic identification technology [20]. It identifies the objects by radio frequency and access to the relevant data without human intervention. In general, the RFID system typically consists of three parts, as described in Fig. 2. RFID tag, as the data carrier, is usually along with the target object. RFID reader is capable of reading and writing the tag, which can be designed as mobile and fixed. The back-end server is typically used to store and process communication data of the system. The whole RFID architecture has features of large data storage capacity, readable and writable, strong penetrating power, far read and write distances, fast reading speed, long service life and good environment adaptability [21]. In medical field, RFID technology is widely used, including the location tracking of medical assets, neonatal and patient identification, medical tracking and validation, patient information management in health centers [22] and surgical process management [23].

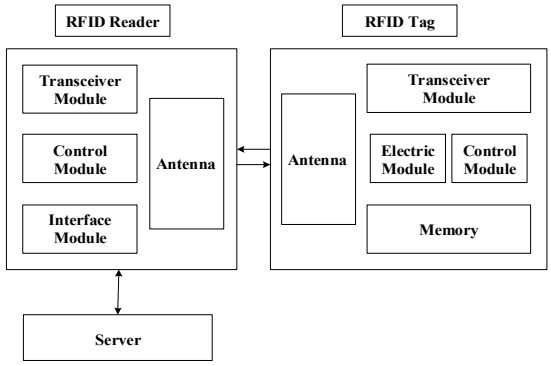

Fig. 2. Communication components of RFID system

B. RFID based Medical System

RFID technology is a communication technology that can identify a specific target and read the data via a radio signal automatically and remotely [24]. In reality, RFID has been widely used in various contactless applications, such as personal identification, libraries, access control systems, and so on [25]. Importantly, RFID system has received considerable attention in the medical health field for almost a decade now, which is expected to efficiently track hospital supplies, medical equipment, medications and patients [26, 27]. Fig. 3 introduces a RFID-enabled medical health system, in which the RFID tags

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2794996, IEEE Transactions on Industrial Informatics

are attached to some objects, such as medication management devices, medical auxiliary equipment, medical assets, and even the patients themselves. Moreover, the fixed or portable readers can recognize these tags to get the useful information about these objects and then communicate reliably with the server over some computer terminals. In addition, the legitimate persons in charge of the different corresponding parts can get access to the information in the server through the Internet, the whole of which is efficient and intelligent. For example, an authorized doctor can remotely get the patient's vital signs and give the patient reasonable advice so that the patient can get better rapidly. Of course, the patient's relatives can also obtain their family's health status immediately and they can communicate with the doctors in time and give better medical solutions together. Therefore, the RFID-enabled Healthcare System supplies a better method of controlling and administration in medical healthcare field. In addition, in medical health environment, RFID promotes better management of critical healthcare assets such as wheel-chairs as well as medical supplies by enabling real-time identification, tracking and tracing, to avoid some unnecessary medical accidents. Besides that, the effective use of RFID technology in the medical field has the potential to provide tremendous benefits in terms of efficiency, quality and management [28].

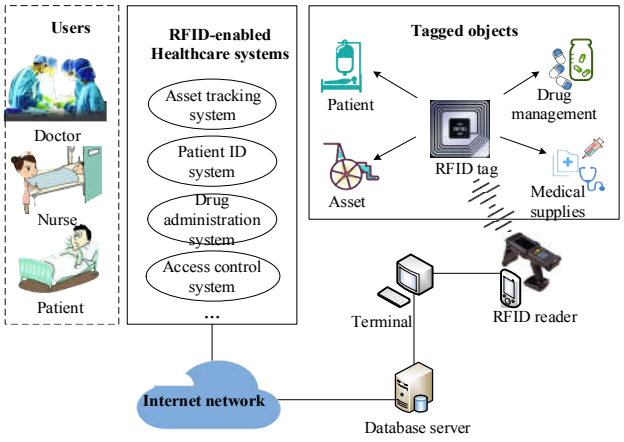

Fig. 3. RFID based medical health system

RFID technology holds tremendous potential in terms of improving the management of patients within the medical supply chain, which also faces the huge risk of medical privacy leakage. Medical privacy is of the utmost importance. It is related to the patient's health and privacy information. Once leaked, it not only brings huge economic losses and loss of credibility to the hospitals and other related institutions, but also does potential harm to patients, and more importantly, it even endangers the lives of patients, which will seriously damage the healthy development of the medical industry. Therefore, while improving the medical workflow management, there is a requirement for RFID technology to strengthen the security of medical privacy.

C. Requirement of RFID based Medical System

RFID is one of the core technologies of IoT, and in RFID system the reader relays signals from tag to the back-end server, and the back-end server helps the reader to verify tag according to the backend database. As showed in Fig. 4, there are two typical architectures for RFID system, one is that the connection between the server and the reader is wired, and the reader accordingly is fixed without the ability to move easily, while another is that the connection between the server and the reader is wireless, and the reader is portable.

In the first architecture mode, it is special cable connection between the reader and the server, so the channel is deemed to be safe, while the channel of the second one is regarded as unsafe because of the wireless connection between the server and the reader. However, with the rapid development of mobile internet, the second RFID system architecture has been becoming the mainstream, which is the main consideration in this article. In addition, in both architectures, the security of the front-end communication between the RFID tag and the reader needs to be considered.

The application of RFID technology in the medical field means it is necessary to ensure reliable and secure access to medical information of patients as well as sensitive information management. Therefore, the RFID system is required to meet the security authentication and communication between the server and tags. More importantly, it must be ensured that user's sensitive privacy information will not be leaked. Moreover, RFID authentication is the primary method to make an RFID system safe and protect privacy well. Authentication protocol is of importance for wireless communication, and researches on RFID authentication protocols have been very thorough. Chien proposed a mutual authentication protocol [29], which ensures synchronization and anti-replay attacks as well as being conformation to the standards of EPC Class 1 Generation 2, but it lacks of RFID tags anonymity, which are crucial in the healthcare system, the anonymity of the patient's identity is closely related to the safety of the vital signs. From this analysis research [30], we can know the Gossamer protocol lacks the features of forward security and anti-DoS attacks despite its anonymity. Sarah presented a cloud-based RFID protocol [31], it is with good scalability and storage performance. However, like Chien's scheme, it lacks anonymous protection of tags. Another authentication technology proposed by Zhou [32] mainly focuses on using fewer resources on a tag for authentication. The problem is, even if they are able to achieve greater security and efficiency, their approach does not focus on providing privacy to users.

When it comes to designing a suitable protocol that meets the demands of the RFID system architecture, taking into account the development status of mobile Internet, it is not only necessary to consider the security of communication between tags and readers, but also imperative to take the security between the server and the reader into account. In addition, in order to facilitate future deployment, there is a need to design a low-cost RFID tag system, while the whole architecture also needs to be lightweight so that it is indispensable to use some simple operations [33]. More importantly, for the purpose of security concerns in the special medical environment, the system needs to have some protective abilities, like

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2794996, IEEE Transactions on Industrial Informatics

anti-interference, tag anonymity. To meet the requirements in medical context, we propose a RFID authentication scheme with privacy protection.

III. LIGHTWEIGHT RFID SCHEME

A. Notations

Before introducing the proposed authentication protocol, we first present some of the notations involved in the scheme as well as its implication, which are shown in Table I.

TABLE I

Notation	DESCRIPTION
RID	The identification of a RFID reader
TID	The identification of a RFID tag
N_R	A random number generated by a reader
N_T	A random number generated by a tag
N_S	A random number generated by cloud
K	The current session number
K_{new}	The next session number
$PRNG(\ )$	The *PRNG* (Pseudo Random Noise Generation) function
$Cro(x, y)$	The operation of cross
$Rot(x, y)$	The operation of rotation, $x = W(y)$
$\oplus$	The bitwise *XOR* operation
P	The concatenation operation
$Mark$	The status of the last session

B. Cross Operation

$Cro(x,y)$ represents the operation of bit cross. Supposing that and are two bit strings with the same length of N bits, namely

$$X = a_1 a_2 \mathrm{K}\ a_k, a_i \in \{0,1\},\ i = 1,2,\cdots\cdots,k$$

$$Y = b_1 b_2 \mathrm{K}\ b_k,\ b_j \in \{0,1\},\ j = 1,\ 2,\cdots\cdots,k$$

In order to simplify the specific operation, assuming X and Y are 8 bits, for example $X = 10110100$ and $Y = 01011100$, while $\sim X$ means the not operation on X and $\sim Y$ means the not operation on Y. So, $\sim X = 01001011$ and $\sim Y = 10100011$, the length of which is the same with X or Y. In the next, cascade operation on $\sim X$ and Y as well as the cascade operation on $\sim Y$ and X will be executed. Therefore $\sim X \| Y = 0100101101011100$ and at the same time $\sim Y \| X = 1010001110110100$. It is obvious that both $\sim X \| Y$ and $\sim Y \| X$ are 16 bits, the length of which is twice that of X or Y. Then, the core operation is that the odd number bit value of $\sim X \| Y$ makes XOR operation with the even number bit value of $\sim Y \| X$, and the operation result is regarded as the odd digit part of the final result , while the even number bits of $\sim X \| Y$ makes XOR operation with the odd number bit value of $\sim Y \| X$, and the operation result is regarded as the even digit part of the final result, which denotes by $Cro(X,Y)$. Regardless of whether the bit length of X or Y is odd or even, the bit length of $\sim X \| Y$ and $\sim Y \| X$ is even, and so is the bit length of $Cro(X,Y)$ as long as the length of X is Y the same. In the result, the same weight information of X and Y is involved in the final result of the cross operation.

C. Index Data Table

In this scheme, IDT (Index Data Table) is adopted, which will improve the efficiency of information retrieval in server. The details of IDT are shown in Table II, including index value and index content.

TABLE II

Index value	Index content
$Cro(RID \oplus TID, K_1)$	$Rot(K \oplus TID, K_1 \oplus RID)$
$Cro(RID \oplus TID, K_2)$	$Rot(K \oplus TID, K_2 \oplus RID)$
…	…
$Cro(RID \oplus TID, K_i)$	$Rot(K \oplus TID, K_i \oplus RID)$
…	…

In this table, the index content $Rot(K \oplus TID, K_i \oplus RID)$ is located and obtained efficiently through the index value $Cro(RID \oplus TID, K_i)$, and every couple of index value and index content is unique. The way they work is similar to the key-value mode, and both of them are stored in a form of cipher text rather than plaintext by some cross and rotation operation. In addition, as explained in table I, K denotes the session serial number, and i denotes the session number. It is updated in every session process, that is to say it will participate in the next updating calculation operation. Furthermore, in every session, K is updating constantly, and it makes sure that the index value $Cro(RID \oplus TID, K)$ is fresh, which can improve the retrieval efficiency. After every successful session, the status of $Mark$ changes to "10" from "00", and accordingly the index value as well as the index content updates to adapt the next session.

D. The proposed protocol

Our proposed lightweight RFID authentication protocol is showed in Fig. 4.The details of the protocol is as following:

In the 1st step, before communicating with the tag, the reader generates a random number N_R, and it initializes the information of $Query$, then sends it as well as N_R to the tag. The tag obtains N_R, and sets the value of $Mark$ to "00", which indicates a new session starts. Then the tag computes $Cro(RID \oplus TID, K)$ and sends it as well as N_T to the reader, and the reader sends them and N_R to the server directly.

In the 2nd step, the server obtains N_R and N_T, and then searches the corresponding index content in the IDT according to the received index value $Cro(RID \oplus TID, K)$. If not matched, it means that the index value is wrong and the protocol will stop. However, if matched, it indicates the last session is done correctly and the current session is executable. Then N_S is generated in the server end. After those operations are done, the server sends both $Cro(RID \oplus TID, K \oplus N_S)$ and $Rot(K \oplus TID, K \oplus RID) \| N_S \oplus K$ to the reader.

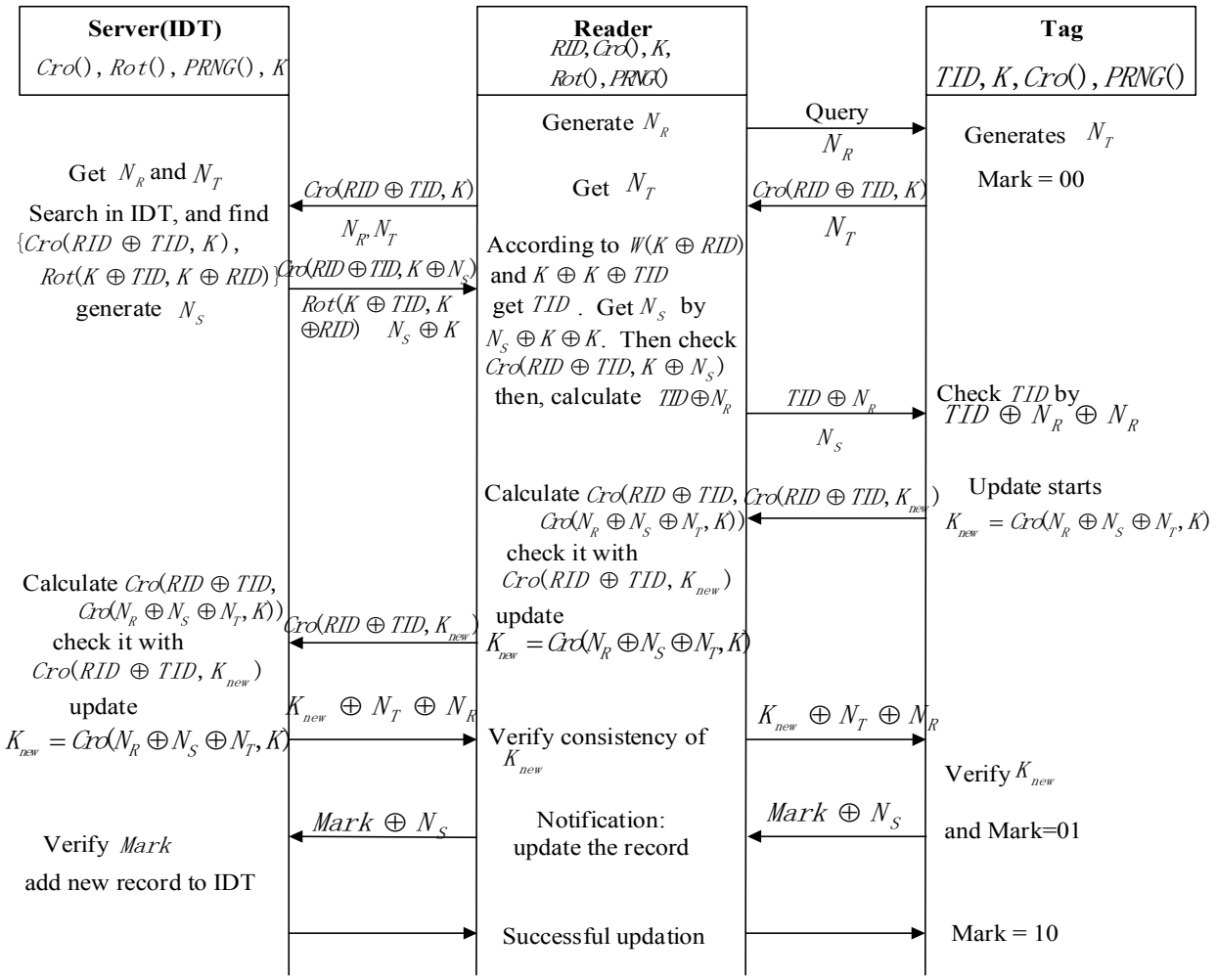

Fig. 4. The proposed authentication protocol

The 3rd step is to check TID and obtain N_S in the reader. According to the hamming weight $W(K \oplus TID)$ of the rotation operation and $K \oplus K \oplus TID$, TID is obtained, and at the same time, N_S is gotten through the XOR operation of conducting $N_S \oplus K \oplus K$. Then verify the value $Cro(RID \oplus TID, K \oplus N_S)$ by comparing the received value with the calculated value in local. If OK, calculate $TID \oplus N_R$ and $TID \oplus N_S$, and send them to the tag.

The 4th step is executed in the tag. Firstly, N_S is obtained, and then TID is checked by conducting the XOR operation between $TID \oplus N_R$ and N_R received before. After that, the three random numbers is acquired, they are N_T, N_R, N_S. Then the session number K starts to update, and the new K is recorded as K_{new}, furthermore $K_{new} = Cro(N_R \oplus N_S \oplus N_T, K)$. It is important to note that during the first session, K is a default value shared by the tag and reader as well as the server. Before the next phase, the tag sends $Cro(RID \oplus TID, K_{new})$ to the reader.

The 5th step is to continue to update K in the reader and in the server. Taking advantage of some calculated parameters, including $RID, TID, N_R, N_S, N_T, K$, the reader as well as the server executes $Cro(RID \oplus TID, Cro(N_R \oplus N_S \oplus N_T, K))$, and compares it with the received $Cro(RID \oplus TID, K_{new})$. If they are equal, the K in the reader updates to be $K_{new} = Cro(N_R \oplus N_S \oplus N_T, K)$.

After step 5, some operations of verifying the consistency of K_{new} are done in the server, the reader as well as the tag. In 6th step. The server sends $K_{new} \oplus N_T \oplus N_R$ to the reader and the reader also sends it to the tag. In addition, both of them conduct the same operation, they verify K_{new} by getting it through the operation of $(K_{new} \oplus N_T \oplus N_R) \oplus N_T \oplus N_R$ and check it with the previous K_{new} value calculated before. If the verification is smooth, $Mark$ is set to be "01", indicating the synchronization about K is completed.

In step 7, the tag sends it to the server, and the server obtains $Mark$ and checks it. If its value is "01", the server knows that K_{new} is of consistency, and a new record $\{Cro(RID \oplus TID, K_{new}), Rot(K_{new} \oplus TID, K_{new} \oplus RID)\}$ will be generated and added to the IDT, after which the notification that the record completes the update is sent to the tag, and the tag set the value of $Mark$ to "10". Until now, the proposed authentication protocol is completed.

IV. A NALYSIS AND EVALUATION

Some related analysis and evaluation about the proposed protocol are given in this section. In addition, the security proof of this protocol is described by BAN logic proof.

A. Security and privacy analysis

In this section, we give brief security analysis of our scheme against some different common possible attacks in an RFID system.

a) Tag Anonymity

The anonymity of the tag is the basis for RFID systems to prevent identity information tracking. In addition, anonymity can help the tag to achieve identity privacy protection. As to the attackers, they cannot define the identity of the tag even they illegally access to relevant information [34, 35]. In our scheme, TID denotes the identity of the RFID tag. As the secret of tag, it is transmitted in the form cipher text of and never disclosed publicly because it is never communicated directly between the tag and reader, and it is only stored locally in the tag and used for a legal identity authentication in step 3 in the protocol. Therefore, the tag anonymity in our scheme is satisfied.

b) Replay attack resistance

Obtaining the message of the current session hardly does a contribution to doing some further operations in the next session for the attackers. In our scheme, the tag generates N_T, the reader generates N_R, and the server generates N_S, moreover, those random numbers will change in the next session. K is the new session key number gotten from $K_{new} = Cro(N_R \oplus N_S \oplus N_T, K)$, and apparently it will also update in the next session. Therefore, if the attackers somehow get those messages, they cannot attack the next session with that information so that the further session is secure still. Therefore, our scheme can withstand replay attacks.

c) Consistent synchronization

Synchronization is critical to a real-time system. In our scheme, the session key number K is updated orderly and its consistency is ensured by verifying the validity. In addition, our scheme sets the $Mark$, which is a two-bit flag and used for signing the current system synchronization status, is very simple and effective. It has three status values, representing three different statuses. If $Mark = 00$, it indicates that it is in the state of establishing session, which means that the synchronization has not yet been completed. $Mark = 01$ represents the consistency of K has been completed. Moreover, it is to say that the synchronization status of the whole session is normal if $Mark = 10$.

d) Forward secrecy

If an attacker gets access to any secret information about the session illegally, the attacker will not able to obtain any useful information about the previous session. In the session of our scheme, the random numbers N_R, N_S, N_T and K are just used for current session, it is hard to obtain their previous value. In addition, they are changed in every session, and $K_{new} = Cro(N_R \oplus N_S \oplus N_T, K)$, indicating that the value of K_{new} changes in each session. It means any secret message containing those parameters or consisting of them is fresh in current session, so it is difficult for the attacker to obtain the any useful previous information according to the current messages. Therefore, the proposed scheme is of forward secrecy.

e) Mutual authentication

In the mobile RFID environment, both of the channels between the tag and the reader as well as the reader and the server should be considered to guarantee security authentication. In our scheme, upon receiving $Cro(RID \oplus TID, K)$ from the reader, the server searches the index value, and if the index content $Rot(K \oplus TID, K \oplus RID)$ accordingly is located, it means the identity of the reader is legitimate; the reader authenticates the server when it obtains K and uses it to verify $Cro(RID \oplus TID, K \oplus N_S)$ from the server. In addition, the tag authenticates the reader by verifying TID when it receives $TID \oplus N_R$ from the reader, while the tag is authenticated by the reader via verifying the $Cro(RID \oplus TID, K_{new})$. Therefore, the mutual authentication is satisfied.

f) Anti-DoS attack

Denial of Service (DoS) attack is a common attack in the RFID system. Its goal is to stop the server system from responding or even make it crash directly. In the proposed protocol, a new data storage format is designed that exists in the form of a group of index values and index content in IDT, and the homologous content can be retrieved based on the index value without violent matching by using traversal search. It is obviously reduces the performance overhead greatly, and will not easily suffer DoS attacks.

In order to facilitate further comparison and analysis, we select some related typical protocol schemes [29, 30, 24, 31] to be compared with our scheme, the security features of which are showed in table IV, in which "√" means the corresponding property is satisfied while "×"means the corresponding property is not satisfied, and "~" means that the protocol doesn't refer to the property. The table III is following:

TABLE III
SECURITY PERFORMANCE COMPARISON

Authentication protocols	Tag anonymity	Replay attack resistance	Synchronization attack resistance	Forward secrecy	Mutual authentication	Anti-DoS attack
Chien Protocol	×	√	√	×	√	×
Gossamer Protocol	√	×	×	√	√	×
Xie Protocol	×	√	√	√	×	√
Sarah Protocol	×	√	√	√	√	√
New Protocol	√	√	√	√	√	√

From the table III, the mutual authentication protocol SASI proposed by Chien. It is of replay attack resistance and ensuring synchronization during the session. However, it is absent of anonymity and forward security as well as the capacity of anti-DoS attack. It is vital to the medical environment to make the tag anonymous, so the absence of this security feature makes it easy to obtain the identity of the tag illegally, and the attacker can get access to the secret information of the previous sessions. The Gossamer protocol was proposed to address the issues of mutual authentication and the anonymity. However, it is weak to resist the attacks like replay and DoS. Moreover, compared with other schemes, its synchronization performance is very poor so that it cannot resist the non-synchronization attack, which will result in wrong communication even system crash during the authentication process. Xie .et.al proposed a RFID authentication protocol. It can withstand replay attack, synchronization attack and the forward security attack. Nevertheless, the protocol has a fatal drawback that mutual authentication is absent between the reader and the server, which will make the RFID system face the risk of identity forgery attacks. Relatively speaking, in terms of security performance, the Sarah protocol does better than those four preceding protocols. This protocol is an upgraded version of the protocol, and it implements mutual authentication and can withdraw various attacks. Unfortunately, some message is transmitted in a form of clear-text during the wireless channel, and therefore both the confidentiality and anonymity cannot be guaranteed if an attacker as an intermediary intercepts those message. Compared with above protocol, the proposed mutual authentication scheme does better in the several security aspects, it can prevent replay attack, non-synchronization attack and DoS attack, moreover, it can ensure forward secrecy and guarantee the RFID tag anonymous.

B. Performance analysis

In this part, we will compare the proposed scheme with some other protocols in performance aspect [36], including the computation cost comparison and communication cost comparison.

TABLE IV
COMPUTATION COST COMPARISON

Schemes	Cost
Chien's protocol	$\oplus$, $\wedge$, P, *Rot*
Gossamer protocol	$\oplus$, $\wedge$, Rot^2
Xie's protocol	$\oplus$, P, *Hash*
Sarah's protocol	$\oplus$, $\wedge$, P, *Hash*
New protocol	$\oplus$, P, *Cro*, *Rot*

In Table IV, "$\oplus$" is the XOR operation, "$\wedge$" is the power exponentiation, "P" is the cascade operation, "*Rot*" is the displacement operation, "*Hash*" is the hash operation and "*Cro*" is the cross operation defined before. Moreover, the cost of operation like "$\oplus$" and "*Rot*" is less relatively. From Table IV, we can know all of Chien's protocol and the Gossamer protocol as well as Sarah protocol use the power exponentiation while both of Xie's protocol and Sarah protocol use hash operation, and the cost of these operation is higher than other operations referred in Table IV. What is different about the proposed scheme compared with those is that it uses the lightweight operations listed in the Table IV and costs less computation resources.

TABLE V
COMPUTATION COST OF CROSS OPERATION IN TAG END

Device Utilization Summary			
Slice Logic Utilization	Used	Available	Utilization
Number of Slice Registers	0	82000	0%
Number of Slice LUTs	1	41000	1%
Number used as logic	1	41000	1%
Number used as memory	0	13400	0%
Number of occupied Slices	1	10250	1%

As it is known, the tag's computational power is limited relative to reader and server. In the tag end, the computation cost of cross operation is showed in Table V. The experiment is carried out in the FPGA system showed in Fig. 5, where all the parameter length of cross operation is set to 1024 bits. As seen from Table V, the computation cost of cross operation is denoted with "Used" column while the available resources are denoted with "Available" column in the FPGA system. "Utilization" is calculated and generated by the experiment system itself. All the data is outputted from the FPGA system. So it is easy to know cross operation consumes less computation resource (just one LUT), which reduces the computational burden on the tag. Therefore, this mutual authentication scheme is lightweight.

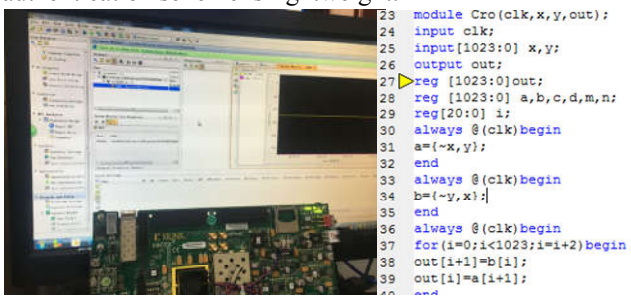

Fig. 5. The FPGA system for performance simulation of cross computation

In addition, in the aspect of communication cost, the comparison analysis is presented in Table VI, in which we compare the proposed protocol with some typical schemes. It should be noted that, L is assumed to be the length of communication data in every time. In addition, "Times" represents the communication times during a whole authentication process, and "Cost" represents the resource consumption of a communication process. From the below table, it is not hard to know that compared with other protocols, the new scheme spends 5 times for an authentication communication, and it is little more than other three protocols. Besides, it costs 8L, which does not have the advantage in the aspect of communications resources. Overall, compared with other protocols, the new scheme is not very outstanding at communication consumption.

TABLE VI
COMMUNICATION COST COMPARISON

Scheme	Times	Cost
Gossamer protocol	4	6L
Xie's protocol	3	8L
Sarah's protocol	4	7L
New protocol	5	8L

C. BAN logic proof

BAN logic [37] is a kind of modal logic based on agreement belief. In the reasoning process of BAN logic, the beliefs of the protocol subjects evolve and change with the exchange of the authentication messages. In the process of BAN logic, the "ideal process" needs to be done firstly, which is aimed at converting the protocol message to the BAN logic formulas. Then with the help of a reasonable assumption according to the specific circumstances, BAN logic proof can test the correctness of the agreement and judge whether the objectives of the protocol have been reached. As a formal analysis method, it has been used in a variety of cryptographic authentication agreements, and it has the advantages of direct viewing, simplicity and high efficiency [38].

Before introducing the BAN logic foundation rules, we briefly introduce the syntax and semantics of it.

1. $P|\equiv X$: The entity P believes X is true.
2. $P<X$: The entity P receives the message containing X, meaning a certain entity Q sends a message containing X to P.
3. $P|\sim X$: The entity P sent out message containing X before.
4. $P|\Rightarrow X$: Entity P has jurisdiction over X.
5. $\#(X)$: X is of freshness.
6. $P\xleftrightarrow{K}Q$: K is a shared key between P and Q, and other entities do not know K except P and Q as well as the entities they believe.
7. $\xrightarrow{K}P$: K is the public key of P, and no entities know the corresponding secret key K^{-1} except P and its trusted entities.
8. $P\overset{K}{\rightleftarrows}Q$: K is the shared secret of P and Q, and other entities do not know K except P and Q and the entities they believe.
9. $<X>_Y$: A message composed of X and the secret Y.
10. $\{X\}_K$: The cipher text obtained by encrypting X with the key K.

Next, some basic proof rules of BAN logic are given based on above syntax and semantics.

1) The basic rules of BAN logic

There are 19 inference rules divided into 7 types in BAN logic, and the nth inference rule is abbreviated as Rn. In the following inference rule, $\vdash$ is a meta-linguistic symbol, which means that the conclusion is drawn from the premise.

(1) Message meaning rules

R1: $P|\equiv Q\xleftrightarrow{K}P, P<\{X\}_K \vdash P|\equiv Q|\sim X$. It means if P believes Q shares key K with P, and P receives the message X enciphered by K, which indicates P believes Q sent message X before. And similarly, for the public secrets and sharing secrets situations, there are R2 and R3.

R2: $P|\equiv \overset{K}{\rightarrow}Q, P<\{X\}_{K^{-1}} \vdash P|\equiv Q|\sim X$.

R3: $P|\equiv P\overset{Y}{\leftrightarrow} Q, P<\{X\}_Y \vdash P|\equiv Q|\sim X$.

(2) Message meaning rule

R4: $P|\equiv \#(X), P|\equiv Q|\sim X \vdash P|\equiv Q|\equiv X$. It means if P believes X is fresh and Q sent X before, which indicates P believes Q believes X.

(3) Jurisdiction rule

R5: $P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X \vdash P|\equiv X$. It means if P believes that Q has jurisdiction over message X and P believes Q believes X, then P believes X.

(4) Seeing rules

There are five rules in this part, they are:

R6: $P<(X,Y) \vdash P<X$.

R7: $P<<X>_Y \vdash P<X$.

R8: $P|\equiv P\xleftrightarrow{K}Q, P<\{X\}_K \vdash P<X$.

R9: $P|\equiv \xrightarrow{K}P, P<\{X\}_K \vdash P<X$.

R10: $P|\equiv \xrightarrow{K}Q, P<\{X\}_{K^{-1}} \vdash P<X$.

Above rules mean if an entity has received a formula and the entity knows the associated key, then the entity has received the component part of the formula.

(5) Freshness rule

R11: $P|\equiv \#(X) \vdash P|\equiv \#(X,Y)$. It means if a part of a formula is fresh, then all of it is fresh.

For the sake of conciseness, only the reasoning rules are listed in the next and the explanations of these rules are omitted.

(6) Belief rules

This part has four rules, and they are:

R12: $P|\equiv X, P|\equiv Y \vdash P|\equiv (X,Y)$

R13: $P|\equiv (X,Y) \vdash P|\equiv X$

R14: $P|\equiv Q|\equiv (X,Y) \vdash P|\equiv Q|\equiv X$

R15: $P|\equiv Q|\sim (X,Y) \vdash P|\equiv Q|\sim X$

(7) Key and secret rules

There are four rules in this part too, and they are:

R16: $P|\equiv R\xleftrightarrow{K}R' \vdash P|\equiv R'\xleftrightarrow{K}R$

R17: $P|\equiv Q|\equiv R\xleftrightarrow{K}R' \vdash P|\equiv Q|\equiv R'\xleftrightarrow{K}R$

R18: $P|\equiv R\overset{X}{\leftrightarrows}R' \vdash P|\equiv R'\overset{X}{\leftrightarrows}R$

R19: $P|\equiv Q|\equiv R\overset{X}{\leftrightarrows}R' \vdash P|\equiv Q|\equiv R'\overset{X}{\leftrightarrows}R$

After introducing the basic rules of BAN logic, we will apply them to prove the proposed scheme.

2) Protocol description

In this part, some formal expressions will be given out to describe the process of transmitting information between the protocol entities, in which T denotes the tag, R denotes the reader and S denotes the server.

(1) $R\rightarrow T: query, N_R$

(2) $T\rightarrow R: \{Cro(RID\oplus TID, K)\}_K, N_T$

(3) $R \to S: \{Cro(RID \oplus TID, K)\}_K, N_R, N_T$

(4) $S \to R: \{Cro(RID \oplus TID, K \oplus N_S), Rot(K \oplus TID, K \oplus RID) \| N_S \oplus K\}_{N_S, K}$

(5) $R \to T: \{TID \oplus N_R\}_{N_R}, N_S$

(6) $T \to R: \{Cro(RID \oplus TID, K_{new})\}_{K_{new}}$

(7) $R \to S: \{Cro(RID \oplus TID, K_{new})\}_{K_{new}}$

(8) $S \to R: \{K_{new} \oplus N_T \oplus N_R\}_{N_T, N_R, K_{new}}$

(9) $S \to R: \{K_{new} \oplus N_T \oplus N_R\}_{N_T, N_R, K_{new}}$

(10) $T \to S: \{Mark \oplus N_S\}_{N_S}$

3) Initial assumptions of protocol

Some reasonable assumptions based on the proposed protocol are as follows:

(11) $T \mid\equiv T \xleftrightarrow{K} R, \mathrm{R} \mid\equiv R \xleftrightarrow{K} T$

(12) $R \mid\equiv R \xleftrightarrow{K} S, S \mid\equiv S \xleftrightarrow{K} R$

(13) $S \mid\equiv S \xleftrightarrow{K} T, T \mid\equiv T \xleftrightarrow{K} S$

(14) $R \mid\Rightarrow N_R, R \mid\equiv \#(N_R), R \mid\equiv T \mid\equiv C \xleftrightarrow{N_R} R$

(15) $T \mid\Rightarrow N_T, T \mid\equiv \#(N_T), T \mid\equiv R \mid\equiv C \xleftrightarrow{N_T} T$

(16) $C \mid\Rightarrow N_C, C \mid\equiv \#(N_C), C \mid\equiv R \mid\equiv T \xleftrightarrow{N_C} C$

(17) $T \mid\equiv R \mid\equiv C \mid\equiv \#(K)$

4) The goals of the protocol

The goal of the agreement in the open environment is to achieve the mutual authentication between the tag and the reader for subsequent communication to establish a new session key.

(a) $S \mid\equiv R \mid\equiv \{Cro(RID \oplus TID, K)\}_K$

(b) $R \mid\equiv S \mid\equiv \{Cro(RID \oplus TID, K \oplus N_S), Rot(K \oplus TID, K \oplus RID) \| N_S \oplus K\}_K$

(c) $R \mid\equiv T \mid\equiv \{Cro(RID \oplus TID, K_{new})\}_{K_{new}}$

(d) $T \mid\equiv R \mid\equiv \{K_{new} \oplus N_T \oplus N_R\}_{K_{new}}$

(e) $T \mid\equiv R \mid\equiv S \xleftrightarrow{K_{new}} T$

5) Proving process of protocol

Next, we will give out the demonstration details about the protocol, in which $A \vdash B$ means that A deduces B.

From the step 1 and step 2, we can know that:

$$S < \{\{Cro(RID \oplus TID, K)\}_K, N_R, N_T\} \tag{18}$$

Eq. (12) indicates that no one knows K apart from the reader and the server as well as other entities they believe. So combining with the message seeing rule $\{P < (X, Y) \vdash P < X\}$, we can know:

$$S < \{Cro(RID \oplus TID, K)\}_K \tag{19}$$

According to the message meaning rule $\{P \mid\equiv Q \xleftrightarrow{K} P, P < \{X\}_K \vdash P \mid\equiv Q \mid\sim X\}$ and Eq. (12) as well as Eq (19), we can deduce:

$$S \mid\equiv R \mid\sim \{Cro(RID \oplus TID, K)\}_K \tag{20}$$

In addition, on the basis of message freshness rule $\{P \mid\equiv \#(X) \vdash P \mid\equiv \#(X, Y)\}$ and Eq. (17), we may obtain:

$$S \mid\equiv \#\{Cro(RID \oplus TID, K)\}_K \tag{21}$$

Since the nonce verification rule $\{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X \vdash P \mid\equiv Q \mid\equiv X\}$, and combine the Eq. (21) and Eq. (20), we can prove:

$$S \mid\equiv R \mid\equiv \{Cro(RID \oplus TID, K)\}_K \tag{22}$$

So, according to the above proof process, the first goal (a) has been demonstrated.

Similarly, we can describe the message sent to the reader from the server as $R < \{Cro(RID \oplus TID, K \oplus N_S), Rot(K \oplus \ TID, K \oplus RID) \| N_S \oplus K\}_K$, and combine the principle of Eq. (20) and Eq. (21) as well as Eq. (22), it is smoothly to achieve $R \mid\equiv S \mid\equiv \{Cro(RID \oplus TID, K \oplus N_S), Rot(K \oplus TID, K \oplus RID) \mathrm{P} N_S \oplus K\}_K$, namely the goal (b).

By the same way, we can demonstrate the both the goal (c) and (d).

According to Eq. (11, 12, 13) and the process of the front demonstration, we can obtain $T \mid\equiv R \xleftrightarrow{K_{new}} T$ and $R \mid\equiv S \xleftrightarrow{K_{new}} R$. Furthermore, combing the message key and secret rules $P \mid\equiv R \xleftrightarrow{K} R_1 \vdash P \mid\equiv R_1 \xleftrightarrow{K} R$ and $P \mid\equiv Q \mid\equiv R \xleftrightarrow{K} R_1 \vdash P \mid\equiv Q \mid\equiv R_1 \xleftrightarrow{K} R$, we can see:

$$T \mid\equiv R \mid\equiv S \xleftrightarrow{K new} T \tag{23}$$

So far, all the goals of the protocol have been proved so that the proposed scheme in this paper satisfies the logic security.

V. CONCLUSION

As a core technology of the Internet of things, RFID technology plays a very important role. In the international background, with the increasing level of medical technology, more and more associated privacy data will be generated, and correspondingly, the security of the RFID system in the medical environment has also received more and more attention.

The application of RFID system to the medical field, can realizes the convenience and safe management of medical privacy information. In this paper, we present a lightweight mutual security authentication protocol that can be applied to mobile medical fields. Medical privacy information is of paramount importance to users or assets, and in this scheme, the consistency and synchronization of the authentication information is guaranteed. Moreover, it can resist against the typical attacks. It is important to emphasize that in the medical context, personal identity information is extremely important and closely related to patient's privacy, and the proposed scheme ensures the anonymity of the tag, in line with the security requirements of medical system. In addition, this protocol uses the innovative index group to carry on the storage of authentication data, which is easy to retrieve and locate.

Next, we will continue to focus on the application of RFID systems in the medical field, and optimize the consumption of the protocol in communication performance.

REFERENCES

[1] G. S. Turner, K. Tjaden, "United Nations, Department of Economic and Social Affairs, Population Division, World Fertility Report 2013: Fertility

at the Extremes," Population & Development Review, 2015, 41(3): R6987-R6989.
[2] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X. Li, "S2M: a lightweight acoustic fingerprints based wireless device authentication protocol," IEEE IoT Journal, 2017, 4(1): 88-100.
[3] J. Linders and G. Björk, "Real-time location and inpatient care systems based on passive RFID," Journal of Network & Computer Applications, 2011, 34(3): 980-989.
[4] G. Z. Papadopoulos, A. Gallais, G. Schreiner, E. Jou, T. Noel, "Thorough IoT test bed characterization: from proof-of-concept to repeatable experimentations," Computer Networks, 2017, 119:86-101.
[5] S. Tedeschi, J. Mehnen, N. Tapoglou, R. Roy, "Secure IoT devices for the maintenance of machine tools,". in *Proc. TLES*, 2017, pp. 150-155.
[6] P. P. Ray, "A survey of IoT cloud platforms," Future Computing & Informatics Journal, 2017, 1-12.
[7] K. Fan, Y. Gong, C. Liang, H. Li, Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," Security and Communication Networks, 2016, 9(16): 3095-3104.
[8] K. Fan, J. Li, H. Li, X. Liang, X. Shen and Y. Yang, "RSEL: revocable secure efficient lightweight RFID authentication scheme," Concurrency & Computation Practice & Experience, 2014, 26(5): 1084-1096.
[9] R. Weinstein, "RFID: a technical overview and its application to the enterprise," It Professional, 2005, 7(3): 27-33.
[10] D. He, S. Chan, Y. Zhang, H. Yang, "Lightweight and confidential data discovery and dissemination for wireless body area networks," IEEE Journal of Biomedical & Health Informatics, 2017, 18(2): 440-448.
[11] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. Luo, "Security and Privacy for Mobile Healthcare Networks-from quality-of-protection perspective," IEEE Wireless Communications, 2015, 22(4): 104-112.
[12] K. Zhang, X. Liang, J. Ni, K. Yang, and X. Shen, "Exploiting social network to enhance human-to-human infection analysis without privacy leakage," IEEE Transactions on Dependable and Secure Computing, to be published.
[13] Y. Tian, G. Chen, J. Li, "A new ultralightweight RFID authentication protocol with permutation," IEEE Communications Letters, 2012, 16(5): 702-705.
[14] Kubo, "The research of IoT based on RFID technology," in *Proc. ICTA*, 2014, pp. 832-835.
[15] J. Zhu, J. Zhu, "RFID technology in Internet of Things," Tachnical Application, 2010, 10: 65-66.
[16] H. Zhu, F. Wang, R. Suo, "The application of the Internet of Things in China modern agriculture," Chinese Agricultural Science Bulletin, 2011, 27(02): 310-314.
[17] Y. Zhang, R. Yu, S. Xie, W. Yao, "Home M2M networks: architectures, standards, and QoS improvement," IEEE Communications Magazine, 2011, 49(4): 44-52.
[18] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, "Cognitive machine-to-machine communications: visions and potentials for the smart grid," IEEE Network, 2012, 26(3): 6-13.
[19] K. Fan, P. Song, Y. Yang, "ULMAP: ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G," Mobile Information Systems, 2017, 2017(2349149): 1-7.
[20] R. Want, "An introduction to RFID technology," IEEE Pervasive Computing, 2006, 5(1): 25−33.
[21] W. Baoyun, "Review on Internet of Things," Journal of Electronic Measurement and Instrument, 2009, 23(12): 1-7.
[22] J. Leu, "The benefit analysis of RFID use in the health management center—The experience in Shin Kong Wu Ho-Su Memorial Hospital," M.A. thesis, College of Management, National Taiwan Univ., Taipei City, Taiwan, 2010.
[23] W. Yao, C. Chu, and Z. Li, "The adoption and implementation of RFID technologies in healthcare: A liter-ature review," Journal of Medical Systems, 2012, 36(6): 3507-3525.
[24] W. Xie, L. Xie, C. Zhang, "Cloud-based RFID authentication," in *Proc. RFID*, 2013, pp. 168-175.
[25] L. Chu and S.-J. Wu, "An integrated building fire evacuation system with RFID and cloud computing," in *Proc. IIHMSP*, 2011, pp. 17-20.
[26] D. He and S. Zeadally, "An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography," IEEE Internet of Things Journal, 2014, 2(1): 72-83.
[27] F. Rahman, M. Z. A. Bhuiyan, S I. Ahamed, "A privacy preserving framework for RFID based healthcare systems," Future Generation Computer Systems, 2017, 72: 339-352.
[28] S. F. Wamba, A. Anand, L. Carter, "A literature review of RFID-enabled healthcare applications and issues," International Journal of Information Management, 2013, 33(5): 875-891.
[29] H. Y. Chien and C. H. Chen, "Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards," Computer Standards & Interfaces, 2007, 29(2): 254-259.
[30] Z. Bilal, A. Masood, F. Kausar, "Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: Gossamer protocol," in *Proc. NBIS*, 2009, pp. 260-267.
[31] S. Abughazalah, K. Markantonakis, K. Mayes, "Secure improved cloud-based RFID authentication protocol," in *Proc. DPMASSSA*, 2015, pp. 147-164.
[32] J. Zhou, "A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification," Journal of Communications, 2015, 10(2): 117-123.
[33] H.Liu, H. Ning, Y. Zhang, D. He, Q. Xiong, L. Yang, "Grouping-proofs-based authentication protocol for distributed RFID systems," IEEE Transactions on Parallel & Distributed Systems, 2013, 24(7): 1321-1330.
[34] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, S. Gjessing, "MixGroup: accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," IEEE Transactions on Dependable & Secure Computing, 2016, 13(1): 93-105.
[35] J. Kang, R. Yu, X. Huang, M. Jonsson, H. Bogucka, S. Gjessing, Y. Zhang, "Location privacy attacks and defenses in cloud-enabled internet of vehicles," IEEE Wireless Communications, 2016, 23(5): 52-59.
[36] K. Fan, N. Ge, Y. Gong, H. Li, R. Su and Y. Yang, "An ultra-lightweight RFID authentication scheme for mobile commerce," Peer-to-Peer Networking and Applications, 2017, 10(2): 368-376.
[37] P. F. Syverson, P. C. Van Oorschot, "On unifying some cryptographic protocol logics," in *Proc. SP*, 1994, pp. 14-28.
[38] X. Zhang and Y. Hu, "RFID mutual-authentication protocol with synchronous updated- keys based on Hash function," Journal of China Universities of Posts and Telecommunications, 2015, 22(6): 27-35.

Kai Fan received his B.S., M.S. and Ph.D. degrees from Xidian University, P. R. China, in 2002, 2005 and 2007, respectively, in Telecommunication Engineering, Cryptography and Telecommunication and Information System. He is working as an associate professor in State Key Laboratory of Integrated Service Networks at Xidian University. He has published over 40 papers in journals and conferences. He received 3 Chinese patents. He has managed 5 national research projects. His research interest include information security. The mailing address is 2 South Taibai Road, Xidian University, Xian 710071, China. The email address is kfan@mail.xidian.edu.cn.

Wei Jiang was born in 1991 in Hubei province of China. He received his B.S. degree in telecommunications engineering from Xidian University in 2015. He is studying as a master in State Key Laboratoty of Integrated Service Networks at Xidian University. His reaserch interest include information security.

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 at Key Lab. of Minist. of Educ. for Wide Band-Gap Semicon. Materials and Devices of Xidian University, Xi'an China. His research interests include semiconductor materials and devices, network and information security.