Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):708-717

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

RFID authentication protocol design via BAN logic

Minghui Wang* and Junhua Pan

Yancheng Institute of Technology, Yancheng, China

ABSTRACT

Tag cost and privacy of RFID technology are two main factors that determine whether it will be applied to Internet of Things on a large scale. Recently, RFID industry and research community have focused on RFID authentication protocols with provable privacy and low tag cost. In this paper, we propose an RFID security protocol that achieves all security requirements based on a hash function and XOR operations. In addition, BAN logic was used to do the formal analysis and proved that the proposed protocol is safe and reachable. The RFID technology is widely used for industrial and individual applications. In the latest design of RFID system, the mobile handheld reader generally is adopted, so considering the RFID system's security and efficiency, we should consider two aspects' security of reader and tags at the same time in the proposed protocol. The ensuring strong privacy has been an enormous challenge due to extremely inadequate computational power of typical RFID tags. In the proposed protocol, to achieve mutual authentication between the server and the Tags, at the same time we also achieve mutual authentication between the server and the mobile reader.

Key words: RFID, Authentication, BAN Logic, Privacy, Security

INTRODUCTION

Radio frequency identification (RFID), based on the MIT Auto-ID project [1], is a technology that uses wireless transmission to identify an object. RFID technology has many advantages, such as without physical contact, quick reading, long recognition distance, obstacle-free and so on. It mainly consists of three components: radio frequency tags, readers, and a backend server/database which maintains information on the tags and readers. RFID tag has the ability to store data, which can be read rapidly without line of sight. This is especially significant in yielding convenience, efficiency and productivity gains in industries, so it has been used by manufacturing management, intelligent school systems, logistics management, management of humans and farm animals, arrangement of books at some libraries, etc. However, the RFID system limitations (such as low cost) bright a lot of security issues, such as mutual authentication, traceability, DoS(Denial of Service), forward security , tag impersonation and tag clone, man-in-the-middle attack etc. Thus, research on RFID authentication protocols in the constrained environment becomes an important direction in the field of RFID technology. The thesis focuses on study low-cost, secure and efficient RFID authentication protocols.

Radio Frequency Identification (RFID)' application in people's daily lives becomes more and more widespread,but its application may have challenges to the security and privacy of individuals or organizations.Many researchers focused on the application and security research of RFID [2, 3, 4]. In radio frequencies, information transmitted between the reader and tag may be easily exposed to a third party, in which the information of the user's privacy may be included. Although a lot of research has already focused on solving the security problems of RFID systems, some existing RFID protocols still suffer from various security weaknesses, including authentication, location privacy, and resynchronization between two entities. A secure RFID system has to avoid eavesdropping, traffic analysis, spoofing and denial of service.

This paper is constructed as follows: Section 2 describes the structure of RFID security systems and security requirements. It also reviews the previous security methods. Section 3 describes related word.Section 4 describes protocol and the running of the proposed protocol. Section 5 gets the overview of the BAN Logic.Section 6 describes the process of protocol analysis with BAN logic and compares the security and efficiency of the proposed protocol with those of the previous security protocols. Section 7 describes conclusion.

RFID SECURITY STRUCTURE AND SECURITY REQUIREMENTS

THE STRUCTURE OF RFID SYSTEM

Generally speaking, an RFID system typically comprises the following three components [5]: An RFID device (tag); a tag reader with an antenna and transceiver; a software system or connection to an enterprise control system (Backend Server).The structure of the RFID system is shown in Fig. 1. In traditional RFID systems, the channel between card reader and the server is the cable transmission medium. In which Signal is generally recognized as safe, the researchers focus on the security problem of the wireless channel between the card readers and tags.But, in many the latest design of RFID system, card reader into a portable mobile reader, thus, the channel between the reader and server becomes wireless channel, such as GPRS, WiFi, etc.

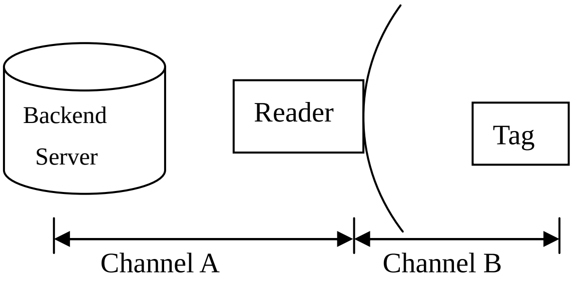


Fig. 1: The structure of RFID system

Tag: Tags are the important part of an RFID system, because they store the information that describes the object being tracked. Specific object information is stored in the memory of tags and is accessed via the radio signal of RFID readers.

An RFID tag is often confused with an RFID label. A tag is a transponder mounted on a substrate. It can be embedded in packaging or stuck on with adhesive. An RFID label is a transponder sandwiched between a layer with adhesive and paper that can be printed on.Due to cost constraints, only by the thousands of logic gate circuit, usually without a microprocessor, resulting in its computing power and storage capacity is very limited. So it is almost unrealistic that the cryptographic algorithms such as DES, AES, RSA, ECC and others are integrated into such devices .

Reader: Transceiver — also known as the reader or the interrogator, transceivers send the electronic signal to the transponder and provide the power for the transponder to send the signal back to the transceiver with the information contained in the transponder's electronic circuit. Transceivers can be powered by batteries or plugged into a traditional power supply.With respect to the RFID tag, its processing power and storage space are relatively large, the general calculation algorithm can be run in it.

The reader in the latest system consists of three parts: GPRS/WiFi Module, data conversion module and RFID tag reader/writer module. The scanning antenna of readers puts out radio-frequency signals in a relatively short range. The reader provides a means of communicating with the transponder (the RFID tag) and it sends data to the database server by the GPRS/WiFi module.

Backend Server: The backend server is considered to be the heart and soul of a comprehensive RFID system. Generally assumed the backend's computation ability, Analysis capability and storage capacity are very powerful and on which uses can run the database systems of hardware platforms ,but also can run the system of the user's own design or choose according to their actual needs, the backend's system contains information of all labels and the algorithms of computing needs, in general, the complex algorithm for computing is deployed in the backend server.It transmits data between transponder and transceiver, and between transceiver and Database system. It's the software that allows you to actually tie electronic identity to production and management information, massage the data and share the information with others.

RFID SECURITY THREATS

The advantage of RFID over barcode technology is that it does not require direct line-of-sight reading. RFID readers can interrogate tags at greater distances, faster and concurrently. Furthermore, one of the most important advantages of RFID technology is that tags have read/write capability, allowing stored information to be altered dynamically. RFID reader and the tag transmit data in the radio frequencies. Therefore, RFID is vulnerable to various forms of attack. For solutions to counter security threats in RFID systems, must carefully study the various forms of such threats. Previous studies [2, 3, 4] addressed several threats to RFID applications.

Eavesdropping: In the case of a third party does not know, the illegal user can listen in secret communication between reader and tag. In wireless communication, Eavesdropping is a common problem. An effective way to solve this problem is that both sides of each pass communication produce changing values. Therefore, the attacker cannot access to significant values even if he acquires data.

Traffic analysis: It is the process of intercepting and examining messages in order to deduce valuable information from patterns in communication between the reader and tag. In order to prevent an attacker from using this method to attack, we need to add a random number in the reader and tag communications data.

Replay attack: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. Therefore, the random value, participated in the communication process, is generated by the common reader and tag.

Tracking attack: Through repeated analysis and comparison of multiple outputs between reader and tag, an attacker gets into a constant value (In some cases, the attacker can even get the tag's ID). In this way, the attacker can track the user's location information and even get more user privacy, which is one of the most serious privacy problems of the RFID systems. Application of the random number or timestamp is an effective way to solve the problem.

SECURITY REQUIREMENTS

The RFID system consists of the tag, reader, and database. The reader sends data information received from tag to the database. The database compares the tag information sent from reader and stored information. After tag is certified by database, the database sends data (need to be certified by tag) to tag with help of reader. In the mutual authentication process, the forged data must be prohibited. However, the communication channel between the tag and reader is radio frequency; we must find effective methods to prevent the attacker to modify the authentication information. In designing our RFID authentication protocol, we set to achieve the following goals:

Confidentiality: During operation of RFID system, the electronic tag should not leak any valuable product information to the reader without permission, information contained in RFID tag once is acquired by the attacker, who will reveal the user's privacy. Thus, a perfect RFID security solution must be able to ensure that the information contained in the tag can only be authorized to read and write access.

Indistinguishability: Tag output must be indistinguishable from truly random values. Moreover, they should be unrelated to ID of the tag. If the adversary can distinguish that a particular output is from a target tag, he can trace the tag. Naturally, this is included in the concept of ID anonymity.

Forward security: Even if the adversary acquires the secret tag data stored in the tag, he cannot trace the data back through past events in which the tag was involved. Needless to say, the adversary who only eavesdrops on the tag output, cannot associate the current output with past output.

Authentication: All components of the system should go through an authentication process. The RFID is comprised of a tag, reader, and database. Each part should provide authentication to each other. The tag should send secret values, which have been previously agreed upon, to each component to become authorized. The database can reply with identification values or secret values to become authenticated by the tag.

Efficiency: Although efficiency is not included in the security requirements, passive tags require hash formulas or XOR calculation. Passive tags require applicable security measures, and therefore efficiency should be provided, too.

RELATED WORK

The user privacy in RFID systems is needed to be protected.Many approaches (how to protect user' privacy) are based on re-encryption, where a cipher text is encrypted again using asymmetric key cryptography [6] or symmetric key cryptography [7]. These approaches are more secure than the presented approaches because of protecting a tag ID using asymmetric or symmetric key cryptography. An encryption-operation requires high computation cost, and is performed in a Tag, sothe solutions based on the re-encryption are difficult to implement.EPCGen2, was approved in 2004, defines a platform for the interoperability of RFID protocols, by supporting efficient tag reading, flexible bandwidth use, multiple read/write capabilities and basic reliability guarantees, provided by an on-chip 16-bit Pseudo-random Number Generator (RNG) and a 16-bit Cyclic Redundancy Code (CRC16). EPCGen2 is designed to strike a balance between cost and functionality, with little attention paid to security.

Recently many RFID authentication protocols specifically designed for compliance with EPCGen2 have been proposed [10, 11, 12]. These combine the CRC-16 of the EPCGen2 standard with its 16-bit RNG to hash, randomize and link protocol flows, and to prevent cloning, impersonation and denial of service attacks. In this paper[13], the researchers analyze these protocols and show that they do not achieve their security goals.

At the same time, many researchers have proposed cryptographic primitives to encrypt TID in sessions. Hash function-based protocols like [14, 15, 16, 17] are taking the advantage of one-way function to prevent direct exposure of TID. They suggested using a hashed value, usually called metaID or secured SID for transmission instead of TID. To verify a tag, a verifier needs to search the back-end database and compute the same hashed value. Once the authentication is successful, the database sends data message included corresponding ID information back to the reader. For example Hash-chain-based solution [18] involves synchronized key update so that both the tag and the back-end database can communicate with each other. This method also provides forward security but often suffers from resynchronization attack.

In order to reduce the occurrence of security vulnerabilities, cryptographic protocols are safer, researchers began to use BAN Logic [19] to analyze cryptographic protocols, and to standardize the behavior of the parties in the protocol. Through this way, we can find out some security vulnerabilities that exist in the protocol.Therefore, in this paper, a Hash function based RFID authentication protocol,secure against security and privacy threats in real RFID systems, is proposed.

PROPOSED AUTHENTICATION PROTOCOL

THE NOTATIONS

The notations used for the entities and computational operations to simplify the description are as shown in table1.

Table1 Node Parameters

Notations	Meaning
T	*Tag of RFID*
R	*Reader of RFID*
S	*backend Server ofRFID system*
ID_T	*identity of tag*
PRNG	*random number generator*
r_R, r_T, r_S	*random number generated by reader R, T, S*
K_{SR}	*K_{SR} is the shared secret between S and R*
K_{ST}	*K_{ST} is the shared secret between S and T*
Query	*Query request generated by R*
H( )	*one-way hash function, H: {0, 1}* →{0, 1}l*
⊕	*XOR operation*

THE INITIALIZATION STAGE

We assume that during system initialization the tag is loaded with an initial identifier ID (secure ID_T), which is set to a random value. In a similar way, the backend server contains the same data stored in the tag. In addition, two tables ($K^{"}_{ST}, K^{"}_{SR}, ID^{"}_{R}, ID^{"}_{T}$) and ($K^{'}_{ST}, K^{'}_{SR}, ID^{'}_{R}, ID^{'}_{T}$) are stored in the database of backend server. When the server has authentication to card reader and tags, system need to query the relevant information in the database. We have to complete the following several jobs:

First, make unique ID_T (ID_R for reader) and K_{ST}, K_{SR} (K_{ST} is a Shared key between server and Tag; K_{SR} is a shared key between server and card reader) to every Tag and Reader, and store the corresponding information to the Database. They can only be aware of the server, reader and legal Tag.

Second, to install the random number generator (*PRNG*) which can generate pseudo random numbers in the Reader, Tag and backend server.

Third, to install the hash function (H) in the backend server, Reader and Tag.

The Detail of Proposed Protocol

In this section, we propose a new protocol to improve the security while preserving the lightweight property. Our proposed protocol is depicted in figure 2 and described as follows:

Step 1: $R \longrightarrow T$: The R generates a random number r_R using $PRNG$ and send r_R to T , when the query began to be broadcast.

Step 2: $S \longleftarrow R \longleftarrow T$: The T generates a random number r_T using $PRNG$ and computes M = $H\left(K_{ST} \square r_{TR} \square ID_T\right)$, then sends M and r_T to Reader R . R Computes $N = H\left(K_{SR} \square r_{TR} \square ID_R\right)$, r_{TR} = $r_R \oplus r_T$ and sends M , N together with r_{TR} to the backend Server S .

Step 3: $S \longrightarrow R \longrightarrow T$: After receiving the message from Reader, In the process of authentication card reader and tag, the server needs to retrieve the corresponding parameters in table 1. If the authentication process is successful, system update the corresponding data (K'ST= K"ST $\oplus$ rTRS) in table-update, the same time computes $Z^{'}$ = $H\left(K_{SR}^{''} \square r_{TRS} \square ID_R^{''}\right)$, $Z = H\left(K_{ST}^{''} \square r_{TRS} \square ID_T^{''}\right)$ and sends $Z^{'}$, Z , r_{TRS} to Reader and Tag. If the above authentication process is not successful, the server needs to retrieve the corresponding parameters in table-update and begin to verify Reader and Tag again. If the certification process is successful, the server computes r_{TRS} = $r_R \oplus r_T \oplus r_S$, $K_{SR}^{''} = K_{SR}^{'}$; $K_{ST}^{''} = K_{ST}^{'}$, $Z^{'} = H\left(K_{SR}^{'} \square r_{TRS} \square ID_R^{'}\right)$, $Z = H\left(K_{ST}^{'} \square r_{TRS} \square ID_T^{'}\right)$, $K_{ST}^{'}$ = $K_{ST}^{'} \oplus r_{TRS}$ and sends $Z^{'}$, Z , r_{TRS} to Reader and Tag.

Step 4: R verifies S : To verify the correctness of Z' received from the backend server S , the R We compares the value of $H\left(K_{SR} \square r_{TRS} \square ID_R\right)$. If their values are equal, S successfully passed the certification of R . After the end of the above calculation, R sends Z, r_S to the Tag.

Step 5: T verifies S: To verify the correctness of Z received from the backend server S , the T We compares the value of $H\left(K_{ST} \square r_{TRS} \square ID_T\right)$. If their values are equal, S successfully passed the certification of T . After the end of the above calculation, T updates the value of K_{ST} .

In terms of current attack on RFID system, the attacker attacks mainly for Tags, its purpose is to get the user's private data. In order to prevent attacks using historical data to the reader, we can add two tables in the database. After the certification we may update the parameters of the reader in the database and the reader. Of course, this kind of attack to card reader is not any benefit for an attacker.

BAN LOGIC

When we look into published security protocols, we find that many of these protocols do not succeed in their stated or implied goals. Many existing protocols are susceptible to various kinds of attacks, which are independent of the veaknesses of the cryptosystem employed. In recent years there has been great interest in the design and analysis of secure protocols. Various new techniguws have been developed and used to find a great variety of different attacks on such protocols.

Burrows, Abadi and Needham [19] developed logic for analyzing authentication protocols. The logic is called BAN-logic. It allows reasoning about beliefs held by the principals involved in the protocols. With the logic all publicand shared key primitives are formalized and also the notion of a “fresh message”. This makes it possible to formalize a challenge response protocol.A proof with the BAN logic is a good proof of correctness, based on the assumptions. The BAN logic has been used to find new weaknesses in various cryptographic protocols. A number of variations and enhancements of the basic BAN logic have been developed. Below we get the overview of the BAN Logic.

BAN LOGICAL NOTATION

In this article, we only use the following a few symbols, more comprehensive term is described in the article[19].

$P \mid\equiv X$: P believes X . P believes as if X is true.

$P \triangleleft X$: P sees X . A principal has sent P a message containing X .

$P \mid\sim X$: P once said X . P at some time believed X and sent it as part of a message.

$P \mid\Rightarrow X$: P controls X . P has authority over X and is trusted on this matter.

$\#(X)$: X is fresh. That is, X has not been sent in a message at any time before the current run of the protocol. A message that is created for the purpose of being fresh is called a nonce.

$P \xleftrightarrow{K} Q$: K is the key shared by P and Q . The key is good and will always be known only to P and Q and to any other principal trusted by either of them.

$\{X\}_K$: Thecipher text of X encrypted by the key K .

$\xrightarrow{K} P$: P has public key K . The corresponding private key is denoted by K^{-1} and assumed to be known only by P .

BAN LOGICAL POSTULATES

BAN logic consists of 19 logical rules. The only fourrules used in the paper are as follows:

Message-meaning rule: The following rule formalizes one of the main semantical principles of BANlogic; namely, if you believe that you and Joe know a public key K , and then you ought to believe that anything you receive enciphered with the key K comes originally from Joe. You may conclude that it was originally created by Joe who once said its contents:

R1: $P \mid\equiv P \xleftrightarrow{K} Q, P \triangleleft \{X\}_K \Rightarrow P \mid\equiv Q \mid\sim X$

Nonce-verification rule: The following rule expresses the check that a statement is recent, and hence that the sender still believes in it. If P believes that X is fresh and that Q once said X, then P believes that Q has said X during the current run of protocol, and hence that Q believes X at present. In order to apply this rule, X should not contain any encrypted text. The nonce verification rule is the only way of “promoting” once said assertion to actual belief:

R2: $P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X \Rightarrow P \mid\equiv Q \mid\equiv X$

Jurisdiction rule: The following rule states that if P believes that Q has jurisdiction over X then P trusts Q on the truth of X:

R3: $P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X \Rightarrow P \mid\equiv X$

Freshness Rule: The following rule is important in reflecting the notion of timeliness exploited as the cardinal principle of authentication

R4: $P \mid\equiv \#(X) \Rightarrow P \mid\equiv \#(X, Y)$

There are a few other inference rules. We shall not list them one by one.

SECURITY ANALYSIS

A protocol analysis with BAN logic consists of the following steps. First, a protocol is transformed into a so-called idealized form; the transformation involves not only protocol syntax changes, but also semantic interpretations. Secondly, logical formulas about the (idealized) protocol are generated and reasoned about by applying the inference rules. The reasoning manipulation starts from a set of formulas called initial assumptions; guided by the idealized protocol speciation, it aims at reaching another set of formulas called conclusions.

AUTHENTICATION FEATURES ANALYSIS WITH BAN LOGIC

In our proposed protocol, in order to reduce the computational burden of the Tags, we do not use the symmetric key encryption to encrypt the passed information, but hash functions instead of the encryption.For example, in the proposed protocol, we use $H\left(K_{ST},M\right)$ to instead of $\left\{M\right\}_{K_{ST}}$ .To analysis protocol with BAN Logic, we need to turn $H\left(K_{ST},M\right)$ to $\left\{M\right\}_{K_{ST}}$, which is more in line with the rules of the BAN for protocol analysis.

Establishment of idealized model
Original protocol :
Message 1 $R \rightarrow T:\ N_R$
Message 2 $T \rightarrow R: N_T,\left\{N_T,N_R,ID_T\right\}_{K_{ST}}$
Message 3 $R \rightarrow S:\ \left\{N_T,N_R,ID_R\right\}_{K_{SR}},\left\{N_T,N_R,ID_T\right\}_{K_{ST}}$
Message 4 $S \rightarrow R:\ N_R,\left\{N_T,N_R,N_R,ID_R\right\}_{K_{SR}}\ \left\{N_T,N_R,N_R,ID_T\right\}_{K_{ST}}$
Message 5 $R \rightarrow T:\ N_R,\left\{N_T,N_R,N_R,ID_T\right\}_{K_{ST}}$
Idealized protocol:
Message 6: $S \lhd \left\{N_T,N_R,ID_R\right\}_{K_{SR}},\left\{N_T,N_R,ID_T\right\}_{K_{ST}}$
Message 7: $R \lhd \left\{N_T,N_R,N_R,ID'_R\right\}_{K_{SR}}$
Message 8: $T \lhd \left\{N_T,N_R,N_R,ID'_T\right\}_{K_{ST}}$
Establishment of security goals
$S\left|\equiv ID_R\right.$ And $R\left|\equiv ID'_R\right.$
$S\left|\equiv ID_T\right.$ And $T\left|\equiv ID'_T\right.$

To establish the initial assumption set of the protocol
P1: $S\left|\equiv S \xleftrightarrow{K_{SR}} R, S\right|\equiv S \xleftrightarrow{K_{ST}} T$
P2: $R\left|\equiv S \xleftrightarrow{K_{SR}} R, T\right|\equiv S \xleftrightarrow{K_{ST}} T$
P3: $R\left|\equiv \#\left(N_S\right), T\right|\equiv \#\left(N_S\right), S\left|\equiv \#\left(N_T\right), S\right|\equiv \#\left(N_R\right)$
P4: $S\left|\equiv R\right|\Rightarrow ID_R, S\left|\equiv T\right|\Rightarrow ID_T$
P5: $R\left|\equiv S\right|\Rightarrow ID'_R, T\left|\equiv S\right|\Rightarrow ID'_T$

Protocol Analysis
Employ the initial assumption and postulate to execute formal analysis for the protocol:

Step1
Message 6, $S \lhd \left\{N_T,N_R,ID_R\right\}_{K_{SR}}$
P1 $S\left|\equiv S \xleftrightarrow{K_{SR}} R\right.$
R1: $P\left|\equiv P \xleftrightarrow{K} Q, P \lhd \left\{X\right\}_K \Rightarrow P\right|\equiv Q\left|\square\ X\right.$, so $S\left|\equiv R\right|\square\ ID_R$
Step2
P3: $S\left|\equiv \#\left(N_R\right)\right.$ and R4: $P\left|\equiv \#\left(X\right) \Rightarrow P\right|\equiv \#\left(X,Y\right)$
So, $S\left|\equiv \#\left(ID_R\right)\right.$
Step3
$S\left|\equiv \#\left(ID_R\right)\right.$ And R2: $P\left|\equiv \#\left(X\right), P\right|\equiv Q\left|\square\ X \Rightarrow P\right|\equiv Q\left|\equiv X\right.$
So, $S\left|\equiv R\right|\equiv ID_R$
Step4

$S\mid\equiv R\mid\equiv ID_R$, P4: $S\mid\equiv R\mid\Rightarrow ID_R$ and R3: $P\mid\equiv Q\mid\Rightarrow X, P\mid\equiv Q\mid\equiv X \Rightarrow P\mid\equiv X$

So, $S\mid\equiv ID_R$

The analysis process of other parts is similar, by the same way we can get $S\mid\equiv ID_T$, $R\mid\equiv ID'_R$ and $T\mid\equiv ID'_T$.

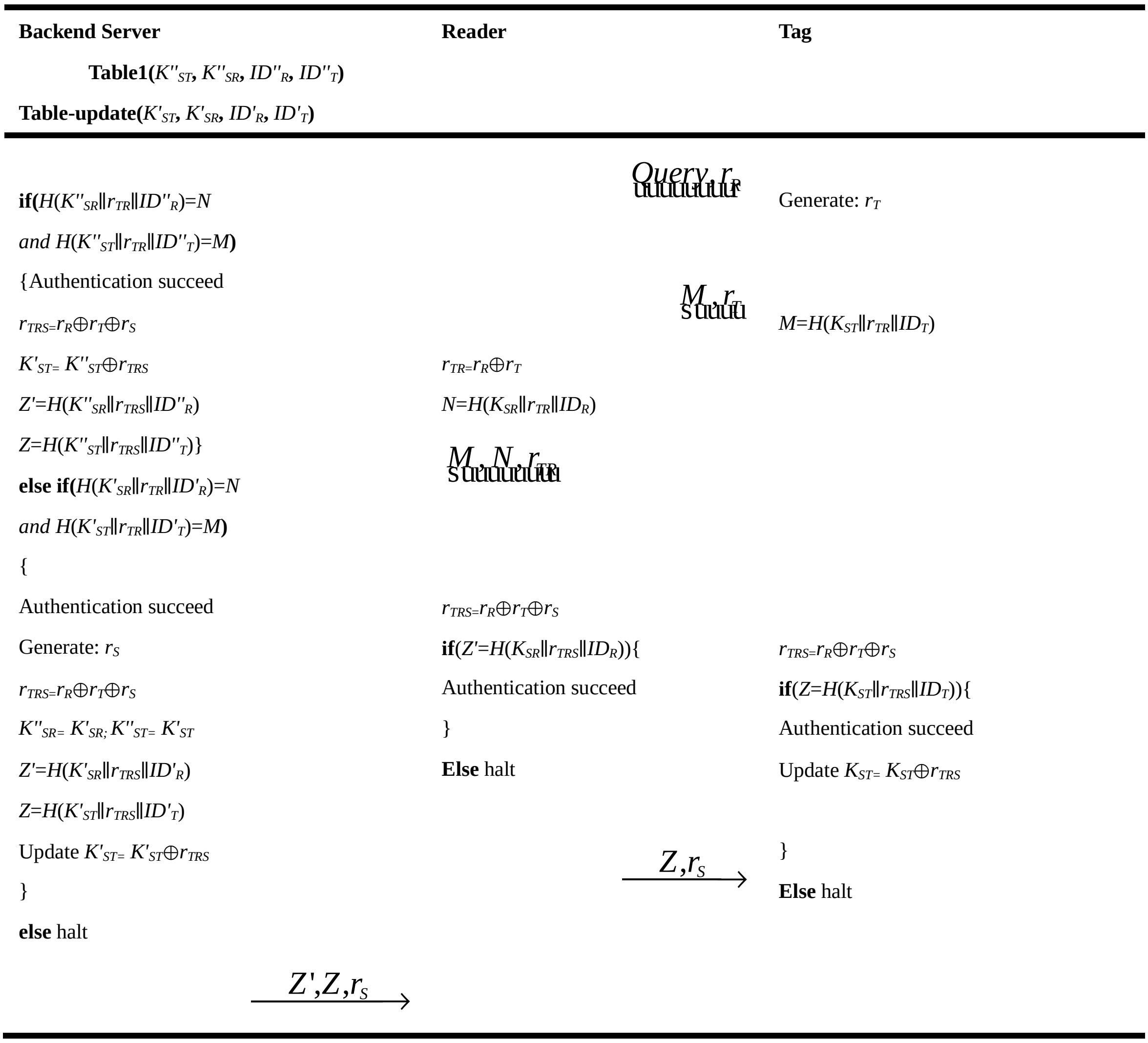
SECURITY FEATURES ANALYSIS

Table 2 shows the proposed schemes are superior to the previous schemes by supporting all major security, privacy and system efficiency criterions in RFID applications environment. We show a comparison of the security with previous mentioned schemes [14, 15, 16, 17] in table 2.

Table2 Type Sizes for Camera-Ready Papers

Protocol	LRPPS[15]	LCAP [14]	A-SRAC [17]	Lee et al. [16]	Our scheme
Mutual Authentication	O	O	O	O	O
Replay attack prevention	×	O	O	O	O
Indistinguishability	×	O	×	O	O
Forward security	O	O	×	×	O
Resynchronization	O	×	O	×	O

Notations of Table: O –secure or support; ×– insecure or not support



Backend Server	**Reader**	**Tag**
Table1(K''_{ST}, K''_{SR}, ID''_R, ID''_T**)**		
Table-update(K'_{ST}, K'_{SR}, ID'_R, ID'_T**)**		
	$\xrightarrow{Query, r_R}$	
if($H(K''_{SR}\Vert r_{TR}\Vert ID''_R)=N$		Generate: r_T
and $H(K''_{ST}\Vert r_{TR}\Vert ID''_T)=M$**)**		
{Authentication succeed		
	$\xleftarrow{M, r_T}$	
$r_{TRS=}r_R\oplus r_T\oplus r_S$		$M=H(K_{ST}\Vert r_{TR}\Vert ID_T)$
$K'_{ST=}$ $K''_{ST}\oplus r_{TRS}$	$r_{TR=}r_R\oplus r_T$	
$Z'=H(K''_{SR}\Vert r_{TRS}\Vert ID''_R)$	$N=H(K_{SR}\Vert r_{TR}\Vert ID_R)$	
$Z=H(K''_{ST}\Vert r_{TRS}\Vert ID''_T)$}		
	$\xleftarrow{M, N, r_{TR}}$	
else if($H(K'_{SR}\Vert r_{TR}\Vert ID'_R)=N$		
and $H(K'_{ST}\Vert r_{TR}\Vert ID'_T)=M$**)**		
{		
Authentication succeed	$r_{TRS=}r_R\oplus r_T\oplus r_S$	
Generate: r_S	**if**($Z'=H(K_{SR}\Vert r_{TRS}\Vert ID_R)$){	$r_{TRS=}r_R\oplus r_T\oplus r_S$
$r_{TRS=}r_R\oplus r_T\oplus r_S$	Authentication succeed	**if**($Z=H(K_{ST}\Vert r_{TRS}\Vert ID_T)$){
$K''_{SR=}$ $K'_{SR;}$ $K''_{ST=}$ K'_{ST}	}	Authentication succeed
$Z'=H(K'_{SR}\Vert r_{TRS}\Vert ID'_R)$	**Else** halt	Update $K_{ST=}$ $K_{ST}\oplus r_{TRS}$
$Z=H(K'_{ST}\Vert r_{TRS}\Vert ID'_T)$		
Update $K'_{ST=}$ $K'_{ST}\oplus r_{TRS}$	$\xrightarrow{Z, r_S}$	}
}		**Else** halt
else halt		
$\xrightarrow{Z', Z, r_S}$		

Fig. 2: Proposed protocol

Attack on the tag. This can happen only when the attacker masquerades as a valid reader. The would-be reader can send a fake random number to Tag, but because the attacker don't know the KST from Tag, and cannot deduce the value of IDT.This type of attack is defeated by the shared secret which is notknown to the attacker. As a result the attacker cannot generate any valuable message, hash function operation is unidirectional and irreversible.

Attack on the reader. In this case the goal of the attacker is to masquerade as a valid tag. Again this type of attack is not possible due to the shared secret. Even if the attacker replays old information, a reader will not accept the tag as authentic since the database will fail to recognize the secure ID_T and ID_R .

Attack on the communication between tag and reader. The goal of this type attack is to find out the valuable information about The Reader and Tag, and to masquerade as a valid tag, which can pass the verification of the database. Listening to messages exchanged in a particular session reveals no information because of the one-wayness of hash function. Furthermore, with every session a new nonce KST is generated guaranteeing the freshness of messages.

CONCLUSION

Previous RFID techniques cause serious privacy infringements such as excessive information exposure and user’s location information tracking due to the wireless characteristics and the limitation of RFID systems. Especially some information security problems may expose user's security privacy. This paper proposes the mutual authentication protocol of low cost using the simple XOR computation and hash function method. In order to guarantee the security of the protocol, we adopt BAN Logic to analysis the security of the protocol. The results proved that the proposed authentication protocol meets the security needs of the RFID system and supports major desirable security features of RFID systems such as mutual authentication, indistinguishability and privacy protection.

Through the analysis of security threats of RFID systems with BAN Logic, we have mastered the methods against these threats and worked on a security model, by which we can design a safe and effective RFID authentication protocol.

Acknowledgments
The authors wish to thank the Foundation of 2013 Yancheng industrial supporting projects (The application security of RFID technology in the emerging industry, the intelligent management system of Campus network) and the research foundation of 2013 National Statistics research project for contract 2013461, under which the present work was possible.

REFERENCES

[1] MIT Auto-ID, retrieved Sep. 10, 2009 from World Wide Web http://autoidlabs.mit.edu, **2004**.
[2] MirzaeeHossein, Pourzaki Abbas, *On-Chip Passive Devices Technology: Component's Characteristics, Fabrication and Commercialization, International Review on Computers and Software*, v 6, n 3, p 434-447, May **2011**.
[3] Jun-JiatTiang, Tien-Sze Lim, Fabian Kung, *International Review on Computers and Software*, v 7, n 1, p 382-386, **2012**.
[4] Zhong, Xiaoqiang, *International Review on Computers and Software*, v 7, n 1, p 450-455, **2012**.
[5] Roberts, C.M.: *Radio Frequency Identification (RFID). Computers & Security* 25, 18–26.**2006**.
[6] A. Juels and R. Pappu, *Squealing euros : Privacy protection in RFID-enabled banknotes. In proceedings of Financial Cryptography -FC'03*, **2003**.
[7] P. Golle, M. Jakobsson, A. Juels, and P. Syversion, *Universal re-encryption for mixnets. In Tatsuaki Okamoto, editor, RSA Conference Cryptographers’ Track, LNCS 2964*, pp.163-178, Springer-Verlag, **2004**.
[8] D. Molnar and D. Wagner, *“Privacy and Security in Library RFID: Issues, Practices, and Architectures,” Proc. 11th ACM Conf. Computer and Comm. Security (CCS ’04)*, Oct. **2004**.
[9] S. Sarma, S. Weis, and D. Engels, *“RFID Systems and Security and Privacy Implications,” Proc. Fourth Int’l Workshop Cryptographic Hardware and Embedded Systems (CHES ’02)*, Aug. **2002**.
[10] Chen, C.-L., and Deng, Y.-Y. *Conformation of EPC Class 1 Generation 2 Standards RFID system with Mutual Authentication and Privacy Protection. Engineering Applications of Artificial Intelligence*, Elsevier, **2008**.
[11] Qingling, C., Yiju, Z., and Yonghua, W. *A minimalist mutual authentication protocol for rfid system and ban logic analysis. Computing, Communication, Control and Management, ISECS International Colloquium*Feb **2008**.
[12] Sun, H.-M., and Ting, W.-C. *A Gen2-based RFID authentication protocol for security and privacy. IEEE Transactions on Mobile Computing 99*, Jan **2009**.
[13] Mike Burmester, Breno de Medeiros, Jorge Munilla, Alberto Peinado, *Secure EPC Gen2 Compliant Radio*

Frequency Identification, In Pedro M. Ruiz(Ed.), Ad-Hoc, Mobile and Wireless Networks, p 227-240, **2009**.

[14] Lee, S.M., Hwang, Y.J., Lee, D.H., Lim, J.I.: *Efficient Authentication for Low-Cost RFID Systems. In: Gervasi, O., Gavrilova, M., Kumar, V., Laganà, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS*, vol. 3483, Springer, Heidelberg ,**2005**.

[15] Kinoshita, S., Hoshino, F., Komuro, T., Fujimura, A., Ohkubo, M.: *Low-cost RFID Privacy Protection Scheme. IPSJ Journal*,Vol.45(8), p 2007–2021, **2004**.

[16] Lee, S., Asano, T., Kim, K.: RFID: *Mutual Authentication Scheme based on Synchronized Secret Information. In: Proceedings of the SCIS*,**2006**.

[17] Lee, Y.K., Verbauwhede, I.: *Secure and Low-cost RFID Authentication Protocols. In: AWiN. 2nd IEEE International Workshop on Adaptive Wireless Networks*, November.**2005**.

[18] M. Ohkubo, K. Suzuki, S. Kinoshita, "*Cryptographic Approach to 'Privacy-Friendly' Tags," Proc. Radio Frequency Identification (RFID) Privacy Workshop*, Nov. **2003**.

[19] Burrows M, Abadi M, Needham R. *ACM Transactions Computer Systems*, Vol.8(1):18-36, **1990**.