A Communication Protocol of RFID Systems in Internet of Things

HuiDan Gao,YaJun Guo*,JianQun Cui, HengGeng Hao and Hui Shi

Department of Computer Science, Central China Normal University
Wuhan 430079, China
ccnugyj@126.com,gaodan8703@126.com

Abstract

Radio frequency identification (RFID) is one of the key technologies which constitute internet of things. Security and privacy issues of RFID systems is the focus of the present study. By analyzing several typical RFID security protocols, for the special security requirements of RFID systems in internet of things, in the paper, we propose a communication protocol SPAP(security-provable authentication protocol), then analyze and demonstrate the security of the protocol in details by the random oracle model. Analysis show that the protocol not only can solve the tag tracking, replay attack, cloning attack and the tag information indistinguishable, but also can solve the internal attack and the ownership transfer of tags and other issues of RFID Systems in internet of things. Finally, according to the comparisons, SPAP has the best performance.

Keywords: *Internet of Things; RFID; EPC; SPAP; Random oracle model.*

1. Introduction

Internet of Things is one of the hottest topics in the IT industry, is the mature stage of the development of Internet. This means it can appear at any time, any place, any object can be linked with this ubiquitous network. Although the concept of internet of things has been widely recognized, scholars from worldwide have been studying and promoting its application all the time, the development of internet of things still faces many difficulties, especially the privacy issues in the RFID systems.

RFID systems in internet of things[1,2] consist of readers, EPC tags, RFID middleware components. The wireless data communication technology between EPC tags and readers can make the systems vulnerable to retransmit, track, tamper, counterfeit. In addition, security issues of the ownership transfer of tags are also very important, designing safe and efficient RFID security systems is necessary for internet of things. The methods to achieve the security of RFID systems conclude physical methods, password mechanisms and combination of them. As physical methods are defective, security mechanisms basing on the password technology are the focus of today's researches. Currently, there are varieties of RFID security protocols that have been proposed, but the protocols have their own shortcomings. To date, there is not a specific security protocol to meet all the security requirements of RFID systems of internet of things. What’s more, using the theory of provable security to prove the security authentication protocol is an important research direction, however, the example of using the provable security theory to analyze security authentication RFID protocol is very poor. For solving the above problems, this paper presents a security authentication that can be successfully used in RFID systems of internet of things, and proves its safety by the random oracle model [3].

This paper is constructed as follows: Section 2 analyses and compares the existing typical RFID security protocols. Section 3 describes the model of RFID systems of internet of things, and defines its security needs. Section 4 proposes a Provable Secure Authentication SPAP, and proves its security. Section 5 analyses the performance of SPAP. Section 6 makes a conclusion.

2. The Existing Typical RFID Security Protocol

Today, RFID technology has been widely used in many areas because of its strong anti-interference, easy operation, etc. At the same time, security and privacy issues of RFID system are increasingly exposed. Scholars from various countries in the world try their best to make a series of solutions, such as the Hash-Lock protocol basing on hash functions and random numbers [4], the randomized Hash-Lock protocol[5];the library RFID protocol basing on shared pseudo and random function keys[6]; the Ownership Transfer Protocol basing on symmetric key algorithms[7]; and EC-RAC protocol basing on public key cryptography algorithms[8].

The Hash-Lock protocol uses hash functions to implement the authentication between readers and tags, using metal ID instead of the real ID to solve the tracking attacks, but the protocol does not use the dynamic ID mechanism, thus an attacker can still replay attacks, and track attacks. The randomized Hash-Lock protocol can resist the tag tracking attacks, but after the certification, the tag ID can still pass through the clear text form, an attacker can still replay attacks. The Library RFID protocol adopts the pre-shared key, pseudo-random function to achieve authentication, to solve the retransmission, tracking, tampering and other security issues, so far, no obvious defects of the protocol are found, but the cost of labels is too high. Ownership Transfer protocol using symmetric encryption algorithms solves the tampering, tracking and ownership transfer of the tag, but it cannot achieve forward security. EC-RAC protocol using elliptic curve public key cryptography algorithms solves the label tracking attacks, protects the security of the system, however, recent experiments reveal that the protocol still cannot resist tracking attacks.

The internet of things asks for even more special security requirements for its RFID system. The connection between tags and readers in internet of things makes the protocol take into account of internal attacks of the systems, as well as the ownership transfer of tags [9]. By analyzing the above protocols, this paper establishes a model of the RFID system in internet of things, defines their security requirements, and proposes a new security protocol.

3. The Model and Security Requirements of RFID System in Internet of Things

3.1 The RFID System Model of Internet of Things

RFID systems in internet of things mainly consist of readers, tags and RFID middle wares. Each object in the system has an unique EPC. We assume that in one RFID system there are N legitimate readers numbered from 1 to N, there are M legitimate readers numbered from 1 to M. $\forall i \in (1, N)$, $\forall j \in (1, M)$,the reader i is denoted as R_i ,the tag j is denoted as T_j.In addition, because the cable channels between the reader and database are generally considered safe, therefore, when we establish the model, the reader and database can be seen as a unified independent entity, that is, the reader and database are collectively referred to as the middleware server.

Random Oracle model [10] is applied to describe the RFID system model in internet of things. The model can be equivalent to a tuple $P=(\Pi,\Phi)$, Π and Φ are time functions of polynomial whose safety factor is $1^k(k \in N)$, Π defines the behavior of a legitimate reader, Φ defines the operation of a legitimate tag. Using the random Oracle to query and definite the behavior of an attacker, that is, the attacker which has Oracle $\Pi^s_{\mathrm{R}_i,\mathrm{T}_j}$ (R_i initiates a session s with T_j) and Oracle $\Phi^s_{T_j,\mathrm{R}_i}$ (T_j initiates a session s with R_i)is an Oracle probability machine. The attacker can achieve the attack target by sending scheduled questions to Oracle $\Pi^s_{\mathrm{R}_i,\mathrm{T}_j}$ and Oracle $\Phi^s_{T_j,\mathrm{R}_i}$ and receiving response information from the random Oracle. Oracle question depicts the real ability of the attacker. The attacker can send the following questions.

Execute $(\Pi_{\mathrm{R}_i},\Phi_{\mathrm{T}_j},P)$: the question depicts an instance P that the attacker execute the protocol between T_j and R_i which can obtain all messages exchanged between the reader and the tag when the protocol P executes.

SendTag $(\Phi_{\mathrm{T}_j},P,m_1)$: the question depicts an instance P that the attacker A sends the message m_1 to tag T_j , and receives the response message of the tag T_j .

SendReader $(\Pi_{\mathrm{R}_i},P,m_2)$:the question depicts instance P that the attacker A sends the message m_2 to reader R_i , and receives the response message of the reader R_i .

CorruptTag (Φ_{T_j}) :the question depicts an active attack on the tag and the attacker's captured capacity. It can make the captured tag T_j actively reveal secret information which is in their private storage space.

CorruptRead (Π_{R_i}) :the question depicts an active attack on the reader and the attacker's captured capacity. It can make the captured reader R_i actively reveal secret information which is in their private storage space.

Test (Φ_{T_j}) :the question is used to test semantic security of confidential information of a tag T_j . By throwing coin b , if $b = 1$, return the secret information stored in the tag. if $b = 0$, return an random number which is equivalent in length to the secret information of the tag.

Test (Π_{R_i}) :the question is used to test semantic security of confidential information of a reader R_i .By throwing coin b , if $b = 1$, return the secret information stored in the tag. if $b = 0$, return an random number which is equivalent in length to the secret information of the reader.

3.2 Security Requirements of Authentication in RFID System of Internet of Things

An RFID system is an important part of internet of things, non-contact automatic identification technology between the reader and the tag in the system which makes the system face serious security problems. Analyzing the security needs met by existing typical RFID protocols and combining the characteristics of RFID system of internet of things, what needs the authentication should meet in RFID system of internet of things are detailed in the following.

Definition1. If for any polynomial $P(K)$ and sufficiently large K ,the function μ can satisfy $\mu(K) < 1/P(K)$, then we say that the function μ can be negligible.

Mutual authentication: The tag should be able to achieve the certification of legitimate reader, that is, if the attacker R achieves tag $\mathrm{T}_j\,(j \in [1,M])$ to certificate for R_i by fabricating reader $\mathrm{R}_a\,(a \notin [1,N])$,we denote it as $\mathrm{Adv}(R)$. Then the probability of success of R is $\Pr(\mathrm{Adv}(R)) < \mu(K)$. The reader should be able to achieve the certification of legitimate tag, that is, if the attacker T achieves reader $\mathrm{R}_i\,(i \in [1,N])$ to certificate for T_j by fabricating legitimate tag $\mathrm{T}_b\,(b \notin [1,M])$, we denote it as $\mathrm{Adv}(T)$. Then the success probability of T is $\Pr(\mathrm{Adv}(T) < \mu(K)$.

Forward security: Even if an attacker obtains the tag status of its current time t_1, the attacker cannot connect the status with the tag status obtained in previous one time $t_1(t_1 < t_2)$.That is, to $\forall j \in [1,M]$, $t_1 < t_2$, the attacker Q has already known the information of tag T_j in time t_2, then calculate the information of the tag T_j in time t_1 by the random oracle query, we denote it as $\mathrm{Adv}(Q)$. Then the success probability of R is $\Pr(\mathrm{Adv}(Q)) < \mu(K)$.

Indistinguishable: $\forall j_1, j_2 \in [1,M]$, the attacker can't distinguish and identify the secret information of T_{j_1} and T_{j_2} , so as to recognize the target. That is, if the attacker D can distinguish and identify the secret information of T_{j_1} and T_{j_2} through random oracle queries, we denote it as $\mathrm{Iden}(D)$ .The success probability of D is $\Pr(\mathrm{Iden}(D)) < \mu(K)$.

Internal security: The legitimate reader and the legitimate tag within the system cannot communicate with each other by forgery and tampering. That is, $\forall i, j \in [1,N]$, $\forall m, n \in [1,M]$. $\mathrm{R}_i(\mathrm{R}_j)$ successfully identify tag $\mathrm{T}_m(\mathrm{T}_n)$ by fabricating $\mathrm{R}_j(\mathrm{R}_i)$, we denote it as $\mathrm{Adv}(NR)$, Then $\Pr(\mathrm{Adv}(NR) < \mu(K)$. If $\mathrm{T}_m(\mathrm{T}_n)$ through fabricating $\mathrm{T}_n(\mathrm{T}_m)$ is identified successfully by $\mathrm{R}_i(\mathrm{R}_j)$, we denote it as $\mathrm{Adv}(NT)$, then $\Pr(\mathrm{Adv}(NT)) < \mu(K)$.

Security transfer of ownership: $\forall j \in [1,M]$, when the tag T_j transfer its ownership, then the tag T_j become $\mathrm{T}_{j'}$ in the new system. The reader in original ownership system of tag T_j cannot inquiry the information of tag $\mathrm{T}_{j'}$. That is, $\forall i \in [1,N]$, $\forall j \in [1,M]$. The event that R_i successfully get the tag $\mathrm{T}_{j'}$ after transferring the ownership of T_j can be denoted as $\mathrm{Adv}(Z)$, $\Pr(\mathrm{Adv}(Z)) < \mu(K)$.

4. SPAP

4.1 Protocol Design

By analyzing the model and safe problems which need to be solved in RFID systems of internet of things, concluding advantages and disadvantages of today's typical RFID security protocols, the article proposes the protocol SPAP which uses symmetric encryption, one-way hash function and XOR. We assume every legitimate readers and tags that contain a unique EPC (Electronic Product Code),Symbols used in the protocol as Table 1

Table 1. Symbols used in the Protocol

EPC_{R_i}	The EPC of reader i
EPC_{T_j}	The EPC of tag j
$\mathrm{Info}(EPC_{\mathrm{T}_j})$	Information contained in EPC_{T_j} of tag j
K_{ij}	Key between reader i and tag j
$K_{ij}^{'}$	Key update once
$K_{ij}^{''}$	Key update twice
$E_{K_{ij}}(x)$	Encryption function with key K_{ij}
$D_{K_{ij}}(x)$	Corresponding decryption function with $E_{K_{ij}}(x)$
$E_{K_{ij}^{'}}(x)$	Symmetric encryption function with key $K_{ij}^{'}$
$E_{K_{ij}^{''}}(x)$	Symmetric encryption function with key $K_{ij}^{''}$
$H(x)$	One-way hash function
$\oplus$	XOR
$\mathrm{Rand}(x)$	Random number generator
r	Random numbers
e	Certification function used in the key update phase
$e^{'}$	Certification function used in the key update phase
$?=$	Is equal to
$\rightarrow$	Update to

Generally, we assume that the reader i communicates with the tag j in the RFID system, The flow chart of the protocol shown in Fig1. It mainly consists of certification stage, key update phase and transfer stage of ownership.

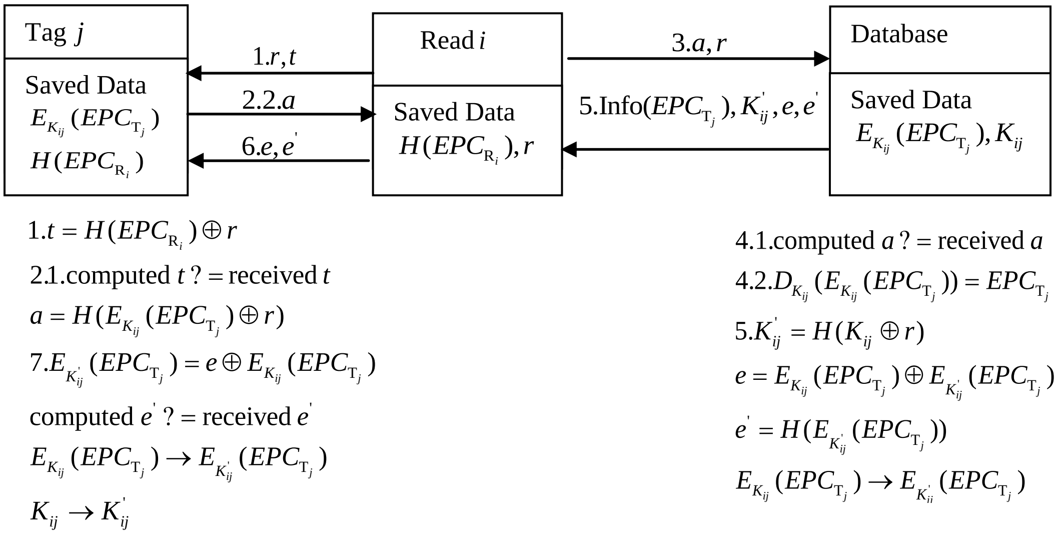
Tag j
Saved Data
$E_{K_{ij}}(EPC_{\mathrm{T}_j})$
$H(EPC_{\mathrm{R}_i})$
$1.r,t$
$2.2.a$
$6.e,e^{'}$
Read i
Saved Data
$H(EPC_{\mathrm{R}_i}),r$
$3.a,r$
$5.\mathrm{Info}(EPC_{\mathrm{T}_j}),K_{ij}^{'},e,e^{'}$
Database
Saved Data
$E_{K_{ij}}(EPC_{\mathrm{T}_j}),K_{ij}$
$1.t=H(EPC_{\mathrm{R}_i})\oplus r$
2.1.computed t ? = received t
$a=H(E_{K_{ij}}(EPC_{\mathrm{T}_j})\oplus r)$
$7.E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})=e\oplus E_{K_{ij}}(EPC_{\mathrm{T}_j})$
computed $e^{'}$? = received $e^{'}$
$E_{K_{ij}}(EPC_{\mathrm{T}_j})\rightarrow E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$
$K_{ij}\rightarrow K_{ij}^{'}$
4.1.computed a ? = received a
$4.2.D_{K_{ij}}(E_{K_{ij}}(EPC_{\mathrm{T}_j}))=EPC_{\mathrm{T}_j}$
$5.K_{ij}^{'}=H(K_{ij}\oplus r)$
$e=E_{K_{ij}}(EPC_{\mathrm{T}_j})\oplus E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$
$e^{'}=H(E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j}))$
$E_{K_{ij}}(EPC_{\mathrm{T}_j})\rightarrow E_{K_{ii}^{'}}(EPC_{\mathrm{T}_j})$

Figure 1. SPAP Flow Chart

Certification Stage

(1)Initialization: save $H(EPC_{R_i})$ in the reader i , save $H(EPC_{R_1})$, $H(EPC_{R_2})$ ...... $H(EPC_{R_N})$ and $E_{K_{1j}}(EPC_{T_j}), E_{K_{2j}}(EPC_{T_j})......E_{K_{Nj}}(EPC_{T_j})$ in tag j as shown in Fig 2. And make sure $H(EPC_{R_1})$ and $E_{K_{1j}}(EPC_{T_j})$, $H(EPC_{R_2})$ and $E_{K_{2j}}(EPC_{T_j})$ ...... $H(EPC_{R_N})$ and $E_{K_{Nj}}(EPC_{T_j})$ put into a one-to-one relationship. The key $K_{1j}, K_{2j}......K_{Nj}$ with corresponding $E_{K_{1j}}(EPC_{T_j})$, $E_{K_{2j}}(EPC_{T_j})$ ...... $E_{K_{Nj}}(EPC_{T_j})$ between all the readers and tag j saved in the RFID middleware database just as shown in Fig 3, and make sure K_{1j} and $E_{K_{1j}}(EPC_{T_j})$, K_{2j} and $E_{K_{2j}}(EPC_{T_j})$ ...... K_{Nj} and $E_{K_{Nj}}(EPC_{T_j})$ put into a one-to-one relationship.

$H(EPC_{R_1})$	$E_{K_{1j}}(EPC_{T_j})$
$H(EPC_{R_2})$	$E_{K_{2j}}(EPC_{T_j})$
⋮	⋮
$H(EPC_{R_N})$	$E_{K_{Nj}}(EPC_{T_j})$

Figure 2. Tag j initialized

$E_{K_{1j}}(EPC_{T_j})$	K_{1j}
$E_{K_{2j}}(EPC_{T_j})$	K_{2j}
⋮	⋮
$E_{K_{Nj}}(EPC_{T_j})$	K_{Nj}

Figure 3. Database Initialized

(2)Reader i generates a random number r by random number generator Rand(x), then generate an authentication request through the XOR $H(EPC_{R_i}) \oplus r = t$, sent r, t to the tag.

(3)When receive certification request, tag j will search the $H(EPC_{R_i})$ to satisfy $H(EPC_{R_i} \oplus r)$ equal to the received t . If not found, authentication fails and the tag stops responding. Otherwise, continue to perform the following steps to find $E_{K_{ij}}(EPC_{T_j})$, which is one-to-one with reader EPC_{R_i} . Then hashes $a = H(E_{K_{ij}}(EPC_{T_j}) \oplus r)$ and send a to the reader.

(4)When the reader receives tag response, sent a and random number r generated first to the RFID middleware.

(5) After receiving a , RFID middleware will search the $E_{K_{ij}}(EPC_{T_j})$ to satisfy $H(E_{K_{ij}}(EPC_{T_j}) \oplus r) = a$. If it is found, certification is completed. Then continue to perform the following steps, search K_{ij} ,which is one-to-one with $E_{K_{ij}}(EPC_{T_j})$ .Otherwise, responding stops to conduct $D_{K_{ij}}(E_{K_{ij}}(EPC_{T_j})) = EPC_{T_j}$ symmetric decryption to obtain EPC_{T_j} .After that, search the Info(EPC_{T_j}) with EPC_{T_j} through the information service system of Internet of Things, and sent it to reader. If the tag needs to update the keys and transfer the ownership, continue do the following steps.

Key Update Phase

(1) RFID middleware databases generate a new key $K_{ij}^{'} = H(K_{ij} \oplus r)$, by using Hash function, then encrypt EPC_{T_j} with the key to generate new $E_{K_{ij}^{'}}(EPC_{T_j})$, then XOR $E_{K_{ij}}(EPC_{T_j})$ and $E_{K_{ij}^{'}}(EPC_{T_j})$, that is $e = E_{K_{ij}}(EPC_{T_j}) \oplus E_{K_{ij}^{'}}(EPC_{T_j})$,then Hash function of

$E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$, that is $e^{'} = H(E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j}))$, make substitution of $K_{ij}^{'}$ and $E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$ to K_{ij} and $E_{K_{ij}}(EPC_{\mathrm{T}_j})$.

(2) Send e and $e^{'}$ to reader, the reader will send them to the tag. When receive e and $e^{'}$, the tag recovers $E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$ through $e \oplus E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$ .Certify if $H(E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j}))$ is equal to $e^{'}$ If it is, the verification is completed, make substitution of $E_{K_{ij}}(EPC_{\mathrm{T}_j})$ to $E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$. Otherwise, Key Update Failed.

Transfer Stage of Ownership

(1)In order to achieve the ownership transfer of tag T_j , the original owner of tag send the tag information to RFID middleware of new system. In the new ownership of the system, RFID middleware, the reader and the tag re-run the key update phase, $K_{ij}^{''} = H(K_{ij}^{'} \oplus r)$, then encrypt EPC_{T_j} to generate $E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j})$,then XOR $E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j})$ and $E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$,that is $e^{'} = E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j}) \oplus E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j})$, then Hash function of $E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j})$, that is $e^{''} = H(E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j}))$. make substitution of $K_{ij}^{''}$ and $E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j})$ to $K_{ij}^{'}$ and $E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$.

(2) Send $e^{''}$ and $e^{'}$ to reader, the reader will send them to tag. When receive $e^{''}$ and $e^{'}$,the tag recover $E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j})$ through $e^{'} \oplus E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$ .Certify if $H(E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j})))$ is equal to $e^{''}$. If it is, the verification is completed, make substitution of $E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$ to $E_{K_{ij}^{''}}(EPC_{\mathrm{T}_j})$ In the new ownership system of tag T_j, reader and RFID middleware systems have tag information of updated keys, the original ownership of the system no longer has any access to visit.

4.2 Security of the SPAP

Theorem1. SPAP can realize mutual authentication

(1)Identity authentication of the reader

Proposition 1.If any attacker R of PPT types successfully calculates the probability of $t = H(EPC_{\mathrm{R}_i}) \oplus r$ to meet $\Pr[t = H(EPC_{\mathrm{R}_i}) \oplus r] < \mu(K)$, it achieve identity authentication of the reader.

Proof. The event that the attacker R can calculate $t = H(EPC_{\mathrm{R}_i}) \oplus r$ without knowing EPC_{R_i} and r is recorded as $\mathrm{Adv}(R)$, it has the following three possibilities:

1. the t maybe known by the attacker itself by inquiring Oracles SendReader, Execute, CorruptRead and Test (Π_{R_i}) . We suppose it had inquired q_{send} times by Oracle SendReader $(\Pi_{\mathrm{R}_i}, P, m_2)$, q_{exe} times by Oracle Execute $(\Pi_{\mathrm{R}_i}, \Phi_{\mathrm{T}_j}, P)$. And output length of $H(.)$ is l_1.According to the characteristics of birth attacking[11],the possibility the attacker have right conjectures is no more than $\frac{q_{send} + q_{exe}}{2^{l_1}}$.

2. Or r has already been inquired by Oracle Execute, CorruptRead, SendReader and Test(Π_{R_i}). We suppose it inquired $q^{'}$ times before and now inquires q times, then the possibility the attacker have right conjectures is no more than $\frac{q^{'}}{q}$.

3. Or the attacker successfully calculates EPC_{R_i} that the length of EPC_{R_i} is l_2, the probability for attacking successfully is $\frac{1}{2^{l_2}}$.

In all, $\Pr[t = H(EPC_{\mathrm{R}_i}) \oplus r] = \Pr[\mathrm{Adv(R)}] < \Pr[\frac{q_{send} + q_{exe}}{2^{l_1}} + \frac{q^{'}}{q} + \frac{1}{2^{l_2}}]$,

$\mu(K) = \Pr[\frac{q_{send} + q_{exe}}{2^{l_1}} + \frac{q^{'}}{q} + \frac{1}{2^{l_2}}]$, So the proposition is proved.

(2)Identity authentication of the tag

Proposition2. If the symmetric encryption is secure, any attacker T of PPT types successfully calculates the probability of $a = H(E_{K_{ij}}(EPC_{\mathrm{T}_j}) \oplus r)$ to meet $\Pr[a = H(E_{K_{ij}}(EPC_{\mathrm{T}_j}) \oplus r)] < \mu(K)$, it achieve identity authentication of the reader.

Proof.The event that the attacker can calculate $a = H(E_{K_{ij}}(EPC_{\mathrm{T}_j}) \oplus r)$ without knowing $E_{K_{ij}}(EPC_{\mathrm{T}_j})$ and r is recorded as $\mathrm{Adv}(T)$, it has the following three possible:

1. the a maybe known by the attacker T itself by inquiring Oracles SendReader, Execute, CorruptRead and Test(Φ_{T_j}) ,We suppose it had inquired q_{send} times by Oracle SendTag$(\Phi_{\mathrm{T}_j}, P, m_1)$, q_{exe} times by Oracle Execute$(\Pi_{\mathrm{R}_i}, \Phi_{\mathrm{T}_j}, P)$.And output length of $H(.)$ is l_1. According to the characteristics of birth attacking[11] ,the possibility the attacker has the right conjectures is no more than $\frac{q_{send} + q_{exe}}{2^{l_1}}$.

2. Or r has already been inquired by Oracle Execute, CorruptRead, SendReader and Test(Φ_{T_j}). We suppose it inquired $q^{'}$ times before and now inquires q times, then the possibility the attacker have right conjectures is no more than $\frac{q^{'}}{q}$.

3. Or the attacker can $E_{K_{ij}}(EPC_{\mathrm{T}_j})$, because the symmetric encryption is secure, so the probability of successfully calculating $E_{K_{ij}}(EPC_{\mathrm{T}_j})$ is neglected.

So $\Pr[a = H(E_{K_{ij}}(EPC_{\mathrm{T}_j}) \oplus r)] = \Pr[\mathrm{Adv(T)}] < \Pr[\frac{q_{send} + q_{exe}}{2^{l_1}} + \frac{q^{'}}{q}]$,

$\mu(K) = \Pr[\frac{q_{send} + q_{exe}}{2^{l_1}} + \frac{q^{'}}{q}]$, proposition is proof.

Theorem 2.If the symmetrical encryption is secure, SPAP can achieve forward security.

Proof. If the attacker Q know the information $e = E_{K_{ij}}(EPC_{\mathrm{T}_j}) \oplus E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j})$, $e^{'} = H(E_{K_{ij}^{'}}(EPC_{\mathrm{T}_j}))$ of the tag at time t_2, and successful get $E_{K_{ij}}(EPC_{\mathrm{T}_j})$ and K_{ij} at time t_1, we note the event as $\mathrm{Adv}(Q)$. The attacker execute the inquiry of Execute, SendReader, SendTag, CorruptRead, CorruptTag, Test $(\varPhi_{\mathrm{T}_j})$ and Test $(\varPi_{\mathrm{R}_i})$ in sequence.

We suppose the attacker Q inquires q_{exe} times by Oracle Execute $(\varPi_{\mathrm{R}_i}, \varPhi_{\mathrm{T}_j}, P)$, q_{send} times by Oracle SendTag $(\varPhi_{\mathrm{T}_j}, P, m_1)$ and SendReader $(\varPi_{\mathrm{R}_i}, P, m_2)$, and the output length of $H(.)$ is l_1. According to the characteristics of birthday attack, the possibility that the attacker successfully get the key of tag at time t_1 is $\Pr[\mathrm{Adv}(Q)] < \frac{2q_{send} + q_{exe}}{2^{l_1}}$, and $\frac{2q_{send} + q_{exe}}{2^{l_1}}$ can be ignored. Similarly, probability of successfully get $E_{K_{ij}}(EPC_{\mathrm{T}_j})$ can also be ignored. And the theorem is tenable.

Theorem 3.SPAP can realize the Tag information indistinguishable.

Proof, $\forall j_1, j_2 \in [1, M]$, If the attacker D want to distinguish and identify the secret information of T_{j_1} and T_{j_2}, the attacker inquiries the Oracles Execute, SendReader, SendTag, CorruptRead, CorruptTag, Test $(\varPhi_{\mathrm{T}_j})$,because SPAP can realize mutual authentication, forward security, internal security, security of ownership transfer, so if the event the attacker D can successfully identify and distinguish the secret information of T_{j_1} and T_{j_2} is recorded $\mathrm{I}den(D)$, $\Pr[\mathrm{I}den(D)] < \mu(K)$.That is to say, the attacker does not have the legitimacy, can't identify the tag information, also can't distinguish between the target. So the theorem is proved.

Theorem 4.SPAP can implement internal security.

Proof. $\forall i, j \in [1, N], \forall m, n \in [1, M]$, suppose that reader $\mathrm{R}_i(\mathrm{R}_j)$ successfully identify tag $\mathrm{T}_m(\mathrm{T}_n)$ by fabricating $\mathrm{R}_j(\mathrm{R}_i)$, we denote it as $\mathrm{Adv}(NR)$. Because it has the only key K_{ij} between every legal reader and tag in the system, and theorem 1 has proved tag can achieve authentication of reader, so $\Pr(\mathrm{Adv}(NR) < \mu(K)$. Similarly, if $\mathrm{T}_m(\mathrm{T}_n)$ successfully identified by $\mathrm{R}_i(\mathrm{R}_j)$ through fabricating $\mathrm{T}_n(\mathrm{T}_m)$, we denote it as $\mathrm{Adv}(NT)$, then $\Pr(\mathrm{Adv}(NT) < \mu(K)$. And the theorem is tenable.

Theorem 5.SPAP can realize the security of ownership transfer

Proof. Because there is the only authentication key between any tag and reader for SPAP, after the ownership transfer, the only authentication key between any tag and reader is updated, at the same time, SPAP also can realize the two-way authentication, therefore, That is, $\forall i \in [1, N]$, $\forall j \in [1, M]$, After ownership transfer of the tag T_j, T_j may become $\mathrm{T}_{j'}$,the event that the read R_i successfully gets information of the tag $\mathrm{T}_{j'}$ can be denoted as $\mathrm{Adv}(Z)$, $\Pr[\mathrm{Adv}(Z)] < \mu(K)$. So the theorem is proved.

5. Performance Analysis

Safety performance[12] for a authentication is of great importance, the security of SPAP and the previous typical authentication protocols are analyzed in table 2, √ and

× indicate whether the protocol has the ability to resist the attacks or not, respectively. From table 2, We can see clearly that SPAP can resist all kinds of security attacks, and will be able to realize the key update and the ownership transfer of tags.

Table 2. Comparison of Safety Performance

RFID Protocol	Hash-Lock	Random	Library RFID	Ownership	EC-RAC	SPAP
		Hash-Lock		Transfer		
Mutual authentication	√	√	√	√	√	√
Forward security	√	√	√	√	√	√
Internal security	×	×	×	×	×	√
Resist tracking attack	×	×	√	×	×	√
Resist replaying attack	×	×	√	√	√	√
Indistinguishable	√	√	√	√	√	√
Key update	×	×	×	√	√	√
Ownership transfer	×	×	×	√	×	√

6. Conclusion and Future Work

RFID systems are critical for internet of things, therefore, the safe problems of RFID systems becomes one of the main tasks for developing the internet of things. This paper analyzes advantages and disadvantages of several typical RFID protocols, summarizes the special security needs of RFID systems in internet of things, proposes a secure-provably authentication SPAP.

Proved by the random oracle model, SPAP can achieve mutual authentications, internal security, ownership transfer of tags, what's more, SPAP can also resist retransmission, tracking of some basic attacks. Finally, according to the result of analyzing the safe performance, SPAP protocol has good performance.

The innovation of SPAP lies in solving the internal attacks and security issues of ownership transfer for setting dynamic authentication keys between any legitimate tags and legitimate readers. In addition, using the random oracle models is also very novel.

References

[1] V. Kolias, I. Giannoukos, C. Anagnostopoulos, I. Anagnostopoulos, V. Loumos and E. Kayafas, "Integrating RFID on event-based hemispheric imaging for internet of things assistive applications", Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments, **(2010)** June 23-25; Samos, Greece.

[2] X. Zhao and X. Wand, "Design and Implementation of Hybrid Broadcast Authentication Protocols in Wireless Sensor Networks", International Journal of Advanced Science and Technology. Vol. 2, **(2009)** January.

[3] G. Martin, "A study of the random oracle model", California, USA: University of California at Davis, **(2008)**.

[4] S. E. Sarma, S. A. Weis and D. W. Engels, "RFID systems and security and privacy implications", Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, **(2002)** August 13–15; CA, USA.

[5] S. A. Weis, S. E. Sarma, R. L. Rivest and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", Proceedings of the 1st International Conference on Security in Pervasive Computing, **(2003)** March 12-14, Boppard, Germany.

[6] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures", Proceedings of the 11th ACM Conference on Computer and Communications Security, **(2004)** October 25 – 29;Washington, DC,USA.

[7] K. Osaka, T. Takagi, K. Yamazaki and O. Takahashi, "An efficient and secure RFID security method with ownership transfer", Proceedings of International Conference on Computational Intelligence and Security, **(2006)** November 3-6; Guangzhou, China.

[8] Y. K. Lee, L. Batina and I. Verbauwhede, "EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol", Proceedings of IEEE International Conference on RFID, **(2008)** April 16-17; Las Vegas, Nevada, USA.

[9] R. J. Robles, T. Kim, "A Review on Security in Smart Home Development", International Journal of Advanced Science and Technology, Vol. 15, **(2010)** February.

[10] B. Alomair, A. Clark, J. Cuellar and R. Poovendran, "Scalable RFID systems: a privacy-preserving protocol with constant-time identification", Proceedings of the International Conference on Dependable Systems and Networks, **(2010)** June 28-July 1, Chicago, USA.

[11] M. Bellare and T. Kohno, "Hash function balance and its impact on birthday attacks" Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, **(2004)** May 2-6;Interlaken, Switzerland.

[12] K. Sharma, M. K. Ghose, D. Kumar, R. P. K. Singh and V. K. Pandey, "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", International Journal of Advanced Science and Technology, Vol. 17, **(2010)** April.

Authors

HuiDan Gao born in 1987, master candidate. Her research interests include information security, internet of things, RFID.

YaJun Guo born in 1965, professor, master's supervisor at Central China Normal University. He received the PhD degree in Information Security from Huazhong University of Science and Technology in 2006. His research interests include information security, pervasive computing, internet of things.

JianQun Cui born in 1974, associate professor and master's supervisor at Central China Normal University. She received the PhD degree in Computer Software and Theory from Wuhan University in 2008. Her research interests include Network management, high-performance computing.

HengGeng Hao born in 1985, master candidate. His research interests include information security, internet of things.

Hui Shi born in 1986, master candidate. His research interests include information security, internet of things.