# An One-way Hash Function Based Lightweight Mutual Authentication RFID Protocol

Xuping Ren
Institute of Software and Intelligent Technology, HangZhou Dianzi University, Hangzhou, China
renxp@hdu.edu.cn

Xianghua Xu and Yunfa Li
Institute of Software and Intelligent Technology, HangZhou Dianzi University, Hangzhou, China
{xhxu, yunfali}@hdu.edu.cn

***Abstract*—With the widespread development of RFID technology, security and privacy issues become more prominent in RFID applications. In this paper, a new one-way hash function based mutual authentication protocol is proposed to address such security and privacy problems. Particularly, access list and pseudorandom flags are adopted for quick search, to ensure good efficiency and scalability. The proposed protocol is analyzed according to three aspects: logic, security and performance. Concretely, GNY logic formal method is used to verify the design correctness of the protocol, the attack model is used to analyze the security, and the performance is evaluated from communication overload, storage, and computation requirement. The analysis results show that the protocol has no obvious design flaws, can resist major attacks, and improves the system reliability and effectiveness. The proposed protocol can be easily scalable for lightweight RFID systems.**

***Index Terms*—authentication protocol, logical analysis, security, privacy, RFID**

## I. INTRODUCTION

Radio Frequency Identification (RFID) systems, thanks to their low cost and their convenience in identifying an object without physical contact, have found many applications in manufacturing, supply chain management, parking garage management, and inventory control[1]. Moreover, RFID technology is envisioned as an economical replacement for traditional barcode counterpart and expected to be massively deployed in consumer object identification. The advantages of RFID system over barcode system include many-to-many communication, wireless data transmission and its computing nature [2].

Despite many prospective applications, RFID technology also poses several security and privacy threats [3] [4] which could harm its global adoption. Many schemes have been proposed to address those security/privacy issues. Authentication of RFID tags is an active research area and protocols have been extensively studied and reported in the literature [5][6]. It is more common that mutual authentication of the tag, reader and back-end server [7][8][9]. Mutual authentication is required to ensure that tag information can only be legitimate reader and server systems to get and reader and server systems only accept legal tag information. Moreover, communication data need to be protected.

Some authentication protocols [10][11][12] provide security based on bitwise operation or other simple functions. Some authentication protocols [13][14][15] [16]mainly execute irreversible hash function and pseudorandom number generator (PRNG). Other authentication protocols [17][18] mainly use typical cryptography to achieve high security and require more system resources. Most authentication protocols have been designed without strict formal proof. However, lack of formal analysis may make those protocols ignoring design flaws and security vulnerabilities. In many cases, people want to achieve good security and privacy guarantee, but do not want to consume too much system resources.

In this paper, we proposed a mutual authentication protocol based on one-way hash function for RFID system, which hope to meet aforementioned requirement. The main contributions of our work are as follows. One-way hash function is used to protect communication data during authentication. Access lists and pseudorandom flags are used to achieve quick search. GNY logic formal method is used to verify the design correctness of the protocol. The attack model is used to do the security analysis.

In next section, related RFID protocols are reviewed and analyzed. The proposed protocol is described in section 3. Formal analysis of the protocol with GNY logic is given in section 4. In section 5, the attack model is used to analyze the security on the major attacks. Performance analysis is done in section 6. Finally, section 7 draws a conclusion

## II. RELATED WORKS

According to the security efficiency and operation complexity, the protocols (including access control, authentication and encryption) can be classified into three categories: ultra-lightweight, lightweight, middleweight. The proposed protocol is a lightweight protocol. So the


doi:10.4304/jcp.8.9.2405-2412

authors focus on some related lightweight authentication protocols.

Song and Mitchell (SM) [13] propose a RFID Authentication Protocol for Low-cost Tags which uses a random number as a temporary secret and a keyed hash function to protect the messages communicated between tag and reader. It is claimed that the scheme can provides the identified privacy and security features. But this scheme resists forward traceability and server impersonation under an assumption. And the scheme has not been proved by formal method and there may be design flaw.

Ning et al. [9] suggest a distributed key array authentication protocol (KAAP) that provides classified security protection. It is synthetically analyzed in three aspects: logic, security and performance. It is claimed that the scheme can resist both external attacks and internal forgery attacks with insignificantly increased complexity. The scheme need hold key array, once the key array is leaked, the entire system security can not be guaranteed. Moreover, the key array method limits the system scalability.

Rhee et al. [14] propose a Challenge-Response Based RFID Authentication Protocol (HIDVP). The protocol is based on Challenge-Response using one-way hash function and random number. It is claimed that the scheme can resist spoofing, replay attack and so on. But it has been found to be unsuitable for distributed database environment [8].

Liu and Ning [8] present a zero-knowledge authentication protocol based on alternative mode in RFID systems (ZKAP). In ZKAP, dual zero-knowledge proofs are randomly chosen to provide anonymity and mutual authentication without revealing any sensitive identifiers. The scheme uses Pseudo-random flags and access lists for quick search and check. And it employs formal proof model and attack model to prove that ZKAP owns no obvious design defects and can resist major attacks. But the scheme requires too many rounds (4 or 5) and too many messages (8 or 10) need to be communicated. The conventional security scheme only need communicate 5 messages.

## III. PROTOCOL DESCRIPTION

### A. System Parameters

Table 1 shows the parameters applied in the protocol.

### B. Authenticate Phase

Figure 1 shows the new protocol. We describe the protocol detail in the following according to the sequence of message exchanges.

1) Phase 1: Challenge messages: R generates a random number $r_R$, then computes $B_R = h(PID_R, r_R)$ and $C_R = PID_R \oplus r_R$, and sends $B_R$ and $C_R$ to T as an initial query.

TABLE I.

NOTATION

| Notation | Description |
|---|---|
| R | The reader in the RFID system |
| T | The tag in the RFID system |
| DB | The database in the RFID system |
| $L_R$ | the access list for tags to retrieve a certain reader |
| $L_T$ | the access list for the database to retrieve a certain tag |
| $r_R$ , $r_T$ | the random numbers generated by R , T |
| $PID_R$ , $PID_T$ | The pseudonym of R,T |
| h( ) | A one-way hash function |
| [ ] | The rounding operation |
| $\oplus$ | XOR bitwise logic operator |
| $\|$ | Concatenate operator |

2) Phase 2: Response messages: Upon receiving the query, T verifies R by search $PID_R$ in the access list and calculates the corresponding $r_R$. If there isn't $PID_R$ to meet $B_R$ and $C_R$, the protocol will terminate with an error code. Otherwise, T gets $PID_R$ and $r_R$, and performs the rounding operation on $r_R$ to gain a round-off integer $d = [r_R]$ along generating a random number $r_T$. T computes $D_T = h(r_R, PID_T)$ and $E_T = (r_T \oplus PID_R) >> d$, then responds $D_T$ and $E_T$ to R.
3) Phase 3: Forward message: When R receives the response, it extracts $r_T$ from $E_T$. Then it forwards $D_T$ and $r_R$ to the database DB for the further authentication.
4) Phase 4: Authenticate the tag: While receiving $D_T$ and $r_R$, DB verifies whether there is $PID_T$ in $L_T$. If it is false, T is considered as an illegal entity and R will terminate the authentication process with an error code. Otherwise, DB forwards $PID_T$ to R and T will be authenticated by R. Then R obtains $F_R = h(PID_T, r_T)$ by performing a one-way hash function and sends $F_R$ to T.
5) Phase 5: Authenticate the reader: Upon receiving $F_R$, T performs the one-way hash function on its current $PID_T$ and $r_T$. If the two values are equal, R will be authenticated by T. Otherwise, R will be considered as an illegal entity and T will terminate the authentication with an error code.

The proposed protocol adopts lightweight mechanisms to realize security, efficiency and reliability, including one-way hash, quick check, and mutual authentication. The main approaches are complementary as follows.

1) One-way hash is adopted to protect $PID_T$ and $PID_R$ to realize no reversibility without revealing any sensitive data. The one-way hash function has the following property: For any output y, it is

computationally infeasible to find an input such that $h(X) = y$, given no corresponding input is known [13]. In the open air interface, $\{B_R, D_T, F_R\}$can be safely published since an attacker may not find useful data from those messages.

2) Access lists ($L_R$, $L_T$) store all the pseudorandom identifiers and are used to mark a certain reader or a certain tag for quick search. *DB* maintains $L_T$ and *T* maintains $L_R$. For example, while receiving $D_T$ and $r_R$, *DB* checks $L_T$ for matching entry. The access lists as index-pseudonyms effectively reduce the time complexity of search operation and enable more scalable for dynamic systems.

3) Pseudorandom identifiers are transmitted instead of the real identifiers. Furthermore, *T* and *R* generate their random numbers $r_T$ and $r_R$ which are to ensure dynamic refresh in each session. Moreover, R and T store the last Pseudorandom identifiers and random numbers, if a new query arrives with the same data within certain time, it will be neglected. This will help the system resist the replaying or jamming attacks.

4) Mutual authentication procedure is performed to realize access control. T verifies R by two steps. The first step is to ensure the validity of $PID_R$. The second is to indeed authenticate R. *DB* authenticates T then transmits the message to R. If and only if both authentications succeed, communication between R and T is secure and will continue.

In summary, the new protocol is a lightweight mutual authentication scheme based on one-way hash function.

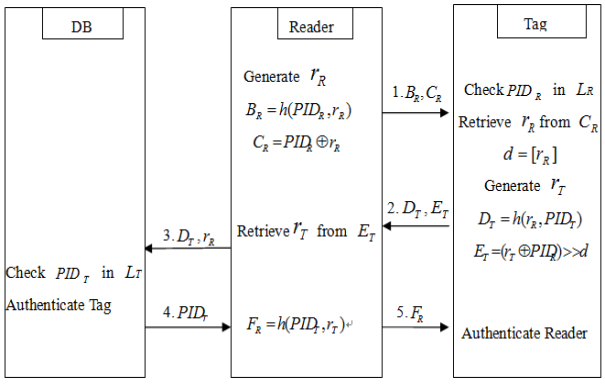


Figure 1. The mutual authentication protocol

## IV. Formal Analysis of the Protocol with GNY Logic

Most authentication protocols have been designed and demonstrated in informal ways. However, informal analysis may ignore design flaws and security errors. In the last section, we have been described basic security verification for the new protocol in the intuitive way. In the section, GNY Logic [19] is applied to analyze the design correctness of the new protocol. The formal method may evaluate the protocol strictly and completely therefore even subtle defects can be found. With the formal method, a protocol can be demonstrated to reasonably achieve its goals using logical postulates.

We do the GNY formal logic analysis like [9], and the analysis comprises of four steps: 1) formalization of the messages; 2) definition of initial assumptions; 3) definition of anticipant goals; 4) verification by logical rules and formulas.

### A. Formalization of Messages

We formalize of the protocol messages in the language of GNY Logic and express each exchanged message as a logical formula. For the sake of clarity, we use the same statements like [19][20]. Table 2 shows those statements.

TABLE II.

Basic Statements

| Notation | Description |
|---|---|
| $S \lhd X$ | S receives a message containing X, S can read and repeat X |
| $S \lhd * X$ | S receives X, X is a not-originated-here formula |
| $S \ni X$ | S possesses, or is capable of possessing X |
| $S \mid\sim X$ | S once conveyed X |
| $S \mid\equiv X$ | S believes, or would be entitled to believe, that statement X holds |
| $S \mid\equiv \phi X$ | S believes, or is entitled to believe that X is recognizable |
| $S \mid\equiv \# X$ | S believes, or is entitled to believe that X is fresh |
| $S \mid\equiv S \overset{V}{\longleftrightarrow} X$ | S believes, or is entitled to believe, that V is a suitable secret for S and X |
| $\{X, Y\}$ | Concatenation |

There are five messages (we called them: M1, M2, M3, M4, M5) between DB, R and T in the authentication phases. With those statements the formalized messages are as follows:

(M1) $T \lhd *h(PID_R, r_R), T \lhd *(PID_R \oplus r_R)$

(M2) $R \lhd *h(r_R, PID_T), R \lhd *(r_T \oplus PID_R) >> d$

(M3) $DB \lhd *h(r_R, PID_T), DB \lhd *r_R$

(M4) $R \lhd *PID_T$

(M5) $T \lhd *h(PID_T, r_T)$,

### B. Initial Assumptions

In order to deduce the security goals from the aforementioned statements, some assumptions are needed. We assume that the following statements can be obtained:

(A1) $R \ni r_R$;

(A2) $R \ni PID_R$, $R \mid\equiv \# PID_R$, $R \mid\equiv R \overset{PID_R}{\longleftrightarrow} T$;

(A3) $T \ni r_T$;

(A4) $T \ni PID_T$, $T \mid\equiv T \overset{PID_T}{\longleftrightarrow} DB$

(A5) $T \mid\equiv \# PID_R$, $T \mid\equiv T \overset{PID_R}{\longleftrightarrow} R$

(A6) $DB \mid\equiv \# PID_T$, $DB \mid\equiv DB \overset{PID_T}{\longleftrightarrow} T$

(A7) $R \mid\equiv DB \mid\Rightarrow (DB \mid\equiv *)$

Those statements show the initial possessions and abilities of each participator. Each tag T possesses $r_T$ and $PID_T$, and it is entitled to believe the $PID_R$ is fresh. The reader R possesses $r_R$ and $PID_R$. The database DB is entitled to believe the $PID_T$ is fresh. The communication channel between R and DB is considered to be secure; so R believes that DB has jurisdiction over all his beliefs.

### C. Anticipant Goals

The aim of the protocol is to mutual authenticate between R and T and assure the messages not used in the previous sessions. The anticipant goal can be expressed as follows:

(G1) $T \mid\equiv R \mid\sim r_R$,

(G2) $T \mid\equiv R \mid\sim PID_R$,

(G3) $R \mid\equiv T \mid\sim r_T$

(G4) $R \mid\equiv T \mid\sim PID_T$

(G5) $DB \mid\equiv T \mid\sim PID_T$

(G6) $T \mid\equiv \#h(PID_R)$

(G7) $R \mid\equiv \#h(PID_T)$

G1 and G2 show that T believes that R conveyed $r_R$ and $PID_R$. G3 and G4 show that R believes that T conveyed $r_T$ and $PID_T$. G5 shows that DB believes that T conveyed $PID_T$. G6 and G7 show that the messages are not used in the previous sessions. The first to fifth goals indicate that the messages are from legal entities. And the sixth and seventh goals indicate freshness requirements.

### D. Logic Verification

In this subsection, we will show that the goals can be deduced from the assumption, the formalized messages and the related GNY Rules.

From M1, T is informed messages $h(PID_R, r_R)$ and $(PID_R \oplus r_R)$. T has not received or sent them in the previous sessions, we have

$T \lhd *h(PID_R, r_R)$, $T \lhd *(PID_R \oplus r_R)$ (1)

Applying the Being-Told Rule T1: $(P \lhd (*X))/(P \lhd X)$ deduces

$T \lhd h(PID_R, r_R), T \lhd (PID_R \oplus r_R)$ (2)

T can retrieve $PID_R$ from $L_R$, and applying the Being-Told Rule T5: $(P \lhd F(X,Y), P \ni X)/(P \lhd Y)$ deduces

$T \lhd PID_R$, $T \lhd r_R$ (3)

Thus, T is considered to have been informed $PID_R$ and $r_R$.

Applying the Possession Rule P1 : $(P \lhd X)/(P \ni X)$ deduces

$T \ni PID_R$, $T \ni r_R$, $T \ni h(PID_R, r_R)$ (4)

Applying the Possession Rule P2: $(P \ni X, P \ni Y)/(P \ni (X,Y), P \ni F(X,Y))$ deduces

$T \ni (PID_R, r_R)$ (5)

From A5, $T \mid\equiv \#PID_R$, and applying the Freshness Rule F1: $(P \mid\equiv \#(X))/(P \mid\equiv \#(X,Y), P \mid\equiv \#F(X))$ deduces

$T \mid\equiv \#(PID_R, r_R)$, (6)

Applying the Message Interpretation Rule I3: $\frac{P \lhd H(X, <S>), P \ni (X,S), P \mid\equiv P \xleftrightarrow{S} Q, P \mid\equiv \#(X,S)}{P \mid\equiv Q \mid\sim (X, <S>), P \mid\equiv Q \mid\sim H(X, <S>)}$

deduces

$T \mid\equiv R \mid\sim (PID_R, r_R)$ (7)

Finally, from I3 interpretation and applying the Message Interpretation Rule I7: $(P \mid\equiv Q \mid\sim (X,Y))/(P \mid\equiv Q \mid\sim X)$ deduces

$T \mid\equiv R \mid\sim (PID_R)$, $T \mid\equiv R \mid\sim (r_R)$ (8)

As a result, T believes that R once conveyed $PID_R$ and $r_R$. Goal G1 and G2 are achieved.

Hereinafter, for simplicity, we directly mark the applied logical rules and formulas behind the formula.

For Goal 3: We can deduce that

$R \lhd *(r_T \oplus PID_R) >> d$ // by M2

$R \lhd (r_T \oplus PID_R) >> d$ //by T1

$R \lhd (r_T \oplus PID_R)$ //by T5

$R \lhd r_T$ // by T5

$R \ni r_T$ // by P1

$R \ni (r_T, PID_R)$ //by P2

$R \mid\equiv \phi(r_T)$ // by P4, R6

$R \mid\equiv \#(r_T, PID_R)$ //by A2, F1

$R \mid\equiv T \mid\sim r_T$ //by I1

According to I1, R is entitled to believe that T once conveyed $r_T$.

For Goal 5: We can deduce that

$DB \lhd *h(r_R, PID_T)$, $DB \lhd *r_R$ //by M3

$DB \lhd h(r_R, PID_T)$, $DB \lhd r_R$ //by T1

$DB \ni r_R$, $DB \ni h(r_R, PID_T)$ //by P1

$DB \ni PID_T$ // by P5 and access list $L_T$

$DB \ni (r_R, PID_T)$ //by P2

$DB \mid\equiv \#PID_T$ //A6

$DB \mid\equiv \#(r_R, PID_T)$ //by F1

$DB \mid\equiv T \mid\sim (PID_T)$ // by I3

According to I3, DB is entitled to believe that T once conveyed $PID_T$.

For Goal 4: we can deduce that

$R \mid\equiv DB \mid\Rightarrow (DB \mid\equiv *)$ //by A7

$DB \mid\equiv T \mid\sim (PID_T)$ // by Goal 5

$R \mid\equiv DB \mid\Rightarrow (T \mid\sim PID_T)$

$R \mid\equiv DB \mid\equiv (T \mid\sim PID_T)$ //by J3

$R \mid\equiv (T \mid\sim PID_T)$ //by J1

As a result, R is entitled to believe that T once conveyed $PID_T$.

For Goal 6: We can deduce that

$T \mid\equiv \#PID_R$ // by A5

$T \ni PID_R$ // from formula (2)

$T \mid\equiv \#h(PID_R)$ // by F10

As a result, T is entitled to believe that $h(PID_R)$ is fresh.

For Goal 7: We can deduce that

$R \mid\equiv DB \mid\Rightarrow (DB \mid\equiv *)$ //by A7

$DB \mid\equiv \#PID_T$ //by A6

$R \mid\equiv DB \mid\Rightarrow \#PID_T$

$R \mid\equiv DB \mid\equiv \#PID_T$ // by J3

$R \mid\equiv \#PID_T$ // by J1

$R \lhd *PID_T$ // by M4

$R \lhd PID_T$ // by T1

$R \ni PID_T$ //by P1

$R \mid\equiv \#h(PID_T)$ // by F10

As a result, R is entitled to believe that $h(PID_T)$ is fresh.

## V. Security Analysis

Like the majority of similar protocols, we suppose the communication between DB and the reader is secure. However, the wireless communication between the reader and the tag is confronted more serious challenges. We consider the following attack in the attack model: spoofing, replaying, tracking and DOS.

We perform the analysis with three steps like [9]. The first step is to suppose the action of the attacker and the second is to simulate the process of the attacking step by step. The last is to deduce the security.

### A. Spoofing Attack

In spoofing attack, the attack forges a legal reader to get the information of the tag or forges a legal tag to cheat the reader.

During the reader spoofing attack, an attacker simulates as a reader R and performs the following actions:

- In one session:

  A: A disguises as a reader $R_a$ and send a query to T.

  $A(R_a) \rightarrow T : h(PID_{Ra}, r_{Ra}), (PID_{Ra} \oplus r_{Ra})$.

  T: T can not find one match to verify $A(R_a)$.

  $T \not\Rightarrow A(R_a)$: Authentication will fail.

- In bad conditions:

  $T \rightarrow A(R_a) : h(r_{Ra}, PID_T), (r_T \oplus PID_{Ra}) >> d_a$ .

  $// d_a = [r_{Ra}]$

  If T responses $A(R_a)$ by mistake, then $A(R_a)$ obtains $r_T$.

- In the next session:

  A: A disguises as a tag $T_a$ first and intercept messages sent to T.

  $R \rightarrow A(T_a) \not\rightarrow T : h(PID_R, r_R), (PID_R \oplus r_R)$

  $A(T_a) \rightarrow R : h(r_{Ra}, PID_T), (r_T \oplus PID_{Ra}) >> d_a$

  R: R obtains $r_T'$ from $(r_T \oplus PID_{Ra}) >> d_a$ using $PID_R$ and $r_R$.

  $R \rightarrow DB : r_R, h(r_{Ra}, PID_T)$

  DB: DB checks whether there is a corresponding $PID_T$ in LT, and it will find that no matching flag since the probability that $r_R$ equals $r_{Ra}$ is negligible.

  $DB \not\Rightarrow A(T_a)$, authentication fails.

- In the worse conditions:

  If DB ignores the mistake and responses $PID_T'$ to R, R calculates to get $h(PID_T', r_T')$, and forwards it to A.

  $DB \rightarrow R : (PID_T')$

  $R \rightarrow A(T_a) : h(PID_T', r_T')$

  $A(T_a)$ can not obtain $PID_T$ from $h(PID_T', r_T')$ even if it possesses $r_T$.

  A: Finally, A disguises as a reader $R_a$ and forwards $h(PID_T', r_T')$ to T.

  $A(R_a) \rightarrow T : h(PID_T', r_T')$

  $T : h(PID_T', r_T') \neq h(PID_T, r_T)$

  $T \not\Rightarrow A(R_a)$, authentication fails.

### B. Replay Attack

Replay attack refers to that an attacker impersonates a legal entity to involve into the communications so as to access, modify, and even delete the messages [8]. The protocol uses a random number to resist the replay attack.

- In one session:

  A has learnt : { $h(PID_R, r_R)$ , $PID_R \oplus r_R$ , $h(r_R, PID_T)$ , $(r_T \oplus PID_R) >> d$ , $h(PID_T, r_T)$ }.

- In the next session:

  A disguises as a tag $T_a$.

  $R \rightarrow A(T_a) \not\rightarrow T : h(PID_R, r_R'), PID_R \oplus r_R'$

  $A(T_a) \rightarrow R : h(r_R, PID_T), (r_T \oplus PID_R) >> d$

  R: If $([r_R] == [r_R'])$ then R obtains $r_T$ from $(r_T \oplus PID_R) >> d$, then will find that $r_T$ has been used in the former session. The protocol terminates.

  Else, R obtains $r_T''$ from $(r_T \oplus PID_R) >> d$, and $r_T'' \neq r_T'$

  $R \rightarrow DB : r_R', h(r_R, PID_T)$

  DB:DB checks whether there is a corresponding $PID_T$ in LT, and it will find that no matching flag since $r_R' \neq r_R$.

- In the worse condition

  If DB ignores and responses $PID_T'$ to R, R calculates to get $h(PID_T', r_T'')$, and forwards it to A.

  $DB \rightarrow R : PID_T'$

  $R \rightarrow A(Ta) : h(PID_T', r_T'')$

Then A disguises as a reader $R_a$.

$$A(R_a) \rightarrow T : h(PID'_T, r''_T)$$

T: $h(PID_T, r'_T) \neq h(PID_T, r''_T)$, the protocol terminates.

*C. Tracking Attack*

The attacker may trace tags through collecting the transferring messages in the past transmissions or through malicious readers.

In the former situation, the reader and tag generate and use different random numbers for each authentication, so the attacker can not find two same messages and is incapable of tracing the certain tag.

In the latter, some malicious readers send the same query to a tag. If the tag responses the same message, the reader may trace the certain tag and achieve its related information.

If the attacker A performs the following actions:

$A(R_i) \rightarrow T$ :

$h(PID_{R_1}, r_{R_1})$ , $PID_{R_1} \oplus r_{R_1}$ ; $h(PID_{R_2}, r_{R_2})$ , $PID_{R_2} \oplus r_{R_2}$ ……

$T$ receives the messages and searches $PID_{R_i}$ in the access list $L_R$, there is no matching entry and the protocol will terminate.

In the worse conditions, $T$ may responses those readers by mistake:

$T \rightarrow A(R_i)$ :

$h(r_{R_1}, PID_T)$ , $(r_{T_1} \oplus PID_{R_1}) >> d_1$ ;

$h(r_{R_2}, PID_T), (r_{T_2} \oplus PID_{R_2}) >> d_2$ ;……

Any two responses are independent since ( $r_{T_1}, r_{T_2}, r_{T_3}$..... ) are diverse from each other and $(r_{R_1}, r_{R_2}, r_{R_3}....)$ are the same situations, while $d_i = [r_{R_i}]$ .Thus, the attacker is no ability to trace the certain tag according to those different messages.

Therefore, no matter which way the attacker employs, it is impossible to trace certain tag and the location privacy is ensured.

*D. DOS Attack*

DOS attack refers to the database and readers are not able to process the normal communications, because the attacker makes sure that their resources struggling to keep up through launching a lot of requests.

The purpose of DOS attack is not to achieve the sensitive data, but rather tying to disturb the normal communication.

In this protocol, we adopt two approaches to provide protection against the DOS attack like [9]. One is access lists ( $L_R, L_T$ ) for preliminary check. The database will block malicious attacks by no matching pseudorandom identifier in the access list $L_T$ and similarly $L_R$ will help the tag discern the illegal reader. Another approach is random/ pseudorandom numbers ( $r_R, r_T, PID_R, PID_T$ ). The legal tag and reader store the last received random numbers and pseudorandom identifiers as temp lists. They can refuse the query with the same random number or pseudorandom identifier within a certain time. So the attacker can not disturb the normal communication.

In the protocol, the forward security can be ensured because of random / pseudorandom numbers. An attacker cannot obtain tag's identifier replaced by $PID_T$ even it correctly guesses the random number $r_T$ . So the protocol offers anonymity.

## VI. PERFORMANCE ANALYSIS

In RFID systems, the performance is another important metric besides the security issue, such that the optimization and balance between security and performance are necessary for RFID systems [22].

Like most authentication protocols, the protocol needs five phases to complete the whole authentication process. In order to properly evaluate the protocol, we compare it with other related protocols in two aspects: storage requirement and computation load.

In our protocol, each tag stores identifier $ID_T$ , pseudorandom identifier $PID_T$ and access list $L_R$, while other related cryptographic algorithms(such as KAAP ) need store the secret keys. Access list stores all readers' pseudorandom identifiers. Additionally, the memory consumption on one-way hash function is another concern. Standardized cryptographic hash functions such as SHA-1 are too expensive for use in today's low-cost RFID tags [22][23]. A potential alternative is the Whirlpool hash function, which has been standardized by ISO/IEC and evaluated by the New European Schemes for Signatures, Integrity and Encryption (NESSIE) project [24]. Pramstalleret al. [25] present a compact hardware implementation of Whirlpool, which uses an innovative state representation that makes it possible to significantly reduce the required hardware resources [13].

During the entire round, each reader and each tag performs one random number generation ( RNG) operation. Each tag also performs one cryptographic hash function while each reader performs twice. Like KAAP, we adopt the access lists $L_R$ and $L_T$ to avoid exhaustive searches in the storage, which reduce the time complexity of search operation.

Table 4 shows the performance comparison with other related protocols. Our protocol has the similar storage requirement as protocols [9][14] and it is more than S-M. There are no exhaustive searches in the protocol like protocols [9][14], while protocol [13] require at least n searches in the storage. In the storage analysis, keys, random numbers and hash function value are ignored for the sake of simplicity. All the other components are assumed L bits sized. The protocol owns acceptable storage requirement and computation load. From Table 4, it shows that the protocol requirements fewer complex function invocations for the tag than the other three protocols.

TABLE III.

PERFORMANCE COMPARISON

| | storage | computation | |
|---|---|---|---|
| | T | T | DB+R |
| S-M | L | R+2H | R+(N+1)H |
| HIDVP | 3L | 3H | R+3H |
| KAAP | 3L | R+2E | R+2E |
| Our protocol | 3L | R+H | R+2H |

R:RNG operation; H: hash operation; E: encryption;
N:number of tags; L: length of identifier/access list;
Note: Ignoring the length of keys, random numbers and hash function value.

## VII. CONCLUSIONS

In this paper, a novel mutual authentication protocol based on one-way hash function is proposed for security protection in RFID-based sensor systems. The protocol adopts mutual authentication mechanism, access lists and random access control mechanism to strengthen security and privacy protection. The design correctness of the protocol is verified by GNY logic using as a formal analysis. According to attack model analysis, the protocol can resist several major attacks. Moreover, the protocol has acceptable storage requirements and computation load based on performance analysis. The protocol has better scalability because it does not need the secret keys. So the protocol is suitable for more large-scale and high-reliability application.

## ACKNOWLEDGMENT

This work was supported in part by a grant from ZheJiang science and technology plan key project, No. 2007 c11023.

## REFERENCES

[1] H. Chien and C. Chen, Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. Computer Standards & Interfaces, 29(2):254–259, February 2007.

[2] Dang Nguyen Duc, Hyunrok Lee and Kwangjo Kim. Enhancing Security of EPCGlobal Gen-2 RFID against Traceability and cloning. Auto-ID Labs White Paper WP-SWNET-016, 2006.

[3] Meingast Marci, King Jennifer and Mulligan Deirdre K. Security and privacy risks of embedded RFID in everyday things: The e-passport and beyond. *Journal of Communications*, v 2, n 7, p 36-48, 2007.

[4] Chen Bing, Tan Chengxiang, Jin Bo, Zou Xiang and Dai Yuebo.RFID-based electronic identity security cloud platform in cyberspace. *Journal of Networks*, v 7, n 7, p 1131-1138, 2012.

[5] Gaurav Kapoor and Selwyn Piramuthu. Vulnerabilities in Some Recently Proposed RFID Ownership Transfer Protocols. IEEE COMMUNICATIONS LETTERS, VOL. 12, NO. 3, MARCH 2010.

[6]S. Piramuthu, "Lightweight cryptographic authentication in passive RFID-tagged systems," *IEEE Trans. Systems, Man, and Cybernetics -Part C*, vol. 38, no. 3, pp. 360–376, 2008.

[7] A. Juels, Yoking-proofs for RFID tags, in: First International Workshop on Pervasive Computing and Communication Security, 2004.

[8] H. Liu, H. Ning,:' Zero-Knowledge Authentication Protocol Based on Alternative Mode in RFID Systems', IEEE Sensors Journal, Dec. 2011,Vol. 11, No. 12, pp.3235-3245.

[9] H. Ning, H. Liu, J. Mao, Y. Zhang.:' Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems', IET Communications,2011,vol. 5, lss.12, pp.1755-1768

[10] Sun, H.M., Ting, W.C.: 'A Gen2-based RFID authentication protocol for security and privacy', IEEE Trans. Mob. Comput.. 2009, 8, (8), pp. 1052–1062

[11] K. Sakai, W. Ku, R. Zimmermann, M. Sun, Dynamic Bit Encoding for Privacy Protection against Correlation Attacks in RFID Backward Channel. IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 1, JANUARY 2013,pp.112-123

[12] Y. Tian, G. Chen, and J. Li. A New Ultralightweight RFID Authentication Protocol with Permutation. IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 5, MAY 2012, pp.702-705

[13] B. Song and C. J Mitchell, RFID authentication protocol for Low-cost Tags, In the Proceedings of WiSec'08, March 2008, pp. 140-147.

[14] Rhee, K., Kwak, J., Kim, S., Won, D.: 'Challenge-response based RFID authentication protocol for distributed database environment', Secur. Pervasive Comput., 2005, 3450, pp. 70–84

[15] R. Doss , W. Zhou, S. Sundaresan, S. Yu, L. Gao. A minimum disclosure approach to authentication and privacy in RFID systems. Computer Networks 56 (2012) 3401–3416.

[16] Bin Wang and Maode Ma. A Server Independent Authentication Scheme for RFID Systems. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 8, NO. 3, AUG. 2012,pp.689-696

[17] M. Feldhofer, S. Dominikus, and J.Wolkerstorfer, "Strong authentication for RFID aystems using the AES algorithm," in *Proc. Cryptogr.Hardw. Embed. Syst., CHES'04*, 2004, vol. 3156, LNCS, pp. 357–370.

[18] S. I. Ahamed, F. Rahman, and E. Hoque, "ERAP: ECC based RFID authentication protocol," in *Proc. 12th IEEE Int. Workshop on Future Trends of Distrib. Comput. Syst. (FTDCS'08)*, 2008, pp. 219–225.

[19] Gong, L., Needham, R., Yahalom, R.: 'Reasoning about belief in cryptographic protocols'. Proc. IEEE Computer Society Symp. Research in Security and Privacy, California, USA, May 1990,pp. 234–248

[20] Godor, G., Imre, S.: 'Security analysis of the simple lightweight authentication protocol'. Proc. 2010 Ninth Int. Conf. Networks (ICN), French Alps, France, April 2010, pp. 231–236

[21]. Olteanu, A., Xiao, Y., Zhang, Y.: 'Optimization between AES security and performance for IEEE 802.15.3 WPAN', IEEE Trans. Wirel. Commun., 2009, 8, (12), pp. 6030–6037

[22] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch. From identification to authentication — a review of RFID product authentication techniques. In Printed handout of Workshop on RFID Security — RFIDSec 2006, 2006.

[23] Stephen Weis. Security and privacy in radio-frequency identification devices. Master's thesis, Massachusetts Institute of Technology (MIT), Massachusetts, USA, May 2003.

[24] B. Preneel et al. Final report of European project IST-1999-12324: New European schemes for signatures, integrity, and encryption. Available at: www.cosic.esat.kuleuven.be/nessie/, April 2004.

[25] N. Pramstaller, C. Rechberger, and V. Rijmen. A compact FPGA implementation of the hash function whirlpool. In ACM/SIGDA 14th international symposium on Field

Programmable Gate Arrays — FPGA'06, ACM Press, pages 159–166, New York, 2006.

**Xueping Ren** was born in 1978 in Zhejiang Province, China.

She received the B.S. degree from Hanzhou Dianzi University, Hangzhou, China, in 2005.

Currently, she is a lecturer at the School of computer science and technology, Hangzhou Dianzi University. She has participated in several research projects at the provincial Science Foundation of Zhejiang and the Development Program of China (973 Project), etc. She has published more than 10 papers in journals, international confer ences and workshops, her current research focuses on RFID.

**Xianghua Xu** is now a professor in the School of Computer Science at Hangzhou Dianzi Unviersity, China. He received his B.Eng. in Computer Science from Hangzhou Dianzi University, China, and his Ph.D. degree in Computer Science from Zhejiang University, China. His research interests include wireless networks, parallel and distributed computing, cloud computing. His recent research has been supported by Natural Science Fundation of China. He has served as program committee member of ChinaGrid'2008/2009/2011, GCC'2009/2010 and the publication chair of APSCC'2010. He is the member of the IEEE, ACM, the senior member of CCF (China Computer Federation). He is also the member of CCF Technical Committee of Service Computing and CCF Technical Committee of High Performance Computing. E-mail: xhxu@hdu.edu.cn.

**Yunfa Li** is an associate professor of the School of Computer Science and Technology, Hangzhou Dianzi University, P.R. China. He received the PhD degree and the Master degree in Computing Science from Huazhong University of Science and Technology, and the bachelor's degree in mathematics from Wuhan University. His research interests include Performance Modeling and Analysis of Software, Virtual Machine, Cloud Computing, System Security, and Network Security. He has published over 30 research papers in the well-established journals and conferences including Cluster Computing, The Journal of Supercomputing, IET Communications, International Journal of Ad Hoc Ubiquitous Computing, Jisuanji Yanjiu yu Fanzhan, and Tien Tzu Hsueh Pao.