基于伪随机数发生器的移动 RFID 双向认证算法

郝伟伟[1],吕　磊[2]
(1. 河南省市场监督管理局 信息中心,河南 郑州 450008;
2. 河南工业大学 信息科学与工程学院,河南 郑州 450008)

摘　要:经典式的射频识别系统中读写器与后台服务器之间通过有线方式交换数据,无法满足现在人们不断增长的各种需求,移动式射频识别系统的出现,则能够解决经典式射频识别系统的困境。为能够适应移动式射频识别系统的运用,需要设计移动式的双向认证协议,以保障服务器与读写器间采用无线方式发送信息的安全性。文中提出一种轻量级的可适用于移动式 RFID 系统的双向认证算法,该算法基于伪随机发生器实现对发送信息的加密;为能够确保每轮消息的新鲜性,所有消息在加密的时候,全部混入随机数,使得每轮消息值不同;因随机数的随机性、互异性,使得前后消息值之间无任何关联性,增加攻击者破解难度。对多个经典协议从不同类型的攻击角度分析,表明文中算法具备良好的安全性能,同时可弥补其他算法的缺陷或不足;在计算量角度对比分析各算法,指出文中算法计算时间复杂度优于其他对比算法。

关键词:射频识别技术;移动系统;伪随机数发生器;双向认证算法;新鲜性
中图分类号:TP393.08　　**文献标识码**:A　　**文章编号**:1673-629X(2022)05-0093-06
doi:10.3969/j.issn.1673-629X.2022.05.016

Mobile RFID Bidirectional Authentication Algorithm Based on Pseudo Random Number Generator

HAO Wei-wei[1],LYU Lei[2]
(1. Information Center,Administration for Market Regulation of Henan Province,Zhengzhou 450008,China;
2. School of Information Science and Technology,Henan University of Technology,Zhengzhou 450008,China)

Abstract:In the classic RFID system,the data exchange between the reader and the server can't meet the growing needs of people. The emergence of mobile RFID system can solve the dilemma of the classic RFID system. In order to adapt to the application of mobile RFID system,it is necessary to design a mobile two-way authentication protocol to ensure the security of wireless information transmission between server and reader. In this paper,a lightweight two-way authentication algorithm for mobile RFID system is proposed,which encrypts the sent information based on pseudo-random generator. In order to ensure the freshness of each round of messages,all messages are mixed with random numbers when they are encrypted,so that the value of each round of messages is different. Because of the randomness and mutuality of random numbers,there is no correlation between the front and back message values,which makes it more difficult for attackers to crack. The analysis of several classical protocols from different types of attacks shows that the proposed algorithm has good security performance,and can make up for the defects of other algorithms. From the point of view of the amount of computation,it is pointed out that the time complexity of the proposed algorithm is better than other algorithms.

Key words:RFID technology;mobile system;pseudo random number generator;mutual authentication algorithm;freshness

0　引　言

射频识别技术是一种不需要与特定商品相接触就可以识别内部存放信息的技术,该技术最早出现于 20 世纪,受限于 20 世纪科技等各方面制约,未能得到较大范围推广使用[1-2]。进入新世纪之后,伴随着云计算、大数据、物联网、区块链等新技术的不断产生,以及全球经济持续快速发展,使得射频识别技术再次得到发展机遇[3-4]。

一个经典的 RFID 系统至少包含有电子标签、读写器、后台服务器三者,受限于当时科技或人类需求等因素,电子标签与读写器间以无线方式交互数据,读写器与后台服务器间以有线方式交互数据。一般认为无线方式交互数据易被第三方人员窃听,存在一定安全风险,认为不安全、不可靠,而有线方式交互数据不易

收稿日期:2021-04-19　　**修回日期**:2021-08-24
基金项目:国家自然科学基金(61705060)
作者简介:郝伟伟(1985-),男,高级工程师,CCF 会员(F9494M),研究方向为电子政务、信息安全、项目管理。

被第三方人员窃听,一般认为安全可靠[5-7]。但随着科技进步、人类需求越来越多,且越来越复杂,经典的 RFID 系统早已无法满足,出现了移动式 RFID 系统。该系统主要不同之处在于:读写器与后台服务器间也采用无线方式交互数据[8-9]。

为能够确保每个无线方式交互数据的安全性,需要设计新的可适用于移动式 RFID 系统的双向认证算法。文献[10]中提出的算法仅适合于在传统的 RFID 系统中使用,无法在移动式系统中使用,使用范围受到制约。文献[11]中设计的算法可在移动式 RFID 系统中使用,但算法采用传统的加密算法对消息进行加密,使得电子标签一端无法使用,该算法仅能在一些特定场合使用。文献[12]中提出的算法具有一定的安全性,但算法未考虑物理克隆的可能性,导致算法无法抵抗假冒攻击。文献[13]中的算法可使用在移动式系统中,但算法使用到不同类型的哈希函数对信息进行加密,使得电子标签一端无法推广使用。文献[14]中基于按位运算给出一种超轻量级的可在移动式系统使用的算法,但根据现有的研究表明,基于按位运算的算法本身安全性还有待商榷,因此该算法的安全性也有待商榷。限于篇幅,更多有关 RFID 双向认证可以参见文献[15-20]。

鉴于现有绝大多数算法无法适用于移动式 RFID 系统或计算量大或存在安全缺陷等不足,文中提出一种轻量级的可适用于移动式 RFID 系统的双向认证算法。

1 算法设计

本章节将从下面两个方面展开,首先对算法中出现的符号给予详细的含义描述,接着对算法具体实现步骤展开描述。

(1)算法符号说明及初始化。

DB 表示后台服务器;

R 表示读写器;

T 表示电子标签;

K 表示 DB、R、T 三者之间共享密钥;

IDR 表示 R 的身份标志;

IDT 表示 T 的身份标志;

x 表示 T 生成的随机数;

y 表示 DB 生成的随机数;

PR( )表示伪随机发生器运算;

&表示按位与运算;

⊕表示按位异或运算。

(2)算法具体实现。

DB 与 R 间以无线方式交换数据,R 与 T 间以无线方式交换数据,都认定为不安全[21]。算法启动之前,即 T 离开工厂之前,经过初始化操作后,T、R、DB 三者均存放有共享密钥 K 值,同时 DB 一端还存放有 IDR、IDT。文中轻量级的移动 RFID 双向认证算法如图 1 所示。

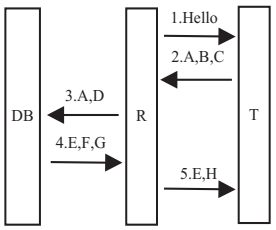

图 1 轻量级双向认证算法

文中算法具体步骤如下描述:

(1)读写器向电子标签发送一个 Hello 消息,用于告知电子标签开始双向认证算法。

(2)电子标签在收到读写器发送来的消息之后,电子标签首先产生一个随机数,可以标记为 x;接着电子标签用产生的随机数 x、自身存放的共享密钥 K 计算得到消息 $A=x\oplus K$、$B=PR(x,K)$,用产生的随机数 x、自身存放的共享密钥 K、自身存放的电子标签的标识符 IDT 计算得到消息 $C=PR(x\oplus IDT,K)$;最后将计算得到的消息 A、B、C 发送给读写器。

(3)读写器在收到电子标签发送来的消息之后,首先对消息 A 进行变形处理,可以得到随机数 $x'=A\oplus K$;接着读写器用变形处理得到的随机数 x'、自身存放的共享密钥 K 计算得到一个消息 $B'=PR(x',K)$,并对比计算得到的消息 B' 与接收到的消息 B 值是否相等。

如果两者值不相等,说明电子标签无法通过读写器的验证,算法停止。

如果两者值相等,说明读写器验证电子标签成功。接着读写器用变形处理得到的随机数 x、自身存放的读写器标识符 IDR、接收到的消息 C 计算得到消息 $D=PR(C\oplus x,IDR)$;最后将消息 A、D 发送给后台服务器。

(4)后台服务器在收到读写器发送来的消息之后,首先对消息 A 进行变形处理可以得到随机数 $x''=A\oplus K$;然后利用计算得到的随机数 x''、自身存放的共享密钥 K、自身存放的电子标签的标识符 IDT 计算得到一个消息 $C'=PR(x''\oplus IDT,K)$,紧接着再用计算得到的消息 C'、变形处理得到的随机数 x''、自身存放的读写器的标识符 IDR 计算得到一个消息 $D'=PR(C'\oplus x'',IDR)$。并对比计算得到的消息 D' 与接收到的消息 D 值是否相等。

如果两者值不相等,表明读写器或电子标签中至少有一方是伪造的,算法停止。

如果两者值相等,可以说明电子标签和读写器同

时通过后台服务器的验证。接着后台服务器生成一个随机数,可以标记为 y ,后台服务器利用生成的随机数 y 、计算得到的随机数 x 计算得到消息 $E=y\oplus x$;用生成的随机数 y 、自身存放的读写器的标识符 IDR、自身存放的共享密钥 K 计算得到消息 $F=PR(y\oplus IDR,K)$;利用计算得到的随机数 x 、自身存放的电子标签的标识符 IDT、自身存放的共享密钥 K 计算得到消息 $G=PR(x\&IDT,K)$ 。最后后台服务器将消息 E、F、G 发送给读写器。

(5)读写器在收到后台服务器发送的消息之后,先对消息 E 进行变形处理得到随机数 $y'=E\oplus x$;然后利用变形处理得到的 y' 、自身存放的共享密钥 K、自身存放的读写器的标识符 IDR 计算得到一个消息 $F'=PR(y'\oplus IDR,K)$,并对比计算得到的消息 F' 与接收到的消息 F 值是否相等。

如果两者值不相等,说明后台服务器无法通过读写器验证,算法停止。

如果两者值相等,表明读写器对后台服务器的验证成功。读写器接着利用接收到的消息 G、变形处理得到的随机数 y' 、自身存放的共享密钥 K 计算得到消息 $H=PR(G\&y,K)$ 。最后读写器将消息 E、H 发送给电子标签。

(6)电子标签在收到读写器发送来的消息之后,首先对消息 E 进行变形处理得到一个随机数 $y''=E\oplus x$;接着电子标签利用自身生成的随机数 x 、自身存放的电子标签的标识符 IDT、自身存放的共享密钥 K 计算得到一个消息 $G'=PR(x\&IDT,K)$,利用变形处理得到的随机数 y'' 、自身存放的共享密钥 K、计算得到的消息 G' 计算得到一个消息 $H'=PR(G'\&y'',K)$,并对比计算得到的消息 H' 与接收到的消息 H 值是否相等。

如果两者值不相等,表明电子标签对读写器的验证失败,算法停止。

如果两者值相等,表明读写器通过电子标签的验证,且也可以说明后台服务器同时通过电子标签的验证,截止到此,双向认证算法顺利结束。

2　算法安全性分析

本章节将主要从双向认证、重放攻击等角度展开分析文中算法安全性。

(1)双向认证。

算法实现双向认证是一个最基本也是必须的要求,文中算法可以保证实现。

通过上一章节算法具体步骤描述可以看出,文中算法每会话实体在接收到消息之后,并不是马上回复消息来源方,而是先对消息来源方进行验证,只有在消息来源方通过接收方验证之后,消息接收方才会开始进行其他操作。一旦消息来源方无法通过接收方验证,则算法即刻停止。基于上述,可得知文中算法可以实现双向认证安全需求。

(2)重放攻击。

因移动式 RFID 系统中,任何两个会话实体之间的数据交换方式都是无线链路,无线链路固有的开放式,使得交互数据易被第三方人员窃听获取,并在下一轮会话中第三方人员重放窃听获取的之前的消息,以企图通过合法实体一方验证。

(3)假冒攻击。

从理论上来讲,第三方人员可以假冒成任何一个会话实体与其他会话实体进行通信,具体的:第三方人员可假冒成电子标签、可以假冒成读写器、可以假冒成后台服务器。鉴于篇幅有限等因素,此处仅选择第三方人员假冒成读写器与合法电子标签进行通信进行分析。

当第三方人员假冒成读写器时,第三方人员会给合法电子标签发送一个 hello 指令,合法电子标签收到消息后,经过一系列操作,最终会响应第三方人员,并给第三方人员返回一些合法消息,但该消息都是加密之后的密文。第三方人员接收到之后,需要先对部分消息解密以获取合法电子标签产生的随机数,从而才可以继续后面的破解操作。但因为第三方人员缺少 DB、R、T 三者间共享密钥,使得第三方人员无法正确破解出合法电子标签生成的随机数,第三方人员无法获取正确随机数值,就无法进行后面破解。第三方人员只能随机选择一些数据作为无法获取的正确值参与运算,并将运算结果发送给后台服务器。后台服务器收到消息后,只需要进行简单的验证,即可识别出消息来源方是假冒的,算法停止。第三方人员假冒失败,未能获取任何有用隐私信息。基于上述,可得知文中算法可以实现抵抗假冒攻击。

(4)追踪攻击。

第三方人员想要追踪电子标签的具体位置,则需要持续监听通信,以获取电子标签发出的消息,并对获取的消息进行分析,以确定电子标签位置。但文中算法对于第三方来说则无法完成消息分析,因消息加密过程中使用到电子标签生成的随机数 x ,将会使得电子标签每轮计算得到消息值发生变更,展现给第三方人员的将是电子标签不断处于变动状态,第三方根本无法追踪定位电子标签的具体位置。基于上述,可得知文中算法可以实现抵抗追踪攻击。

(5)前向安全性。

第三方人员想通过对监听获取的消息进行破解,以便可以分析出之前通信过程中涉及到用户的重要隐

私信息,从而构成前向安全性。但文中算法,第三方人员无法破解分析出之前任何一轮通信中有关用户隐私信息,原因主要如下:每个消息加密过程中都参加入随机数,或加入随机数 x 或加入随机数 y 或同时加入随机数 x 、y ,将使得每轮每个消息值都是处于变化状态中,当第三方人员对第 i 次通信消息进行分析,第 $i-1$ 次消息值已变更,且前后两次消息值间无任何关联性。基于上述,可得知文中算法可以实现前向安全性。

(6)后向安全性。

所谓的后向安全性是说攻击者通过窃听可获取第 i 轮会话的所有消息,通过对第 i 轮消息的分析,企图预测出第 $i+1$ 轮会话实体之间的通信消息,攻击者假冒成其中一方进行通信,破解出标签中更多的隐私信息,从而造成用户存放在标签中的隐私信息泄露。文中主要通过混入随机数的方式来解决上述问题,具体的分析过程如下:文中每个消息在加密的时候都至少加入一个随机数,或加入标签产生的随机数,或加入后台数据库产生的随机数,或同时加入标签和后台数据库产生的随机数,并且随机数每轮由随机数产生器随机产生,将会使得每轮用到的随机数的数值都是不相同的,且时时刻刻处于变动状态;再加上前后两轮随机数间并无关联性,将导致攻击者根本无法从当前通信的消息中分析出任何有帮助预测下轮会话的消息信息。从而使得攻击者按照自己计算的下轮会话消息进行假冒其中一方进行通信时,消息接收方仅只是需要进行简单的计算,即可识别出消息来源方并非真实可靠的会话实体,算法立刻结束,截至此时,攻击者并未获取或分析出有用的隐私信息。基于上述,文中算法能够抵抗后向安全性。

各算法之间的安全性对比见表 1。

表 1 各算法间安全性对比

攻击类型	文献[11]	文献[12]	文献[13]	文献[14]	文中算法
双向认证	√	√	√	√	√
重放攻击	√	√	√	×	√
假冒攻击	√	×	√	√	√
追踪攻击	×	√	√	√	√
前向安全	√	√	×	√	√
后向安全	√	√	√	√	√

注:√表示可以抵抗该种类型的攻击方式;×表示无法抵抗该种类型的攻击方式。

3 算法性能分析

在移动式 RFID 系统中,虽包含电子标签、读写器、服务器三个实体,但只有电子标签在计算能力和存储方面受到严重制约,因此这里仅选择电子标签作为性能对比分析对象,具体见表 2。

表 2 不同算法间性能对比

对比算法	通信量	计算量	存储量
文献[11]	13 L +1 bit	1 T_1 +5 T_6	4 L
文献[12]	11 L +1 bit	2 T_1 +3 T_5	3 L
文献[13]	9 L +1 bit	3 T_1 +6 T_3	2 L
文献[14]	15 L +2 bit	5 T_1 +7 T_4	3 L
文中算法	10 L +1 bit	2 T_1 +4 T_2	2 L

对于表 2 里面部分符号给出下面的解释:约定所有算法中消息长度都为 L 。T_1 表示按位运算(比如异或运算、与运算、连接运算等)的计算时间, T_2 表示伪随机发生器运算的计算时间, T_3 表示哈希函数运算的计算时间(不同形式的哈希函数计算时间可能存在差别,这里统一看成相同的计算时间), T_4 表示可基于按位运算实现的超轻量级的运算计算时间, T_5 表示物理不可克隆函数的计算时间, T_6 表示模运算的计算时间。

在上述涉及到的运算中, T_1 和 T_4 的计算时间最短,可称之为超轻量级的计算; T_3、T_5、T_6 的计算时间最长; T_2 的计算时间介于上述两者之间。各运算的运算时间可大致按照如下方式由小到大进行排序: $T_1 < T_4 < T_2 < T_3 < T_5 < T_6$。

存储量的由来:电子标签一端存放的数据有 IDT、K,根据上述约定,可得知存储量为 2 L 。

通信量的由来:一个 DB、R、T 三者间完整通信包含的消息有,A 消息 2 次、B 消息 1 次、C 消息 1 次、D 消息 1 次、E 消息 2 次、F 消息 1 次、G 消息 1 次、H 消息 1 次、Hello 指令 1 次,其中 Hello 指令消息仅需要 1 bit 来存放即可,故一个完整会话过程中的通信量为 10 L +1 bit。

电子标签一端计算量的由来:在计算消息 A 时第一次用到按位异或运算,在计算消息 B、C、G′、H′时分别依次第一次、第二次、第三次、第四次用到伪随机数发生器运算,在计算随机数 y'' 时第二次用到按位异或运算。因此,电子标签一端总的计算时间为 $2T_1+4T_2$。

通过表 2 综合分析可得知,在通信量和存储量方面文中算法与其他算法大致相当;在计算量方面,文中算法比文献[14]中算法计算量要大,比其他文献中算法计算量都要小。但文献[14]中算法存在一定的安全缺陷,文中算法可以弥补其算法不足。综合安全性和性能两方面分析,文中算法在计算量角度存在一定的优势,同时安全方面可弥补其他算法存在的安全隐患问题,使得文中算法具有推广使用价值。

4　逻辑化形式证明

(1)形式化模型。

Msg1: R → T:Hello

Msg2: T → R:A,B,C

*Msg*3: R → DB:A,D

Msg4: DB → R:E,F,G

Msg5: R → T:E,H

(2)初始化假设。

读卡器 R 所拥有的:

A1: R ∋ IDR

A2: R ∋ K

电子标签 T 所拥有的:

A3: *T* ∋ K

A4: T ∋ IDT

后台服务器 DB 所拥有的:

A5: DB ∋ IDT

A6: DB ∋ IDR

A7: DB ∋ K

读写器 R 对拥有信息新鲜性的相信:

A8: R | ≡ #(x)

A9: R | ≡ #(y)

电子标签 T 对拥有信息新鲜性的相信:

*A*10: T | ≡ #(x)

A11: T | ≡ #(y)

后台服务器 DB 对拥有信息新鲜性的相信:

A12: DB | ≡ #(x)

A13: DB | ≡ #(y)

后台服务器 DB 与电子标签 T 间彼此相信共享信息:

A14: DB | ≡ $\mathrm{DB} \overset{\mathrm{IDT}}{\leftrightarrow} T$

A15: DB | ≡ $\mathrm{DB} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{T}$

电子标签 T 与后台服务器 DB 间彼此相信共享信息:

A16: T | ≡ $\mathrm{T} \overset{\mathrm{IDT}}{\leftrightarrow} \mathrm{DB}$

A17: T | ≡ $\mathrm{T} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{DB}$

读写器 R 与后台服务器 DB 间彼此相信共享信息:

A18: R | ≡ $\mathrm{R} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{DB}$

A19: R | ≡ $\mathrm{R} \overset{\mathrm{IDR}}{\leftrightarrow} \mathrm{DB}$

后台服务器 DB 与读写器 R 间彼此相信共享信息:

A20: DB | ≡ $\mathrm{DB} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}$

A21: DB | ≡ $\mathrm{DB} \overset{\mathrm{IDR}}{\leftrightarrow} \mathrm{R}$

电子标签 T 与读写器 R 间彼此相信共享信息:

A22: T | ≡ $\mathrm{T} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{R}$

读写器 R 与电子标签 T 间彼此相信共享信息:

A23: R | ≡ $\mathrm{R} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{T}$

(3)证明目标。

G1: T | ≡ R | ~ #(E)

G2: T | ≡ R | ~ #(H)

G3: R | ≡ T | ~ #(A)

G4: R | ≡ T | ~ #(B)

G5: R | ≡ T | ~ #(C)

G6: DB | ≡ R | ~ #(A)

G7: DB | ≡ R | ~ #(D)

G8: R | ≡ DB | ~ #(E)

G9: R | ≡ DB | ~ #(F)

G10: R | ≡ DB | ~ #(G)

(4)推理证明。

因为上面十个需要证明的目标证明过程大致相同,同时加上篇幅有限等因素,文中这里仅选择证明目标 G1 为例进行推导证明,具体证明推导过程如下:

首先,因为初始化假设 A10: T | ≡ #(x)、A11: T | ≡ #(y) 和新鲜性规则 F1: $\dfrac{P \mid \equiv \#(X)}{P \mid \equiv \#(X,Y), P \mid \equiv \#(F(X))}$ 可得知: T | ≡ #(x,IDT)。

在 Msg5 中, R◁ ∗ x,即 R ∋ x,同时结合初始化假设 A3、A4 和规则 P2 可得知: T ∋ (x,IDT)。

接着,由已推导出的 T | ≡ #(x,IDT)、T ∋ (x,IDT),再根据新鲜性规则 F10: $\dfrac{P \mid \equiv \#(X), P \ni X}{P \mid \equiv \#(H(X,Y))}$ 可得知: T | ≡ #(E)。

最后,根据 Msg5、初始化假设 A22、已推导出的 T ∋ (x,IDT)、T| ≡ #(E)、消息解析规则 I3 可得到: T | ≡ R | ~ (E)。

由新鲜性的定义可推导出证明目标 G1: T | ≡ R | ~ #(E)。

5　结束语

文中介绍了经典的 RFID 系统的优缺点,提出一个适用于移动 RFID 系统的双向认证算法。该算法不仅可使用在经典的 RFID 系统中,同时也可适用于移动 RFID 系统中,具备更为广泛的使用推广范围;算法采用伪随机数发生器对发送隐私信息进行加密,能够确保信息安全性,同时随机数数发生器的使用,可在一定程度上减少系统整体计算量。从不同类型攻击方式对算法进行安全性分析,表明算法能够提供抵抗常见类型攻击方式安全需求;同时从计算量、通信量角度对

算法进行性能分析,表明算法具有较低的计算开销。

参考文献:

[1] TANG Fei, HUANG Dong. A BLS signature scheme from multilinear maps[J]. International Journal of Network Security,2020,22(5):728-735.

[2] XIE Rui,LING Jie,LIU Daowei. Wireless key generation algorithm for RFID system based on bit operation[J]. International Journal of Network Security,2018,20(5):938-949.

[3] 王 萍,周治平,李 静. 无后端数据库的 RFID 安全认证协议的改进方案[J]. 计算机科学与探索,2018,12(7):1117-1125.

[4] TEWARI A,GUPTA B B. Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags[J]. The Journal of Supercomputing,2017,73(3):1085-1102.

[5] 李艳俊,汪书北,杨晓桐,等. 基于移动端的轻量级 NFC 安全认证方案[J]. 计算机工程与应用,2020,56(16):84-89.

[6] WANG J Q,ZHANG Y F,LIU D W. Provable secure for the ultra-lightweight RFID tag ownership transfer protocol in the context of IoT commerce[J]. International Journal of Network Security,2020,22(1):12-23.

[7] 石乐义,贾 聪,宫 剑,等. 基于共享秘密的伪随机散列函数 RFID 双向认证协议[J]. 电子与信息学报,2016,38(2):361-366.

[8] ZUO Cen. Defense of computer network viruses based on data mining technology[J]. International Journal of Network Security,2018,20(4):805-810.

[9] GOPE P,LEE J,QUEK T Q S. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions[J]. IEEE Transactions on Information Forensics and Security,2018,13(11):2831-2843.

[10] 刘道微,凌 捷,杨 昕. 一种改进的满足后向隐私的 RFID 认证协议[J]. 计算机科学,2016,43(8):128-130.

[11] XIE Rui,JIAN Biyuan,LIU Daowei. An improved ownership transfer for RFID protocol[J]. International Journal of Network Security,2018,20(1):149-156.

[12] LIU Y L,YIN X C,DONG Y Q,et al. Lightweight authentication scheme with inverse operation on passive RFID tags[J]. Journal of the Chinese Institute of Engineers,2019,42:74-79.

[13] SHEN Gaofeng,GU Shumin,LIU Daowei. An anti-counterfeit complete RFID tag grouping proof generation protocol international[J]. Journal of Network Security,2019,21(6):889-896.

[14] 黄可可,刘亚丽,殷新春. 基于位重排变换的超轻量级 RFID 双向认证协议[J]. 计算机应用,2019,39(1):118-125.

[15] ZHAO Mingju,PENG Yuping. A novel certificateless aggregation signcryption scheme under internet of things[J]. International Journal of Network Security,2021,23(2):238-245.

[16] LIU Ting,CUI Zhe,DU Hongjiang,et al. Privacy-preserving and verifiable electronic voting scheme based on smart contract of blockchain[J]. International Journal of Network Security,2021,23(2):296-304.

[17] ALORNYO S,MENSAH A E,ABBAM A O. Identity-based public key cryptographic primitive with delegated equality test against insider attack in cloud computing[J]. International Journal of Network Security,2020,22(5):743-751.

[18] YIN Shoulin,LIU Jie,TENG Lin. A sequential cipher algorithm based on feedback discrete hopfield neural network and logistic chaotic sequence[J]. International Journal of Network Security,2020,22(5):869-873.

[19] YAO Huijun,LI Chaopeng,SUN Peng. Using parametric t-distributed stochastic neighbor embedding combined with hierarchical neural network for network intrusion detection[J]. International Journal of Network Security,2020,22(2):265-274.

[20] MINAAM D S A,IBRAHIM M A,BADR E. Chaotic NHCP:building an efficient secure framework for cloud computing environment based on chaos theory[J]. International Journal of Network Security,2020,22(2):283-295.

[21] 殷秋实,陈建华. 多服务器环境下基于椭圆曲线密码的改进的身份认证协议[J]. 计算机科学,2018,45(6):111-116.