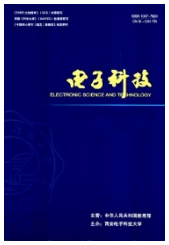

电子科技
Electronic Science and Technology
ISSN 1007-7820,CN 61-1291/TN

《电子科技》网络首发论文

题目：RFID 系统的安全性和隐私保护方法
作者：史志才
DOI：10.16180/j.cnki.issn1007-7820.2025.02.010
收稿日期：2023-08-04
网络首发日期：2024-04-09
引用格式：史志才．RFID 系统的安全性和隐私保护方法[J/OL]．电子科技．
https://doi.org/10.16180/j.cnki.issn1007-7820.2025.02.010

doi: 10.16180/j.cnki.issn1007-7820.2025.02.010

RFID 系统的安全性和隐私保护方法

史志才 [1,2]

（1.上海工程技术大学 电子电气工程学院，上海 201620；2.上海中侨职业技术大学 信息工程学院，上海 201514）

摘要：针对 RFID(Radio Frequency IDentification)系统因射频标签结构简单、与阅读器间采用无线方式传输数据，易产生隐私泄露和受到安全攻击的问题，文中提出通过双向轻权认证协议来保护 RFID 系统的安全性和隐私。该协议通过随机化标签的秘密信息再哈希的方法生成会话消息，标签与阅读器间采用二次相互认证，提升了协议的安全性。该协议通过哈希运算确保认证过程中会话信息的保密传输和完整性，通过对标签端每次发出会话消息的随机化确保了消息的新鲜性，系统秘密信息的更新确保协议满足前向安全性。RFID 认证协议不仅能抵抗窃听、追踪、重放、去同步化等攻击，还能满足 RFID 系统的安全性和隐私保护需要。.

关键词:RFID 系统；认证协议；安全；隐私；哈希函数；射频标签；保密性；完整性；伪随机数

中图分类号: TP393.08 **文献标识码:** A

Research on the Security and Privacy Preserving Method of RFID Systems

SHI Zhicai[1,2]

（1.School of Electronic and Electrical Engineering,Shanghai University of Engineering Science,Shanghai 201620,China;2.School of Information Engineering,Shanghai Zhongqiao Vocational and Technical University,Shanghai 201514,China）

Abstract：In view of the problem of privacy leakage and security attack in RFID system due to the simple structure of radio frequency tag and the wireless transmission of data between reader and RFID system, this study proposes to protect the security and privacy of RFID system through two-way lightweight authentication protocol. The protocol generates session messages by randomizing the secret information of tags and then Hashing them, and adopts secondary mutual authentication between tags and readers, which improves the security of the protocol.The protocol ensures the confidential transmission and integrity of session information in the authentication process through Hash operation. The randomization of each session message sent by the tag side ensures the freshness of the message, and the update of the system secret information ensures the forward security of the protocol. RFID authentication protocol can not only resist attacks such as eavesdropping, tracking, replay, and de-synchronization, but also meet the security and privacy protection needs of RFID systems.

Keywords：RFID system;authentication protocol;security;privacy;Hash function;radio frequency tag;confidentiality;integrity; pseudo random number

随着物联网和智能感知技术的发展，射频识别（RFID）技术因具有非接触、成本低等优点而被广泛应用于物品识别、定位追踪和信息收集等领域[1]。然而，因 RFID 标签具有计算存储资源有限、开放的无线通信信道等特点，使 RFID 系统的隐私保护和安全性成为制约其应用的障碍和瓶颈。由于当前 RFID 产品大多采用价格低廉的被动式标签，这类标签计算、存储资源有限，难以支持复杂的加密操作。在这种情况下，RFID 系统的隐私保护和安全问题只能采用轻量级的加密和认证方法来解决。研究者采用哈希、循环冗余校验、伪随机数生成等轻量级函数，结合位运算提出了多种 RFID 加密和认证协议，但均存在一定的不足之处[2-3]。

文献[4]采用二进制字符串的奇偶分离、取反、异或等操作，提出了一个安全的轻量级认证协议 SelLAP。文献[5]指出该协议存在秘密泄露隐患，易受到跟踪攻击。文献[6]利用哈希函数的单向性及随机性实现了抗去同步化的 RFID 双向认证协议，但该协议无法满足标签位置隐私信息的保护，攻击者通过监听可以定位标签的位置。同时，因标签先于阅读器更新密钥信息，导致系统无法抵抗去同步化攻击。文献[7]采用哈希函数和异或运算提出一种基于

伪 ID 的双向认证协议，该协议假设阅读器事先知道要认证标签的伪名 ID，但通常阅读器无法事先获取该信息。同时，标签连续多次接收到阅读器的询问后会返回相同的伪名 ID 给阅读器，从而泄露标签位置信息，易于受到跟踪攻击。文献[8]提出了一种 RFID 跨层认证协议，能够抵抗跟踪、假冒和拒绝服务等攻击。但该协议同时使用哈希链和模幂运算，计算开销较大。文献[9]提出了基于云计算的 RFID 双向认证协议，以置换和旋转运算代替哈希函数，以时间戳代替伪随机函数，减少了计算开销。文献[10]提出一个基于 CRC(Cyclic Redundancy Check)、PUF(Physical Unclonable Functions)和位运算的认证协议，但无法抵抗跟踪攻击。文献[11]采用哈希、伪随机和异或运算实现了双向认证协议，但因会话仅采用异或运算，比较简单，加密强度有限。当阅读器反复询问标签时，标签均回复相同的伪名，从而暴漏位置信息，易于受到跟踪攻击。文献[12]提出一种基于动态共享密钥的移动 RFID 双向认证协议，该协议中的标签不能对阅读器的合法性进行验证，攻击者可以假冒合法阅读器查询标签，即该协议无法抵抗假冒和跟踪攻击[13]。文献[14]提出基于伪随机数和位运算的认证协议，并论证其满足各种安全性。通过分析，该协议每轮认证所使用的标签密钥 k 固定不变。若敌手非法获得了标签密钥 k，则可以通过简单的异或运算获得每次认证所产生的随机数 x 和 y，进而可以解密以前认证过程产生的会话信息。因而该认证协议不满足前向安全性。文献[15]提出了轻权认证协议 Slap，但难以抵抗去同步化攻击。文献[16]同时使用哈希、非对称加密、物理不可克隆等函数研究认证方法，但在服务器更新标签标识时没有保留旧的标签标识信息，易导致去同步攻击。每次认证结束后均没有更新密钥，认证协议不具有前向安全性。阅读器和标签必须保证时间同步，否则导致协议无法正常工作。非对称加密函数过于复杂，需要一定的计算能力支撑，难以应用于被动式标签。

针对上述认证协议中存在的问题，本文采用哈希函数和随机数产生函数以及简单位运算提出一种简单、实用、安全的轻权认证协议，并通过可证明安全理论分析证明协议的安全性。

1 RFID 系统的组成及其安全性描述

RFID 系统包括射频标签、阅读器和后端服务器 3 个组成部分，如图 1 所示。标签由收发天线、逻辑控制电路、存储器等部分组成，存储器中存有该芯片的唯一标识码。阅读器具有一定计算和存储能力，其以射频信号形式读取标签中的数据，并与后端服务器进行信息交换。后端服务器存储标签相关的详细数据，与阅读器协同完成标签的认证和相关的信息处理工作。

对于一个 RFID 系统，标签是决定系统功能和特点的重要组成部分，包括主动式标签和被动式标签两种。其中，被动式标签是一种无源标签，只能在较小的范围内发送和接收信息。但因其具有简单、成本低等特点广泛应用于各领域。

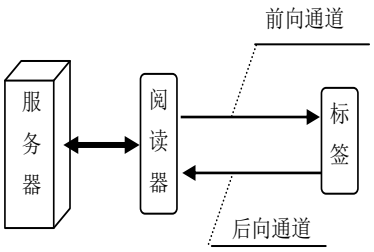

图 1 RFID 系统的组成

Figure 1. The component diagram of RFID systems

在安全方面，RFID 系统的安全威胁包括窃听、伪装、跟踪、重放、去同步化、前向安全性等[17-18]。窃听指敌手利用 RFID 系统开放的无线通信信道截获标签与阅读器间的会话，通过分析会话进一步获得标签的标识等秘密信息。跟踪攻击意味敌手通过窃听等手段能够识别出会话信息的来源标签，进而跟踪标签。在认证过程中，若标签反复发出同样的信息，则易发生跟踪攻击。重放指敌手重新发送以前截获的会话，进而伪装成合法标签获得阅读器的信任和认证，达到非法获取有用信息的目的。去同步化攻击是因为标签端和服务器端存储的密钥等秘密信息没有同步更新，导致标签端和服务器端存储的密钥等信息不一致，进而破坏认证过程的正常进行。前向安全性指敌手在获得当前密钥等秘密信息的情况下，仍无法揭示以前的会话信息。

RFID 系统涉及的用户包括诚实用户、半诚实用户和恶意用户。半诚实用户指通过监听等手段获取系统信息，通过分析获取系统的位置等隐私信息跟踪标签，但不对认证过程造成影响。恶意用户不但可以监听系统信息，也可以通过篡改、重放、暴力破解等手段破坏系统的认证过程。

为了确保 RFID 系统认证协议的安全强度，假设系统所面临的用户都是恶意用户。对于 RFID 系统的 3 个组成部分，阅读器与后端服务器的计算和存储资源较为丰富，支持高强度的加密操作，因而假设其之间的通信安全，其被看作一个整体，以下简称为阅读器。标签的计算、存储资源有限，仅能完成哈希、随机数生成、位运算等轻量级操作和运算。阅读器和标签间通过不安全的无线开放信道进行通信，易引起 RFID 系统的安全问题和隐私泄露。

2 基于哈希函数的双向增强型认证协议

本文通过哈希、随机数生成等轻量级函数以及简单位运算提出一个具有增强安全性的轻量级双向认证协议，协议使用的符号如表 1 所示。

表 1 认证协议使用的各种符号

Table 1. All used symbols in the proposed authentication protocol

符号	含义
ID	标签的唯一标识符
curID	当前轮认证过程中阅读器使用的标签标识符
oldID	上一轮认证过程中阅读器使用的标签标识符
k	阅读器和标签的共享密钥
cur$k$	当前轮认证过程中阅读器和标签的共享密钥
old$k$	上一轮认证过程中阅读器和标签的共享密钥
d	标签标识、密钥等秘密信息的长度
$\mathrm{hash}(\ )$	哈希函数
$\mathrm{prng}(\ )$	随机数生成函数
r,s	阅读器和标签生成的随机数
$\|\|$	连接运算符
$\oplus$	异或运算符

假设标签端存储其唯一标识符 ID 以及标签与阅读器的共享密钥 k，假设其长度均为 d 比特。阅读器存储 curID、oldID、cur$k$、old$k$ 等信息。其中，curID、oldID 是当前轮和上轮认证所使用的 ID，cur$k$、old$k$ 是当前轮和上轮认证所使用的共享密钥。上轮认证参数的设置是为了抵抗去同步化攻击。初始化时，curID、oldID 与标签的标识符相同 ID，cur$k$、old$k$ 与标签的密钥 k 相同。标签和阅读器共享哈希函数 hash( )和随机数生成函数 prng( )。通过 hash( )单向性处理会话信息，确保会话信息传输的完整性以及保密性。通过 prng( )生成随机数处理会话信息，保证会话的新鲜性，防止跟踪和重放攻击。哈希函数 hash( )和随机数生成函数 prng( )定义如式（1）~式（2）所示。

$$\mathrm{hash}(\ ):\{0,1\}^{*}\rightarrow\{0,1\}^{d} \tag{1}$$

$$\mathrm{prng}(\ ):\{0,1\}^{d}\rightarrow\{0,1\}^{d} \tag{2}$$

协议的认证过程如图 2 所示，具体描述如下所示：

步骤 1 阅读器生成一个随机数 r，并以消息形式广播给附近的标签，从而启动新一轮认证。

步骤 2 标签接收消息 r 后，调用 $prng(\ )$ 生成一个随机数 s=prng( )，然后生成 A

$$A=hash(ID\oplus k\oplus s) \tag{3}$$

标签形成消息 $A||s$ 发送给阅读器。

步骤 3 阅读器接收到消息 $A||s$ 后，从服务器的数据库中依次取出记录各个标签秘密信息的参数对 $(\mathrm{curID},\mathrm{curk})$ 和 $(\mathrm{oldID},\mathrm{old}k)$，并分别赋给 (ID,k)，计算 $\mathrm{hash}(ID\oplus k\oplus s)$。若存在一组 (ID,k)，使 $\mathrm{hash}(\mathrm{ID}\oplus k\oplus s)==A$ 成立，则阅读器完成了对标签的初次认证。否则协议失败，退出本次认证。

完成对标签的初次认证后，阅读器调用哈希函数生成消息 B，并发送给标签。

$$B=\mathrm{hash}(\mathrm{ID}\oplus k\oplus r) \tag{4}$$

步骤 4 标签接收到 B，使用本地存储的 ID 和 k，计算 $\mathrm{hash}(\mathrm{ID}\oplus k\oplus r)$，并判断 $\mathrm{hash}(ID\oplus k\oplus r)==B$ 是否成立。若不成立，则退出本次认证。若成立，则标签完成了对阅读器的初次认证。标签生成消息 C，并发送 C 给阅读器。

$$C=\mathrm{hash}(\mathrm{ID}\oplus k\oplus s\oplus r) \tag{5}$$

步骤 5 阅读器接收到 C 后，利用步骤 3 确定的本地秘密参数 ID 和 k 计算 $\mathrm{hash}(ID\oplus k\oplus r)$，并判断 $\mathrm{hash}(ID\oplus k\oplus r)==C$ 是否成立。若不成立，则退出本次认证。若成立，则完成了对标签的第二次认证。

然后阅读器开始更新本地秘密参数，具体如下所示：

若 ID == curID，则

$$\mathrm{oldID}==\mathrm{curID} \tag{6}$$

$$\mathrm{curID}=\mathrm{prng}(\mathrm{curID}\oplus s\oplus r) \tag{7}$$

$$\mathrm{old}k==\mathrm{cur}k \tag{8}$$

$$\mathrm{cur}k=\mathrm{prng}(\mathrm{cur}k\oplus s\oplus r) \tag{9}$$

若 ID == oldID，则

$$\mathrm{curID}=\mathrm{prng}(\mathrm{oldID}\oplus s\oplus r) \tag{10}$$

$$\mathrm{cur}k=\mathrm{prng}(\mathrm{old}k\oplus s\oplus r) \tag{11}$$

阅读器生成消息 D，并发送给标签。

$$D=\mathrm{hash}((\mathrm{ID}\oplus r)\|(k\oplus s)) \tag{12}$$

步骤 6 标签接收到 D 后，调用哈希函数，使用本地参数计算 $\mathrm{hash}((\mathrm{ID}\oplus r)\|(k\oplus s))$，并判断 $\mathrm{hash}((\mathrm{ID}\oplus r)\|(k\oplus s))==D$ 是否成立。若不成立，则退出本次认证。若成立，则标签完成了对阅读器的第二次认证，并更新本地秘密参数，即

$$\mathrm{ID}=\mathrm{prng}(\mathrm{ID}\oplus s\oplus r) \tag{13}$$

$$k=\mathrm{prng}(k\oplus s\oplus r) \tag{14}$$

至此，系统完成了阅读器与标签间的双向认证。其中，步骤 3 和步骤 5、步骤 4 和步骤 6 分别完成了阅读器对标签、标签对阅读器的两次认证。

3 认证协议的安全性分析

对于 RFID 系统，通常假设敌手是一个概率多项式时间算法，其能够截获、窃听、跟踪、重放、篡改、阻断协议的每个会话。如果敌手能够从截获的会话中通过暴力破解等手段解密系统的秘密，或者能够区分两个不同的标签，则认为敌手赢得了这场游戏。假设敌手获胜的概率为 σ。

定义 1 敌手可以连续发起对哈希函数 $\mathrm{hash}(\ )$ 和随机数生成函数 $\mathrm{prng}(\ )$ 的随机查询。因 $\mathrm{hash}(\ )$ 和 $\mathrm{prng}(\ )$ 的输出均为 d 比特，根据这两种函数的性质可知，敌手成功猜测到正确输出的概率为 $\sigma\le 2^{-d}$。

定义 2 假设敌手是一个概率多项式时间算法，如果其不能以不可忽略的概率揭示 RFID 系统的秘密信息，则认为协议隐私安全。

定义 3 假设敌手是一个概率多项式时间算法，

其能够区分两个不同标签的概率 $\sigma = 2\Pr[\mathrm{ID} = \mathrm{ID}'] - 1$，其中 $\mathrm{ID} \neq \mathrm{ID}'$。如果 σ 可忽略，则认为协议具有不可区分安全性。

定义 4 敌手是一个概率多项式时间算法，如果其从当前密钥能够猜测出更新前的密钥，进而解密以前轮会话的概率可忽略，则认为协议满足前向安全性。

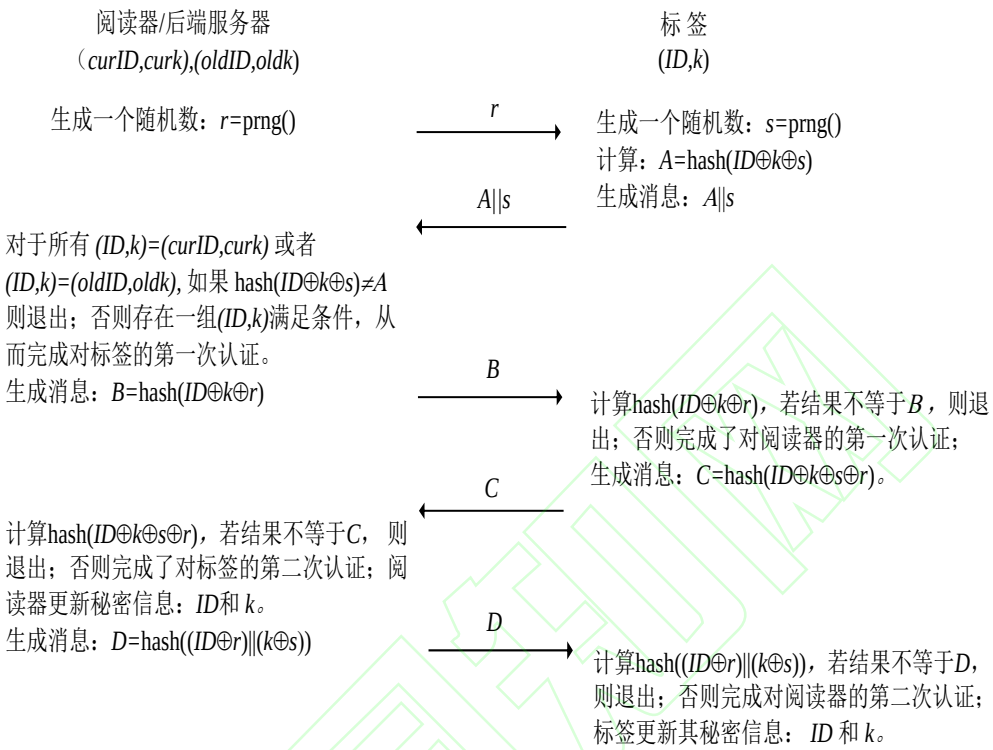

图 2 协议的认证过程

Figure 2. The authentication procedure of the proposed protocol

对于本文认证协议，消息 A、B、C、D 中包括了系统的密钥等秘密信息。由定义 1 可知，敌手可以通过随机查询 $\mathrm{hash}(\,)$ 和 $\mathrm{prng}(\,)$ 猜测系统的秘密信息。假设猜测正确的概率是 σ，根据这些特殊函数的性质有 $\sigma \le 2^{-d}$。假设 $d \ge 32$，则 σ 可忽略，所以协议隐私安全。

对于一个具有概率多项时间算法的敌手，其可伪装成合法阅读器，多次向标签发起认证请求，可以截获多次会话，判断获得的应答消息是否来自同一个标签，进而区分和跟踪标签。假设敌手截获了两个不同认证过程中来自标签的消息 A（或者 C），其中包括标签的标识符 ID 和 ID'。由于每轮认证过程标签均产生一个新的随机数，显然相邻两轮认证的消息 A（或者 C）不同。如果敌手能够区分这两个标签是否是同一个标签，其获得成功的概率定义为

$$\Pr[\mathrm{ID} = \mathrm{ID}'] = 1/2 + \varepsilon \tag{15}$$

式中，ε 为敌手同时猜测出 ID 和 ID' 的概率。根据定义 1 以及哈希函数的单向性，有 $\varepsilon \le 2^{-d} \times 2^{-d}$。若 $d \ge 32$，有 $\varepsilon \le 2^{-64}$。由定义 3 可知，有 $\sigma = 2\Pr[\mathrm{ID} = \mathrm{ID}'] - 1 = 2\varepsilon \le 2^{-63}$，$\sigma$ 可忽略，敌手无法区分两个标签。故协议具有不可区分安全性，可以抵抗跟踪攻击。

协议具有前向安全性。假设敌手可以截获协议中的所有消息，其中仅消息 A、B、C、D 包含标签秘密 k 和 ID。设敌手从每个消息成功猜测密钥的概率是 $\varepsilon 1$。因为上述每个消息均包括两个秘密信息的组合，故有 $\varepsilon 1 \le 2^{-d} \times 2^{-d}$。每成功运行一次协议，均需更新密钥信息，即 $k = \mathrm{prng}(k \oplus s \oplus r)$。如果敌手要得到更新前的密钥，其需要发起对 $\mathrm{prng}(\,)$ 的随机查询。敌手从中猜测出更新前密钥的概率是 $\varepsilon 2$，显然 $\varepsilon 2 \le 2^{-d}$。具体分为两种情况：

1）敌手攻破了标签，获得了当前密钥 k。敌手通过随机查询 $\mathrm{prng}(\,)$ 从当前密钥成功猜测出更新前密钥的概率 $\sigma 1 = \varepsilon 2 \le 2^{-d}$。

2）敌手不知道标签的当前密钥，只能从截获的消息 A、B、C、D 中通过随机查询 $\mathrm{hash}(\,)$ 猜测更新前的密钥，其猜测成功的概率 $\sigma 2 = 4\varepsilon 1 \le 4 \times 2^{-2d} = 2^{2-2d}$。

无论是上述哪种情况，当 $d \ge 32$ 时，$\sigma 1$ 和 $\sigma 2$

均可忽略。即敌手无法从截获的当前会话中推测出以前认证轮的密钥，所以本文协议具有前向安全性。

去同步化攻击是认证协议经常受到的另一种攻击。此时，敌手通过阻断或者篡改阅读器和标签间的会话，使阅读器和标签上存储的秘密信息不能同步更新，从而导致后续认证过程失败。秘密信息包括标签密钥 k 和标识 ID，这些信息的更新发生在步骤 5 和步骤 6。敌手的攻击有两种可能：1）敌手阻断步骤 4 和步骤 5 中消息 C 、 D 的发送。此时，阅读器和标签中的密钥 k 和标识 ID 均没有更新，仍保持一致，故不会发生去同步化攻击。2）敌手仅阻断步骤 5 消息 D 的传输，此时阅读器保留当前轮秘密消息到 $(\text{oldID},\text{old}k)$ 中，然后才进行密钥的更新，即生成新的 $(\text{curID},\text{cur}k)$；但标签没有接收到消息 D，因而没有更新其秘密信息 (ID,k)。此时，标签端的 (ID,k) 与阅读器端的 $(\text{oldID},\text{old}k)$ 相同，仍可以保证协议正常运行，从而有效抵御去同步攻击的发生。

在其他安全性方面，协议各实体间传输的含有秘密的消息均经过哈希函数处理，敌手可以窃听这些消息。但因哈希函数具有单向性，敌手无法解密，从而防止了秘密泄露，确保了协议的匿名性。由于敌手无法获得标签的秘密信息，因而其无法假冒合法的标签和阅读器。对于每次认证，阅读器和标签均生成一个新的随机数去随机化认证过程中交换的会话。尽管一定时间后敌手可以重放截获的会话，但标签又产生了新的随机数，重放的会话不会得到标签的响应，故认证协议可以抵抗重放攻击。

表 2 与其他典型认证协议的比较

Table 2. The comparison with other typical authentication protocols

协议	匿名性	假冒	跟踪	重放攻击	去同步攻击	前向安全性
文献[6]	×	√	×	√	×	√
文献[7]	×	√	×	√	×	√
文献[10]	×	√	×	√	√	√
文献[11]	×	√	×	√	√	√
文献[12]	×	×	×	√	×	√
文献[14]	√	√	×	√	√	×
文献[16]	√	√	√	√	×	×
本文	√	√	√	√	√	√

表 3 各协议标签端调用的函数及其资源消耗情况

Table 3. The called functions and resource using of some authentication protocols in tag

协议	标签端 调用函数	标签端 计算量	标签端 存储量	标签-阅读器间 通信量
文献[6]	hash()	3hash()	3d	7d
文献[7]	prng()	3prng()	3d	7d
文献[10]	CRC()+PUF()	11CRC()+2PUF()	5d	5d
文献[11]	hash()+prng()	5hash()+1prng()	3d	7d
文献[12]	hash()+prng()	1hash()+4prng()	3d	5d
文献[14]	prng()	1prng()	2d	7d
文献[16]	E()+F()+PUF()	5E()+3F()+2PUF()	4d	10d
本文	hash()+prng()	4hash()+3prng()	2d	6d

表 2 给出了本文协议与其他几个典型认证协议安全性能的对比情况。多数协议无法抵抗跟踪攻击；敌手通过反复发送询问消息给标签，而标签均回复相同的消息（或者消息中包括固定不变的部分信息），从而易实现对标签的跟踪。而且这些协议采用一次认证，安全强度有限。同时，文献[6]、文献[7]、文献[12]和文献[16]不能抵抗去同步攻击，文献[14]和文献[16]不具备前向安全性。本文所提协议可以抵抗假冒、跟踪、重放、去同步等攻击，具有较好的匿名性和前向安全性，其安全性能明显优于其他几个典型的认证协议。表 3 给出各协议在标签端调用的函数种类和次数以及发生的通信量。其中，CRC( )为循环冗余校验函数，PUF( ) 为物理不可克隆函数，F( ) 为非线性移位寄存器，E( ) 为非对称加密函数，函数前面的数字表示调用该函数的次数，d 为密钥长度，其前面的数字分别表示标签端的存储量以及与阅读器间的通信量。在标签端的存储、计算、通信量方面，本文协议与其他几个协议没有明显差别，但在隐私保护和安全性能上明显优于其他协议。

4 结束语

针对目前广泛应用的低值 RFID 标签，本文对 RFID 系统的安全性和隐私保护方法进行研究，提出了一种基于哈希函数的轻权双向认证协议。通过可证明安全理论进行了分析，结果表明本文提出的 RFID 轻权认证协议具有前向安全性，能够抵抗窃听、跟踪、重放、假冒、去同步化等攻击。该协议

通过随机化标签的秘密信息再哈希的方法生成会话消息，同时采用二次双向认证确保认证协议具有更强的安全性，使 RFID 系统能够更好地满足各应用领域的安全需求。

参考文献

[1] 王鸽,惠维,丁菡.一种基于无源射频技术的用户步态识别及认证方法[J].电子科技,2020,33(6):1-7.
Wang Ge,Xi Wei,Ding Han.Human gait recognition and identification with passive RFID[J].Electronic Science and Technoligy,2020,33(6):1-7.

[2] 苏庆,李倩,彭家进,等.基于假名标识的加密ＲFID 系统无线密钥生成协议[J].计算机工程,2017,43(8):173-177.
Su Qing,Li Qian,Peng Jiajin,et al.Wireless key generation protocol for encrypted RFID system based on pseudonym logo[J].Computer Engineering,2017,43(8):173-177.

[3] Alaauldin I,Gokhan D.Review of different classes of RFID authentication protocols[J].Wireless Neworks,2019,25(3):961-974.

[4] Seyed F A,Hamid M.SecLAP:Secure and lightweight RFID authentication protocol for medical IoT[J].Future Generation Computer Systems,2019,101(12):621-634.

[5] Masoumeh S,Samad R,Ygal B.IoT in medical and pharmaceutical:Designing lightweight RFID security protocols for ensuring supply chain integrity[J].Computer Networks,2020,181(11):1-18.

[6] 赵太飞,尹航,赵思婷.抗去同步化的高效 RFID 双向认证协议[J].计算机工程与应用,2019,55(12):90-96.
Zhao Taifei,Yin Hang,Zhao Siting.Anti-desynchronization and efficient RFID mutual authentication protocol[J].Computer Engineering and Applications,2019,55(12):90-96.

[7] 邹同浩.一种新型的射频识别系统双向认证协议[J].控制工程,2020,27(11):2044-2049.
ZOU Tonghao.A new mutual authentication protocol for RFID system[J].Control Engineering of China,2020,27(11):2044-2049.

[8] Hoorin P,Heejun R,Wonjun L,et al.A collision-exploitative RFID authentication protocol based on cross-layer approach[J].IEEE Internet of Things Journal,2020,7(4):3571-3585.

[9] Kai F A,Qi L A.Cloud-based lightweight secure RFID mutual authentication protocol in IoT[J].Information Sciences,2020,527(7):329-340.

[10] 柳毅,陈添笑,洪洲.抗同步化攻击的轻量级 RFID 双向认证协议[J].计算机应用研究,2020,37(4):1136-1139.
Liu Yi,Chen Tianxiao,Hong Zhou.Lightweight RFID mutual authentication protocol with anti-synchronization attack[J].Application Research of Computers,2020,37(4):1136-1139.

[11] 陈惠红,陈志刚.基于伪 ID 的改进的双向认证协议[J].控制工程,2021,28(10):2038-2044.
Chen Huihong,Chen Zhigang.An improved pseudo ID-based mutual authentication protocol[J].Control Engineering of China,2021,28(10):2038-2044.

[12] 王国伟,贾宗璞,彭维平.基于动态共享密钥的移动 RFID 双向认证协议[J].电子学报,2017,45(3):612-618.
Wang Guowei,Jia Zongpu,Peng Weiping.A mutual authentication protocol of mobile RFID based on dynamic shared-key[J].Aata Eletronica Sinica,2017,45(3):612-618.

[13] 王艳,雷雪梅,高通.基于变模与自更新密钥矩阵的高效 RFID 安全认证协议[J].密码学报,2022,9(2):210-222.
Wang Yan,Lei Xuemei,Gao Tong.Efficient RFID security authentication protocol based on variable modulus and self-updating key matrix[J].Journal of Cryptologic Research,2022,9(2):210-222.

[14] 郝伟伟,吕磊.基于伪随机数发生器的移动 RFID 双向认证算法[J].计算机技术与发展,2022,32(5):93-98.
Hao Weiwei,Lv Lei.Mobile RFID bidirectional authentication algorithm based on pseudo random number generator[J].Computer Technology and Development,2022,32(5):93-98.

[15] Luo H G,Wen G G,Su J,et al.Slap:Succinct and lightweight authentication protocol for low-cost rfid system[J].Wireless Network,2018,24(1):69-78.

[16] Bhatia K,Pandey S,Singh V,et al.Hash and physical unclonable function based mutual authentication mechanism[J].Sensors,2023,23(14):1-15.

[17] Alireza A K,Mahdi S,Mohammad R Y.Reconstructing a lightweight security protocol in the radio-frequency identification systems[J].IET Computers and Digital Techniques,2023,17(6):209-223.

[18] Gao M,Lu Y B.URAP:A new ultra-lightweight RFID authentication protocol in passive RFID system[J].Journal of Supercomputing,2022,78(8):10893-10905.

收稿日期：2023-08-04

基金项目：
科技部科技创新 2030-新一代人工智能重大项目(2020AAA0109300)
The Scientific and Technological Innovation 2030-Major Project of New Generation Artificial Intelligence(2020AAA0109300)

作者简介：
史志才（1964-），男，博士，教授。研究方向：网络安全、隐私计算等。
Shi Zhicai(1964-),male,doctor,professor.Research direction: Network security,privacy computing,etc.