



文章编号:1001-9081(2019)03-0774-05

DOI:10.11772/j.issn.1001-9081.2018081648

可扩展及可证安全的射频识别认证协议

史志才*, 王益涵, 张晓梅, 陈珊珊, 陈计伟

(上海工程技术大学 电子电气工程学院, 上海 201620)

(*通信作者电子邮箱 szc1964@163.com)

摘要:针对目前广泛应用的被动式射频识别(RFID)标签中的计算、存储资源有限,导致RFID认证协议的安全和隐私保护,特别是可扩展性一直没有得到很好解决的问题,提出一种基于哈希函数、可证安全的轻权认证协议。该协议通过哈希运算和随机化等操作确保认证过程中会话信息的保密传输和隐私性;在认证过程中,标签的身份信息通过伪名进行确认,其真实身份没有透露给阅读器等不信任实体;后端服务器进行身份确认仅需进行一次哈希运算,通过标识符构造哈希表可使身份信息查找时间为常数;每次认证后,标签的秘密信息和伪名等均进行更新,从而确保协议的前向安全性。分析证实,该RFID轻权认证协议具有很好的可扩展性、匿名性和前向安全性,能够抵抗窃听、追踪、重放、去同步化等攻击,而且标签仅需提供哈希运算和伪随机数生成操作,非常适合应用于低成本的RFID系统。

关键词:认证协议; 可扩展性; 安全性; 隐私保护; 哈希函数

中图分类号: TP393.08 **文献标志码:**A

Proviable radio frequency identification authentication protocol with scalability

SHI Zhicai*, WANG Yihan, ZHANG Xiaomei, CHEN Shanshan, CHEN Jiwei

(School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

Abstract: The popular Radio Frequency IDentification (RFID) tags are some passive ones and they only have very limited computing and memory resources, which makes it difficult to solve the security, privacy and scalability problems of RFID authentication protocols. Based on Hash function, a security-provable lightweight authentication protocol was proposed. The protocol ensures the confidentiality and privacy of the sessions during the authentication process by Hashing and randomizing. Firstly, the identity of a tag was confirmed by its pseudonym and was preserved from leaking to any untrusted entity such as a reader. Secondly, only one Hashing computation was needed to confirm a tag's identity in the backend server, and the searching time to the tag's identity was limited to a constant by using the identifier to construct a Hash table. Finally, after each authentication, the secrecy and pseudonym of the tag were updated to ensure forward security of the protocol. It is proved that the proposed protocol satisfies scalability, forward security and anonymity demands and can prevent eavesdropping, tracing attack, replay attack and de-synchronization attack. The protocol only needs Hash function and pseudorandom generating operation for the tag, therefore it is very suitable to low-cost RFID systems.

Key words: authentication protocol; scalability; security; privacy preserving; Hash function

0 引言

随着物联网的普及,射频识别(Radio Frequency IDentification, RFID)技术作为重要感知手段而得到普遍关注,已经广泛应用于金融、交通运输、物流等领域^[1];然而,因RFID标签的资源有限、使用开放的无线通信方式等特点,使得很难解决RFID系统的隐私保护和安全问题。虽然目前有物理方法可以保护RFID系统的隐私,但研究结果表明通过软件实现的加密和认证技术是实现隐私保护的较灵活、较有效的方法。由于处于主流的被动式标签计算、存储资源有限,难以支持高强度加密运算。在这种资源受限的特殊条件下,安全、高效、低资源消耗的RFID加密和认证方法的研究就成为了信息安全领域关注的热点。目前已提出多种RFID加密和认证协议,但均被证明存在一定的缺陷。此外,为了实现标

签身份的匿名传输,绝大部分认证协议均将哈希后的标签标识信息传递给后端服务器;为了确认标签的身份,后端服务器不得不哈希本地存储的每个标签身份信息,需要哈希的次数与标签的数量呈线性增长,导致系统的可扩展性差。本文针对上述缺陷,采用哈希函数和伪随机数产生函数以及简单位运算提出一种可证安全的轻权认证协议;该协议采用标签伪名和密钥的随机化及更新来保证协议的可扩展性、匿名性和前向安全性,最后通过分析证明了协议的安全性。

1 RFID系统及其安全和隐私保护

一个RFID系统一般包括三部分:射频标签、读写器和后端服务器,如图1所示。标签是一块具有天线和少量存储计算资源的硅片。读写器是一个以射频信号形式发送和接收信息的设备,它对标签中存储的信息进行读写,与后端服务器进

收稿日期:2018-08-09;修回日期:2018-10-03;录用日期:2018-10-22。

作者简介:史志才(1964—),男,吉林磐石人,教授,博士,CCF高级会员,主要研究方向:信息安全、隐私保护; 王益涵(1981—),男,上海人,讲师,硕士,主要研究方向:信息安全; 张晓梅(1981—),女,湖北荆门人,讲师,博士,主要研究方向:传感器网络安全; 陈珊珊(1995—),女,安徽六安人,硕士研究生,主要研究方向:室内定位; 陈计伟(1992—),男,江苏徐州人,硕士研究生,主要研究方向:网络安全。



行通信。后端服务器中存储与标签相关的具体信息,负责完成身份认证、数据处理等工作。



图1 RFID系统的组成
Fig. 1 Components of RFID system

对于一个RFID系统,标签是决定系统功能和特点的一个关键组件。目前有两种标签:主动标签和被动标签。主动标签内置有供电电池,能够在较大的范围内通信;被动标签是一种无源标签,它内部没有供电电池,需要通过读写器发射的射频信号感应出供电电压,因而只能在较小的范围内通信。由此可见,对于被动标签,由读写器到标签的前向通道和由标签到读写器的后向通道是不对称的;这两个无线通信信道是开放的、不安全的,RFID系统的安全问题和隐私泄露大都是由这些不安全的信道引起的。RFID系统的这些安全问题常采用加密认证协议来解决。理想的加密认证协议能满足匿名性、保密性和不可区分性,并具有前向安全性和可扩展性,能够抵抗窃听、跟踪、重放、去同步等攻击。

2 RFID 轻权认证协议

从本世纪初,国内外就开始关注轻权加密和认证方法的研究,已有很多研究成果。目前,许多RFID认证协议都采用Hash函数,经典的有Hash-Lock协议、Hash-chain协议等。

Weis等^[2]最先提出了Hash-Lock协议。该协议使用伪名metaID代替标签的真实ID来确保其隐私。但是在认证过程中,协议使用明文传输固定不变的metaID,攻击者很容易跟踪标签。为了克服Hash-Lock协议的缺点,Weis等对Hash-Lock协议进行了改进,提出了随机Hash-Lock协议;该协议使用了伪随机数发生器来随机化标签和阅读器间的会话信息,但是最终还是以明文形式传输标签ID;攻击者很容易窃听和获取标签的标识信息,进而跟踪、伪造标签,进行重放攻击。

不同于Hash-Lock协议,Ohkubo等^[3]使用两个Hash函数: $h()$ 和 $g()$ 参与认证,提出了Hash-chain协议。该协议使用Hash函数更新密钥以获得前向安全性,但是它难以抵抗欺骗和重放攻击,而且它只实现对标签的单向认证。Lee等^[4]使用挑战-响应机制提出了认证协议(Low-Cost RFID Authentication Protocol, LCAP);该协议试图通过更新标签ID以提供前向安全性,但因更新操作简单,只要破译当前ID和截获各次认证的随机数,通过简单的异或运算就可以获得以前的ID;所以该协议不能确保前向安全性,也不能抵抗跟踪攻击。Cho等^[5]也提出了一个基于Hash函数的认证协议,然而,Kim^[6]指出这个协议对于拒绝服务攻击非常脆弱;Khadr^[7]指出敌手通过篡改协议会话,可以完成去同步化攻击,指出该协议不能确保前向安全性。

Ha等^[8]提出一个基于Hash函数的RFID认证协议,并证明能保证前向安全性。然而,Sun等^[9]发现敌手通过观察以前失败的会话就可以跟踪标签,协议实际上并不能提供前向安全性。

Liu等^[10]基于Hash函数提出了标签、阅读器和后端服务器的三方认证协议,但是在每次认证过程中,标签和阅读器多次调用Hash函数,计算开销较大,而且协议的可扩展性差。

Dehkordi等^[11]对Cho等提出的协议进行了分析,指出他们的协议无法抵抗拒绝服务攻击、流量分析攻击和假冒攻击,并进行了改进;但认证标签的计算复杂性与标签的数量成正比,系统的扩展性差。Abidin^[12]基于哈希函数和椭圆曲线函数提出了RFID的认证协议,协议总共使用11次哈希、6次点积、6次椭圆曲线相关运算,标签的计算负担较重。

Habibi等^[13]分析了Duc等提出的两个认证协议,指出这些协议易于发生跟踪攻击和去同步攻击,也不满足前向安全性。Gope等^[14]在对以往协议分析的基础上提出了一个能够抵抗跟踪攻击的RFID认证协议,提供了匿名性和前向安全性,但标签端的计算负担较重。李松等^[15]提出了基于PUF的认证协议,但标签端使用了哈希、不可克隆、伪随机数生成等多个函数,计算负担较重;而且每次认证后秘密信息没有更新,难以确保前向安全性。

还有很多类似的轻权认证协议,这些协议大都不满足前向安全性,可扩展性差。这类协议的主要特征是采用Hash函数来保证会话信息的完整性和隐私性,通过伪随机数产生器保证会话信息的新鲜性,但是标签端的计算不能过于复杂,且还要保证一定的安全强度,这是一个非常矛盾的问题,有时只能采取折中方案,即设计一种即具有一定安全强度而且计算、存储消耗适中的认证协议。

3 可扩展的RFID匿名认证协议

RFID系统的安全威胁有窃听、跟踪、重放、去同步、前向安全性等,这些安全威胁通常假设来自一个概率多项式时间算法的敌手;这个敌手能够窃听、截获、篡改、跟踪、重放协议的每个会话,进而达到攻击RFID系统、使认证协议失效,最终获取系统秘密信息的目的。下面通过哈希函数、伪随机数生成函数以及异或运算处理标签与后端服务器/阅读器间的会话,同时通过随机化和更新密钥、标签伪名等手段,防止上述攻击的发生,同时保证系统的可扩展性。

假设后端服务器存储各个标签的 ID 、 pID 、 $oldpID$ 、 $k1$ 、 $oldk1$ 、 $k2$ 、 $oldk2$ 、 k 等信息,它们的长度均为 d 比特;其中 ID 是标签的标识符,用于唯一地标识一个标签; pID 是标签的伪名,用来替代 ID 在信道上传输,以防止隐私泄露, pID 的初始值为 ID 的哈希值; $oldpID$ 为上次成功认证时 pID 的值; $k1$ 和 $k2$ 为当前的密钥值,而 $oldk1$ 和 $oldk2$ 为上次成功认证时 $k1$ 和 $k2$ 的值。保留上次成功认证时的密钥值和伪名是为了避免去同步攻击;每次认证成功后,都要对 pID 、 $k1$ 、 $k2$ 进行更新以确保前向安全性;更新 pID 的另一个目的是为了防止泄漏标签的隐私。 k 为所有标签和后端服务器共享的公共密钥,用来确认各个标签的身份。认证协议使用的符号如表1所示。

标签端存储其 ID 、 pID 、 $k1$ 、 $k2$ 、 k 等信息。标签和后端服务器共享哈希函数 $h(): \{0,1\}^* \rightarrow \{0,1\}^d$ 和伪随机数生成函数 $prng(): \{0,1\}^* \rightarrow \{0,1\}^d$ 。这两个函数的作用是:1)通过哈希函数 $h()$ 的单向性处理会话信息,以确保会话信息的完



整性以及秘密传输。2) 通过伪随机数生成函数 $prng()$ 产生伪随机数去随机化会话信息以防止跟踪和重放攻击。 $h()$ 和 $prng()$ 均为输出为 d 比特的函数。认证过程如图 2 所示, 具体描述如下:

步骤 1 后端服务器调用 $prng()$ 生成一个随机数 r , 连同系统目前的时间戳 t , 形成消息 $r \parallel t$, 经阅读器转发给标签, 从而启动一次认证过程。

步骤 2 标签接收消息 $r \parallel t$ 后, 调用 $prng()$ 生成一个随机数 s , 然后按照式(1) 生成会话消息:

$$m1 = h(k \oplus r \oplus s \oplus t) \oplus pID \quad (1)$$

标签形成消息 $m1 \parallel s$, 并经过阅读器转发给后端服务器。

步骤 3 后端服务器接收到消息 $m1 \parallel s$ 后, 用本身存储的密钥 k 以及 r, t 和接收的消息 $m1 \parallel s$, 按式(2) 进行计算, 得到 PID' 。

$$PID' = m1 \oplus h(k \oplus r \oplus s \oplus t) \quad (2)$$

后端服务器将其数据库中存储的 PID 和 $oldpID$ 与 PID' 进行比较, 具体情况如图 2 所示。

表 1 认证协议使用的各种符号

Tab. 1 All symbols of the authentication protocol

符号	含义
ID, pID	标签的唯一标识符和伪名
$oldpID$	上轮认证过程中的标签伪名
$k1, k2, k$	标签的当前密钥和共享密钥
$oldk1, oldk2$	上轮认证过程中的标签密钥
d	标签标识等秘密信息的比特数
$h()$	哈希函数
$prng()$	伪随机数生成函数
r, s	伪随机数
t	后端服务器的时间戳
\parallel, \oplus	连接运算和异或运算



图 2 协议的认证过程

Fig. 2 Authentication procedure of the proposed protocol

1) 若数据库中任何一条记录中的 pID 和 $oldpID$ 都不等于 pID' , 则说明这个标签没有在数据库中登记, 或者是一个伪造标签, 认证失败并退出。

2) 若数据库中存在一条记录, 其中存储的 pID 或者 $oldpID$ 等于 pID' , 则说明这个标签已在数据库中登记, 后端服务器因而初步确认该标签的身份。若 pID 等于 pID' , 则令 $psID = pID, symbol = 1$; 若 $oldpID$ 等于 pID' , 则令 $psID = oldpID, symbol = 0$ 。

然后, 后端服务器依据 $symbol = 1$ 或 $symbol = 0$, 分别按照式(3) 或(4) 生成消息 $m2$, 并发送给标签, 通知标签后端服务器已经确认该标签的存在。

$$m2 = h((k1 \oplus psID \oplus r) \parallel (k2 \oplus psID \oplus s)) \quad (3)$$

$$m2 = h((oldk1 \oplus psID \oplus r) \parallel (oldk2 \oplus psID \oplus s)) \quad (4)$$

步骤 4 标签接收到消息 $m2$, 按照式(5) 计算得到 $m3$, 然后比较 $m2$ 和 $m3$; 若两者不等, 则说明会话信息被篡改, 协议停止; 若两者相等, 标签进行后续认证过程, 按照式(6) 和



式(7)计算 $m4$ 和 $m5$ 。

$$m3 = h((k1 \oplus pID \oplus r) \parallel (k2 \oplus pID \oplus s)) \quad (5)$$

$$m4 = h((k1 \oplus pID \oplus s \oplus t) \parallel (k2 \oplus pID \oplus r \oplus t)) \quad (6)$$

$$m5 = h((k2 \oplus pID \oplus s) \parallel (k1 \oplus pID \oplus r)) \quad (7)$$

然后,标签经过阅读器将消息 $m4$ 发送给后端服务器。

步骤5 后端服务器接收消息 $m4$ 后,依据 $symbol = 1$ 和 $symbol = 0$,分别按照式(8)或者(9)生成消息 $m6$ 。

$$m6 = h((k1 \oplus psID \oplus s \oplus t) \parallel (k2 \oplus psID \oplus r \oplus t)) \quad (8)$$

$$m6 = h((oldk1 \oplus psID \oplus s \oplus t) \parallel (oldk2 \oplus psID \oplus r \oplus t)) \quad (9)$$

后端服务器比较 $m6$ 与 $m4$,若不等则对标签的认证失败,退出协议;若相等则完成了对标签的认证。然后,依据 $symbol = 1$ 和 $symbol = 0$,按照式(10)或者式(11)生成消息 $m7$,并经过阅读器发送给标签。

$$m7 = h((k2 \oplus psID \oplus s) \parallel (k1 \oplus psID \oplus r)) \quad (10)$$

$$m7 = h((oldk2 \oplus psID \oplus s) \parallel (oldk1 \oplus psID \oplus r)) \quad (11)$$

后端服务器依据 $symbol = 1$ 和 $symbol = 0$ 开始更新其伪名和密钥等信息,具体如下:

如果 $symbol = 1$,则按照式(12)~(17)更新该标签的伪名和密钥等信息。

$$oldk1 = k1 \quad (12)$$

$$k1 = prng(k1 \oplus s \oplus r) \quad (13)$$

$$oldk2 = k2 \quad (14)$$

$$k2 = prng(k2 \oplus s \oplus r) \quad (15)$$

$$oldpID = pID \quad (16)$$

$$pID = prng(pID \oplus t \oplus s) \quad (17)$$

如果 $symbol = 0$,则按照式(18)~(20)更新标签的密钥和伪名等信息。

$$k1 = prng(oldk1 \oplus s \oplus r) \quad (18)$$

$$k2 = prng(oldk2 \oplus s \oplus r) \quad (19)$$

$$pID = prng(oldpID \oplus t \oplus s) \quad (20)$$

步骤6 标签接收到后端服务器/阅读器发送来的消息 $m7$,并与 $m5$ 进行比较;若两者不等,则认证失败,退出协议;若两者相等,则对后端服务器/阅读器的认证成功,然后按照式(21)至(23)更新其密钥和伪名等信息。

$$k1 = prng(k1 \oplus s \oplus r) \quad (21)$$

$$k2 = prng(k2 \oplus s \oplus r) \quad (22)$$

$$pID = prng(pID \oplus t \oplus s) \quad (23)$$

4 认证协议的性能及安全性分析

通过上述认证过程可以看出,为了提高可扩展性和匿名性,本协议通过伪名在后端服务器和标签间传输标签的身份信息。后端服务器仅需要一次哈希运算就可以获得标签的伪名,进而获得标签身份;而以往基于哈希函数的认证协议一般要对数据库中的每条记录均要进行一次哈希运算,以确认标签的身份,故需要 $O(n)$ 次查找和 $O(n)$ 次哈希运算,其中 n 是标签的数量;若服务器端按照标签标识的哈希值(即散列值)组织标签信息的存储,假设标签的标识都是唯一的,在哈希函数不存在冲突的理想情况下可以获得 $O(1)$ 的查找时间,故系统具有很好的可扩展性。

下面分析协议的安全性。在 RFID 系统的安全模型中,假设敌手是一个概率多项式时间算法,它能够窃听、截获、篡改、跟踪、重放协议的每个会话。如果敌手能够从所窃听、截获的会话中猜出系统的秘密信息,或者能够区分不同的标签,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 $prng()$ 和 $h()$ 的随机查询, $prng()$ 和 $h()$ 的输出为 d 比特。显然敌手成功猜测到正确输出的概率 $\sigma \leq 2^{-d}$ 。

定义2 敌手是一个概率多项式时间算法,如果它揭示 RFID 系统秘密信息的概率是可以忽略的,则认为协议是隐私安全的。

定义3 敌手是一个概率多项式时间算法,它能够区分两个不同标签的概率 $\sigma = 2\Pr[pid_i = pid_j] - 1 (i \neq j)$;如果 σ 是可以忽略的,则认为协议满足不可区分安全性。

定义4 敌手是一个概率多项式时间算法,如果它从当前密钥能够猜测出更新前的密钥的概率是可以忽略的,则认为协议满足前向安全性。

对于所提出的认证协议,假设敌手可以截获协议的每个会话;其中,消息 $m1$ 、 $m2$ 、 $m4$ 和 $m7$ 中包括了系统的密钥、标识等秘密信息。由定义1可知,敌手从任何一个消息中猜测出秘密信息的概率是 σ ,而且 $\sigma \leq 2^{-d}$ 。当 $d = 32$,有 $\sigma \leq 2^{-32}$ 。显然 σ 是可以忽略的,故协议是隐私安全的。

对于一个具有概率多项式时间算法的敌手,它也可以截获任意多个会话,猜测它们是否来自于同一个标签,以达到区分和跟踪标签的目的。假设敌手截获了两个不同认证过程中的 $m1$ (或者 $m4$),其中包括标签的伪名 pid_i 和 pid_j 。如果敌手能够区分 pid_i 和 pid_j ,它获得成功的概率^[16] 定义为:

$$\Pr[pid_i = pid_j] = 2^{-1} + \varepsilon$$

其中: ε 为敌手同时猜测出 pid_i 和 pid_j 的概率。根据定义1,有 $\varepsilon \leq 2^{-d} \times 2^{-d}$ 。若 $d = 32$,有 $\varepsilon \leq 2^{-64}$ 。由定义3,有 $\sigma = 2\Pr[pid_i = pid_j] - 1 = 2\varepsilon \leq 2^{-63}$ 。所以 σ 是可以忽略的,所以协议具有不可区分安全性;显然,攻击者无法区分两个标签,因而协议可以抵抗跟踪攻击。

下面分析前向安全性。对于所提出的协议, $m2$ 、 $m4$ 和 $m7$ 等消息中包含标签秘密 $k1$ 和 $k2$ 。假设敌手截获这些消息,它从每个消息成功猜测密钥的概率是 $\varepsilon 1$,很容易得出 $\varepsilon 1 \leq 2^{-32}$ 。协议每成功运行一次,密钥信息都要进行更新,即 $ki = prng(ki \oplus s \oplus r)$;如果敌手想要得到更新前的密钥,它需要发起对 $prng()$ 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 $\varepsilon 2 \leq 2^{-32}$ 。具体有两种情况:

1) 敌手没有攻破标签 i ,它并不知道标签 i 的密钥;敌手可以从截获的历史消息 $m2$ 、 $m4$ 和 $m7$ 中去猜测更新前的密钥,其猜测成功的概率 $\sigma 1 = 3 \times \varepsilon 1 \leq 3 \times 2^{-32}$;或者敌手截获了并破译了当前消息 $m2$ 、 $m4$ 和 $m7$,再通过随机查询 $prng()$ 去猜测出更新前的密钥,其猜测成功的概率 $\sigma 1 = 3 \times \varepsilon 1 \times \varepsilon 2 \leq 3 \times 2^{-64}$ 。

2) 敌手攻破了标签 i ,它知道标签 i 的当前密钥 $k1$ 和 $k2$;敌手通过随机查询 $prng()$ 从当前密钥成功猜测出更新前密钥的概率 $\sigma 2 = \varepsilon 2 \leq 2^{-32}$ 。

显然,无论哪种情况, $\sigma 1$ 和 $\sigma 2$ 均是可以忽略的,所以本文协议具有前向安全性。

此外,在隐私保护和其他安全性方面,协议各实体间传输的所有秘密消息均经过随机化和哈希函数处理,敌手尽管可



以对标签和读写器间的无线信道进行窃听,但它无法解密,从而防止了秘密信息的泄露,有效地防止了窃听攻击,确保了协议的匿名性。对于每次认证,后端服务器/读写器/标签均生成一个新的随机数,使得各次认证过程中交换的会话信息具有一定的时效性;尽管攻击者获得了某次会话并在一定时间后进行重放,但此时该消息已经失去了意义,故认证协议可以抵抗重放攻击。同时,该协议通过密钥信息的更新和保留还可以确保抵御去同步攻击。

本文协议与其他典型认证协议在安全性能方面的对比情况如表2所示;显然,本文协议比其他典型的几个认证协议具有更好的安全性能。各协议在标签端调用的函数、发生的计算量和通信量等如表3所示;其中,计算量一栏函数前面的数字表示调用该函数的次数,d为会话消息的长度。尽管本文提出的协议在标签端需要的计算、通信量略高于其他协议,但是在隐私保护和安全性能上明显优于其他协议。

表2 本文协议与其他典型认证协议的比较

Tab. 2 Comparison of the proposed protocol with other typical authentication protocols

协议	匿名性	窃听	跟踪	重放攻击	去同步攻击	前向安全性
Hash-Lock	×	×	×	×	—	×
随机 Hash-Lock	×	×	×	×	—	×
Hash-chain	✓	✓	✓	×	✓	✓
LCAP	✓	✓	✗	✓	—	✗
本文协议	✓	✓	✓	✓	✓	✓

表3 各协议标签端调用的函数及其资源消耗

Tab. 3 Called functions and resource consuming on the tag of all protocols

协议	调用函数	计算量(调用次数)	通信量
Hash-Lock	$h()$	$1h()$	$3d$
随机 Hash-Lock	$prng(), h()$	$1prng() + 1h()$	$3d$
Hash-chain	$h(), g()$	$h() + g()$	$1d$
LCAP	$h()$	$2h()$	$3d$
本文协议	$prng(), h()$	$4prng() + 4h()$	$7d$

5 结语

随着RFID技术的广泛应用,标签的安全和隐私保护显得越来越重要。对于低值RFID标签,其计算存储资源有限,这给其安全和隐私保护问题的解决造成很大难度。针对这种低值RFID标签,本文提出了一个基于哈希函数的轻权认证协议。通过分析证实,尽管本文所提出的认证协议在计算量和通信量方面略高于其他协议,但是本协议具有很好的可扩展性和前向安全性,能够抵抗窃听、追踪、重放、去同步化等攻击;该协议通过使用伪名及随机化等措施确保了系统的可扩展性和匿名性。该协议仅使用了哈希函数、伪随机数生成函数和位运算等操作,仅需较少的计算和存储资源就可以达到RFID系统的安全目标。

参考文献 (References)

- [1] AAKANKSHA T, 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.
 - [2] WEIS S A, SARMA S E, RIVEST R L, et al. Security and privacy aspects of low-cost radio frequency identification systems [C]// Proceedings of the 1st International Conference on Security in Pervasive Computing, LNCS 2802. Berlin: Springer, 2003: 201–212.
 - [3] OHKUBO M, SUZUKI K, KINOSHITA S. Cryptographic approach to “privacy-friendly” tags [C]// Proceedings of the 2003 RFID Privacy Workshop. Cambridge: MIT Press, 2003: 1–9.
 - [4] LEE S M, HWANG Y J, LEE D H, et al. Efficient authentication for low-cost RFID systems [C]// Proceedings of the 2005 International Conference on Computational Science and Its Applications, LNCS 3480. Berlin: Springer, 2005: 619–627.
 - [5] CHO J-S, JEONG Y-S, PARK S O. Consideration on the brute-force attack cost and retrieval cost: a hash-based Radio-Frequency Identification (RFID) tag mutual authentication protocol [J]. Computers and Mathematics with Applications, 2015, 69(1): 58–65.
 - [6] KIM H. Desynchronization attack on hash-based RFID mutual authentication protocol [J]. Journal of Security Engineering, 2012, 9(4): 357–365.
 - [7] KHEDR W I. SRFID: a hash-based secure scheme for low cost RFID systems [J]. Egyptian Informatics Journal, 2013, 14(1): 89–98.
 - [8] HA J H, MOON S J, ZHOU J, et al. A new formal proof model for RFID location privacy [C]// Proceedings of the 2008 European Symposium on Research in Computer Security, LNCS 5283. Berlin: Springer, 2008: 267–281.
 - [9] SUN D-Z, ZHONG J-D. A hash-based RFID security protocol for strong privacy protection [J]. IEEE Transactions on Consumer Electronics, 2012, 58(4): 1246–1252.
 - [10] LIU Y, PENG Y, WANG B, et al. Hash-based RFID mutual authentication protocol [J]. International Journal of Security and Its Applications, 2013, 7(3): 183–194.
 - [11] DEHKORDI M H, FARZANEH Y. Improvement of the hash-based RFID mutual authentication protocol [J]. Wireless Personal Communications, 2014, 75(1): 219–232.
 - [12] ABIDIN S. Novel construction of secure RFID authentication protocol [J]. International Journal of Security, 2014, 8(4): 33–36.
 - [13] HABIBI M H, AREF M R. Attacks on recent RFID authentication protocols [J]. Journal of Signal Processing Systems, 2015, 79(3): 271–283.
 - [14] GOPE P, HWANG T. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system [J]. Computers and Security, 2015, 55(C): 271–280.
 - [15] 李松, 孙子文. 基于PUF适用于大规模RFID系统的移动认证协议[J]. 计算机工程与科学, 2018, 40(6): 1046–1053. (LI S, SUN Z W. PUF based authentication protocol in mobile and large-scale RFID systems [J]. Computer Engineering and Science, 2018, 40(6): 1046–1053.)
 - [16] 周永彬, 冯登国. RFID安全协议的设计与分析[J]. 计算机学报, 2006, 29(4): 581–589. (ZHOU Y B, FENG D G. Design and analysis of cryptographic protocols for RFID [J]. Chinese Journal of Computers, 2006, 29(4), 581–589.)
- SHI Zhicai, born in 1964, Ph. D., professor. His research interests include information security, privacy preserving.
- WANG Yihan, born in 1981, M. S., lecturer. His research interest includes information security.
- ZHANG Xiaomei, born in 1981, Ph. D., lecturer. Her research interest includes sensor network security.
- CHEN Shanshan, born in 1995, M. S. candidate. Her research interest includes indoor positioning.
- CHEN Jiwei, born in 1992, M. S. candidate. His research interest includes network security.