Journal of Computer Applications
计算机应用,2012,32(3):683 -685,698
ISSN 1001-9081
CODEN JYIIDU
2012-03-01
http://www.joca.cn

文章编号:1001 -9081(2012)03 -0683 -03
doi:10.3724/SP.J.1087.2012.00683

基于 PUF 的高效低成本 RFID 认证协议

贺章擎[1,2*],郑朝霞[1],戴 葵[1],邹雪城[1]
(1.华中科技大学 电子科学与技术系,武汉 430074; 2.湖北工业大学 电气与电子工程学院,武汉 430068)
(*通信作者电子邮箱 ivan_hee@126.com)

摘 要:已提出的针对低成本 RFID 系统的安全机制,要么存在安全缺陷,要么硬件成本太高。为此设计了一个基于物理不可克隆功能(PUF)的 RFID 安全认证协议,利用 PUF 和线性反馈移位寄存器(LFSR)实现了阅读器和标签之间强的安全认证,解决了已有安全协议存在的问题。安全性分析表明:该协议成本低、安全性高,能够抵抗物理攻击和标签克隆,并有极强的隐私性。

关键词:射频识别;安全认证协议;物理不可克隆功能;线性反馈移位寄存器;加密
中图分类号:TP309 **文献标志码**:A

Low-cost RFID authentication protocol based on PUF

HE Zhang-qing[1,2*], ZHENG Zhao-xia[1], DAI Kui[1], ZOU Xue-cheng[1]
(1. *Department of Electronic Science and Technology, Huazhong University of Science and Technology, Wuhan Hubei* 430074, *China*;
2. *School of Electrical and Electronic Engineering, Hubei University of Technology, Wuhan Hubei* 430068, *China*)

Abstract: The available security mechanisms for the low-cost Radio Frequency IDentification (RFID) systems are either defective or high-cost. Therefore, this paper proposed an efficient security authentication protocol for low-cost RFID system based on Physical Unclonable Function (PUF) and Linear Feedback Shift Register (LFSR). The protocol provides strong security and can resist physical attack and tag clone with strong privacy.

Key words: Radio Frequency IDentification (RFID); security authentication protocol; Physical Unclonable Function (PUF); Linear Feedback Shift Register (LFSR); encryption

0 引言

射频识别(Radio Frequency IDentification, RFID)技术作为一种全新的非接触自动识别技术,可广泛应用于生产、零售、物流、交通、医疗、国防各个行业,是目前发展最为迅速和最具潜力的新兴技术之一。典型的 RFID 系统由标签、阅读器和后端服务器 3 个部分组成,当标签进入阅读器产生的电磁场中,阅读器和标签相互发送射频信号进行通信,阅读器获得标签存储的信息,进而传递给后端数据处理系统进行管理控制。由于 RFID 系统中阅读器和标签之间采用无线通信的方式,RFID 系统可能面临着监听、欺骗、篡改和跟踪等威胁,带来通信安全问题和用户隐私泄露问题,这已经成为制约 RFID 技术发展的关键问题之一。尤其是在低成本的 RFID 系统中,电子标签有限的硬件资源极大地制约了 RFID 安全机制的实现,传统的安全与加密技术很难直接应用到 RFID 系统中来。因此,如何实现 RFID 系统的安全并保护电子标签持有人隐私将是目前和今后发展 RFID 技术十分关注的课题。

为了解决 RFID 安全与隐私问题,国内外研究人员展开了大量研究,提出了一系列解决方案。除了针对部分极低成本的标签提出了一些物理机制,譬如 Kill 命令机制、静电屏蔽、主动干扰以及 Blocker Tag 方法等外,大部分的安全机制都采用安全认证协议[1]。

目前提出的安全认证协议有很多,影响较大的主要有 Hash-Lock 协议[2]、随机化 Hash-Lock 协议[3]、Hash-Chain 协议[4]、分布式 RFID 挑战-响应认证协议[5]、数字图书馆 RFID 协议[6]等,另外还有 HASP 协议[7]、轻量级认证协议 SASI[8]等。但是 Hash-Lock 协议和随机化 Hash-Lock 协议存在明显安全缺陷。分布式 RFID 询问-响应认证协议、数字图书馆 RFID 协议和 HASP 协议需要在标签中集成随机数产生和安全伪随机函数两大功能模块,标签成本太高。而 SASI 协议虽然对标签成本要求较低,但无法抵抗物理攻击和标签克隆。至今仍未能提出一种针对 RFID 系统低功耗低成本特点,满足各种安全需求,高效实用的安全认证机制。

1 基于 PUF 的 RFID 安全认证机制

传统的 RFID 安全认证协议大多采用 Hash 函数来执行加密运算,需要大量的硬件开销。例如标准的 MD4、MD5 和 SHA-256 大概需要 7 350 ~ 10 868 个门电路来实现,即使是根据 RFID 系统特点而简化设计的 Hash 运算和高级加密标准(Advanced Encryption Standard, AES)加密运算也分别需要 1 700个[9]和 3 400 个门电路[10],对成本非常敏感的低成本 RFID 标签显然难以承受。而且使用这些加密机制的 RFID 系统还存在一个致命的缺陷,就是无法抵抗物理攻击和标签克隆。攻击者可以通过解剖芯片的方式获取标签内部存储的密钥,在此基础上进行芯片的反向设计实现标签的克隆。

物理不可克隆功能(Physical Unclonable Function, PUF)[11]的出现能有效解决上述问题。PUF 是一组微型延迟电路,当收到一个随机的二进制输入口令之后,会生成一个唯一的、随机的二进制序列作为响应,而这个响应是利用芯片制

收稿日期:2011-08-30;**修回日期**:2011-11-20。 **基金项目**:武汉市重点科技攻关计划项目(201150699190)。
作者简介:贺章擎(1980 -),男,湖北天门人,讲师,博士研究生,主要研究方向:信息安全、嵌入式系统; 郑朝霞(1975 -),女,重庆人,讲师,博士,主要研究方向:大规模数字集成电路设计; 戴葵(1968 -),男,湖北恩施人,教授,博士,主要研究方向:高性能处理器系统、计算机系统结构、信息安全; 邹雪城(1965 -),男,湖北监利人,教授,博士,主要研究方向:大规模集成电路设计。

造过程中的光刻、掺杂等环节所产生的差异来生成的。由于芯片制造过程中产生的差异本身具有不可模仿和复制的特性,所以每个芯片中的 PUF 电路可以生成无限多个、唯一的、不可复制的口令/响应序列。即使是芯片的制造厂商也不可能从另外一个芯片上复制出一套一模一样的口令/响应序列。所以,如果在标签芯片内部集成一个 PUF 模块,则该标签就具有反克隆的功能,同时 PUF 唯一的口令/响应序列也可以用来对标签进行认证。同时,PUF 电路所需的硬件开销很小,一个 64 位的 PUF 电路大概需要 545 个门电路[12],大大少于简化后的 Hash 运算和 AES 加密电路。正是由于 PUF 的这些特点,使得利用 PUF 来设计 RFID 认证协议成为一个新的研究热点。

Suh 等[11]首先提出基于 PUF 的 RFID 认证机制,如图 1 所示。每个包含 PUF 的标签芯片在安全的环境下提取足够多的口令/响应对,并将这些口令/响应对存储于阅读器的后台数据库中。如果阅读器要对某个标签进行认证,就从后台数据库中提取该标签的一对口令/响应对,将口令发送给标签,然后将标签传送过来的响应与存储的响应值进行比较,如果相同,则通过认证,同时在数据库中删除该条口令/响应对。该方案是一种最简单的认证方案,但只实现了阅读器对标签的单向认证。同时每个标签需要预先在数据库中存储大量的口令/响应对,如果标签数量很多,数据库对口令/响应对的查找和管理将是一个浩大的工程。

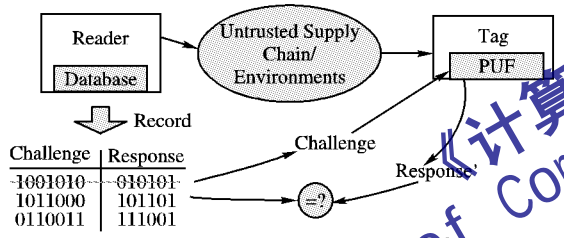

图 1 基于 PUF 的 RFID 认证机制[11]

杨灵等[13]提出了一种很有意思的认证协议(下面简称杨灵协议)。该协议使用了 PUF 和线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)模块。LFSR 是用来生成二进制序列的一种机制,如果 LFSR 的种子保持机密,LFSR 就可作为伪随机数产生器。同时,对于相同的密钥种子,两个相同结构的 LFSR 会产生相同的伪随机数,这个特点也用来对阅读器和标签的共享密钥进行同步更新。

在杨灵协议中,阅读器对标签进行认证时不需要在后台数据库中预先存储大量的口令/响应对,而是共享一个密钥,该密钥由标签内的 PUF 电路实时产生,而且每次成功认证后在阅读器和标签内同步更新。由于 PUF 的物理不可克隆性特性,使得对手无法预测和破解密钥。同时利用 LFSR 产生随机序列,加密阅读器与标签之间密钥交换信息。该协议的认证过程如图 2 所示。

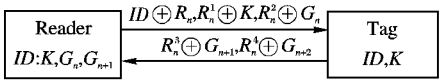

图 2 杨灵协议[13]

文献[13]中称该协议能抵抗重放攻击、跟踪攻击、物理攻击、窃听攻击等多种攻击。实际上该协议存在几个明显的缺陷:

1) 在协议认证阶段的第一步,阅读器首先确定需要查询的标签 ID,然后在通信范围内广播查询信号 $ID \oplus R_n$ 给标签,标签通过该 ID 判断阅读器查询的标签是否是自己。但在实际的认证机制中,阅读器在和某个标签进行认证之前,很多情况下事先根本不知道该标签是哪个 ID,也就不知道要广播哪个信号。

2) 该协议无法抵抗物理攻击。如果攻击者通过物理探测或者其他手段,获取了某个标签的 ID 和密钥 K,同时知道了 LFSR 的结构,那么攻击者就可以假冒阅读器通过标签的认证。

2 基于 PUF 的高效低成本 RFID 安全认证协议

虽然已提出的基于 PUF 的安全认证机制存在一些问题,但是为设计更好的认证机制提出了很好的参考思路。本文设计的安全认证协议,解决了以上协议存在的问题,能够抵抗窃听攻击、重放攻击、物理攻击和标签复制,防止跟踪,具有很好的前向安全性和后向安全性。

协议的认证过程如图 3 所示。简单起见,本文将阅读器和后台数据作为一个整体看待。

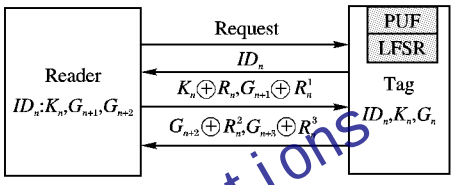

图 3 基于 PUF 的 RFID 认证机制

本协议中,标签使用如下参数和函数:

1) 随机置换函数 P。P 函数由 PUF 构成,输入为 l 位口令,输出 l 位响应。由于 PUF 的物理不可克隆性,对于同样的输入,每个标签的 P 函数都将产生不同的输出。

2) 线性移位寄存函数 L。L 是一个随机函数发生器,输入输出都是 l 位整数,由 LFSR 构成。同时,L 函数的构成是公开的,所有的标签和攻击者都能使用。

3) ID_n。指目标标签第 n 轮认证的 ID,是一个 l 位整数。每个标签都有自己的 ID,阅读器里面存储了所有合法标签的 ID。每次认证成功之后,ID_n 在标签和阅读器里面同步更新。

4) 密钥 K_n。K_n 是阅读器和标签第 n 轮认证的共享密钥,长度也为 l 位。每个标签都和阅读器共享不同密钥,每次认证成功之后,K_n 也在标签和阅读器里面同步更新。

5) 共享参数 G_n。标签通过该参数对阅读器进行认证。

本协议中,阅读器使用如下参数和函数:

1) 阅读和后台数据存有每个标签合法对应的记录项 $ID_n:K_n,G_{n+1},G_{n+2}$,其中 G_{n+1} 和 G_{n+2} 为共享参数,长度均为 l 位。在初始化时,这两个参数与对应的标签内存储的 G_n 之间的关系为 $G_{n+1} = P(G_n)$,$G_{n+2} = P(G_{n+1})$。阅读器通过这两个参数对标签进行认证。

2) 线性移位寄存函数 L,和标签内结构相同的线性移位寄存器。

协议的认证过程如下:

1) 阅读器发送认证请求给标签。

2) 标签发送它的 ID_n 作为响应。

3) 阅读器找到 ID_n 对应的记录项,产生一个随机数 R_n,利用 L 函数计算 $R_n^1 = L(R_n)$,然后发送 $K_n \oplus R_n, G_{n+1} \oplus R_n^1$ 给标签。

4) 标签利用存储的 K_n 与接收的 $K_n \oplus R_n$ 异或,获取随机数 R_n,然后利用同样结构的 L 函数计算 $R_n^1 = L(R_n)$,再利用 R_n^1 与 $G_{n+1} \oplus R_n^1$ 异或提取 G_{n+1}。

5) 标签利用存储的 G_n 和 P 函数计算 $P(G_n)$,验证

$P(G_n) = G_{n+1}$ 是否成立,如果相等,则阅读器通过认证,进入下一步;否则认证失败,返回一个随机值。

6) 标签利用 L 函数产生 $R_n^2 = L(R_n^1)$, $R_n^3 = L(R_n^2)$, $R_n^4 = L(R_n^3)$, $R_n^5 = L(R_n^4)$,计算 $G_{n+2} = P(G_{n+1})$, $G_{n+3} = P(G_{n+2})$,然后发送 $G_{n+2} \oplus R_n^2$, $G_{n+3} \oplus R_n^3$ 给标签。同时更新存储的 $G_n = G_{n+1}$, $ID_n = ID_n \oplus R_n^4$, $K_n = K_n \oplus R_n^5$。

7) 阅读器收到 $G_{n+2} \oplus R_n^2$, $G_{n+3} \oplus R_n^3$ 后,利用 L 函数产生相同的 $R_n^2, R_n^3, R_n^4, R_n^5$,利用 R_n^2 和 R_n^3 提取出 G_{n+2} 和 G_{n+3},然后验证阅读器中存储的 G_{n+2} 和接收的 G_{n+2} 是否相等,如果相等,则标签通过认证,同时更新该标签对应的记录项 $ID_n = ID_n \oplus R_n^4$, $K_n = K_n \oplus R_n^5$, $G_{n+1} = G_{n+2}$, $G_{n+2} = G_{n+3}$,用于下一轮搜索;否则认证失败。

3　协议安全性分析

一个安全可靠的 RFID 认证协议,需要满足正确性(Correctness)、安全性(Security)和隐私性(Privacy)3 个特性。正确性确保合法的阅读器和标签能够可靠地对对方进行认证;安全性确保该协议能抵抗各种攻击;而私密性则确保标签的私有信息不被非法获取,或者被跟踪。本文将从这 3 个方面对协议进行分析。

1)正确性。

本协议中阅读器和标签通过共享密钥,实现了双向认证。假设信道传输可靠,且在 PUF 发生错误的概率可忽略的情况下,协议的错误肯定(False-positive)和错误否定(False-negative)的概率是可忽略的,系统满足正确性。协议中标签只需要集成 PUF 模块和 LFSR,PUF 需要 545 个等效门,LFSR 需要 300 个等效门[14],少于 Hash 函数的至少 1 700 个门电路。协议对标签硬件的需求少,执行效率高。

2)安全性。

为了分析协议的安全性,我们先对对手进行定义。我们假设攻击者可以随时窃听阅读器和标签之间的通信,对信息进行分析或者重放;也可以通过反向工程等物理手段打开标签获取标签内存储的信息,然后利用这些信息进行假冒和哄骗攻击;或者对标签进行跟踪。

窃听攻击　通过分析发现,在阅读器和标签的每轮通信中,除了 ID_n 之外,所有传输的信息都与随机数进行异或操作,且每一轮都采用了一个新的随机数。Shannon 理论证明,如果在异或操作中至少有一项是随机的,那么一个简单的异或加密有极好的安全性。同时每次认证成功后,标签内存储的信息都与阅读器同步更新,更新使用随机数和标签内的 PUF 运算,攻击者无法通过多轮窃听来分析获取任何有用信息。

重放攻击　由于每次认证中都采用了不同的随机数,且标签和阅读器的共享密钥即时更新,攻击者通过重放阅读器的查询或者标签的响应无法对系统构成威胁。

物理攻击　假设攻击者可以通过反向工程或者物理探测等手段获取存储在标签内的 ID_n, K_n, G_n 信息,但是获取的信息不足以对系统构成威胁。因为标签对阅读器的认证是依据第 5) 步中阅读器发送过来的 G_{n+1},而阅读器对标签的认证则是通过第 7) 步中的 G_{n+2},这两个信息由标签中的 PUF 实时产生,由于 PUF 的不可克隆特性,攻击者不可能模仿 PUF 产生这两个信息,从而假冒标签或者阅读器通过认证。

标签复制　由于标签内 PUF 的物理不可克隆特性,攻击者不可能复制该标签。

假冒和哄骗攻击　该认证机制中,攻击者不管是从无线信道上,或者通过物理手段获取了标签内部的密钥,也无法假冒阅读器或者标签进行假冒和哄骗攻击。

前向安全性和后向安全性　每次认证之后,标签内 ID_n 和 K_n 通过和一个随机数异或来更新,而 G_n, G_{n+1}, G_{n+2} 则是通过标签内 PUF 产生的输出进行更新。在这种更新机制中,即使攻击者知道了某一轮中 ID_n, K_n, G_n 的值,也无法推导出前一轮和后一轮的秘密值。所以,该协议具有前向安全性和后向安全性。

3) 隐私性。

保护隐私的一个重要方面要求标签具有不可跟踪性。所谓的不可跟踪性,就是攻击者不能从一个协议通信报文集中区分出两个具有不同密钥的标签。

本协议中,每次认证都由阅读器发送认证请求开始,在它通信范围内的标签接到请求后发送它的 ID_n 作为应答。由于标签的 ID_n 每次成功认证之后都会更新,而且每次更新都是和一个新的随机数异或,即使对手窃听了同一标签多次通信所使用的 ID,也无法将这几个 ID 联系起来,也就是对手无法跟踪该标签。当然,如果标签没有成功认证,也就是 ID_n 没有更新的情况下,跟踪是可能的。但是由于对手跟踪某一标签的目的常常是分析同一标签多次通信中的信息,如果跟踪到的标签每次都没有通过合法阅读器认证,也就是未执行任何操作,这种跟踪也就没有意义。

4　结语

本文设计了一个基于 PUF 的低成本高效率 RFID 认证协议,解决了已有的安全认证协议存在的问题,能够抵抗窃听攻击、重放攻击、物理攻击和标签复制,防止跟踪,具有很好的前向安全性和后向安全性。需要指出的是,该协议设计的基础是假定 PUF 是不可克隆的,也就是攻击者无法建立一个精确的攻击模型来模拟 PUF。但根据最新的研究成果,如果攻击者能够获取某个 PUF 足够多的口令/响应对,就可以利用建模攻击(modeling attacks)构造一个计算算法,以比较高的准确率预测该 PUF 的口令/响应对[15]。但是在本文设计的认证机制中,攻击者很难获取足够的口令/响应对来建立破解模型,所以该机制能够抵抗这种攻击。另外,本协议可能会受到拒绝服务攻击,也就是在认证中当标签更新存储的信息后,由于受到攻击致使阅读器内的信息没有同步更新,就会造成信息不同步的情况。为了解决这个问题,可以在标签内存储上一次认证时的密钥,必要时采用旧的密钥进行认证。

参考文献:

[1] JUELS A, WEIS S A. Authenticating pervasive devices with human protocols[C]// CRYPTO 2005: Proceedings of 25th Annual International Cryptology Conference, LNCS 3621. Berlin: Springer-Verlag, 2005: 293 - 308.

[2] SARMA S, WEIS S, ENGELS D. Radio frequency identification: Secure risks and challenges[J]. RSA Laboratories Cryptobytes, 2003, 6(1): 2 - 9.

[3] 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-Verlag, 2004: 201 - 212.

[4] OHKUBO M, SUZUKI K, KINOSHITA S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID [C]// SCIS 2004: Proceedings of the 2004 Symposium on Cryptography and Information Security. Berlin: Springer-Verlag, 2004: 719 - 724.

(下转第 698 页)

数)/码文长度,原文长度 = kl,码文长度 $L = k(l + \lceil \mathrm{lb}(k-1) \rceil) + l + 2\mathrm{lb}\,k$,$D = kl/L$。如文献[15]所述,当 k 和 l 足够大时,背包密度可以接近1。经测算,当 $k = 512$,$l = 256$,m_i 的长度为265,背包密度为0.9641,处于安全区域。

4.4.2 私钥恢复攻击

模 m' 群有如下关系:

$w'^{-1}a''_i - t_i m' = a'_i; 1 \leqslant i \leqslant k$

破译者可以从公钥出发,运用格基规约算法[6]推算出 t_i,但由于 m' 是保密的,破译者要继续下去,需要利用 a''_i 或 a'_i 中遗留的冗余度,但这些冗余度都被隐藏了,破译者无法利用,文献[13]所展示的攻击法无法成功。即使攻击者从公钥出发追踪到 a'_i,由于 a'_i 是模 m 加运算后的余,也不能通过联立方程组的方法解出 a_i。

5 结语

在背包密码普遍不被看好的情况下,本文以新的视角对其进行研究和分析。本文认为,背包公钥序列是由初始序列变换来的,初始序列代表着易解背包,具有一定的规律和特性,故背包公钥序列不可能是完全随机的。这些规律和特性形成初始序列的冗余度,利用此冗余度是破译成功的必要条件。可以将初始序列看作需加密的文本,变换看作加密过程,公钥序列看作密文。背包公钥算法的安全性有两个方面:一是保证背包密度,抵御低密度子集和攻击;二是优化变换过程,使攻击者难以从公钥出发利用初始序列的冗余度。目前大多数被破译的背包公钥密码只使用了属混乱技术的模乘运算,不能充分隐藏初始序列的冗余度,本文引入加法扩散技术,进一步隐藏初始序列的冗余度,使攻击者难以利用。以实际例子说明了两种加法扩散技术,即项内扩散技术和项间扩散技术。分析表明,运用了扩散技术后,攻击者难以利用初始序列的冗余度,目前已知的破译方法不再奏效。

参考文献:

[1] MERKLE R C, HELLMAN M H. Hiding information and signatures in trapdoor knapsacks[J]. IEEE Transactions on Information Theory, 1978, 24(5): 525 - 530.

[2] COSTER M J, JOUX A, LAMACCHIA B A, *et al*. Improved low-density subset sum algorithms [J]. Computational Complexity, 1992, 2(2): 111 - 128.

[3] ODLYZKO A M. The rise and fall of knapsack cryptosystems[EB/OL]. [2010-05-10]. http://www.dtc.umn.edu/~odlyzko/doc/arch/knapsack.survey.pdf.

[4] LAI M K. Knapsack Cryptosystems: The Past and the Future [EB/OL]. [2011-09-15]. http://www.ics.uci.edu/~mingl/knapsack.html.

[5] 王保仓,韦永壮,胡予濮. 基于随机背包的公钥密码[J]. 电子与信息学报,2010,32(7):1580 - 1584.

[6] LENSTRA A K, LENSTRA H W, Jr, LOVASZ L. Factoring polynomials with rational coefficients [J]. Mathematische Annalen, 1982, 261(4): 513 - 534.

[7] 王保仓,巨春飞. 对一个背包公钥密码的格攻击[J]. 计算机应用研究,2010,27(4):1466 - 1492.

[8] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656 - 715.

[9] SHAMIR A. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem[J]. IEEE Transactions on Information Theory, 1984, 30(5): 699 - 704.

[10] SCHNEIER B. 应用密码学[M]. 吴世忠,祝世雄,张文政,等译. 北京:机械工业出版社,2000:185 - 250.

[11] LAGARIAS J C. Knapsack public key cryptosystems and diophantine approximation[C]// Proceedings of CRYPTO '83. Berlin: Springer-Verlag, 1984: 3 - 23.

[12] 王保仓,韦永壮,胡予濮. 基于中国剩余定理的快速公钥加密算法[J]. 西安电子科技大学学报:自然科学版,2008,35(3):449 - 454.

[13] 章照止. 破译一个新的背包公钥密码系统[J]. 系统科学与数学,1991,11(1):91 - 96.

[14] 韩立东,刘明洁,毕经国. 两种背包型的公钥密码算法的安全性分析[J]. 电子与信息学报,2010,32(6):1485 - 1488.

[15] 何敬民,卢开澄. 背包公钥系统的安全性与设计[J]. 清华大学学报:自然科学版,1988,28(1):89 - 97.

(上接第685页)

[5] MOLNAR D, WAGNER D. Privacy and security in library RFID: Issues, practices, and architectures[C]// CCS'04: Proceedings of the 1th ACM Conference on Computer and Communications Security. New York: ACM Press, 2004: 210 - 219.

[6] RHEE K, KWAK J, KIM S, *et al*. Challenge-response based RFID authentication protocol for distributed database environment[C]// SPC 2005: Proceedings of the 2nd International Conference on Security in Pervasive Computing, LNCS 3450. Berlin: Springer-Verlag, 2005: 70 - 84.

[7] 丁振华,李锦涛,冯波. 基于Hash函数的RFID安全认证协议研究[J]. 计算机研究与发展,2009,46(4):583 - 592.

[8] CHIEN H Y. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity [J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 337 - 340.

[9] YUKSEL K. Universal hashing for ultra-low-power cryptographic hardware applications[D]. Worcester: Worcester Polytechnic Institute, Electrical & Computer Engineering Department, 2004.

[10] FELDHOFER M, DOMINIKUS S, WOLKERSTORFER J. Strong authentication for RFID systems using the AES algorithm[C]// Proceedings of CHES. New York: ACM Press, 2004: 85 - 140.

[11] SUH G E, DEVADAS D. Physical unclonable functions for device authentication and secret key generation[C]// DAC'07: Proceedings of the 44th Annual Design Automation Conference. New York: ACM Press, 2007: 9 - 14.

[12] GASSEND B, CLARKE D, van DIJK M, *et al*. Silicon physical random functions[C]// Proceedings of the 9th ACM Computer and Communication Security. New York: ACM Press, 2002: 148 - 160.

[13] 杨灵,闰大顺. 基于PUF的低成本RFID系统安全协议[J]. 计算机工程,2010,36(15):148 - 155.

[14] LEONID B, GABRIEL R. Physically unclonable function - based security and privacy in RFID Systems [C]// PerCom'07: Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications. Piscataway, NJ: IEEE Press, 2007: 211 - 220.

[15] RUHRMAIR U, MUNCHEN T, DROR G, *et al*. Modeling attacks on physical unclonable functions[C]// Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM Press, 2010: 237 - 249.