一种新的轻量级RFID双向认证协议

柳 毅 顾国生
(广东工业大学计算机学院 广州 510006)

摘 要 RFID技术是一种广泛应用于各种物体识别和跟踪的自动识别技术,它适用于多个领域。然而,设计出一个安全的轻量级的RFID认证协议是一项具有挑战性的任务。最近Kulseng等人提出了一种轻量级RFID认证协议,该协议采用物理不可克隆技术和线性反馈移位寄存器来实现,非常适合轻量级操作。分析发现,该协议存在几个严重的安全问题。在分析上述协议的基础上,提出了一种新的轻量级RFID双向认证协议。分析表明,新协议在保持轻量级操作的同时,具有更好的安全性和保密性。

关键词 RFID,轻量级,物理不可克隆函数,线性反馈移位寄存器,双向认证
中图法分类号 TN918 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.02.033

New Mutual Authentication for Lightweight RFID Protocols

LIU Yi GU Guo-sheng
(School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China)

Abstract Radio frequency identification (RFID) technology is an automated identification technology which is widely used to identify and track all kind of objects. It is well suitable for many fields. However, it is a challenging task to design an authentication protocol because of the limited resource of lightweight RFID tags. Recently, a lightweight RFID authentication protocol of RFID tags were presented by Kulseng et al. This protocol uses physically unclonable functions (PUFs) and linear feedback shift registers (LFSRs) which are well known for lightweight operations. Unfortunately, their protocols face several serious security issues. In this paper, based on PUFs and LFSRs, we suggested a new mutual authentication for low-cost RFID Systems. Security analysis shows that our protocol owns better security and privacy.

Keywords RFID, Lightweight, PUF, LFSR, Mutual authentication

1 引言

无线射频识别(Radio Frequency Identification, RFID)已被广泛应用于许多领域,如物流、国防、交通等。RFID系统是一个自动识别系统,通常由3部分组成:标签、阅读器和后端数据库[1-2]。阅读器可以访问存储在标签内部的信息,也可以转发标签和后端数据库之间通信的消息。后端数据库可以提供多样化的服务,如身份验证服务、库存管理服务等。RFID系统具有标签小而轻并且多个标签可以同时通信的优点,因此预计将取代目前的条形码系统用于供应链管理[3]。

许多基于伪随机数生成器的RFID认证协议被提出,这类协议可以实现安全与隐私保护,如文献[4-5]。同时,一些基于位运算和HASH函数的轻量级RFID认证协议也被提出,如文献[6-9]。但是这些协议都存在安全隐患或是认证效率低等问题。

近些年的研究成果中,文献[10]中提出的认证方案不能提供向后的隐私安全性;文献[11]中提出的认证方案不能抵抗去同步攻击,攻击者可以通过重放消息使阅读器与标签两者之间的密钥不一致,从而破坏两者之间的后续认证;文献[12]中提出的认证方案不能抵抗主动攻击,攻击者可以通过不断地询问标签来分析标签的回复信息,从而完全推导出标签中存放的所有密钥信息;文献[13]中提出的方案不能抵抗暴力破解攻击,攻击者可以采用穷举法推导出标签中存放的密钥信息。

物理不可克隆函数(PUF)一个是利用物体的物理特征把输入值映射到应答值的函数[14]。PUF具有不可克隆性,给定一个特定的输入,标签的PUF将产生一定的输出,而其他标签的PUF将产生不同的输出。

基于物理不可克隆函数(PUF)和线性反馈移位寄存器(LFSR),Kulseng等人[15]提出了一种RFID双向认证协议,该协议不需使用复杂的密码操作,非常适用于轻量级RFID。但是,Kardas等人[16]指出上述协议存在一些严重的安全问题。针对文献[15]提出的协议所存在的安全问题,本文提出了一种新的轻量级RFID双向认证协议。新协议在保持轻量

到稿日期:2015-11-30 返修日期:2016-03-06 本文受国家自然科学基金项目(61572144),广东省自然科学基金项目(2014A030313517),广东省科技计划项目(2013B040500009)资助。

柳 毅(1976-),男,博士,副教授,CCF会员,主要研究方向为网络与信息安全;顾国生(1978-),男,博士,讲师,主要研究方向为信息安全,E-mail:gsgu@gdut.edu.cn(通信作者)。

级操作的同时，具有更好的安全性和保密性。

2　Kulseng 协议及分析

2.1　符号描述

ID：标签的唯一标识符；

IDS：标签的索引（在每一轮中更新）；

G_0：初始随机数；

F：随机置换函数，映射区间为$[1,q]$，其中 q 是 IDS 的长度（LFSR 可以作为 F 函数）；

P：随机置换函数，映射区间为$[1,q]$（P 函数是基于 PUF 功能实现的）。

2.2　协议描述

首先将初始化的 ID，IDS 以及 G_0 存放到每个标签中，然后通过储存在标签内部的 PUF 函数进行运算得到 $G_{n+1}=P(G_n)$，接着将(IDS,ID,G_n,G_{n+1})存放到后端数据库中，最后把(IDS,ID,G_n)放入标签中。Kulseng 等人提出的协议的流程如图 1 所示。

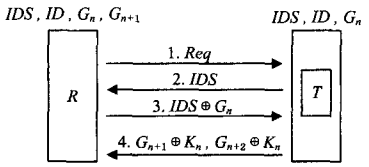

图 1

但是，Kardas 等人[16]指出该协议存在 3 种不同的安全缺陷，下面作简要介绍。

假设 R 是一个合法的阅读器，T 是一个合法的标签，A 是一个攻击者。

(1)消息阻塞攻击

1)R 广播发送请求认证命令，T 把自己的 IDS 发给 R。

2)R 计算 $ID\oplus G_n$，并将它发给 T。在 R 和 T 传输信息的过程中，易发生阻塞攻击。

3)A 广播发送请求认证命令，T 把自己的 IDS 发给 A。

4)A 发送 $ID\oplus G_n$ 给 T。

5)T 计算 $K_n\oplus G_{n+1}$ 和 $K_n'\oplus G_{n+2}$，并将它们发给 A；然后 T 更新 $IDS=F(IDS\oplus G_n)$ 和 $G_n=G_{n+1}$。

6)T 不能验证 R 的身份，因为 R 将发送 $ID\oplus G_n$，但是 T 只有 G_{n+1}，无法验证 ID。

(2)去同步攻击

该协议不能保证信息的完整性。在原协议的步骤 4 中，当 A 插入一个随机消息时，T 和 R 的消息传输过程将会被打乱。

1)R 广播发送请求认证命令，T 把自己的 IDS 发给 R。

2)R 计算 $ID\oplus G_n$，并将它发给 T。

3)T 计算 $K_n\oplus G_{n+1}$ 和 $K_n'\oplus G_{n+2}$，并将它们发给 R。A 将在消息 $K_n'\oplus G_{n+2}$ 中插入一个随机数 n_x，从而得到 $K_n'\oplus G_{n+2}\oplus n_x$；最后 T 更新 $IDS=F(IDS\oplus G_n)$ 和 $G_n=G_{n+1}$。

4)在收到消息 $K_n\oplus G_{n+1}$ 以及修改的消息 $K_n'\oplus G_{n+2}\oplus n_x$ 之后，R 开始验证 $K_n\oplus G_{n+1}$ 的正确性，如果正确，则 R 更新 $G_{n+1}=K_n'\oplus G_{n+2}\oplus n_x\oplus K_n'=G_{n+2}\oplus n_x$ 和 $IDS=F(IDS\oplus G_n)$。

5) 下一步中，R 有了 G_n，G'_{n+1} 和 $G'_{n+1}\neq P(G_n)$。根据该协议，T 可以认证 R，但是 R 不能认证 T。

(3)LFSR 的误用

Kardas 等人指出，LFSR 的使用使得攻击者可以很容易地获取标签的 ID，并且跟踪此标签。攻击过程如下：假设攻击者监控到标签和阅读器之间一次完整的认证会话过程，那么攻击者就可以获取会话消息：Req，IDS_{old}，$ID\oplus G_n$，$G_{n+1}\oplus K_n$，$G_{n+2}\oplus K_n'$；然后攻击者向标签发送一个假的查询命令，标签将会以 $IDS_{new}=F(IDS_{old}\oplus G_n)$ 作为响应发给攻击者。攻击者可以从 $F(IDS_{old}\oplus G_n)$ 中得到 $IDS_{old}\oplus G_n$ 这个非常重要的信息，进而可以通过 IDS_{old}，$ID\oplus G_n$ 和 $IDS_{old}\oplus G_n$ 得到标签的 ID，最终跟踪标签。

3　新的协议

本节提出了一种新的轻量级双向认证 RFID 协议，并对其安全性进行了分析，协议的符号描述与 2.1 节相同。新协议示意图如图 2 所示。

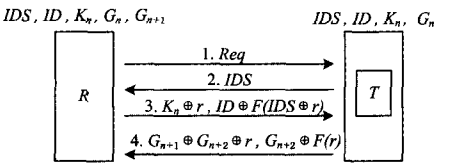

图 2　新协议示意图

协议过程详细描述如下。

(1)阅读器首先发送认证请求命令。

(2)标签收到阅读器发送的认证请求命令并对其作出响应，将自己的 IDS 发送给阅读器。

(3)如果阅读器能找到与之相对应的 IDS，则首先更新 $IDS=F(IDS\oplus G_n\oplus K_n)$；然后产生一个随机数 r，并且计算 $K_n\oplus r$ 和 $ID\oplus F(IDS\oplus r)$；最后阅读器将 $K_n\oplus r$ 和 $ID\oplus F(IDS\oplus r)$ 发送给标签。

(4)标签在收到 $K_n\oplus r$ 和 $ID\oplus F(IDS\oplus r)$ 以后，首先通过 $K_n\oplus r\oplus K_n$ 得到随机数 r，然后计算 $F(IDS\oplus r)$。此外，标签还可以通过 $ID\oplus F(IDS\oplus r)\oplus F(IDS\oplus r)$ 来验证 ID 的正确性。如果正确，标签开始计算 $G_{n+1}=P(G_n)$ 和 $G_{n+2}=P(G_{n+1})$，接着发送 $G_{n+1}\oplus G_{n+2}\oplus r$ 和 $G_{n+2}\oplus F(r)$ 给阅读器。最后标签更新 $IDS=F(IDS\oplus G_n\oplus K_n)$，$K_n=K_n\oplus F(K_n\oplus r)$ 和 $G_n=G_{n+1}$。

(5)根据步骤(4)，阅读器首先可以通过计算 $G_{n+1}\oplus G_{n+2}\oplus r\oplus G_{n+1}\oplus r$ 得到 G_{n+2}；然后阅读器开始验证 $G_{n+2}\overset{?}{=}G_{n+2}\oplus F(r)\oplus F(r)$ 的正确性，如果正确，阅读器就开始更新 $K_n=K_n\oplus F(K_n\oplus r)$，$G_n=G_{n+1}$ 和 $G_{n+1}=G_{n+2}$。

4　安全分析

本节将对所提出的新的认证协议进行安全性分析。新协议除了要求有较少的存储空间、较低的计算和通信开销外，还要求能抵抗假冒攻击、去同步攻击、信息泄漏攻击、重放攻击、中间人攻击、向后安全性、向前安全性、克隆攻击，同时能实现双向认证、标签的匿名性和不可分辨性。

(1)假冒攻击

在所提协议中，无论协议中消息的哪一部分被修改，标签或阅读器都是可以发现的，因为 IDS，G_n，G_{n+1}，K_n 这部分是

动态变化的，对于攻击者而言，IDS 是随机的。因此，阅读器或标签能够确认协议中的每一个消息的正确性，从而保证攻击者根本无法获得任何有价值的信息，故该协议可以抵抗假冒攻击。

(2)去同步攻击

攻击者可能会尝试去同步攻击标签和阅读器之间的 IDS,G_n。为了达到上述攻击目的，攻击者会对认证协议中的步骤(4)进行监控。为了处理这个同步问题，建议将以前的有用信息 IDS,G_n 存放在标签中。当后端数据库中未存放 IDS 时，阅读器将会告知标签使用以前的信息 IDS,G_n。

(3)信息泄漏攻击

信息泄漏攻击的关键步骤是攻击者可以对来自阅读器的消息稍微进行修改，然后从响应的标签中推导出部分有用的信息。但是在本文协议中，阅读器和标签都存放有保密数据 ID,G_n,G_{n+1},K_n，并且所有传输的信息都是随机的和保密的，所以攻击者只要修改任何一个传输的信息，此协议都将会被终止，最终攻击者将无法获取任何有用的信息。因此该协议可以抵抗信息泄漏攻击。

(4)重放攻击和中间人攻击

攻击者可能伪装成合法的标签或阅读器，从而发出重放攻击。如果攻击者伪装成合法的阅读器，那么攻击者将会重播第一条和第三条消息，但是攻击者无法成功，因为 IDS 在每一轮中都会更新，并且 IDS 在每一轮中都是随机的，而且第三条消息与 IDS 紧密相关，因此标签将很快发现系统遭受攻击。如果攻击者伪装成合法的标签，那么攻击者将会重播第二条和第四条信息，同样，攻击者也无法成功，因为 IDS,G_n,G_{n+1},K_n 这部分早已经更新，并且消息与这部分是紧密相关的。当攻击者发起中间人攻击时，也不可能成功，因为第二条、第三条和第四条消息都是动态的，并且攻击者缺少必要的参数信息，比如 ID,G_n,G_{n+1},K_n。

(5)向后安全性和向前安全性

本文所提出的协议可以阻止攻击者获取标签信息，通过数据的加密传输来响应消息中的每一个会话。此外，IDS 在每次认证之后都会更新，对于攻击者而言，IDS 是随机的；当阅读器和标签成功认证完成之后，便会更新 G_n,G_{n+1},K_n；随机数 r 是由阅读器随机产生的，通过断开先前发送的信息和未来发送的信息的关系，来保证该协议的后向安全性和前向安全性。

(6)克隆攻击

为了抵抗克隆攻击，本文协议在标签中使用独特的 PUF 技术。PUF 是不可克隆的，因此不可能生产出两个一模一样的 PUF 函数，所以即使攻击者复制或克隆本协议中用到的 PUF 也是无意义的，故该协议可以抵抗克隆攻击。

(7)匿名性和不可分辨性

匿名是指攻击者无法识别标签的身份且无法跟踪标签；不可分辨是指攻击者无法确定消息来源于哪个标签。本文协议通过采用 PUF 函数、LFSR 函数以及随机数产生器来保护标签的认证信息，从而确保只有合法的对象才可以获取 ID，G_n,G_{n+1},K_n。此外，如前面所述，该协议不仅具有后向安全性和前向安全性，而且能够保证匿名性和不可分辨。

(8)双向认证

本文协议提供了标签和阅读器之间的相互认证，标签通过 ID 来认证阅读器，阅读器通过 G_{n+1} 来认证标签。该协议满足所有的安全要求，彻底解决了 RFID 系统中存在的隐私和伪造问题。

下面讨论本文协议是如何解决 Kulseng 等人的协议中存在的 3 种不同的安全隐患问题的。

(1)消息阻塞攻击

抵抗消息阻塞攻击的方法与抵抗去同步攻击的方法一样。IDS,G_n 存放在标签中，如果后端数据库没有查找到 IDS，阅读器告知标签采用以前的 IDS 进行计算。

(2)去同步攻击

攻击者如果尝试插入任何消息去破坏协议的同步性，将会导致协议两端的元素无法获得正确的认证信息，任何部位消息的改变都会被阅读器或标签所察觉。例如：将一个随机数 n_x 插入到步骤(4) $G_{n+1}\oplus G_{n+2}\oplus r$ 和 $G_{n+2}\oplus F(r)\oplus n_x$ 中，对于本文协议来言，这次攻击是失败的，因为阅读器会发现 $G_{n+2}\neq G_{n+2}\oplus F(r)\oplus n_x\oplus F(r)$。

(3)LFSR 的误用

在本文协议中，LFSR 的使用不会泄漏标签的任何有用信息。假使攻击者获取了一个完整的认证过程中的所有消息，当攻击者给标签发送假的查询命令后，标签会将 $IDS_{new}=F(IDS_{dd}\oplus G_n\oplus K_n)$ 发送给攻击者；攻击者可以从 $F(IDS_{dd}\oplus G_n\oplus K_n)$ 中获取 $IDS_{dd}\oplus G_n\oplus K_n$，从而进一步获得 $G_n\oplus K_n$；但是，这些都是没有任何价值的，因为仅仅只靠获取的 $G_n\oplus K_n$ 和先前发送的消息是无法跟踪标签的。

表 1 对本文协议与 Kulseng 等人的协议进行比较。Y 表示具有抗攻击能力，N 表示不具有抗攻击能力。

表 1 本文协议与 Kulseng 等人的协议的比较

攻击类型	Kulseng 等人的协议	本文协议
假冒攻击	N	Y
去同步攻击	N	Y
信息泄漏攻击	N	Y
重放攻击和中间人攻击	N	Y
后向安全和前向安全	N	Y
克隆攻击	Y	Y
匿名性和不可分辨	N	Y
双向认证	Y	Y

结束语 RFID 技术为多个领域带来了巨大的利益，同时也为企业和个人提供了多种应用。与其他技术一样，RFID 技术也面临着类似的安全问题：身份验证、保密性和可用性。对于不安全的 RFID 系统，用户的隐私面临极大的威胁；同时，应当避免使用复杂的加密计算，以降低设备的成本。本文在充分分析前人工作的基础上提出了一种新的轻量级 RFID 双向认证协议。通过分析，该协议能够抵抗各种类型的常见攻击，满足所有的安全要求，并且协议所需的门电路总数较少，非常适用于轻量级的 RFID 系统。

参 考 文 献

[1] ZHOU S J, ZHANG W Q, LUO J Q. Overview of radio frequency identification (RFID) privacy protection technology [J]. Journal of Software, 2015, 26(4): 960-976. (in Chinese)
周世杰，张文清，罗嘉庆. 射频识别(RFID)隐私保护技术综述[J]. 软件学报，2015，26(4)：960-976.

(下转第 227 页)

Ninth European Conference on Computer Systems. ACM, 2014: 1-15.

[5] SHA H M, CHEN X, ZHUGE Q, et al. Designing an efficient persistent in-memory file system[C]// IEEE Non-Volatile Memory System and Applications Symposium (NVMSA). IEEE, 2015.

[6] LEE E, HOON YOO S, BAHN H. Design and Implementation of a Journaling File System for Phase-Change Memory[J]. IEEE Transactions on Computers, 2015, 64(5): 1349-1360.

[7] NORCOTT W D, CAPPS D. Iozone filesystem benchmark[J/OL]. http://www.iozone.org.

[8] REDEH O, BACIK J, MASON C. BTRFS: The Linux B-tree filesystem[J]. ACM Transactions on Storage (TOS), 2013, 9(3): 317-318.

[9] PRABHAKARAN V, ARPACI-DUSSEAU A C, ARPACI-DUSSEAU R H. Analysis and Evolution of Journaling File Systems [C]// USENIX Annual Technical Conference. General Track, 2005: 105-120.

[10] ZHENG L C, SUN Y L. The Implementation of Journaling File system on Embedded Memory Device [J]. Computer Science, 2002, 29(1): 72-74. (in Chinese)
郑良辰，孙玉芳. 日志文件系统在嵌入式存储设备上的实现[J]. 计算机科学，2002，29(1)：72-74.

[11] JOSEPHSON W K, BONGO L A, LI K, et al. DFS: A file system for virtualized flash storage[J]. ACM Transactions on Storage (TOS), 2010, 6(3): 37-47.

[12] ROSENBLUM M, OUSTERHOUT J K. The design and implementation of a log-structured file system[J]. ACM Transactions on Computer Systems (TOCS), 1992, 10(1): 26-52.

[13] WAN H, XU Y C, YAN J F, et al. Mitigating Log Cost through Non-Volatile Memory and Checkpoint Optimization [J]. Journal of Computer research and Development, 2015, 52(6): 1351-1361. (in Chinese)
万虎，徐远超，闫俊峰，等. 通过非易失存储和检查点优化缓解日志开销[J]. 计算机研究与发展，2015，52(6)：1351-1361.

[14] LI T, LIANG H L. Design and Implement of Event-recovery File System [J]. Computer Science, 2009, 36(3): 270-272. (in Chinese)
李涛，梁洪亮. 具有事件恢复功能的文件系统的研究与实现[J]. 计算机科学，2009，36(3)：270-272.

[15] RAOUX S, BURR G W, BREITWISCH M J, et al. Phase-change random access memory: A scalable technology[J]. Ibm Journal of Research & Development, 2008, 52(4/5): 465-480.

[16] PARKIN S S P, MASAMITSU H, LUC T. Magnetic Domain-Wall Racetrack Memory[J]. Science, 2008, 320(5873): 190-194.

[17] MATHUR A, CAO M, BHATTACHARYA S, et al. The new ext4 filesystem: Current status and future plans[C]// Proceedings of the Linux Symposium. 2007.

(上接第 208 页)

[2] JIN Y M, WU Q Y, SHI Z Q, et al. RFID Lightweight Authentication Protocol Based on PRF[J]. Journal of Computer Research and Development, 2014, 51(7): 1506-1514. (in Chinese)
金永明，吴棋滢，石志强，等. 基于 PRF 的 RFID 轻量级认证协议研究[J]. 计算机研究与发展，2014，51(7)：1506-1514.

[3] LU L. Wireless Key Generation for RFID System[J]. Chinese Journal of Computers, 2015, 38(4): 822-832. (in Chinese)
鲁力. RFID 系统密钥无线生成[J]. 计算机学报，2015，38(4)：822-832.

[4] WANG L M, YI X L, LV C, et al. Security Improvement in Authentication Protocol for Gen-2 Based RFID System[J]. JCIT, 2011, 6(1): 157-169.

[5] ZHANG J S, WANG W D, MA J, et al. A Novel Authentication Protocol suitable to EPC Class 1 Generation 2 RFID system[J]. JCIT, 2012, 7(3): 259-266.

[6] AVOINE G, LAURADOUX C, MARTIN T. When Compromised Readers Meet RFID[C]// Workshop on Information Security Applications (WISA'09). 2009: 36-50.

[7] LU L, HAN J, HU L, et al. Dynamic key-updating: Privacy-preserving authentication for rfid systems[C]// Fifth Annual IEEE International Conference on Pervasive Computing and Communications. 2007: 13-22.

[8] SONG B, MITCHELL C J. RFID authentication protocol for low-cost tags[C]// Proceedings of the First ACM Conference on Wireless Network Security. 2008: 140-147.

[9] LO N W, YEH K H. An efficient mutual authentication scheme for epcglobal class-1 generation-2 rfid system[C]// Proceedings of the 2007 Conference on Emerging Direction in Embedded and Ubiquitous Computing. 2007: 43-56.

[10] ALOMAIR B, CUELLAR J, POOVENDRAN R. Scalable RFID systems: A privacy-preserving protocol with constant time identification [J]. IEEE Trans on Parallel and Distributed Systems, 2012, 23(8): 1-10.

[11] GODOR G, IMRE S. Hash-based mutual authentication protocol for low-cost RFID systems[C]// Proc of the 18th EUNICE Conf on Information and Communications Technologies. Berlin: Springer, 2012: 76-87.

[12] MAMUN M S I, MOUAKJI A, RAHMAN M S. A secure and private RFID authentication protocol under SLPN problem[C]// Proc of the 6th Int Conf on Network and System Security. Berlin: Springer, 2012: 476-489.

[13] WANG S H, LIU S J, CHEN D W. Scalable RFID Mutual Authentication Protocol with Backward Privacy [J]. Journal of computer Research and Development, 2013, 50(6): 1276-1284. (in Chinese)
王少辉，刘素娟，陈丹伟. 满足后向隐私的可扩展 RFID 双向认证方案[J]. 计算机研究与发展，2013，50(6)：1276-1284.

[14] BOLOTNYY L, ROBINS G. Physically unclonable function-based security and privacy in RFID systems[C]// Fifth Annual IEEE International Conference on Pervasive Computing and Communications. 2007: 211-220.

[15] KULSENG L, YU Z, WEI Y, et al. Lightweight mutual authentication and ownership transfer for rfid systems[C]// Proceedings of the 29th Conference on Information Communications. 2010: 251-255.

[16] KARDAS S, AKGUN M, KIRAZ M S, et al. Cryptanalysis of Lightweight Mutual Authentication and Ownership Transfer for RFID Systems[C]// Workshop on Lightweight Security & Privacy: Devices, Protocols, and Applications. 2011: 20-25.