第37卷　第21期　　　计 算 机 工 程　　　2011年11月
Vol.37　No.21　　　Computer Engineering　　　November 2011

·开发研究与设计技术·　　文章编号：1000—3428(2011)21—0249—03　　文献标识码：A　　中图分类号：TP393.02

基于PUF的RFID协议分析与改进

马昌社，王　涛，王立斌

(华南师范大学计算机学院，广州 510631)

摘　要：对一个基于PUF构造的低成本RFID安全协议进行分析，发现该协议不能保护标签的隐私性，即任何一个攻击者通过重放协议消息就可以跟踪同一个标签。并且由于识别标签的时间复杂度和通信复杂度都与标签个数呈线性关系，因此协议不具有扩展性。为此，提出一个改进的RFID协议，使得协议在效率和安全性两方面得到改善。

关键词：射频识别；隐私性；可扩展性；物理不可克隆函数；跟踪攻击

Analysis and Improvement of RFID Protocol Based on PUF

MA Chang-she, WANG Tao, WANG Li-bin

(School of Computer, South China Normal University, Guangzhou 510631, China)

【Abstract】This paper analyses a low-cost RFID protocol based on Physical Unclonable Function(PUF). The protocol cannot guarantee the claimed privacy and is not scalable. Concretely, any adversary is able to trace the same tag by replaying the protocol messages and its computational complexity and communication overhead of identifying a tag are both linear to the number of tags. Furthermore, a new PUF based RFID protocol is proposed which beats down the protocol from both security and efficiency.

【Key words】 Radio Frequency Identification(RFID); privacy; scalability; Physical Unclonable Function(PUF); trace attack

DOI: 10.3969/j.issn.1000-3428.2011.21.085

1　概述

射频识别(Radio Frequency Identification, RFID)是一种利用射频通信实现的非接触式自动识别技术。一般地，一个RFID系统由RFID标签、阅读器和后端数据库3个部分构成。近年来，RFID技术已应用于零售业、道路自动收费、图书管理等领域。

尽管目前RFID技术在工业界得到了大量的关注，但安全问题、可扩展性问题以及成本问题是制约RFID技术能否在工业界得到广泛应用的3大关键因素。安全领域的学者们设计了一系列RFID协议来增强RFID系统的安全性。考虑到RFID标签的成本问题，这些协议大多采用轻量级密码算法。实际上，目前安全的轻量级密码算法仍不能在低成本的标签上得以实现。因此，基于协议设计的RFID标签，其生产成本仍不能满足工业界的要求。

但是物理不可克隆函数(Physical Unclonable Function, PUF)的发明，给低成本RFID标签的设计带来了曙光。基于PUF和LFSR，文献[1]设计了一个低成本的RFID协议(称为YY协议)，其标签能符合EPC Generation 1 Class 2的要求[2]。文献[1]宣称YY协议满足RFID的各种安全要求，特别地，可以保证标签的隐私性，即具有不可跟踪性。本文对YY协议进行分析，并提出了一个新的基于PUF和LFSR的RFID协议。

2　RFID系统安全相关研究

目前，业界提出了若干RFID隐私安全解决方案和协议，但是它们大部分都存在这样或那样的问题：要么不具有安全性，要么不具有可扩展性。

基于树的结构，文献[3]首次提出了一个具有可代理特性的RFID认证系统，然而该系统不能抵抗主动攻击。因为被动式RFID标签是无源的，它的硬件系统不具有任何防篡改技术，任何一个恶意的阅读器可以访问并设置该标签。设计RFID能够抵抗主动攻击是最起码的安全要求。在基于树而设计的RFID系统，所有标签需要或多或少地共享某些秘密信息，读取某一标签的内部状态，就可以把它用来攻击其他标签的隐私性。所以，基于树设计的RFID系统都不能抵抗主动跟踪攻击。

基于哈希函数，文献[4]设计了一个简单安全的RFID系统，但是该系统的可扩展性很差，因为阅读器端识别标签所需要的计算量与RFID系统中标签的数目呈线性关系。这制约了OSK不能用于标签数目比较大的应用场合。后来的研究者们采用状态同步，并结合哈希链提出了各种各样的RFID协议[5]，这些协议中大部分仍不具有安全性[5]。因此，设计简单、实用且安全的RFID协议仍是研究者们主要工作所在。

3　YY协议描述

这里首先介绍文献[1]中的RFID认证协议，YY协议由以下2个阶段组成：初始化阶段和搜索阶段。对于PUF函数和LFSR的介绍请参阅文献[1]，这里不再赘述。

3.1　初始化阶段

通过初始化阶段，在阅读器和标签之间共享了3个参数，并设置了标签的PUF函数P。

(1) ID_T：ID_T是标签的身份。

(2)密钥K：K是阅读器和标签之间共享的认证密钥。

(3)随机置换函数L：L是一个由LFSR构成的伪随机数发生器。

基金项目：国家自然科学基金资助项目(61070217)

作者简介：马昌社(1974－)，男，博士，主研方向：信息安全，射频识别；王　涛、王立斌，博士

收稿日期：2011-04-25　　**E-mail：**changshema@gmail.com

最后，系统还需要设置好标签上的 PUF 函数 P，同时保存该函数的一个输入输出对 (G_n, G_{n+1})，这里 $G_{n+1} = P(G_n)$。这样，系统为该标签保存 (ID_T, K, G_n, G_{n+1}) 在后端数据库中。

3.2 搜索阶段

搜索阶段是 RFID 协议的执行阶段或标签的识别阶段，主要由以下步骤组成(如图 1 所示)。其中，$m_1 = R_n \oplus ID_T$；$m_2 = R_n^1 \oplus K$；$m_3 = R_n^2 \oplus G_n$；$m_4 = R_n^3 \oplus G_{n+1}$；$m_5 = R_n^4 \oplus G_{n+2}$。$R_n$ 是阅读器选择的随机数，且 $R_n^1 = L(R_n)$，$R_n^2 = L(R_n^1)$。

步骤 1 阅读器在其后端数据库中随机选取一条记录 (ID_T, K, G_n, G_{n+1})，然后广播消息 m_1, m_2, m_3。

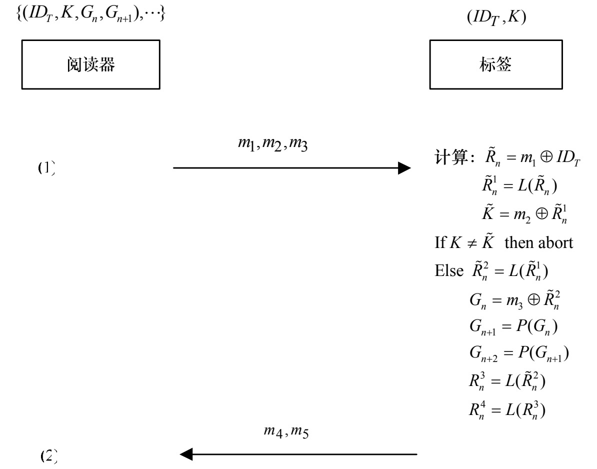
$\{(ID_T, K, G_n, G_{n+1}), \cdots\}$
(ID_T, K)
阅读器
标签
m_1, m_2, m_3
(1)
计算：$\tilde{R}_n = m_1 \oplus ID_T$
$\tilde{R}_n^1 = L(\tilde{R}_n)$
$\tilde{K} = m_2 \oplus \tilde{R}_n^1$
If $K \neq \tilde{K}$ then abort
Else $\tilde{R}_n^2 = L(\tilde{R}_n^1)$
$G_n = m_3 \oplus \tilde{R}_n^2$
$G_{n+1} = P(G_n)$
$G_{n+2} = P(G_{n+1})$
$R_n^3 = L(\tilde{R}_n^2)$
$R_n^4 = L(R_n^3)$
m_4, m_5
(2)

图 1 YY 协议

步骤 2 每一个标签收到广播消息后，按图 1 所示进行计算，如果验证通过就发送消息 m_4, m_5 给阅读器。

步骤 3 阅读器收到消息 m_4, m_5 后，计算 $R_n^3 = L(R_n^2)$、$R_n^4 = L(R_n^3)$ 和 $\tilde{G}_{n+1} = m_4 \oplus R_n^3$，如果 $\tilde{G}_{n+1} = G_{n+1}$，那么对标签的认证通过，并设置 $G_n = G_{n+1}$ 和 $G_{n+1} = G_{n+2}$；否则，对标签的认证不通过。

4 YY 协议的分析

4.1 可跟踪攻击

文献[1]宣称 YY 协议能够抵抗跟踪攻击，实际上，YY 协议不具有这一属性。对 YY 协议的跟踪攻击如下：攻击者 A 首先通过窃听技术截获 YY 协议的第 1 轮挑战消息 m_1, m_2, m_3 和第 2 轮应答消息 m_4, m_5。

假设发出应答的标签为 T^*，接下来攻击者 A 就可以跟踪 T^*：攻击者 A 重放挑战消息 m_1, m_2, m_3 询问某个目标标签，如果该标签返回应答消息 m_4', m_5'，攻击者 A 比较 $m_4 = m_4'$ 和 $m_5 = m_5'$。如果都相等，就认为目标标签是 T^*，从而实现了对 T^* 的跟踪。根据 YY 协议，对于标签 T^* 而言，只要挑战消息 m_1, m_2, m_3 保持不变，那么其应答消息也会保持不变，这就是 YY 协议可以被跟踪的主要原因。

4.2 效率分析

根据 YY 协议，如果身份为 ID_T 的标签不在阅读器的广播范围之内，就会导致阅读器对标签的识别失败。并且阅读器不能事先知道进入其广播范围的标签的身份，因此，为了实现对一个标签的识别，阅读器采用试探的方法，逐次以不同的 ID_T 和对应的 G_n 生成协议的第 1 轮挑战消息。假设 RFID 系统有 n 个标签，每一个标签进入阅读器的广播范围的概率均为 p，那么阅读器能够以大于 1/2 的概率识别某个标签所需要的时间至少为 T_L / p，所需的通信轮数至少为 1/2p+1 轮。这里仅考虑函数 L 计算所需要的时间，而忽略了其他计算所需要的时间，假设一次 L 函数计算所需时间为 T_L。一般地，取 $p = 1/n$，那么阅读器识别一个标签所需要的时间至少为 $n \cdot T_L$，所需要的通信轮数至少为 $n/2+1$ 轮。如果 RFID 系统中标签数目较多，比如中等规模的 RFID 系统中标签至少有 2^{20} 个，那么识别一个标签所需要通信轮数至少为 2^{19} 轮，完成这么多轮通信所需要的时间大约为 $2^9 = 512$ s，假设 1 s 内一个阅读器可以完成 2^{10} 轮通信。显然，这样的 RFID 不具有实用性。

5 基于 PUF 的新 RFID 协议

基于 PUF 和 LFSR 提出一个新的 RFID 协议，新协议从安全和效率 2 个方面改善 YY 协议。新协议由 2 个阶段组成：初始化阶段和标签识别阶段。

5.1 初始化阶段

初始化阶段步骤如下：

(1)在标签上设置一个 PUF 函数 P，并赋予其一个初始输入 S，然后得到 $K = P(S)$。

(2)为标签选择一个初始索引 I_0，并把 I_0 存储在标签中。

(3)设置标签中的 LFSR 函数 L，并计算 $L_1 = L(K \oplus I_0)$。

(4)把 (I_1, K, ID_T) 存入后端数据库中，这里 ID_T 是标签的身份。

5.2 标签识别阶段

对标签的识别协议如图 2 所示。

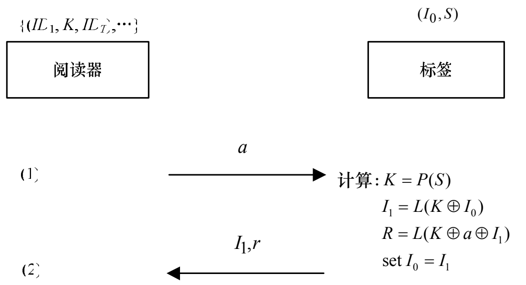

图 2 新的 RFID 协议

协议分 2 轮执行。

第 1 轮：阅读器选择一个随机的挑战消息 a，并把它发送给标签。

第 2 轮：当标签收到挑战消息 a 之后，先用 PUF 函数计算自身的密钥 $K = P(S)$，然后计算索引 $I_1 = L(K \oplus I_0)$ 和应答消息 $r = L(K \oplus a \oplus I_1)$，最后把 I_1 和 r 发送给阅读器，并更新索引 $I_0 = I_1$。

最后，当阅读器收到标签的应答消息 I_1 和 r 后，按如下方式对标签做出识别：

(1)用 I_1 做索引在后端数据库中查找 (I_1, K, ID_T)，如果没有找到就转步骤(2)，否则执行以下步骤：

计算并比较 $r = L(K \oplus a \oplus I_1)$。如果相等就返回识别成功，并标记该标签的身份是 ID_T，更新 $I_1 = L(K \oplus I_1)$；否则就返回识别失败。

(2)逐次从数据库中随机选取 $(\tilde{I}_1, \tilde{K}, ID_T)$，然后计算 $\tilde{r} = L(\tilde{K} \oplus a \oplus I_1)$，如果存在 $(\tilde{I}_1, \tilde{K}, ID_T)$ 满足 $r = \tilde{r}$，那么就返回识别成功，并标记该标签的身份是 ID_T，更新 $\tilde{I}_1 = L(\tilde{K} \oplus I_1)$；否则就返回识别失败。

6 安全分析

在 RFID 系统中，安全性要求主要在于保护用户隐私性和认证性。这里主要从认证性和隐私性 2 个方面分析本文协议的安全性。

(1)认证性

首先，在标签端采用 PUF 函数生成标签和阅读器之间的共享认证密钥这一机制，用于保护认证密钥的安全性：由于 PUF 函数具有物理上不可复制的安全属性，因此任何一个敌手都很难获得这一认证密钥。

其次，采用标准的基于询问——应答模式的认证协议对标签做出认证，这种模式能够抵抗重放攻击等各种类型的身份冒充攻击，从而保证了协议运行的认证性和正确性。

(2)隐私性

跟踪攻击是威胁用户隐私最主要的一种攻击手段，在这种攻击中，敌手通过观测阅读器和标签之间的通信跟踪同一个标签。

在本文的新协议中，采用随机化技术随机化每一轮协议消息，从而使敌手无法区分 2 个标签与阅读器之间的通信。在新协议中，询问消息 a 是由阅读器选取的随机数，标签的应答消息 I_1 和 r 也是伪随机的。如果把 LSFR 看成是一个伪随机数发生器，从这个意义上来说，丢手无法区分任意 2 个标签和阅读器之间的通信，从而无法跟踪同一个标签。另一方面，采用随机的伪 ID 方法传递标签的身份，在通信没有泄露任何关于标签身份的信息。因此，新协议保证了标签的隐私性。

7 效率分析

对于 RFID 系统，设计认证协议除了要考虑安全性之外，协议的性能也是至关重要的。下面从计算复杂性和通信复杂性 2 个方面对本文协议和 YY 协议进行分析和比较，如表 1 所示。假设 RFID 系统中有 n 个标签，为了分析和比较的方便，把 PUF 函数的计算和 LFSR 的计算看作具有相同的计算开销 t，同时忽略其他计算所需的开销。

表 1 效率比较

协议	计算开销	通信轮数
YY 协议[1]	$O(10n)\,t$	$O(n)$
本文协议	$5\,t$	2

从表 3 可以看出，无论从计算开销还是从通信开销考虑，本文协议都要优于 YY 协议。具体地说，识别一个标签，YY 协议需要 $O(10n)t$ 的计算代价，而本文协议仅需要 $5t$ 的计算代价。就通信开销方面来说，识别一个标签，YY 协议需要 $O(n)$轮通信，而本文协议仅需要 2 轮通信。

8 结束语

本文对一个基于 PUF 的低成本 RFID 系统的隐私性和效率进行了分析，提出了一个安全实用的 RFID 认证协议和系统。安全分析和效率比较表明：本文协议可以抵抗身份冒充攻击、重放攻击等认证方面的攻击，同时还能抵抗跟踪攻击等隐私性方面的攻击。本文协议的通信复杂性和计算复杂性都要优于其他基于 PUF 函数设计的 RFID 协议。

参考文献

[1] 杨 灵, 闫大顺. 基于 PUF 的低成本 RFID 系统安全协议[J]. 计算机工程, 2010, 36(15): 148-150, 155.

[2] EPCglobal. EPC Radio-frequency Identity Protocols[EB/OL]. (2005-01-30). http://www.epcglobalinc.org.

[3] Molnar D, Wagner D. Privacy and Security in Library RFID: Issues, Practices, and Architectures[C]//Proc. of the 11th ACM Conference on Computer and Communications Security. Washington D. C., USA: ACM Press, 2004.

[4] Ohkubo M, Suzuki K, Kinoshita S. Efficient Hash-chain Based RFID Privacy Protection Scheme[C]//Proc. of International Conference on Ubiquitous Computing. Nottingham, England, UK: [s. n.], 2004.

[5] Deursen T, Radomirovic S. Attacks on RFID Protocols[EB/OL]. (2008-03-10). http://eprint.iacr.org/2008/310.

编辑 顾逸斐

(上接第 240 页)

过程基本相同，不同的是首先要从 ROM 中读出通过电路故障模拟得到的测试矢量。当移位操作 16 次之后，判断 Nchain 信号，如果为高电平则继续移位，直到 Nchain 为低电平才结束一个矢量的施加[6]。

4.5 测试判断

如果在测试开始时读到全 0 指令，就表示测试过程结束，将使电路进入正常工作模式。

5 结束语

本文在研究了内建自测试原理的基础上自主设计了一个混合测试模式下工作的 BIST 控制器，给出了各功能模块的具体实现方案，设计工作流程，并用 VHDL 语言在 Quartus II 软件中加以实现，通过了对所设计 BIST 控制器进行功能仿真和验证。

该芯片级 BIST 控制器已用于某型航电设备的自检测电路，测试使用效果良好，已初步达到其自检测电路要求。今后要进一步对各个功能模块进行优化设计。

参考文献

[1] 晏新晃, 茹惠素, 吴荣泉. 高速边界扫描主控器设计[J]. 计算机工程, 2009, 35(1): 210-212.

[2] Dufaza C. Theoretical Properties of LFSRs for Built-in Self Test[J]. the VLSI Journal on Integration, 1998, 25(1): 17-35.

[3] 段军棋. 基于边界扫描的测试算法和 BIST 设计技术研究[D]. 成都: 电子科技大学, 2004.

[4] 于 薇, 来金梅, 孙承绶, 等. FPGA 芯片中边界扫描电路的设计实现[J]. 计算机工程, 2007, 33(13): 251-254.

[5] 吴继娟, 孙媛媛, 刘桂艳. 基于 BIST 的 FPGA 逻辑单元测试方法[J]. 哈尔滨工业大学, 2004, 36(8): 1074-1076.

[6] Tehranipour M H, Navabi Z. An Efficient BIST Method for Testing of Embedded SRAMs[C]//Proc. of IEEE International Symposium on Circuits and Systems. Sydney, Australia: IEEE Computer Society Press, 2001: 73-76.

编辑 顾逸斐