第34卷 第21期 计 算 机 工 程 2008年11月
Vol.34 No.21 Computer Engineering November 2008
·博士论文· 文章编号：1000—3428(2008)21—0018—02 文献标识码：A 中图分类号：TP309.2

基于PRNG的低成本RFID认证协议设计

祝胜林[1,2]，杨 波[1]，张明武[1]，胡月明[1]
(1. 华南农业大学信息学院，广州 510642；2. 中山大学广东省信息安全技术重点实验室，广州 510275)

摘 要：低成本无线射频识别(RFID)的标签是被动式的，由于受成本和资源限制，系统不能提供公约加密、对称密钥加密、杂凑函数等。EPCglobal Class-1 Gen-2 RFID规范定义一种低成本的标签，仅提供PRNG和CRC操作。该文遵循EPCglobal Class-1 Gen-2 RFID规范，仅使用PRNG操作设计一个认证协议，实现双向认证、标签的匿名性和前向安全性。

关键词：低成本无线射频识别；伪随机数生成器；认证协议

Design of Low-cost RFID Authentication Protocol Based on PRNG

ZHU Sheng-lin[1,2], YANG Bo[1], ZHANG Ming-wu[1], HU Yue-ming[1]
(1. College of Information, South China Agriculture University, Guangzhou 510642;
2. Guangdong Province Key Laboratory of Information Security, Sun Yat-Sen University, Guangzhou 510275)

【Abstract】 Low-cost Radio Frequency Identification(RFID) tags are passive, on account of the limitation of cost and resources, can not afford the public key encryptions, symmetric encryptions, or even hash functions. EPCglobal Class-1 Gen-2 RFID specification defines the low-cost RFID tag which only can support on-chip 16 bit Pseudo-Random Number Generator(PRNG) and a 16 bit Cyclic Redundancy Code(CRC) checksum. In this paper, an authentication protocol conforming to EPCglobal Class-1 Gen-2 RFID specification only using PRNG is proposed, and it achieves tag-to-reader and reader-to-tag authentications, the anonymity of tag and forward secrecy.

【Key words】 low-cost Radio Frequency Identification(RFID); Pseudo-Random Number Generator(PRNG); authentication protocol

1 概述

无线射频识别(Radio Frequency Identification, RFID)作为实现普适计算环境的有效且应用广泛的一项技术，可以在开放系统环境中实现对对象的识别，这种识别无需物理接触、无需直接可视，并且可以实现识别自动化。随着标签成本的降低，可代替传统的条形码而被广泛地应用于供应链管理、数字图书馆管理和智能交通等。

RFID系统由3个主要部件构成[1]：RFID标签(tag)，RFID读卡器(reader)和后台数据库(back-end database)。RFID系统的工作流程[1]：读卡器通过射频(Radio Frequency, RF)询问标签得到其唯一的ID，再以ID作为指针，到后台数据库查找到该标签所标识对象的描述信息。显然，如果标签允许被任何读卡器询问得到它的ID，就会出现隐私(privacy)问题和由此而产生的可追踪(tracking)问题，为了解决这些问题，需要在工作流程中增加认证功能。

2 低成本RFID及其认证协议

RFID标签根据能量的来源[1]可分为：(1)主动式标签，主动向读卡器发送射频信号，通常由内置电池供电，又称为有源标签。(2)被动式标签，不带电池，工作能量来源于将接收到的读卡器发出的电磁波信号转化而成的电能。被动式标签由于价格便宜、使用方便等特点而被采用，EPCglobal Class-1 Gen-2 RFID标签就属于这样一类的低成本RFID标签。

2.1 EPCglobal Class-1 Gen-2 RFID

EPCglobal统一了2个负责条形码的最大组织(EAN和UCC)，因此，它具有在全球范围对RFID技术标准的潜在影响力。EPCglobal Class-1 Gen-2 RFID规范是EPCglobal提出的重要标准之一——Gen-2 RFID。

Gen-2 RFID标签具有如下特性[2]：(1)Gen-2RFID标签是被动式的，通信频段为800 MHz~ 960 MHz，通信范围在2 m~10 m。(2)Gen-2 RFID标签，由于受成本和资源的限制，不能提供成本昂贵的公钥加密、对称密钥加密，或者甚至Hash函数。它仅支持单片16 bit伪随机数生成器(Pseudo-Random Number Generator, PRNG)和用于数据传输过程中探测错误的循环冗余码(Cyclic Redundancy Code, CRC)校验。(3)Gen-2 RFID的隐私保护机制使用Kill命令，即标签一旦接收带有合法的32 bit Kill PIN的Kill命令，将永久不可再用。(4)Gen-2 RFID标签接收带有有效的32 bit Access PIN的存取命令后进入安全模式，仅在该模式下对它的内存进行读/写操作才被允许。

所以，利用Gen-2 RFID标签的有限资源设计认证协议提高它的安全特性，是一项具有挑战性的工作。

2.2 RFID系统具有认证功能的工作流程

一般地，具有认证功能的RFID系统工作流程具有如下步骤[3]：

(1)读卡器向标签提出询问请求。

基金项目：国家自然科学基金资助项目(40671145)；现代通信国家实验室基金资助项目(9140c1108010606)；广东省信息安全技术重点实验室开放基金资助项目(H06002)

作者简介：祝胜林(1969－)，男，副教授、博士研究生，主研方向：信息安全，数据库理论与技术；杨 波，教授、博士生导师；张明武，副教授、博士研究生；胡月明，教授、博士生导师

收稿日期：2008-01-24 **E-mail：**zhusl@scau.edu.cn

(2)标签对读卡器的询问进行响应。

(3)读卡器将标签的响应消息转送到后台数据库；后台数据库根据认证协议验证该标签是否为合法标签。

(4)如果该标签被验证合法，后台数据库就根据读卡器的权限将该标签所标识对象的描述信息传送给它；如果该标签被验证为不合法，则该标签被拒绝。

(5)如果认证协议是双向的，标签还需要认证读卡器。后台数据库经读卡器转送进一步地认证消息，如果标签能够验证该消息为有效，标签就更新其用于认证的数据，否则标签不进行任何更新。

2.3 遵循 Gen-2 RFID 规范的认证协议

针对 RFID 标签的安全威胁，近几年来已经有不少安全协议被提出来，但它们大部分使用了 Hash 函数或加密函数，与 Gen-2 RFID 规范不相符。目前，仅有极少的协议遵循了 Gen-2 RFID 规范，譬如：文献[4]提出了一个模式防止克隆的标签假冒合法的标签；基于简单的异或(XOR)操作和矩阵操作，文献[5]设计了一个有效的标签识别和 Reader 认证模式；文献[6]使用 PRNG 和 CRC 操作，设计了一个协议实现了 reader-to-tag 和 tag-to-reader 的认证，通过通信流量加密和隐私保护以防止追踪。

借鉴文献[6]，本文不采用 CRC 操作，而仅使用 PRNG 操作来设计认证协议。

3 仅使用 PRNG 的低成本 RFID 认证协议

3.1 PRNG

伪随机数产生的形式有多种，本文采用线性同余算法：

$$r_{i+1} = (ar_i + b) \bmod N$$

其中，a,b和N是PRNG的参数；r_0是PRNG的种子。当参数确定后，PRNG产生的随机序列决定于种子，即不同种子产生不同随机序列，而相同种子产生 2 条完全相同的序列。

Gen-2 RFID标签生成的 16 bit伪随机数具有如下属性[3]：

(1)单一 16 bit 数 x 被抽到的概率范围为

$$\frac{0.8}{2^{16}} < probability(x) < \frac{1.25}{2^{16}}$$

(2)在 10 000 个标签中，任何 2 个标签同时生成一样的 16 bit 伪随机数的机会不到 0.1%。

(3)假设攻击者知道 PRNG 所有先前的输出，但标签生成的下一个伪随机数被猜中的概率还是不到 0.25%。

3.2 符号说明

下面将协议流程中用到的符号作一个简单说明：

(1)T 表示 Gen-2 RFID 标签。

(2)R 表示 RFID 阅读器。

(3)S 表示后台数据库系统(服务器)。

(4)EPC 表示产品电子码(electronic product code)类似于条形码，是生产厂家为每个标签分配的独一无二的代码。

(5)PIN 表示个体身份识别码(personal identification number)，是 T 和 S 间长期共享的秘密，执行 Kill 和 Access 命令需要附带 PIN。

(6)$srand(\cdot)$表示设置伪随机函数的种子，如：$srand(1\ 238)$，表示伪随机函数种子为 1 238。

(7)$r=rand()$表示从伪随机序列中得到一个随机数并存入到 r 中。

(8) r_S^i 和 r_T^i 分别表示 S 和 T 的随机数，i 表示序号。

(9) $\oplus$ 表示异或操作。

(10)$\|$表示连接操作。

(11)A 表示在实体 A 这边发生的动作。

(12)$A \rightarrow B$ 表示从 A 到 B 的通信。

(13) $A \leftrightarrow B$ 表示 A 和 B 之间的交互。

3.3 协议流程

该协议包括 2 个阶段：初始化阶段和认证阶段。

3.3.1 初始化阶段

Gen-2 RFID 标签存储了一个 EPC, 1 个随机的 PIN 和 1 个后台数据库选定的随机的种子 $seed$ 3 个数，而在后台数据库中也同样存储有这 3 个数。每一轮认证结束后，S 和 T 中的 PIN 和 $seed$ 必须更新。

3.3.2 认证阶段

仅使用 PRNG 的认证协议执行步骤如下：

(1)$R \rightarrow T$：读卡器向标签发出询问请求。

(2)T：生成一个一次性随机数 r，再设置 PRNG 的种子 $srand(seed)$，得到第 1 个随机数 $r_T^1 = rand()$，计算

$$M_1 = EPC \oplus r_T^1 \oplus r$$

其中，$r < r_T^1$。

(3)$T \rightarrow R$: M_1, r。

(4) $R \leftrightarrow S$: R 和 S 相互认证，譬如：使用 SSL。认证通过后，R 将 M_1 和 r 转发给 S。

(5)S：对后台数据库中的每一个元组(EPC,$seed$)，首先设置PRNG的种子$srand(seed)$，再得到第一个随机数 $r_S^1 = rand()$，最后验证 $EPC \oplus r_S^1 \oplus r$ 与M_1是否相等，如果没有符合条件的元组被发现，该标签就被拒绝并且协议结束。如果找到了符合条件的元组继续下一步操作。

(6)$S \rightarrow R$：从随机序列中再取两个随机数 r_S^2 和 r_S^3，计算

$$M_2 = PIN \oplus (r_S^2 \| r_S^3)$$

将 M_2 和根据 R 的权限得到的被标识对象的描述信息转发给 R。同时，从随机序列中继续取出 1 个随机数更新 $seed$，再继续取出 2 个随机数连接起来作为对 PIN 的更新。

(7)$R \rightarrow T$： M_2。

(8)T：从随机系列中取 2 个随机数 r_T^2 和 r_T^3，验证 $PIN \oplus (r_T^2 \| r_T^3)$ 与 M_2 是否相等，如果相等，从随机序列中继续取出 1 个随机数更新 $seed$，再继续取出 2 个随机数连接起来作为对 PIN 的更新，否则结束协议且不做任何更新。

4 安全性和复杂性分析

本文协议与文献[6]协议一样实现了双向认证，标签的匿名性和隐私保护，克服文献[6]协议不能实现的前向安全性。

(1)双向认证。标签对读卡器的询问请求作出响应，后台数据库利用与标签共享的秘密对标签进行认证，如果收到的 M_1 与计算的值相等，则标签被认证(tag-to-reader)；标签利用本身存储的数据验证来自读卡器的 M_2，如果计算的值与 M_2 相等，则读卡器被认证(reader-to-tag)。

(2)标签的匿名性。标签每次以 $M_1 = EPC \oplus r_T^1 \oplus r$ 响应读卡器的询问请求，由于每次 r 的值都在变化，这样读卡器每次得到的响应都不同，另外，EPC 从来没有被明文方式传送，因此，实现了标签的匿名性和隐私保护，并且防止了被跟踪。

(3)前向安全性。假设敌手已经获得一个标签的 EPC 和对应的 PIN，并且已经偷听到了 M_1, M_2, r，那么

$$M_1 \oplus M_2 + r = EPC \oplus PIN \oplus r_T^1 \oplus r_S^2 \oplus r_S^3$$

由于每次认证成功都要进行种子更新，因此随机数序列

（下转第 22 页）