**引用格式**:甘勇,李天豹,贺蕾,等. 基于动态重载的 RFID 标签所有权转换协议研究[J]. 轻工学报,2016,31(2):97 – 102.
**中图分类号**:TP309 **文献标识码**:A
**DOI**:10.3969/j.issn.2096 – 1553.2016.2.013
**文章编号**:2096 – 1553(2016)02 – 0097 – 06

# 基于动态重载的 RFID 标签所有权转换协议研究

## Research on ownership transfer protocols of RFID tags based on dynamic overload

甘勇,李天豹,贺蕾,许允倩
GAN Yong, LI Tian-bao, HE Lei, XU Yun-qian

郑州轻工业学院 计算机与通信工程学院, 河南 郑州 450001
*College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450001, *China*

**关键词**:
RFID 标签;动态重载;所有权转换;安全隐私

**Key words**:
RFID tag; dynamic overload; ownership transfer; security and privacy

**摘要**:针对 RFID 标签在认证授权及所有权转换过程中存在的安全隐私问题,结合类编程思想和重载原理,提出一种基于动态重载的 RFID 标签所有权转换协议. 其要点为:在 PUF 部件的基础上改进伪随机序列生成器的迭代机制,以芯片产生的自编译扩展因子增强输出的随机性;为通信双方构建轻量级候选函数集,利用面向对象编程中的“重载”原理实现所有权转换过程中算法的动态执行. 协议安全性及计算开销分析对比结果表明,新协议在认证授权的基础上提供标签所有权的安全转移,与同类协议相比具有较高的安全性和较低的计算开销.

**收稿日期**:2015 – 05 – 19
**基金项目**:国家自然科学基金项目(61340059)

**作者简介**:甘勇(1965—),男,湖南省株洲市人,郑州轻工业学院教授,博士,主要研究方向为分布式计算机系统、计算机网络、信息安全.

**Abstract**: Aiming at security and privacy issues existing in the process of authentication and authorization of RFID tags ownership transfer, combining with the principles of Class-Programming and overload, a RFID tag ownership transfer protocol based on dynamic overload was presented. It improved iterative mechanism of pseudo-random sequence generator on the basis of an PUF component, utilized self-compiling extension factor generated by chips to enhance randomness of output, constructed lightweight set of candidate functions for both communication sides so as to achieve dynamic execution of algorithms in ownership transfer process which via the overload principle in Object-Oriented programming. The security and computing cost of protocol analysis results showed that the new protocol provided tag with secure ownership transfer on the basis of authentication efficiency and authorization, and it had higher security and lower computation cost compared with similar protocols.

## 0 引言

RFID(radio frequency identification)是一种非接触式的目标自动识别技术,有着广泛的应用前景. RFID 标签具有成本低、体积小、可重复使用等诸多优点,可在供应链环境中有效控制管理成本. 跟踪产品来源、质量、售后等环节出现的问题,会涉及标签所有权的转移,而标签设计的特点和局限性带来的潜在问题也使标签所有者的信息安全受到威胁,同时随着 RFID 的产业化,系统的安全性及隐私性要求也越来越高.

现阶段 RFID 系统的安全与隐私问题主要体现在以下两个方面:标签与读写器的数据交互基于无线信道,攻击者可能会对通信过程进行各种被动攻击或主动攻击;标签对读写器发起的访问请求作被动响应,而响应信息可能会泄露所有者个人隐私信息,同时会暴露所有者物理位置,从而使标签存在被跟踪的危险.

国内外学者对标签所有权转换的安全隐私问题进行了多方面的研究. K. Osaka 等[1]提出了基于 Hash 函数和对称密码体制的 RFID 安全协议,通过改变对称密钥保护原所有者和新所有者隐私,该协议运算量适中,但标签存在遭受跟踪和 DoS 攻击的隐患;L. Kulseng 等[2]提出了采用物理不可克隆功能(PUF)和线性反馈移位寄存器(LFSR)的所有权转移协议,该协议效率较高但需可信第三方参与,且协议未明确指出如何抵御重传攻击、异步攻击等;B. Song 等[3]提出了一个基于 Hash 链标签标识符的所有权转移协议,但该协议在所有权转移过程中有可能会遭到上一个所有者的窃听;G. Kapoor 等[4]提出了改进的所有权可转移的 RFID 协议,但其在实现安全目标时忽略了标签端的存储运算承载力,在低成本标签上不易实现;B. R. Ray 等[5]提出的通用组合安全的 RFID 通信协议安全性较好,但是每轮会话标签所有权前节点实体都要向可见性管理中心获取标签密钥,成本过高,不适用于低成本标签.

鉴于此,本文对原有用于轻量级标签的所有权安全转换理论进行创新性的移植,提出基于动态重载的标签所有权的安全转换协议,以期在降低计算量的同时解决供应链环境下标签所有权转换的安全问题.

## 1 协议设计

### 1.1 设计思路

在标签与读写器的通信过程中,对算法进行动态重载可使结构不同的算法具有一致的表述形式. 在以往协议采用随机数作为算法随机输入的基础上[6],新协议为标签设置了两个 bit 的状态位,用于服务器和标签在不同阶段的同步标识,同时本文协议重点从以下两方面加强

标签所有权转移过程中的安全隐私保护.

**1.1.1 构建轻量级伪随机数发生器** 在标签中 PUF 部件的基础上,进一步加强伪随机序列输出的随机性. 利用标签物理芯片唯一特性产生的自编译扩展因子改进伪随机序列生成器的迭代机制,使伪随机数发生器的输出随芯片而异.

伪随机序列通常情况下通过设置数学乱源产生,其周期足够长时可拥有随机序列的良好特性,同时种子很大程度上决定了伪随机序列的安全性. 本文为随机序列算法采用元件例化语句,采用自编译语言为标签物理芯片生成唯一的扩展因子 $m$,对简单的线性同余及迭代方式进行改进.

在每次迭代中加入随机因素(该随机因素源于读写器),使得每次迭代的输出均匀分布,并在自编译程序中采用规范的长度以保持伪随机序列的周期,从而保证安全性. 假设 $f:\{0,1\}^{\lambda}\rightarrow\{0,1\}^{\lambda}$ 是任意的线性置换,$iter:\{0,1\}^{\lambda}\rightarrow\{0,1\}$ 是 $f$ 的随机化迭代. 对于原始输入 $m$,随机函数 $f$ 的第 $k$ 次递归迭代定义为 $f^{(k)}(m)=f(f^{(k-1)}(m))$. 通过将每一次迭代结果重新作为输入计算,伪随机数序列 $G(m,k)$ 构建为 $b:f^{(0)}(m)\parallel\cdots\parallel b:f^{(k-1)}(m)$.

常规的随机序列中,单纯的迭代会损失熵,甚至第二次迭代就很容易被翻转,改进后的随机序列生成器输出的随机性增强,形成伪长度保持函数,对改进后的伪随机序列生成器的安全性和性能进行分析,符合伪随机序列生成器应具备的两个特征,即多项式时间不可分辨性和不可预测性.

其中,多项式时间不可分辨性指的是由 $N$ 标记总体变量 $X^{def}=\{X_n\mid n\in N\}$ 和 $Y^{def}=\{Y_n\mid n\in N\}$,如果对于每个概率多项式时间算法 $A$,每个正多项式 $p(\cdot)$ 和所有足够大的 $n$,有

$$\left|Pr[A(X_n,1^n)=1]-Pr[A(Y_n,1^n)=1]\right|<\frac{1}{p(n)}$$

则称这两个总体在多项式时间内不可分辨.

多项式时间不可预测性指的是,若有

$$Pr[A(1^{|X_n|},X_n)=next_A(X_n)]<\frac{1}{2}+\frac{1}{p(n)}$$

而且没有任何概率多项式时间算法能以高于 0.5 不可忽略的概率完成后一任务 $next_A(X_n)$,那么这个总体就被称为在多项式时间内是不可预测的.

**1.1.2 基于轻量级候选函数集的动态重载机制** 为通信双方设定一个轻量级算法集合$\{f_1,f_2,\cdots,f_n\}$,并为每种算法设置加权因子$\{w_1,w_2,\cdots,w_n\}$. 由生成的伪随机数确定所用的轻量级候选函数集中的算法,然后从轻量级算法集中随机选取算法,构成函数序列. 为该函数序列输入加权因子 $w_i$,密钥 $k$ 和数据 $data$ 后,得到输出的消息 $f_i(w_i,k,data),\cdots,f_j(w_i,k,data)$. 需要注意的是,对于同样的参数而言,函数序列须满足 $f_i(w_i,k,data),f_j(w_i,k,data)\neq f_j(w_i,k,data),f_i(w_i,k,data)$.

协议运行时,将标签中生成的伪随机序列映射为算法控制密钥之后,确定轻量级候选函数集中所用算法. 通过认证授权,为后续所有权转移过程的完成提供安全基础.

## 1.2 协议初始化

协议基于以下假设:标签是具有可读写非易失性存储特征的低成本无源标签,可以运行带密钥的轻量级函数;标签与读写器上均有包含编译扩展因子的伪随机数发生器;读写器与标签之间通过不安全的无线信道进行通信;新旧所有者之间、读写器与数据库之间通过安全信道进行通信[7].

协议初始化阶段,每个标签有唯一的标识符($ID$),后端数据库为每一个标签生成各自的密钥,并创建一个三元组数据项$[ID,k_{\text{new}},k_{\text{old}}]$,标签状态 $S$ 标识位归零. 密钥同时存储在标签的非易失性存储器中;读写器与标签有初始的共享密

钥 $k_{\text{Init}}$,新旧所有者与标签都拥有同一轻量级候选函数算法集合.

### 1.3　协议执行过程

#### 1.3.1　认证授权阶段

**步骤 1**　协议初始,标签状态位为 00(待通信),读写器向标签发送查询请求 request.

**步骤 2**　标签收到 request 后状态位置为 01(待认证),产生随机数 $m$ 并计算 $i = k \bmod n$, $M = f_i(w_i, k, ID)$, $N = m \oplus M$,向读写器发送 $M$ 和 $N$,其中 $n$ 为轻量级候选函数集中的函数个数.

**步骤 3**　读写器在后台数据库检索遍历使 $i = k_{\text{new}'} \bmod n$ 且 $f_i(w_i, k_{\text{new}}, ID') = M$ 的三元组 $[ID', k_{\text{new}}, k_{\text{old}}]$,若不存在,则计算是否存在 $i = k_{\text{old}'} \bmod n$ 且 $f_i(w_i, k_{\text{old}'}, ID') = M$,若未查找到,则对标签认证失败,向标签发送认证失败消息,协议终止;若存在对应的三元组 $[ID', k_{\text{new}'}, k_{\text{old}'}]$,读写器计算 $m' = N \oplus M$,同时更新密钥 $k_{\text{new}} = f_i(w_i, ID, k)$ 并向标签发送 $P = m' \oplus k_{\text{new}}$.

**步骤 4**　标签收到 $P$ 后计算 $m' = P \oplus f_i(w_i, ID, k)$:若 $m' = m$,则更新与读写器的共享密钥 $k$,同时释放存储的临时随机数 $m$;否则协议终止,认证失败.

密钥更新之后,认证与授权完成,双方交互数据完成后,标签状态位置重置为 00.

#### 1.3.2　所有权转换阶段

**步骤 1**　新所有者向当前所有者发起标签所有权转换请求 *req*,并向对方发送自己的身份标识,即读写器标识符 *RID*;

**步骤 2**　当前所有者在后台数据库中检索相关数据并对新所有者身份进行验证,如果验证失败向新所有者发送失败消息;若身份验证通过,当前所有者计算 $j = k \bmod n$, $Q = f_j(w_j, k, ID)$,并向新所有者发送 *ID* 和 $Q$;

**步骤 3**　新所有者接收 *ID* 和 $Q$,并产生随机数 $r$,计算 $U = Q \oplus r$, $h = r \bmod n$, $Q = f_j(w_j, k, ID)$ 并向标签发送所有权转换请求 *TransReq* 和 $U$;

**步骤 4**　标签接收请求和 $U$,状态置为 10(所有权待转换),计算 $j' = k \bmod n$, $Q' = f_{j'}(w_{j'}, k, ID)$, $r' = U \oplus Q'$, $V = ID \oplus r'$,向当前所有者发送 $V$;

**步骤 5**　新所有者接收 $V$,计算 $r' = ID \oplus V$,若 $r = r'$,则更新与标签的共享密钥 $k = f_n(w_h, r, ID)$,同时计算 $W = ID \oplus k$,并向标签发送 $W$;

**步骤 6**　标签接收 $W$,计算 $k = ID \oplus W$, $h' = r' \bmod n$, $s = f_{h'}(w_h, r', ID)$,若 $s \neq k$,返回所有权转换失败消息,标签状态位恢复 00;否则标签更新共享密钥 $k = f_{h'}(w_{h'}, r', ID)$;

至此,新所有者与标签认证成功并进行密钥更新,标签所有权转换过程完成.

## 2　协议安全性分析

本文的研究重点是应用层的安全协议,因此在对本文协议进行安全性分析时,忽略其底层可能存在的弱点,不涉及底层破解密码算法的分析,只基于安全可靠的物理层假设[8]. 分析基于以下安全需求,其与同类协仪安全性的比较结果见表 1.

表 1　与同类协议安全性比较

Table 1　Comparisons with the similar protocols in security

| 协议 | 匿名性 | 双向认证 | 前向安全 | 后向安全 | 重传攻击 | 异步攻击 | 假冒攻击 |
|---|---|---|---|---|---|---|---|
| 文献[1] | × | √ | × | √ | × | × | √ |
| 文献[2] | √ | √ | √ | √ | × | × | √ |
| 文献[3] | √ | √ | × | √ | √ | × | × |
| 文献[5] | √ | √ | √ | √ | × | √ | √ |
| 文献[6] | √ | √ | √ | × | √ | √ | √ |
| 本协议 | √ | √ | √ | √ | √ | √ | √ |

匿名性:经轻量级运算的 *ID* 密文(假名)是合法标签的指纹,随机的轻量级候选函数集保证攻击者无法通过窃获的密文破解出标签

*ID*,为标签提供了不可区分性,只有授权用户才能识别该标签并正确计算出与该标签的共享密钥,避免攻击者通过分析标签响应造成泄露标签隐私和所有者位置被跟踪.

双向认证:在安全性相对较高的应用中,要求实现双向认证,以确保只有合法标签才能与读写器通信. 本文协议在实现读写器对标签认证的同时也要实现标签对读写器的认证,新密钥基于上一轮会话密钥和新鲜会话中的随机数产生,而随机数未在无线信道上进行明文传输. 在双方认证成功的基础上进行密钥协商并更新,确保只有授权用户才可以访问标签、只有合法标签才能与读写器通信.

前向安全:新所有者不能获得标签与前一个所有者的共享密钥,即使攻击者破解了标签内部状态和当前会话密钥或物理上复制了某个标签,也无法用来跟踪标签过期会话中的有效交互信息和数据;当前所有者只能对标签查询其自身相关信息,因此保证了本文协议的前向安全.

后向安全:新所有者与标签通过带有随机输入的轻量级函数进行数据交互,并采用概率算法进行密钥协商及更新,而上一个所有者无法获取新所有者产生的新鲜随机数和算法,为标签的所有权转移提供后向安全.

重传攻击:本文协议基于挑战 - 响应机制以随机数来抵御重传攻击. 在认证与授权的每轮会话中,读写器与标签的通信数据都包含新鲜随机数 $m$ 和 $r$,这使敌手无法通过重放上一轮会话中的交互消息伪装合法标签或读写器来参与新会话的认证授权.

异步攻击:攻击者在密钥协商更新过程中可能会拦截双方交互信息造成标签更新秘密数据失败,从而后端数据库和标签所存储的共享密钥不同步. 本文协议中后端数据库存储标签的三元组数据项$[ID, k_{new}, k_{old}]$,即便新密钥认证失败,协议也可采用密钥恢复机制用旧密钥进行二次认证.

假冒攻击:敌手可能在会话中窃听并记录双方交互信息,在标签与读写器的每一轮会话中,双方在不同阶段各自生成新鲜伪随机数,作为通过动态重载算法生成密文的输入,而敌手对伪随机数的猜测在概率上不具有任何优势,因此认证过程将检测出篡改行为,能有效抵御消息篡改.

## 3 协议计算开销分析

如何在保证安全性的前提下降低标签所有权转换过程中的计算量,尤其是标签的计算量,是影响该协议应用的重要因素. 在现有的研究成果中,大多数协议都采用 Hash 算法或对称密钥密码算法,而本文给出的新算法采用轻量级 PRBG 和 XOR 等逻辑运算,协议效率相对较高,通信过程中无需可信第三方(TTP)加密新的密钥,标签的唯一标识符固定,从而避免了标签进行频繁的写操作,采用标签动态标识机制,每次与读写器认证时别名动态变化,由轻量级候选函数集给标签带来的存储开销是可接受的,对于低成本标签也是可实现的. 本协议与同类协议的计算开销对比结果如图 1 所示.

由图 1 及前面安全性分析可知,本协议改进了伪随机序列生成器的迭代机制,同时轻量

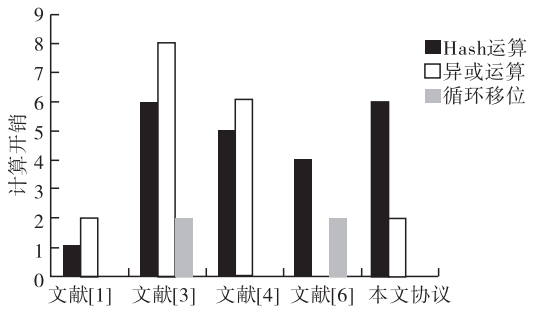


图 1 本协议与同类协议的计算开销之对比

Fig. 1 Comparison of computational cost among the proposed protocols and the similar protocols

级候选函数基于重载原理动态执行,与同类安全协议相比,在计算开销相对较低的水平上实现了安全性能的大幅提高. 因此基于轻量级函数集合的动态重载机制具有更低的计算消耗和通信开销,适用于计算资源非常有限的低成本标签.

## 4 结语

针对标签与读写器在通信过程中的安全隐私问题,结合类编程思想和重载原理,提出一种面向 RFID 标签的安全协议. 对协议中通信交互过程的分析结果表明,该协议能够防止重传攻击、消息篡改、假冒、异步攻击、标签跟踪等多种攻击,提供对标签数据安全和隐私的保护,同时新协议在标签内部状态存储信息被非法破解的情况下实现了前/后向安全,保证了标签所有权转换过程的安全性. 与同类相关安全协议相比,本协议的安全性和计算性能更高效,在实现更高安全级别的同时,还可提供对数据安全和标签隐私的保护. 如何保证每一个轻量级函数集中算法等概率随机出现,是下一步拟解决的关键问题.

**参考文献:**


[1] OSAKA K,TAKAGI T,YAMAZAKI K,et al. An efficient and secure RFID security method with ownership transfer[C]// Proceedings of CIS 2006 International Conference, Heidelberg: Springer,2007:778.

[2] KULSENG L, YU Z, WEI Y W, et al. Lightweight mutual authentication and ownership transfer for RFID systems[C]// Proceedings of the 29th Conference on Computer Communications, Piscataway: IEEE, 2010:1.

[3] SONG B, MITCHELL C J. Scalable RFID security protocols supporting tag ownership transfer [J]. Computer communications, 2011, 34(4): 556.

[4] KAPOOR G, PIRAMUTHU S. Vulnerabilities in some recently proposed RFID ownership transfer protocols [J]. IEEE communications letters, 2010, 14(3): 260.

[5] RAY B R, CHOWDHURY M, ABAWAJY J. Secure mobile RFID ownership transfer protocol to cover all transfer scenarios[C]// Proceedings of 2012 7th International Conference on Computing and Convergence Technology (ICCCT), Piscataway: IEEE, 2012: 1185.

[6] 张学军,王玉,王锁萍,等. 基于循环移位的轻量型相互认证协议研究[J]. 电子学报,2012, 40(11):2270.

[7] GAN Y, HE L, LI N N, et al. An improved forward secure RFID privacy protection scheme [C]// Proceedings of 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR), Piscataway: IEEE, 2010:273.

[8] 张素智,王朝辉,孙培锋. 基于动态更新 ID 的 RFID 安全认证协议研究[J]. 郑州轻工业学院学报,2011,26(6):1.