文章编号:1671 - 6833(2013)06 - 0024 - 04

基于随机排列函数的 RFID 标签所有权转换协议

贺 蕾,甘 勇,尹毅峰,金松河

(郑州轻工业学院 计算机与通信工程学院,河南 郑州 450002)

摘 要:针对 RFID 系统中标签在进行所有权转换时所遇到的安全问题,提出了一种基于随机排列函数的所有权转换协议.其中,随机排列函数在线性反馈移位寄存器和物理不可克隆函数的基础上进行构建.采用 GNY 逻辑对协议的安全性进行分析,该协议能够抵御重放攻击、中间人攻击和去同步化攻击,保护标签信息的前向安全和后向安全,并能提供不可跟踪性保护.在 Linux 中对该协议进行了仿真实现,获取了标签计算耗时等实验数据,并与其他研究成果进行了对比.结果表明:该协议中标签计算耗时较短,适用于低成本标签.

关键词:无线射频识别;所有权转换;线性反馈移位寄存器;物理不可克隆函数;GNY 逻辑

中图分类号:TP393 **文献标志码**:A doi:10.3969/j.issn.1671 - 6833.2013.06.006

0 引言

无线射频识别技术(Radio Frequency Identification, RFID)是一种无需被识别物品在可视范围内就能进行自动识别的技术.一个典型的 RFID 系统通常由标签、读写器和后端数据库组成.标签所附的物品在其生存期内大多需要经历多个所有者,当物品在不同所有者之间进行流通时,需要进行所有权的转换.相应地,物品上所附的标签也要进行所有权转换.标签所有权转换协议除了要满足认证协议所需满足的安全性以外,还要能提供标签信息的前向安全和后向安全.前者指的是新所有者不能依据自己掌握的机密信息获得标签与原所有者共享的机密信息,后者指的是原所有者不能获取标签与新所有者之间共享的机密信息.

1 相关工作

Zhou 等[1]提出了一种包含原所有者、新所有者、标签、第三方物流(Third Party Logistics, TPL)和可信第三方(Trusted Third Party, TTP)的所有权转换协议.该协议不能抵御去同步化攻击.Jia 等[2]所提出的所有权转换协议通过改变标签密钥的方式达到所有权转换的目的,但该协议不能抵御跟踪攻击.Song[3]提出了一种所有权转换协议.Wang[4]对该协议分析后设计了一种攻击方案,破坏了标签信息的前向安全.Kapoor 等[5]提出了一个有 TTP 和一个没有 TTP 的所有权转换协议,这两个协议都需要使用对称密钥密码算法,计算量较大.

2 协议描述

2.1 初始化阶段

在初始化阶段,标签和所有者共享 3 个机密信息,分别是标签的身份标识 ID、密钥 k_i 和秘密值 s_j.其中,下标 i 和 j 分别表示这是标签与所有者共享的第 i 个密钥和第 j 个秘密值.在本协议中,标签中内置了两个轻量级的随机排列函数,分别用 F 和 P 表示.其中,F 函数是与所有者共享的随机排列函数,可以用线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)[6]实现,P 函数则基于物理不可克隆函数(Physical Unclonable Function, PUF)[7]进行构建.利用 LFSR 可以构建具有较好统计特性的伪随机排列函数,如果该伪随机排列的种子值是秘密的,则其输出序列是无法预测的.PUF 的输出排列中由于嵌入了标签的物理信息,因而具有唯一性、不可克隆性、不可预测性和防篡改等安全属性.

收稿日期:2013 - 07 - 01;**修订日期**:2013 - 08 - 27

基金项目:国家自然科学基金资助项目(61272038),河南省科技攻关计划项目(122102210124)

作者简介:贺蕾(1980 -),男,山西平遥人,郑州轻工业学院讲师,主要从事无线网络安全和密码学方面的研究,E-mail: heleiresearch@126.com.

2.2 协议流程

笔者提出的标签所有权转换协议见图 1.

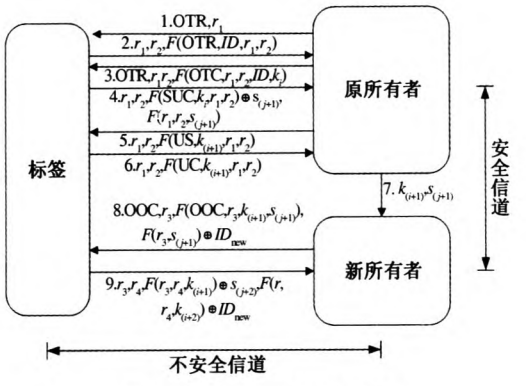

图 1　标签所有权转换协议

Fig. 1　Ownership transfer protocol of RFID tag

(1)标签的原所有者发送所有权转换请求 OTR(Ownership Transfer Request)和一个随机数 r_1给标签，即$\{\text{OTR}, r_1\}$.

(2)标签收到消息后生成随机数 r_2，并发送$\{r_1, r_2, F(\text{OTR}, ID, r_1, r_2)\}$给原所有者.

(3)原所有者收到标签发来的消息后，通过在数据库中搜索是否存在适当的 ID，使其满足 $F(\text{OTR}, ID, r_1, r_2)$，以此来判断该消息是否是需要进行所有权转换的标签发来的消息. 若不是，则协议终止；若是，则通过对标签的认证，发送$\{\text{OTR}, r_1, r_2, F(\text{OTC}, r_1, r_2, ID, k_i)\}$给标签. 其中，OTC 表示所有权转换命令(Ownership Transfer Command).

(4)标签用自己的 ID 和密钥验证收到的 $F(\text{OTC}, r_1, r_2, ID, k_i)$是否正确. 若不正确，则协议终止. 若正确，则计算 $s_{(j+1)} = P(s_j)$，$k_{(i+1)} = F(s_{(j+1)})$，发送$\{r_1, r_2, F(\text{SUC}, k_i, r_1, r_2)\oplus s_{(j+1)}, F(r_1, r_2, s_{(j+1)})\}$. 其中，SUC 表示机密信息更新命令(Secret Update Command, SUC)，符号“⊕”表示异或运算.

(5)原所有者收到标签发来的消息后，用检索到的标签 ID 所对应的密钥计算出 $F(\text{SUC}, k_i, r_1, r_2)$，进而求出 $s_{(j+1)}$，并用收到的 $F(r_1, r_2, s_{(j+1)})$检查计算出的 $s_{(j+1)}$是否正确，再由 $k_{(i+1)} = F(s_{(j+1)})$计算出 $k_{(i+1)}$. 原所有者发送$\{r_1, r_2, F(\text{US}, k_{(i+1)}, r_1, r_2)\}$给标签，其中 US(Update Success)为更新成功标识.

(6)标签收到所有者发来的消息后，检查收到的 $F(\text{US}, k_{(i+1)}, r_1, r_2)$是否正确. 若不正确，则协议终止；若正确，则发送$\{r_1, r_2, F(\text{UC}, k_{(i+1)}, r_1, r_2)\}$给所有者，其中 UC(Update Completed)为更新结束标识.

(7)若原所有者长时间未收到标签发来的更新结束消息，则从步骤 1 开始重新执行协议. 若原所有者收到标签发来的更新结束消息，并确认该消息正确，则表明信息更新结束. 原所有者通过安全的信道将密钥 $k_{(i+1)}$和秘密值 $s_{(j+1)}$发送给新所有者.

(8)新所有者收到原所有者发来的消息后，在原所有者的通信范围之外与标签进行通信. 生成随机数 r_3和标签的新身份标识 ID_{new}，发送$\{\text{OOC}, r_3, F(\text{OOC}, r_3, k_{(i+1)}, s_{(j+1)}), F(r_3, s_{(j+1)})\oplus ID_{new}\}$给标签. 其中，OOC(Ownership Obtain Command)为所有权获取命令.

(9)标签根据 OOC 确定收到的消息是新所有者请求获取所有权的消息，用自己存储的$\{k_{(i+1)}, s_{(j+1)}\}$验证 $F(\text{OOC}, r_3, k_{(i+1)}, s_{(j+1)})$是否正确. 若不正确，则协议终止. 若正确，则通过对所有者的认证. 标签求出新所有者为标签分配的新的身份标识 ID_{new}，生成随机数 r_4，标签计算 $s_{(j+2)} = P(s_{(j+1)})$，$k_{(i+2)} = F(k_{(i+1)}, s_{(j+2)})$，发送$\{r_3, r_4, F(r_3, r_4, k_{(i+1)})\oplus s_{(j+2)}, F(r_3, r_4, k_{(i+2)})\oplus ID_{new}\}$.

(10)新所有者计算出 $F(r_3, r_4, k_{(i+1)})$，进而得到 $s_{(j+2)}$，并由 $k_{(i+2)} = F(k_{(i+1)}, s_{(j+2)})$得到新密钥 $k_{(i+2)}$. 计算 $F(r_3, r_4, k_{(i+2)})$，以得到 ID_{new}，确定标签获得了正确的 ID_{new}. 若标签获得的 ID_{new}不正确，则返回步骤 8 重新开始.

3 协议安全性分析

笔者采用 GNY 逻辑对协议的安全性进行分析. 为了分析的方便，假设只有标签与所有者之间的信道是不安全的. 本节所采用的表述方式和推理规则遵照文献[8-9]中的相关内容.

3.1 形式化表述

对协议流程按照 GNY 逻辑的要求进行形式化表述，其中 QO 表示原所有者(Quondam Owner, QO)，NO 表示新所有者(New Owner, NO)，T 表示标签. 为了研究的方便，考虑到 F 函数和 Hash 函数在本协议中所起的作用类似，故在进行 GNY 分析时用 Hash 函数代替 F 函数.

M1: $\text{T} \lhd *\text{OTR}, *r_1$

M2: $\text{QO} \lhd r_1, *r_2, *H(\text{OTR}, ID, r_1, r_2)$

M3: $\text{T} \lhd \text{OTR}, *r_1, r_2, *H(\text{OTC}, r_1, r_2, ID, k_i)$

M4: $\text{QO} \lhd r_1, *r_2, *\{S_{(j+1)}\}_{H(\text{SUC}, k_i, r_1, r_2)}, *H(r_1, r_2, S_{(j+1)}))$

M5: $\text{T} \lhd *r_1, r_2, *H(\text{US}, k_{(i+1)}, r_1, r_2)$

M6: $QO \lhd r_1, *r_2, *H(UC, k_{(i+1)}, r_1, r_2)$

M7: $T \lhd *OOC, *r_3, *H(OOC, r_3, k_{(i+1)}, s_{(j+1)}), *\{ID_{new}\}_{H(r_3, s_{(j+1)})}$

M8: $NO \lhd r_3, *r_4, *\{s_{(j+2)}\}_{H(r_3, r_4, k_{(i+1)})}, *\{ID_{new}\}_{H(r_3, r_4, k_{(i+2)})}$

3.2 初始化假设

A1: $QO \mid \equiv QO \xleftrightarrow{ID} T$

A2: $T \mid \equiv QO \xleftrightarrow{k_i} T$

A3: $NO \mid \equiv NO \xleftrightarrow{k_{(i+1)}} T$

A4: $NO \mid \equiv T \ni k_{(i+1)}$

A5: $NO \mid \equiv NO \xleftrightarrow{k_{(i+2)}} T$

3.3 证明目标

G1: $QO \mid \equiv T \ni ID$(由 M2, A1, I3, I6 得 G1)

G2: $T \mid \equiv QO \ni k_i$(由 M3, A2, I3, I6 得 G2)

类似地,可以得到 G3, G4, G5.

G3: $T \mid \equiv QO \ni k_{(i+1)}$

G4: $QO \mid \equiv T \ni k_{(i+1)}$

G5: $T \mid \equiv NO \ni k_{(i+1)}$

从以上分析过程可以看出,标签与原所有者进行了双向认证,互相确认了对方的身份.同时,对存储的密钥进行了更新,保护了机密信息的前向安全.

G6: $T \ni ID_{new}$(由 M7, P6 得 G6)

G7: $NO \mid \equiv T \sim s_{(j+2)}$(由 M8, A3, I1 得 G7)

G8: $NO \ni k_{(i+2)}$(由 *M*8, *P*6 和 $k_{(i+2)}$ 的生成方式得 G8)

G9: $NO \mid \equiv T \ni k_{(i+2)}$(由 G7, I6 得 $NO \mid \equiv T \ni s_{(j+2)}$;由 A4 和 $k_{(i+2)}$ 的生成方式得 G9)

G10: $NO \mid \equiv T \ni ID_{new}$(由 M8, A5, I1, I6 得 G10)

从以上分析过程可以看出,新所有者与标签协商出了新的共享密钥 $k_{(i+2)}$,保护了标签信息的后向安全,并且为标签分配了新的身份标识、抵御了跟踪攻击.

对于去同步化攻击,在原所有者与标签的通信过程中,标签首先更新密钥.若遭到去同步化攻击,原所有者可以使用标签的 *ID* 和密钥重新执行协议.在新所有者与标签的通信过程中,若遭到去同步化攻击,新所有者可以再次发送含 OOC 的消息给标签,以重新进行信息同步.因此,该协议能够抵御去同步化攻击.

将笔者所提出的协议与部分现有研究成果进行对比,可以发现笔者所提出的协议具有较好的安全性,如表 1 所示.

表 1 与现有部分研究成果的安全性对比

Tab.1 Comparison with other research results

文献	不可跟踪性	抗重放攻击	抗中间人攻击	抗去同步化攻击	前向安全	后向安全
文献[1]	√	√	√	×	√	√
文献[2]	×	√	√	√	√	×
文献[3]	√	√	√	√	×	√
文献[5](无 TTP)	√	√	√	√	√	√
文献[5](有 TTP)	√	√	√	√	√	√
本文协议	√	√	√	√	√	√

4 协议仿真实现

在 Linux 系统中对笔者所提出的协议和其他研究人员所提出的研究成果进行了仿真实现,所用计算机的 CPU 为 3.2 GHz,内存为 2.0 GB.通过仿真实现,主要获取了标签进行计算所消耗的时间等实验数据,并进行了对比,如图 2 所示,单位为微秒.从图 2 可以看出,与其他研究成果相比,笔者所提出的所有权转换协议中标签所消耗的计算时间较短,适用于低成本的标签.

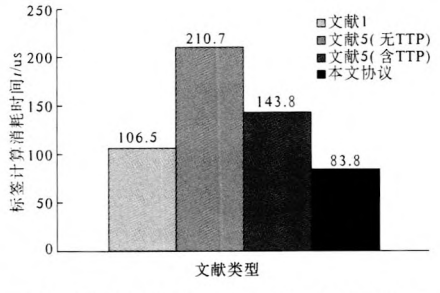

图 2 不同研究成果中标签计算消耗时间

Fig.2 Cost time by tag in different research results

5 结论

笔者提出了一种标签所有权转换协议,该协议使用了基于 LFSR 和 PUF 的轻量级随机排列函数.原所有者与标签进行认证和密钥更新后,将更新后的机密信息发送给新所有者,以保护标签信息的前向安全.新所有者再次与标签进行认证和

机密信息更新，以保护标签信息的后向安全. 使用 GNY 逻辑对协议安全性进行了分析，该协议能够抵御重放攻击、中间人攻击、去同步化攻击，并能保护标签附着物的位置隐私. 对协议进行了仿真实现，获取了标签计算时间等数据. 通过与其他协议的数据进行对比发现，笔者所提出的协议中标签的计算时间比其他协议的计算时间短，更适合用于低成本 RFID 标签.

参考文献：

[1] ZHOU Wei, YOON E J, PIRAMUTHU S. Varying levels of RFID tag ownership in supply chains[C]// On the Move to Meaningful Internet Systems: OTM 2011 Workshops. Berlin: Springer Berlin Heidelberg, 2011:228 - 235.

[2] JIA Han, WEN Jun. A novel RFID authentication protocol with ownership transfer[J]. Lecture Notes in Electrical Engineering, 2012, 122:599 - 606.

[3] SONG B. RFID tag ownership transfer[EB/OL]. http://rfidsec2013.iaik.tugraz.at, 2008 - 12 - 01.

[4] WANG Shao-hui. Analysis and design of RFID tag ownership transfer protocol[C]//Proceedings of the 2011 International Conference on Informatics, Cybernetics, and Computer Engineering. Berlin: Springer Berlin Heidelberg, 2012:229 - 236.

[5] KAPOOR G, PIRAMUTHU S. Single RFID tag ownership transfer protocols[J]. IEEE Transactions on, Systems, Man, and Cybernetics, Part C: Applications and Reviews. 2012, 42(2): 164 - 173.

[6] 杨波. 现代密码学[M]. 北京：清华大学出版社，2010:15 - 19.

[7] 张紫楠，郭渊博. 物理不可克隆函数综述[J]. 计算机应用，2012, 32(11): 3115 - 3120.

[8] GONG Li, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocols[C]//1990 IEEE Computer Society Symposium on Research in Security and Privacy. Washington D C: IEEE Computer Society, 1990:234 - 248.

[9] 李建华，张爱新，薛质，等. 网络安全协议的形式化分析与验证[M]. 北京：机械工业出版社，2010:27 - 33.

Ownership Transfer Protocol of RFID Tags Based on Random Permutation Functions

HE Lei, GAN Yong, YIN Yi-feng, JIN Song-he

(School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)

Abstract: This paper proposed a lightweight ownership transfer protocol based on random permutation functions to protect the ownership transfer procedure in RFID system. The random permutation functions were structured on the basis of linear feedback shift register and physical unclonable function. Our protocol analyzed its security by GNY logic. The result shows it can resist replay attack, man-in-middle attack and desynchronization attack. It also provides forward security, backward security and untraceability. The protocol was simulated and implemented in Linux. We obtained experiment data including computation time cost by tag. Compared with other protocols, the experiment data shows that our protocol is suitable for low - cost tags because the computation time is shorter.

Key words: radio frequency identification; ownership transfer; linear feedback shift register; physical unclonable function; GNY logic