【信息科学与控制工程】　　doi：10.11809/bqzbgcxb2019.08.031

改进的基于位运算的 RFID 标签所有权转移协议

罗韶杰，张立臣

（广东工业大学计算机学院，广州　510006）

摘要：在标签生命周期中，归属权应随着所属者的改变而变化，为保障归属权无误及存放信息的安全，提出一种基于按位运算的标签所有权转移协议。所提协议具备如下特征：对传送信息，采用字合成运算、交叉位运算加密；字合成及交叉位运算均属于超轻量级的计算，能一定程度上降低计算量；共享密钥作为加密的变量，能减少参数的引入，降低存储空间；引入归属权标志位，明确归属权所属者。对协议进行安全性及性能分析，表明协议具备系统所需的安全要求。

关键词：射频识别；所有权转移；共享密钥；标签；位运算

本文引用格式：罗韶杰，张立臣. 改进的基于位运算的 RFID 标签所有权转移协议[J]. 兵器装备工程学报，2019，40(8)：157－164.

Citation format：LUO Shaojie，ZHANG Lichen. Improved RFID Tag Ownership Transfer Protocol Based on Bit Operation [J]. Journal of Ordnance Equipment Engineering，2019，40(8)：157－164.

中图分类号：TP393　　**文献标识码**：A　　**文章编号**：2096－2304(2019)08－0157－08

Improved RFID Tag Ownership Transfer Protocol Based on Bit Operation

LUO Shaojie，ZHANG Lichen

（School of Computers，Guangdong University of Technology，Guangzhou 510006，China）

Abstract：In the tag life cycle，the ownership should change with the change of the owner. In order to ensure the right of ownership and the security of information storage，a tag ownership transfer protocol based on bitwise operation is proposed. The proposed protocol has the following characteristics：for the transmission of information，word synthesis and cross-bit operation are used to encrypt；word synthesis and cross-bit operation belong to ultra-lightweight calculation，which can reduce the amount of calculation to a certain extent；shared key as a variable of encryption can reduce the introduction of parameters and reduce storage space；and the introduction of ownership flag bit to clarify the ownership. The security and performance analysis of the protocol shows that the protocol has the security requirements of the system.

Key words：RFID；pseudo random function；word synthesis operation；mobile system；tripartite authentication

RFID(Radio Frequency Identification)是一种利用无线射频通信方式实现的非接触式的能够自动识别特定实体的技术。RFID 系统包括后台数据库、标签、读写器三种实体组成，因系统中的标签具有耐磨损、成本低、寿命长、易携带等优点，现 RFID 系统已被广泛应用于物流、交通运输、门禁系统等各行各业中[1]。因读写器与标签之间采用无线方式进行传输信息，使得链路易受到信号干扰、通信消息被攻击者窃听等缺陷，RFID 系统的安全性和隐私问题成为其更进一

收稿日期：2019－01－14；**修回日期**：2019－02－20

基金项目：国家自然科学基金项目(61572142，61873068)

作者简介：罗韶杰(1993—)，男，硕士研究生，主要从事信息物理融合系统、射频识别、信息安全等研究，E-mail：370533211@qq.com。

通讯作者：张立臣(1962—)，男，博士，教授，主要从事面向方面的信息物理融合系统、并行处理和实时系统等研究，E-mail：zlctongxun@126.com。

步的推广的限制因素。

RFID 系统中的标签会在其生命周期中,标签的所有权会经常发生变化,相对应的标签内部存放的数据信息也在不断更换。因此需确保标签所有权在不断变更过程中具备一定的安全要求:(1)所有权转移协议要能够抵抗较为常见的攻击方式,比如,重放攻击、去同步化攻击等;(2)待标签的所有权发生变化之后,标签的原所有者便失去控制和访问标签隐私信息的权限,从而保证标签新所有者的隐私安全性;(3)标签的新所有者在确定获取标签的所有权之后,新所有者不能根据已有的信息推导出原所有者的隐私信息,用以来保护标签原所有者的隐私安全性[2-3]。

Saito 等[4]提出一种所有权转移协议,协议基于可信第三方(TTP),协议虽然很好地解决了标签所有权归属问题,但可信第三方的引入,使得整个系统的成本增加,且通信量也增加。Molnar 等[5]给出一种所有权转移协议,协议通过"假名"的方法来确保隐私信息不被泄露,该协议的实现需要引入一个共同的可信中心(TC),可信中心的引入,会导致系统成本的增加,同时可信中心在监管不当的情况下,容易造成隐私信息外泄。Song 等人首先在文献[6]中设计出一种所有权转移协议,协议利用对称加密的思想、HASH 函数加密的算法对通信消息进行加密,一定程度上优化了协议的计算复杂度。因文献[6]中协议存在一定安全缺陷,Song 等又在文献[7]中设计出一种基于文献[6]改进的协议方案,但改进后的方案仍存在无法抵抗攻击者的去同步化攻击缺陷。Kapoor 等[8]详细分析了 Song 等人设计出的方案存在的安全性不足问题,提出一种轻量级别的所有权转移协议,其协议的创新点之处在于:新所有者的密钥是随机产生的。Munilla 等[9]对 Kapoor 等提出的协议进行了严谨的数学推理,得出所提协议不适用于日常生活中的实际场景中,并同时 Munilla 等人利用噪声标签来替换可信第三方(TTP)的机制,提出一种新的轻量级别的所有权转移协议。Doss. R 等[10]提出一种所有权转移协议,所提协议基于二次剩余定理来完成对信息的加密,二次剩余定理背景来源于数学中大数分解问题,具备较高的安全性,使得协议安全性很高;但协议所能适应的范畴仅仅只有无源标签,使得协议的应用受到极大的限制。文献[11]中提出一个所有权转移协议,该协议基于 Rabin 算法实现对信息的加密,优化之后的 Rabin 算法具有较低的计算量特征,使得文献[11]中的协议具备轻量级的特征。文献[12]中详细分析了文献[11]中所提方案的不足之处。文献[12]中指出,攻击者通过三次完整的窃听、重放、假冒等手段,最终可使得标签新所有者与标签之间的共享密钥失去同步性,得出文献[11]中所提协议无法抵抗重放攻击和去同步化攻击的结论。并在分析之后,在文献[12]中给出一个改进的协议。

对文献[12]中的协议进行分析发现,该协议仍旧存在一定的不足及可改进之处,仍有改进的空间,本文提出一种基于共享密钥的所有权转移协议。本文所提协议采用简单的位运算对传输消息进行加密,降低通信实体的计算复杂度;协议中,为确保标签所有权归属的唯一性,引入归属权标志位变量,根据变量当前的值,唯一确定标签的所有权归属;为减少通信实体的存储空间,同时也为减少变量的引入,将通信实体之间的共享密钥作为一参数进行计算。通过安全性分析,说明所提协议具备所有权转移所需的安全需求;性能分析,说明所提协议能够减少通信实体计算复杂度。

1 对被改进协议的分析

1.1 被改进协议的原理简述

结合图 1,文献[12]协议的步骤可简述如下。

步骤 1 标签原所有者向标签发出所有权转移协议申请。

步骤 2 标签计算 M,同时将 ID_L 和 M 作为响应信息发送给标签原所有者。

步骤 3 标签原所有者查找 ID_L 是否存在。若不存在,协议结束。若存在,取出相对应的量,计算 M',然后比对 M' 与 M。若相等,计算 N 和 P,并将 N 和 P 发送标签;若不相等,协议结束。

步骤 4 标签对 N 和 P 进行验证。验证结果为真,计算 Q,且将 Q 发送给标签原所有者;验证结果为假,协议结束。

步骤 5 标签原所有者将 Q、$r1$、IDi_L 发送给标签新所有者。

步骤 6 标签新所有者查找 IDi_L 是否存在。若不存在,协议结束。若存在,取出相对应的量,并计算出 X 和 Y,同时将 X 和 Y 的值发送给标签。

步骤 7 标签对 X 和 Y 进行验证。验证结果为真,开始更新信息,所有权转移协议顺利结束;验证结果为假,协议结束,所有权转移协议失败。

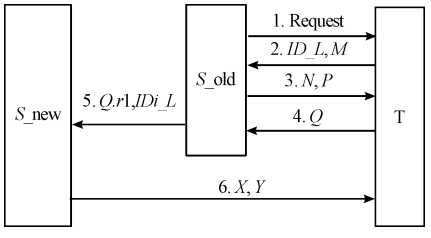

图 1 文献[12]的所有权转移协议

1.2 被改进协议的不足分析

文献[12]协议中存在的不足:(1)协议无法确保数据 $r1$ 的新鲜性。数据 $r1$ 的更新操作是在协议开始之时利用赋值操作,即:$r1 = r\_x$ 来实现,故通信过程中,当标签在接收到验证消息以后,即便是 r_x 立即动态刷新,也仍然无法确保 $r1$ 的及时更新。因为攻击者可在标签动态刷新 r_x 之后,将 r_x 赋值给 $r1$ 之前,阻塞该过程,从而使得协议无法确保数据 $r1$ 的新鲜性。(2)协议存在安全缺陷。攻击者通过窃听两轮完整的通信过程,便可在第三轮通信过程中假冒标签发起攻击,通过重放消息 Q 的方式,可截获得到消息 X、Y。阻塞合

法标签新所有者发送给标签的信息,攻击者将截获的消息 X、Y 重放的方式发送给标签,标签将会进行反复认证通过,且进行信息更新,两轮操作之后,导致标签与新数据库两端的共享密钥失去同步性,攻击者的去同步化攻击成功。

本文改进协议与文献[12]中的协议对比,不同之处在于:

1)改进的协议未采用 Rabin 加密算法对传输信息进行加密,而是采用字合成运算及交叉位运算进行加密;

2)现有的文献中,对于 Rabin 加密算法进行优化后,其计算量最多也只能达到轻量级的级别,而字合成运算及交叉位运算的本质属于按位运算,该运算属于超轻量级的级别,因此改进的协议在计算量方面较文献[12]改进较大;

3)改进的协议引入标签所有权归属权标志位参量,能够唯一确定归属权;

4)改进的协议能够弥补文献[12]中存在的安全缺陷,具体弥补方式参见文章安全性分析章节。

2 所有权转移协议

本文协议与其他此类 RFID 标签所有权转移协议一样,做出如下假定[13-14]:1)标签与标签原所有者 *S_old* 之间通过无线方式通信,该链路不安全,易被攻击者攻击;2)标签与标签新所有者 *S_new* 之间通过无线方式通信,该链路不安全,易被攻击者攻击;3)标签原所有者 *S_old* 与标签新所有者 *S_new* 之间通过有线方式通信,该链路安全,不易被攻击者攻击;4)标签、标签原所有者 *S_old*、标签新所有者 *S_new* 中存放的信息是安全的,且攻击者无法获取;5)协议开始之前,标签一端存放以下信息:$(K, IDt, IDS, FLAG)$,标签新所有者 *S_new* 一端存放以下信息:(S, IDt, IDS),标签原所有者 *S_old* 一端存放以下信息:(K, IDS, IDt)。

2.1 协议符号说明

设 X、Y 是两个具有 L 位的二进制数,$X = x_1x_2x_3\cdots x_L$,$Y = y_1y_2y_3\cdots y_L$。其中,x_i、y_i 取值范围为 $\{0,1\}$,$i = 1,2,\cdots,L$,$Syn(X,Y) = Y_{L-M+1}\, Y_{L-M+2}\cdots Y_L X_1 X_2 \cdots X_{L-M}$。字合成运算 $Syn(X,Y)$ 是指由 X 的前 $L-M$ 位与 Y 的后 M 位组合而形成新的 L 位数组;其中 M 的设定为:$M = Hw(Y)$,也可以为 $M = L - Hw(Y)$,$Hw(Y)$ 表示为 Y 的汉明重量。有关字合成运算更多规定可参考文献[15]。图 2 给出了一个字合成运算例子。

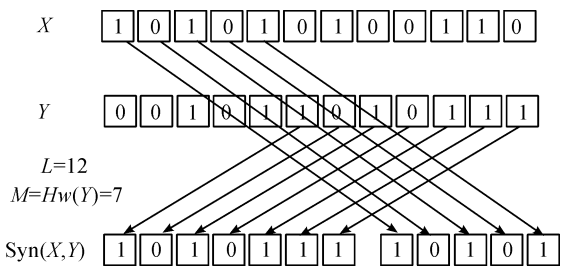

图 2 字合成运算检测

交叉位运算 $Cro(X,Y)$ 是指由 X 的奇数位和 Y 的偶数位相互交叉形成新的 L 位数组。交叉位运算可在标签中按如下方式实现:定义两个指针 $p1$ 和 $p2$ 分别指向 X 和 Y,当 $p1$ 指向 X 的奇数位时,把此位置上的值赋予运算结果的偶数位;当 $p2$ 指向 Y 的偶数位时,则把此位置上的值赋予运算结果的奇数位。有关交叉位运算更多规定可参考文献[16]。图 3 给出了一个交叉位运算例子。

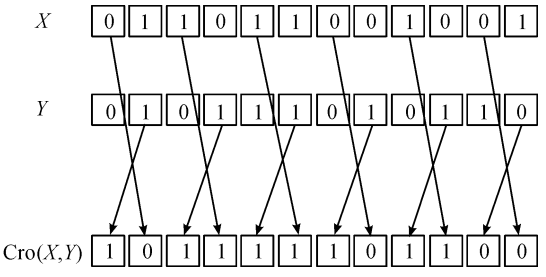

图 3 交叉位运算

表 1 给出所有权转移协议符号所表示的含义。

表 1 符号说明

符号	含义
T	标签
S_new	标签的新所有者
S_old	标签的原所有者
IDt	标签的标识符
IDS	标签的标识符假名
IDt_L	标签的标识符左半部分
IDt_R	标签的标识符右半部分
IDS_old	标签的旧标识符假名
IDS_new	标签的新标识符假名
K	标签与原所有者之间当前的共享密钥
S	标签与新所有者之间当前的共享密钥
K_old	标签与原所有者之间上一轮的共享密钥
K_new	标签与原所有者之间更新后的共享密钥
K_L	标签与原所有者之间当前的共享密钥的左半部分
K_R	标签与原所有者之间当前的共享密钥的右半部分
x,*y*,*z*	标签原所有者产生的随机数
t	标签新所有者产生的随机数
FLAG	归属权标志位。值为 0,归属权为原所有者
$\oplus$	异或运算
&	与运算
$Syn(X,Y)$	字合成运算
$Cro(X,Y)$	交叉位运算

2.2 协议过程

所有权转移协议过程如图4所示。

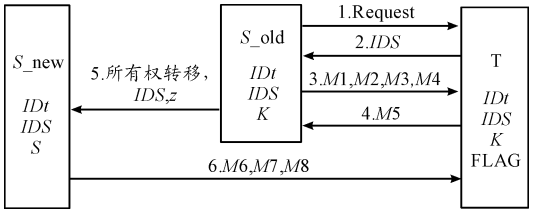

图4 所有权转移协议框图

图4中出现的公式解释如表2所示。

表2 公式解释

公式	解释
$M1$	$x \oplus Syn(IDt\_L, K\_R)$
$M2$	$Cro(K\_L, IDt\_R) \oplus y$
$M3$	$Cro(IDt\_L, K\_R) \oplus Syn(K\_L, IDt\_R) \oplus z$
$M4$	$x\&y\&z\&K\&IDt$
$M5$	$Syn(x, IDt)\&Cro(K, y)\&z$
$M6$	$Syn(z, IDt) \oplus t$
$M7$	$Cro(z, IDt) \oplus S$
$M8$	$Syn(t, S)\& Cro(t, S)$

结合图4,所有权转移协议步骤描述如下:

步骤1 标签原所有者 *S_old* 向标签发送所有权转移请求。

步骤2 标签在接收到标签原所有者 *S_old* 发送来的消息后,标签首先查阅归属权标志位 *FLAG* 的值,当前 *FLAG* = 0,表示标签原所有者拥有标签的所有权,标签可进行后续操作。标签将 *IDS* 发送给标签原所有者 *S_old*。

步骤3 标签原所有者 *S_old* 在接收到标签发送来的消息后,查找是否存在 *IDS* = *IDS_old* 或 *IDS* = *IDS_new*,若未找到,协议终止;反之,进行如下操作。

1) 标签原所有者 *S_old* 中的线性反馈移位寄存器 *LFSR* 通过初始化得到三个随机数,依次记作:x, y, z。其中后续操作中,随机数 x、y 由 *MIXBITS* 函数实时进行刷新。

2) 利用找到的与 *IDS* 相对应的 *IDt*、*K* 及1)中生成的随机数 x、y、z,计算得到 *M1*、*M2*、*M3*、*M4*。

3) 标签原所有者 *S_old* 将 *M1*、*M2*、*M3*、*M4* 发送给标签。

其中有关 *M1*、*M2*、*M3*、*M4* 的计算公式见表2。

步骤4 标签在接收到标签原所有者 *S_old* 发送来的消息后,标签按照如下操作来验证标签原所有者 *S_old* 的真伪。

1) 用自身存放的标识符 *IDt*,自身存放的共享密钥 *K*,接收到的 *M1*,计算得到随机数 x。即:$x = Syn(IDt\_L, K\_R) \oplus M1$。

2) 用自身存放的标识符 *IDt*,自身存放的共享密钥 *K*,接收到的 *M2*,计算得到随机数 y。即:$y = Cro(K\_L, IDt\_R) \oplus M2$。

3) 用自身存放的标识符 *IDt*,自身存放的共享密钥 *K*,接收到的 *M3*,计算得到随机数 z。即:$z = Syn(K\_L, IDt\_R) \oplus Cro(IDt\_L, K\_R) \oplus M3$。

4) 用1)计算得到的随机数 x,用2)计算得到的随机数 y,用3)计算得到的随机数 z,用自身存放的标识符 *IDt*,自身存放的共享密钥 *K*,计算得到 $M4'$。

5) 比对计算到的的 $M4'$ 与接收到的 *M4* 是否相等。若不想等,表明标签原所有者 *S_old* 是伪造的,协议终止;反之,标签原所有者 *S_old* 通过标签的验证,并进行第6)步。

6) 标签用1)计算得到的随机数 x,用2)计算得到的随机数 y,用3)计算得到的随机数 z,用自身存放的标识符 *IDt*,自身存放的共享密钥 *K*,计算得到 *M5*。

7) 标签将 *M5* 发送给标签原所有者 *S_old*。其中有关 *M5* 的计算公式见表2。

步骤5 标签原所有者 *S_old* 在接收到标签发送来的消息后,标签原所有者 *S_old* 进行如下操作。

1) 自身产生的随机数 x、y、z,自身存放的 *IDt*、*K*,计算得到 $M5'$。然后比对计算得到的 $M5'$ 与接收到的 *M5* 是否相等。若不相等,表明标签是伪造的,协议终止;反之,表明标签通过标签原所有者 *S_old* 的真伪验证,并进行第2)步。

2) 标签原所有者 *S_old* 开始更新随机数 x、y,即:$x = MIXBITS(x, IDt \oplus K)$、$y = MIXBITS(y, IDt \& K)$。

3) 标签原所有者 *S_old* 开始更新共享密钥,即:$K\_old = K, K = K\_new$。

4) 标签原所有者 *S_old* 告知标签新所有者 *S_new* 开始进行所有权转移操作,且将〈*IDS*、z〉一并发送给标签新所有者 *S_new*。

步骤6 标签新所有者 *S_new* 在接收到标签原所有者 *S_old* 发送来的消息后,标签新所有者 *S_new* 进行如下操作。

1) 标签新所有者 *S_new* 产生一个随机数,记作 t。

2) 用接收到的随机数 z,自身生成的随机数 t,计算得到标签与标签新所有者 *S_new* 之间的共享密钥 *S*,即 $S = MIXBITS(t, z)$。

3) 用自身存放的 *IDt*,接收到的随机数 z,自身生成的随机数 t,计算可得到 *M6*。用自身存放的 *IDt*,接收到的随机数 z,计算得到的共享密钥 *S*,计算可得到 *M7*。用自身生成的随机数 t,计算得到的共享密钥 *S*,计算可得到 *M8*。

4) 更新标签的假名标识符,即:$IDS\_new = IDS \oplus t$。

5) 标签新所有者 *S_new* 将〈*M6*、*M7*、*M8*〉一并发送给标签。

其中有关 *M6*、*M7*、*M8* 的计算公式见表2。

步骤7 标签在接收到标签新所有者 *S_new* 发送来的消息后,标签进行如下操作。

1) 用自身存放的标识符 *IDt*,之前计算得到的随机数 z,接收到的 *M6*,计算可以得到随机数 t,即:$t = M6 \oplus Syn(IDt,$

z)。

2) 用自身存放的标识符 IDt,之前计算得到的随机数 z,接收到的 $M7$,计算可以得到共享密钥 S,即:$S = M7 \oplus Cro(IDt,z)$。

3) 标签用 1)计算得到的随机数 t,用 2)计算得到的共享密钥 S,计算可以得到 $M8'$。然后比对计算得到 $M8'$ 与接收到的 $M8$ 是否相等,若不相等,表明标签新所有者 S_new 是伪造的,协议终止;反之,标签新所有者 S_new 通过标签的真伪验证,进行第 4)步。

4) 标签开始更新自身的标识符假名,更新标签与标签新所有者 S_new 之间的共享密钥,即:$IDS\_new = IDS \oplus t$,$K = M7 \oplus Cro\ (IDt,z)$。

5) 标签将归属权标志位 FLAG 的值由 0 置为 1,即 $FLAG = 1$,表示所有权当前不再归属原所有者,而是归属于标签新所有者 S_new 所有。到此,所有权转移顺利结束。

改进的所有权转移协议具体流程如图 5。

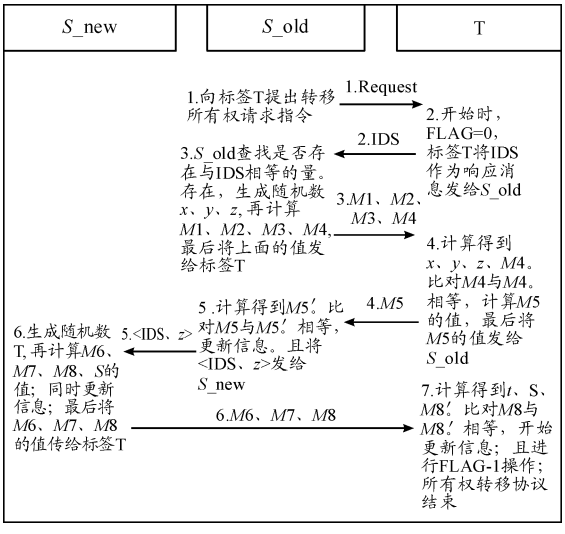

图 5 所有权转移协议的流程

3 协议安全性分析

3.1 同步化攻击

去同步化攻击也称作异步攻击,是指攻击者通过某种手段使得通信实体之间相互认证用到的共享密钥失去一致性,从而导致通信实体之间无法完成下次认证及通信。本文协议中,标签原所有者 S_old 中不仅存放有当前标签的标识符假名 IDS 信息,同时也存放上一次通信过程中用到的标签的标识符假名 IDS_old 信息,因此即便是调用当前标签的标识符假名 IDS 信息比对失败,也可以调用上一次通信过程中用到的标签的标识符假名 IDS_old 信息再次进行比对,从而抵抗住攻击者的去同步化攻击。

3.2 所有权唯一性

所有权唯一性是指标签的所有权归属者必须唯一确定,不存在任何的不确定性。本文协议中,引入归属权标识位 $FLAG$ 变量完成该任务。协议开始之前,归属权标识位 $FLAG$ 变量的值为 0,表明当前标签的所有权归属者为标签原所有者 S_old 拥有,使得标签新所有者 S_new 无法访问标签。在所有权协议转移结束之时,标签中的归属权标识位 $FLAG$ 变量的值为设置为 1,表示所有权转移完成,且当前标签的所有权归属者为标签新所有者 S_new 拥有,同时标签原所有者 S_old 已失去访问标签的权限。整个过程中,标签中的归属权标识位 $FLAG$ 变量的值要么为 0,要么为 1,不可能存在其他状态,使得标签的所有权归属清晰且明确。故协议能够确保所有权的唯一性。

3.3 重放攻击

重放攻击是指攻击者通过窃听某一轮完整的通信过程在获取通信消息之后,重放某通信信息,以破解隐私信息。本文协议中,在不安全的通信实体链路中均采用密文传输机制,攻击者即便是截获通信消息,获取的也只是密文;其次,传输信息加密过程中均混入随机数,且不同的随机数短时间内不会重复出现,加之随机数的难预测性,使得前后两次通信消息并不一样,攻击者无法通过重放上一轮的信息破解出有用信息。因此协议可以抵抗攻击者的重放攻击。

3.4 假冒攻击

协议中有三个通信实体,因此攻击者可以假冒其中任一个通信实体。下面将一一进行讨论。

当攻击者假冒标签时,攻击者伪装成标签向标签原所有者 S_old 发送消息,企图蒙混过关,但攻击者缺少关键隐私信息,比如:缺少标签的标识符 IDt,缺少标签与标签原所有者 S_old 之间共享密钥 K,使得攻击者根本无法计算出随机数 x、y、z,从而更进一步无法计算出通信消息 $M5$ 的正确值。在协议第五步骤中,标签原所有者 S_old 通过简单的计算,便可以识别出标签的真伪,攻击者伪装成标签失败。因此协议可以抵挡攻击者伪装成标签发起的假冒攻击。

当攻击者伪装成标签原所有者 S_old 时,向标签发送信息,攻击者可以自己随意生成随机数 x、y、z,进一步随机选取 IDt、K 的值进行计算得到 $M1$、$M2$、$M3$、$M4$,并一起发送给标签。攻击者这样进行假冒攻击,无法获取任何有用隐私信息,因为标签在第四步骤中对 $M1$、$M2$、$M3$、$M4$ 进行验证过程中,会识别出攻击者的伪造的身份。攻击者缺少正确的 IDt、K 的值,就无法计算出正确的 $M1$、$M2$、$M3$、$M4$ 的值。当标签一旦识别出攻击者假冒身份之后,协议立刻终止。因此协议可以抵抗攻击者伪装成标签原所有者 S_old 发起的假冒攻击。

当攻击者伪装成标签新所有者 S_new 时,向标签发送信息,攻击者因为缺少正确的标签的标识符 IDt,使得攻击者无法正确计算出 $M6$、$M7$、$M8$ 的值。当攻击者把错误的 $M6$、$M7$、$M8$ 传输给标签之后,标签在步骤七中,通过简单的计算便可识别出攻击者的真伪。因此协议可以抵抗攻击者伪装成标签新所有者 S_new 发起的假冒攻击。

3.5 暴力破解攻击

攻击者可以通过监听一个完整的通信过程,获取所有的通信信息,企图采用穷举的方式暴力的破解出一些有用的隐私信息。本文协议能够抵抗攻击者这种暴力的破解攻击,原因如下:(1)本文协议中,但凡涉及到不安全的通信链路,在传输数据时,都是传输密文,而非明文传输;(2)通信信息不仅仅只是密文传输,且信息在加密过程中混入随机数,使得前后两次的通信信息值是不完全一致的,更进一步增大攻击者的破解难度;(3)所有传输的通信信息在加密过程中,都至少有两个量,对于攻击者来说,是不可能知晓的,比如:在公式 $M1 = x \oplus Syn(IDt\_L, K\_R)$ 中,攻击者对于公式里面的三个变量都是不知道,无法采用穷举的方式进行破解。因此协议可以抵抗攻击者发起的暴力破解攻击。

4 BAN 逻辑证明

本文采用 BAN 逻辑对文章中所提的认证协议进行形式化证明,证明过程中做出如下规定:标签新所有者 *S_new* 与标签原所有者 *S_old* 两个通信实体中都含有读写器,将标签原所有者 *S_old* 中的读写器用 *R*1 符号表示,将标签新所有者 *S_new* 中的读写器用 *R*2 符号表示,标签用 *T* 符号表示,证明过程如下。

4.1 协议的理想化模型

消息① $R1 \rightarrow T: REQUEST$;

消息② $T \rightarrow R1: IDS$;

消息③ $R1 \rightarrow T: M1, M2, M3, M4$;

消息④ $T \rightarrow R1: M5$;

消息⑤ $R1 \rightarrow R2: IDS, z$;

消息⑥ $R2 \rightarrow T: M6, M7, M8$。

4.2 协议的初始假设

$P_1: R2 \mid \equiv R2 \overset{S}{\leftrightarrow} T$,表示标签新所有者 *S_new* 中的读写器相信读写器与标签之间的共享密钥 *S*。

$P_2: T \mid \equiv R2 \overset{S}{\leftrightarrow} T$,表示标签相信标签新所有者 *S_new* 中的读写器与标签之间的共享密钥 *S*。

$P_3: R1 \mid \equiv R1 \overset{K}{\leftrightarrow} T$,表示标签原所有者 *S_old* 中的读写器相信读写器与标签之间的共享密钥 *K*。

$P_4: T \mid \equiv R1 \overset{K}{\leftrightarrow} T$,表示标签相信标签原所有者 *S_old* 中的读写器与标签之间的共享密钥 *K*。

$P_5: R2 \mid \equiv R2 \overset{IDS}{\leftrightarrow} T$,表示标签新所有者 *S_new* 中的读写器相信读写器与标签之间的标签的标识符假名 *IDS*。

$P_6: T \mid \equiv R2 \overset{IDS}{\leftrightarrow} T$,表示标签相信标签新所有者 *S_new* 中的读写器与标签之间的标签的标识符假名 *IDS*。

$P_7: R2 \mid \equiv R2 \overset{IDt}{\Leftrightarrow} T$,表示标签新所有者 *S_new* 中的读写器相信读写器与标签之间的标签的标识符 *IDt*。

$P_8: T \mid \equiv R2 \overset{IDt}{\Leftrightarrow} T$,表示标签相信标签新所有者 *S_new* 中的读写器与标签之间的标签的标识符 *IDt*。

$P_9: R1 \mid \equiv R1 \overset{IDS}{\leftrightarrow} T$,表示标签原所有者 *S_old* 中的读写器相信读写器与标签之间的标签的标识符假名 *IDS*。

$P_{10}: T \mid \equiv R1 \overset{IDS}{\leftrightarrow} T$,表示标签相信标签原所有者 *S_old* 中的读写器与标签之间的标签的标识符假名 *IDS*。

$P_{11}: R1 \mid \equiv R1 \overset{IDt}{\Leftrightarrow} T$,表示标签原所有者 *S_old* 中的读写器相信读写器与标签之间的标签的标识符 *IDt*。

$P_{12}: T \mid \equiv R1 \overset{IDt}{\Leftrightarrow} T$,表示标签相信标签原所有者 *S_old* 中的读写器与标签之间的标签的标识符 *IDt*。

$P_{13}: R1 \mid \equiv \#(x)$,标签原所有者 *S_old* 中的读写器相信随机数 *x* 的新鲜性。

$P_{14}: T \mid \equiv \#(x)$,标签相信随机数 *x* 的新鲜性。

$P_{15}: R2 \mid \equiv \#(x)$,标签新所有者 *S_new* 中的读写器相信随机数 *x* 的新鲜性。

$P_{16}: R1 \mid \equiv \#(y)$,标签原所有者 *S_old* 中的读写器相信随机数 *y* 的新鲜性。

$P_{17}: T \mid \equiv \#(y)$,标签相信随机数 *y* 的新鲜性。

$P_{18}: R2 \mid \equiv \#(y)$,标签新所有者 *S_new* 中的读写器相信随机数 *y* 的新鲜性。

$P_{19}: T \mid \equiv R1 \mid \Rightarrow M1$,标签相信标签原所有者 *S_old* 中的读写器对消息 *M*1 的管辖权。

$P_{20}: T \mid \equiv R1 \mid \Rightarrow M2$,标签相信标签原所有者 *S_old* 中的读写器对消息 *M*2 的管辖权。

$P_{21}: T \mid \equiv R1 \mid \Rightarrow M3$,标签相信标签原所有者 *S_old* 中的读写器对消息 *M*3 的管辖权。

$P_{22}: T \mid \equiv R1 \mid \Rightarrow M4$,标签相信标签原所有者 *S_old* 中的读写器对消息 *M*4 的管辖权。

$P_{23}: T \mid \equiv R2 \mid \Rightarrow M6$,标签相信标签新所有者 *S_new* 中的读写器对消息 *M*6 的管辖权。

$P_{24}: T \mid \equiv R2 \mid \Rightarrow M7$,标签相信标签新所有者 *S_new* 中的读写器对消息 *M*7 的管辖权。

$P_{25}: T \mid \equiv R2 \mid \Rightarrow M8$,标签相信标签新所有者 *S_new* 中的读写器对消息 *M*8 的管辖权。

$P_{26}: R1 \mid \equiv T \mid \Rightarrow M5$,标签原所有者 *S_old* 中的读写器相信标签对消息 *M*5 的管辖权。

4.3 协议的安全目标

$G_1: T \mid \equiv M1$,标签相信消息 *M*1。

$G_2: T \mid \equiv M2$,标签相信消息 *M*2。

$G_3: T \mid \equiv M3$,标签相信消息 *M*3。

$G_4: T \mid \equiv M4$,标签相信消息 *M*4。

$G_5: T \mid \equiv M6$,标签相信消息 *M*6。

$G_6: T \mid \equiv M7$,标签相信消息 *M*7。

$G_7: T \mid \equiv M8$,标签相信消息 *M*8。

$G_8: R1 \mid \equiv M5$,标签原所有者 *S_old* 中的读写器相信消

息 $M5$。

4.4 协议的分析推理

由协议的理想化模型中的消息③得 $T \lhd \{M1\}$(T 曾经收到消息 $M1$),并且由初始假设 P_4 和 P_{12} 及消息含义法则 $\frac{P \mid \equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P \mid \equiv Q \mid \sim X}$(若主体 P 相信 P 和 Q 的共享秘钥 K,且 P 曾经收到用 K 加密的密文 X,则 P 相信主体 Q 发送过来的消息 X),得到 $T \mid \equiv R1 \mid \sim M1$。

由假设 P_{14} 及消息新鲜性法则⊕(如果一个消息的一部分是新鲜的,则整个消息也是新鲜的),得 $T \mid \equiv \#(M1)$。

由已经推导出来的 $T \mid \equiv R1 \mid \sim M1$、$T \mid \equiv \#(M1)$ 及随机数验证法则⊕,得到 $T \mid \equiv R1 \mid \equiv M1$。

由 $T \mid \equiv R1 \mid \equiv M1$、初始化假设 P_{19} 以及管辖法则 $\frac{P \mid \equiv Q \Rightarrow X, P \mid \equiv Q \mid \equiv X}{P \mid \equiv X}$,可得 $T \mid \equiv M1$。因此,目标 G_1 得证。

运用上述条件和法则,同理可证得 G_2 至 G_8。此处不再赘述。

5 协议性能分析

本文协议与其他此类 RFID 标签所有权转移协议进行性能分析,分析对象为标签,性能分析主要包括标签一端的计算量、标签一端的存储空间大小等。性能分析结果如表 3 所示。

表 3 性能分析结果

协议	计算量	存储空间
文献[6]	6 *ph*3 + 13 *ph*4	l
文献[8]	3 *ph*3 + 4 *ph*4	$2l$
文献[11]	3 *ph*4 + 2 *ph*6	$2l$
文献[12]	6 *ph*4 + *ph*5 + 2 *ph*6 + *ph*7	$4l$
本文协议	5 *ph*1 + 5 *ph*2 + 15 *ph*4	$3l+1$

对表 3 中的符号进行具体含义说明,说明如下:*ph*1 表示交叉位运算的计算量;*ph*2 表示字合成运算的计算量;*ph*3 表示 HASH 函数操作的计算量;*ph*4 表示位运算的计算量(异或运算、与运算均、移位运算属于按位运算,因位运算属于超轻量级的计算,计算量非常小,因此可将异或运算的计算量、与运算的计算量、移位运算的计算量看成是等量的计算量,用一个相同的符号表示);*ph*5 表示 MIXBITS 函数操作的计算量;*ph*6 表示 *Rabin* 加密算法操作的计算量;*ph*7 表示生成随机数操作的计算量。约定共享密钥 S(或 K)、标签的标识符 *IDt*、标签的标识符假名 *IDS* 的长度均为 l、归属权标志位 *FLAG* 只需要 1 位就可以。

因本文协议中,标签一端事先需要存放的信息有:共享密钥 K、标签的标识符 *IDt*、标签的标识符假名 *IDS*、归属权标志位 *FLAG*,因此标签一端的存储空间大小为($3l+1$)即可满足需求。本文协议与其他协议比较,标签一端满足低成本的要求。

在 *ph*1、*ph*2、*ph*3、*ph*4、*ph*5、*ph*6、*ph*7 中,计算量由大到小依次排列的顺序是:*ph*3、*ph*6、*ph*5、*ph*7、*ph*2、*ph*1、*ph*4。其中 *ph*4 属于超轻量级的计算,相对于 *ph*6、*ph*3 来说,*ph*4 的计算量要远远少于 *ph*6、*ph*3 的计算量,因此 *ph*4 的操作次数多几次,对整体的计算量影响几乎可忽略。*ph*2、*ph*1 是采用移位的方式进行的计算,计算量也不大,两者的计算量相错不大,且小于 *ph*6、*ph*3 的计算量。

从表 3 中,本文协议与其他所有权转移协议进行计算量比较,本文协议摒弃计算量较大的哈希函数及 Rabin 算法加密方法,采用交叉位运算、字合成运算、按位运算进行加密,基于上述分析,本文协议标签端的计算量要少于其他协议的计算量,达到降低标签一端计算量的目标;同时本文协议能够弥补其他协议存在的安全隐患问题。

为进一步解释清楚表中计算量相关数据得来原因,此处选择本协议作为研究对象,进行详细展开讲解;同时考虑到篇幅因素,这里选择对本协议 *ph*2 表示字合成运算的计算量的 5 次数据进行详细讲解。详细过程描述如下:

第 2.2 节步骤四的 1)中,在计算随机数 x 的时候,第一次用到 *ph*2 表示字合成运算。$x = Syn(IDt\_L, K\_R) \oplus M1$。

第 2.2 节步骤四的 3)中,在计算随机数 z 的时候,第二次用到 *ph*2 表示字合成运算。$z = Syn(K\_L, IDt\_R) \oplus Cro(IDt\_L, K\_R) \oplus M3$。

第 2.2 节步骤四的 6)中,在计算 $M5'$的时候,第三次用到 *ph*2 表示字合成运算。$M5' = Syn(x, IDt) \& Cro(K, y) \& z$。

第 2.2 节步骤七的 1)中,在计算随机数 t 的时候,第四次用到 *ph*2 表示字合成运算。$t = M6 \oplus Syn(IDt, z)$。

第 2.2 节步骤七的 3)中,在计算 $M8'$的时候,第五次用到 *ph*2 表示字合成运算。$M8' = Syn(t, S) \& Cro(t, S)$。

6 结论

1)针对现有的所有权转移协议进行分析,指出协议存在的安全缺陷,并在此基础之上设计出一种改进的所有权转移协议。

2)改进的协议为降低标签端的存储空间,将标签的标识符 *IDt* 作为计算中一个参量,从而减少其他参数的引入;改进的协议为确保所有权具备唯一确定性,引入归属权标志位 *FLAG* 变量,根据归属权标志位 *FLAG* 变量的值唯一确定所有权归属问题;改进的协议中采用字合成运算、交叉位运算对传输信息进行加密,能够有效减少通信实体的计算量。

3)安全性分析部分表明本文协议具备完整的安全需求,性能分析部分表明本文协议具备低成本、低计算量的要求。

参考文献:

[1] 刘鹏.一种RFID系统多标签共存证明协议设计[J].兵器装备工程学报,2018,39(2):124-126.

[2] WANG W C,YONA Y,DIGGAVI S N,GUPTA P. Design and Analysis of Stability-Guaranteed PUFs [J]. IEEE Trans. on Info. Foren. And Sec.,2018,13(4):978-992.

[3] 刘道微,凌捷.一种改进的满足后向隐私的RFID认证协议[J].计算机科学,2016,43(8):128-130.

[4] SAITO J,IMAMOTO K,SAKURAI K. Reassignment scheme of an RFID tags key for owner transfer[C]//LNCS 3823: Proc. of Embedded and Ubiquitous Computing—EUC 2005 Workshops. Berlin:Springer,2005:1303-1312.

[5] MOLNAR D,SOPPERA A,WAGNER D. A scalable,delegate able pseudonym protocol enabling ownership transfer of RFID tags[C]//LNCS 3897: Proc. of Selected Areas in Cryptography—SAC 2005. Berlin: Springer, 2005: 276-290.

[6] SONG B. RFID tag ownership transfer[EB/OL]. http://Hrfidsec-2013. iaik. tugraz. at/RFIDSec08/Papers.

[7] SONG B,MITCHELL C J. Scalable RFID security protocols supporting tag ownership transfer[J]. Computer Communications,2011,34(4):556-566.

[8] 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.

[9] MUNILLA J. PEINADO A. YANG G M,et al. Enhanced ownership transfer protocol for RFID in an extended communication model [J/OL]. [2013-04-02]. http://eprint,acr,org/2013/187. pdf.

[10] DOSS R,ZHOU W L,YU S. Secure RFID tag ownership transfer based on quadratic residues[J]. IEEE Trans on Information Forensics and Security,2013,8(2):390-401.

[11] 金永明,孙惠平,关志,等.RFID标签所有权转移协议研究[J].计算机研究与发展,2014,48(8):819-824.

[12] XIE R,JIAN B Y,LIU D W. An Improved Ownership Transfer for RFID Protocol[J]. International Journal of Network Security,2018,20(1):149-156.

[13] GOPE P,LEE J,QUEK T Q S. Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks[J]. IEEE Sensors Journal,2017,17(2):498-503.

[14] WANG W C,YONA Y,DIGGAVI S N,GUPTA P. Design and Analysis of Stability-Guaranteed PUFs [J]. IEEE Trans. on Info. Foren. And Sec.,2018,13(4):978-992.

[15] 蓝耿,刘道微.基于字合成运算的群组RFID标签所有权转移协议[J].计算机工程,2017,43(8):151-155.

[16] XIE R,LING J,LIU D W. Wireless Key Generation Algorithm for RFID System Based on Bit Operation[J]. International Journal of Network Security,20(5):938-949.

(责任编辑 杨继森)