一种全新的 RFID 标签所有权转移协议

甘 勇 王 凯 贺 蕾

(郑州轻工业学院计算机与通信工程学院 郑州 450002)

摘 要 RFID 标签在所有权转移过程中面临安全和隐私泄露的风险。针对这一问题,提出了一种带有转移开关并基于 Hash 函数的新型标签所有权转移协议。原所有者和新所有者分别拥有不同的通信密钥,前者的密钥用于原所有者与标签之间的认证,后者的密钥用于标签与新所有者之间的所有权转移。由于存在转移开关(Ownership Transfer Switch,OTS),因此可以通过对 OTS 的设置来实现抵抗去同步化攻击。对该协议的安全性分析结果表明,该协议能够满足标签所有权转移的安全需要,并能抵抗常见的主被动攻击,使标签的所有权实现完全转移。最后对协议进行了性能分析,结果表明所提协议在效率性能方面比已有的 RFID 标签所有权转移协议有明显提高。

关键词 无线射频识别,所有权转移,认证,转移开关,哈希函数,去同步化攻击

中图法分类号 TP393.04 **文献标识码** A

New Ownership Transfer Protocol of RFID Tag

GAN Yong WANG Kai HE Lei

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

Abstract There exists risk of security and privacy disclosure in the process of ownership transfer of RFID tag. Thus a new tag ownership transfer protocol with transfer switch based on Hash function was proposed . The original owner and the new owner have different communication keys respectively,the former key is used for authentication between the original owner and the tag while the latter key is for ownership transfer between the tag and the new owner. Because of the transfer switch, namely OTS, it is possible to implement OTS configuration to resist desynchronization attack through OTS configuration. The safety analysis of the protocol shows that the protocol can meet the safety requirements of tag ownership transfer and resist common active and passive attack,thus achieving complete transfer of tag ownership. Finally,the performance of protocol was analyzed and the results show that efficiency performance of proposed protocol is significantly improved compared with existing ownership transfer protocol of RFID tag.

Keywords Radio frequency identification(RFID),Ownership transfer,Authentication,Ownership transfer switch,Hash function,Desynchronization attack

RFID(Radio Frequency Identification)技术是一种不需要直接与对象物理接触,而是通过无线电波主动进行数据捕获和数据存储的技术,并且捕获的数据可以用于唯一地识别对象[1]。作为一种能存储无线通信信息及实时自动识别和跟踪物体的技术,RFID 技术被认为是物联网时代最重要的技术之一。随着 RFID 技术的不断发展及其在国民经济各个领域中的广泛应用,RFID 标签安全和隐私保护问题也日渐突出,RFID 标签所有权的安全转移成为了当前 RFID 技术应用的热点问题之一,因此如何安全地转移标签所有权这一问题值得深入研究。目前已经存在的方法是通过设计密码协议来完成所有权的转移,对于较低成本的 RFID 系统,设计安全、高效、可靠的 RFID 标签所有权转移协议是本文研究的重点。针对上述情况,本文提出了一种带有转移开关并基于 Hash 函数的新型 RFID 标签所有权转移协议。

1 相关工作

RFID 系统本身的安全和隐私泄露问题已经制约了其发展,但涉及到多个 RFID 系统协调工作时,不仅要求原所有者把某些共享信息发送给新所有者,同时还要保证新所有者不能得到其中的机密信息,并且原所有者也不可以继续访问该标签[2]。下面就已存在的几个所有权转移协议进行简要分析。

文献[3]基于是否带有可信第三方提出了两种不同的协议,第一种涉及可信第三方的协议,第二种没有用可信第三方,但这两种协议也仅涉及到密钥交换,它需要结合其他的安全认证协议来实现所有权的转移。文献[4]设计了一个可以实现所有权完全转移的双向认证协议,但该方案中标签的成

本文受国家自然科学基金(61572445,61772477),河南省高等学校重点科研项目(16A520075)资助。

甘 勇(1965-),男,博士,教授,CCF 会员,主要研究方向为分布式计算机系统、计算机网络、信息安全;**王 凯**(1993-),男,硕士生,主要研究方向为无线网络安全、RFID 密码协议安全,E-mail:2403411494@qq.com(通信作者);**贺 蕾**(1980-),男,讲师,主要研究方向为无线网络安全、密码学、软件安全与保护。

本和计算量都较高。

文献[5]也针对标签所有权转移提出了一套符合 RFID 系统安全需求的 RFID 安全机制。在该协议中,标签用对称密钥对其 ID 加密并将其作为唯一标识。当标签进行所有权转移时,协议通过改变对称密钥来实现该目标,从而使得原所有者和新所有者的安全信息得以保护。但是通过分析发现,其仍然无法抵抗去同步化攻击,而且攻击者很容易进行跟踪。文献[6]对这些安全漏洞如何影响其安全参数进行了详细描述。此后,其他的一些研究学者对文献[5]中的协议进行了改进,如文献[7]以及文献[8]中提出的改进协议。前者修改了后端数据库发给阅读器以及阅读器发给标签的最后一条信息;后者添加了一条由阅读器发给标签的消息。但两者的计算复杂度较高。文献[9]也基于文献[5]进行了改进,提出了一种简单有效的所有权转移协议。在该方案中,标签并不存储自己的身份标识 ID,而是存储加密后的身份标识 ID,将其作为自己的一个假名并用于认证通信。该协议虽然修正了原方案中的一些缺陷,提高了原方案的执行效率,但是不能抵抗跟踪攻击。

文献[10]提出了一个由 3 个子协议组成的标签所有权转移机制,该机制通过所有权转移、密钥值更新和授权恢复 3 个子协议来解决所有权转移过程中的各种安全问题,其中所有权转移协议和密钥值更新协议是基于 SM 协议[11]的。首先通过执行所有权转移协议来获得标签的所有权,接着再执行密钥值更新协议以对标签的密钥进行更新,从而确保新所有者的信息安全。但该协议不能抵抗去同步化攻击,并且协议的整体执行过程较复杂,可以对其做进一步的改善。

文献[12]利用 Hash 函数技术设计了一种安全高效的 RFID 所有权转移协议。在该协议中,当所有者要进行所有权更新时,首先需要生成一个随机数,并向标签发送密钥更新信息;标签收到消息后,根据收到的信息以及自己存储的信息对其进行验证,如果验证成功就更新密钥,并将其发送给所有者。但该协议也存在漏洞,即标签和后端数据库不能同时更新密钥,这样不能很好地抵抗去同步化攻击,并且在对标签进行认证时,需要依次从后端数据库中读取信息进行计算,看其是否与收到的信息匹配,因此不适合在标签的整个周期内使用。

文献[13]提出了一种基于 SQUASH 方案的轻量级所有权转移协议,但该协议中存在不安全的因素,例如不能很好地抵御去同步化攻击。文献[14]详细地论述了文献[13]中所提协议存在的安全漏洞:攻击者可以通过三轮的窃听、重放以及假冒,最终使所有者与标签共享的密钥不相同,使攻击者能够成功地实施拒绝服务攻击和重放攻击。因此,该协议提出了改进的轻量级所有权转移协议,该协议虽然很好地弥补了该安全漏洞缺陷,但经研究发现,其仍然存在新的安全漏洞和成本花销问题。

文献[15]详细地阐述了文献[14]中存在的安全漏洞和成本问题,并提出了一种基于密钥共享的超轻量级 RFID 标签所有权转移协议,该协议可以抵御去同步化攻击,拒绝服务攻击、重放攻击、假冒攻击、中间人攻击,以及能够保护标签信息的前向安全。但是,该协议并不能有效地保护标签信息的后向安全。

文献[16]提出了一种改进的基于 Rabin 加密算法的 RFID 标签所有权转移协议,该协议采用挑战响应机制,利用 Status 标志位来标志标签当前所有权的归属,虽然该协议具有很好的安全性,但是其计算量、通信量和所占存储空间花销太大,不适用于低成本标签。文献[17]提出了一种基于云计算的 RFID 标签所有权转移协议,这是一个可证明安全的 RFID 标签所有权转移协议,但是该协议的成本花销太大。

综上,现有协议有各自的优势,同时也都存在着不同的安全问题。因此,本文提出了一种带有转移开关并基于 Hash 函数的新型标签所有权转移协议,标签与原所有者和新所有者分别共享不同的密钥值,并能满足所有权转移过程中的安全需求,实现了所有权的完全转移。

2 标签所有权转移协议的描述

2.1 安全需求

由于 RFID 标签和阅读器之间使用的是无线网络通信,在这固有的特性下任何实体都可以进行消息的发送和接收,加上 RFID 有限的计算能力和存储能力,使得 RFID 系统在这信道上极易受到各种攻击。RFID 系统的工作原理如图 1 所示。

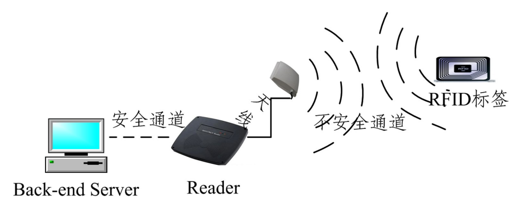

图 1 RFID 系统的组成结构

结合实际需要,RFID 标签所有权转移协议需要满足的安全需求有如下含义:

1)原所有者无关性(Independence of Old Owner,IOO),指所有权成功转换后,标签的所有权不再为原所有者所拥有,而为新所有者唯一拥有,原所有者不能再对标签进行任何操作。

2)能抵御常见的主动攻击和被动攻击,例如去同步化攻击(Desynchronization Attack,DA)、假冒攻击(Impersonation Attack,IA)、中间人攻击(Man-in-the-Middle Attack,MITM)、重放攻击(Replay Attack,RA)、拒绝服务攻击即异步攻击(Denial of Service,DoS)等。

3)标签信息的前向安全性(Forward Security,FS)和后向安全性(Backward Security,BS)。前者指的是新所有者即便获取了标签的控制权,并且窃听了原所有者与标签之间的所有通信信息,也无法获取原所有者与标签此前的秘密信息;后者指的是所有权转移后,原所有者无法获取标签与新所有者之间通信的所有秘密信息。

2.2 协议描述

在该协议中,原所有者和新所有者与标签分别共享不同的密钥,标签内设置了一个所有权转移开关 OTS,其取值为 0 或者 1。当进行所有权转移时,转移开关 OTS 取值为 1,即转移开关 opening;当所有权转移过程结束时,转移开关 OTS 取值为 0,即转移开关 closing。

下面说明协议中用到的符号含义,如表 1 所列。

表 1 协议中变量的定义

PO(previous owner)	标签的原所有者。
NO(new owner)	标签的新所有者。
S	新所有者与标签进行所有权转移的密钥，在所有权转移开关 OTS 打开之前为原所有者所储存。
S_{PO}	PO 与标签共享的密钥，长度为 L 比特。
S_{NO}	NO 与标签通信的新密钥，长度为 L 比特。
OTS	所有权转移开关，长度为 1bit，只读。OTS 为 0 表示原所有者对标签具有控制所有权，OTS 为 1 表示标签同意进行所有权转移，原所有者将对标签的控制所有权转移给新所有者。
$H_x()$	对变量 x 进行 Hash 运算，输出函数长度均为 L 比特的字符串。
OTR(ownership transfer request)	所有权转移申请。
OTF(ownership transfer failure)	所有权转移失败消息。
OOR(ownership obtain request)	所有权获取请求。
$Q_i(i=1,2,3,\cdots)$	协议中的通讯信息数据。$R_i(i=1,2,3,\cdots)$ 为所有权转移过程中生成的随机数，长度均为 L 比特。
ID_{PO}	原所有者的唯一身份标识。
ID_{NO}	新所有者的唯一身份标识。

为了便于研究，现假设原所有者与新所有者之间的通信信道是安全可靠的，而其他信道是不安全的。协议转移流程如下：

1)原所有者向标签发出所有权转移申请 OTR，并生成随机数 R_1，发送$\{OTR, R_1, ID_{PO}\}$给标签 Tag。

2)标签 Tag 收到信息后，检查 ID_{PO}是否与自己后端数据库存储的一致。若不一致，则终止协议；若一致，则标签生成随机数 R_2，同时计算 $Q_1=H_{S_{PO}}(R_1, R_2)$，并发送 Q_1 和 R_2 给原所有者 PO。

3)原所有者收到标签发来的 Q_1 和 R_2 后，用自己与标签共享的密钥 S_{PO}来计算 $Q_1'=H_{S_{PO}}(R_1, R_2)$与收到的 Q_1 是否相等。若相等，则对标签的认证，计算 $Q_2=H_{S_{PO}}(R_2, R_1)$发送给标签 Tag，若不相等，则协议停止执行。

4)标签收到原所有者发来的信息 Q_2 后，用自己的后端数据库事先存储的 R_1，R_2 来计算 $Q_2'=H_{S_{PO}}(R_2, R_1)$是否与之相等，若不相等，则协议停止运行；若相等，则对原所有者进行认证，并认为原所有者要进行所有权转移，即将对标签的控制所有权转移给其他通信实体，此时标签将 OTS 所有权转移开关设置为 1，并生成随机数 R_3，发送 OTS，R_3，Q_1，Q_2 给新所有者 NO。

5)新所有者收到标签发来的信息后，检查 OTS 的值是否为 1，若不为 1，则表示所有权转移开关并未打开，此前原所有者并没有与标签进行所有权转移过程，此时发送 OTF 给原所有者，通知原所有者标签中的 OTS 所有权转移开关没有打开，需要原所有者重新从步骤 1)开始执行，直到打开所有权转移开关为止。若 OTS 的值为 1，则表示所有权转移开关已经打开，新所有者发送 OTS，Q_1，Q_2 给原所有者。

6)原所有者收到新所有者发来的信息后，检查收到的 OTS，Q_1，Q_2 是否正确，若不正确，则协议停止；若正确，则认为所有权转移开关 OTS 已经打开，可以进行所有权的转移，并将密钥 S 发送给新所有者。

7)新所有者收到原所有者发来的密钥 S 后，开始与标签进行通信，生成随机数 R_4，发送 S，R_4，ID_{NO}，OOR 给标签。

8)标签收到新所有者发送的消息后，检查密钥 S 是否与自己后端数据库存储的一致，若不一致，则协议终止运行；若一致，则表示原所有者同意将对标签的控制所有权转移给新的所有者，此时标签更新原来的密钥，并生成新的密钥 S_{NO}，标签生成随机数 R_5，并计算 $Q_3=H_{S_{NO}}(R_4, R_5)$，发送 R_5，Q_3，S_{NO}，ID_{NO}给新所有者。

9)若新所有者长时间没有收到标签的信息，或收到的信息不正确，则需要从第 7)步重新开始执行。若新所有者收到了标签的信息，并且收到的 $H_{S_{NO}}(R_4, R_5)$正确，则表示标签同意新所有者对其获得控制所有权，所有权转移过程已经完成，新所有者与标签之间可以使用新的密钥 S_{NO}进行通信。图 2 是协议转移的流程图。

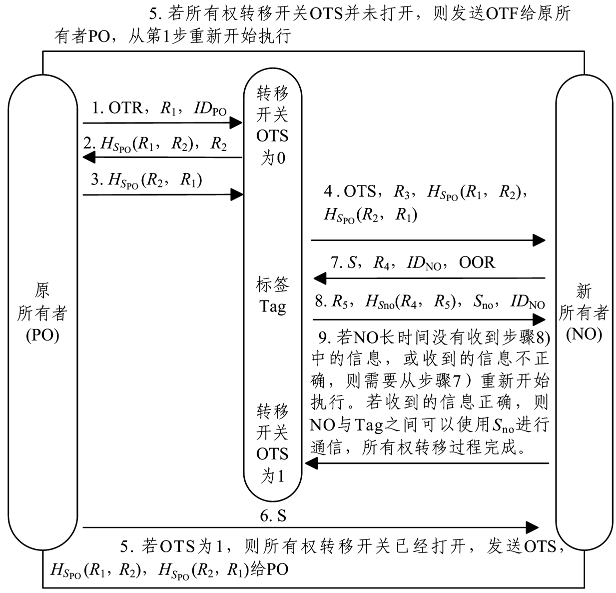

图 2 协议转换流程图

3 安全性分析

3.1 原所有者无关性

在本文协议中，原所有者和新所有者与标签分别共享不同的密钥，因此原所有者无法知道新所有者与标签共享的密钥，同时新所有者也无法知道原所有者与标签共享的密钥。首先，协议执行前，新所有者无法得到原所有者与标签之间的共享密钥 S_{PO}，所有权转移开关 OTS 并没有打开，因此标签的控制所有权属于原所有者，新所有者并未拥有。RFID 标签的物理特性是标签的所有权不会自发地发生转移，只有原所有者发出所有权转移申请时，所有权才会发生转移，因此当所有权发生转移后，这个过程是不可逆的。因此，当原所有者发送 S 给新所有者时，新所有者与标签之间完成所有权转移过程，并更新密钥为 S_{NO}，原所有者此时不具有 S，并且也没有拥有标签的所有权，原所有者也无法得知新所有者与标签之间通信的新密钥 S_{NO}，标签被新所有者唯一拥有。因此，该协议能够实现标签所有权的完全转移，并具有原所有者无关性。

3.2 抵抗常见的主被动攻击

1)去同步化攻击

该协议可以抵抗去同步化攻击,具体分析如下:当所有权转移过程遭受到去同步化攻击时,会导致后端数据库存储的密钥和标签中正在使用的密钥不一致;此时,NO与Tag可以通过查看所有权转移开关OTS的值来判断是否遭受到了攻击,如果遭受到攻击,NO与Tag之间可以协商出新的密钥值进行通信。因此该协议可以抵抗去同步化攻击。

2)假冒攻击

假设攻击者假冒原所有者PO,当协议执行到步骤3)时,假冒PO的攻击者无法获得S_{PO},从而无法计算出正确的Q_1发送给标签进行认证,不能通过标签的认证,因此原所有者是不能被假冒的。类似地,对于新所有者,由于攻击者无法正确地计算出Q_1,对于步骤6),就无法继续进行,冒充新所有者的攻击者也不会得到密钥S,也就无法与标签进行所有权转移过程,进而不能与标签进行合法的通信。因此,假冒攻击对于该协议是无效的。

3)中间人攻击

由于标签与读写器之间传播的信道是不安全的,且是无线传播方式,攻击者可以窃听信息Q_1,Q_2,Q_3来进行攻击。如果攻击者想要篡改或者更换信息,则很难通过标签的认证。该协议满足了PO与Tag之间的双向认证,同时也满足了NO与Tag之间的双向认证,并协商出新的通信密钥进行通信。因此,该协议能够抵抗中间人攻击。

4)重放攻击

攻击者如果试图重放消息Q_3来误导新所有者,使新所有者不知道接收到的消息Q_3是否为标签发来的,也不知道标签是否同意进行所有权转移;此时,由于在步骤7)和步骤8)中新所有者和标签都生成了一个新的随机数R_4和R_5,因此当新所有者接收到消息Q_3时,可以通过自己生成的新随机数R_4来进行检查,也可以重新发送Q_3给标签以验证其新鲜性,看接收到的消息是否为重放消息。由于协议执行过程中不断地生成新的随机数,因此保证了协议消息发送的新鲜性,能够抵御重放攻击。

5)拒绝服务攻击

通过对所有权转移开关OTS的设置,标签可以确定是否进行所有权转移,并且新所有者NO只有在OTS打开之后才能与标签之间的所有权转移,因此不会出现标签的所有权在某一时刻不被任何所有者所拥有,标签的控制所有权只能被PO或者NO唯一拥有。因此,该协议能够很好地抵抗拒绝服务攻击。

3.3 前向安全和后向安全

原所有者和新所有者与标签共享不同的通信密钥,S_{PO}用于PO与标签之间的通信认证,不直接参与所有权转移过程;S用于新所有者与标签进行通信认证;S_{NO}是新所有者与标签通信的新密钥。因此,原所有者在进行所有权转移时,将密钥S直接发给新所有者,不使用S进行认证,保护了标签信息的前向安全。当原所有者与标签认证完毕后,将密钥S发送给新所有者,此后新所有者与标签进行认证,并协商出新的通信密钥S_{NO},保护了标签信息的后向安全。

通过分析文献[5,9-10,13-15]的安全性,表2给出本文协议与其他几种协议的安全性对比,可以看出本文协议比其他几种协议在安全性方面有较大的优势。

表2 所有权转移协议的安全性对比

攻击类型	文献[9]	文献[10]	文献[13]	文献[14]	文献[15]	文献[16]	本文协议
去同步化攻击	√	×	×	×	√	√	√
重放攻击	×	√	√	√	√	√	√
假冒攻击	√	×	×	×	√	√	√
中间人攻击	√	√	√	√	√	×	√
拒绝服务攻击	×	×	√	×	√	√	√
前向安全	√	×	√	√	√	√	√
后向安全	√	√	√	√	×	√	√
原所有者无关性	×	×	√	√	×	×	√

注:√ 表示满足安全性;×表示不满足安全性

4 性能分析

本节主要从3个方面对该协议进行性能分析,包含标签计算量、存储量和通信量,如表3所列。其中,h表示计算哈希函数的计算量,R表示Rabin加密方案的运算量,p是异或运算量,q是移位运算量,t是与运算量,Cro是交叉位运算量,L是密钥的长度,T表示标签所有权转换过程中的临时存储空间,l为标签通信量的单位。

标签计算:该协议中标签在步骤2),4),8)中计算了哈希函数共3次,因此标签的计算量为$3h$。

标签存储:在所有权转移开关OTS打开前,标签内存储了3个变量,包含原所有者与标签共享的密钥S_{PO}、新所有者与标签进行所有权转移的密钥S,以及所有权转移开关OTS。其中,S_{PO}和S的长度均为L,而所有权转移开关OTS为1 bit,此时标签的存储量为$2L+1$ bit,当所有权转移开关OTS打开后,新所有者与标签进行所有权转移时,标签将存储密钥S,并会生成新的通信密钥S_{NO},废弃掉原有的通信密钥S_{PO},加上所有权转移开关OTS占有的存储1 bit,此时标签的存储量仍为$2L+1$ bit。

标签通信:在整个通信过程的步骤1)—步骤8)中,标签端发出的通信量共有10个,若通信设备的传输长度为l,则标签的通信量为$10l$。

表3 所有权转移协议的性能对比

所有权转换协议	标签计算	标签存储	标签通信
文献[5]协议	$h+2p$	L	$3l$
文献[10]协议	$6h+9p+4q$	L	$9l$
文献[13]协议	$3p+2R$	$L+T$	$2l$
文献[14]协议	$6p+2R$	$3L+T$	$2l$
文献[15]协议	$6p+4q+3Cro$	$2L+T+1$	$2l$
文献[16]协议	$8p+7t+4R$	$4L+1$	$11l$
本文协议	$3h$	$2L+1$	$10l$

从表3可以看出,本文协议较其他协议在标签计算复杂度方面有明显的优势,标签所需的存储量也不大,标签的通信量在可接受的范围内。

结束语 随着RFID技术的不断发展及其在各个领域的

(下转第392页)

像(一般情况下,可分解成若干低像素值的图像)。即使攻击者截取到一些图像,破解也会出现一定的困难。如果攻击者获取的载密图像不完整或者在合成加密图像时的组合矩阵出现顺序错误,也可能破解不成功。只有将所有的载密图像都接收,且提取的所有低像素加密图像在合成时组合矩阵的顺序也正确后,才可能从所有的载密图像中提取完整的加密信息。攻击者想要获取解密后的真实图像,也需要经过大量的对合矩阵的计算,这极大地增加了破解的难度。

结束语 本文阐述了一种基于对合矩阵、矩阵分解和信息隐藏相结合的图像加密方法。原始图像通过对合矩阵加密后分解为若干低像素值的图像,再隐藏到掩护图像中。与单一使用对合矩阵加密、隐藏强度参数对比,该方法不仅实现了加密的目的,而且减少了加密图像在传输过程中的可感知性,防止图像信息被破坏和损毁,增强了抗攻击能力,为原始图像增加了双层保护。实例验证,这种方法的安全性能较高,加密和隐藏的效果良好。这项图像加密技术无论从理论上还是应用上都具有良好的研究价值。

参 考 文 献

[1] 杜长斌.基于JPEG算法的数字图像压缩技术应用研究[D].哈尔滨:黑龙江大学,2013.

[2] VAFERI E,SABBAGHI-NADOOSHAN R. A New Encryption Algorithm for Color Images based on Total Chaotic Shuffling Scheme[J]. Optik-International Journal for Light and Electron Optics,2015,126(20):2474-2480.

[3] KANSO A,GHEBLEH M. An algorithm for encryption of secret images into meaningful images[J]. Optics & Lasers in Engineering,2017,90(3):196-208.

[4] WIKRAMARATNA R S. The centro-invertible matrix:A new type of matrix arising in pseudo-random number generation[J]. Linear Algebra & Its Applications,2011,434(1):144-151.

[5] LEBTAHI L,ROMERO O,THOME N. Characterizations of {K,s+1}-potent matrices and applications[J]. Linear Algebra & Its Applications,2012,436(2):293-306.

[6] CONNELL E H. Elements of Abstract and Linear Algebra[J]. American Mathematical Monthly,1999,81(3):301.

[7] ASHRAFI N,SHEIBANI M,CHEN H. Certain decompositions of matrices over abelian rings[J]. Czechoslovak Mathematical Journal,2017,67(2):1-9.

[8] 邢坤.二次Arnold变换与中心可逆矩阵研究[D].哈尔滨:东北林业大学,2015.

[9] 申健,雷菁,李保国,等.一种新型信息隐藏技术的研究与实现[J].通信技术,2013,46(2):100-102.

[10] 闫伟齐.数字图象信息隐藏中的数学方法及应用研究[D].北京:中国科学院研究生院(计算技术研究所),2001.

[11] 李用江.数字图像置乱算法的研究[D].西安:西安电子科技大学,2011.

(上接第372页)

广泛应用,所有权的转移也成为了RFID系统的一个重要特征,与此同时,所有权转移的安全问题也日益突出。本文提出了一种带有转移开关并基于Hash函数的新型RFID标签所有权转移协议。经安全性分析,该协议能够满足标签所有权转移的安全需求,具备原所有者无关性,并能够抵御重放攻击、假冒攻击、中间人攻击、去同步化攻击、拒绝服务攻击,保护标签信息的前向安全和后向安全。同时经性能分析,该协议中标签的计算量较低,标签所需存储量和标签通信量都在可接受的范围内,适合低成本RFID标签系统。下一步的研究工作是在不降低标签安全性的前提下,更进一步降低标签所需的存储量和通信量。

参 考 文 献

[1] 周永彬,冯登国.RFID安全协议的设计与分析[J].计算机学报,2006,29(4):581-589.

[2] 邵婧,陈越,常振华.RFID标签所有权转换模式及协议设计[J].计算机工程,2009,35(15):143-145.

[3] SAITO J,IMAMOTO K,SAKURAI K. Reassignment Scheme of an RFID Tag's Key for Owner Transfer[M]// LNCS 3823: Proceedings of Embedded and Ubiquitous Computing-EUC2005 Workshops. Berlin:Springer,2005:1303-1312.

[4] LIM C H,KWON T. Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer[M]// Information and Communications Security. Springer Berlin Heidelberg,2006:1-20.

[5] OSAKA K,TAKAGI T,YAMAZAKI K,et al. An Efficient and Secure RFID Security Method with OwnershipTransfer[C]// Proceedings of Computational Intelligence and Security-CIS 2006. Berlin:Springer,2006:778-787.

[6] LEI H,CAO T. RFID Protocol Enabling Ownership Transfer to Protect against Traceability and DoS Attacks[C]// IEEE International Symposium on Data. Wuhan,China,2007:508-510.

[7] YOON E J,YOO K Y. Two security problems of RFID security method with ownership transfer[C]// IFIP International Conference on Network and Parallel Computing. Washington D C: IEEE,2008:68-73.

[8] CHEN H B,LEE W B,ZHAO Y H,et al. Enhancement of the RFID security method with ownership transfer[C]// Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication. ACM,2009:251-254.

[9] JAPPINEN P,HAMALAINEN H. Enhanced RFID security method with ownership transfer[C]// Proceedings of 2008 Interational Conference on Computational Intelligence and Security. Piscataway,NJ:IEEE,2008:382-385.

[10] SONG B. RFID tag ownership transfer[C]// Proceedings Workshop on RFID Security. 2008.

[11] SONG B,MITCHELL C J. RFID authentication protocol for low-cost tags[C]// Proceedings of ACM Conference on Wireless Network Security-WiSec'08. New York:ACM,2008:140-147.

[12] DIMITRIOU T. rfidDOT:RFID delegation and ownership transfer made simple[C]// International Conference on Security and Privacy in Communication Netowrks. ACM,2008:34.

[13] 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,2011,48(8):1400-1405.

[14] 沈金伟,凌捷.一种改进的超轻量级RFID所有权转移协议[J].计算机科学,2014,41(12):125-128.

[15] 苏庆,李倩,张俊源,等.基于共享密钥的超轻量RFID标签所有权转移协议[J/OL].[2017-02-27]. http://kns.cnki.net/kcms/detail/11.2127.TP.20170227.1544.042.html.

[16] 吴伟民,陈超雄,蓝炯江,等.基于Rabin加密算法的RFID标签所有权转移协议[J].计算机应用研究,2017,34(5):1531-1535.

[17] CAO T,CHEN X Q,ROBIN D,et al. RFID ownership transfer protocol based on cloud[J]. Computer Networks,2016,105(32):47-59.