图书馆 RFID 安全认证协议①

周朝阳　(湖北大学 图书馆 湖北 武汉 430062)

摘　要： 分析了 RFID 技术的安全性问题，构建了图书馆 RFID 系统的安全模型，设计了一个确保图书馆 RFID 系统安全性的认证协议 PA-Lock 协议，以解决标签与读写器之间的保密和双向鉴别问题。最后，对 PA-LOCK 协议进行了安全性能分析并与其他协议做了比较，证明了该协议的安全性和高效性。

关键词： 射频识别；保密 ；鉴别；认证协议；协议设计

RFID Security Authentication Protocol in the Library

ZHOU Zhao-Yang (Library, Hubei University, Wuhan 430062, China)

Abstract: This paper analyzes the security problems of RFID technology, builds the security model of RFID in library, designs a security protocol PA-Lock, which ensures the security of library RFID system. This paper solves the privacy and mutual authentication between Tag and Tag reader. Lastly, this paper analyzes the security and performance of PA-Lock protocol and compares it with other protocols to prove that PA-Lock protocol is secure and efficient.

Key words: RFID; privacy; authentication; authentication protocol; protocol design

1　引言

射频识别(radio frequency identification，RFID) 是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据。RFID 可广泛应用于工业自动化、商业自动化、交通运输控制管理、图书管理系统等众多领域[1]，被列为本世纪十大重要技术之一。

RFID 技术在图书馆领域的应用实践正在蓬勃发展之中：Molnar 2004 年指出北美有超过 130 家图书馆使用 RFID 系统[2]。在国内，厦门集美大学诚毅学院于 2006 年 2 月率先成为国内第一家使用 RFID 馆藏管理系统的图书馆；随后深圳图书馆新馆也选择 RFID 系统作为图书馆服务体系改进的技术手段[3]；接着，武汉图书馆成为第三家研发并全线使用 RFID 智能馆藏管理系统的图书馆[4]。

保密和鉴别等安全问题是当前 RFID 技术的研究热点，而且不同的应用领域对 RFID 安全性的要求也不尽相同。为了保障图书馆应用环境下 RFID 系统的安全性，有必要对安全需求进行系统的研究，并提出安全的解决办法。

本文将针对 RFID 技术在图书馆文献管理中的应用，来探讨其认证协议问题。本文首先分析了 RFID 系统的组成结构及安全协认证议研究现状，在构建了图书馆 RFID 系统安全模型的基础上，设计了一个保证图书馆 RFID 系统安全通信的认证协议：PA-Lock 协议，最后，对该 PA-LOCK 协议进行了安全性能分析并与其他协议做了比较。

2　RFID系统构成及安全协议现状

本部分简要介绍 RFID 系统的基本组成结构、通信模型和安全协议的研究现状。

2.1 RFID 系统组成

RFID 系统一般由三大部分组成：RFID 标签(tag)、RFID 读写器(reader)和后端数据库(database，后端服务器)，如图 1 所示。

1) RFID 标签：由芯片和耦合元件(天线)构成，芯片用于计算，天线用于无线通信，芯片的计算和存储能力十分有限。每个标签具有唯一的电子编码。

① 收稿时间:2010-01-14;收到修改稿时间:2010-03-01

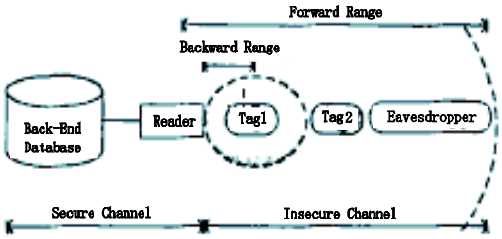

图 1 图书馆 RFID 系统组成[5]

2) RFID 读写器：由射频接口和控制单元组成，其计算能力和存储能力都比较大，RFID 读写器通过射频接口来获取标签中的数据，并将其传递给后端数据库。RFID 读写器和标签之间的信道是不安全信道。

3) RFID 后端数据库：接收来自 RFID 读写器的数据，存储有标签的信息或关联信息，RFID 读写器和后端数据库之间是安全信道。

2.2 RFID 安全认证协议研究现状

RFID 技术的无线传输、信号广播以及标签只具有很弱的计算能力等特征对 RFID 系统安全机制的设计提出了特殊的要求，设计安全、高效、低成本的 RFID 协议一直是一个具有挑战性的课题。

使用密码学方法来设计 RFID 安全认证协议是一种主要的研究方法。迄今为止，已经有许多 RFID 安全认证协议被提出。这些协议大致可以分为两类：一类是从协议的通用安全性方面着手设计，如 Hash-Lock 协议、Hash 链协议、基于杂凑的 ID 变化协议等[6]，这些认证协议主要解决在标签识别过程中的安全问题，如保密性、信息泄露、和不可追踪性等；另一类是从应用领域的特殊性方面来着手设计 RFID 安全认证协议。通过详细分析应用的特性过程，对 RFID 安全问题作针对性的设计，使之满足该应用领域的需求，如供应链环境下通用可组合安全的 RFID 通信协议，该协议就是通过对供应链管理领域中 RFID 技术的安全机制进行深入的研究，从而设计出具有应用针对性的 RFID 安全认证协议。

与其他特定的 RFID 应用领域一样，图书馆文献资源管理领域的特点也对 RFID 安全协议提出了特殊的需求。其特点主要表现在以下几个方面：

1) 图书在整个流通期间具有两个状态：在馆典藏状态和外借状态。图书管理中对不同状态的图书具有不同的约束规则，如对于在馆典藏状态的图书则不允许被带出图书馆，而对于外借状态的图书则可以自由出入图书馆。

2) 图书的状态变化具有周期性。每本图书从在馆典藏状态开始，经外借状态再回到在馆典藏状态，周而复始，循环变化。

3) 图书管理需要对图书进行实时跟踪、状态定位以及统计分析。分析图书的使用状况及利用率。

目前，还没有针对图书馆文献资源管理中 RFID 安全机制的深入研究成果。本文的重点是针对图书馆文献资源管理中的各种主要流程，分析设计出对 RFID 标签认证识别的安全认证协议，保证只有授权用户才能够识别特定标签，同时攻击者无法对这些标签进行跟踪。

3 图书馆RFID安全需求建模

设计 RFID 安全认证协议的一个重要前提就是需要定义 RFID 系统的安全模型。安全模型又与系统的实际应用场景有着密切的联系。因此，在设计图书馆 RFID 系统安全认证协议之前，首先要详细分析图书馆 RFID 系统的应用模型、主要的安全威胁以及系统的安全需求等问题。

3.1 图书馆 RFID 系统模型

通常情况下，图书馆 RFID 系统有标签、读写器和后台数据库三部分组成。由于读写器和后台数据库之间是安全信道，所以，我们在设计安全协议时，把这两部分作为一个整体来考虑，因此，主要关心读写器和标签两部分。对于标签，我们假设既有鉴定合法的标签，也有恶意的标签。而读写器主要有四类：标签转换器、排架器、自助借还机和安全检测门。标签转换器主要用于实现从条码到 RFID 的快速转换，负责相关信息的写入操作。排架器通过对图书 RFID 标签进行扫描，结合层位标签进行定位盘点，需要获取的信息量较少。自助借还机对 RFID 实施扫描，对图书进行借还处理，还需要连接访问后台数据库。安全检测门对图书进行识别，判定图书是否处于借阅状态。

在图书馆中使用的 RFID 标签主要是工作频率为 13.56MHZ 的被动式标签。这种标签存储容量小，只能存储书名、书架号等少量图书信息；同时标签的计算能力也很弱，只能进行两个数比较大小、执行 hash 散列、产生随机数、检索自身的信息等简单功能，这些功能在 Class 1 Generation 2 标准的标签上容易实现[7]。

3.2 主要的安全威胁

结合图书馆 RFID 系统应用模型的特征，可以做出以下重要假设：

假设：在图书馆内部发生的读写器与标签之间的通信是安全的，可以采用明文传输；在图书馆外的通信存在安全威胁，需要采用保密和鉴别措施。

在此安全性假设的基础上，图书馆 RFID 系统所面临的安全威胁主要包括以下几种：

1) 攻击者作为一个正常的读写器具有扫描标签的能力。

2) 攻击者具有克隆标签的能力，即改写标签的内容。

3.3 协议安全性要求

本文提出的 RFID 安全认证协议是基于一个状态锁(lock)的实现通信保密(Privacy)与身份鉴别(Authentication)的认证协议：Privacy and Authentication protocol based on a Lock，简记 PA-Lock 协议。

安全认证协议 PA-Lock 试图满足两个要求：保密性和鉴别性。保密性要求每一个标签只能把保密信息发送给经过鉴别的读写器。鉴别性则要求标签和读写器之间能实现相互鉴别，即标签能够鉴别读写器、读写器也能够鉴别标签。此外，锁是一个图书状态位，表示图书处于借出或者在馆的状态。

保密性和鉴别性也将作为本文分析 PA-Lock 协议安全性能的两个指标，将在第 5 部分详细讨论。

4 PA-Lock协议描述

在 PA-Lock 协议中，RFID 标签具有一个伪随机数发生器，具有 hash 计算及数值大小比较能力，所存储的数据包括四部分：(1)标签 ID，此 ID 具有全球唯一性；(2)书目信息，包括图书条码号(图书的唯一识别)、书名、架位号等；(3)图书馆 RFID 系统的共享密钥 k；(4)图书状态锁 bit(0 表示在馆状态、1 表示借出状态)，在图书典藏时设置 bit 值为 0。RFID 读写器具有一个伪随机数发生器，能执行 hash 计算，能转发后台数据库和标签之间传输的数据。RFID 后台数据库存储着标签 ID 与图书条码号之间的关联信息，能执行 hash 计算、快速查找等能力。

在该协议中，当状态锁为 0 时，采用不需保密与鉴别的方式通信；当状态锁为 1 时，通过先对私密信息进行 hash 加密然后再传输的措施实现保密功能，读写器通过共享密钥 k 来鉴别标签，标签通过图书的条码号来鉴别读写器，从而实现读写器与标签的双向相互鉴别。PA-Lock 协议中使用的参数如表 1 所示。

表 1　协议中的参数符号描述

Symbol	Definition
T	RFID 标签
R	RFID 读写器
B	后台数据库
Query	读写器发出的认证请求
ID	Tag 标示
ID`	数据库中存储的标签标示
hash()	单向hash 函数
r_R	读写器生成的伪随机数
r_T	标签生成的伪随机数
k	RFID共享密钥
bit	图书状态锁
name	图书名
bookshelf ID	书架号
barcode ID	图书条码号

下面，按照图书馆 RFID 系统的三种应用场景来对 PA-Lock 协议做详细的描述，三种应用场景分别是：排架、外借和自动还书。

4.1 排架

由于排架工作发生在图书馆预览室内部，有理由假设此时的通信是安全的，因此可以设计不需保密鉴别的认证协议，这样有利于提高通信效率。协议的执行过程如图 2 所示。

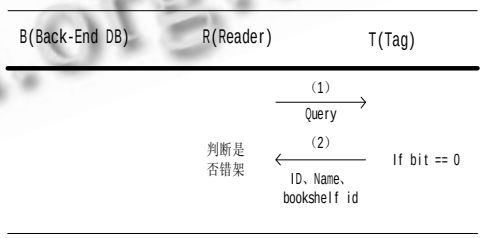

图 2　排架场景安全认证协议流程图

执行步骤说明如下：

①Tag 读写器向 Tag 发送 Query 认证请求；

②如果 bit 值为 0，Tag 将标签 ID、图书名、书架号发送给 Tag 读写器。

4.2 借书

借书场景的认证协议的前两步与排架场景认证协议相同。在借书的过程中，管理系统需要做借书操作，此外，标签还要把其状态位 bit 设置为 1，以表示图书

处于借出状态。该协议通过由读写器给标签发送图书的条码号（barcode ID）作为验证信物，驱使标签修改状态位的值。协议执行过程如图 3 所示。

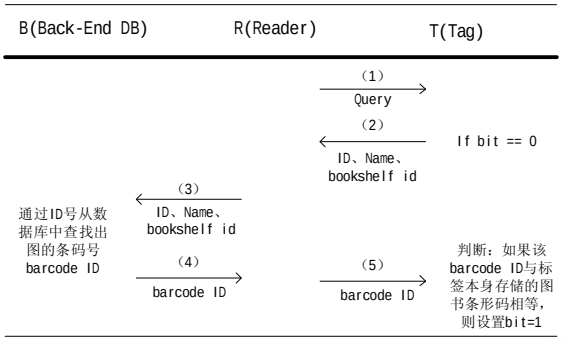

图 3 借书场景安全认证协议流程图

执行步骤说明如下：

①Tag 读写器向 Tag 发送 Query 认证请求；

②如果 bit 值为 0，Tag 将标签 ID、图书名、书架号发送给 Tag 读写器；

③Tag 读写器将标签 ID、图书名、书架号发送给后台数据库；

④后台数据库根据标签 ID 查找图书的条形码 barcode ID，并把该 barcode ID 发送给 Tag 读写器；

⑤Tag 读写器把该 barcode ID 发送给 Tag。Tag 判断该 barcode ID 和自身存储的 barcode ID，是否相等，如果相等则设置 bit 值为 1 ，表示该图书已外借。

4.3 自动还书

自动还书的过程中，除了文献管理系统需要办理还书操作以外，还要驱动标签设置 bit 的值为 0。这是具有高威胁性的过程，需要实现读写器和标签的相互鉴别并且需要对发送的信息进行加密，以防止重要私密信息泄露和标签克隆。协议执行过程如图 4 所示。

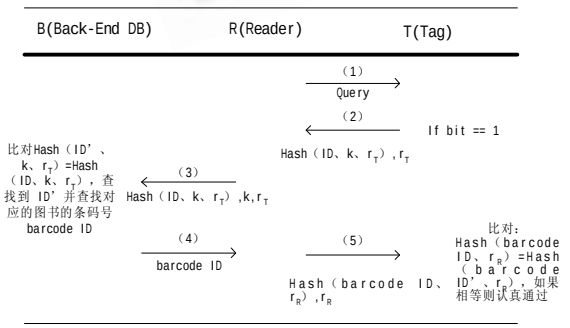

图 4 自动还书场景安全认证协议流程图

执行步骤说明如下：

①Tag 读写器向 Tag 发送 Query 认证请求；

②如果 bit 值为 1，Tag 产生一个伪随机数 rT，将 Hash（ID、k、rT）和 rT 发送给 Tag 读写器，其中 ID 为 Tag 标示，k 为 RFID 系统公共密钥；

③Tag 读写器将 Hash（ID、k、rT）、k 和 rT 发送给后台数据库。后台数据库查找是否存在一个 ID`(数据库中存储有所有 Tag 的 ID)使得 Hash( ID`、k、rT）= Hash（ID、k、rT）成立。如果有，则可鉴别该 Tag 是合法标签，并根据该 ID 查找图书的条形码 barcode ID。如果没有，则返回给 Tag 读写器认证失败信息。

④后台数据库把该 barcode ID 发送给 Tag 读写器；

⑤Tag 读写器产生一个伪随机数 rR，把 Hash (barcode ID、rR), rR 发送给 Tag。Tag 根据自己存储的图书条形码 barcode ID`计算 Hash(barcode ID`、rR), 并比较 Hash(barcode ID`、rR)= Hash (barcode ID、rR)是否成立。如果成立，则可鉴别该 Tag 读写器是合法读写器,并设置 bit=0，否则认证失败。

5 协议安全性能分析

本文第 3 部分讨论了图书馆 RFID 系统的安全需要及对安全协议的要求，下面将围绕保密性能和鉴别性能来分析 PA-Lock 协议的安全性及性能。

保密指保护信息不被未授权者访问。由于 RFID 系统借助无线信号广播，这为偷听者提供了便利，所以为了保密，只能通过加密的办法避免重要的私密信息的明文传送。PA-Lock 协议中通过基于伪随机数的 hash 函数来对共享密钥 k、标签 ID、图书条码 barcode ID 等重要私密信息进行加密保护，减小了因这些信息的明文传输而被窃取的威胁。单向 hash 函数的不可逆性为保密提供了可靠地保障，即使偷听者窃取到了 Hash（ID、k、rT）和 rT 的值，它也不可能知道 ID 和 k 的值，而且每次传输的 Hash（ID、k、rT）都不同，有效避免了 Tag 被跟踪的可能。

鉴别主要指在揭示敏感信息或进行事物处理之前先确认对方的身份。PA-Lock 协议实现了 Tag 与 Tag 读写器之间的相互鉴别功能。协议中，Tag 读写器通过系统共享密钥 k 来鉴别 Tag 的身份，Tag 通过图书条码号 barcode ID 来鉴别 Tag 读写器的身份。由于

共享密钥 k 和来源于后台数据库的图书条码号 barcode ID 可以保证安全性，所以该协议能够保证相互鉴别的正确和安全性。

PA-Lock 协议中通过图书状态锁 bit 的值对协议作了分支设计，既适合图书馆 RFID 系统的实际需求，又减少了 Tag 与 Tag 读写器之间传输的信息量，提高了该安全协议的效率。此外，PA-Lock 协议对各部分设备的计算能力要求也较低， Tag 和 Tag 读写器只需具有比较大小、hash 计算、生成随机数的能力，后台数据库只需具有 hash 计算以及时间复杂度为 O(Logn)的快速查询能力，这些计算需求不会增加系统的硬件成本。所以，PA-Lock 协议具有较高的效率。

6 协议性能分析比较

RFID 系统所面临的常见安全威胁包括假冒攻击、重传攻击、追踪、去同步化等类型。本文基于这些常见的攻击类型，对 Hash-Lock 协议、基于杂凑的 ID 变化协议、LCAP 协议及 PA-Lock 协议的安全性能在文献[8]的基础上进行了详细的比较分析，分析结果如表 2 所示。由于基于杂凑的 ID 变化协议和 LCAP 协议是动态 ID 协议，标签 ID 在不停的刷新，这就存在去同步化的问题（即标签内 ID 与其在数据库内 ID 不一致）；而 Hash-Lock 协议和 PA-Lock 协议是静态 ID 协议，不存在 ID 不一致的安全威胁，但是 Hash-Lock 协议的安全性问题基本没有解决，本文提出的 PA-Lock 协议较好的解决了假冒攻击、重传攻击、追踪等安全问题。

表 2　几个安全认证协议比较

攻击类型	Hash-Lock	杂凑ID	LCAP	PA-Lock
假冒攻击	不满足	满足	满足	满足
重传攻击	不满足	满足	满足	满足
追　踪	不满足	满足	满足	满足
去同步化	满足	不满足	不满足	不存在

7 结语

RFID 技术是改进图书馆服务体系的重要技术手段之一，随着图书馆 RFID 系统的逐渐推广，其安全认证问题成为一个关注的焦点。基于密码技术的 RFID 安全认证协议是实现 RFID 系统安全性的重要方法。本文在详细分析图书馆 RFID 系统的应用特征及其特殊的安全性需求的基础上，设计了一个针对被动式 RFID 标签能够实现保密和相互鉴别的 PA-Lock 协议，结合图书馆 RFID 系统的实际应用场景，对 PA-Lock 协议做了详细的描述，并通过对该认证协议的安全性分析以及和相关协议的分析比较，证明了 PA-Lock 协议的安全性和高效性。

参考文献

1 张帆,孙璇,马建峰等.供应链环境下通用可组合安全的 RFID 通信协议.计算机学报, 2008,(10):1754－1767.

2 Molnar D, Wagner D. Privacy and security in 1ibrary RFID：Issues, practices, and architectures. Proc. of the 11th ACM conference on computer and communications security. ACM Press, 2004, 210－219.

3 吴晞,马瑞,李星光. RFID 系统及其在图书馆中的应用. 图书馆论坛, 2005,(1):4－8.

4 叶莉. RFID 技术在图书馆的应用实例及障碍分析. 图书馆论坛, 2008,(5):71－73.

5 丁振华,李锦涛,冯波.基于 Hash 函数的 RFID 安全认证协议研究.计算机研究与发展, 2009,(4):583－592.

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

7 Liu AX, Bailey LA. PAP: A privacy and authentication protocol for passive RFID tags. Computer Communications, 2008(3):1194－1199.

8 邓淼磊,马建峰,周利华.RFID 匿名认证协议的设计. 通信学报, 2009,(7):21－26.