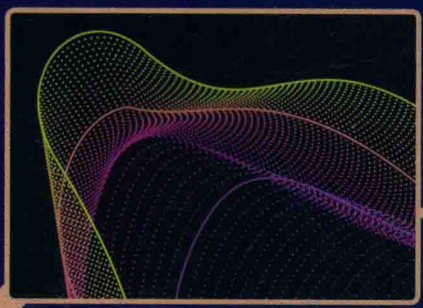
RFID

标签所有权安全转换

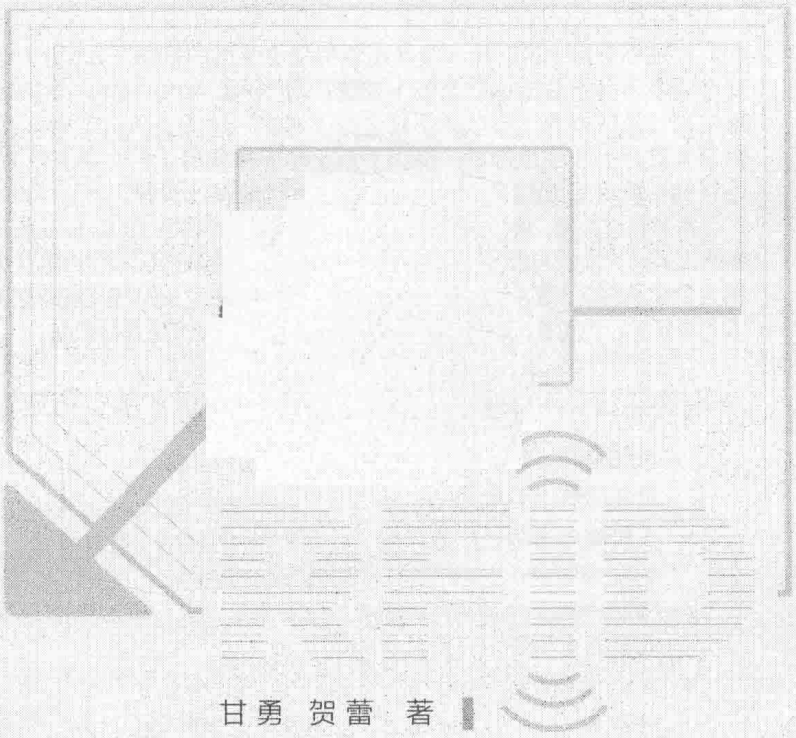
甘勇 贺蕾 著



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

RFID

标签所有权安全转换



甘勇 贺蕾 著

人民邮电出版社
北京

图书在版编目（CIP）数据

RFID标签所有权安全转换 / 甘勇，贺蕾著. -- 北京：人民邮电出版社，2018.11
ISBN 978-7-115-48283-9

Ⅰ. ①R… Ⅱ. ①甘… ②贺… Ⅲ. ①无线电信号－射频－信号识别－应用 Ⅳ. ①TN911.23

中国版本图书馆CIP数据核字(2018)第209139号

内 容 提 要

本书在介绍RFID技术及其面临的安全挑战的基础上，介绍了RFID系统安全协议所涉及的信息安全基本理论；对RFID系统中的认证、密钥协商和所有权转换的概念、模型和协议进行了阐述，设计了RFID所有权安全转换协议并进行了安全性分析；提出了基于动态重载的RFID标签所有权安全转换机制；给出了RFID标签所有权转换系统的设计实例。

本书取材新颖、内容翔实、实用性强，反映了国内外RFID标签所有权安全转换协议的研究现状与发展趋势，适合于对RFID、物联网技术和信息安全感兴趣的相关专业本科生、研究生和从事物联网及安全研究、工程与应用的学者及工程技术人员阅读，也可作为电子信息相关专业本科生、研究生课程教材。

◆ 著　　甘 勇 贺 蕾
责任编辑　代晓丽
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫丰华彩印有限公司印刷

◆ 开本：880×1230　1/32
印张：6　　2018年11月第1版
字数：134千字　　2018年11月北京第1次印刷

定价：68.00元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前言

射频识别（Radio Frequency Identification，RFID）技术是利用无线射频的方式在阅读器和应答器之间进行非接触式的双向数据传输的新技术，以达到目标识别和数据交换的目的。随着 RFID 技术的广泛应用，所有权转换和安全隐私问题也越来越凸显，RFID 标签的安全问题主要包括个人隐私保护、企业商业机密保护以及安全防范等多个方面。RFID 标签有可能在没有感知的情况下被附近的阅读器读取，造成个人信息泄露，尤其是可能暴露用户的位置隐私，导致用户被跟踪，因此 RFID 安全协议研究引起了国内外同行的重视，并在安全协议研究与设计方面取得了一些成果。在国家自然科学基金项目“基于动态重载的 RFID 标签所有权安全转换机制研究”（No. 61340059）和“多所有者 RFID 标签所有权可验证动态安全转换机制研究”（No. 61572445）及河南省重点科技攻关计划项目“RFID 系统安全性研究”的支持和资助下，本书作者及所在项目组对 RFID 标签所有权安全转换协议进行了研究并进行了总结，希望能为从事相关研究与工程的科研工作者提供参考。

本书主要内容包括：第 1 章介绍了 RFID 技术及其面临的安全挑战，以及 RFID 所有权安全转换协议研究背景与意义；第 2 章介绍了 RFID 系统安全协议所涉及的信息安全基本理论，

包括密码学基本概念与常用算法、数字签名及常用算法、数字认证和数字证书、安全协议、密钥协商协议等；第 3 章介绍了 RFID 系统中的认证、密钥协商和所有权转换；第 4 章介绍了 RFID 标签所有权转换的概念、模型和协议，设计了 RFID 所有权转换协议并进行了安全性分析；第 5 章介绍了基于动态重载的 RFID 标签所有权转换机制；第 6 章给出了 RFID 标签所有权转换系统的设计实例。

甘勇编写了第 1 章、第 2 章和第 6 章，并对全书进行了统稿，贺蕾编写了第 3～5 章，项目组的硕士研究生李天豹、杨佳佳、许允倩、薛峰、杜超、杨宗琴、王凯、郭胜娜、张云霄参与了项目研究，并为本书的文字校阅、插图绘制等做了大量的工作；本书的编写得到了郑州轻工业学院、郑州工程技术学院和人民邮电出版社的支持和帮助，在此由衷地向他们表示感谢！作者在编写本书的过程中参考了大量国内外相关项目的专业知识和研究成果，在此对原作者和出版单位表示诚挚的谢意！

由于作者水平所限，同时 RFID 所有权安全转换协议的研究仍在快速发展和完善中，因此书中难免存在缺点甚至错误之处，敬请广大读者批评指正。

作　者

2017 年 12 月

目录

第 1 章

RFID 技术及其面临的安全挑战

本章简要介绍 RFID（Radio Frequency Identification，无线射频识别）技术及基本工作原理，包括 RFID 电子标签及种类、相关标准、RFID 应用面临的安全问题与挑战、RFID 安全协议研究的意义等内容。

1.1 RFID 技术及其基本工作原理

1.1.1 RFID 技术与发展

RFID 是一种通过无线射频信号识别特定目标并读写相关数据的无线通信技术，它可自动识别、收集、处理、转换实体的相关信息。RFID 技术源于军事方面的应用，目前 RFID 技术作为物联网的核心技术之一发展迅速，已在物流、医药、零售业、制造业、航空业、石化、银行、公共交通、校园卡、产品追踪与溯源等领域广泛应用，甚至私人物品的运输都可用电子标签进行监管。作为物联网技术应用的排头兵，RFID 不仅被广泛应用于各行各业，而且将变革现有的商业模式，使各行业更大限度地把人力物力投入到创新发展以及尽可能提供更好的服务上来。例如在供应链管理等物流领域，RFID 的应用将成为重头戏。在物流供应链环境下，RFID 技术可以有效跟踪，收集产品相关信息，提高产品流通中的管理效率，降低管理成本。

目前 RFID 技术和市场正日趋成熟[1-2]，美国及欧盟等多国把 RFID 作为重点产业投入巨资积极推动。中国也在高度关注和重视物联网技术，自 2010 年物联网发展被正式列入国家发展战略以来，我国 RFID 及物联网产业迎来了难得的发展机遇。2011 年 4 月，工业和信息化部（以下简称“工信部”）、财政部设立物联网专项资金，推动产业快速发展。2011 年中国 RFID 产业的市场规模达到了 179.7 亿元，比 2010 年增长了 47.94%。2011 年中国 RFID 产业链各环节如射频芯片、标签封装产品与设备、软件/中间件、系统集成都呈现出高速增长的势头。2012 年 2 月，工信部正式发布《物联网“十二五”发展规划》，指明产业未来发展道路，在政府大力推动物联网产业发展的背景下，国家的一系列促进政策成为中国 RFID 产业发展的强大动力来源，2012 年我国 RFID 市场规模达 236.6 亿，位居世界第三。2013 年我国 RFID 市场规模达 318.4 亿。从 2015 年开始，中国 RFID 行业将再一次进入快速扩张的阶段，预计市场增长速度将从当前的 25%左右提升到 30%以上，2015 年中国 RFID 行业市场规模达 373 亿，预计 2017 年将高达 621 亿。从 2013—2017 年，中国 RFID 行业市场规模将增长约 2.4 倍，年均增长率约为 27.88%。

我国 RFID 行业在过去的几年间经历过了一段高速的成长期，目前 RFID 已经在国内的身份识别、交通管理、军事与安全、资产管理、防盗与防伪、金融、物流、工业控制等领域的应用中取得了突破性的进展，并在部分领域开始进入规模应用阶段。随着 RFID 技术的进一步成熟和成本的进一步降低，必将广泛应用到各行各业之中。

1.1.2 RFID 标签的基本工作原理

RFID 标签又称为射频标签、应答器、数据载体，阅读器又称为读出装置、扫描器、读头、通信器、读写器（取决于电子标签是否可以无线改写数据）。RFID 技术的基本工作原理如下：标签进入磁场后，接收读写器发出的射频信号，凭借感应电流所获得的能量发送出存储在芯片中的产品信息（Passive Tag，无源标签或被动标签），或者主动发送某一频率的信号（Active Tag，有源标签或主动标签）；读写器读取信息并解码后，送至管理信息系统进行有关数据处理。

RFID 系统由两部分组成：读/写单元和电子标签。读/写器通过天线发出电磁脉冲，电子标签接收这些脉冲，并发送已存储的信息到阅读器作为响应。实际上，这就是对存储器的数据进行非接触读、写或删除处理。电子标签包含了 RFID 射频处理电路和一个超薄天线环路，天线与一个塑料薄片一起嵌入标签内，最常见的标签一般为信用卡大小，也可以根据不同的应用需求设计不同形状、不同大小的标签。

与条形码或磁条等其他 ID 技术相比较而言，RFID 技术的优势在于阅读器和收发器之间的无线连接：读/写单元不需要与收发器之间的可视接触，因此可以完全集成到产品里面。RFID 标签适合于恶劣的环境，收发器对潮湿、肮脏和机械影响不敏感，具有非常高的读可靠性和快速数据获取的能力。电子标签与读/写器之间通过耦合元件实现射频信号的空间（无接触）耦合；在耦合通道内，根据时序关系，实现能量的传递和数据交换。电子标签处于开放待访问状态，当进入读写器的电磁场信号覆盖范围中时，接收读写器

发出的射频信号（查询请求），根据电感耦合（Inductive Coupling）原理或电磁反向散射耦合标签收到读写器功率相匹配的电磁信号后产生感应能量并解析接收到的信号，标签内部处理器（微电子芯片）利用内部产生的电流返回特定的响应信息与读写器进行数据交换。读写器接收标签响应信息并解码，送至后端数据库服务器进行标签身份认证识别和有关数据处理。射频信号的耦合类型分为两类：电感耦合和电磁反向散射耦合。

1. 电感耦合

根据法拉第电磁感应定律产生感应电动势，通过空间高频交变磁场实现互感耦合，也称磁耦合。其中一个重要的、广泛的应用就是变压器。一般适用低、高频工作的近距离 RFID 系统。工作频率主要有 125 kHz、225 kHz 和 13.56 MHz。识别距离小于 1 m，典型作用距离为 10～20 cm。电感耦合原理示意如图 1-1 所示。

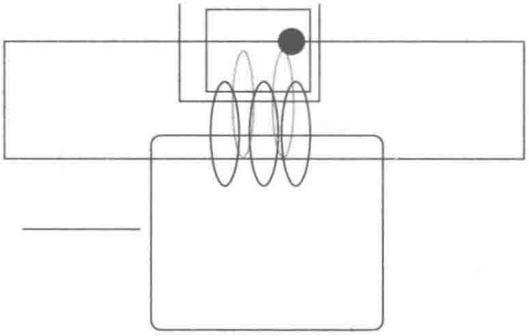


图 1-1　电感耦合原理示意

2. 电磁反向散射耦合

这种类型是雷达原理模型，依据电磁波的空间传播规律，发射出的电磁波反射同时携带回碰到的目标信息。一般适用于超高频、

微波工作的远距离 RFID 系统。工作频率主要有 433 MHz、915 MHz、2.45 GHz 和 5.8 GHz。识别距离大于 1 m，典型作用距离为 3～10 m。电磁反向散耦合原理示意如图 1-2 所示。

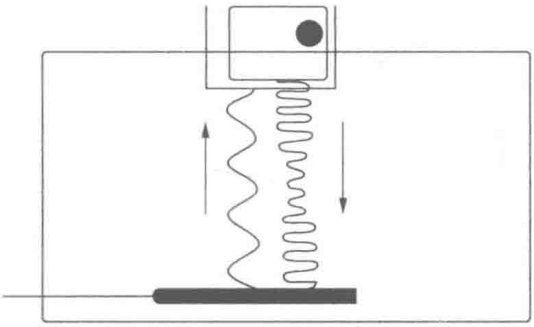


图 1-2　电磁反向散射耦合原理示意

1.1.3　RFID 标签及分类

RFID 标签由耦合元件及芯片组成，每个 RFID 标签具有唯一的电子编码，附着在物体上标识目标对象，又称为电子标签或智能标签。

1. 按标签供电方式

（1）无源标签

无源标签没有内置供电电源，其内部集成电路（电磁元件）驱动能量来源于通过接收读写器发射的电磁波（信号）转换的感应电流。

当标签所处电磁场的射频信号足够强时，可以向读写器发出存储在芯片中的数据信息，通常包含标签身份信息、识别目标或所有者的相关数据。由于无独立供电电源，因此标签的工作距离受到限