清华大学 计算机系列教材

王爱英 编著

物联网与智能卡技术基础

清华大学出版社

清华大学 计算机系列教材

王爱英 编著

物联网与智能卡技术基础

清华大学出版社
北京

内 容 简 介

物联网是在计算机、互联网和移动通信技术的基础上，采用智能卡、射频识别标签、传感器等设备组成的，设备与设备或网络之间，可通过固定导线或空中射频接口传送数据。

智能卡是射频识别(RFID)标签的前驱，在中国居民身份证、金融卡和手机 SIM 卡的发行量早已超过几十亿张，在技术、功能、安全和标准制定等方面可供 RFID 借鉴。

本书主要内容包括计算机和互联网的基础知识，射频信号的处理与频段分配，智能卡、RFID 标签和传感器的硬件结构，智能化设备的操作系统与测试，空中传输信号的防冲突方案，纠错、识别、安全和防欺诈措施、国际标准，以及互联网、物联网的应用和创新。

本书主要提供给高等院校的信息技术、计算机、通信、自动控制和物联网等专业作为技术基础课的教材。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

物联网与智能卡技术基础/王爱英编著. —北京：清华大学出版社，2019
(清华大学计算机系列教材)
ISBN 978-7-302-49456-0

Ⅰ. ①物… Ⅱ. ①王… Ⅲ. ①互联网络－应用－高等学校－教材 ②IC 卡－技术－高等学校－教材 Ⅳ. ①TP393.4 ②TN43

中国版本图书馆 CIP 数据核字(2018)第 020925 号

责任编辑：白立军　王冰飞
封面设计：常雪影
责任校对：时翠兰
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：17　　**字　　数**：300 千字
版　　次：2019 年 1 月第 1 版　　**印　　次**：2019 年 1 月第 1 次印刷
定　　价：45.00 元

产品编号：076472-01

安徽大学图书馆 藏书 www.lib.ahu.edu.cn

序

“清华大学计算机系列教材”已经出版发行了30余种，包括计算机科学与技术专业的基础数学、专业技术基础和专业等课程的教材，覆盖了计算机科学与技术专业本科生和研究生的主要教学内容。这是一批至今发行数量很大并赢得广大读者赞誉的书籍，是近年来出版的大学计算机专业教材中影响比较大的一批精品。

本系列教材的作者都是我熟悉的教授与同事，他们长期在第一线担任相关课程的教学工作，是一批很受本科生和研究生欢迎的任课教师。编写高质量的计算机专业本科生（和研究生）教材，不仅需要作者具备丰富的教学经验和科研实践，还需要对相关领域科技发展前沿的正确把握和了解。正因为本系列教材的作者具备了这些条件，才有了这批高质量优秀教材的产生。可以说，教材是他们长期辛勤工作的结晶。本系列教材出版发行以来，从其发行的数量、读者的反映、已经获得的国家级与省部级的奖励，以及在各个高等院校教学中所发挥的作用上，都可以看出本系列教材所产生的社会影响与效益。

计算机学科发展异常迅速，内容更新很快。作为教材，一方面要反映本领域基础性、普遍性的知识，保持内容的相对稳定性；另一方面，又需要跟踪科技的发展，及时地调整和更新内容。本系列教材都能按照自身的需要及时地做到这一点。例如，王爱英教授等编著的《计算机组成与结构（第5版）》、戴梅萼教授等编著的《微型计算机技术及应用（第四版）》都已经出版了，严蔚敏教授的《数据结构》也出版了第三版，使教材既保持了稳定性，又达到了先进性的要求。

本系列教材内容丰富，体系结构严谨，概念清晰，易学易懂，符合学生的认知规律，适合于教学与自学，深受广大读者的欢迎。系列教材中多数配有丰富的习题集、习题解答、上机及实验指导和电子教案，便于学生理论联系实际地学习相关课程。

随着我国进一步的开放，我们需要扩大国际交流，加强学习国外的先进经验。在大学教材建设上，我们也应该注意学习和引进国外的先进教材。但是，“清华大学计算机系列教材”的出版发行实践及它所取得的效果告诉我们，在当前形势下，编写符合国情的具有自主版权的高质量教材仍具有重大意义和价值。它与国外原版教材不仅不矛盾，而且是相辅相成的。本系列教材的出版还表明，针对某一学科培养的要求，在教育部等上级部门的指导下，有计划地组织任课教师编写系列教材，还促进了对该学科科学、合理的教学体系和内容的研究。

我希望今后有更多、更好的优秀教材出版。

清华大学计算机系教授，中国科学院院士

张钹

前　言

集成电路、计算机、互联网和移动通信技术的应用，促进了物联网的诞生与发展。计算机的使用改变了人类传统的计算方法和对万物的控制能力，智能化的理念已普及各个领域，计算机或微处理器的应用已深入军事、经济、商务、工业控制、通信、文化、游戏、影视等各个方面。

智能手机、平板电脑已成为可随身携带的电话机、计算机。

智能卡的发行量在我国已超过几十亿张，无论是在应用、安全还是在一卡多用等方面都有扩展，性能在提高而产品的价格在下降。物联网的应用向射频识别(RFID)和传感器等产品在技术、性能和质量等方面提出了要求。在人工智能方面，语音识别、机器翻译、人机对话、机器人、无人驾驶飞机和汽车等领域已取得进展。

物联网、互联网、移动通信网的功能相互渗透。平板电脑、智能手机的科技水平和服务内容竞争激烈并趋向一致。大屏幕的智能电视机虽然不能移动，但发展前景毋庸置疑。

我国在军事、经济、科技和工业等领域都向国际水平追赶、迈进，在某些方面已处于举足轻重或领先地位，因此人才的培养极为重要。我国已有几十所大学增设了物联网专业。

自 20 世纪 90 年代开始，清华大学和中国电子技术标准化研究院，联合相应的智能卡研发公司，完成智能卡的设计、制造和标准制定工作，为教学与应用付出了劳动。中国电子技术标准化研究院与社会各界联合提出的标准经上级批准后，发布为国家标准，并申请了专利。

1996 年，参加 IC 卡研发的清华大学教授和研究生编写了《智能卡技术》一书。20 世纪 90 年代正值 IC 卡在国内兴起之时，该书成为不少业界人士的参考书或入门培训教材。随着科技和应用的发展和创新，2015 年《智能卡技术(第四版)——IC 卡、RFID 标签与物联网》问世，并萌发了编写物联网与智能卡技术基础教材的设想。

2016 年，电子技术标准化研究院的金倩和冯敬两位高级工程师为本书的编写提供了资料。

本书是为高等院校培养物联网与相关领域的“产、学、研、用”人才而编写的技术基础教材，为后续的学习和工作服务做准备。当今技术飞速发展，学习不能间断，对作者来说也是这样，书中的某些内容会很快地被新技术更新，但不会很快地被排斥。书中难免存在疏漏和不妥之处，欢迎广大读者指正。

作者

2018 年 5 月

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

此为试读,需要完整PDF请访问: www.ertongbook.com

第1章 概 论

在全球范围内，无论是军事领域还是民用领域，集成电路、计算机、互联网和移动通信技术都得到蓬勃的发展和广泛的应用，从而促进了智能标识（智能卡、射频识别标签等）和物联网的产生、发展和应用。

在中国，智能卡广泛应用于居民身份证、金融卡、手机中的 SIM 卡、交通卡、移动终端和门禁系统等方面，已发行几十亿张，并从有线技术向无线技术方向发展，促进了互联网、物联网和移动通信网的融合。

智能卡和射频识别标签用于识别“人”和“物”，并根据应用需求完成其与读写器之间的数据传送、数据处理等。

物联网是指通过各种信息传感设备，如传感器、射频识别标签和 IC 卡等，实时采集各个物品需要监控的信息，并进行处理，是实现人与人、物与物、人与物连接的网络。

1.1 计算机的应用

计算机是从军事上的科研和应用开始的，并推广到下述各方面。

1. 科学计算

在国防、尖端科学技术、数学等学科领域要进行大量的复杂运算，具有计算量大、数据值变化范围大等特点。高性能计算机在先进集成电路工艺的支持下，具有浮点运算和信号处理等功能。

2. 数据处理

在金融企业与管理等领域内，数据处理具有大量数据输入、存储和处理功能，其主要特点是运算比较简单、联系比较广泛（个人、单位、银行、政府、国际），要求精确、安全、防诈骗。

当前在数据中心、大数据和云服务领域有很大发展。

3. 计算机控制

在工业生产和交通运输等过程中的自动控制，包括零部件的设计与制造（传感器、仪器、设备等）和整机组装。

4. 人工智能

人工智能包括知识获取与处理、语音识别、图像处理、搜索、下棋、智能机器人。

其他方面的应用不胜枚举，近年来发展极为迅速，计算机和互联网的发展和应用已普及（参见 2.2 节），并深入到各个领域，在大学中有很多专业将它列为必学的基础课程。

1.2 智能卡、射频识别标签与读写器

1. 智能卡与读写器

智能卡（Smart Card）又称集成电路卡，即 IC 卡（Integrated Circuit card）。它将一个

集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似。

IC卡的概念是20世纪70年代初提出来的，它将微电子技术和计算机技术结合在一起，提高了人们生活和工作的现代化程度。

IC卡芯片具有写入数据、存储数据和读出数据的能力，IC卡存储器中的内容根据需要可以有条件地供外部读取，或者供内部信息处理和判定之用。根据卡中所镶嵌的集成电路的不同，IC卡可以分为以下两类。

(1) 逻辑加密卡。卡中的集成电路具有加密逻辑功能和E^2PROM(可用电擦除的可编程只读存储器)。

(2) 智能卡(CPU卡)。卡中的集成电路包括微处理器、E^2PROM、随机存储器(Random Access Memory，RAM)，以及固化在只读存储器(Read Only Memory，ROM)中的片内操作系统(Chip Operating System，COS)。随着集成电路工艺的提高、价格的下降，当前主要使用智能卡。

按应用领域来分，IC卡分为金融卡和非金融卡两种。金融卡又分为信用卡(credit card)和现金卡(debit card)等。信用卡主要由银行发行和管理，持卡人用它作为消费时的支付工具，可以使用预先设定的透支限额资金；现金卡又称储蓄卡，可用作电子存折和电子钱包，不允许透支。非金融卡往往出现在各种事务管理、安全管理场所，如身份证明、健康记录和职工考勤等。此外，还有一些预付费卡，如用于公交系统中的交通卡、超市中使用的购物卡等，由相应的管理单位发行。

按卡与外界数据传送的形式来分，有接触式IC卡和非接触式IC卡两种。在接触式IC卡上，IC芯片有8个触点可与外界接触。非接触式IC卡的集成电路不向外引出触点，因此它除了包含前述IC卡的电路外，还带有射频收发电路、天线及其相关电路。非接触式卡出现较晚，但由于它具有一些接触式IC卡所不能替代的优点，因此在某些应用领域发展较快。

在IC卡推出之前，磁卡已得到广泛应用，为了从磁卡平稳过渡到IC卡，也是为了兼容，使某些IC卡仍保留磁卡原有的功能。也就是说，在IC卡上仍贴有磁条，因此IC卡也可同时作为磁卡使用。图1.1所示为兼有接触式和非接触式功能的IC卡外观示意图，正面中左侧的小方块中有8个触点，如果是金融卡，则其下面为凸形字符(账号)，背面有磁条。正面还可印刷各种图案，如身份证的人像。卡的尺寸、触点的位置与用途、磁条的位置及数据格式等均有相应的国际标准予以明确规定，卡内四周有天线。

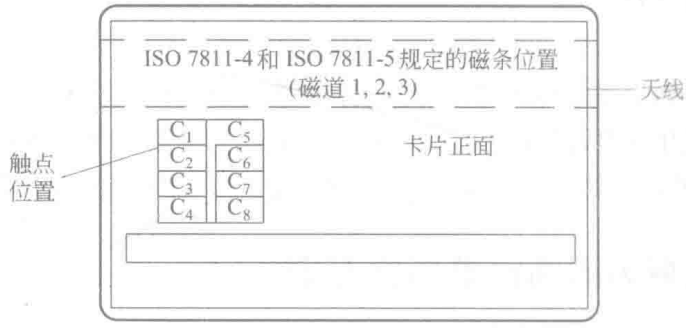

图1.1 IC卡的外观示意图

卡上有发行单位和持卡人的识别标志，可以称为“识别卡”。

2. IC 卡的读写器

为了使用卡片，还需要有与 IC 卡配合工作的读写器或称为接口设备（InterFace Device，IFD），IFD 是 interface device 的缩写词，从原词中选取字母，并用大写英文字母替代。IFD 可以是一个由微处理器、键盘、显示器与 I/O 接口组成的独立设备，通过 IC 卡上的 8 个触点或天线（射频电路）向 IC 卡提供电源，并与 IC 卡相互交换信息，也可以是一个简单的接口电路，IC 卡通过该电路与通用微机相连接。在卡上能存储的信息总是有限的，因此大部分信息需要存放在读写器或计算机中。

3. 射频识别标签与读写器

射频识别（Radio Frequency IDentification，RFID）技术的基本原理是利用无线射频信号的空间耦合（电磁感应或电磁传播）实现对被识别物体的自动识别。RFID 系统的基本工作方式是将 RFID 标签安装在被识别物体上（粘贴、嵌入、佩挂或植入等），当被识别物体进入 RFID 读写器的读写范围内（射频场）时，标签与读写器之间建立起联系，其过程一般由读写器启动，然后标签向读写器发送自身信息，如标签编号和标签内存储的数据等，读写器接收信息并解码后，传送给计算机进行处理。RFID 系统一般由两部分组成，即 RFID 和读写器，RFID 又称电子标签。电子标签和读写器内部都装有天线，电子标签所需的能量可从读写器的射频场内取得（无源标签）或自带电源（有源标签）。

非接触 IC 卡可认为是电子标签的一种。电子标签的形式多样化，且不引出触点。

由于在读写器的射频场内可能存在多张非接触式 IC 卡或 RFID 标签，因此读写双方都要增加功能，以实现读写器逐一联系标签的方法。

1.3 安全问题

智能卡可用作金融卡和非金融卡，其中金融卡需要处理的内容较多，并需重视安全问题。其主要功能是识别卡、读写器和持卡人的真假，以及存储数据和处理数据等。

1. 举例

下面以自动柜员机（Automatic Teller Machine，ATM）为例来说明金融卡取款操作过程。

自动柜员机是放在银行或商店大堂中供客户自动提款的机器（有的 ATM 还有自动存款功能）。执行从 ATM 提取现金的操作仅需十几秒钟，总共需要持卡人做出如下 4 个动作。

（1）插入金融卡，然后按 ATM 屏幕提示进行操作。

（2）输入个人标识码（Personal Identification Number，PIN），即输入密码。

（3）选择交易类型（取款）。

（4）给出申请提取的金额。

当 ATM 判别没有问题时，自动输出卡和现金，并打印凭证。ATM 是一种操作方便的信息处理系统，可以 24h 提供服务。假如存在任何问题，则在 ATM 的屏幕上显示存在的问题和下一步应该进行的操作。

ATM 是安装在柜里的计算机系统。它的内部有严密可靠的物理和逻辑安全措施。

它的每一笔交易通常接受正确的授权和严格的控制，因此 ATM 系统既是一个操作简单的系统，又是一个构造复杂的系统。

ATM 将 IC 卡或磁条上(对磁卡)的数据，诸如发卡单位和客户账号识别码(用来获取自动授权信息的基础)通过通信线路与发卡单位的计算机及其账户数据库相连，用以检查金融卡的编号(查对黑名单)，以防止他人使用已挂失的或偷窃来的金融卡，同时核对客户的账面记录，以查明可供支用的金额，并根据交易的金额随即更新账面记录，供金融卡下次使用。此外，为了避免某些可能发生的弊端(如已挂失但尚未列入黑名单)，还要限制金融卡在一天内允许使用的次数和一天内允许提取现金的总金额。

绝大多数 ATM 取款时还需输入个人标识码 PIN(即密码)，并将 PIN 传送到计算机，用来核对持卡人是否是卡的主人。例如，在通信线路上明文传送 PIN，存在被窃听的危险，为此有时需对 PIN 进行加密，这就要提供一个加密算法和“密钥”，让经过加密后的 PIN 在通信线路上传送，在接收端解密，因此在接收端提出了密钥的管理和保护的要求。

2. 影响安全的若干基本问题

(1) 智能卡和读写器之间的信息流通。这些流通的信息可以被截取分析，从而可被复制或插入假信号。

(2) 模拟的智能卡(或伪造的智能卡)。模拟智能卡与读写器之间的信息，使读写器无法判断出是合法的还是模拟的智能卡。

(3) 非法使用他人的 IC 卡。因此要验证持卡人的身份。

(4) 诈骗。通过电信、电话等进行诈骗，骗取钱财。

(5) 篡改读写器的作弊行为。造成读/写卡中的数据不正确，因此不允许借用、私自拆卸或改装读写器。

其他卡有相似的或不同的安全问题(根据应用要求)。

3. 安全措施

为了安全防护，一般采取以下措施。

(1) 使用时，对持卡人、卡、标签和读写器的合法性要相互检验。

(2) 重要数据加密后传送。

(3) 检验数据的完整性，以防止卡内数据被删除、增加或修改，并纠正读写或传送时产生的差错。

(4) 设备中设置安全区，在安全区中包含有逻辑电路或外部不可读的存储区。如果有不合规范的操作，将自动禁止进一步操作。

(5) 设计、生产和发行的有关人员明确各自的责任，并严格遵守。相应的单位要取得合法认证。

(6) 设置黑名单。

(7) 对犯法行为进行法律制裁。

4. 密钥与认证

1) 密钥

密钥是存放在卡和读写器中的秘密数码，绝对不允许向外界泄露，智能卡和读写器的相互认证及重要数据的发送和接收都是通过密钥和相应的密码算法实现的。在数据发送

方，用密钥对数据进行加密运算后发送；在接收方，用密钥对数据进行解密运算后恢复成加密前的数据。

与加密和解密有关的还有密钥管理。密钥管理包括密钥的生成、分配、保管和销毁等。

对传输的信息进行加密，以防被窃取、更改，从而避免造成损失。对存储的信息进行加密保护，使得只有掌握密钥的人才能理解信息。

2）认证

（1）单位的合法性认证。对发行和运营等单位的合法性通过公正的权威机构进行认证。

（2）数字签名（电子签名）。要求：收方能确认发方的签名；发方签名后，不能否认自己的签名；发生矛盾时，公证人（第三方）能仲裁收、发方的问题。

（3）身份认证。用 password 或个人标识码 PIN 进行认证，或利用生物特征（指纹、人脸识别）进行认证。

密钥与认证问题将在第 5 章详细讨论。

1.4 国际标准

就标准而言，可以有国际标准、国家标准、行业标准和事实上的标准（工业标准）。其中，国际标准是由世界上一些国家或团体组成的国际标准化机构成员通过投票而确定的。在世界各地有多个国际标准化机构，其中影响较大的有国际标准化组织（International Organization for Standardization，ISO）、国际电工委员会（International Electrotechnical Commission，IEC）和国际电信联盟（International Telecommunication Union，ITU）。

国家标准是由国内的相关单位讨论通过并报请标准主管部门批准而确定的。

对一些影响范围相对较小或尚不完全成熟而确有实际需要的规范，则被确定为行业标准，这也需要经过行业主管部门批准。

某些单位或公司制定的一些规范，虽然没有经过有关标准化机构组织的讨论，但是由于其大量使用而造成不可忽视的影响，从而成为事实上的标准。

ISO 和 IEC 一起组成了国际标准化工作的专门委员会，作为 ISO 或 IEC 成员的国家团体通过技术委员会参与国际标准的制定。ISO 与 IEC 的技术委员会在彼此有兴趣的领域互相合作。

在信息技术领域，ISO 和 IEC 共同建立了一个技术委员会——ISO/IEC JTC 1，被该委员会所采纳的国际标准草案由各国家团体投票，被发布作为国际标准至少需要得到 75％参加投票的国家团体的赞成。

已发布的国际标准，在今后仍可能被修改，因此，在使用国际标准时，要注意应用国际标准的最新版本。

我国在制定国家标准时，主要参照 ISO 的国际标准，因此在本书中主要讨论 ISO/IEC 制定的 IC 卡和 RFID 标签的国际标准。

1. IC 卡的国际标准

IC 卡分接触式 IC 卡和非接触式 IC 卡两种。接触式 IC 卡推广应用较早，而近年来

由于非接触式 IC 卡使用的便捷性及成本的下降，应用范围迅速扩大。

接触式 IC 卡遵循的是 ISO/IEC 7816 国际标准，非接触式 IC 卡国际标准为 ISO/IEC 14443 和 ISO/IEC 15693，以及 ISO/IEC 7816 中对非接触式 IC 卡也适用的部分标准。

(1) ISO/IEC 7816 国际标准的标题是识别卡—集成电路卡。

① 适用于接触式 IC 卡的部分有 7816-1/2/3/10/12。符号"/"解释为"或"，如 7816-1/2 表示为 7816-1 或 7816-2。

② 对接触式 IC 卡和非接触式 IC 卡均适用的部分有 7816-4/5/6/7/8/9/11/13/15。

(2) ISO/IEC 14443 国际标准的标题是识别卡—非接触式集成电路卡—接近式卡。

(3) ISO/IEC 15693 国际标准的标题是识别卡—非接触式集成电路卡—邻近式卡。

2. RFID 标签的国际标准

RFID 标签形状尺寸各异，应用范围极广，有多个国际标准化组织为之制定了国际标准。本书介绍了 ISO/IEC 18000 国际标准，该标准规定了空中接口协议。

根据标签与读写器之间的工作频率不同确定了 6 部分：ISO/IEC 18000-1/2/3/4/6/7。

此外，非接触 IC 卡的国际标准 ISO/IEC 15693 也适用于 RFID 标签。

3. 其他卡与标签使用的相关标准、规范、协议

(1) 互联网。

(2) 解决安全问题的密钥密码体制。

(3) 卡与标准中表示信息的数据元和数据对象。

在新的国际标准制定或有创新技术和产品出现时，一般都会申请相关的专利，应予以关注，以防经济上的纠纷。

1.5 物联网的诞生与发展

IC 卡、RFID 标签促进了物联网的诞生与发展。

1. 接触式 IC 卡

1977 年，Motorola 与它的一个计算机客户合作开发了一张智能卡，形成了第一代智能卡产品。该智能卡将一个可编程的微控制器及一个非易失性的存储器集成在一个模块内，然后嵌入到一张符合 ISO 7810 标准的信用卡中。该产品在法国进行了试验，目的是为了对进行脱机(off-line)交易所需的技术予以评估。自此以后，智能卡开始迅猛发展，它所采用的技术也日新月异地发生着变化。1979 年产生了世界上第一片专为智能卡所设计的单片机芯片，从而形成了第二代智能卡产品，并在法国、瑞士、斯堪的纳维亚得到应用。当时主要是用作银行卡(bank card)。进入 20 世纪 90 年代后，在通信、健康和交通等方面，智能卡的应用也开始蓬勃发展。

早期的智能卡大多是一种单功能卡，即一张卡只适用于某一种应用。以后的智能卡则向着多功能卡的方向发展。例如，可以发行城市卡(city card)，这种卡将包括用户在一个城市中可能经常需要接触的大部分应用功能，如作为电子钱包(electronic purses)、医

此为试读，需要完整PDF请访问：www.ertongbook.com