Smart Card Security and Design

智能卡安全与设计

张之津　李胜广　薛艺泽　等 编著

清华大学出版社

Smart Card Security and Design

智能卡安全与设计

张之津　李胜广　薛芃泽　等 编著

清华大学出版社
北京

内 容 简 介

智能卡已经走入平常百姓家，第二代居民身份证、手机 SIM 卡、市政公交一卡通、社保卡、电子护照、USBKey 等智能卡已经得到广泛应用，但是智能卡内含的私人信息或账户财产也越来越受到安全威胁。本书在深入介绍智能卡原理的基础上，着眼于智能卡安全内容，逐层描述了安全攻击、安全目标、安全算法、安全机制和安全规范等内容；然后介绍智能卡系统设计，包括低层设计、应用设计等内容；最后给出了智能卡未来发展的趋势。本书附有大量的研发实例。

本书的主要读者对象为从事智能卡安全开发和应用、智能卡芯片开发、芯片操作系统 COS 开发、嵌入式安全产品、机具开发和系统软件开发等工程技术人员以及高等院校相关专业师生，可作为移动通信、法定证件、市政公交一卡通、社保卡、电子政务、金融等行业专业人员的参考书籍，也可作为高校智能卡、信息安全和嵌入式等专业的本科生、研究生教材。

图书在版编目(CIP)数据

智能卡安全与设计/张之津，李胜广，薛艺泽等编著. —北京：清华大学出版社，2010.11
ISBN 978-7-302-23599-6

Ⅰ. ①智…　Ⅱ. ①张… ②李… ③薛…　Ⅲ. ①智能卡—安全技术 ②智能卡—设计
Ⅳ. ①F830.46

中国版本图书馆 CIP 数据核字(2010)第 159239 号

责任编辑：王一玲
责任校对：焦丽丽
责任印制：何　芊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：22.75　**字　数**：553 千字
版　　次：2010 年 11 月第 1 版　　**印　　次**：2010 年 11 月第1 次印刷
印　　数：1～3000
定　　价：38.00 元

产品编号：038408-01

前言

智能卡已经走入平常百姓家，第二代居民身份证、手机 SIM 卡、市政公交一卡通、社保卡、电子护照、USBKey 等智能卡应用已经不再是新生事物，并已被广泛接受。

21 世纪初的近十年里，智能卡市场在全球稳步发展，智能卡的应用涉及了各行各业。然而平静的智能卡行业的湖面被第 24 届黑客大会（Chaos Communication Congress）投进了一块巨石，激起了世界级的安全波浪。

2008 年 4 月，在第 24 届黑客大会上，德国学者 Henry Plotz 和弗吉尼亚大学博士 Karsten Nohl 公开了全球广泛应用的 Mifare 智能卡芯片加密算法的破译方法。同年 5 月，内嵌 Mifare 芯片的伦敦公交卡被成功克隆。该事件掀起一场大范围的安全风暴，引起全球对智能卡安全的广泛关注。

中国智能卡行业深受该风暴的影响。工业和信息产业部发布了《关于做好应对部分 IC 卡出现严重安全漏洞的通知》，要求各地机关和部门开展对智能卡使用情况的调查和应对工作。智能卡专家频繁奔波于各行各业的智能卡应用系统安全评审会议中，智能卡芯片提供商不停地向用户和行业主管领导进行安全方面的解释和保证。

一张张卡片，如何让老百姓放心地使用，不必担心隐私信息的泄露，不必恐慌财产的损失。这是智能卡设计者势必每时每刻都要关心的问题。

我们必须时刻谨记：智能卡应用中，没有绝对安全的芯片，没有绝对安全的算法。任何智能卡（包括物理芯片和上层算法）都可能被攻破。因此，如何延长攻击时间、增加攻击代价或者将攻击损失降到最低是智能卡安全设计的最大理念。

正是基于以上背景，作者萌生了编写《智能卡安全与设计》这本书的想法。作者不仅是长期从事智能卡研发的科技人员，也是公安部第一研究所的专业技术警察，担负着公共安全领域的科技研究工作。

公安部第一研究所是公安部直属的警察建制的多学科、科工贸一体的综合性研究所，始建于 1960 年，主要从事警用电子设备和社会公共安全器材的研制及生产。研究所现有员工 2300 多名，其中技术人员 650 多名，包括研究员 40 余人，副研究员 150 余人；涉及警用通信、安防安检、法定证件、信息安全等多个专业。自 1993 年起，公安部第一研究所开始组织第二代居民身份证的研制工作，2004 年第二代居民身份证正式发行。自 2005 年起，研究所又承担了我国电子护照的芯片操作系统、生物特征、安全架构和一体机等全方位多层次的技术研发工作。

从事本书编写的所有作者均是公安部第一研究所法定证件领域的研究人员，在第二代居民身份证和电子护照项目研发过程中，积累了大量的实践经验。本书编写紧密联系研发经验，注重科研理论与工程实践并重，摒弃过时陈旧理论，着重未来技术应用，并附加详细开发范例供读者参考。

本书内容总共分12章，分成两大部分：智能卡安全研究和智能卡系统设计。

本书从智能卡基础（第1章）引出话题，然后按照智能卡应用的安全层次的顺序，编写了安全攻击（第2章）、安全目标（第3章）、安全算法（第4章）、安全机制（第5章）、生物特征识别（第6章）、安全规范（第7章）。

智能卡系统设计包括低层设计（第8章）、CSP应用与开发（第9章）、应用系统设计（第10章）和系统测试（第11章）。

最后给出未来智能卡发展的趋势和技术（第12章）。每章都附有详细的参考文献，为读者深入研究相关专题提供了资料。

本书由张之津研究员、李胜广博士和薛艺泽主编，其中第1、2章由李莉编写，第3、7章及11.7节由薛艺泽编写，第4章、5章、7.5节及第8章由李胜广编写，第6、10章由孙健编写，第9、11章由张小波编写，10.3节、第12章和附录由朱元硕编写。李胜广博士对全书进行了详细的审校。由于作者水平有限，书中难免存在缺点和不足，真诚地欢迎广大读者批评指正（意见或者建议请发至E-mail：lishengg@163.com）。

在本书编写过程中，公安部第一研究所厉剑所长、于锐所长助理都给予了大力支持和精心指导。科研处、证件部的同事们提供了许多技术素材，作者在此致以最诚挚的感谢！

中电智能卡、中电华大、上海华虹、NXP、Infineon、ST、握奇数据、北京航空航天大学等友好单位为本书的编写提供了技术上的支持和帮助，作者在此一并感谢！

感谢清华大学出版社王一玲主任的卓有成效的工作，使得本书得以顺利出版。

本书的出版得到了国家科技支撑计划项目“国家法定身份证件关键技术研究与应用示范”（课题编号2007BAK25B00）的支持，在此表示感谢。

作　者

公安部第一研究所

2010年4月

目录

第1章

智能卡基础

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在某种材质中,封装成卡式、本式或者其他形式。目前智能卡的应用已经进入高峰发展时期,智能卡广泛应用在法定证件、电信(电话卡、GSM卡、3G卡)、医疗保健、娱乐、公交、门票、门禁、识别、银行、有线电视节目收视收费和顾客消费等领域。典型智能卡应用如图1-1所示。

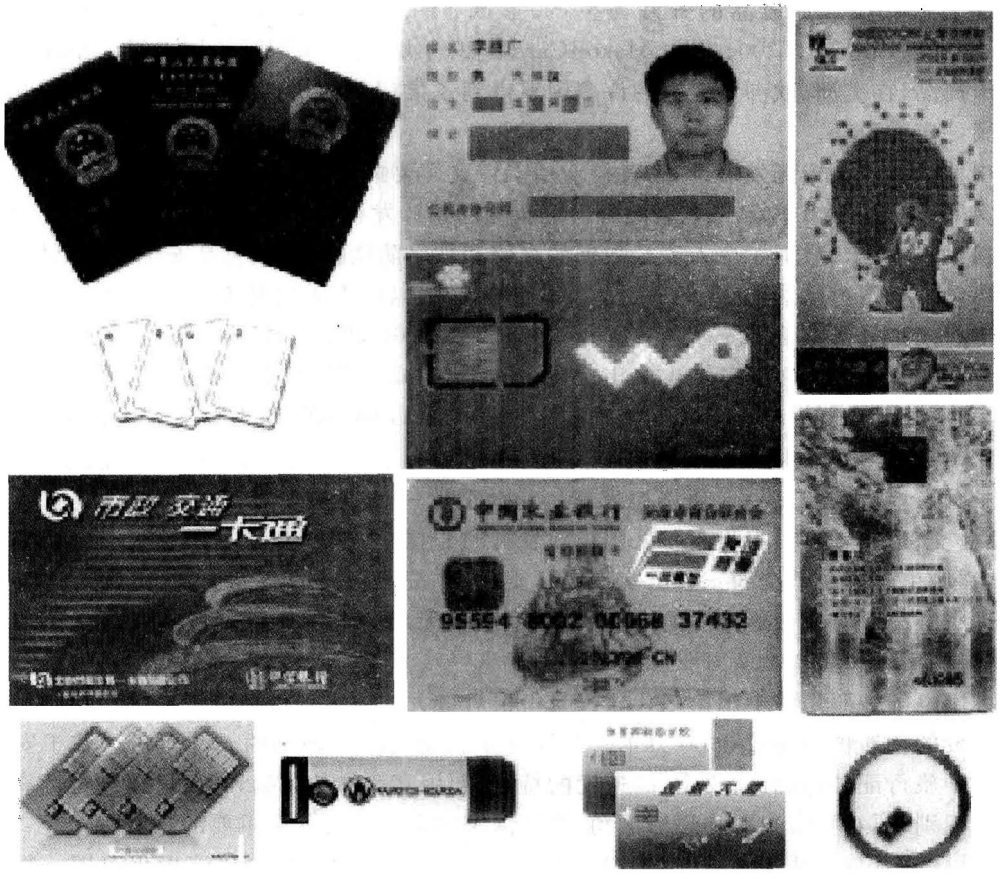

图1-1 典型智能卡应用

智能卡是随着半导体技术的发展和社会对信息安全性等要求的日益提高应运而生的,它里面所包含的集成电路芯片具备微处理器及大容量存储器,具有存储、加密及数据处理能

力，被公认为世界上最小的个人计算机。与目前仍在广泛应用的磁卡相比，智能卡具有安全性高、存储容量大等许多优点，可承载比磁卡多达数百倍的信息，并能与终端结合进行复杂的计算。这种既具有智能性，又便于携带的卡片，为现代信息的处理和传递提供了一种全新手段。智能卡凭借其存储量大、可靠性强、安全性高等优点，风靡全球。

1.1 智能卡发展

智能卡的概念最初由法国人 Roland Moreno 在 1972 年提出，此后法国 Bull 公司率先投入了对这一潜力无穷的高新技术产品的研究和开发。1976 年 Bull 公司高级研究员 Ugon 先生领导的研究小组首先研制成了世界上第一张由双晶片(微处理器和存储器)组成的智能卡，接着又于 1978 年制成了单晶片智能卡并取得了技术专利。

在 20 世纪 80 年代初期，法国和德国开始了最初的智能卡应用实验。除了法国的 Bull 以外，先后有 NXP、Infineon、ST、Motorola、Sharp、Atmel、Samsung 等十几家公司相继投入了智能卡芯片和卡片成品的开发与生产，形成了一个世界性的新兴技术产业。VISA、MasterCard、EuroPay(2001 年与 MasterCard 组织合并)等三大国际信用卡组织相继推出了智能卡产品，在美洲、欧洲及亚洲的许多国家得到了推广和应用，并在各地的信用卡市场上占据了一定的份额。

中国的智能卡市场发展迅猛，各行业用卡情况简要描述如下：

2005 年始发的中国第二代居民身份证至今已累计发行 10 亿张。第二代居民身份证采用非接触式 IC 卡，集成了个人安全数据的存储和数字防伪技术，具有高安全性和可机读性。

移动手机用户已达 7.38 亿人，仅 2009 年的移动电话卡采购量就已超过 8 亿张。移动电话卡有多种分类方法：按容量可分为 16KB、32KB、64KB、128KB 甚至更高；按照无线技术可分为 GSM 网络的 SIM(subscriber identity module，用户身份识别模块)卡、CDMA 网络的 UIM(user identity module，用户识别模块)卡、3G 网络的 USIM(universal subscriber identity module，全球用户识别模块)卡。

中国各地市政公交一卡通飞速发展。市政公交一卡通是在城市公共交通应用环境中(包括公交、地铁、轻轨、出租车)，采用统一发行的非接触式 IC 卡介质作为城市公共交通储值卡，在城市不同公共交通工具上实现统一支付，并按照协定的商务规则，由统一建设的清算管理中心完成对应交通费用的结算和划转，实现无现金电子支付。目前仅北京市政公交一卡通持有量已超过 3200 万张。

中国电子护照是继中国第二代居民身份证后最大的法定证件智能卡应用项目。目前中国已签发的普通护照超过 3000 万本。预计每年新发的电子护照约 650 万份。基于安全芯片的电子旅行证件，具有高安全、高速度的特点，利用其存储的数据，不仅可以进行可靠的个人身份识别，还对打击犯罪和恐怖活动、维护国家的安全具有非常重要的意义。

美国的“智慧地球”、中国的“感知中国”又一次把物联网的概念传遍世界范围。物联网中非常重要的技术是 RFID 电子标签技术。据 ABI Research 市场技术研究公司于 2009 年 11 月统计：2009 年从 RFID 标签、读写器、软件和服务等方面获得的收入估计突破 56 亿美元，涨幅比 2008 年提高 4.25%。

为积极应对银行卡犯罪，全球 EMV 迁移战略规划正在实施中。尽管我国银行卡从磁

条卡向智能卡迁移的步伐因为技术和设备升级的巨额成本而进程缓慢，但毕竟这是一种历史的趋势。央行批准的试点城市——宁波正在推广的市民卡已带有金融应用功能，除了日常支付功能的电子钱包外，还可以直接到 ATM 上取现。中国农业银行天津市分行也发行了带有接触式智能卡的金穗卡。

其他如社保卡、医疗卡、居住证、市政公交一卡通、校园卡、旅游票卡等智能卡应用也正在稳步发展。

据国家金卡工程协调领导小组办公室统计，截止到 2009 年 12 月 23 日，全国各类智能卡发行量已达 70 亿张，在电信、交通、公安、社会保障、医疗卫生等领域得到普及应用。城市市民卡和手机支付等多功能智能卡与智能标签的应用正在创新发展中。

1.2 智能卡分类

智能卡可根据不同方式进行分类：

按照内嵌芯片的电路结构不同，智能卡可分为非加密存储卡(memory card)、逻辑加密卡(memory card with security logic)和 CPU 卡(smart card)。

(1) 非加密存储卡内嵌芯片为存储卡芯片，相当于普通串行 EEPROM(电可擦写可编程只读存储器)，有些芯片还增加了特定区域的写保护功能。这类卡信息存储方便，使用简单，价格便宜，很多场合可替代磁卡。但由于其本身不具备信息保密功能，因此，只能应用于保密性要求不高的场合。

(2)逻辑存储卡是在非加密存储卡的基础上增加了加密逻辑电路，加密逻辑电路通过校验密码的方式来判断卡内的数据对于外部访问是否开放，这样提高了卡的保密性和安全性。但这只是低层次的安全保护，无法防范恶意攻击。

(3) CPU 卡内的集成电路带有微处理器(CPU)、存储单元(包括随机存储器(RAM)、只读存储器(ROM)、电可擦除存储器(EEPROM))以及芯片操作系统(chip operating system,COS)。装有 COS 的 CPU 卡不仅具有数据存储功能，同时具有命令处理和数据安全保护等功能。由于 CPU 卡具有存储容量大、处理能力强、信息存储安全等特性，所以被广泛应用于信息安全性要求特别高的场合。本书后面提到的智能卡如不特殊说明，均指 CPU 卡。

按照封装方式，智能卡又可分为卡式、本式或者其他方式。

按照数据 I/O 接口方式，智能卡可分为接触式智能卡、非接触式智能卡、光通信和 USB 接口智能卡。

不同的分类方式如图 1-2 所示。

本节主要按照数据读写方式进行重点描述。其中，接触式智能卡由读写设备的触点和卡片上的触点相接触，进行数据读写。非接触式智能卡则与读写设备无电路接触，由非接触式的读写技术进行读写(如光通信或无线射频通信)。其内嵌芯片除了存储单元、控制逻辑外，增加了射频收发电路。而同时具有接触式和非接触式接口的卡片称为双界面智能卡。双界面智能卡同时具有射频天线和触点，两者互不影响，两种通信接口的组合扩展了智能卡的应用领域。

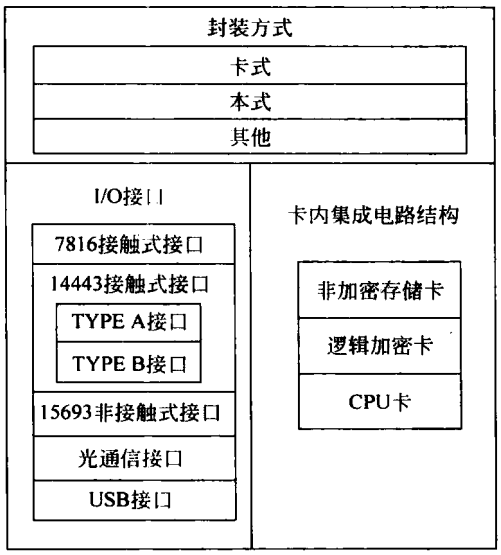

图 1-2 智能卡分类

1.2.1 接触式 IC 卡

接触式 IC 卡片的外形尺寸与基本结构遵循 ISO/IEC 7810 标准，具体参数如图 1-3 所示。

接触式 IC 卡(contact card)通过一组 6～8 个金属触点(如图 1-4 所示)，建立与外界的接口，由读写器的接触弹簧和 IC 卡上的触点产生电流接触，读写器通过接触触点给 IC 卡提供能量和时钟脉冲，读写器与 IC 卡之间的数据传输是通过双向串行接口(I/O)进行。接触式 IC 卡系统由卡基(塑料卡片)、触点、芯片、读写器等组成。

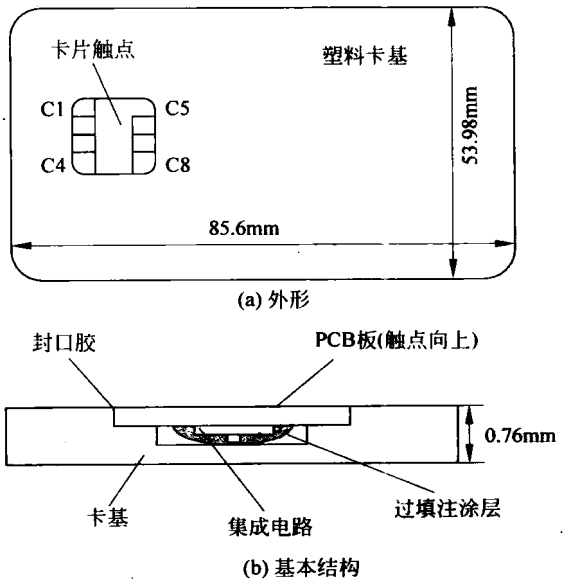

图 1-3 接触式 IC 卡的外形与基本结构

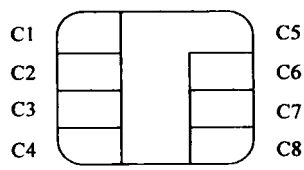

图 1-4 IC 卡触点定义