中文摘要

银行卡从出现至今不过几十年的历史，但是发展十分迅猛。1952 年，美国加利福尼亚洲的富兰克林国民银行首先发行了银行信用卡，之后各家银行纷纷效仿，进入到发卡银行的行列之中。1985 年中国银行正式推出长城卡之后，工行的牡丹卡、农行的金穗卡、建行的龙卡等等陆续推出，银行卡的品种也逐渐丰富，有准贷记卡、借记卡和贷记卡等多个卡种。

银行卡基本上以磁条卡为主，由于近年来针对银行卡的犯罪愈演愈烈，涉及金额逐年成倍增加，各家银行意识到磁条卡存在的技术缺陷，开始推出具有芯片的智能卡。而随着 EMV 迁移战略规划的实施，智能卡将逐步取代磁条卡成为银行卡的主要载体。

本论文结合中国农业银行天津市分行金穗智能卡系统建设项目，对其所涉及的安全机制展开深入研究。金融智能卡系统安全机制涉及的范围十分广泛，除了银行传统的帐务安全体系如总分核算、帐务平衡，必要的管理机制如机具管理、黑名单管理之外，在密钥管理、卡片管理以及交易过程中处处体现出安全机制的重要性。

在密钥管理方面，通过对人行三级密钥体系的研究，结合天津农行智能卡系统发展的要求，设计出灵活的密钥系统，来应对人行二级密钥中心建成之后对系统的影响；在卡片结构设计上，根据行业应用的需要，合理设计文件结构，充分利用卡片空间，针对不同的需求使用不同容量的卡片；在卡片管理方面，除了完成常规的管理之外，提出在线追加应用以及卡片的回收再利用等卡片生命周期管理的关键环节，充分保护已有投资，最大限度地节省成本；在重要交易方面，严格按照 PBOC 的标准设计交易处理流程，保障交易的完整性和安全性。

总之，本文对金融智能卡系统安全方面的问题进行了深入研究，取得了一些成果，为金融智能卡系统安全机制的建立和实施提供了可行方案。

关键词　金融智能卡 安全机制　密钥　卡片管理　交易安全

ABSTRACT

Bank card is growing quickly though it just emerged from several decades of history. Since Franklin National Bank in United States California issued the first bank credit card in 1952, the banks have followed suit and entered the ranks of issuers. The Great Wall Card was officially launched by Bank of China in 1986. Subsequently, the Industrial and Commercial Bank of Peony Card, the Agricultural Bank of Jinsui Card, the Construct Bank of Dragon Card, etc., have emerged one after another. Bank cards are beginning to have the variety of credit card, debit card and other varieties of credit card.

Basically, bank cards are with magnetic cards mainly. Because the offenses have grown in recent years against bank cards and the amount has greatly increased, the banks realized magnetic card itself technical defects. The launch has begun to make some chip bank cards. With the implementation of EMV migration strategic planning, the smart card will gradually replace magnetic cards and become the main carrier of bank cards.

In this paper, we will involve in the conduct in-depth studies for the security mechanisms which are the Agricultural Bank of China's Tianjin Branch of Jinsui smart card systems projects. Financial smart card systems involved in a very broad range of security mechanisms, in addition to traditional banking accounts such as a security system scores accounting, Accounts balance, and the necessary management tools such as facility management, management of the blacklist, in the password management, cardholder management and process card transactions reflected the importance of the safety mechanism.

In the key management, according to the Agricultural Bank of smart card systems for the development of Tianjin, Key design a flexible system to deal with the People's Bank of the system that is three-tier system after the second key center; for the structural design of the cards, according to industry application needs, design the structure of the document, and make full use of a card room The capacity of the different needs of different cards; in the cardholder management, beside completing the conventional management, we talked about the online cards put additional applications and the use of recycling cards and the key to life-cycle management for the full protection of investment, the maximum cost savings. For the important transactions in the security mechanism, this paper focuses on how to implement the relevant requirements of PBOC standards and the correct use the key in the transaction process.

In short, this article on the financial aspects of the smart card system security conducted an in-depth study has yielded some results. It provides the implementation of the options for the establishment of the financial smart card security mechanisms.

Keywords: financial smartcard security mechanism key card management transaction security

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作和取得的研究成果，除了文中特别加以标注和致谢之处外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得 天津大学 或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

学位论文作者签名：李爵　　签字日期：2007 年 1 月 31 日

学位论文版权使用授权书

本学位论文作者完全了解 天津大学 有关保留、使用学位论文的规定。特授权 天津大学 可以将学位论文的全部或部分内容编入有关数据库进行检索，并采用影印、缩印或扫描等复制手段保存、汇编以供查阅和借阅。同意学校向国家有关部门或机构送交论文的复印件和磁盘。

（保密的学位论文在解密后适用本授权说明）

学位论文作者签名：李爵　　导师签名：

签字日期：2007 年 1 月 31 日　　签字日期：2007 年 1 月 31 日

第一章 绪论

1.1 引言

1985 年中国银行正式推出长城卡后，从磁条卡到智能卡的发展给银行卡注入了新的活力[1]。随着人们对智能卡认识的提高，金融业务服务领域的不断拓宽，金融与社会其他领域合作的日益密切，金融智能卡逐渐被人们所接受。卡片可以实现的功能也不断增强，同一张卡上可以实现多种行业应用功能，使得金融智能卡可以全方位为社会服务，日益成为人们生活中不可或缺的支付手段和电子服务工具[2]。

据《金融时报》报道，以银行卡、IC卡为代表的“电子货币”正在我国得到广泛应用。过去 10 年，全国累计发行这种“电子货币”18.69 亿张，包括 5.69 亿张银行卡和 13 亿张各类IC卡。到 2003 年 6 月底，全国累计发行使用各类IC卡 13 亿张，包括电信行业发行的公用电话IC卡约 7 亿张、移动电话SIM卡 3 亿张和社会保障卡、组织机构代码卡、交通卡、加油卡等其它各类IC卡约 3 亿张。近年来随着电子银行业务的发展，使智能卡在网上银行安全认证中也得到了较为广泛的应用[3] [4] [5]。

由国家建设部主导的数字化城市正在积极推行之中，各种非金融智能卡应用不断出现，一些尚未发展自己系统的应用单位也迫切需要与银行联合，以保证其在“城市一卡通”的快速发展之中不致落伍。因此，是否具备自己的金融智能卡系统，支持非金融应用，就成为商业银行占领市场、发展业务的关键。

金融智能卡在天津的金融市场上并不多见，主要原因是人民银行的二级密钥中心尚未完全建成，各家大型商业银行虽然可以从各自的总行得到二级密钥，但是目前在天津暂时还没有支持全国统一消费密钥的机具——特别是银联的机具。如何加快发展符合人民银行标准的智能卡系统，并且能够灵活定制非金融的行业应用，并随着行业应用的发展而不断发展，是摆在各家商业银行面前的课题。

1.2 选题意义

银行业为了应对越来越激烈的同业竞争，特别是外资银行进入中国经营人民币业务以后的竞争，投入更多的资源进行产品创新、渠道整合和数据集中等提升竞争力的工作，对于信息技术的运用也达到了前所未有的程度[6]。银行卡产品在国外已经十分成熟，而且产品和服务的创新层出不穷，已经将我国的大型商业银

行落在了后面。面临这种形势，必须加快银行卡产品的发展，跟上国外银行的脚步，才具备竞争者的资格。银行卡的竞争从产品本身的金融功能竞争扩展到跨行业服务功能的竞争，而除了享受其他行业的打折优惠等“增值服务”功能之外，银行卡需要和行业应用更紧密的结合起来，智能卡对这种“结合”可以提供最好的支持[7]。

随着银行卡数量增多，用卡环境的发展，银行卡的安全问题日益突出。由于目前的银行卡基本上都使用磁条卡，而磁条卡上记录的磁信息易于破解和复制，虽然在磁道加密方面上有一些防范措施，可是这些技术不足以抵挡越来越高明的犯罪分子和越来越先进的犯罪手段。智能卡的特性决定了其具有较高的安全性，作为新一代的银行卡是非常合适的。

各家商业银行都开始研究、实践金融智能卡系统。金融智能卡系统涵盖多方面的技术，实施起来较为复杂，包括发卡、密钥、帐务、交易、接口等多个子系统。除了要熟悉卡片特性之外，还要掌握发卡机、加密机、读写器、圈存机、ATM、POS等相关硬件设备的接口。对于金融应用，有人民银行规定的标准；对于非金融应用，有行业自己的标准，在设计时要统筹兼顾[8]。

智能卡是以安全性著称的，金融卡对安全的要求使得智能卡成为其最好的载体，而安全机制始终贯穿智能卡系统的设计和实现之中。

1.3 智能卡简介

智能卡的名称来源于英文名词“Smart card”,又称IC卡(Integrated Circuit card)，即集成电路卡[9]。它将一个集成电路芯片镶嵌于塑料基片中，封装成卡片的形式，其外形与覆盖磁条的磁卡相似。

IC 卡的概念是 70 年代初提出来的，法国布尔(BULL)公司于 1976 年首先创造出 IC 卡产品，并将这项技术应用到身份证明、通讯、金融、交通等多个领域，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和存储数据的能力，其存储器中的内容根据需要可以有条件地提供外部读取和内部信息处理。带有CPU芯片的IC卡，具有独立运算、加解密和存储能力，所以安全性高。由于芯片卡的复制难度要比磁条卡大得多，所以能有效防范伪造[10]。

1.3.1 智能卡分类

一、按芯片类型划分：

1. 存储器卡 (Memory Card)：卡内芯片为电可擦除可编程只读存储器EEPROM(Electrically Erasable Programmable Read Only Memory)，以及地址译码电路和指令译码电路。为了能把它封装在0.76mm的塑料卡基中，特制成0.3mm的薄型结构。存储卡属于被动型卡，通常采用同步通信方式。这种卡片存储方便、使用简单、价格便宜，在很多场合可以替代磁卡。但该类IC卡不具备保密功能，因而一般用于存放不需要保密的信息。

2. 逻辑加密卡 (Logic Encrypt Card，Security Card)：该类卡片除了具有存储卡的EEPROM外，还带有加密逻辑，每次读/写卡之前要先进行密码验证。如果连续几次密码验证错误，卡片将会自锁。从数据管理、密码校验和识别方面来说，逻辑加密卡也是一种被动型卡，采用同步方式进行通信。该类卡片存储量相对较小，价格相对便宜，适用于有一定保密要求的场合。

3. CPU卡 (Smart Card)：卡中的集成电路包括MPU、CAU、EEPROM、RAM以及ROM等。其中在ROM中固化了片内操作系统COS(Chip Operating System)。这种卡片具有存储容量大，处理能力强，信息存储安全等特性。因此，广泛用于信息安全性要求特别高的场合。从严格意义上说，具有CPU和COS的芯片卡才是真正的智能卡。

CPU卡硬件结构如图1-1，具体说明见表1-1。

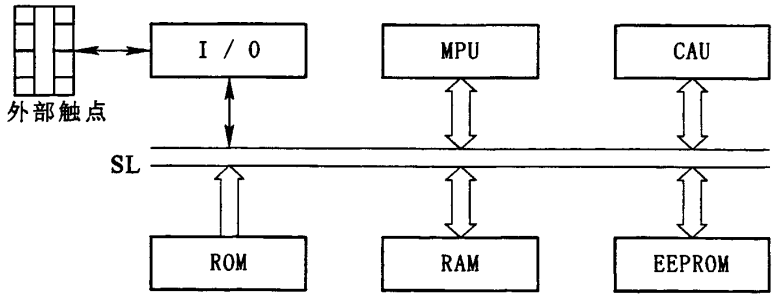

图1-1 CPU卡硬件结构

表 1-1 CPU 卡有关硬件资源说明

硬件资源	说 明	主要功能
MPU	微处理器	系统的中央运算、处理、管理
CAU	加密运算协处理器	执行有关加密、解密运算
ROM	只读存储器	存储操作系统程序
RAM	随机存储器	临时工作数据的暂存
EEPROM	电可擦除存储器	应用程序、数据的存储
I/O	通信接口	通信传输
SL	安全逻辑	内部资源的硬件保护

4. 超级智能卡：在 CPU 卡的基础上增加键盘、液晶显示器、电源，即成为超级智能卡，有的卡上还具有指纹识别装置。VISA 国际信用卡组织试验的一种超级卡即带有 20 个健，可显示 16 个字符，除有计时、计算机汇率换算功能外，还存储有个人信息、医疗、旅行用数据和电话号码等。

二、按读写形式划分

1. 接触式 IC 卡：该类卡是通过 IC 卡读写设备的触点与 IC 卡的触点接触后进行数据的读写。国际标准 ISO7816 对此类卡的机械特性、电器特性等进行了严格的规定。

2. 非接触式IC卡：该类卡与IC卡设备无电路接触，而是通过非接触式的读写技术进行读写（如光或无线技术）。其内嵌芯片除了CPU、逻辑单元、存储单元外，增加了射频收发电路，又可称为感应式IC卡（RF射频卡）。国际标准 ISO10536 系列阐述了对非接触式IC卡的规定。该类卡一般用在使用频繁、信息量相对较少、可靠性要求较高的场合[11]。

3. 双界面卡：近年，国外知名的大厂商推出了一种将射频卡和接触卡合而为一的复合卡，以增强智能卡的兼容性能和增加智能卡的应用灵活性。主要是对接触型的 CPU 卡增加非接触模块，使其具备非接触访问能力。如图 1—2。

图1-2 双界面卡示意图

智能卡表面可印刷各种图案，甚至人像。卡的尺寸、触点的位置、用途及数据格式等均有相应的国际标准予以明确规定。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，在IC卡上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，一般称其为磁条、芯片复合卡。如图1—3所示，黑色的长方框代表磁条，虚线框代表芯片。

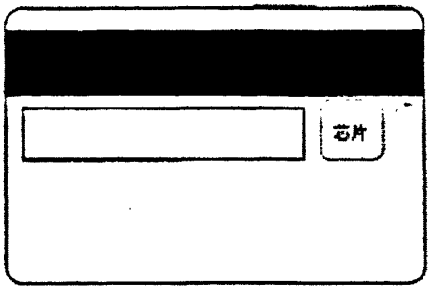

图1-3 复合卡（背面）示意图

三、按数据交换方式划分

1. 串行IC卡：当卡片与外界进行数据交换时，数据流按照串行方式输入输出，电极触点较少，一般为6个或者8个。由于串行IC卡接口简单、使用方便，目前使发卡量最大。

2. 并行IC卡：卡片与外界进行数据交换时以并行方式进行，有较多的电极触点，一般在28个到68个之间。并行卡主要具有两方面的好处，一是数据交换速度提高，二是现有条件下存储容量可以显著增加。

四、按应用领域划分

1. 金融卡：又可分为贷记卡、准贷记卡(以前称为信用卡)和借记卡三种。贷记卡和准贷记卡的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。借记卡可用作电子存折和电子钱包，不允许透支。

2. 非金融卡：又称行业卡，分布在电信、社保、公交、石化、商业等领域外，还延伸到身份识别、校园、烟草、三表、停车、交管等多个领域，如二代身份证、驾驶员管理卡和水电表卡等等[12]。

1.3.2 智能卡的特点

由于智能卡采用了半导体制造技术和信息安全技术，相对于其它种类的卡具有以下四大特点：

1. 存储容量大：其内部有RAM、ROM、EEPROM等存储器，存储容量可以从几个字节到几兆字节。卡上可以存储文字、声音、图像等各种信息。

2. 安全性高：从硬件和软件等几个方面实施其安全策略，可以控制卡内不同区域的存取特性。如遇外部非法攻击，卡片还具备自毁能力。

3. 性能可靠：IC卡防磁、防静电，抗干扰能力强，可靠性高。

4. 使用寿命长：一般至少可重复读写十万次以上。

1.4 COS 简介

1.4.1 COS 基本介绍

COS的全称是Chip Operating System(片内操作系统)，它一般是紧紧围绕着智能卡的特点而开发的[13]。由于受智能卡内微处理器芯片的性能及内存容量的影响，因此COS在很大程度上不同于微机上的操作系统。

COS 一般都是根据某种智能卡的特点及其应用范围而特定设计开发的，尽管它们在所实际完成的功能上可能大部分都遵循着同一个国际标准。COS 在本质上更加接近于监控程序，而不是一个真正意义上的操作系统。COS 所需要解决的主要还是对外部的命令如何进行处理、响应的问题，这其中一般并不涉及到共享、并发的管理及处理。

COS 的主要功能是控制智能卡和外界的信息交换，管理智能卡内的存储器并在卡内部完成各种命令的处理。其中，与外界进行信息交换是 COS 最基本的要求。在交换过程中，COS 所遵循的信息交换协议目前包括两类：异步字符传输的 T=0 协议以及异步分组传输的 T=l 协议。

智能卡的 COS 中最重要的两方面就是文件与安全。

1.4.2 COS 的文件系统

智能卡中的“文件”概念与我们通常所说的文件是有区别的。尽管智能卡中的文件内存储的也是数据单元或记录，但它们都是与智能卡的具体应用直接相关的。一般而言，一个具体的应用必然要对应于智能卡中的一个文件，因此，智能卡中的文件不存在一般的文件共享的情况。而且，这种文件不仅在逻辑上必须是完整的，在物理组织上也都是连续的。此外，智能卡中的文件尽管也可以拥有文件名(File Name)，但对文件的标识依靠的是与卡中文件一一对应的文件标识符(File Identifier)，而不是文件名。因为智能卡中的文件名是允许重复的，它在本质上只是文件的一种助记符，并不能完全代表整个文件。

COS 的文件按照其所处的逻辑层次可以分为三类：主文件(Master File)，专用文件(Dedicated File)以及基本文件(Elementary File)。其中，主文件对任何 COS 都是必不可少的，它是包含有文件控制信息及可分配存储区的唯一文件，其作用相当于是 COS 文件系统的根文件，处于 COS 文件系统的最高层；基本文件也是必不可少的一个部分，它是实际用来存储备应用的数据单元或记录的文件，处于文件系统的最底层，而专用文件类似于目录，它存储的主要是文件的控制信息、

文件的位置、大小等数据信息。我们可以用图 1-4 的树状结构来形象地描述一个 COS 的文件系统的基本结构。

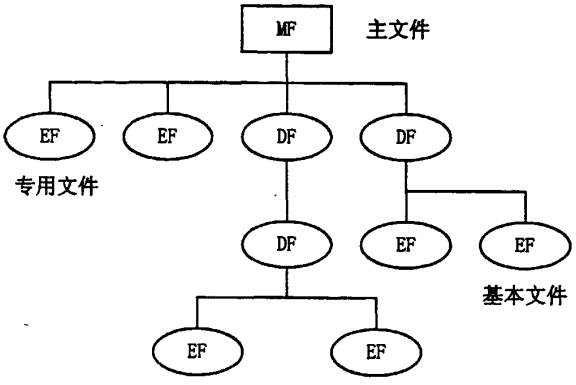

图1-4 COS文件结构示意图

1.4.3 COS 的安全体系

智能卡的安全体系是智能卡的 COS 中一个极为重要的部分，它涉及到卡的鉴别与核实方式的选择，包括 COS 在对卡中文件进行访问时的权限控制机制，还关系到卡中信息的保密机制。可以认为，智能卡之所以能够迅速地发展并且流行起来，其中的一个重要的原因就在于它能够通过 COS 的安全体系给用户提供较高的安全性保证。

安全体系在概念上包括三大部分：安全状态(Security Status)，安全属性(Security Attributes)以及安全机制(Security mechanisms)。

安全状态是指智能卡在当前所处的一种状态，这种状态是在智能卡进行完复位应答或者是在它处理完某命令之后得到的。事实上，我们完全可以认为智能卡在整个的工作过程中始终都是处在这样的或是那样的一种状态之中，安全状态通常可以利用智能卡在当前已经满足的条件的集合来表示。

安全属性实际上是定义了执行某个命令所需要的一些条件，只有智能卡满足了这些条件，该命令才是可以执行的。因此，如果将智能卡当前所处的安全状态与某个操作的安全属性相比较，那么根据比较的结果就可以很容易地判断出一个命令在当前状态下是否是允许执行的，从而达到了安全控制的目的。

和安全状态与安全属性相联系的是安全机制。安全机制可以认为是安全状态实现转移所采用的转移方法和手段，通常包括：通行字鉴别，密码鉴别，数据鉴

别及数据加密。一种安全状态经过上述的这些手段就可以转移到另一种状态，把这种状态与某个安全属性相比较，如果一致的话，就表明能够执行该属性对应的命令，这就是COS安全体系的基本工作原理[14]。

1.4.4 典型的 COS 系统

一般的芯片厂商都有自己开发的 COS，比较知名的卡片厂商捷德（G&D）、握奇(WATCHDATA)由于卡片应用较为广泛，所以他们各自的 COS 也为人熟知。

STARCOS

智能卡芯片操作系统 STARCOS（Smart Cark Chip Operation System）是由德国 G&D 公司和 GMD 公司合作开发的智能卡卡片级的一个完整的操作系统。它提供适合具体应用的操作和管理的 20 余条指令，而且其透明的结构使得用户可以集成自定义的指令。

TIMECOS

TIMECOS（Time Card Operating System）是握奇数据（WATCHDATA）系统有限公司自行开发的智能卡操作系统，符合相关标准，支持一卡多应用，各应用之间相互独立，支持多种安全访问方式和权限。

1.5 金融智能卡的安全

智能卡本身具有较高的安全性。卡片在出厂时由厂家将测试电路熔断，并且对不同批次的卡片都给以不同的初始保护密钥。卡片在运输过程中也受到了严格的保护，卡片在交付发卡行之前由厂商负责其安全。而交付之后，发卡行必须用厂商提供的密钥卡（称之为洗卡母卡）和控制卡来洗卡，即将厂商的出厂密钥替换成用户自己的密钥，从而保障了卡片本身的安全[14]。

卡片的操作系统COS在设计时也充分考虑了安全控制机制，对卡片的初始化、读出、写入等等做了非常严密的安全控制。COS可以做到对卡片本身的各个文件分区加以不同的密钥保护，不同分区之间是不可访问的[15]。

做为银行这样的金融机构，对客户资金安全、系统安全等等有着更高的要求。从人民银行对智能卡的有关标准来看，有专门的部分来规范卡片的物理安全和应用安全。商业银行在智能卡系统设计实现时除利用卡片、操作系统提供的安全特性之外，又增加了多个安全控制环节。

密钥子系统是智能卡系统的安全核心，作为省市级的商业银行，是人行设计的密钥体系中的三级中心，从二级中心（即商业银行总行）获得密钥母卡，经过

密钥分散之后发行自己的用户卡。银行机具中使用的SAM（安全存取模块 Secure Access Module）卡可以直接由上级中心领用，也可以根据需要，按照密钥体系统一规范自己制作。没有总行的城市商业银行，则可以在当地人行的二级密钥中心获得二级密钥。由于银行卡必须支持联网通用，所以消费密钥必须是在全国的密钥体系中统一管理的。

1.6 本文研究的主要内容

本文主要对智能卡系统的密钥子系统、卡片结构设计、卡片管理子系统和部分重要的交易涉及到的安全机制进行研究，并给出实现过程。

由于多年来的银行卡的超常规发展造成磁条卡的发卡量巨大，而换用智能卡的成本非常高，使得人民银行全国统一的密钥系统建设速度比较缓慢。在实现密钥子系统时，我们充分考虑了面临的这种情况，力争在设计上注重灵活性，把密钥子系统设计成一级和三级密钥中心的混合体，以满足未来平滑切换以及业务发展的需要。

卡片作为银行的“重要凭证”，从入库、出库、领用，到个人化、挂失、作废和销毁，都有一系列严格的规定。在设计实现发卡管理子系统时，对卡片的各项操作都做了严格管理，重要操作必须要求双人操作、互相监督。卡片发到用户手中之后，如果用户增加新的行业应用，也必须由银行柜员在严格的权限控制之下完成。而对于一些专门用于消费的联名卡，客户常常使用完卡内的金额之后就会丢弃，为了节省成本，系统还专门实现了卡片回收循环使用的方案。

在交易子系统的设计实现中，完全按照行业标准对重要金融交易进行了研究，保证其安全性。在交易过程中具有三种验证模式，系统都完全实现，包括卡片和机具之间互相验证、卡片加密机之间联机验证以及脱机交易批量入帐时和加密机之间的验证。电子存折交易由于金额比较大，必须后台进行联机验证的。而金额较小的电子钱包交易，则可以不用联机，只要和机具之间 MAC（报文认证码 Message Authentication Code）验证通过就可以消费。消费时由机具记载交易明细并计算出 TAC（交易验证码 Transaction Authorization Crypogram），送到主机通过验证并记帐之后，银行就可以给商户划拨资金来完成清算。

第二章 智能卡系统综述

2.1 设计思想

金融智能卡系统首先必须满足金融交易的所有应用，具备一卡多帐户、多币种和理财功能，在网点、ATM、CDM 进行存取款、卡内转帐、卡卡转帐、商户 POS 消费。系统卡支持智能卡主帐户、电子存折帐户和电子钱包帐户。电子存折应支持圈存、圈提、存现、取现、消费、查询余额、查询交易明细等。电子钱包应支持圈存、消费、查询余额等功能。支持磁条和芯片的复合卡，支持各种中间业务和理财功能，确保银行卡业务的连续性和可持续发展。

智能卡在使用过程中，银行应该提供各种交易设备和方式，方便客户完成各种交易。所以智能卡系统需要支持柜台、POS、ATM、圈存机、自助服务终端等各个渠道。

IC 卡有很多的应用领域，银行的金融卡必须做到与这些应用相结合才能取得发展空间。如果每一种应用都要用不同的卡，那么会给客户带来极大的不便。因此，智能卡应支持多种应用，真正做到“一卡多用”[16]。目前已有的 IC 卡应用领域包括以下内容：交通、石化、社保、医疗、校园、配送行业、智能小区、行政事业收费、公共事业收费等等。

由于卡片存储空间的限制，而且持卡人身份的不同，消费环境的不同，所以一张金融 IC 卡不可能包含所有的应用。我们可以根据持卡人的特点，将不同的应用有机的结合起来。客户在使用过程中可以根据自己的实际需要随时开通非金融应用。

此外，系统应该具有良好适应性，拓展灵活，支持定制功能，可以根据于不同的业务应用完成有关设置。

2.2 系统架构

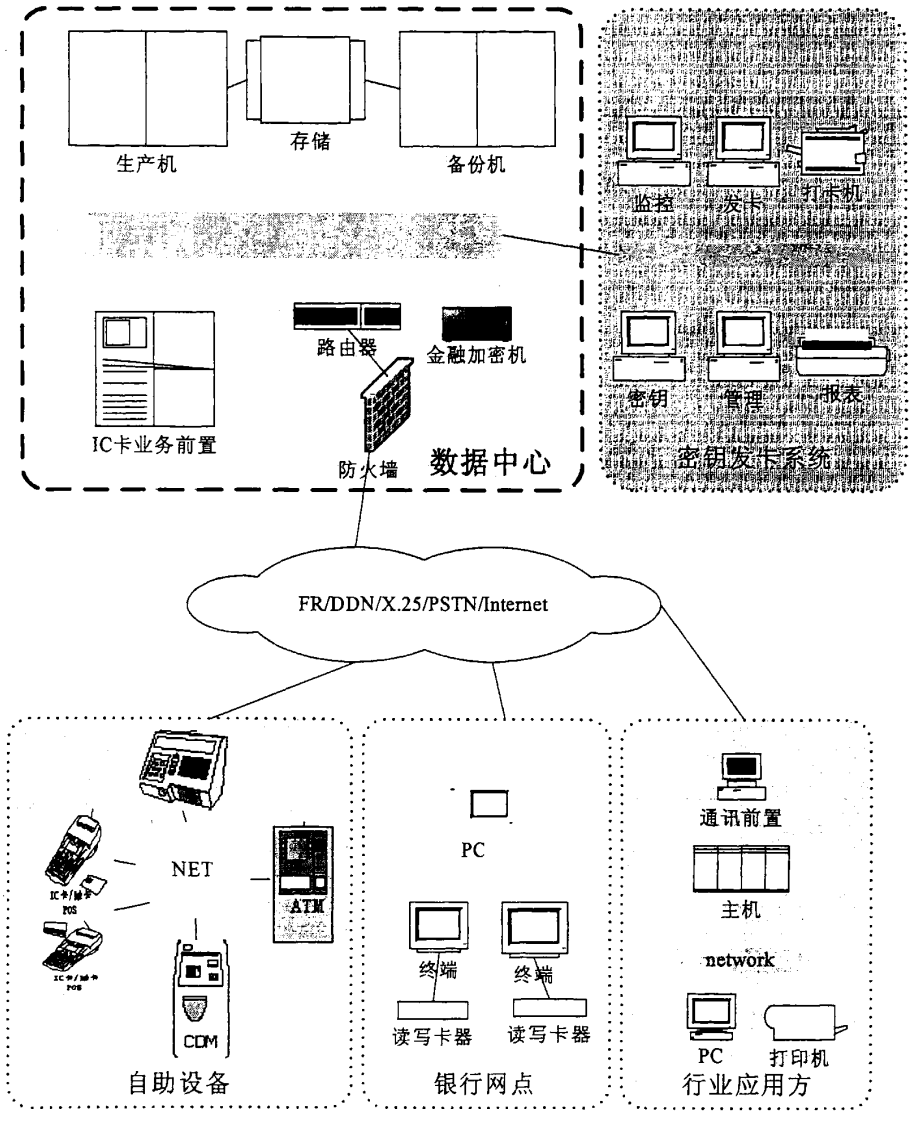

图 2-1 系统架构

如图 2-1，目前大型商业银行都实现了数据集中，帐务系统上收到了总行数据中心，分行端配置了业务处理的前置机，作为交易汇总转发的中间层。智能卡系统的主机可以认为是中间层的前置或者扩展，放置在分行数据中心。另外配置加密机，作为交易验证使用。密钥子系统可以部署在分行数据中心也可以部署在

银行卡管理中心，发卡子系统直接部署在银行卡管理中心。银行网点要配置 IC 卡读写设备，自助机具要做相应的改造，支持磁条和芯片的双重读写。

2.3 环境要求

以中国农业如银行天津市分行的智能卡系统为例，对软硬件环境和网络环境的要求说明如下：

2.3.1 硬件环境

主机采用 IBM RS/6000－4CPU 8G 内存 36Gx12 磁盘阵列；前端设备采用基于 inter 的微机、服务器；硬加密机使用五十六所的 SJT06；专用打卡机使用 DataCard 的 DC7000；IC 卡读写器一般要配备 2 个读写槽和 4 个 PSAM 卡槽，并且具有在 windows 和 unix 下的驱动。在 ATM 等自助设备上要配备吸入式 IC 卡读写设备。

2.3.2 软件环境

主机操作系统 AIX v4.3.3 ；数据库使用 Sybase v12.0；微机、服务器操作系统一般为 windows 2000；网点前置机操作系统 SCO UNIX 5.0.5；开发语言使用 Power builder 以及 ANSI C。

2.3.3 网络环境

商业银行的网络系统都比较成熟，天津地区网络服务提供商（网通、联通、铁通、广电、电信、移动）都有自己的网络体系，支持铜线或光纤，协议支持 DDN、FR 到 ATM 等等。本文中涉及的金融智能卡系统运行在商业银行的现有网络架构之上，对网络带宽、协议等无特殊要求。

2.4 系统功能逻辑结构

如图 2-2 所示，系统共分为八个子系统：发卡管理子系统、密钥管理子系统，监控统计子系统，帐务处理子系统、交易处理子系统、业务管理子系统、对外接

口子系统和功能定制子系统。其中密钥管理子系统、发卡管理子系统和交易处理子系统是本文研究的主要部分。

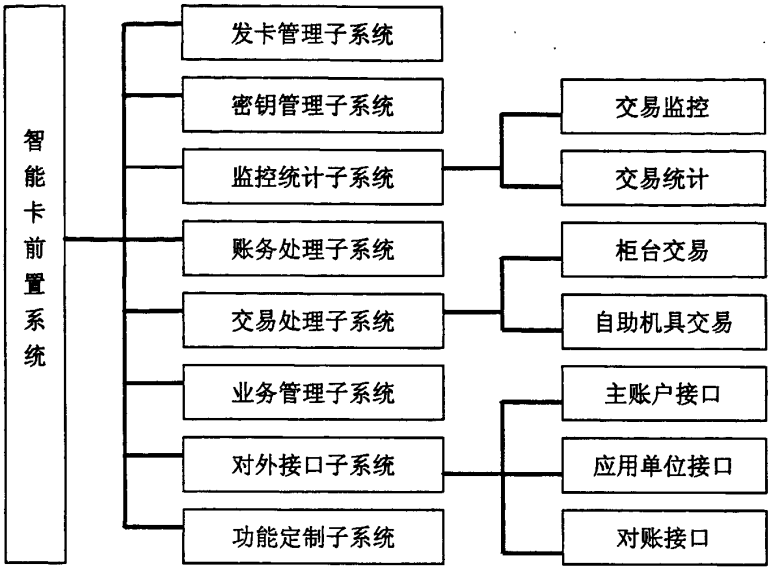

图 2-2 系统功能逻辑结构图

2.5 系统有关安全机制

从图 2-3 中我们可以看出，密钥子系统、发卡子系统和交易子系统的关系十分密切。

密钥子系统从上级中心收到密钥后，可以为发卡系统制作发卡母卡，向交易系统中的加密机下装验证密钥。发卡子系统利用发卡母卡制作用户卡和 PSAM 卡。用户卡经过个人化之后发到用户手中，PSAM 卡则安装在机具之中。在交易时，用户卡和 PSAM 卡之间做脱机认证，在联机交易中，用户卡和帐务中心的加密机之间做联机认证。商户在营业结束之后银行日终处理之前，机具将脱机交易流水批量发送到帐务主机，由主机调用加密机的有关功能来校验 TAC，即校验流水的合法性。

在用户卡中，可以根据操作的不同规定不同的应用密钥；在不同的应用分区中，可以根据合作方的要求灵活设置发卡模式，即银行自主模式、双方合作模式和银行代管模式。这些发卡模式同样需要密钥系统具备相应的支持，有时候甚至

可以根据合作方的需要为其单独设置密钥系统，并完全由银行来代管，合作方只需派人来输入密钥的种子，由密钥系统完成计算处理。

在脱机交易中，早期的 PBOC 标准规定了电子钱包可以不记载交易明细。在新的标准中，电子钱包也可以记载交易明细，同时增加了状态控制和灰锁等更加安全的控制机制，使得交易安全得到了更充分的保证。

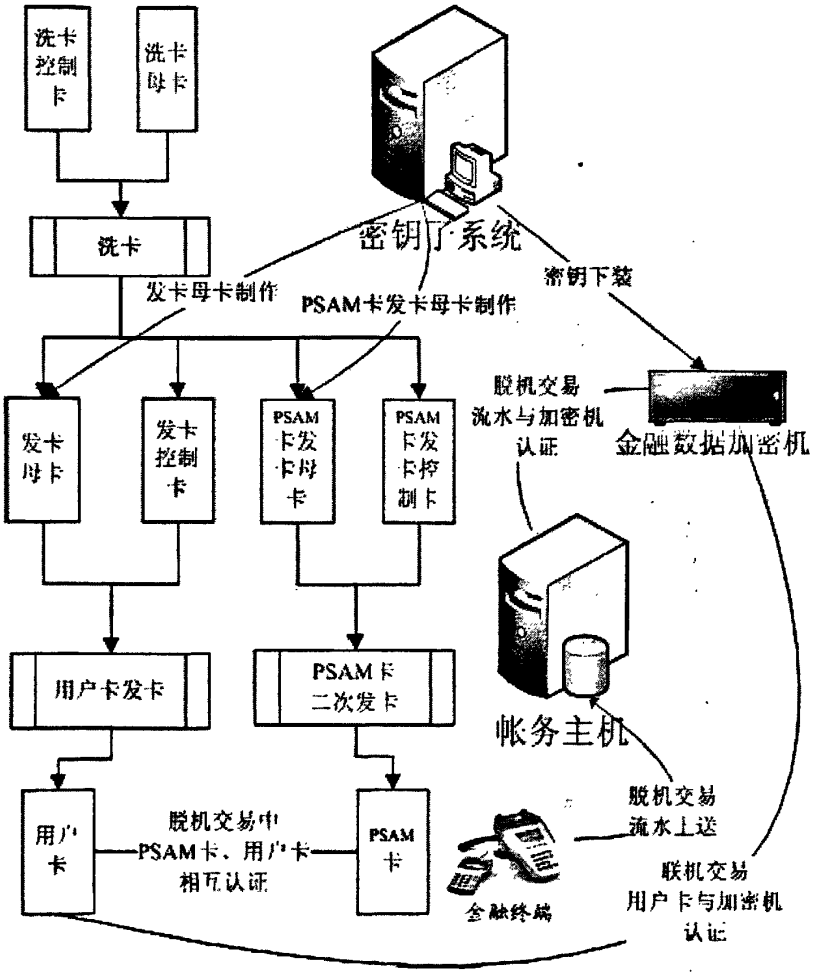

图 2-3 发卡、密钥和交易子系统的关系

第三章 密钥子系统设计

3.1 密钥体系

根据人民银行《全国银行IC卡密钥管理规则》规定，银行IC卡密钥采用三级管理体制，即人民银行全国密钥管理中心（一级中心）、城市人民银行或商业银行密钥管理中心（二级中心）及发卡银行密钥管理中心（三级中心）。整个安全体系结构主要包括三类密钥：全国通用的消费/取现主密钥 GMPK、发卡银行的消费/取现主密钥MPK和发卡银行的其他主密钥。

GMPK是整个系统的根密钥，全国密钥管理总中心用GMPK对各二级机构标识进行分散，产生二级机构消费/取现主密钥BMPK，生成二级机构发卡母卡，并且将它与二级机构外部认证密钥卡一起传输给二级机构。同时，全国密钥管理总中心还需对要下发的所有PSAM卡进行统一洗卡，装入GMPK，和PSAM外部认证卡一起传递给二级机构。

MPK 由二级密钥管理中心（如商业银行总行和人民银行区域分行）利用全国密钥管理总中心下发的二级机构发卡母卡产生，在接收到全国密钥管理总中心传来的二级机构发卡母卡和外部认证卡后，用BMPK对各成员行标识进行分散，生成成员行消费/取现主密钥MPK，产生成员行发卡母卡和成员行外部认证卡一起传送给各成员行。同时，二级机构还要向成员行转交 PSAM 外部认证卡和PSAM卡。

成员行可直接向成员行发卡母卡中注入银行专用密钥，利用成员行发卡母卡来提供密钥服务（如发放客户卡，PSAM 二次发卡、清算等）。成员行也可自己产生专用密钥，将成员行发卡母卡中的消费/取现主密钥MPK注入到硬件加密机或母卡，利用硬件加密机或母卡来提供密钥服务。

如图3-1所示，以人民银行总行为一级中心，密钥通过银行和地区代码不同分散到二级中心，即商业银行总行和人民银行的地区分行，再通过一次分散到三级中心，即各商业银行的分行和无全国总行的地区商业银行。

在密钥子系统的设计中，我们结合了人民银行全国密钥系统的发展要求以及天津市的的实际情况，设计实现了模拟一级中心产生根密钥，实现三级中心的所有功能，先发展本行自己的业务，待全国密钥系统成熟之后可以实现平滑切换。

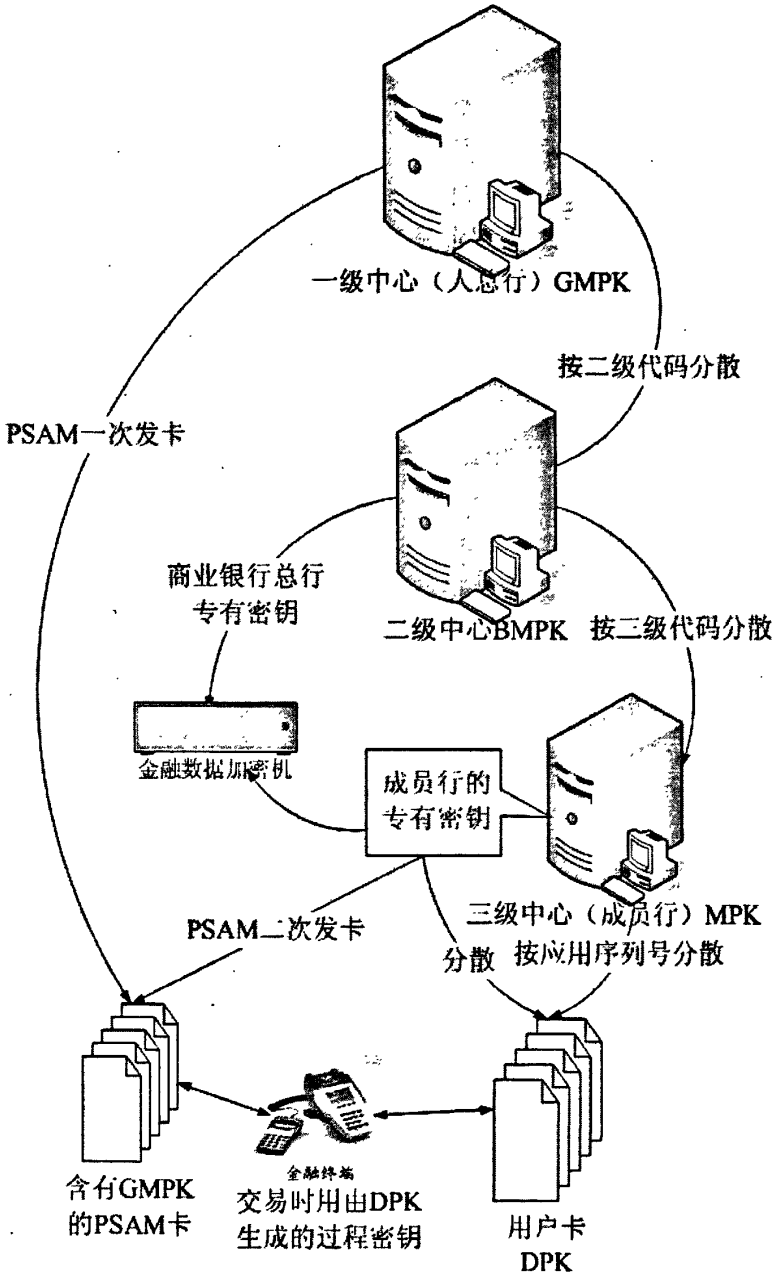

图 3-1 三级密钥体系示意图

3.2 版本和索引的应用

为了降低密钥泄漏导致的风险，IC卡密钥管理系统使用了密钥的多版本和多索引技术[17]。如图 3-2 所示。下面以消费主密钥为例说明密钥的多版本和多索引技术是如何降低系统风险的：消费主密钥总共有 5x5=25 个不同密钥，在用户卡中存放的是其中的同一版本的 5 个密钥，在PSAM卡中存放的是其中的同一索引的 5 个密钥，在交易时，使用的用户卡和PSAM卡所共同拥有的密钥。当其中的一个密钥泄漏时，可以将所有包含该密钥PSAM卡销毁，替换成其他索引的PSAM卡，这样使泄漏的密钥不会在消费中再次使用，保证了交易的安全。由于只更换少量的PSAM卡，大量的用户卡不用作任何变动，从而降低了密钥泄漏所导致的风险。消费密钥的多版本和多索引如图 3-2 所示。

在设计中，我们考虑到系统面临全国数据集中而有上收的可能性，并且由于金融智能卡在我国使用范围不算广泛，面临的风险不大。同时为了节省管理成本和卡片存储资源，决定采用三组密钥，每组三个索引，即 9 个不同的密钥来作为本系统的消费密钥。

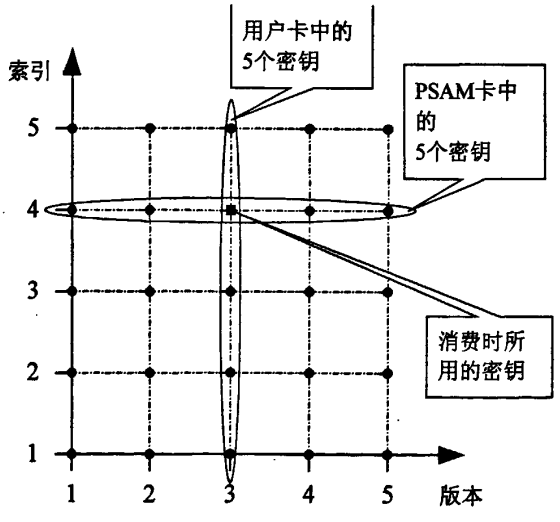

图 3-2 消费密钥的多版本和多索引技术示意图

3.3 应用密钥分隔原则

根据PBOC标准，为了解决独立地管理一张卡上的不同应用的安全问题，每一个应用应该放在一个单独的文件中[18]。亦即在应用之间应该设计一道“防火

墙”以防止跨过应用进行非法访问。另外，每一个应用也不应该与卡中共存的个人化要求和应用规则发生冲突。

密钥可以保存在文件内，也可以是一个独立数据元。密钥不能从外部被引用。对保存在文件内的密钥，应用管理数据维护了在执行应用管理数据定义的命令和加密算法时定位密钥所必须的文件标识和指向密钥的引用。PIN 或者口令可以保存在文件内，也可以是一个独立数据元。PIN 和口令只能从外部通过应用管理数据和安全通信共同定义的命令被引用。

根据这个原则，我们为不同的应用定义了不同的密钥，严格实现应用分隔。表 3-1 中列出用户卡电子存折、电子钱包的各类应用密钥。从表中我们可以看到，每项功能在卡片中都有对应的密钥。在设计时。不但在卡片每个分区对应的各类密钥不同，在分区中对应的各功能的密钥也是不同的。

表 3-1 电子存折和电子钱包应用密钥

密钥	发卡方	用户卡	应用
用于消费/取现交易的密钥	消费主密钥(MPK)	消费子密钥（DPK），由 MPK 用应用序列号推导获得。	存折 钱包
用于圈存交易的密钥	圈存主密钥（MLK）	圈存子密钥（DLK），由 MLK 用应用序列号推导获得。	存折 钱包
消费/取现交易中用于产生 TAC 的密钥	TAC 主密钥（MTK）	TAC 子密钥（DTK），由 MTK 用应用序列号推导获得。	存折 钱包
用于解锁 PIN 的密钥	PIN 解锁主密钥（MPUK）	PIN 解锁子密钥（DPUK），由 MPUK 用应用序列号推导获得。	存折 钱包
用于重装 PIN 的密钥	PIN 重装主密钥（MRPK）	PIN 重装子密钥（DRPK），由 MRPK 用应用序列号推导获得。	存折 钱包
用于应用维护功能的密钥	应用主控密钥（MAMK）	应用主控子密钥（DAMK），由 MAMK 用应用序列号推导获得。	存折 钱包
用于圈提交易的密钥	圈提主密钥(MULK)	圈提子密钥(DULK)，由 MULK 用应用序列号推导获得。	存折
用于修改透支限额交易的密钥	修改主密钥(MUK)	子修改（透支限额）密钥（DUK），由 MUK 用应用序列号推导获得。	存折

智能卡系统的安全是建立在完备的密钥管理之上，对各类密钥管理无疑加大了系统的管理成本。从密码学角度来看，密码的强度是根据保护的信息价值的、以及普及范围的来确定。对于仅限于天津农行范围内使用，这种规模采取的密钥

设计是足够的。密钥本身也是具有生命周期的，包含生成、回收、销毁等过程。在密钥子系统中，对密钥的生命周期管理是十分重要的。

3.4 加密算法的选择

目前智能卡中常用的数据加密算法是 DES 算法，DES 算法全称为 Data Encryption Standard，即数据加密算法，它是 IBM 公司于 1975 年研究成功并公开发表的。DES 算法的入口参数有三个：Key、Data、Mode。其中 Key 为 8 个字节共 64 位，是 DES 算法的工作密钥；Data 也为 8 个字节 64 位,是要被加密或被解密的数据；Mode 为 DES 的工作方式，有两种：加密或解密。这种算法的运算复杂度相对而言也较小，比较适用于智能卡这样运算能力不是很强的情况。

COS把数据加密时要用到的密码组织在一起，以文件形式储存起来，称为密码文件。最简单的密码文件就是长度为 8 个字节的记录的集合，其中的每个记录对应着一个DES密码；较为复杂的密码文件记录中则可能还包含着该记录所对应的密码的各种属性和为了保证每个记录完整性而附加的校验和信息[19][20]。

DES ECB（电子密本方式）算法比较简单，基本原理是将数据按 8 个字节一段进行 DES 加密或解密得到一段 8 个字节的密文或者明文，最后一段不足 8 个字节，按照需求补足 8 个字节（通常补 00 或者 FF，根据实际要求不同）进行计算，之后按照顺序将计算所得的数据连结在一起即可。

一般 DES 加密算法，使用的密钥长度为 64 位。根据有关规范和行业经验，为进一步提高系统安全强度，系统采用的是三重 DES 算法，采用的密码长度为 128 位。

3DES 算法是指使用双长度（16 字节）密钥 K=（KL||KR）将 8 字节明文数据块进行 3 次 DES 加密/解密。如下所示：

$Y = DES(KL)[DES^{-1}(KR)[DES(KL[X])]]$

解密方式为：

$X = DES^{-1}(KL)[DES(KR)[DES^{-1}(KL[Y])]]$

其中，DES(KL[X])表示用密钥 K（左半部分）对数据 X 进行 DES 加密，DES^{-1}(KL[Y])表示用密钥 K（左半部分）对数据 Y 进行解密。

3.4.1 子密钥推导

在人行规范中描述了一种利用一个 16 字节的发卡行主密钥 IMK 分散得出用于密文生成、发卡行认证和安全报文的 IC 卡子密钥的方法。这一方式以应用主账号（PAN）和应用主账号序列号来组成一个 8 字节（16 个数字）长的输入数

据，以及 16 字节的发卡行主密钥 IMK 作为输入，生成 16 字节的 IC 卡子密钥 MK 作为输出。

图 3-3 描述了 DPK（消费/取现密钥）的推导过程。

1.DPK 左半部的推导

将应用序列号的最右 16 位数字作为输入数据，将 MPK（消费主密钥）作为加密密钥，用 MPK 对输入数据进行 3DES 运算。

2. DPK 右半部的推导

将应用序列号的最右 16 位数字求反作为输入数据，将 MPK 作为加密密钥，用 MPK 对输入数据进行 3DES 运算。

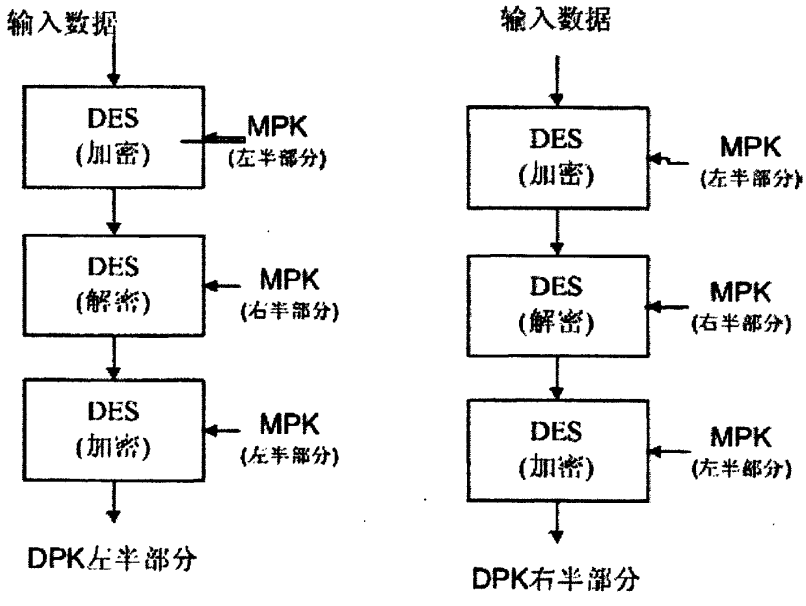

图 3-3 推导 DPK 示意图

上述的方法同样适用于电子存折的消费/取现、圈存和圈提、修改等子密钥的推导，及电子钱包的消费和圈存子密钥的推导。

3.4.2 过程密钥推导

过程密钥是在交易过程中用可变数据产生的单倍长密钥，产生的过程类似于图 3-3 中 DPK 的左半部分。过程密钥产生后只能在某过程/交易中使用一次。电子钱包进行消费交易时产生过程密钥的机制也用于不同交易类型的过程密钥的产生，但输入的数据取决于不同的交易类型。各交易的具体输入数据可参考人行应用规范中的约定。

在进行脱机消费时，在 PSAM 卡内部，对 GMPK 进行与用户卡中 DPK 相同的三级分散，得到于用户卡相同的 DPK，该 DPK 再依据当时的交易数据产生过程密钥，进行相互的验证和交易。在第五章交易流程的说明中给出了部分过程密钥推导的实例。

3.4.3 MAC 的产生

根据 PBOC 规范，信息安全认证码（MAC）的产生使用以下单倍长 DEA 算法，如图 3-4 所示。

1、将一个 8 个字节长的初始值（Initial Vector）设定为 16 进制的‘0x 00 00 00 00 00 00 00 00’。

2、将所有的输入数据按指定顺序连接成一个数据块。

3、将连接成的数据块分割为 8 字节长的数据块组，标识为 D1, D2, D3, D4 等等。分割到最后，余下的字节组成一个长度小于等于 8 字节的最后一块数据块。

4、如果最后一个数据块长度为 8 字节，则在此数据块后附加一个 8 字节长的数据块，附加的数据块为：16 进制的‘0x 80 00 00 00 00 00 00 00’。如果最后一个数据块长度小于 8 字节，则该数据块的最后填补一个值为 16 进制 ‘0x80’ 的字节。如果填补之后的数据块长度等于 8 字节，则进行下一步。如果填补之后的数据块长度仍小于 8 字节，则在数据块后填补 16 进制‘0x00’的字节至数据块长度为 8 字节。

5、MAC 的产生是通过上述方法产生的数据块组，由过程密钥进行加密运算。TAC 的产生是通过上述方法产生的数据块组，由 DTK 密钥进行加密运算。

6、最终值的左 4 字节为 MAC。

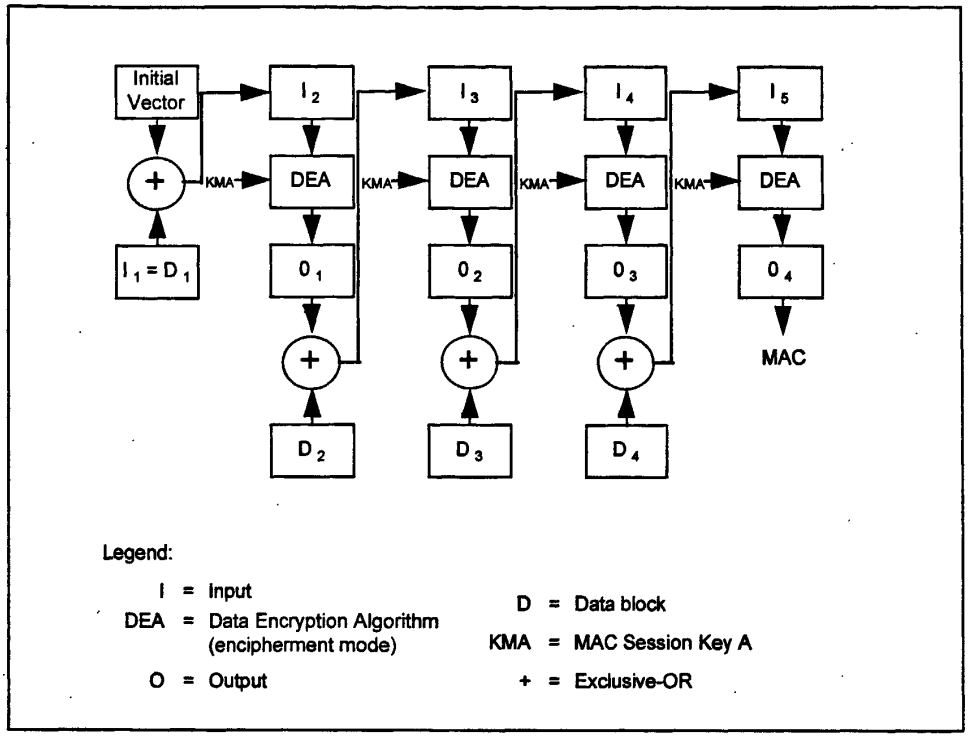

图3-4 MAC的单倍长DEA密钥算法

3.5 系统设计

3.5.1 目标及原则

在智能卡系统中，密钥的安全控制和管理直接关系到整个系统的安全机制，密钥子系统是整个系统的核心部分。与密钥相关的是加密算法，智能卡能够完成复杂的加密运算，真正体现其“智能”特性[21] [22]。

密钥管理子系统包括各类密钥的产生、继承、派生、传递和存放等几个方面，一般包括三个部分功能，即密钥生成、密钥下载和密钥传输。密钥统一管理是系统安全的重要保证，密钥管理的设计将遵循以下的原则：

✧通用性原则

充分分析现行 IC 卡应用的基础上，结合未来业务的发展，针对密钥管理系统的自身特点，最大限度地支持和满足各种应用需求。

✧安全性原则

在系统设计中，必须把安全作为首要考虑的因素；在开发过程中，对各个环节必须进行严格的安全控制。

✧扩展性原则

具有对系统方便的进行扩展、新增功能的能力，并能方便地支持新的应用。客户可以根据定制选择系统功能，方便组合。

✧灵活性原则

支持向用户卡发卡母卡中注入不同应用的密钥，如接收总行下发的母卡密钥或其他行业应用母卡密钥。

3.5.2 系统硬件结构

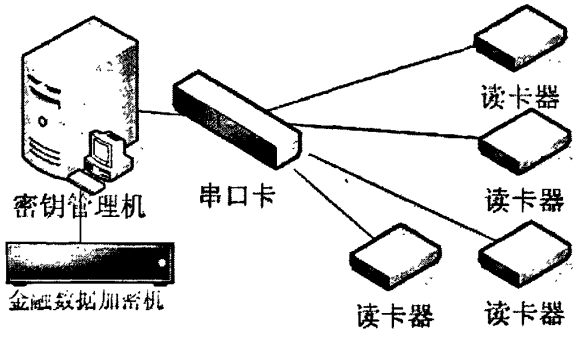

图 3-5 密钥子系统硬件结构图

图 3-5 给出了密钥系统最基本的硬件组成。系统主要由管理主机、金融数据加密机，多串口卡和 IC 卡读写卡器构成。其中金融数据加密机，是用于密钥管理的硬件加密设备，在硬件上具有一定的防物理攻击能力，在软件上对密钥的生成、存放、备份和运算进行权限控制。由于金融数据加密机具备了攻击防范能力，所以密钥可以在金融数据加密机中安全地保存，而且所有密钥运算可在安全的物理环境中完成。

3.5.3 密钥系统接轨

1、与上级行接轨

由于农行天津分行业务发展的需要，整个系统特别是密钥管理子系统不可能等待总行二级密钥中心建成以后在进行开发，所以需要做好全面的规划工作，在系统设计方面和业务规划方面充分考虑兼容和接轨的问题。

分行密钥系统与总行二级密钥中心的接轨可以分为三个阶段：

（1）分行系统建成阶段

首先采用分行密钥管理系统的一级中心部分生成自己的种子密钥直接下发到三级中心部分，经过分散之后，用于分行标准的金融应用和其他专用应用。专用应用在分行的网点和设备上使用，以后也不考虑在他行 POS 机上使用。

（2）总行密钥中心建成阶段

总行二级密钥中心完成以后，分行会从总行得到发卡母卡，即总行下发给分行的消费主密钥。此阶段分行发行的卡片装入由总行下发密钥分散的密钥，其他密钥还沿用原有密钥。通过总行 PSAM 卡的二次发卡加入分行特色业务的专用密钥，则分行特色应用可以在本行的 POS 机上使用。

（3）全面和总行接轨阶段

全面接轨阶段，要求分行各个阶段发行的用户卡都可以在全国各分行之间的机具上使用。这个阶段发行的新卡的做法和第二阶段完全相同。对于第一阶段发出的卡，将其中金融应用的消费密钥全部更新成总行下发密钥的分散后的密钥。同时当分行机具上的 SAM 卡全部换成有总行密钥的 SAM 卡，机具的接轨也就完成了。

2、与行业用户密钥系统接轨

为了保证智能卡的通用和机具共享能够顺利实现，往往需要在应用单位针对某种应用建立专门而独立的 IC 卡密钥管理系统，统一管理某种应用所需的根密钥。与应用单位的密钥管理系统进行对接，一方面要求能够接受应用方的密钥，另一方面要能够向应用方传递密钥。

在应用方与行内密钥管理系统之间进行密钥传递的渠道主要式密钥母卡及其认证卡。密钥管理系统要能对得到的应用方密钥进行分散导出，并导入到密钥母卡或发卡母卡中。

与行业用户密钥系统接轨同时带来发卡系统的发卡模式问题，在下一章中对于发卡模式有专门的叙述。密钥系统的设计要具备充分的灵活性，以达到应对上述的“接轨”问题。

第四章 卡片管理设计

发卡管理系统也称为卡片个人化管理系统，它将进行 IC 卡个人化的密钥、加密设备、应用项目的数据格式和加密信息等集中进行管理，为分布于不同地点的 IC 卡个人化设备提供个人化加密信息服务。如果考虑卡片的领用、作废等管理，也可以称之为卡片生命周期管理。

4.1 用户卡片结构设计

按 ISO/IEC 7816 标准，智能卡的数据结构有线性固定结构（Linear Fixed）、线性可变结构（Linear Variable）、环形结构（Cyclic）、透明结构（Transparent）四种。本系统的用户卡使用的是固定结构，即采用定长度记录，其中每一记录的存储位置均由一个唯一的记录号标识，可以随机读写。

金融区的设计应参照《中国金融集成电路（IC）卡规范》中关于卡片的要求；非金融区的设计一般要符合建设部关于城市建设一卡通系统中对于用户卡的要求。非金融应用要在卡片上建立多个应用区，应用区的数量只受卡片容量的限制。如果在以后系统增加其他的应用，在保证安全的情况下，可以启用预留的应用区。

卡片分区如下所示：

公共信息区：存储发卡机构和持卡人的基本信息。

银行金融区：依照金融标准建立的应用目录，文件结构和交易流程完全符合《中国金融集成电路（IC）卡规范》中的定义，密钥由发卡银行产生并写入。

包括：电子存折文件、电子钱包文件

（1）电子存折对应银行内的一个帐户，用于大额消费，消费和圈存时需要输入 PIN（个人口令），可以挂失，计算利息；

（2）电子钱包用于小额消费，里面只可以存储少量的金额，消费时不需要提交个人口令，不能挂失，不计算利息。

（3）除特殊应用之外的其他所有与金额有关的消费操作都发生在银行应用目录下，根据行业的实际情况选择从电子存折或电子钱包中扣款。

非金融应用区：根据合作方不同的需求设计。

预留的非金融应用分区数量根据卡片容量的不同决定。一般的消费卡，可不具备非金融区，用容量为 1K 的卡就可以满足。图 4-1 给出了一个利用捷德 8K 容量卡片设计的含有非金融应用的卡片结构设计。

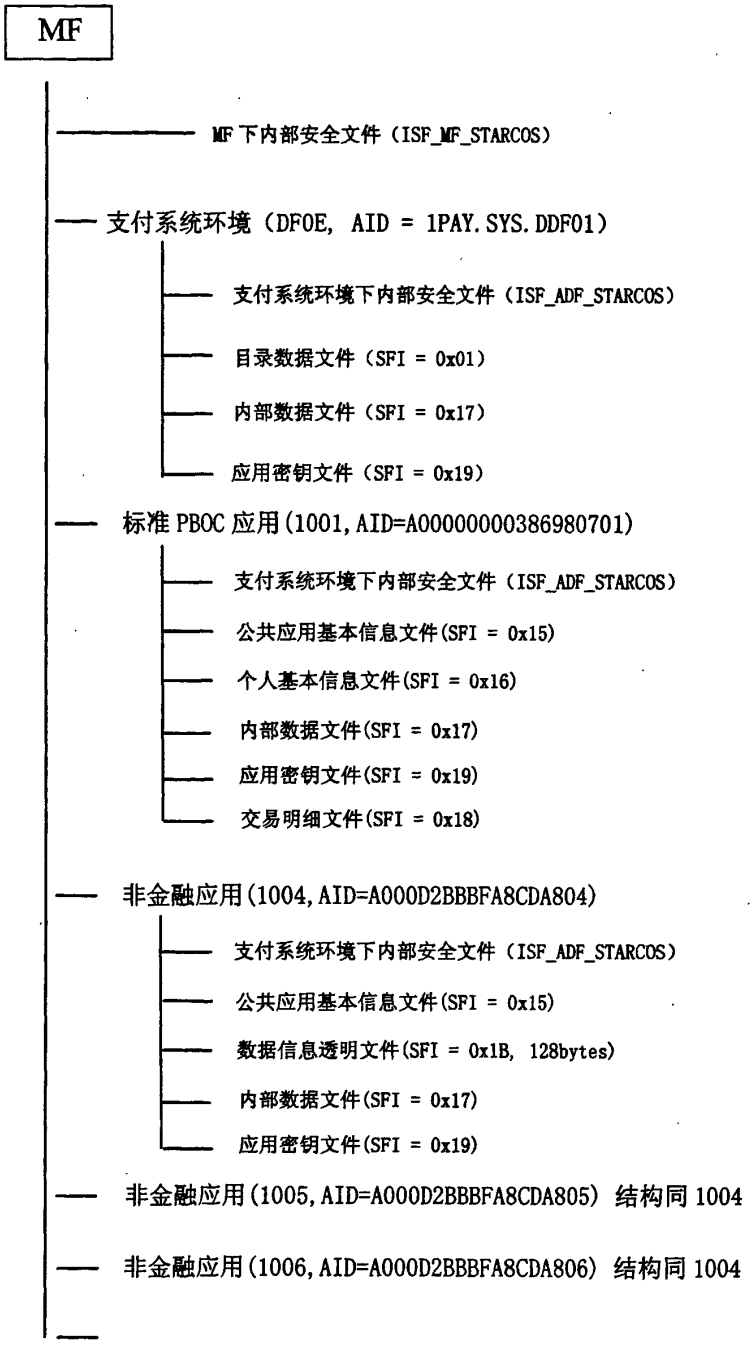

图 4-1　含有非金融应用的卡片结构设计

4.2 发卡系统设计

发卡系统负责IC卡的初始化、个人化，完成银行从厂商处购置IC卡片后，应用发卡母卡及其控制卡以及主控传输卡通过制卡设备（打卡机），将发卡母卡产生的密钥安全的写入IC卡，并在持卡人申请后，根据客户信息初始化，并在IC卡芯片中写入持卡人金融应用基本信息和有关的非金融应用所必需的资料。

4.2.1 硬件结构

图4-2给出了发卡系统的硬件构成，以及简单发卡流程。管理主机将发卡资料数据传给发卡主机，在发卡母卡、母卡控制卡和主控传输卡的控制之下，发卡主机将数据传给打卡机，将白卡制成用户卡。

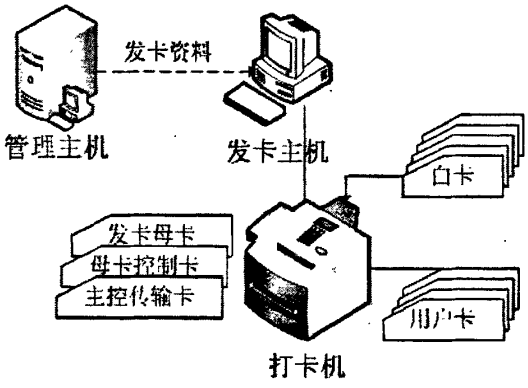

图4-2 发卡系统硬件结构

4.2.2 发卡模式

根据对应用情况的分析，我们设计了两种发卡模式，即批量发卡模式和实时发卡模式：

1、批量发卡模式

由发卡中心根据有关部门提供的持卡人相关资料，同时可能还有持卡人的其它中介应用的资料（参保信息、医疗信息、驾驶员管理信息等），进行客户信息批量初始化，在数据处理中心数据库建立客户信息、开户并建立帐户信息、生成发卡文件，写入IC卡芯片中。再进行卡片个人化以及卡面个人信息印刷、写磁、打凸字。客户到网点领卡时做卡启用。

2、实时发卡模式

由发卡中心统一对 IC 卡芯片进行金融应用预初始化，将发卡母卡的相关主密钥分散并安全导入到用户卡中、写入公共应用集体数据信息、在卡表面印刷卡号及有效期等，负责 IC 卡的芯片个人化、写磁条、印刷或打凸字，个人密码均为通码（缺省密码）。由各发卡网点领回后，当客户申请办理智能卡时，在柜台上即时写入持卡人的户名和证件号码，开立主帐户、电子存折户、电子钱包户并由持卡人设置个人密码，交易成功即可将卡片交给客户。除基本定制外，增添其他应用由持卡人提出申请。

4.2.3 功能设计

1. 空白卡管理

发卡行从上级分行调入空白 IC 卡或从供货商处购进空白 IC 卡片时，要将空白 IC 卡登记入库；发卡时领用空白 IC 卡时要有 IC 卡出库登记；同时完成任何时候 IC 卡出入库情况的统计、查询等功能。

2. 制卡管理

➢洗卡

由于用于制卡的空白IC卡片上都有厂商设置的用于控制IC卡安全传输的传输密钥，因此制卡中心在使用这些卡片前要进行洗卡[23]，即先用厂商提供的生产商母卡对卡片进行认证，以确认卡片的合法性和可用性，认证成功后用银行或应用行业产生的洗卡密钥替代卡片中的厂商密钥。

➢制卡

制卡是指通过发卡母卡完成持卡人密钥的分散、载入以及将卡片的个人信息写入卡片的过程。包括批量发卡、单张发卡（应用与补卡操作）、批量预发卡、代理发卡、增加新应用等功能。

➢坏卡、废卡的处理

洗卡、制卡过程中发生的坏卡、废卡通过清点，登记入库并记录原因，按不同情况做相应的处理。

➢成品卡管理

成品卡是已经经过制卡的 IC 卡，卡中已注入实际应用的密钥及个人信息，基本上就是可以流通的卡，必须严格管理。要进行严格的调入、调出登记。要有一定的领用凭证记录入库。

3. 操作员管理

完成系统中操作员的管理工作，包括操作员信息管理、操作员登录管理等。

4. 日志管理

完成日志的备份、打印等工作。日志记录制卡信息、制卡过程中的异常信息等关键性的信息。

5. 系统配置管理子系统

完成对配置文件的增加、修改、发布工作。

4.2.4　管理界面示例

图 4-3 入库管理交互界面

图 4-3 显示的是卡片入库管理的界面设计。在这个界面中可以输入不同的卡片种类，选择生产厂家，输入数量和起止序号。数据输入之后还要和数据库中已有数据进行核对，避免序号重复。

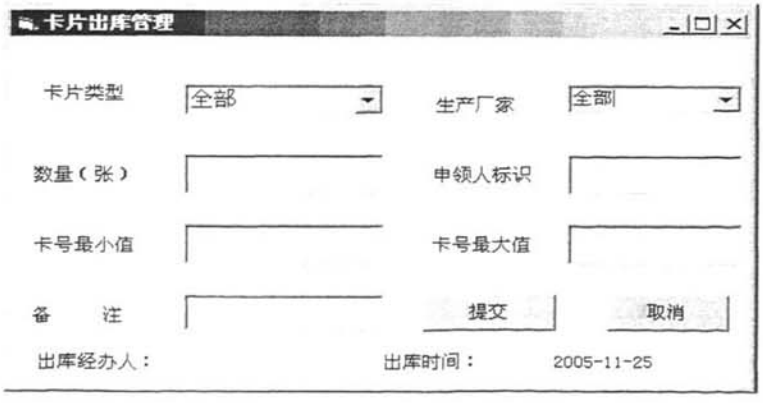

图 4-4 出库管理交互界面

图 4-4 是卡片出库管理的界面，要选择卡片类类型和生产厂家，此外要输入数量、起止序号和申领人的信息。

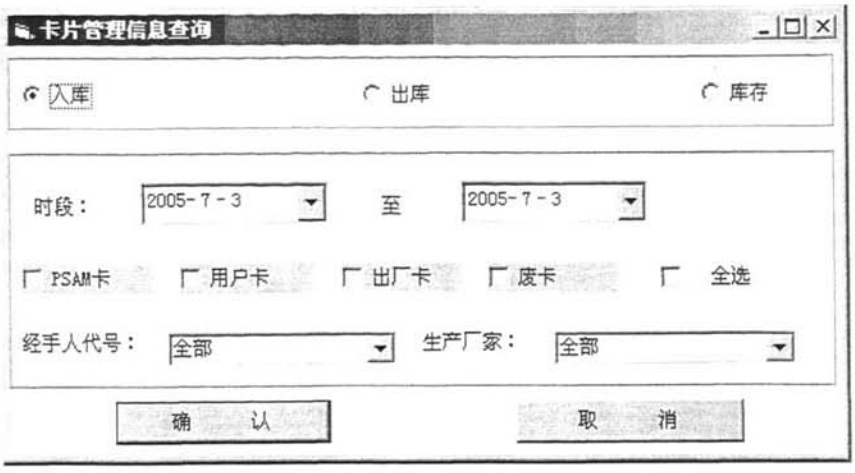

图 4-5 出入库及库存查询交互界面

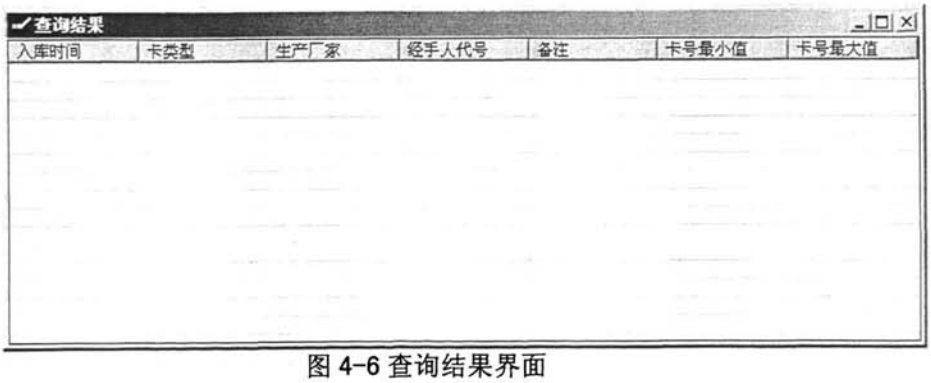

图 4-6 查询结果界面

图 4-5 和图 4-6 给出的是卡片出入库管理的查询条件输入界面和查询结果显示界面。

4.2.5　批量个人化

受 IC 卡自身技术的制约，发卡速度环节是 IC 卡应用的一个瓶颈，因为大量的数据出于安全需要或其它制约因素，只能在发卡机构中完成写入 IC 卡的芯片中的工作，而非在 IC 卡的制造厂家进行，这就要求发卡机构要配备相应的发卡设备以及发卡软件。一般的小型发卡设备只配有一个 IC 卡个人化的编程站，只

能处理单张卡片。以一张符合中国人民银行 PBOC 标准的 4K 的 CPU 卡为例，其完成全部数据写入，即个人化所需的时间为 80—90 秒。

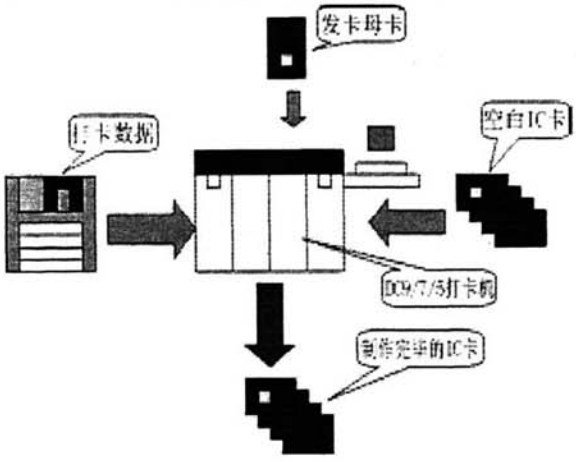

图 4-7 打卡机使用示意图

在天津农行的智能卡发卡系统中，采用的方案是在打卡机 DC7000 中安装一个 IC 卡模块（Smart Card Module）。如图 4-7 所示。IC 卡模块由控制平台、编程站（Program Station）和保安站（Key Reader）组成。一个 IC 卡模块配置了 7 个编程站，可同时对 7 张 IC 卡进行个人化处理，而且系统完成 IC 卡个人化后，还可进行卡磁条数据录入、卡面信息印刷等个人化处理，发卡过程一次性完成，无需人工干预，大大提高了发卡效率。

4.3 应用在线扩展

应用扩展是设计中的关键之一，通过对卡片安全机制的分析，我们提出应用在线扩展的方案，可以通过安全的处理流程，在银行的网点完成新的非金融应用的开启。

我们知道，PIN（Personal Identification Number）是 IC 卡中的保密数据。PIN 的主要用途是保证只有合法持卡人才能使用该卡或该卡中的某一项或几项功能，以防止拾到该卡的人恶意使用或非法伪造。多功能卡中的每一功能就可具有一个 PIN，每一个 PIN 一般还配有一错误计数器（Error Counter）。该计数器用以记录、限制 PIN 输入错误的次数，若一次连续的输入错误次数超过卡中规定次数则卡自锁，一旦卡自锁，简单的 IC 卡就不可再用，而复杂的智能 IC 卡还可通过个人解锁码（Personal Unblocking Code,PUC）将卡打开。根据国内的标准，一般把 PIN 也成为各种的“key”。

卡片在设计时已经为多个应用预留了空间，可以根据需要开启使用。主要做法是再初始化时预留多个大小不同的分区，每个分区用临时密钥保护起来。由于目前IC卡卡片不支持动态格式化（JAVA卡除外）[22]，所以在预留分区时一定要根据今后的发展做好仔细的计算，使得预留的空间不至于过小而不支持一些大型的行业应用，同时也不能过大而浪费空间。

当银行和某一行业谈好合作以后，可以根据其需要选择使用卡中预留的分区，替换成真正的应用密钥。当用户申请金融智能卡的时候，面对已有的多种行业应用，可以选择开通其中的一部分，而其他应用等到需要时再开通。

本节主要解决金融智能卡的在线应用扩展问题，不必耗费大量的人力物力进行回收重发工作。所谓在线应用扩展，就是通过网络从数据中心或密钥子系统的加密机中获得应用密钥，来替换批量初始化时预留分区里的临时密钥，这样就使新的应用“取得”了应用分区的控制权。根据需要，也可以更新卡片的主控密钥和维护密钥[23]。

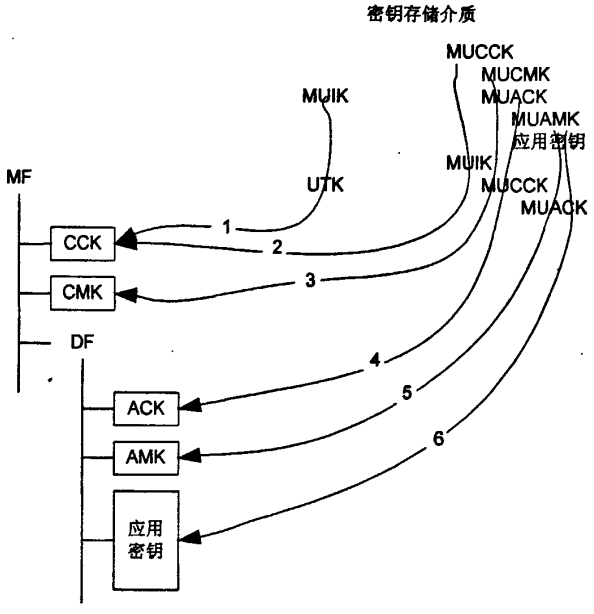

图 4-7 密钥装载流程图

如图 4-7 所示，在密钥存储介质（密钥卡或加密机）中存放着新旧密钥两套，在更新时，只需要执行图中的④—⑥步，通过旧密钥获得卡片控制权，然后分别写入不同的密钥。其中 CCK 是卡片主控密钥，CMK 是卡片维护密钥，ACK 是应用主控密钥，AMK 是应用维护密钥。

在IC卡密钥保护机制中，ACK的写入是受CCK保护的，应用密钥的写入又受ACK控制，应用密钥进而控制该应用下的操作。不同的应用有不同的ACK，从而实现不同应用之间的“防火墙”隔离。而在卡片发卡后，应用密钥的更新是受应用主控密钥保护更新的，而应用主控密钥在发卡后是由自身保护更新的。这就保证了只有拥有IC卡的应用主控密钥的机构才有权力对IC卡中的相关应用进行密钥更新。IC 卡密钥的更新采用了每次约定随机数及通过应用主控密钥加密保护更新的技术，保证了密钥在更新过程中的安全性。

在柜面系统中，将写卡流程分为了若干步骤，如果在交易时发生通讯失败等情况导致写卡中断时，系统将自动记录失败的步骤，待通讯恢复时，可继续由上次失败的步骤开始完成写卡。

4.4 卡片的回收利用

对于一般只有电子钱包而没有电子存折帐户的消费卡，客户在使用过一次之后就会丢弃，很少继续充值重复使用。而银行发卡一般都是免收卡片费用的，这样会带来巨大的浪费和发卡成本压力。能否将旧卡片回收再利用，就成为节省发卡成本的关键问题[24]。经过研究，我们找到了可行的方法：

1、通过超市收银员将顾客不再使用的消费卡收回，并给予客户和收银员以一定的补偿和奖励；

2、将收回的旧卡做一定的分拣处理，主要是消毒和丢掉污染严重的卡片，挑选出比较新的卡片并整理好；

3、将整理好的旧卡放入打卡机的进卡槽，批量读取卡中的有关信息，如卡号、余额（有时会由几分钱的剩余）等，形成回收信息文件；

4、根据回收信息文件中的数据，在卡片管理系统中做凭证状态的重置，在帐务系统中做好卡片钱包帐户余额的回收，并更新回收信息文件为发卡文件；

5、然后利用4中形成的回收卡发卡文件，批量格式化回收卡，并根据文件中的发卡信息重制卡片。

经过上述操作，回收的卡片就可以再次作为新卡使用。而对于不能使用的废卡，要做废卡处理。对于没有回收来的卡片，在系统经过一段时间之后，卡片仍没有使用或者重新充值，则作为睡眠卡处理，从系统中转储相关信息出来，这样可以大量节省系统资源[25]。

第五章 交易实现

本章说明了系统对电子存折/电子钱包应用的几个比较重要的交易是如何实现的，特别是卡片和终端之间如何校验 MAC，机具将脱机交易批量送到帐务后台之后，主机如何校验 TAC 来完成帐务处理。

5.1 交易预处理

图5-1给出了对电子存折/电子钱包应用的所有交易类型共有的预处理流程，此流程对柜台和自助机具都适用。

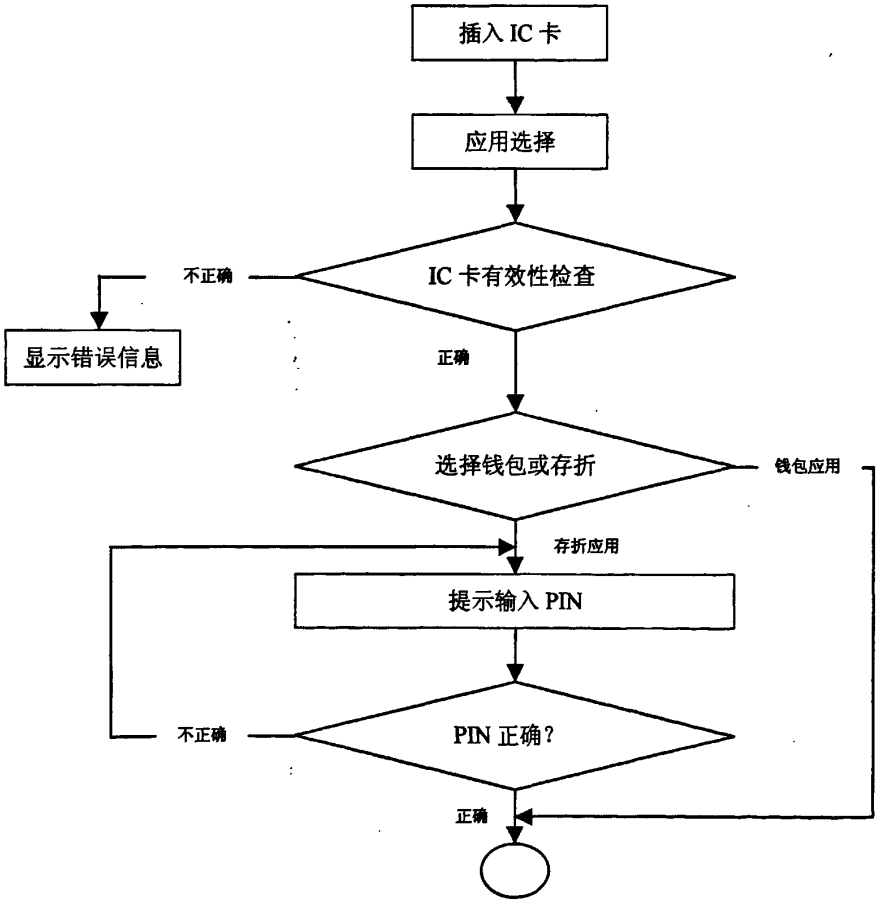

图5-1 交易预处理流程

1、插入 IC 卡：根据 PBOC 标准，终端应具有检测 IC 卡是否已经插入读卡器的功能。读卡器检测 IC 卡是否已经插入。如果 IC 卡已经插入，将继续执行应用选择功能。否则在屏幕上提示用户插入 IC 卡。

2、应用选择：读卡器要求 IC 卡选择卡中的目录文件，然后读取该文件的记录并与柜台终端选择的应用标识进行比较，直至找到一致的记录为止，该记录中的应用标识所代表的应用即为我们选择的应用。如果遍历所有记录仍然找不到相同应用标识的记录，则表明卡片中没有该应用，显示出错信息并将出错代码回传给柜台终端，交易结束。应用类型标识 (ATI) 在应用选择时由 IC 卡回送给终端。 它标明电子存折和电子钱包应用在卡上的存在情况。

3、IC 卡有效性检查：对于回送的数据，终端将下检查该卡是否在终端存储的黑名单卡之列，终端是否支持该发卡方标识符，终端是否支持 IC 卡上的应用，应用是否在有效期内。如果以上任一条件不满足，显示出错信息并将出错代码返回给柜台终端，交易结束。

4、选择电子存折或电子钱包：终端根据应用选择时获得的应用类型标识判别 IC 卡支持 ED、EP 的情况。如果 IC 卡和终端只同时支持 ED 或 EP 之一，则终端将自动地选择到 ED 或 EP，继而进行下面的步骤；如果 IC 卡仅支持一种应用并且该应用不被终端支持，则该过程终止；如果 IC 卡和终端彼此都支持 ED 和 EP 两种应用，终端应向持卡人提供选择 ED 或 EP 的过程，在这一过程中持卡人可以从中选择一种应用进行交易。

5、提示输入个人密码：如果选择了电子存折，终端将提示持卡人输入 PIN。

6、校验 PIN：持卡人输入 PIN 后，终端将使用 VERIFY 命令来校验持卡人输入的 PIN 是否正确。当 IC 卡收到校验（VERIFY）命令后，它将检查 PIN 尝试计数器。如果 PIN 尝试计数器为零，此时 PIN 已锁定，因此不执行该命令。这种情况下，IC 卡回送状态码‘6983’（认证方式锁定）结束交易过程。

➢如果PIN没有被锁定，则将命令数据中的PIN和IC卡中存放的PIN进行比较。

➢如果以上两个PIN相同，IC卡将PIN尝试计数器置为允许PIN重试的最大次数并回送状态码‘9000’。IC卡必须记住PIN成功验证的结果，直到断电或选择了其他应用。。

➢如果以上两个PIN不同，IC卡将PIN尝试计数器减1并回送状态码‘63Cx’，这里’x’是PIN尝试计数器的新值。在这种情况下，终端将检查x的值。如果x是零，将终止交易，且卡片自动锁定PIN。否则，终端将提示重新输入PIN并重复以上过程。

➢如果持卡人输入的PIN正确，IC卡必须记住PIN成功验证的结果，直到断电、

卡片复位、PIN再次验证错误或选择了其他应用。验证正确后，交易流程执行下面的步骤。

5.2 圈存交易

下面给出的是在圈存机上如何实现圈存交易，即客户如何利用圈存机将主帐户的资金存入电子存折或电子钱包帐户。

5.2.1 交易流程

图5-2给出了电子存折/电子钱包应用的圈存交易处理流程。通过圈存交易，持卡人可将其在银行相应帐户上的资金划入电子存折或电子钱包中。这种交易必须在金融终端上联机进行并要求提交个人密码（PIN）。

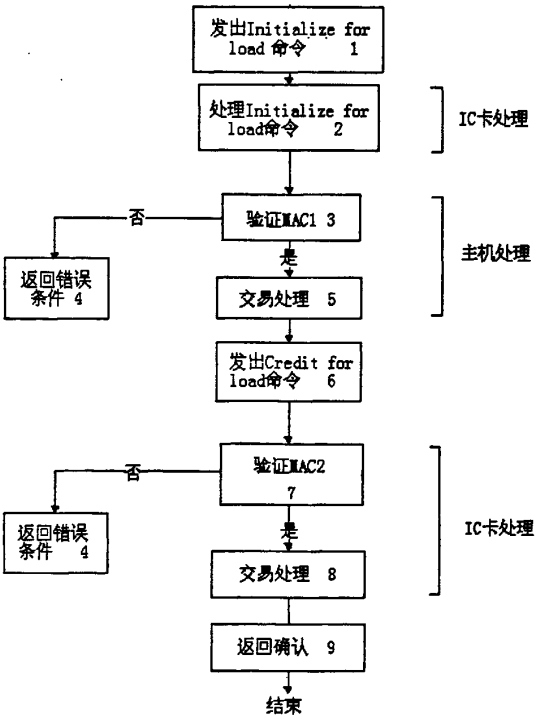

图5-2 圈存交易处理流程

1.发出初始化命令：终端发出INITIALIZE FOR LOAD命令启动圈存交易。

圈存初始化指令码 密钥索引号 交易金额 终端编号

2.处理初始化命令：收到INITIALIZE FOR LOAD命令后，IC卡将进行下列操作。

➢检查是否支持命令中包含的密钥索引号。如果不支持，则回送“不支持的密钥索引”的状态码‘9403’，但不回送任何其他数据，同时终止命令的处理过程。

➢产生一个伪随机数（ICC），过程密钥SESLK和一个报文签别码（MAC1），用以供主机验证圈存交易及IC卡的合法性。SESLK是用于电子存折或电子钱包圈存交易的过程密钥。用来产生过程密钥SESLK的输入数据如下：

SESLK：伪随机数（ICC）||电子存折或电子钱包联机交易序号||‘8000’

MAC1的计算见第三章3.4.3节。用SESLK对以下数据加密产生MAC1:

•电子存折余额（交易前）或者电子钱包余额（交易前）

•交易金额

•交易类型标识

•终端机编号

IC卡将把INITIALIZE FOR LOAD响应报文回送给终端处理。如果IC卡回送的状态码不是‘9000’，则交易终止。

3.验证 MAC1：收到INITIALIZE FOR LOAD命令响应报文后，终端把数据传给发卡方主机。主机将生成SESLK并确认MAC1是否有效。如果MAC1有效，交易处理将按5中描述的步骤继续执行。否则，交易处理将执行4中所描述的步骤。

4.回送错误状态：如果不接受圈存交易，则主机应通知终端。

5.交易处理：在确认能够进行圈存交易后，主机从持卡人在银行的相应帐户中扣减圈存金额。主机产生一个报文签别码(MAC2)，用于IC卡对主机进行合法性检查。用SESLK对以下数据加密产生MAC2:

•交易金额

•交易类型标识

•终端机编号

•交易日期(主机)

•交易时间(主机)

成功地进行了圈存交易后，主机将电子存折联机交易序号或电子钱包联机交易序号加1，并向终端发送一个圈存交易接受报文，其中包括MAC2、交易日期（主机）和交易时间（主机）。

6.发出CREDIT FOR LOAD命令：终端收到主机发来的圈存交易接受报文后，发出CREDIT FOR LOAD命令更新卡上电子存折或电子钱包余额。

7.验证MAC2：收到CREDIT FOR LOAD命令后，IC卡必须确认MAC2的有效性。如果MAC2有效,交易处理将执行8中描述的步骤。否则将向终端回送状态码'9302'（MAC无效）。

8.交易处理：IC卡将电子存折联机交易序号或电子钱包联机交易序号加1，并且把交易金额加在电子存折或电子钱包的余额上。IC卡必须成功地完成以上所有操作或者一个也不完成。在电子存折圈存交易或电子钱包圈存交易中，IC卡用以下数据组成的一个记录更新交易明细：

- 电子存折联机交易序号或电子钱包联机交易序号
- 交易金额
- 交易类型标识
- 终端机编号
- 交易日期(主机)
- 交易时间(主机)

TAC的计算不采用过程密钥方式，它用DTK左右8位字节异或运算的结果对以下数据进行加密运算来产生:

- 电子存折余额（交易后）或电子钱包余额（交易后）
- 电子存折联机交易序号（加1前）或电子钱包联机交易序号（加1前）
- 交易金额
- 交易类型标识
- 终端机编号
- 交易日期（主机）
- 交易时间（主机）

9.返回确认：在成功完成步骤8后，IC卡通过CREDIT FOR LOAD命令的响应报文将TAC回送给终端。主机可以不用马上验证TAC。

5.2.2 圈存机界面设计

下面几个图分别给出了圈存机主界面、圈存菜单界面、存折圈存主界面和交易成功界面。

1. 主界面

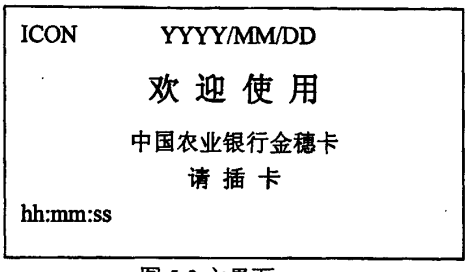

图 5-3 主界面

2. 圈存菜单界面

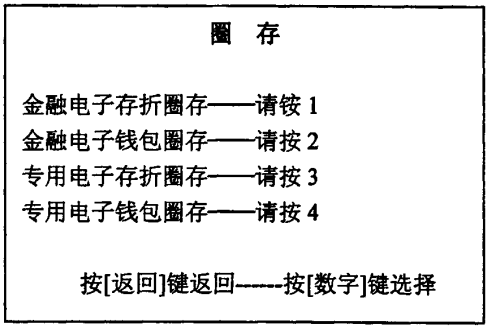

图 5-4 圈存菜单界面

3. 存折圈存界面

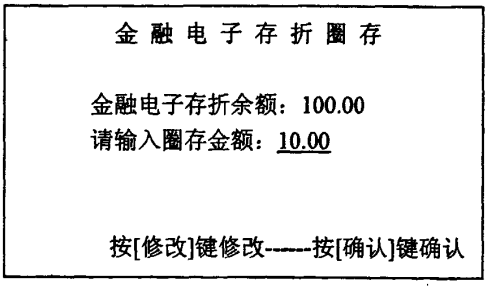

图 5-5 存折圈存界面

4. 交易成功界面

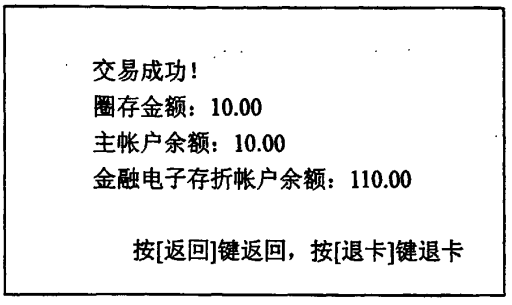

图 5-6 圈存成功界面

5.2.3 程序伪码

```
Load(char  ucPurseType)
// In  : ucPurseType : 0 : ED load
//                     1 : EP load
{
if(电子存折圈存)
显示界面 <  电 子 存 折  圈 存 交 易  >;
else
显示界面 <  电 子 钱 包  圈 存 交 易  >;
选择金融应用;
if(失败)
return;
if(电子存折圈存且无ED应用) {
显示界面<无电子存折应用>;
return;
}
if(电子钱包圈存且无EP应用) {
显示界面<无电子钱包应用>;
return;
}
输入圈存金额;
if(取消)
return;
对用户卡片做圈存初始化;
if(失败) {
显示界面<圈存初始化错>;
return;
}
输入6位主帐号密码;
```

```
电话拨号;
if(失败)
return;
发送系统报文;
if(失败)
return;
累加交易序号;
保存交易序号;
填圈存请求8583报文;
发送请求并接收响应;
if(通讯失败或后台不同意) {
          if(! 密码错误) return ;
          输入6位主帐号密码;
          电话拨号;
          发送请求并接收响应;
         if(通讯失败或后台不同意) return ;
 if(密码错误) {
  显示界面<密码错>;
  return ;
        }
    }
做圈存操作;
if( 中途拔卡 ){
做中途拔卡处理;
把圈存的返回值改成正确;
}
if( 圈存错误 或 中途拔卡返回TAC错 ) {
显示界面<圈存失败,冲正>;
打冲正包;
发送待发送交易;
return;
}
填圈存提交TAC请求8583报文;
发送请求并接收响应;)
if(通讯失败)
置位待发送请求标志;
else {
检查8583返回码;
if(需要重发) {
置位待发送请求标志;
发送待发送交易;
}
}
挂机;
```

记录各要素;
显示界面〈圈存成功〉;
累加交易笔数;
保存系统数据;
}

5.3 圈提交易

以下给出在银行网点的柜台上如何实现圈提交易。通过圈提交易，持卡人可以把电子存折中的部分或全部资金划回到其在银行的相应帐户上。这种交易必须联机进行并要求提交个人密码（PIN）。只有电子存折应用支持圈提交易。

5.3.1 交易流程

图5-6出了对电子存折/电子钱包应用的圈提交易处理流程。

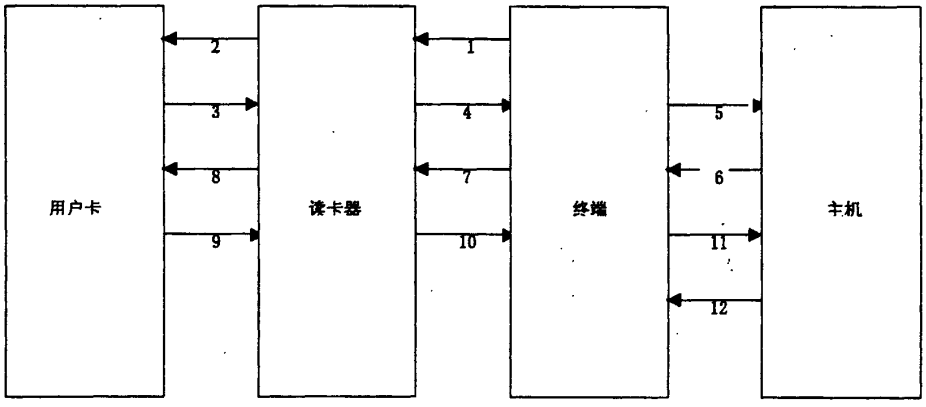

图5-6 柜台圈提交易处理流程

1.终端选择 IC 卡电子存折圈提交易菜单，输入圈提金额后，终端要求读写卡器对用户卡进行预处理并发圈提初始化指令。

圈提初始化指令码 交易步骤1 交易金额 密钥索引号 终端机编号

2.读写卡器收到终端数据后对用户卡进行预处理，预处理完成后得到卡片的应用序列号并向用户卡发 INITIALIZE FOR UNLOAD 命令启动圈提交易。

圈提初始化指令码 密钥索引号 交易金额 终端机编号

3.用户卡收到 INITIALIZE FOR UNLOAD 命令，检查是否支持得到的密钥索引号，如果不支持则返回错误，否则生成交易随机数并产生 MAC1（通过对应用序列号的发散及密钥版本号的值可以定位 IC 卡中使用的 DULK，再由伪随机

数和联机交易序号可以计算出过程密钥 SESULK，再用过程密钥对 ED 余额、交易金额、交易类型标识和终端编号用算法标识定义的算法进行加密，就可以得到 MAC1），读写卡器收到用户卡回送数据后传给终端：

●密钥版本号

●算法标识

●伪随机数

●ED 联机交易序号

●ED 余额

●MAC1

●应用序列号(卡号)

4. 终端接收读写卡器回送数据后构成主机交易数据上送给主机进行 MAC1 校验、黑名单检查及帐务处理。如果在规定的时间内没有收到读写卡器的回送数据，则作为超时处理,交易结束。

●行部号

●终端号

●应用序列号

●密钥版本号

●算法标识

●伪随机数

●ED 联机交易序号

●ED 余额

●交易金额

●交易类型标识

●MAC1

5. 主机接收到交易数据后，首先检查卡号是否在黑名单中，若是则发锁应用命令，否则检查帐户余额及 MAC1 验证，如余额不足或验证错误则回送错误信息，否则生成 MAC2（）回送。MAC2 由过程密钥 SESULK 对交易金额、交易类型标识、终端编号、交易日期、交易时间用算法标识(DLK)定义的算法进行加密产生。

6. 终端接收到主机回送数据后，同读写卡器进行串口通讯要求其让用户卡对主机下传的 MAC2 进行校验及圈提处理。终端向读写卡器发送的数据如下：

圈提确认指令码 交易步骤 2 交易日期 交易时间 MAC2

7. 读写卡器收到终端数据后，向用户卡发圈提确认命令及相应数据。如果在给定的时间内读写卡器没有收到终端的返回信息，则作为超时处理，交易失败。

圈提确认指令码 交易日期 交易时间 MAC2

8. 用户卡收到读写卡器的圈提确认命令后，先对 MAC2 进行校验，如不通过就发 错误信息，否则用户卡进行圈提处理、计算出 MAC3（MAC3 由过程密钥 SESULK 对 ED 交易后余额、ED 联机交易序号、交易金额、交易类型标识、终端机编号、交易日期、交易时间进行加密运算产生）并与相应的计算数据传送给读写卡器一用户卡。传送的数据如下：

●ED 交易后余额

●MAC3

9. 终端收到读写卡器传送的信息上传主机进行交易处理。如果终端不能将交易信息上送给主机，到一定次数后记异常交易流水供调帐处理。

10. 主机收到终端上送的数据后，对 MAC3 进行校验。如果正确则进行主机帐务处理并终端发确认信息，否则返回错误。终端收到主机返回信息后，如果交易成功则向读写卡器发成功信息提示用户拔卡，否则发送应用锁定命令。

11. 用户卡收到应用锁定命令后进行应用锁定处理并将处理结果返回给读写卡器一终端，终端将结果后在终端上显示。

5.3.2 接口设计

1. 用户接口

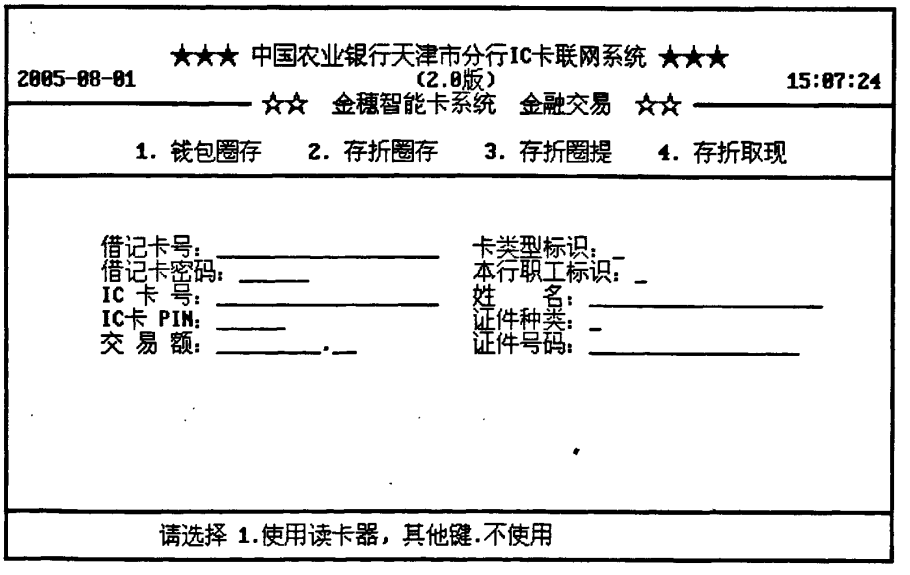

图 5-7 柜台终端圈提交易界面

2. 终端与智能读卡器通讯接口

(1). 发初始圈提指令（终端→读卡器）

INITIALIZE FOR UNLOAD

DATA

jy_amount	交易金额
jy_key_index	密钥索引号
term_id	终端编号
jy_date	交易日期
card_pin	IC 卡密码

(2). 读卡器回送 MAC1（读卡器→终端）

DATA

ed_balance	ED 旧余额
jy_counterED	联机交易序号
jy_key_version	密钥版本号
jy_algorithmic_flag	算法标识
random	伪随机数
mac	MAC1

(3). 发圈提确认指令（终端→读卡器）

DEBIT FOR UNLOAD

DATA

jy_date	前置机交易日期4byte	
jy_time	前置机交易时间3byte	
mac	MAC2	4byte

(4). 读卡器回送 MAC3（读卡器→终端）

DATA

ed_balance	ED 新余额
Mac	MAC3

5.3.3 C 程序代码

```
/*****************************************************************
 ** 函数名：unload
 ** 功  能：圈提交易
*****************************************************************/
int unload(int card_no,char *qtje,char *jjkno,char *package_head,char *err_val)
{
unsigned char qcje1[5],termno[7],termno1[13],sdata[15],sw[3];
unsigned char re_val[17],qcval[37],sdata1[23],tmp[200];
unsigned char edye2[5],edye1[13],sdate[17],edye[13],serial[5],ran[9],mac[9],verflag[5],tmp1[9];
char err_str[50],track[200],slCommarea[500];
int ff,i,ffcz;
long int qcnew,cardmoney,qc1;
unsigned char res_head[100];
unsigned char key_head[7];
char tradetype[3];
```

```
memset(tradetype,0,sizeof(tradetype));
memcpy(tradetype,"03",2);
qc1=atoi(qtje);
/*读出密钥*/
if(hsmKey("mulkhead",key_head,err_val)){return -21;}
for(i=0;i<4;i++)memcpy(qcje1+i,(unsigned char *)&qc1+3-i,1);
qcje1[4] = 0;
no[6]=0;
sdata[0]=1;//圈提密钥标识
for(i=0;i<4;i++) sdata[i+1]=qcje1[i];
memcpy(sdata+5,termno,6);
ff=Initialize_For_Unload(card_no,5,sdata,re_val,sw);//5 pboc
sw[2]=0;
if(ff!=0) {
  strcpy(err_val,turn_errormsg(sw));
  strcat(err_val,"存折圈提交易初始化失败");
  return -1;
}
BinToCHex((unsigned char *)qcval,(unsigned char *)re_val,16);
qcval[32]=0;
for(i=0;i<4;i++) cardmoney=cardmoney*256+re_val[i];
sprintf((char *)edye,"%012d",cardmoney);//余额转换
memcpy(serial,qcval+8,4);//联机交易序列号
serial[4]=0;
memcpy(ran,qcval+16,8);
ran[8]=0;
memcpy(mac,qcval+24,8);
mac[8]=0;
sprintf(slCommarea,"%s%s%s%s%s%s%s%s%s",package_head,ran,key_head,mac,qtje,edye,trad
etype,serial,jjkno);
ff=con_send(slCommarea,sdata1,70,22,res_head,err_str);
if(ff!=0){
  strcpy(err_val,"第一次通讯失败,");
  strcat(err_val,err_str);
  return -1;
}
sdata1[22]=0;
memcpy(sdate,sdata1,14);
sdate[14]=0;
CHexToStr(sdata,sdata1);
sdata[11]=0;
if(Debit_For_Unload(card_no,5,sdata,tmp,sw)==0)//返回 tac(tmp)
{
  tmp[4]=0;
```

```
  BinToCHex(tmp1,tmp,4);
  tmp1[8]=0;
}
else{
  strcpy(err_val,turn_errormsg(sw));
  strcat(err_val,"圈提写卡错误！");
  return -1;
}
memcpy(edye2,re_val,4);
qcnew=0;
for(i=0;i<4;i++)  qcnew=qcnew*256+edye2[i];
qcnew=qcnew-qc1;
sprintf((char *)edye1,"%012d",qcnew);//余额转换
sprintf(slCommarea,"%s%s%s%s%s%s%s%s%s",package_head,ran,key_head,tmp1,qtje,serial,ed
ye1,tradetype,sdate);
slCommarea[6]='2';
ff=con_send(slCommarea,tmp,84,106,res_head,err_str);
/* 超时重发 */
if(ff==-99){
  ffcz=con_send(slCommarea,tmp,84,126,res_head,err_str);
  if(ffcz!=0){
    strcpy(err_val,err_str);
    return -88;
    }
}
memcpy(prHead,res_head,84);prHead[84] = 0;
memcpy(prBody,tmp,126);prBody[126] = 0;
  //（打印凭证部分从略）
strcpy(err_val,"存折圈提交易成功!              ");
return 0;
}
```

5.4 消费交易

5.4.1 交易流程

图5-8给出了对电子存折/电子钱包应用的消费交易处理流程。消费交易允许持卡人使用电子存折或电子钱包的余额进行购物或获取服务。此交易可以在销售点终端（POS）上脱机进行。 使用电子存折进行的消费交易必须提交个人密码（PIN），使用电子钱包则不需要。

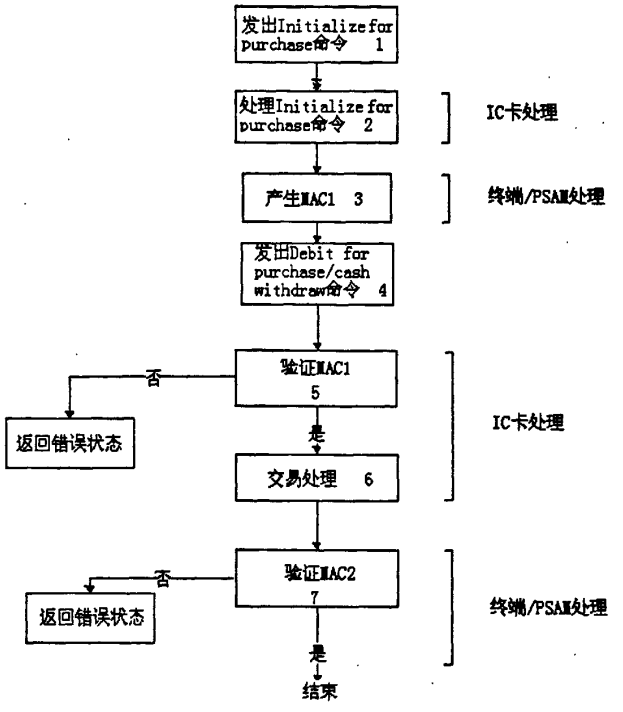

图5-8 消费交易处理流程

1.发出初始化命令：终端发出INITIALIZE FOR PURCHASE命令启动消费交易。

2.处理初始化命令：IC卡收到消费交易命令后，检查是否支持命令中提供的密钥索引号。如果不支持，则回送状态码‘9403’（不支持的密钥索引），但不回送其他数据。检查电子存折余额或电子钱包余额是否大于或等于交易金额。如果小于交易金额，则回送状态码‘9401’（资金不足），但不回送其他数据。

在通过以上检查之后，IC卡将产生一个伪随机数(ICC)和过程密钥（SESPK）用于验证MAC1。

3.产生 MAC1:使用伪随机数（ICC）和IC卡回送的电子存折脱机交易序号或电子钱包脱机交易序号，终端的安全存取模块（PSAM）将产生一个过程密钥（SESPK）和一个报文认证码（MAC1），供IC卡来验证PSAM的合法性。用SESPK对以下数据进行加密产生MAC1(按所列顺序)：

- 交易金额
- 交易类型标识
- 终端机编号
- 交易日期（终端）
- 交易时间（终端）

4.发出消费交易命令:终端发出DEBIT FOR PURCHASE/CASH WITHDRAW命令。

5.验证MAC1:在收到DEBIT FOR PURCHASE/CASH WITHDRAW命令后，IC卡将验证MAC1的有效性。如果MAC1有效，交易处理将继续执行6中所描述的步骤。否则将向终端回送错误状态码‘9302’（MAC无效）。

6.交易处理:IC卡从电子存折余额或电子钱包余额中扣减消费的金额，并将电子存折或电子钱包脱机交易序号加1。IC卡必须成功地完成以上所有步骤或者一个也不完成。只有余额和序号的更新均成功后，交易明细才可更新。

IC卡产生一个报文签别码(MAC2)供PSAM对其进行合法性检查，并通过DEBIT FOR PURCHASE/CASH WITHDRAW命令响应报文回送以下数据，作为PASM产生MAC2的输入数据。用SESPK对以下数据进行加密产生MAC2:

•交易金额

IC卡用密钥DTK左右8位字节异或运算后的结果产生TAC。TAC将被写入终端交易明细，以便于主机进行交易验证。下面是用来生成TAC的数据，它们以明文形式通过CREDTE FOR PURCHASE/CASH WITHDRAW命令的响应报文从IC卡传送到终端:

•交易金额

•交易类型标识

•终端编号

•终端交易序号

•交易日期（终端）

•交易时间（终端）

对于电子存折消费交易和电子钱包消费交易（可选），IC卡将用以下数据组成的一个记录更新交易明细。

•电子存折脱机交易序号或电子钱包脱机交易序号

•交易金额

•交易类型标识

•终端机编号

•终端交易序号

•交易日期（终端）

•交易时间（终端）

7.验证MAC2：在收到IC卡(经过终端)传来的MAC2后，PSAM要验证MAC2的有效性。MAC2验证的结果被传送到终端以便采取必要的措施。在新的PBOC标准中，提出了灰锁控制机制，即重要操作前要制灰锁，交易结束后解开，这样可以保证交易的完整性。

5.4.2 POS 界面设计

图5-9给出的是电子钱包POS消费的界面显示序列。

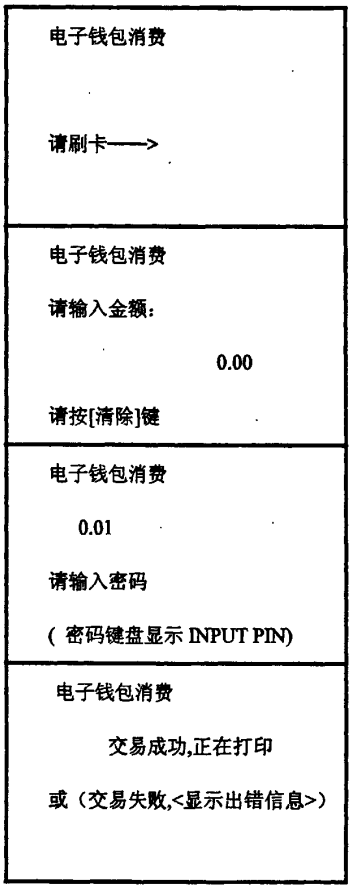

图5-9消费交易的POS界面

5.5 主机批量记帐

5.5.1 简单流程

电子钱包进行脱机交易时，交易明细记载在商户的机具之中。交易明细是以循环记录文件形式保存在卡片的某一文件中，该交易明细文件的修改由卡片内部完成，终端只能对其进行读取操作。每天在银行营业结束前，商户通过网络将机具中存储的当天交易明细流水发送到银行帐务主机，和银行结算交易款。因为不是联机的交易，如何鉴别流水的真伪（即对商户发来的交易明细进行鉴别）就是

在主机记帐时需要做的一个重要操作过程。这个过程就是TAC的校验过程[26][27]。

上一节中我们提到了TAC的计算。它是通过交易金额、交易类型标识、终端编号、终端交易序号、交易日期、交易时间等作为要素，由3.5.4节说明的算法计算出TAC数值，附加在流水之后一并上传。帐务主机在日终批量入帐时，将每一笔脱机交易的TAC发送到加密机，调用相关功能进行校验，只有校验通过的才记入当日交易发生额，而校验未通过的则进入异常交易登记簿，次日和商户进行核对，处理后续情况。

5.5.2 TAC 校验代码

```
char *test_TAC()
    {
//(变量定义从略)
        if ( umspAdapConfig( &sgAdapCfg, "HSM") != SUCCESS)
          {
            sprintf( string, "取加密机通讯参数失败!\n");
            writeposlog( string);
            strcpy( return_code, "PP02");
            goto out_line;
          }
        sprintf( string, "ip = [%s], port = [%d]\n", sgAdapCfg.sPeer_addr,
sgAdapCfg.iPeer_port);
        writeposlog( string);
        sockId = socket( AF_INET, SOCK_STREAM, 0);
        hsmAddr.sin_family = AF_INET;
        hsmAddr.sin_addr.s_addr = inet_addr( sgAdapCfg.sPeer_addr);
        hsmAddr.sin_port = htons( sgAdapCfg.iPeer_port);
        result = connect( sockId, ( struct sockaddr*)&hsmAddr, sizeof( struct sockaddr)
);
        if ( result < 0)
          {
            strcat( return_code, "M7");
            goto out_line;
          }
        stTimeOut.l_onoff = 1;
        stTimeOut.l_linger = 0;
        setsockopt( sockId, SOL_SOCKET, SO_LINGER, ( char*)&stTimeOut,
sizeof( stTimeOut));
        memset( string_hsm, 0, sizeof( string_hsm));
```

```
            sprintf( string, "keyver = [%s],\nalgflag = [%s],\nkeyindex = [%s],\nickh =
[%s],\nmac3 = [%s],\nhexamount = [%s],\ntranflag = [%s],\nmtermno = [%s],\nofflineno =
[%s],\ntrandate = [%s],\nvertime = [%s]。 ", keyver, algflag, keyindex, &ickh[ 3], mac3,
hexamount, tranflag, mtermno, offlineno, trandate, vertime);
            writeposlog( string);
            sprintf( string_hsm,
"58%2s%2s%2s%16s%8s030000000000000000%8s%2s%12s%8s%8s%6s", keyver, algflag,
keyindex, &ickh[ 3], mac3, hexamount, tranflag, mtermno, offlineno, trandate, vertime);
            writeposlog( string_hsm);
            result = send( sockId, string_hsm, strlen( string_hsm), 0);
            if ( result != strlen( string_hsm))
              {
                strcat( return_code, "M8");
                goto out_line;
              }
            memset( string_hsm, 0, sizeof( string_hsm));
            result = recv( sockId, string_hsm, sizeof( string_hsm), 0);
            if ( result < 0)
              {
                strcat( return_code, "M9");
                goto out_line;
              }
            strncat( return_code, string_hsm + 2, 2);
    out_line:
            close(sockId);
            return( return_code);
          }
```

第六章 结论

智能卡在我国的发展比较迅速，但是在金融业智能卡系统的发展却比较缓慢，主要原因是从磁卡升级到IC卡所要面临的巨额成本，使各家商业银行换卡的动力不足[28]。有人预测，如果中国的银行卡全部更新成智能卡，总体投入要以百亿计。而银行卡犯罪所带来的资金损失还不足以触动各家商业银行立即采取措施更换卡片和系统。

本文从天津农行智能卡系统建设项目，对智能卡系统所涉及的主要安全技术和安全机制做了研究，设计了密钥子系统、发卡子系统和交易子系统的有关环节，主要研究成果归纳如下：

1、密钥作为智能卡系统的核心，遍布整个系统的各个关键环节，起到及其重要的作用。针对目前的情况，灵活设计密钥子系统，既可在将来做为三级中心使用，又可在现在做为一、三级混合中心使用。

2、发卡系统除了完成对卡片的严格管理之外，对联机扩展应用和旧卡回收做了尝试，并取得比较好的效果。

3、在交易子系统中，要严格按照人民银行的有关规范的要求来完成功能设计，在各类金融机具上实现。

系统在设计实现过程中，需要各环节的紧密配合，从中心帐务主机到前置机到终端机具的每个环节都十分重要，由于我们的经验不足，肯定存在一些只有在实际环境中才能遇到的问题，后来的实践也证明了这点；同时我们应该看到，出于成本考虑，受选择卡片的限制，在功能自由扩展上还存在一些缺憾，这要靠技术的进一步发展来弥补[29]。

总之，虽然系统还有许多升级优化工作等待我们去完成，但是随着金融智能卡的辅助功能逐渐被开发，功能将不断增强，金融智能卡逐步演变成真正的“电子货币”[30]。金融智能卡系统将会变得越来越强大，越来越贴近客户的实际需求，从而为丰富银行的金融产品，提升竞争力作出贡献。

参考文献

[1] 申淑文. 透视银行卡[J].《金融电子化》,2003,(8)：56-57

[2] 胡伟敏. 浅谈银行智能卡在我国的推广应用[J].《中国信用卡》,2003,(2)：28-29

[3] 高建平. 电子银行客户密码安全保护策略的探讨[J].《南平师专学报》,2006,25(2):54-56

[4] 段泽强. 中国网上银行面临三大问题[J].《金卡工程》,2005,9(3):50-50

[5] 胡鹏. 握奇智能卡—在网上银行安全领域的应用[J].《金卡工程》2003,(11)：28-29

[6] 李军. 当前银行信息化发展的重点[J].《金卡工程》,2005,9(3)：48-48

[7] 吴彦军. 我国银行信息化任重而道远[J].《金卡工程 》,2005, 9(3)：49-49

[8] 孙战平. 中国银行业智能卡遵循标准的困惑与出路[J].《中国信用卡》,2003(5)：53-55

[9] 王爱英. 智能卡技术--IC 卡(第二版)[Z]. 清华大学出版社, 2003

[10] 杨振野. IC 卡技术及其应用:高等教材[Z]. 科学出版社, 2006.7

[11] 陆永宁. 非接触 IC 卡原理与应用[Z]. 电子工业出版社, 2006.9

[12] 编委会. 建设事业 IC 卡应用技术与发展[Z]. 中国建筑工业出版社, 2003

[13] 李翔. 智能卡研发技术与工程实践--智能卡开发技术系列[Z]. 人民邮电出版社,

[14] 2003 牟大中 刘启明：金融智能卡交易系统安全性研究[J]《金卡工程》,2003,(10)：54-57

[15] (美)Wolfgang Rankl Wolfgang Effing. 智能卡大全--智能卡的结构·功能·应用(第 3 版)[Z]. 电子工业出版社, 2002

[16] Mike Hendry. 智能卡安全与应用（第二版）[Z]. 人民邮电出版社,2002

[17] 刘守义. 智能卡技术[Z]. 西安电子科技大学出版社, 2004

[18] 周玉洁 冯登国. 公开密钥密码算法及其快速实现[Z]. 国防工业出版社, 2002

[19] 旋奈尔(Schneier B.). 网络与信息安全技术丛书-应用密码学协议.算法与 C 源程序[Z]. 机械工业出版社, 2000

[20] 杨义先 钮心忻. 应用密码学[Z]. 北京邮电大学出版社, 2005

[21] 宁宇鹏. PKI 技术[Z]. 机械工业出版社, 2004

[22] 谢冬青，冷健. PKI 原理与技术[Z]. 清华大学出版社,2004

[23] 桂兵元. 存款人信息智能卡管理的设想[J].《金融电子化》,2006(9):68-69

[24] 何流. Java 智能卡开发关键技术与实例[Z]. 电子工业出版社, 2003

[25] 李裕华，李舫，孙明. 自装IC智能卡机[Z]. 西安交通大学出版社, 2005

[26] 格思里. 智能卡开发者指南[Z]. 电子工业出版社, 2000

[27] 黄淼云，李也白，王福成. 智能卡应用系统[Z]. 清华大学出版社, 2000

[28] 崔晓梅. 智能卡市场及展望[J].《今日电子》,2005,(7)：91-91

[29] 黄雁，苏海斌. 银行系统智能卡的研究及一种新思想的提出[J].《金卡工程》,2005,9(4)：46-49

[30] 尹龙. 网络金融理论初论：网络银行及电子货币发展及其影响[Z] 西南财经大学出版社,2003

攻读硕士期间参加科研情况

1、主持开发中国农业银行天津市分行《经营分析系统》
2、主持开发中国农业银行天津市分行《短信平台》

攻读硕士期间发表论文

《智能卡系统的密钥应用》发表于《天津理工大学学报》

致　谢

在本论文完成之际，首先向老师冯志勇教授致以崇高的敬意。在论文研究期间，导师从选题到论文撰写的方方面面都给予了悉心的指导和关怀。先生严谨求实的治学态度、高瞻远瞩的眼光、深厚渊博的知识、高深的学术造诣和锐意进取的精神将使作者受益终身。在先生的指导下，我不仅增长了知识，提高了科研能力，也学到了对待知识和工作的严谨、认真的态度，为我今后的学习和工作打下了坚实的基础。在此衷心感谢冯教授给予我的关心和教导。

在本课题的研制开发过程中，得到了中国农业银行天津市分行信息电脑中心的多位同志在软件和硬件方面的指导，同时格尔、捷德、亿阳等公司的有关人士也给予了我许多热心的帮助，提出了大量宝贵的意见，在此对他们表示感谢，祝他们今后的工作取得更大的成功。

感谢我的父母和家人，是他们的支持使我能够专心的完成我的学业，祝愿他们健康、快乐！