目 录

CONTENTS

内 容 简 介

本书系统介绍现代密码学的基本原理、核心技术及其在金融信息系统安全服务方面的实用技术。内容包括：密码学的数学基础与算法分析基础，金融领域的安全需求，适合普通大众的加密技术和现代密码体制的设计技巧，DES、IDEA、AES 等对称密码算法，RSA、EIGamal、ECC 等公匙密码算法，信息完整性鉴证、数字签章与抗抵赖技术，密匙重构、数字现金、隐私权保护等金融信息安全实用技术，公匙密码制攻击算法与改进算法，NTRU 密码技术、量子密码学、概率加密技术。

本书内容翔实，表述严谨，提供了大量具体的算法伪代码和许多追踪算法的实例，读者可以据以编成计算机程序进行模拟实验，领会信息安全技术的精华。

本书可作为高等院校计算机科学、信息科学、金融学、通信工程、应用数学等专业的本科生教材及研究生教学参考书，也可以作为通信系统、金融系统、网络与电子商务系统的技术培训教材和实用工具书。

图书在版编目（CIP）数据

现代密码学与金融信息安全技术/王泽辉 编著. —广州：暨南大学出版社，2004. 8
ISBN 7-81079-407-8

Ⅰ. 现… Ⅱ. 王… Ⅲ. 密码术—应用—金融—信息系统—安全技术 Ⅳ. F830.49

中国版本图书馆 CIP 数据核字（2004）第 053529 号

出版发行：暨南大学出版社

地　址：中国广州暨南大学
电　话：编辑部（8620）85220289　85225262　85225277
　　发行部（8620）85223774　85225284　85220602（邮购）
传　真：（8620）85221583（办公室）　85223774（发行部）
邮　编：510630
网　址：http://www.jnupress.com　http://press.jnu.edu.cn

排　版：暨南大学出版社照排中心
印　刷：暨南大学印刷厂

开　本：850×1168　1/16
印　张：20.25
字　数：442 千
版　次：2004 年 8 月第 1 版
印　次：2004 年 8 月第 1 次
印　数：1—6000 册

定　价：30.00 元

序

王泽辉近日捧来数十万字的《现代密码学与金融信息安全技术》一书手稿，说已列入学校教材资助项目准备出版，请我为之作序。我知道他是我们计算数学及其应用软件专业的一名学术思想活跃，知识涉猎甚广，校内忙于教学、科研，校外敢辟专栏的青年骨干教师，居然还在笔耕不息，且还结出硕果，实在令我欣喜。因此，尽管我对密码学知之甚少，对他作序之请，也就未加推却。

我从头至尾，将书稿仔细读了一遍，该书有几个特点，给我留下了很深的印象。

第一，面向多层次、各专业的读者群。该书是在他几年来现代密码学研究心得结合教学实践的讲稿基础上形成的，他讲授这门课，听者既有大专生、本科生，又有研究生；既有理科学生，又有文科学生。要想做一道适合各种口胃的美味菜肴，是一件难事，更何况是写一本书，但本书在这方面的处理是相当成功的。他呈现给读者的是一本由浅入深、深入浅出的杂味书。浅则浅到像听故事一样有趣，深则深到暂时还没有答案，引起有志研究者的浮想，可以说是抓住了基础和前沿这两头，带动了中间。为学之道，好比登山，先要由下往上看，若隐若现的远景，使你的好奇心油然而生，下决心一步一步往上攀登，一面攀登，一面欣赏点评；到了山上，又要停住脚步，由上往下看，环顾四周，体会群峰在脚下，一览众山小的心境，从而更激发你攀登绝顶的理想和决心。

第二，密码学的数学基础、加密解密方法、算法和编码及其在计算机上的实现，贯通起来，一气呵成。这既利于初学者入门，又利于应用者使用，是很可贵的。本来密码学是一门应用数学，从古典密码学到现代密码学都离不开数学，任何学过一点数学，想问数学有什么用的人，密码学给出了一个直截了当而又十分有说服力的例子。比如，书中反复用到的求两个整数的最大公约数的辗转相除法（欧几里德算法），这是小学算术中就学过的，但小学生中知道它们在密码学中有用的恐怕很少。该书所述密码技术主要用到数论的方法，还涉及到代数中的群、环、域等基本概念和理论。这些数学基础都糅合在密码体制的设计中，书中对此均做了简明的处理和阐述。

但如果仅止于此，这一类作为应用数学的密码学的书并不少见，更有意义的是该书讲出了密码学的计算科学的特色，不仅有模型、有思路、有方法，还有算法，有在计算机上进行编码和实现的指引和大量例子。有兴趣的读者，还可循此进行编程，开展更大规模的数学实验，激发更多的奇想，做出新的创造。这类密

码学的书是很符合信息和计算科学时代的要求的。因为一切信息都可以通过“0”、“1”两个基本码的组合来表示，信息的加密和解密，无非是按一定想法（常与某数学难题相关），对信息做变换和反变换，也就是对“0”、“1”代码做正反的计算，但信息是大得惊人的，离开了计算机这一强有力的工具，尽管我们可以想得很深、很远以至想入非非，但却走不了很远，因为力不从心。因此，光把密码学讲到数学层面还是不够的，必须讲到计算科学的层面。该书作者正是做到了这一点，也如实地反映了我在开头所提到的作者的专业和兴趣广泛的特点。

第三，该书尤其紧扣金融信息系统的安全问题，介绍了这方面重要的密码体制、许多实用技术和作者本人的研究成果。这从目录就可一目了然，无需赘述。当然，现代密码学还在不断发展，如图视密码学（Visual Cryptography）将密码学与计算机图形学相结合，是当今一个很活跃的研究方向，该书没有涉及，也不可能涉及，否则篇幅会太大。

该书涉及到的数学知识有的还是很深的，有些要领对新学者可能还有突兀之感，好在作者对不同层次的读者如何使用本书，提出了不同的建议和要求。由于有上述特色，不同读者是可从中找到自己感兴趣的东西的，我相信本书会受到广大读者的欢迎。

李岳生

2004 年 2 月 4 日

（本序作者是中山大学老校长）

前　言

密码学的历史可以追溯到公元前 11 世纪的周武王时代，但作为一门学科则是 20 世纪 70 年代才形成的，自动化技术促使电信行业、金融行业飞速发展，也带来安全问题，催生了密码学的大量研究成果。

现代密码学是在古典密码学的基础上发展起来的，古典密码基于初等数论的同余算法、模 n 运算，实际上也是在整数环 $<Z_n, +, \times>$ 及素数模域 $<Z_p, +, \times>$ 上展开加密解密变换。现代密码学采用了大量近世代数的研究成果。从最抽象的群论出发，构造了 EIGamal 密码体制，体制安全性基于大整数阶循环群上离散对数问题的求解困难性。为了解决电信、金融信息系统存储空间不大问题，利用了有 100 多年历史的椭圆曲线理论，在环（域）H 上椭圆曲线 E（H）中构造循环（子）群，根据特征 char（H）的分类，形成了 E（Z_p）与 E（F_{2^m}）上两个实用 EIGamal 体制，其中应用了多项式环、伽罗瓦域的研究结果。

在密匙交换理论上，古老的辫群（阿廷群的子类）被发掘出使用价值。被誉为只有量子计算机成熟化才可能破译的公匙密码 NTRU 体制，则应用了另一个近世代数结构——“格”，其安全性基于寻找格上最短向量的困难性。不过，这两个体系的算法研究尚未完成，后者还可能出现解密失败的情况，本书只作简单叙述。现代抽象数学理论，只有在能找到多项式时间的加密变换，密匙攻击却找不到多项式时间算法（基于某个数学难题），且满足体制的归一性情况下，才能广泛应用于密码学中。

相形之下，第一个成熟的公匙密码体制 RSA，其安全性基于大整数因子分解的困难性，虽然只用到古典数论的欧拉定理，但由于满足复合密码变换可交换性、公匙私匙可逆性，至今仍被广泛应用于金融等领域，形成一系列行业标准，本书对此作了详细介绍。另一个被证明有漏洞的背包公匙体制，本书不再介绍。与 RSA、EIGamal 体制发展同步的是数字签名体制的建立并大量应用于金融、电信、电子商务等领域。适应金融信息系统的特点，现代密码学的一个重点内容是研究受限空间上的密码技术，以降低对带宽、存储空间、处理器的要求，成果之一是 ECC（椭圆曲线密码系统）。本书加重了这方面的分量。限于篇幅，有些内容虽然重要但本书涉及不多，如序列密码。

公匙密码体制是单密匙体制。单匙制的迅速发展并没有削弱双匙密码体制的使用，相反，它们在不同领域各有所长。实际上，大量一次性会话通信是采用单匙制进行通信，而双匙制则用于加密会话密匙。双匙密码体制已有成熟的行业标

准，所用工具大多从整数环、多项式环、伽罗瓦域中发掘，其构造思路可从作者提出的同体、异体开关变换去理解，以进行更复杂的构造。

为了彻底解决搭线信道上的窃听、截获密匙、密文问题，现代密码学还应用了量子物理的技术。利用信息的量子比特一经测量就会有不可还原的改变这一特性，可以防止窃听、截获信息，传递和保存密匙和关键信息，其中部分受到 Rabin 公匙制的启发，后者还被应用于“不经意传输”之中。越来越高级的技术科学手段、越来越深奥的数学理论将被用于现代密码学中，尽管本书尽可能反映前沿密码技术，但当本书付印之时，又有许多新理论提出。

现代密码学离我们并不遥远。伴随着因特网技术在人类生活的深入，网上认证、身份鉴别、保密传输、电子政务、电子商务、网上支付问题，均与我们息息相关；我们使用的银行智能卡，其中就应用了 DES、AES 加密技术，而电子钱包、电子支票则使用了更复杂的加密技术；数字现金用于保护金融客户的隐私权，应用了密码学中的秘密协议技术。我国网络金融发展迅速，据报道，《电子签章条例》即将出台，这将确立我国电子文件和电子签章的法律效力。电子签章在国外称为数字签名，其发展与密码体制同步。网上证券、网上期货、网上外汇交易，涉及全球上亿上兆的资金，其安全责任巨大，各国都花费巨资进行密码学研究。现代密码技术已经标准化、产业化、法规化。

本书撰写历时两年多，大的修改有数十次，主要原因是要融合多个目标。在向本科生授课时，许多学生都明白现代密码技术的重要性，但对数论内容望而生畏，特别是文科学生都希望能以一种快速的途径切入密码技术。毕业班学生则希望能提供详细的算法程序，想马上能开展工作；研究生则希望能进一步接触最前沿的理论，以便进行深入研究。学生们普遍反映密码学书籍不少，但例子不多，缺乏追踪密码学关键步骤的同步算例，以及涉及中文信息处理的例子。

基于这些要求，作者最后做了一个重要改动，形成这本适合浅、中、深各个层次读者，文科、理工科学生，数学、非数学类学生能同时阅读、有不同取舍的教材。第六章之前采用了难易分拆、错开编排的处理，每章按严格逻辑顺序讲述内容，但重要定理的证明、复杂的推导则留在第 X 节列出。具有中学文化程度的读者可以很快理解第二章前部分的多数密码技术，并应用于与友人的中英文加密通信，或保存、记忆一系列银行密码。自第三章起，内容由浅入深，读者可以用“黑箱原理”跳过难懂的数学理论，即把数学理论看成一个“黑箱”，只需知道有关输入参数，通过“黑箱”之后形成什么样的输出参数，能解决什么样的技术难题，从而尽快切入技术领域，以后再回头做深入研究。各章节都提供大量算法伪代码，读者可以用自己熟悉的计算机语言编成程序去实现，一步步地追踪、熟悉算法的各个流程。

第六章涉及近世代数的复杂理论，没有采用难易分拆编排，但独立开辟了第二节和第五节两节作为该章的浓缩本，供学生在不熟悉近世代数的情况下阅读。另外，通过算法和算例也可以领悟 ElGamal 密码体制与 ECC 的精华。第七章、第八章介绍金融领域上的安全技术，实际上也适用于非金融领域。第九章用到的

数学理论均来自前面章节，但多数节基本独立成编，提供了可继续进行研究的素材及算法伪代码。

本书一些新思路、新提法是在授课中、调试程序中发现的。作者提出了同体开关变换、异体开关变换的概念（本书设计了记号 T_d、T_e 分别代表开变换、关变换），以便读者可以像理解开电源、关电源般，去理解加密解密过程、数字签名原理，可以像设计家庭电源线路一样，去设计密码体制以完成安全保护。本书企图通过教学实践使读者体会到：密码学并不神秘！

本书设计了一个新记号 MOD n，以区别于传统的同余记号 mod n。这是作者在长期调试密码学程序、多次出错排错中领悟到的。mod n 不具唯一性（可正可负、可奇可偶），一些密码算法虽然数学推导无错，但却会导致编程出错。采取 MOD n 记号可使算法程序更具操作性，本书采用 MOD n 记号描述各个密码体制，稍微有别于其他教材，目的在于方便学生上机实验。

对于密码体制，本书不仅介绍其数学基础，更重要是介绍如何设计、配置参数，用优化算法去实现，这是本书另一特色。部分内容采用作者近年一些研究结果，如对 RSA 体制的低阶攻击技术（不同于主流的平方同余攻击算法、椭圆曲线因子分解法、随机碰撞攻击等）、EIGamal 体制密匙设计技术（基于古典数论同余方程的深入研究）、素数检测加速技术（提出了超强伪素数的概念及新算法，优于目前主流的 Miller – Rabin 检测）等。

在本书的撰写过程中得到计算数学的学术前辈，特别是李岳生教授、黄友谦教授的多次鼓励。李岳生教授对计算数学的学科发展做了巨大的工作，对计算数学与信息科学的结合、对于文理结合学科渗透早有前瞻性的研究，使作者领悟了不少为学之道。黄友谦教授鼓励作者写出一本适合不同层面读者的教材。作者对李岳生教授、黄友谦教授表示衷心的感谢，师恩难忘！暨南大学出版社张仲玲编辑为本书出版做了大量工作，不少学术界同仁和出版界朋友提供了宝贵意见，作者一并表示衷心感谢。

本书尽管做了多次修改，但疏漏之处仍在所难免，如蒙读者斧正，作者将不胜感激。

王泽辉

2004 年 2 月于康乐园

第一章
金融信息系统安全问题

【本章简介】 本章概述了信息系统与信息系统安全的概念、信息系统应遵循的设计原则和应建立的安全机制。介绍境内证券市场运作的四大系统、交易与结算的技术细节和安全问题，并与境外证券市场进行比较分析。介绍了网上金融交易市场，以及3个范例——网络证券、网络期货、网络保险，指出其发展潜力及信息安全问题。介绍了电子银行、网络银行及电子货币（智能卡、数字现金、电子支票、电子钱包等）的特点及所用安全技术。通过对现代金融数字化、电子化、网络化发展趋势的分析，阐述现代密码学在金融信息系统中的地位和作用。

第一节 信息系统安全概述

人类社会已告别了农业经济时代，由工业经济时代迈向知识经济时代。工业经济以物质和能源为基础，知识经济则以信息和知识为基础，知识经济社会在生产、流通、消费、技术、管理、产业结构等方面都表现出一些与农业经济时代、工业经济时代明显不同的特征，信息产业现已成为发达国家、发展中国家的主导产业之一。因而学术界也将当今社会称为信息经济社会。

信息经济社会尚保留工业经济社会的若干特点，其中之一是金融资本依然是社会最核心、最活跃的生产要素，不过社会金融活动已步入更高的层次：金融业务处理自动化，金融营业网点虚拟化，金融信用工具无纸化，国际金融活动一体化，国际金融资本流动巨额化，金融组织全球集中化。

促成这些变化的契机，是进入20世纪90年代以来，在计算机与通信技术日趋成熟的同时，计算机硬件和通信设备的价格不断下降，而且因特网（Internet）技术取得惊人的发展，全球各种不同的计算机、软件平台、网络设备，基于TCP/IP协议集进行相互通信，实现资源共享。因特网缩短了时空距离，促成数字化生存，为知识经济带来勃勃生机。金融业也由传统金融——自动化金融进入网络金融时代，准确而言，是以计算机网络和现代通信技术为支撑的信息系统在金融领域发挥了巨大的作用。

水能载舟，亦能覆舟。金融信息系统处理每一笔金融业务的时间越来越短，但通过金融信息系统进行的交易量却越来越大。一个银行职员轻按一下终端机的

鼠标，可以在几分钟内使数以百亿计的资金在国际金融网络中运转数次；同时，一个高科技窃贼也可以使数以百亿资金在瞬间化为乌有。国际金融信息系统变得越来越先进，同时也变得越来越脆弱，一个发达国家的某个银行系统一旦崩溃，可以使整个国家以至全球的支付系统陷于瘫痪。

因而，当人们在赞叹网络信息技术给全球经济带来勃勃生机的同时，信息系统安全问题也成为各国科技界的一个重要的研究问题。

准确而言，信息系统是基于计算机的系统，是人员、进程、数据、硬件、软件的有机集合，它基于一定目标和规则，对所有形态、所有形式的信息进行采集、组织、加工、存储、提取、传输、检索和显示。现代信息系统广泛应用了数学理论（特别是统计与运筹理论）、科学管理理论、计算机技术、通信技术，由早期的数据处理、事务处理信息系统发展为管理决策支持信息、多媒体信息系统和办公自动化系统。而金融信息系统就是服务于金融领域的现代信息系统。

信息系统安全是指信息在存储、提取、加工、传输、检索过程中，保持其机密性、完整性、有效性、可用性、可靠性、可审查性、抗抵赖性的系统辨识、系统协调和系统控制过程。

机密性指信息对非授权用户保密，不会泄密给非授权用户或为非授权用户所使用，这里授权用户的定义是动态的，授权用户进行超越权限的操作便变成非法用户，机密性是最基本的安全目的。

完整性指信息在存储和传输过程中不被删除、更改、添加，甚至恶性破坏，能保持原有数据及组织方式的完整。

有效性指系统及信息交换的双方，能够检验接收到的信息从内容到顺序是否是真实的，是否是某种信息的重播。

可用性指授权用户在需要时不必经过太多延迟便能使用系统，而不会产生拒绝访问、长时间等待系统响应的情况。

可靠性指系统的软件和硬件不会产生故障和差错，具有完成指定任务的能力，同时拒绝合法用户的非法操作。

可审查性指系统能对访问者进行正确的身份鉴别，区分授权用户与非授权用户，也指系统及信息交换的双方，能对信息的存取、传输进程进行必要记录，以便影响安全的行为可以被追溯到责任方。

抗抵赖性指对信息向授权客户的传送保留正确的记录，防止授权接收方作出事后抵赖。

信息系统存在安全威胁，固然有其外因——基于某种目的的人为因素，但也同其内因——计算机系统的弱点和网络协议的脆弱性有关（有关协议的内容见第七章）。

计算机系统本身的弱点包括：（1）电磁辐射的易泄露性。借助专门仪器可截获信息。（2）数据的易复制性。数据集合一旦被访问到，可以方便复制而不留痕迹。（3）高密度存储的易失性。信息能进行高密度的存储，但一旦受到意外损害会丢失大量数据。（4）剩磁的易分辨性。信息的存储介质具有剩磁的特点，擦除

信息时未必完全擦尽，通过专门设备能够分辨出可用信息或会泄密。（5）网络通信的双向性。互联互通是优点也是“缺点”，可以造成搭线截获信息，同时网络无法拒绝成千上万的“敌意访问”，易造成网路堵塞。

基于 TCP/IP 通信协议集合的 Internet 技术，原本就是在可信任网络环境中开发出来的成果，总体构思旨在互联互通、共享资源，基本上未考虑安全性的需要。Internet 的脆弱性在于：（1）Internet 使用 IP 地址作为节点的唯一标识，缺乏对用户身份的鉴别；（2）缺乏对路由协议的鉴别，对路由信息缺乏保护；（3）子协议 TCP/UDP 作为传输协议本身有一定的缺陷，可能造成“拒绝服务”、“隐身攻击”的安全威胁。

其他类型的计算机网络，主要为局域网（LAN）及城域网（MAN），以减少互联互通范围的代价换来比 Internet 相对安全的使用环境，但仍存在信息的电磁泄露性和基于协议分析的搭线截获（搭线攻击）等安全威胁。

为了消除对信息系统的安全威胁，美国著名信息安全专家 C·C·沃德提出了信息系统设计的 23 条设计原则，其中最重要的为下列 10 条原则。

（1）简单性原则。简单易行的控制比复杂控制更可靠更有效。

（2）最小特权原则。任何主体只限于需要才被赋予所必须的特权。

（3）失效保护原则。一旦系统运行出错必须完全关闭系统。

（4）纵深防御原则。不能只靠一种防御机制，应建立互相支撑的多种安全机制。

（5）分割保护原则。

（6）环状结构原则。

（7）门岗设置原则。

这 3 个原则结合即是：把需要保护的整体分成若干部分一一予以保护；采用环状结构的控制方式最保险；在系统对外通道上要设置多个“门岗”进行监控，所有进入“门岗”的访问系统都要做登记。

（8）护“短”原则。系统最脆弱部分的安全状况决定了系统整体的安全状况，应随时保护“软肋”部分。

（9）敌对环境原则。系统应能抵御最坏的用户企图、容忍最差的用户能力。

（10）人工干预原则。不能完全依赖计算机自动处理，必要时应启动人工干预机制。

根据以上原则，信息系统应建立一系列安全机制，包含而不限于下列 9 个：①数据加密机制；②认证鉴别交换机制；③完整性保护机制；④访问控制机制；⑤审计机制；⑥公证机制；⑦路由选择控制机制；⑧冗余填充机制；⑨备份机制；⑩数字签名机制。

为了消除不同网络结构之间进行通信的安全威胁，国际标准化组织（ISO）早在 1978 年就提出了开放系统互联 OSI（Open System Interconnection）的七层参考模型。ISO 建议在这 7 层的安全服务与安全机制之间，应具有如下关系。

（1）最底层：物理层。可提供数据保密服务，由上述 A（数据加密）和 H

（业务流填充）机制实现。

（2）次底层：链路层。可提供数据保密服务，由A（数据加密）机制实现。

（3）第三层：网络层。可提供数据保密、数据完整性、数据源点识别、同等层实体识别、访问控制等安全服务，由上述A、B、C、D、F、G、H、I、J 9种机制单独或组合起来实现。

（4）第四层：传输层。可提供同等层实体识别、访问控制、数据保密、数据源点识别等安全服务，由上述A、B、C、D、E、J 6种机制单独或组合起来实现。

（5）第五层：会话层。不提供任何安全服务，故不需要安全机制。

（6）次高层：表达层。可提供数据保密、数据完整性、数据源点识别、网络实体识别、访问控制、抗抵赖等安全服务，由上述B、C、D、F、J 5种机制单独或组合起来实现。

（7）最高层：应用层。可提供数据保密、访问控制等安全服务，由上述A、D、H 3种机制单独或组合起来实现，同时用户也可自行开发专用的机制。

我国颁布的GB17859—1999《计算机信息系统安全保护等级划分标准》，将计算机信息系统安全性从低到高划分为五个等级，分别为用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级，计算机信息系统安全保护能力随着安全保护等级的增高而逐渐增高（具体见参考文献［27］）。

这些安全机制或安全手段，相当部分是建立在现代密码学之上，明显的如数字签名机制；而依赖于计算机硬件或软件的安全手段有其局限性，为了满足系统本身的基本功能往往导致出现更高明的攻击手段，造成新的安全威胁，有效的解决之道是采用数学方法。本书将由浅入深、逐层推进地阐述建立于数学理论之上的现代密码技术，如何构建各种安全机制，来实现信息系统特别是金融信息系统的安全保护、消除各种安全威胁。

第二节　证券市场运作信息系统概述

一、境内证券市场

金融信息系统最生动的代表是证券市场运作信息系统。

证券市场运作信息系统大体可分为四大部分：交易信息系统、结算信息系统、公众信息披露系统与专用信息服务系统。

我国境内证券市场尽管只有十余年的历史，但政府为市场建设投下了大量人力、物力、财力。目前，境内证券交易运作系统的技术装备在全世界应属领先地步，我们侧重点在于境内市场，对境外市场主要做比较分析。

按照我国《证券法》规定，我国境内经依法核准上市的股票、公司债券和其

他证券，应在证券交易所挂牌交易，并采用公开的集中竞价交易方式。我国现有两个证交所是深圳证券交易所（简称深交所）与上海证券交易所（简称沪交所），进入证交所参与交易的，必须是具有证交所会员资格的证券公司或证券经纪商（简称证券商）。证券商通过在证交所购买一定数量的交易席位方式进场交易，证券投资者应当在证券商处开立证券交易账户和资金账户，以电话、终端操作等方式，委托证券商代其买卖证券。具有自营资格的证券公司，也可利用自己的交易席位或其他证券商的交易席位，自营买卖证券。

我国境内的证券交易采用无纸化操作，证券与资金都记录在账户中，证券交易以转账方式进行，经证交所确认，A 投资者买入证券，B 投资者卖出证券，证券将从 B 投资者的证券账户转入 A 投资者的证券账户，相应的资金在扣除交易费用后，从 A 投资者的资金账户转入 B 投资者的资金账户。因而要理解证券市场的运作，可以从投资者——证券商——证交所这个关系链入手。

在理解上述内容的基础上，下面分析境内证券市场运作信息系统的四大部分。

（1）交易信息系统。由证券商交易委托终端、证券商柜台（报盘）系统、通信网络、证交所交易主机 4 部分组成。

证券商交易委托终端是投资者作出投资委托的各种设备，委托方式包括：电话委托、上网委托、现场自助委托、现场填单（书面）委托、传真电报合同委托等，在作出第一次委托之前，投资者要与证券商签订使用终端的书面合同，并设定交易密码。在上海证交所开户的，还要签订指定交易（限定于该营业部做沪股买卖）的合同书。委托类别包括买、卖、撤销原先买卖指令等，申购新股、配股包括在买入类中。

证券商柜台（报盘传输）系统，是证券商接收各种委托终端的委托信息，按照交易所规定的固定格式，通过通信网络向证交所交易（撮合）主机报盘，接收委托成交（买卖成交及撤销指令成交）信息并传送给投资者，或存储入券商系统备查的专用计算机信息系统。

通信网络是连系证券商报盘传送系统、交易席位和证交所交易主机的通讯线路及设备，如单向卫星、双向卫星传输设备和地面数据专线。严格地说还应包括出市代表（“红马甲”）用于传递委托、成交回报及实时行情等信息的现场报盘设备；不同的交易席位使用不同的通信方式。目前，我国所用通讯网络非常先进，深交所与沪交所都租用亚洲一号卫星的通讯线路，证券商利用地面卫星小站传输信息，交易所还要求证券商再租用地面数据专线，保证数据传送的双重保险。

交易主机也称撮合主机，是整个交易信息系统的运作中心，它将通迅网络传来的各个席位的买卖委托、撤单委托读入计算机内存，进行撮合配对，或撤销原来的买卖委托。撮合配对的顺序遵循价格优先、（同种价格）时间优先的的原则，同时分为开市前的集合竞价与其后的连续竞价，撮合主机先对接收的委托进行合法性检测，对合格的买卖委托按价格优先、（同价格时）时间优先的顺序安排撮