内容摘要

电子支付作为电子商务的核心环节和关键步骤，其实现程度一直是影响电子商务发展速度的主要因素之一。如何在不安全的因特网上实现安全的支付，是人们密切关注的焦点，也是一个值得深入研究的课题。

本文从现实生活中各种支付手段出发，总结各自的支付流程和网络应用，分别给出了将现实支付手段映射到电子支付手段的系统描述，从电子支付的安全需求及安全攻击入手，结合多种网络安全技术，针对电子信用卡提出了基于 SET 协议的安全电子支付系统，该系统可以从根本上保证了交易的安全性，是一种很好的电子商务模式的解决方案。

现代密码学是网络安全的基础，而公钥加密算法又是密码学的基础内容，本文对于基于 IFP、DLP 和 ECDLP 问题的三种密码体制进行了深入的分析，并举例进行了讲解。之后，针对当今电子支付领域的研究热点，即电子现金，进行了深入的研究。Brands 受限盲签名方案是离线电子现金协议的理论基础，使用该技术可以实现用户身份的匿名性并能保证事后揭示双重花费用户的身份。本文对该方案的盲变换表达式进行了简化，并将其模拟到椭圆曲线上实现，在保证安全性的前提下，降低其计算复杂度，提高了执行效率。

在基于 ECDLP 的改进的 Brands 受限盲签名方案的基础上，提出了一种基于 ECDLP 的安全离线电子现金协议，具体描述了提取、支付和存储三个子协议，并从八个方面对该协议的安全性进行了详细的论证，同时对其性能进行了有益的探讨。之后是对本电子现金系统的模块分析，界面介绍及部分代码的实现，为电子现金的进一步实用化打下了一定的基础。

最后,本文给出了基于 ECDLP 的安全离线电子现金协议进一步应该完善的地方，并对电子现金未来的发展方向进行了展望。

关键词：电子支付，电子现金，椭圆曲线，盲签名

Abstract

As the core factor and crucial process, electronic payment has long time been a primary bottleneck hindering the rapid growth of e-commerce. How to realize the secure payment in the insecure network environment, has become not only the focus which people keep close watch on, but also an important subject to be devoted deep and thorough research.

This paper gives the subsystem's payment processing description, through the mapping of the payment methods in reality to electronic payment methods in network. Aiming at the electronic payment's security and its security attacks, combining with many network security techniques, this paper gives a secure electronic payment system based on SET protocol for the electronic credit card. This system can assure the security of the transaction ultimately, it is an efficient solution of electronic trade.

Modern cryptography is the basis of the network security ,and the public key algorithm is also the basis of the modern cryptography .This thesis gives a deep research on the three algorithms based on IFP， DLP and ECDLP ,gives a example for explanation .Aiming at the focus of electronic payment field, namely electronic cash, this thesis carry through deeply research.

Brands' restrictive blind signature scheme is the theory basis of off line electronic cash protocol ,which can assure the anonymity of honest users and detect the double spending activities afterwards .The thesis improves the Brands' restrictive blind signature scheme ,through simplifying the blind expression ,and simulates it to ellipse curve .On the premise of ensuring security ,it declines the computing complexity ,enhances the efficiency

Based on the improvement of Brands' restrictive blind signature scheme, the thesis not only proposes a secure off line electronic cash based on ECDLP, but also gives a comprehensive analysis of its three sub protocols of withdrawal, payment, and deposit. Its security is particularly demonstrated from eight aspects, the efficiency of this scheme is beneficial discussed. Subsequently, this thesis gives module analyzing of the electronic cash system, the interface introduction and a part of source code, which sets up a solid foundation for the practical utility of electronic cash.

In the end, this paper proposes the further work to perfect the secure off line

electronic cash based on ECDLP, and prospects the future of development of the electronic cash.

Key words: electronic payment, electronic cash, ellipse curve, blind signature scheme

Y 797442

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 天津工业大学 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：刘剑　　签字日期：05年 3月 2日

学位论文版权使用授权书

本学位论文作者完全了解 天津工业大学 有关保留、使用学位论文的规定。特授权 天津工业大学 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：刘剑　　导师签名：石振东

签字日期：05 年 3 月 2 日　　签字日期：05年 3月 2日

学位论文的主要创新点

1. 结合多种网络安全技术，针对电子信用卡支付提出了基于SET协议的安全电子支付系统，该系统可以从根本上保证了交易的安全性，是一种很好的电子商务模式的解决方案。

2. 本文对 Brands 受限盲签名方案的盲变换表达式进行了简化，并将其模拟到椭圆曲线上实现，提出了一种基于 ECDLP 的改进的 Brands 受限盲签名方案，在保证安全性的前提下，降低其计算复杂度，提高了执行效率。

3. 在基于 ECDLP 的改进的 Brands 受限盲签名方案的基础上，提出了一种基于 ECDLP 的安全离线电子现金协议，具体描述了提取、支付和存储三个子协议，并从八个方面对该协议的安全性进行了详细的论证，确保了该协议的安全性。

第一章 绪论

1.1 电子商务的概念

电子商务(E-Business,E-Commerce,E-Trade)从英文的字面意思上看就是利用现在先进的电子技术从事各种商业活动的方式。电子商务的实质应该是一套完整的网络商务经营及管理信息系统。它是利用现有的计算机硬件设备、软件和网络基础设施，通过一定的协议连接起来的电子网络环境进行各种各样商务活动的方式。

Internet 上的电子商务可以分为三个方面：信息服务、交易和支付。主要内容包括：电子商情广告；电子选购和交易、电子交易凭证的交换；电子支付与结算及售后服务等。其交易类型有九种，主要交易类型有企业与个人的交易(B to C)和企业之间的交易(B to B)两种。参与电子商务的实体有四类：顾客、商家、银行和认证中心。

电子商务是 Internet 爆炸式发展的直接产物，是网络技术应用的全新发展方向。Internet 本身所具有的开放性、全球性、低成本和高效率的特点，也成为电子商务的内在特征，并使得电子商务大大超越了作为一种新型的贸易形式所具有的价值，它不仅会改变企业本身的生产、经营、管理活动，而且将影响整个社会的经济运行与结构。

1.2 电子商务发展状况及趋势

1.2.1 电子商务的发展历程

电子商务并不是一个新概念，可以说，在几十年前主机系统出现时就诞生了。但是，近年来，Internet 的出现给了电子商务以新的活力，基于 Internet 的电子商务已经引起了全世界的注意。

电子商务始于网络计算。网络计算是电子商务的基础。没有网络计算，就没有电子商务。其发展形式多种多样，从最初的电话、电报到电子邮件以及其后的 EDI，都可以说是电子商务的某种发展形式。

电子商务的发展有其必然性和可能性。传统的商业是以手工处理信息为主，并且通过纸上的文字交换信息，但是随着处理和交换信息量的剧增，该过程变得

越来越复杂，这不仅增加了重复劳动量和额外开支，而且也增加了出错机会，在这种情况下需要一种更加便利和先进的方式来快速交流和处理商业往来业务；另一方面，计算机技术的发展及其广泛应用和先进通信技术的不断完善及使用导致了 EDI 和 Internet 的出现和发展，全球社会迈入了信息自动化处理的新时代，这又使得电子商务的发展成为可能。

70 年代，美国银行家协会(American Bankers Association)提出的无纸金融信息传递的行业标准，以及美国运输数据协调委员会(Transportation Data Coordinating Committee, TDCC)发表的第一个 EDI 标准，开始了美国信息的电子交换。

随着美国政府的参与和各行业的加入，美国全国性的 EDI 委员会禀 X12 委员会于 80 年代初出版了第一套全国性的 EDI 标准，接着，80 年代末期联合国公布了 EDI 运作标准 UN/EDIFACT(United Nations Rules for Electronic Data Interchange for Administration, Commerce and Transport)，并于 90 年由国际标准化组织正式接受为国际标准 IDO9735。随着这一系列的 EDI 标准的推出，人们开始通过网络进行诸如产品交换、订购等活动， EDI 也得到广泛地使用和认可。

不过，EDI 始终是一种为满足企业需要而发展起来的先进技术手段，必须遵照统一标准，与普通老百姓一直无缘。而且由于网络在那时仍没有得到充分发展，这使很多商务活动的电子化，仅仅处于一种想法阶段。

直到 90 年代，随着基于 WWW 的 Internet 技术的飞速发展，这些想法逐步成熟，Internet 网络开始真正应用于商业交易，这时电子商务才日益蓬勃起来，并成为 90 年代初期美国、加拿大等发达国家的一种崭新的企业经营方式。因此我们可以说电子商务在今天成为继电子出版和电子邮件之后出现在 Internet 上的又一焦点的主要原因就是 Internet 技术的成熟、个人电脑互联性的增强和能力的提高。

1.2.2 中国电子商务的发展现状

2003 年岁末，中国互联网市场却丝毫感觉不到一丝寒意，风险投资、并购、上市这些激动人心的消息充斥了各类媒体，新一轮的互联网大潮已经悄悄到来！

市场研究机构对 2003 年我国电子商务市场给予充分的肯定，来自互联网实验室的报告称，03 年我国网上购物市场规模达到 18.8 亿，各类互联网电子服务市场规模达到 42.8 亿。来自艾瑞市场研究的报告则显示，03 年我国网上购物额为 7.9 亿，预计 04 年将达 16 亿；而来自中国电子商务协会和中国网络评测中心的相应研究数据为 1.9 亿美元与 3.2 美元。03 年岁末，各大购物网站也相继传出利好消息，大有决战 2004 之势头。种种迹象表明，2004 年，我国电子商务将进

入全新的发展阶段。

业界普遍认为，非典促进了电子商务的发展，然而从近期来看却并非如此。非典确实刺激了网民，甚至非网民的电子商务欲望，但是，当我们亲自进行电子商务体验的时候，才发现并非理想中的那样方便与高效。以远程教育为例，大多数产品与服务都是政府支持与仓促上阵，质量与售后服务难以保证，给消费者带来的更多是麻烦与不满，交易环节的障碍此时才真正显现。因而，对于非典产生的影响，更确切的说法应该是，非典让我们真正发现了我国电子商务发展的症结。消除交易环节的障碍，促进交易大量而顺利地发生，才是电子商务公司应该首要考虑的问题。

中国电子商务这 4 年，我们不断进行着烧钱与试验。但是，我们复制了 Amazon、eBay，却无法复制支撑着它们高效运转的物流系统、支付机制与消费环境。我们的电子商务，一度沉迷于网络营销，吸引了大量的眼球与游客，却难以产生出相应规模的营收与利润。数据显示，我国在线零售商务交易额仅占零售市场总体规模的 0.02%，远低于欧盟的 1-2%。经过 4 年的探索，我们的电子商务公司已经逐渐找到了发展的道路，电子商务不再是口号与旗帜，而是实实在在的生意经。电子商务公司应当发挥主动创新的精神，利用拥有 IT 技术的优势，深入分析交易的每一个环节，去设计与创造推进交易发生的机制。7000 万网民的底盘，平均 3 至 4 年的互联网使用经验，已经足够支撑起一个巨大的电子商务消费市场，电子商务将进入真正的交易时代。

网络游戏超乎预期的成长为数字产品交易市场的形成做出了重要的贡献。虽然游戏公司的点卡销售大多数仍然通过传统渠道完成，但在线交易无疑是这类电子服务产品最适合的销售方式。而游戏经营带来的后续效应更加对在线交易平台的供应提出了要求，网友间虚拟装备的交易也有可能成为最容易实现的在线 C2C 交易。

我国目前的互联网支付体系为建立在电子银行基础上的借记账户(借记卡)信用转账系统，该体系自 1999 年首信创立二级结算的支付网关模式以来一直在不断完善之中，在具备安全优势的同时，支付手段显得较为单一，尚无法覆盖除了 B2C 支付之外的其他支付需求，如 P2P 支付、匿名支付等互联网商务的潜在需求。虽然一些网站已经在试验电子货币系统，但还没有大型跨系统方案的出现。随着电子商务的深入发展，支付领域的创新将成为可能。尤其对于潜力巨大的 C2C 市场，合适的支付机制的出现，将改变目前在线竞价市场热闹而缺乏交易的局面。

必须承认，我们的电子商务还处于初级阶段，基本的 B2C 交易条件已经具备，但金融体制的限制仍制约了跨国界交易的发展，信用卡的推广与普及也将对

现有的支付体系带来冲击。在 B2B 领域，虽然银行方面的数据显示已经产生了可观的交易，但绝大多数的交易仍发生在企业的内部转账过程，基于 XML 的跨界交易标准还没有真正实现，B2B 交易的电子集市仍然只起到网络营销的单一功能。我们还需要进行更多的基础建设与务实的推进，电子商务才得以进入真正的交易时代。

1.3 电子支付

电子支付是电子商务的关键环节，是电子商务得以顺利发展的基础。没有实时的电子支付手段相配合，网上交易就无法实现。电子支付指的是电子交易的当事人，包括消费者、商家和金融机构之间，使用安全电子手段，通过网络进行的货币或资金流转，即把新型支付手段(包括电子现金、信用卡、借记卡、智能卡等)的支付信息，通过网络安全地传送到银行或相应的处理机构来实现电子支付。

1.3.1 我国电子支付的发展现状

在我国，应用最广泛的非现金零售支付工具为借记卡账户，互联网支付功能的开发自然从借记卡开始。网上银行功能是在线支付服务的基础，几年来，各家主要商业银行的网络银行业务不断地发展完善，并各自向商家提供不同规范的支付接口。由于金融机构的大集中还在进展当中，现有商业银行的多级结构给商家和消费者造成了诸多混乱与不便。

银联的存在解决了多银行接口集成的问题，利用金卡工程已经建立的地方跨行 ATM/POS 网络，地方银联有条件向商家提供多银行卡在线支付接口，消费者的 PC 作为虚拟的 ATM/POS 终端，通过 Web 页面输入银行卡账号与 ATM 密码即可方便地实现在线支付。广州银联、厦门金卡中心以及上海的 China Pay 发展较早，在消费者当中已经建立了良好的口碑。

1998 年，首信公司借助首都电子商务工程的优势率先进入市场，集成了多家银行的接口，向电子商务公司提供统一的第三方支付网关服务，该模式为我国在线支付体系的形成奠定了基础并沿用至今。

随着支付接口技术的逐步透明，以及各种电子商务支付需求的不断增长，2003 年以来全国范围涌现了数十家中小规模的增值支付服务商，以较低廉的接入价格吸引中小商户的加盟。然而，中小型商户的需求与在线支付数量短期内还难以达到临界规模，以及业务模式上没有更多的创新是这类服务商未来生存与发展的最大障碍。

总的来看，中国的互联网支付服务自 1998 年起由银行、地方银联、政府工

程以及商业支付网关并行发展，各类支付服务机构拥有不同优势的资源并互相交错渗透，共同向商家提供在线支付与结算服务。虽然该体系还存在诸多混乱与不便，但无论如何，互联网支付服务模式在近两年已经逐步成熟，商家和消费者已经能够找到安全有效的在线支付办法。

1.3.2 我国电子支付的前景及未来

信用卡与借记卡并非互联网支付的全部，至目前为止，几乎每一种传统支付机制都已开发出相应的互联网版本，如电子现金、电子支票；IT 技术公司也开发出多种完全基于互联网的创新支付机制，并在全球范围内已经对传统金融支付系统发起了挑战。这些支付机制或者具有匿名性的优势，或者具备微支付的能力，或者在交易费率上拥有价格优势，已经在不同的应用领域取得了越来越广泛的接纳。

在我国，借记卡支付目前还占据着互联网支付的绝对统治地位，这种基于"储蓄+密码"的支付机制符合我国消费者长期以来形成的支付习惯，该架构将仍然继续沿用。由于信用卡与借记卡能够共享同一套技术体系，未来广泛使用的信用卡也将建立在此架构基础之上，并逐渐与国际卡支付机制相容。环讯与新加坡 NETS 电子转账网络的合作已经为跨边界卡支付做出有益的尝试。

创新支付机制在我国的发展还处于初生阶段。虽然各种规模的网站出现了很多基于预付费机制的忠诚度及电子点数方案，但几乎没有跨商家品牌的出现，金融机构尚未开始部署这类基于互联网的电子货币系统。国外的创新支付品牌事实上已经进入国内市场，但由于金融政策体制的限制暂时还不能在国内提供更完善的服务，目前云网、当当网上书店等少数商家已经尝试提供 Papal 支付。随着电子商务交易规模的不断扩大，这类创新支付机制将更多地为国内商家所采纳。

银联的成立使得各地方银联的资源实现互联互通，银联所操作的卡支付系统成为国家支付系统的重要组成部分，将形成以银联为中心的跨行电子资金转账网络(EFT)。近日银联已经开始独立向大型互联网商家提供在线支付解决方案，国内互联网支付服务的格局有望产生巨变。然而，银联的优势在于实时跨行转账，该业务的互联网应用市场目前还远未开发，银联未来的业务模式应当着眼于此。对于支付服务商来说仍然具有生存的空间，除了作为银联的代理机构，支付服务商仍可继续与银行直接合作，以及进行跨边界支付的合作，或者开发基于创新支付机制的增值服务产品。

第二章 电子支付领域分析与设计

电子支付领域分析的主要任务是通过分析现实生活中的支付手段来推导出适合网络应用需求的电子支付，给出电子支付总体功能模型和相应于各种支付手段的具体功能模型。相应的，在设计阶段，在对领域对象的抽取以后，利用 UML 建模技术给出领域对象的静态模型和动态模型。

2.1 传统的支付方式

电子支付技术是建立在对传统的支付方式的深入研究基础之上的。人们总是通过传统支付方式来比较电子支付，所以在讨论电子支付总体功能模型前，有必要对传统支付方式进行一次再认识。传统支付方式有现金、票据和信用卡等多种支付方式。

1．现金支付

现金有两种基本形式：纸币和硬币，由国家组织或者政府授权的银行发行。其中，纸币本身没有价值，它只是一种国家发行并强制使用的货币符号，但是却可以代替货币加以流通，其价值由国家加以保证。硬币本身具有价值。

在现金交易中，买卖双方处于同等位置，而且交易是匿名进行的。卖方不需要了解买方的真实身份，因为现金本身是有效的，其价值是由发行厅机构加以保证的，而不需要买方认同。加之现金所具有的使用方便和灵活的特点，故多数的个体与个体之间或者个体与组织之间的小额交易是通过现金支付来完成交易的。

这种交易程序上很简单，一手交钱，一手交货；交易双方在交易结束后马上就可以实现交易目的：买方用现金买到货物，卖方用货物换取现金。然而这种交易存在一些缺陷：①纸币作为纸张的特性决定了现金易于伪造、磨损和偷盗等；②受交易时间和地点的限制。对于不在同一时间、同一地点进行的交易，就无法采用先进支付；③对于一些大额交易，纸币本身存在的小安全性使它很难适应需求。

2．票据支付

这里的票据专指票据法所规定的汇票、本票和支票等票据。汇票是出票人委托他人于到期日无条件支付一定金额给受款人的票据；本票是出票人自己于到期日无条件支付一定金额给受款人的票据；支票则是出票人委托银行或者其他法定金融机构于见票日无条件支付一定金额给受款人的票据。因此，可以说，票据是

出票人依顺《票据法》发行的、无条件支付一定金额或者委托其他人无条件支付一定金额给受款人或持票人的一种文书凭证。

在商业交易中，交易双方往往不在同一个地方，所以常常发生异地之间的兑换金钱的需要。在这种情况下，如果输出现金，那数量可能是惊人的，这就可能带来许多麻烦和风险。但是，如果通过在甲地将现金转化为票据，再在乙地将票据转化为现金的办法，以票据为转移代替以现金为转移，则可以减少麻烦，使得交易可靠。

汇票、本票作为汇兑工具的功能逐渐形成后，在交易中以支付票据代替现金支付的方式逐渐流行起来。票据支付可以避免清点现金可能并生的错误，并可以节省时间，因此，人们在经济生活中都普遍使用票据特别是支票作为支付的工具。

下面简要阐述一下生活中用支票作为支付手段的流程。在支票交易中，支票由客户签名后即可生效，商家需要通过银行来处理支票，并需要为此支付一定的费用。因此，与先进交易相比，这种交易方式不再匿名，而且费用也较高，其交易流程见图 2-1。

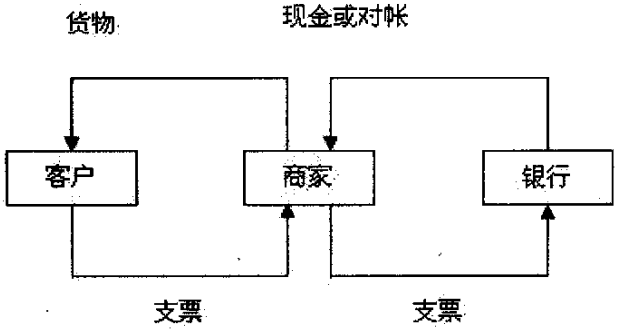

图 2-1 支票交易流程

3．信用卡支付

信用卡是银行或者金融公司发行的，授权持卡人在指定的商店或者场所进行记账消费的信用凭证。

信用卡诞生于美国，由于其极大的刺激了顾客的消费，同时对客户来说的方便性使得它深受大家的钟爱。随着银行业的发展，信用卡也由商业领域的应用转变成为金融领域的应用。电脑的发明和在银行的普遍运用，使信用卡的使用范围大大扩大，跨越了国家界限，遍及了全世界。

信用卡进入中国是在改革开放以后。随着对外贸易的迅猛发展，客观上要求改变原来的结算方式，从国外引进先进的结算方式。在这方面，走在最前列的是中国银行，随之其他各大商业银行也纷纷提供了此项服务。信用卡，在十余年中，得到了迅速的推广和发展。

由此看出，信用卡在全世界都得到了普遍的支持，这一点是与信用卡本身的

特点分不开的，具体说来，它有两个鲜明的特点：

(1) 功能丰富。不同的信用卡，其功能和用途各异，但概括起来，主要有四种：转账结算功能、消费借贷功能、储蓄功能和汇兑功能。

(2) 高效便捷。由于银行为持卡人和特约商户提供了高效的结算服务，这样消费者就便于也乐于持卡购物和消费；同时，便于异地存取，而且又有安全保障。

有关信用卡的交易流程，见下图 2-2

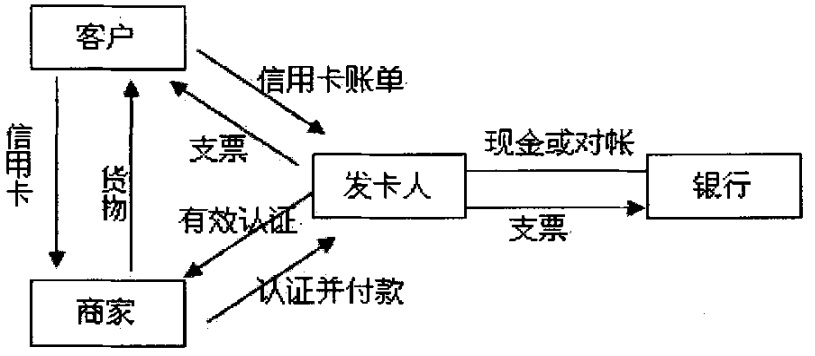

图 2-2 信用卡交易流程

2.2 电子支付系统的功能模型

网上交易需要有支付者和付款接受者，同时还要求至少有一个金融机构。付款接受者为支付者提供商品或服务，支付者支付相应现金，金融机构则提供资金的转移服务。根据支付者和付款接受者之间是否有直接的通信，支付系统可以分为直接支付(Direct Payment)和间接支付(Indirect Payment)；根据支付者实际付款的时间，可以分为提前支付(Pre-paid Payment)、立即支付(Pay-now Payment)和延期支付(Pay-later Payment)；根据用户在银行中是否有账号，可以分为基于账号(Account-based)的支付和基于代币(Token—based)的支付，基于账号的电子支付又可分为电子信用卡支付和电子支票支付，基于代币的电子支付又称为电子现金或数字现金；根据支付者和付款接受者是否与第三方(如发卡行和收单行)在线连接，可以分为在线支付(On-line Payment)和离线支付(Off-line Payment)。下面我们主要电子信用卡支付和电子支票支付两种支付方式，对于电子现金的研究，由于其复杂性，放到后几章进行专门的讨论。

2.2.1 电子信用卡支付

2.2.1.1 信用卡支付的系统描述

前面介绍的传统的信用卡业务处理流程中可以看出其具有四方交易实体。所

以将传统的信用卡支付映射到完整的电子信用卡支付过程时，一般来说，参与者也需要四方：持有信用卡的顾客、提供买卖服务并接受信用卡支付的商家、最终处理信用卡业务中结算的商家开户行和发卡机构。当然，也可以把商家开户行和发卡机构的共性业务统一由银行网关来代理，再由银行网关来处理开户行和发卡机构的结算，如此对该系统来说，参与实体只有三方。不过可以看出二者本质上是一致的。

各个参与主体之间的关系,如图 2-3：

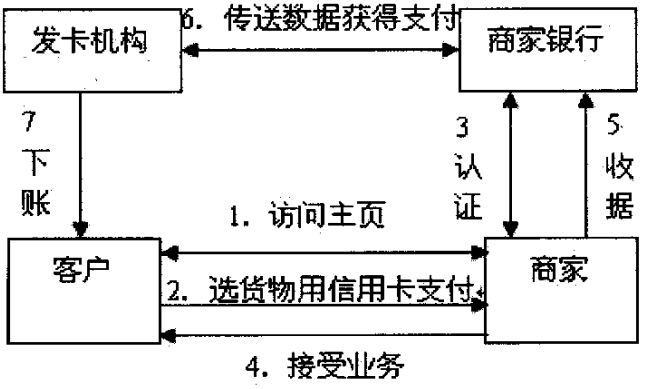

图 2-3 电子信用卡支付系统示意图

具体的业务过程可以有三个阶段。

第一阶段(完成客户的购物)

(1)客户访问商家的主页，得到商家的货物明细单，包括商品目录和报价单。

(2)客户挑选所需要的货物，并用信用卡向商家支付。

(3)商家服务器访问其银行，以要求银行对客户的信用卡号码以及所购货物的数量

进行认证。银行完成认证后，通知商家购物过程是否可以继续。

(4)商家将认证结果通知客户，即是否可以接收业务。

当然，上面的模式更加适用于 B2C 模式。及时购物后，商家生成电子订单提供给用户确认，确认后用户根据电子订单进行信用卡支付活动。然而，对子 B2B 模式，或者说对于供应链管理中供应商-制造商-分销商之间的支付模式，上述过程仅仅适用于它们之间小规模的支付活动。而对于 B2B 中的大宗交易，其订购过程将是一个非常复杂的过程，所以往往将客户挑选货物达成协议的阶段从整个过程中分离，形成单独的订购子系统，而支付系统只是订购成功以后进行的纯粹的支付活动。不过，对于这种纯粹的支付，上述过程中的第三步和第四步是必须的，因为支付活动中涉及到资金流动而支付活动后将涉及到物流，这些和顾客利益及商家利益密切联系的，所以，对支付方的认证是一个不能忽略的过程。

第二阶段(从客户账目向商家账目转账)

(5)商家服务器访问商家的开户行，并向银行提供购物的所有相关数据。

(6)商家银行访问发卡机构，以取得商家售物所得到的钱。

第三阶段

(7)发卡机构根据一段时间客户购物时向各商家支付款项，为客户下账以通知客户。

由于订单信息和支付信息是基于开放的 Internet 网络进行传送，而 Internet 的开放性和匿名性使冒名顶替变得容易，所以，必须保证支付过程的安全性，这便是电子支付的安全性问题，在信用卡支付中具体的安全性要求可以从以下几个方面来考虑：

保密性：客户的信用卡号码、截至日期、购物数量、购物种类等等的一些敏感信息在网上传输时，应该确保得到保护，以免被其他人拦截(Intercept)或者偷听(Eavesdropping)。

认证性：系统必须保证提供一个对客户、商家、商家银行这三方的身份进行有效认证的机制。

完整性：系统必须保证任何一方所发送的消息在途中不被篡改(Tampering)，保证消息的一致性。

不可否认性：必须建立一个处理过程，以解决客户、商家和银行三方在卡支付过程小的争端。不可否认性又称为数字签名，和手写签名一样，一旦签了名，相应的操作行为便不可否认。

从上述系统描述可以看出，信用卡支付系统可以分成两类：其一，实时信用卡支付系统；其二，非实时信用卡支付系统。前者指系统的订购过程和支付过程是一气呵成，完成订购以后，紧接着进行与订购相关的支付，支付结束后再形成财务上需要的发票或者凭证(订单即为原始凭证)以便入账。对于后者指系统订购过程和支付过程是分开的，订购过程可以单独称为一个子系统(该子系统由 ISCM 分销系统来完成)，订购过程的结束应该以双方签订的产，已购销合同为标志，当然，合同中应该就产品相关细节和支付的相关细节达成一致。所以，订购过程和支付过程两个阶段之间的时间间隔应该依照合同的相关条款来决定，而不是实时的。需要指出的是此时的支付数据来源于合同，从财务的角度来看可以认为来源于原始订单，这便于总体功能模型更加的吻合：通过原始订单来进行支付活动，支付结束后需要填制记账凭证，并根据记账凭证入账。无论是实时的还是非实时的支付活动，商家在支付成功后，便可以发送货物。

2.2.1.2 信用卡支付功能模型

无论是实时信用卡支付系统还是非实时的，都是基于现有银行的信用卡管理

系统的，所以对于信用卡的管理工作可以交由银行系统处理。本支付系统其功能模型一般来说主要包括五个部分：客户支付应用(Client_App)、商家支付应用(MeChant_App)、安全代理(Secure_Proxy)、外币汇兑代理(Forei_Exch_Proxy)、支付网关代理(Bank_Gate_Proxy)。客户支付应用的功能主要包括对支付模式选择、订单预处理、支付消息处理(包括安全既定格式进行消息组装、消息解析、消息发送、消息接收、消息转发、消息存储等等)，凭证预处理。商家支付应用和客户支付应用相对，不仅处理与商家销售相关的凭证，还要处理来自客户的支付消息。需要的话，与外币汇兑代理交互获得不同币种的结算办法，最终与支付网关代理交互来对顾客进行认证和转发客户支付指令促使交易成功。安全代理模块主要满足交易过程中存在的安全性需求：保密性、认证性、完整性和不可否认性。实际上安全代理模块的实现不仅要从软硬件上来考虑(加密算法)还必须有相应的安全基础设施来加以保证。外币汇兑代理卡要处理交易双方可能存在的不同币种之间的结算，不同币种的信用卡结算可以从信用卡的种类来区分，外币汇兑代理应该能够就不同币种的信用卡结算给出换算办法。支付网关代理本质上是银行支付网关的通信客户端，通过对支付指令或者认证信息进行协议封装来实现与银行支付网关的通信。故其功能结构图如下：

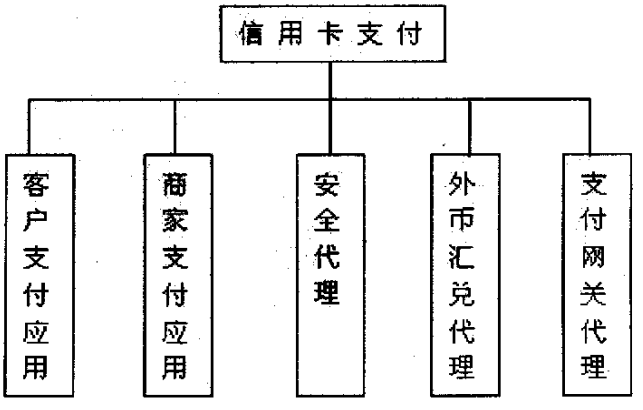

图 2-4 电子信用卡的功能模型

2.2.2 电子支票支付

2.2.2.1 电子支票支付过程描述

电子支票就是纸支票的电子版.它包含纸支票一样的信息,如支票号、收款人姓名、签发人账号、支票金额、签发日期、开户银行名称等；执行和纸支票一样的金融功能。电子支票支付系统用于发出支付和处理支付的网上服务。付款人向受款人发出电子支票，受款人将其存入银行，以换取现金。每宗业务都是在

Internet 上进行的。电子支票与通常支票工作方式大致相同，都应该具有一种类似的电子签名。

图 2-5 是对电子支票系统的描述。从传统支票支付系统演变而来，电子支票系统参与方有客户、商家、银行。而银行可以具体分为：客户的开户行、商家的开户行和票据交易所。票据交易所可由一个独立的机构或者现有的一个银行系统来承担，其功能是在不同的银行之间处理票据。

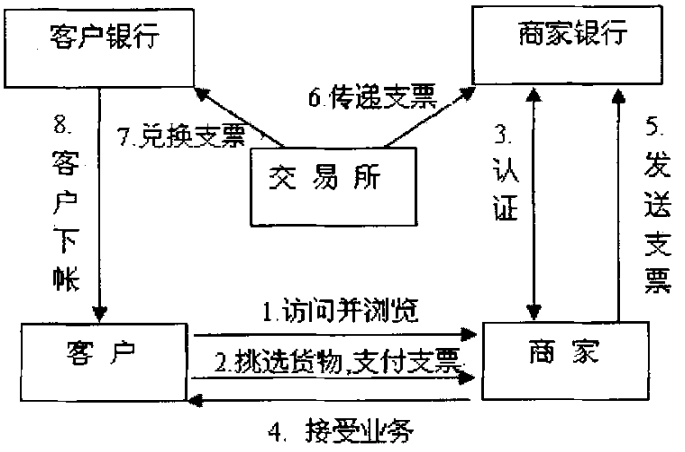

图 2-5 电子支票系统描述

客户端通过使用相应的客户端软件，或者可以访问 Internet 上不同 Web 服务器的浏览器，与相应的服务端软件通信或者浏览网上的商店或者商城。一宗完整的电子支票业务由下面的若干步构成，这些步骤可以分成 3 个不同阶段。第一阶段是客户的购买阶段；第二阶段，商家把客户电子支票发送给商家开户行，以得到现款；第三阶段，商家开户行通过交易所要求客户开户行兑换电子支票。

第一阶段(购买阶段)

(1)客户访问商家的服务器，商家的服务器向客户介绍其货物和价格。

(2)客户挑选货物并向商家发出电子支票。

(3)商家通过商家银行对客户支付进行认证，验证客户支票的有效性。

(4)如果客户支票是有效的，则接收业务，否则拒绝业务。

第二阶段(商家把电子支票发送给它的开户行)

(5)商家把接收的客户支票电子形式发送给它的开户行。商家可以根据自己的需要，决定何时发送。

第三阶段(不同银行之间交换支票)

(6)商家的开户行把电子支票发送给交易所，以兑换现金。

(7)交易所向客户的开户行兑换支票，并把现金发送给商家的开户行。

(8)客户开户行为客户下账，并通知客户。

电子支票系统建立在传统纸支票系统基础上，但纸支票系统中的签字、盖章、笔迹等安全机制对电子支票系统已不适用。电子支票中的所有信息都以数据文件的形式存储、传送，且涂改后不留痕迹、此外，由于 Internet 的开放性也带来了相应的安全风险问题和可靠性问题。所以，电子支票系统还必须采用一些安全措施使其具备纸支票的安全性质，同时应该可以防止 Internet 中存在的安全攻击，在这一点上电子支票支付处理拥有和信用卡支付一样的安全性要求。同时，还有一些额外的要求：首先，电子支票的签发，电子支票的签发实际上是一个初始化过程，但是，必须由客户开户行根据客户的银行账目来生成，同时，应该具有银行的签名，以使得客户相信的确是由其银行发行的；其次，电子支票的认证，传统支票是由客户签署一个文件(即通过签字、盖章等)来进行认证，并同时具有了不可否认性，对子电子支票也必须由用户进行签名，以保证接收者相信发送者的确签署了电子支票，从而，确保不可否认性。所以电子支票具有双重签名。这使得接收者相信所接收的支票是客户签发的，并且通过对银行签名的认证看出是根据发送者在银行的有效账户填写的。

2.2.2.2 电子支票支付系统功能模型

通过比较电子支票支付系统和信用卡支付系统，我们可以简单看出，二者的处理流程基本是一致的，但也有一定的差别，其功能上分成六部分：系统初始化、安全代理、客户支付应用、商家应用、外币汇兑代理和支付网关代理。

之所以存在系统初始化模块，这是由支票系统本身的性质决定的。所有能够签发电子支票的主体应该拥有基于某种安全硬件的电子支票簿设备。“支票簿”是由电信设备公司生产的、被称作“智能辅币机”的安全硬件设备。该设备采用 PC 卡的形式，并在卡中内置了一个加密支持处理器。该设备的功能是安全地存储密钥和证书信息，并保持最近签发或背书过的支票记录，这一过程可以由系统初始化功能模块来完成。安全代理的功能和信用卡支付的功能上基本一致，即都必须能够满足网上支付的安全性要求。

客户支付应用功能与信用卡的不一致，因为这是两种支付手段，从而涉及的订购信息、支付指令的数据结构不一致，相应的对信息进行组装、解析、转发、存储都会有相应的变化。同样商家应用功能也应该针对不同的客户应用功能的改变而改变，客户和商家利用电子支票进行支付时所使用的消息格式可以由交易双方自定义，也可以按照行业内存在的标准。

外币汇兑代理功能与信用卡支付相应功能基本相似，只是具体的实现上有一些差别，因为，电子支票存在不同的币种，所以，外币汇兑代理功能主要针对这些不同种类的电子支票，来与外币汇兑处理模块交互给出一个换算办法。

第三章 安全电子支付系统的设计与实现

3.1 电子支付的安全要素

从传统的基于纸张的贸易方式向电子化的贸易方式转变的过程中，如何保持电子化的贸易方式与传统方式一样安全可靠是人们关注的焦点，同时也是电子商务全面应用的关键问题之一。那么，安全的电子支付有哪些要求呢？

1.信息传输的安全性

电子支付作为交易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面交易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子支付是建立在一个较为开放的网络环境上的(如 Internet 这一开放的网络)，维护商业机密是电子商务全面推广应用的重要保障。因此，所谓信息传输的安全性就是要预防非法的信息存取和信息在传输过程中被非法窃取。

2.交易各方身份的认证

要使网上交易成功，参与交易的人首先要能确认对方的身份，确定对方的真实身份与对方在网上交易的身份是否一致。网上交易的双方可能素不相识。对于商家来说，要确定与自己进行交易的对方的真实身份，而客户也应该能够确定商家是一个合法的真实的商家，因此，能够方便而可靠地确认对方身份，是实现网上交易的前提。

3.信息的防抵赖性

如何确定要进行交易的贸易方正是进行交易所期望的贸易方这一问题，是保证电子支付顺利进行的关键。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。而在网上，一条信息被发送或被接收后，应该通过一定的方式，保证信息的收发各方都有足够的证据证明接收或发送的操作确实发生了，并能够确定发送方或接收方的身份，发送方或接收方都不能否认其发送或接收操作已经发生。由于市场商情千变万化，交易一旦达成，是不能被否认的，因此电子商务中信息交流过程的各个环节，都必须设法防止交易中任何一方抵赖。

4.信息的完整性

电子支付简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商

业信息完整、统一的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复，并保证信息传送次序的统一。

3.2 电子支付的安全隐患

电子支付的安全隐患五花八门，我们把它们划归为两个大类：一类是技术层面；另一类属于非技术层面。

3.2.1 技术层面的安全隐患

从技术上看，对网络的攻击包括对静态数据的攻击和对动态数据的攻击。对静态数据的攻击主要有：

(1)口令猜测。通过穷举方式搜索口令空间，逐一测试，得到口令，进而非法入侵系统。

(2)IP 地址欺骗。攻击者从一个外部地点伪装成源自一台内部主机传送信息包，这些信息包中包含有内部系统的源 IP 地址，冒名他人，窃取信息。

(3)指定路由。发送方指定一个信息包到达目的地的地点的路由，而这条路由是经过精心设计的，绕过设有安全控制的路由。

根据对动态信息的攻击形式不同，可以将攻击分成为主动攻击和被动攻击两种。

被动攻击主要是指攻击者监听网络上传递的信息流，从而获取信息的内容，或仅仅希望得到信息流的长度、传输频率等数据，称为流量分析，达到破坏系统机密性的目的。被动攻击和窃听示意图如下：

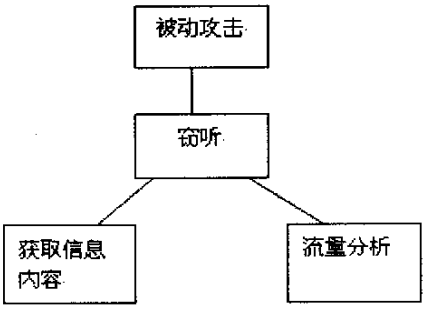

图 3-1 被动攻击

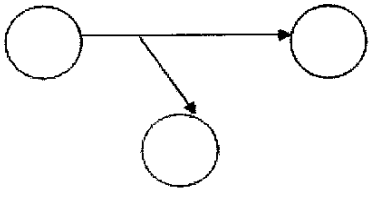

图 3-2 窃听示意图

除了被动攻击的方式外，攻击者还可以采用主动攻击的方式。主动攻击是指

攻击者通过有选择的修改、删除、延迟、乱序、复制、插入数据流或数据流的一部分以达到其非法目的。主动攻击可以归纳为中断、篡改和伪造三种。(见图 3-3)

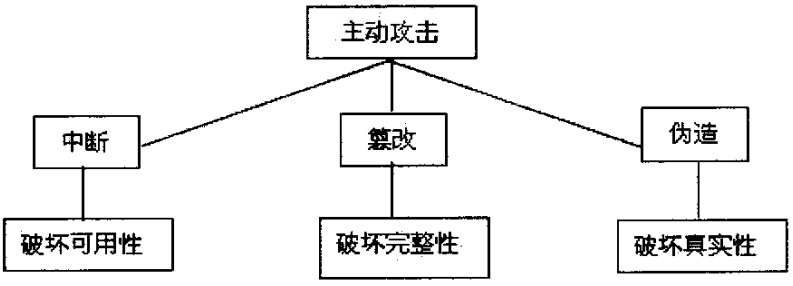

图 3-3 主动攻击

(1)中断是指阻断由发送方到接受方的信息流，使接受方无法得到该信息，这是针对信息可用性的攻击(见图 3-4)。

(2)篡改是指攻击者修改、破坏由发送方到接收方的信息流，使接收方得到错误的信息，从而破坏信息的完整性(见图 3-5)。

(3)伪造是针对信息的真实性的攻击，攻击者或者是首先记录一段发送方与接收方之间的信息流，然后在适当时间向接收方或发送方重放这段信息，或者是完全伪造一段信息流，冒充接收方可信任的第三方，向接收放发送(见图 3-6)。

图 3-4 中断示意图

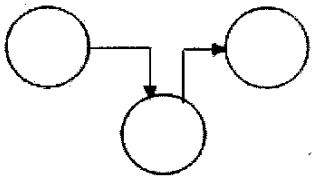

图 3-5 篡改示意图

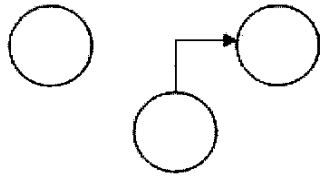

图 3-6 伪造示意图

3.2.2 非技术层面的安全隐患

非技术层面的安全隐患主要包括管理方面的风险和法律方面的风险。

1．管理方面的风险

严格管理是降低网络交易风险的重要保证，特别是在网络商品中介交易的过程中，客户进入交易中心，买卖双方签订合同，交易中心不仅要监督买方按时付款，还要监督卖方按时提供符合合同要求的货物。在这些环节上，都存在大量的管理问题。防止此类问题的风险需要有完善的制度设计，形成一套相互关联、相互制约的制度群。

2．法律方面的风险

电子商务的技术设计是先进的、超前的，具有强大的生命力，现代电子交易手段已越来越被人们所认识，电子商务代表着未来贸易方式的发展方向，其应用

推广将给经济和社会带来极大的效益。但必须清楚地认识到，传统的经济和社会形态下的法律制度不能适用，甚至不利于电子商务的发展。在目前的法律上找不到现成的条文保护网络交易方式，在网上交易可能会承担由于法律滞后而造成的风险。也使得政府对这一贸易形式的鼓励和引导方向及调控目的难以实现，而市场经营主体之间的经营活动处于无章可循的状态，消费者权益难以保障。

由于非技术层面的问题不是本文研究的重点，所以在此不再赘述！

3.3 电子支付的安全技术

1.加密算法

加密是用来保护敏感信息的传输，保证信息的安全性。在一个加密系统中，信息使用加密密钥进行加密后，得到的密文传送给接收方，接收方使用解密密钥对密文解密得到原文。目前主要有两种加密体系：对称密钥加密和非对称密钥加密。

(1)对称密钥加密

对称密钥加密(Symmetric Cryptography)也称为秘密 / 专用密钥加密，发送和接收效据的双方必须使用相同的密钥对明文进行加密和解密运算。

对称加密算法最大的优势就是开销小，加密速度快。它的缺点是：密钥本身必须进行安全交换，以使接收者能解密数据；密钥的分发和管理非常复杂，当某一贸易方有 N 个贸易关系，那么他就要维护 N 个专用密钥；无法鉴别贸易发起方或贸易最终方；不能实现数字签名。

著名的对称加密算法包括：DES，3 重 DES，RC2，RC4 和 IDEA。

(2)非对称密钥加密

非对称密钥加密(Asymmetric Cryptography)也称作为公开密钥算法。非对称加密算法需要两个密钥：公开密钥和私有密钥。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密(数字签名)，那么只有用对应的公开密钥才能解密。

密钥对中的一把作为公开密钥(加密密钥)通过非保密方式向他人公开，而另一把则作为私有密钥(解密密钥)加以保存。由于公开密钥是公开存放，可以被其他用户访问，因此密钥的分配管理问题就很容易解决。非对称密钥加密最大的不足，就是处理速度慢。

著名的不对称加密算法包括 RSA、Diffie-Hellman、DSA 和椭圆曲线密码系统。

2.数字签名

数字签名(Digital Signature)是非对称加密技术的一类应用。它的主要方式如下：报文发送方从报文文本中生成一个 128 位的散列值(或报文摘要)，并用自己的专用密钥对这个散列值进行加密，形成发送方的数字签名；然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方；报文接收方首先从接收到的原始报文中计算出 128 位的散列值(或报文摘要)，接着再用发送方的公开密钥来劝•报文附加的数字签名进行解密。如果两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别和不可否认性。

3.数字证书

数字证书(Digita Certificate,Digital ID)用以证实一个用户的身份和对网络资源的访问权限，是目前电子商务广泛采用的技术之一。在网上的电子交易中，如果双方都出示了各自的数字证书，并用它们进行交易操作，那么双方就可以不必为对方身份的真实性担心了。

数字证书是一个加密并用口令保护的文件，它把一个密钥同一个用户的一个或多个属性进行绑定。它含有证书拥有者的一些个人信息，如持有者姓名、邮件编号和电子邮件地址，其他一些个人信息也可以编码，如信用卡等，这取决于商业的需要。文件中包含一个公开密钥以用来验证消息发送者事先用匹配的私有密钥签过的数字签名，文件中还包含发放该数字证书的验证机构 CA(Certification Authority)和证书的有效期。其内部格式是有 CCITT X.509 国际标准所规定的。

数字证书与传输密钥和签名密钥对的产生相对应。对每一个公钥做一张数字证书，私钥用最安全的方式交给用户或用户自己生产密钥对。数字证书的内容包括用户的公钥、姓名、发证机构的数字签名及用户的其他信息。公钥的拥有者是身份的象征。对方可以据此验证身份。对于密钥的丢失情况、则采用恢复密钥、密钥托管等方法。另外对于证书的有效期在政策上加以规定，已过期的证书应重新签发，对于私钥丢失或被非法使用应废止。数字证书可用于电子邮件、电子支付、电子基金转移等各种用途。

4.数字信封

数字信封(Digital Envelope)是用密码技术的手段保证只有规定的收信人才能阅读信的内容。在数字信封中，信息发送方使用密码对信息进行加密，再利用 RSA 算法对该密码进行加密，则被 RSA 算法加密的密码部分称之为数字信封。采用数字信封技术后，即使加密文件被他人非法截获，因为截获者无法得到发送方的通信密钥，也不可能对文件进行解密，从而保证了信息传输的保密性和安全性。

5.数字摘要

这种编码法采用单向 Hash 函数，将需要加密的信息原文通过特定的变换后，将其“摘要”成一串 128bit 的密文，这串密文又称为数字指纹(Finger Print)。它是有固定长度的一段代码，而且，对于不同的信息原文，将它摘要成密文后的结果总是不同的，而同样的信息原文所形成的摘要必定是一致的。于是，利用这段摘要，就可以验证通过网络传输收到的文件是否是未被非法篡改的文件原文了。

3.4 基于 SET 电子支付交易流程

目前，比较完善的电子商务安全技术通常采用基于 SSL 协议和采用基于 SET 协议的两种技术。基于 SET 的电子商务安全技术是专门为电子支付设计的，保证了电子交易的机密性、数据完整性、身份的合法性和抗否认性。下面我们所介绍的这个安全电子支付系统就是基于 SET 协议。

电子商务模式的参与方有客户、商家、认证中心、商业银行和支付网关。参与电子商务交易的各方，他们都必须拥有 CA(即数字证书认证中心，Certification Authorlty)所发放的数字证书。数字证书包含了证书拥有者的信息和所签发证书的 CA 的相关信息，该证书既可以对信息进行加密，又可以用于签名，它保证了信息传输的机密性、真实性、完整性和交易的不可否认性。CA 作为独立的、客观的、公正的、可信赖的第三方机构，专门为参与网上交易各方提供认证服务。参与网上交易的各方通过彼此验证证书，确认对方的身份，防止欺诈，从而保证了交易的安全。参与交易的各方及交易流程如图 3-7 所示。

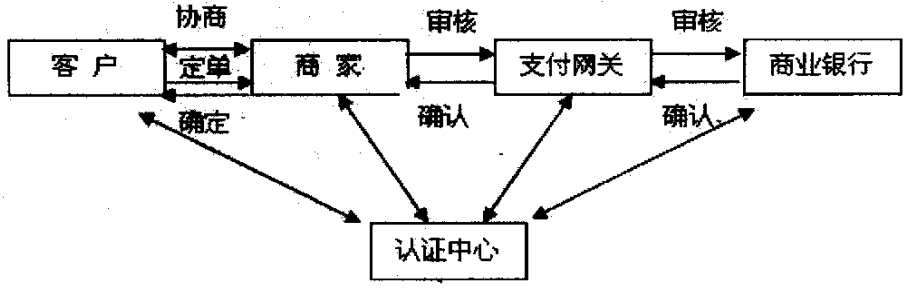

图 3-7 参与交易的各方及交易流程图

电子商务的工作流程与实际的购物流程非常接近，使得电子商务与传统商务可以很容易融合，用户使用也没有什么障碍。从顾客通过浏览器进入在线商店开始，一直到所定货物送货上门或所定服务完成，以及账户上的资金转移，所有这些都是通过公共网络完成的。如何保证网上传输数据的安全和交易对方的身份确认是电子商务能否得到推广的关键，这正是 SET 所要解决的最主要的问题。一个包括完整的购物处理流程的 SET 的工作过程如图 3-8 所示。

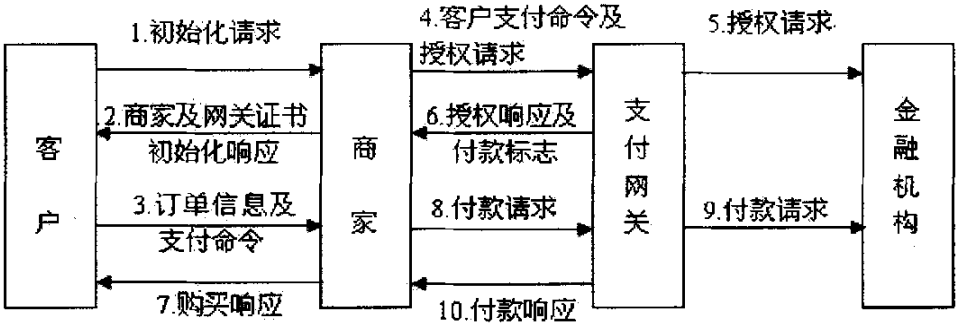

图 3-8 基于 SET 协议的交易流程图

3.5 电子支付的安全设计

3.5.1 数据的私有安全性设计

数据的私有性如果不采用特别的保护措施，那么在订购过程和支付过程中的定单信息甚至包括密码等在 Internet 中开放传输的数据都可能被第三者监视和阅读。考虑到巨大的传输量和难以计数的传输途径，想任意窃听一组数据传输是不可能的，但是一些设置在 Web 服务器的黑客程序却可以查找和收集特定类型的数据。这些数据包括信用卡、存款的账号和相应的口令。同时因为 Internet 的开放性设计，数据私有性和安全性还包括数据传输之外的问题，例如连入 Internet 的数据存储网络驱动器的安全性，所以任何存储在 Web 服务器上的数据必须采取保护措施。

其保护措施是采用在客户向商家订购或支付过程中，客户填写定单，包括项目列表、价格、总价、运费、搬运费和税费，定单可通过电子化方式从商家传过来，或由客户的电子购物软件建立。其次商家根据定单形成账单，然后商家将账单和确认单发送到客户的金融机构请求支付认可。其中，客户和商家之间需进行双向身份认证，定单、账单、确认单进行数字签名，同时利用双重签名技术保证商家看不到客户的账号信息，即被发送文件用 Hash 编码加密产生 128bit 的数字摘要。发送方用自己的私用密钥对摘要再加密，这就形成了数字签名。将原文和加密的摘要同时传给对方，对方用发送方的公共密钥对摘要解密，同时对收到的文件用 Hash 编码加密产生又一摘要。将解密后的摘要和收到的文件在接收方重新加密产生的摘要相互对比。如两者一致，则说明传送过程中信息没有被破坏或篡改过，否则不然。其身份认证与数据加密过程如图 3-9 所示：

3.5.2 数据的完整性安全设计

由于 Internet 的开放体系，如果某些黑客或有意破坏者具备了特定的知识和工具完全可以更改传输中的数据，从而破坏数据的完整性。因此，要采取适当的存取访问控制，以保证数据存取系统的安全。在电子商务中务必保存数据最初的格式和内容。它的保护措施是采用在客户向商家订购或支付过程中，商家从客户的金融机构请求支付，其安全需求包括商家与银行之间的双向身份认证。保证除商家外的任何第三方均不能了解账单的内容，除商业银行外的任何第三方均不能了解支付信息的内容，同时对支付信息进行数字签名以及支付信息应包括解决争议的足够信息。商业银行还需要对确认单进行数字签名，提供防篡改和不可否认保护。确认信息中包括发票号、交易号、转账金额和转账结果等。

3.5.3 身份认证安全设计

在电子商务的具体实现中，首先要确认当前的通讯、交易和存取要求是合法的。例如 Internet 中的计算机系统的身份是其由 IP 地址确认的。黑客通过 IP 欺骗，使用虚假的 IP 地址，从而达到隐瞒自己身份盗用他人身份的目的。在日常电子邮件的使用中可以很容易地发匿名邮件，或者使用不真实的邮件用户名。因此，在电子商务系统中必须建立严格的身份认证机制以确保参加交易各方的身份真实有效，其安全措施是采用 CCITTX.509 国际标准所规定的数字证书。

3.5.4 不可否认安全设计

不可否认主要包含数据的原始记录和发送记录，确认数据已经完成发送和接收，防止接收用户更改原始记录，或在已经收到数据以后否认收到数据，并拖延自己的下一步工作。为了保证交易过程的可操作性，必须采取可靠的方法确保交易过程的真实性，保证参加电子交易的各方承认交易过程的合法性。

3.6 系统组成及功能设计

根据参与电子商务的角色和交易流程，可以将整个电子支付系统划分为客户子系统、商家子系统、支付网关子系统、数字证书授权与认证子系统四部分组成。其系统框架结构图如图 3-10 所示。

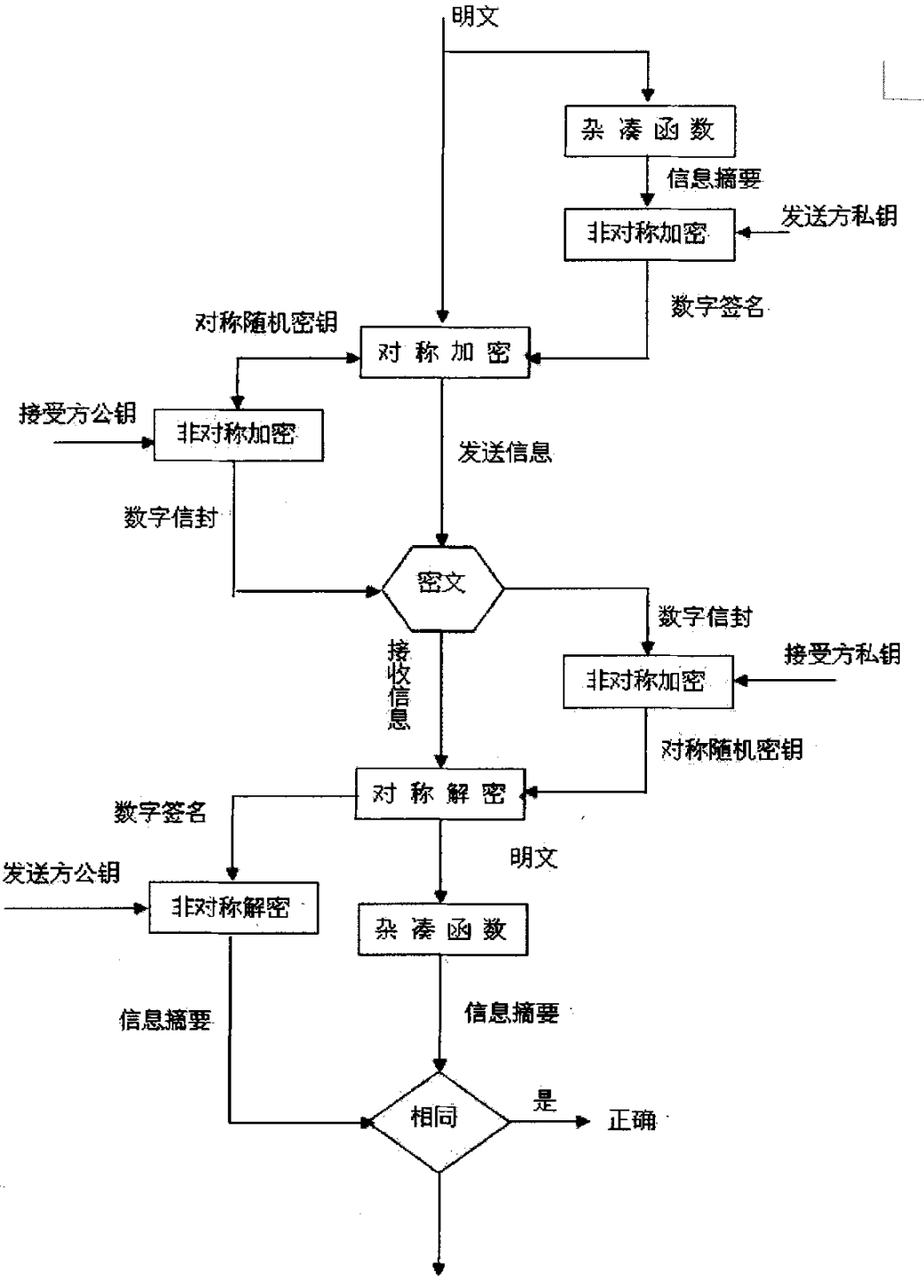

图 3-9 身份认证与数据加密过程

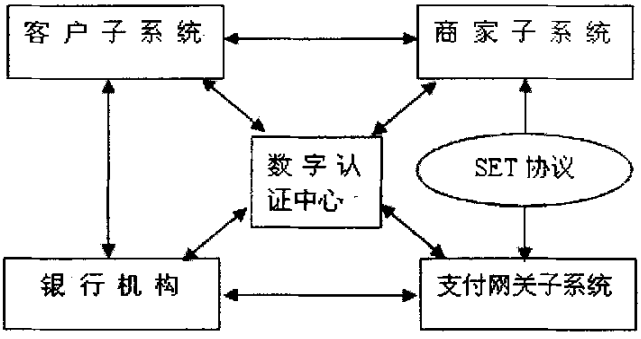

图 3-10 系统框架结构图

(1) 客户子系统。

包括与商家之间的双向身份认证、产生客户对定单的数字签名、验证商家对账单和承诺的数字签名、加解密与商家之间传递的信息。其次提供支付过程所需的安全功能，采用商业银行的公钥加密提交的转账信息、生成商家需保存的交易证据、产生对交易证据的数字签名。

(2) 商家子系统。

包括与客户之间的双向身份认证、验证客户对定单的数字签名、生成商家对账单和承诺的数字签名、加解密与购买商之间传递的信息。其次提供支付过程所需的安全功能，验证银行返回的支付结果的数字签名。

(3) 支付网关子系统。

支付网关子系统是指由银行运行的一套设备，用来处理商户的付款信息以及客户发出的付款指令。其技术特点是采用 IBM 的电子商务框架结构。本电子商务系统具有如下的安全交易特点：①遵循 SET 国际标准、具有 SET 标准规定的安全机制，是目前国际互联网上运行的比较安全的电子支付系统；⑦兼顾国内信用卡、储蓄卡与国际信用卡的业务特点，具有一定的中国特色；③具有开放特性，可与经 SETCO 国际组织认证的任何电子支付系统进行互操作。

(4) 数字证书授权与认证子系统。

客户可从公开媒体上获得商家的公开密钥，但客户无法确定商家不是冒充的，于是客户请求 CA 对商家认证。CA 对商家进行调查、验证和鉴别后，将包含商家公开密钥的证书经过数字签名传给客户。同样，商家也可对客户进行验证。

本电子支付 CA 的主要功能包括：接收注册请求、处理、批准请求和颁发证书。

第四章 电子支付相关的密码算法研究与分析

4.1 数学背景

4.1.1 初等数论

定义 1 设$a,b\in Z,a\neq 0$如果存在$c\in Z$,使得$b=ac$，则称a整除b，并称a是b的因子，b是a的倍数，记为$a|b$。

定义 2 设$a,b\in Z,a,b$不全为 0，如果$c|a$且$c|b$，则c称为a和b的公因子，所有公因子中最大的称为最大公因子，记为$\gcd(a,b)$。

定义 3 设$a,b\in Z,a,b$不全为 0，如果$a|D$，$b|D$且 D≥1,则称 D 为a和b的公倍数，其中最小的称为最小公倍数，记为$lcm(a,b)$。

定义 4 设$p\in Z,p\geq 2$,如果p只有正因子 1 和p,则称p为一个素数，否则称为合数。

定义 5 设$n\geq 1,\varphi(n)$表示在区间$[1,n]$中与n互素的整数的数目，函数$\varphi(n)$称为 Euler 函数。

定义 6 同余式 设$a,b\in Z$，如果$n|(a-b)$，则我们说a和b模n同余，记为$a\equiv b(\mathrm{mod}\,n)$整数$n$称为同余模。

定义 7 设$a\in Z_n$,如果存在$x\in Z_n$使得$ax\equiv 1(\mathrm{mod}\,n)$那么我们就说$a$是可逆的，称$x$为$a$的逆元。如果$a$是可逆的，那么容易证明其逆元是唯一的，记为$a^{-1}$。

定理 1 (Fermat 定理) 若p是素数，a是正整数且$\gcd(a,p)=1$,则$a^{p-1}\equiv 1\mathrm{mod}\,p$。

4.1.2 近世代数

4.1.2.1 群

定义 1 设 S 是一个集合，在 S 上的一个二元运算*是一个从 S×S 到 S 的映射。

定义 2 设<G,* >是代数系统,* 为二元运算。如果*运算是可结合的,存在单位元$e\in G$,并且对G中的任何元素x都有$x^{-1}\in G$,则称G为群。

一个群G是阿贝尔群或交换群或加法群，如果它还满足下列条件：对所有的$a,b\in G$有$a*b=b*a$。

定义 3　如果|G|是有限的，那么称群G是有限群，有限群的元素的个数称为它的阶。

定义4　设G是群,H是G的非空子集,如果H关于G中的运算构成群,则称H是G的子群,记作H≤G。若H是G的子群,且H$\neq G$,则称H是G的真子群,记作H<G

定义 5　设G是群,若存在$\alpha \in G$使得　$G=\{\alpha^k \mid k \in Z\}$则称$G$是循环群,记作$G=<\alpha>$,称α为$G$的生成元。

4.1.2.2 环

定义 1　设<R,+,*>是代数系统,+和*是二元运算。如果满足以下条件:

(1) <R,+>构成交换群，

(2) <R,*>构成半群，

(3) *运算关于+运算适合分配律，

则称<R,+,*>是一个环。

如果一个环<R,+,*>还满足条件：对所有的$a,b \in R$，有$a*b=b*a$,则称<R,+,*>为交换环。

定义 2 设R是环,S是R的非空子集。若S关于环R的加法和乘法也构成一个环,则称S为R的子环.若S是R的子环,且S R,则称S是R的真子环。

4.1.2.3 域

定义 1　满足下列条件的一个交换环称为一个域：所有的非零元素都有乘法逆。

有限域F_q的元素表示有两种，$q=p$或$q=2^m, m>1$。

定义 2　有限域F_p由整数集合{0，1，2，…，$p-1$ }组成，每个这样的整数可以用一个长度恰为 t=[log2p](其中[]表示不小于)的二进制表示，该表示由整数的二进制表示及在其左边添加适当个数的0组成。

定义 3　F_p^*表示F_p中所有非零元素。

定义 4　有限域$F_2{}^m$有很多构造元素个数为素数方幂的有限域的方法，我们这里利用多项式的加、乘、除和剩余来构造有限域。

令　$f(x)=x^m+f_{m-1}x^{m-1}+\cdots+f_2x^2+f_1x+f_0 \quad (f_i \in F_2, 0 \le i \le m-1)$

是F_2上次数为m的多项式的积。有限域F_{2^m}由F_2上所有次数小于m的多项式组成，即：

$$F_{2^m}=\{a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0 : a_i \in \{0,1\}\}$$

域元素(am-1xm-1 + am-2xm-2 +… a1x + a0)通常用长度为m的二进制串(am-1 am-2… a1a0)表示，使得

$$F_{2^m} = \{(a_{m-1}a_{m-2}\cdots a_1a_0) : a_i \in \{0,1\}\}$$

因此，F_{2^m} 中的元素可以用所有长度为 m 的二进制串的集合来表示。

F_{2^m} 中的元素可以用一种特殊的正规基—最优正规基(ONB)来表示，用它表示的向量可以用一个简单循环移位来完成，这个在硬件中非常容易实现。

定理 1　ONB 表示的 F_{2^m} 中元素的乘积

ONB 存在 I 型和 II 型，下面我们讨论的是 I 型

ONB 的建立过程：

(1)令 $f(x) = x^m + x^{m-1} + \cdots + x^2 + x + 1$

(2)构造 $m \times m$ 矩阵 A，A 的第 I 行，0≤i≤m-1)是对应于多项式 $x^{2^i} \bmod f(x)$ 的二进制向量。

(3)确定 A 的逆矩阵 A^{-1}。

(4)构造 $m \times m$ 矩阵 T，T 的第 i 行可按如下方法得到：首先计算多项式 $x^* x^{2^i} \bmod f(x)$,然后将对应的二进制向量表示成 V，则 T 的第 i 行是二进制向量 $V \cdot A^{-1}$。

(5)用 λ i ,j=T(j-i,i) 确定 λ i,j (0≤i,j≤m-1)的值。这里，T(i,j)表示矩阵 T 的(i,j)表值，下标用模 m 约简。每个 λ i ,j 是 F2 中的一个元素，满足：对所有 j(0≤j≤m-1),恰好只有一个 j，使得 λ i ,j=1；对每一个 i (0≤i≤m-1),恰好有两个不同的 j,使得 λ i ,j=1。

4.2 对称密码

密码体制从原理上可分为两大类，即对称密码体制和非对称密码体制。

对称密码体制的加密密钥和解密密钥相同。采用对称密码体制的系统的保密性主要取决于密钥的保密性，与算法的保密性无关，即由密文和加解密算法不可能得到明文。换句话说，算法无需保密，需保密的仅是密钥。根据对称密码体制的这种特性，对称密码加解密算法可通过低费用的芯片来实现。密钥可由发送方产生然后再经一个安全可靠的途径送至接受收方，或由第三方产生后安全可靠地分配给通信双方。如何产生满足保密要求的密钥以及如何将密钥安全可靠地分配给通信双方是这类体制设计和实现的主要课题。

对称体制对明文消息的加密有两种方式：一是明文消息按字符(如二元数字)逐位地加密，称之为流密码；另一种是将明文消息分组(含有多个字符)，逐组地进行加密，称之为分组密码。

最常用的对称密钥算法是数据加密标准 DES，它是由 IBM 公司在美国国家安全局授意之下研制的一种使用 56 位密钥的分组密码算法，1997 年被公布成为

美国政府的商用加密标准。DES 的主要问题是密钥长度较短，已不适合当今分布式开放网络对数据安全性的要求。1998 年美国政府终于决定不再继续延用 DES 作为联邦加密标准；一种新的、安全强度高、适合软硬件实现的高效加密标准—高级数据加密标准 AES 应运而生。

AES(advanced encryption standard)即高级加密标准，是一种非保密的、可以公开技术细节的、全球免费使用的分组密码算法。1997 年 9 月 12 日，美国联邦登记处公布了正式征集 AES 候选算法的通告。对 AES 的基本要求是：比三重 DES 快、至少与三重 DES 一样安全、数据分组长度为 128 比特、密钥长度为 128/192/256 比特。经过 3 年多讨论，终于决定将 Rijndael 算法作为新的 AES。

Rijndael 由比利时的 Joan Daemen 和 Vincent Rijmen 设计，算法的原型是 Square 算法，它的设计策略是宽轨策略。宽轨迹策略是针对差分分析和线性分析提出的，它的最大优点是可以给出算法的最佳差分特征的概率及最佳线性逼近的偏差的界；由此，可以分析算法抵抗差分密码分析及线性密码分析的能力。

下面介绍一下该算法的设计思想及算法描述。

4.2.1 AES 算法设计思想

Rijndael 密码的设计满足以下三条准则：

- 抵抗所有已知的攻击
- 在多个平台上速度快，编码紧凑。
- 设计简单。

当前的大多数分组密码，其轮函数是 Feistel 结构，即将中间状态的部分比特不加改变地简单放置到其他位置。Rijndael 没有这种结构，其轮函数是由 3 个不同的可逆平均变换组成的，称它们为 3“层”。所谓“均匀变换”是指状态的每个比特都是用类似的方法进行处理的。不同层的特定选择大部分是建立在“宽轨迹策略”的应用基础上的。简单地说，“宽轨迹策略”就是提供抗线性密码分析和差分密码分析能力的一种设计。为实现“宽轨迹策略”，轮函数 3 个层中的每一层都有它自己的功能：

- 线性混合层　确保多轮之上的高度扩散；
- 非线性层　将具有最优的“最坏情况非线性特性”的 S 盒并行使用；
- 密钥加层　单轮子密钥简单地异或到中间状态上，实现一次性掩盖。

在第一轮之前，用了一个初始密钥加层，其目的是在不知道密钥的情况下，对最后一个密钥加层以后的任一层可简单地剥去，因此初始密钥加层对密钥的安全性无任何意义。

为了使加密算法和解密算法在结构上更加接近，最后一轮的线性混合层与前

面各轮的线性混合层不同，这类似于 DES 的最后一轮不做左右交换。可以证明这种设计不以任何方式提高或降低该密码的安全性。

4.2.2 AES 算法描述

AES 是美国在世界范围内公开征集的新一代数据加密标准，于 2001 年 5 月正式颁布使用。AES 是一种对二进制数据进行加密的算法，数据分组长度可为 128 位、192 位或 256 位，密钥长度可为 128 位、192 位或 256 位，数据分组长度和密钥长度可独立选择，并由数据分组长度和密钥长度决定加密圈数 N 为 10、12 或 14 圈 c 明文经过 N 圈的 S 盒变换、行移位变换、列混淆变换、圈密钥加密变换等编码过程输出密文。

当数据分组长度和密钥长度均为 128 位时，要加密的数据分成 128 位一组，按每行 4 个字节排成 4 行，称为一个状态，数据的写入和读出均按列优先顺序，以字节为单位操作；将明文数据分组后，对每一个分组都有要进行 10 圈加密，每一圈要进行如下变换：S 盒变换 BYTESUB、行移位变换 SHIFTOW、列混淆变换 MIXCOLUMN、圈密钥加密变换 ADDROUNDKEY，最后一圈要少做第 3 步的列混淆变换。

其中 s 盒变换：首先把要加密的每个字节都用其 $GF(2^8)$逆元素来代替，并规定“00”的逆元素就是“00”，再进行一次仿射运算。

行移位变换：状态中第一行不移，第二行移 1 字节，第三行移 2 字节，第四行移 3 字节。

列混淆变换：把状态的列看成 $GF(2^8)$上的多项式 A(X)，然后把它与固定多项式 C(X)相乘，再进行 $MOD(X^4+1)$，其中

C(X)=“03” X^3+“01” X^2+“01” X+“02” 。

4.3 非对称密码

非对称密码又称公钥密码，即密钥分为公钥和私钥，因此称双钥体制。双钥体制的公钥可以保密也可以公开，当一对密钥中公开一半密钥时称公钥密码，而当一对密钥全部作为秘密变量时则称双钥密码。公钥密码的出现，为密码的发展开辟了新的方向。公钥算法虽然已经历了 20 多年的发展，但仍具有强劲的发展势头，在鉴别系统和密钥交换等安全技术领域起着关键的作用。

公钥密码的种类很多，这里只介绍具有代表性的三种算法体制：基于整数分解难题(IFP)的算法，基于离散对数难题(DLP)的算法；基于椭圆曲线离散对数(ECDLP)的算法。

4.3.1 基于 IFP 的 RSA 算法分析

令 p 和 q 是随机选取的两个大素数(大约为十进制 100 位或更大)，n=pq，n 是公开的，而 p，q 是保密的。我们知道 Euler 函数$\varphi(n)=(p-1)(q-1)$，但如果不知道 n 的因子分解，就不能利用这个公式计算。随机选取一个数 e，e 为小于$\varphi(n)$且与它互素的正整数。

利用辗转相除法，可以找到整数 d 和 r，使

$ed+r\varphi(n)=1$　　即　　$ed \equiv 1 \bmod \varphi(n)$

数 n，e 和 d 分别称为模、加密密钥和解密密钥。数 n 和 e 组成公钥，而其余的项 p，q，$\varphi(n)$，和 d 组成了秘密陷门 ，私钥。很显然，陷门信息包含了四个相关的项。例如，如果知道了 p，其余三项立即可以求出。如果不知道$\varphi(n)$，由已知的加密密钥 e，很难算出解密密钥 d。若知道$\varphi(n)$，则由

$$pq=n \qquad p+q=n-\varphi(n)+1$$

可知 p，q 是二次方程 $X2+(\varphi(n)-n-1)X+n=0$ 的根，可以算出 p 和 q，从而将 n 因子分解。所以 RSA 公钥密码的安全性与因子分解密切相关，若能知道 n 的因子分解，该密码就能被破译。因此，要选用足够大的 n ,使得在当今条件下要分解它是困难的。

为加密信息 m，首先将它分成小于 n 的数据块，即如果 p 和 q 都为十进制 100 位的素数，则 n 刚好在 200 位以内，因此每个数据块 m_i 的长度也应在 200 位以内。加密信息 c 由类似划分的同样长度的数据块组成。加密公式为

$c_i=m_i^e \bmod n$

要解密信息，取每个加密块 c_i 并计算

$m_i=c_i^d \bmod n$

因为 $ed \equiv 1 \bmod \varphi(n)$，因此

$$c_i^d \equiv (m_i^e)d \equiv m_i^{1-r\varphi(n)} \equiv m_i (m_i^{\varphi(n)})^{-r} \equiv m_i \bmod n = m_i$$

其中，r 为整数。这里,利用了 Euler 定理：$m_i^{\varphi(n)} \equiv 1 \bmod n$。以上公式从密文恢复出了明文。

信息用 d 加密与用 e 解密一样容易。表 4-1 总结了 RSA 加密、解密算法

表 4-1 RSA 加密、解密算法

公钥	n:素数 p 和 q 的乘积 e:与(p-1)(q-1)互素
私钥	d:e-1mod((p-1)(q-1))
加密	c=me mod n
解密	m=cdmod n

下面举一个简单的例子来阐述一下 RSA 加密、解密算法。

如果 p=47,q=71，则 n=pq=3337。随机选取加密密钥 e，e 与(p-1)(q-1)=46×70=3220 无公因子，如取 e=79,则

$$d=79^{-1}\bmod 3220=1019$$

d用扩展的Euclidean算法计算(因为1019×79=80501, 80501÷3220=25余1)。

公开 e 和 n,将 d 保密，隐藏 p 和 q。设需要加密的信息为 m=688232

首先将它分成小块，每三位分成一块，所以 m_1=688，m_2=232。

以第一块为例，对它加密为 $68879\bmod 3337=1570=c_1$

解密密文需要用解密密钥 1019 进行同样的指数运算，所以

$$15701019\bmod 3337=688=m_1$$

4.3.2 基于 DLP 的 ElGamal 算法分析

4.3.2.1 离散对数问题

对实数来说，取幂运算(b^x)不比它的逆运算($\log_b x$)容易很多。但对有限域，诸如整数单位群(Z|nZ)*,n 是一个合数或有限域 F_q 乘法群 F_q^* 来讲，用取幂算法，可以相当快地对较大的整数 x 计算出 b^x，但如果给定一个元素 y ，且已知存在一个整数 x，对一固定的基 b，有 $y=b^x$，但如何求出 x，则是一个非常困难的问题。这个问题就是离散对数(DLP)。“离散”是为了将有限域的情形与传统的(如实数上的对数问题)情形区别开来。

定义 1　离散对数问题是指：给定一个素数 p，Z_p^* 的一个生成元 α 及一个元素 $\beta \in Z_p^*$，寻找整数 x(0≤x≤p-2)，使得 $\alpha^x \equiv \beta \bmod p$。

上述定义也可以推广到任意的有限循环群上。

与离散对数问题密切相关的是 Diffie-Hellman 问题，它对公钥密码是很重要的，因为该问题显而易见的难解性，构成了包括 Diffie-Hellman 密钥分配，ElGamal 公钥密码等在内的很多密码体制安全性的基础。

定义 2　Diffie-Hellman 问题是指：给顶一个素数 p，Z_p^* 的一个生成元 α 及元素 $\alpha^a \bmod p$ 和 $\alpha^b \bmod p$，求 $\alpha^{ab} \bmod p$。

4.3.2.2 ElGamal 加密算法

ElGamal 加密算法是基于离散对数问题和 Diffie-Hellman 问题的难解性。

首先每个使用者(用 A，B 表示)按如下方法生成自己的一对公钥和相应的私钥。

生成一个大的随机素数 p 和整数模 p 的乘法群 Z_p^* 的一个生成元 α。

选取一个随机整数 a(1≤a≤p-2)，计算 $\alpha^a \bmod p$。

A 的公钥(p, α, α^a);A 的私钥是 a 。

假设 B 加密信息 m 给 A，A 解密，用 ElGamal 加密算法的加密、解密过程如下：

(1)B 执行如下步骤：

获取 A 的真实公钥(p, α, α^a)；

将消息 m 表示成{0，1，…，p-1}范围内的整数；

选取随机整数 k(1≤k≤p-2);

计算 $\gamma=\alpha^k \bmod p$ 和 $\delta=m(\alpha^a)k \bmod p$;

发送密文 c=(γ，δ)给 A 。

(2)为从 c 中恢复出明文 m，A 执行：

使用私钥 a 计算 $\gamma^{p-1-a} \bmod p$($\gamma^{p-1-a} \bmod p=\gamma^{-a}=\alpha^{-ak}$);

通过计算 $\gamma^{-a}\,\delta \bmod p$ 恢复出 m(因为$(\gamma^{-a})\cdot\delta\equiv\alpha^{-ak}m\,\alpha^{ak}\equiv m \bmod p$) 。

下面我们举个例子来说明 ElGamal 加密算法：

生成密钥：使用者 A 选取素数 p=2357 及 Z_{2357}^* 的生成元 α=2,A 选取私钥 a=1751 并计算

$\alpha^a \bmod p=22357 \bmod 2357=1185$ 。

A 的公钥是 p=2357，α=2，α^a=1185。

加密过程：为加密信息 m=2035,B 选取一个随机整数 k=1520 并计算

$$\gamma=21520 \bmod 2357=1430$$

$$\delta=2035\times 11851520 \bmod 2357=697$$

B 发送 γ=1430 和 δ=697 给 A。

解密过程：为解密，A 计算

$$\gamma^{p-a-1}=1430605 \bmod 2357=872$$

并做下面的计算来恢复 m=872×697 mod 2357 =2035

4.3.3 基于 ECDLP 的椭圆曲线算法分析

4.3.3.1 椭圆曲线的定义

所谓椭圆曲线指的是由维尔斯特拉斯(Weiertrass)方程：

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \qquad (*)$$

所去顶的平面曲线。若 F 是一个域，$a_i\in F, i=1,2,\cdots\cdots 6$ 满足(*)数偶(x,y)称为 F 域上的椭圆曲线 E 的点。F 域可以是有理数域，也可以是复数域，还可以是有限域 GF(p^r).椭圆曲线通常用 E 表示。除了曲线 E 的所有点外，尚需加上一个

叫做无穷远点的特殊点 O 。若令

$x = X/Z, y = Y/Z$ 以之代入(*)得

$(Y/Z)^2 + a_1(XY/Z^2) + a_3(Y/Z) = (X/Z)^3 + a_2(X/Z)^2 + a_4(X/Z) + a_6$

当 Z≠0 时，整理得：

$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$

显然(x,y)和(X,Y,Z)是相对应。而且任取一非零常数 λ ,使得(X,Y,Z)和(λ X, λ Y, λ Z)表达同一个点。但若 Z=0 时，以(0，1，0)为例，它可以看作是(0，1，ε)，当 ε →0 而得到的，相应的可以理解为沿 y 轴趋向无穷远。

在实际的密码学应用中，主要研究和应用的椭圆曲线方程有以下两种：

有限域上的椭圆曲线 F_P(表示 p 个元素的有限域)

$y^2=x^3+ax+b$　其中 $a,b \in F_P$, $4a^3+27b^2 \neq 0$

有限域上的椭圆曲线 F_{2^m}

$y^2+xy=x^3+ax^2+b$　其中 $a,b \in F_{2^m}$，$b \neq 0$

4.3.3.2 椭圆曲线上的离散对数问题

令 E 是定义在 F_q(q=p,p 是素数，或 $q=2^m$，m>1)上的椭圆曲线，若给定一条有限域 F_q 上的椭圆曲线 $E(F_q)$，G 为 E 上的一点，则 E 上关于 G 的 ECDLP 为：给定一点 Q，求解整数 r 使得 rG＝Q(rG 倍乘，即 r 个 G 相加)。对该系统的攻击依赖于在 F_q 上求解方程：Gr=Q mod P 或 r＝logG Q mod P。DLP 求解是非常困难的，ECDLP 比有限域上的 DLP 更难求解。在 F_q 上选择一条椭圆曲线 E 及一个具有较高阶的基点 $G \in E(F_q)$，计算该点的倍乘 rG，相对来说较容易，们已知 G 和 rG 要求 r 则是很困难。基于椭圆曲线密码的安全性最终归结为解 ECDLP 问题。当数据量足够大以至此 ECDLP 问题无法解决时，认为该密码体制是安全的。

4.3.3.3 椭圆曲线上点的加法运算

在 E 上定义“+”运算，P＋Q＝R，R 是过 P、Q 的直线与曲线的另一交点关于 x 轴的对称点，当 P＝Q 时 R 是 P 点的切线与曲线的另一交点关于 x 轴的对称点。这样，(E, +)构成可换群(Abel 群)，O 是加法单位元(零元)。下面的图 4-1、图 4-2 分别为“+”运算的几何意义。

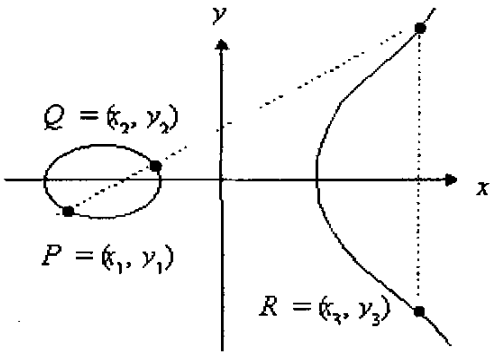

图 4-1 椭圆曲线上的加法: P + Q = R

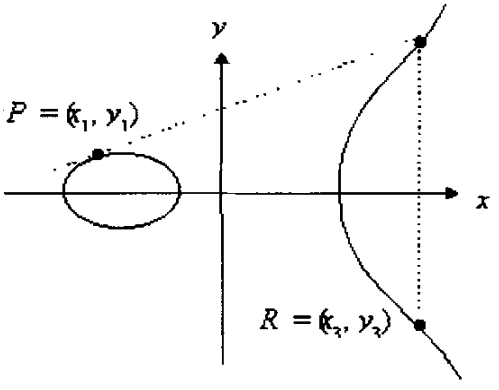

图 4-2 椭圆曲线上一点的 2 倍: P + P = R.

4.3.3.4 F_p 上的椭圆曲线

设 F_p 是一个特征 $p\neq 2,3$ 的有限域，a，$b\in F_p$ 满足 $4a^3+27b^2\neq 0$ 。则椭圆曲线 $E(F_p)$ 满足方程 $y^2=x^3+ax+b$ 的点$(x,y)\in F_p\times F_p$和“无穷远点”所组成的点的集合。这些点在下面定义的加法运算下构成一个 Abelian 群：

(1)O+O=O;

(2)$\forall (x,y)\in E(F_p)$, $(x,y)+O=O+(x,y)$;

(3)$\forall (x,y)\in E(F_p)$, $(x,y)+(x,-y)=(x,-y)+(x,y)=O$;

(4)设$(x_1,y_1)\in E(F_p)$, $(x_2,y_2)\in E(F_p)$满足 $x_1\neq x_2$,则

$(x_1,y_1)+(x_2,y_2)=(x_2,y_2)+(x_1,y_1)=(x_3,y_3)$，其中 $x_3=\lambda^2-x_1-x_2$，

$y_3=\lambda(x_1-x_3)-y_1$ ，$\lambda=(y_2-y_1)/(x_2-x_1)$;

(5)设$(x_1,y_1)\in E(F_p)$，则 $2(x_1,y_1)=(x_3,y_3)$，其中 $x_3=\lambda^2-2x_1$ ，

$y_3=\lambda(x_1-x_3)-y_1$，$\lambda=(3x_1^2+a)/(2y_1)$。

由定义可知群运算的单位元是 O

4.3.3.5F_{2^m}上的椭圆曲线

定义在特征为 2 的有限域上的非超奇异椭圆曲线 $E(F_{2^m})$定义为：满足方程 $y^2+xy=x^3+ax^2+b$ 的点$(x,y) \in F_{2^m}\times F_{2^m}$和“无穷远点”所组成的点的集合。这些点在下面定义的加法运算下构成一个 Abelian 群：

(1)O+O=O;

(2)$\forall (x,y)\in E(F_{2^m})$, $(x,y)+O=O+(x,y)=(x,y)$;

(3)$\forall (x,y)\in E(F_{2^m})$, $(x,y)+(x,-y)=(x,-y)+(x,y)=O$;

(4)设$(x_1,y_1)\in E(F_{2^m}), (x_2,y_2)\in E(F_{2^m})$满足 $x_1\neq x_2$,则

$(x_1,y_1)+(x_2,y_2)=(x_2,y_2)+(x_1,y_1)=(x_3,y_3)$，其中 $x_3=\lambda^2+\lambda+x_1+x_2+a$,

$y_3=\lambda(x_1+x_2)+x_3+y_1$， $\lambda=(y_2+y_1)/(x_2+x_1)$;

(5)设$(x_1,y_1)\in E(F_{2^m})$，则 $2(x_1,y_1)=(x_3,y_3)$，其中 $x_3=\lambda^2+\lambda+a$,

$y_3=x_1^2+(\lambda+1)x_3$， $\lambda=(x_1+y_1/x_1)$。

由定义可知群运算的单位元是 O

4.3.3.6 椭圆曲线公钥密码算法分析

1)系统的建立

选取一个基域F_q,一个定义在F_q上的椭圆曲线 E 和 E 上一个素数阶 n 的点 p。点 p 的坐标用(x_p, y_p)表示。

有限域 F_q，椭圆曲线参数，亦即域元素 a 和 b(定义椭圆曲线的参数)，点 p 和阶 n 是公开信息。

2)密钥的生成

系统建成后，每个使用者(简称实体)执行下列计算：

- 在区间[1，n-1]中随机选取一个整数 d;
- 计算点 Q=dP;
- 实体的公钥包含点 Q;
- 实体的私钥是整数 d。

3)加密过程

当实体 B 发送信息 M 给实体 A 时，实体 B 执行下列步骤：

- 查找 A 的公钥 Q;
- 将数据 M 表示成一个域元素$\in F_q$;
- 在区间[1，n-1]内选取一个随机整数 k;

- 计算点$(x_1,y_1)=kP$；
- 计算点$(x_2,y_2)=kQ$ ；
- 计算 $c=mx_2$ ；
- 传送加密数据(x_1,y_1,c)给 A 。

4)解密过程

当实体 A 解密从 B 收到的密文(x_1,y_1,c)时，A 执行下列步骤：

- 使用它的私钥 d，计算点$(x_2,y_2)=d(x_1,y_1)$；
- 通过计算 $m=c\,x_2^{-1}$,恢复出数据 m。

下面举个例子来直观的解释一下上面的算法，考虑到计算的复杂性，所以我们用正规基表示，这样可以极大的加快椭圆曲线公钥密码的实现速度。

例 3 F_2^4 上的一条椭圆曲线(其中的元素用最优正规基 ONB 来表示)，F_2^4 中的元素是由多项式 $f(x)=x^4+x+1$ 的根 $\alpha=x$ 生成的区域，则 α=(1100)是非零元素的一个生成元，(1111)是乘法单元。

所以 $F_{2^4}^*$ 可以由 α 的幂来表示，即：

$\alpha^0=(1111)\alpha^1=(1100)\alpha^2=(0110)\alpha^3=(0100)\alpha^4=(0011)\alpha^5=(1010)$

$\alpha^6=(0010)\alpha^7=(0111)\alpha^8=(1001)\alpha^9=(1000)\alpha^{10}=(0101)\alpha^{11}=(1110)$

$\alpha^{12}=(0001)\alpha^{13}=(1101)\alpha^{14}=(1011)\quad \alpha^{15}=\alpha^0=(1111)$

对于方程 $y^2+xy=x^3+ax^2+b$，令 $a=0$, $b=\alpha^3$,

考虑 F_2^4 上由方程 $y^2+xy=x^3+\alpha^3$ 定义的非超奇异曲线。

椭圆曲线方程在 F_2^4 上的解是$(0,\alpha^9)$，(α,α)，(α^3,α^5),(α^5,α^3),(α^5,α^{11}),(α^6,α^6),$(\alpha^6,0)$等共有 20 个元素，它们一起构成阶为 20 的循环群。

1)系统的建立

选取基域 F_2^4(用 ONB 表示)，选取点 $P=(x_p,y_p)=(\alpha^5,\alpha^{11})$。由于 5P=O，所以点 P 的阶 n=5。

2)密钥的生成

实体 A 执行下列步骤：

- 选取区间[1，4]中一个随机整数 d=3；
- 计算点 Q=dP=3P=(α,0)=((1100),(0000))；
- 将点 Q 公开；
- A 的私钥是整数 d=3。

3)加密过程

当实体 B 发送数据 M=0111 给实体 A 时，B 执行下列步骤：

- 查找 A 的公钥：$Q=(x_0,y_0)=(\alpha,0)$；
- 将数据 M 表示成一个域元素 $m=\alpha^7$；
- 在区间[1,4]中选取一个随机整数 k=2；
- 计算点 $2P=(x_1,y_1)=(\alpha,\alpha)=((1100),(1100))$；
- 计算点 $2Q=(x_2,y_2)=(\alpha^5,\alpha^{11})=((1010),(1110))$；
- 计算 $c=mx^2=\alpha^7\alpha^5=\alpha^{12}=(0001)$；
- 传送加密数据$(x_1,y_1,c)=(\alpha,\alpha,\alpha^{12})=((1100),(1100),(0001))$给 A。

4)解密过程

当实体 A 解密从 B 收到的密文 $c=(\alpha,\alpha,\alpha^{12})$时，A 执行下列步骤：

- 计算点 $d(x_1,y_1)=3(\alpha,\alpha)=(\alpha^5,\alpha^{11})=((1010),(1110))=(x_2,y_2)$ ；
- 恢复数据 $m=c\,x_2^{-1}=\alpha^{12}\alpha^{-5}=\alpha^7=(0111)$。

第五章 电子现金协议的相关理论基础

5.1 哈希函数

哈希函数又称“散列函数’，散列函数可以将任意长度的二进制串映射为固定长度的二进制串〔称为散列值)。散列函数应该是易于计算的，而且是公开的，散列函数的保密性基于其单向性。散列函数在现代密码学中具有广泛的应用，在签名方案中，散列函数可以将任意长度的二进制串映射为签名算法所要求的长度:在知识证明系统中，散列函数可以替代验证者从而构造非交互式签名方案。

定义1 散列函数:将任意有限长度的二进制串映射为固定长度1的二进制串的函数，即 H : $\{0,1\}^* \rightarrow (0,1)^l$，该函数具有下列特性:

1)公开性：H()的描述是公开的，其处理过程无需保密；

2)单向性：给定 x，计算其散列值 c = H(x)是容易的；但是，给定散列值 c，找到满足 H(x) = c 的 x 在计算上是困难的；

如果还具备强无碰撞特性条件：找到满足 H(x) = H(x')和 x'≠x 的消息 x'和 x 在计算上是困难的，则称为抗碰撞散列函数。

散列函数的坚固性因不同的安全性需求而不同。假设计算逆的最好的算法是强力攻击，则坚固性主要取决于输出的比特数。由生日攻击，在 $2^{1/2}$ 个散列值中找到一个碰撞的概率为 1/2，因此 160 比特的散列函数值已经能够满足一般的安全性要求。现有的密码散列函数可分为两种：

1) 分组密码的散列函数，如基于 IDEA；

2) 专门设计的散列函数，如 SHA-1；

SHA 是美国国家标准与技术局与美国国家安全局共同设计的一个与美国数字签名算法(DSA)一起使用的安全哈希算法，1993 年 5 月 11 日起被采纳为标准，1994 年 7 月 11 日作了一次修改，1995 年 4 月 17 日正式公布，改名为 SHA-1 。SHA 的设计原则与 MD4 算法的设计原则极其相似，似乎是 MD4 算法的一种变形，但 SHA 的设计者没有公开 SHA 的详细设计准则。SHA 的输入的长度限制在 2 64 比特之内，输出长度为 160 比特。

尽管 MD5 算法已经被破解，这也就意味着 SHA-1 也很快就变的不可信任，但它仍然是当今网络安全中最安全的散列函数，所以下文中用到的散列函数即为 SHA-1。

5.2 交互式证明

交互式证明系统是证明者(Prover，用 P 表示)向验证者(Verifier，用 V 表示)证明一个命题的正确性。交互式证明过程通常包含多次“询问一应答”交互，在协议执行结束时，验证者要么拒绝，要么接受证明者的证明，验证者的判断取决于证明者是否正确回答了验证者的所有询问。交互式证明系统通常分为以下两种类型:

1)身份证明系统(proof of membership)：P 向 V 证明某一输入 I 属于某一集合 L,即 $I \in L$ 。这种交互式证明系统最先由 Goldwasser, Micali 和 Rackoff 提出[25]

2)知识证明系统(proof of knowledge)：给定输入为 h, P 向 V 证明他知道某个证据满足一个多项式时间命题 Pr ed (x, h) = true。

在这里我们重点讨论在电子现金中广泛采用的三步认证协议。

5.2.1 零知识身份证明

零知识证明最初是由Goldwasser等人[25]在80年代初提出的。在这类协议中，证明者向验证者证明某个命题的正确性，却不向验证者泄漏关于命题的任何有用的信息。零知识证明可以是交互的，也可以是非交互的。零知识身份证明是一种具有零知识特性的身份证明系统，通常是交互式方式。一个零知识身份证明系统必须满足以下三个条件:

1)完备性(completeness):如果$I \in L$,那么V以极大的概率接受P的命题。

2)合理性(soundness):如果$I \notin L$，那么V以极大的概率拒绝P的命题。

3)零知识特性(zero-knowledge)：V无法获得P的任何有用的秘密信息

5.2.2 三步认证协议

三步认证协议是交互式知识证明系统的一个特例，因为它具有以下两个特性:

1) P和V之间的交互操作包括三个步骤;

2)给定公共输入h的证据为x，满足Pred(x, h) = true，则x代表P的秘密身份。

令$(\psi, \oplus, 0)$和$(\tau, \otimes, 1)$为两个阿贝尔群，f为一个单向同态f: $\psi \rightarrow \tau$，即:

$$\forall x, y \in \psi, f(x \oplus y) = f(x) \otimes f(y)$$

假设群ψ中的$\oplus$操作和群τ中的$\otimes$操作都是可有效计算的和可逆的，同时假定存在有效算法来验证群中元素的从属关系和验证群中两个成员是否相等。此外，还假定存在一个从ψ中选取伪随机数的高效算法。-x为$x \in \psi$关于操作$\oplus$的

逆元，也就是：

$-x \oplus x = x \oplus (-x) = 0$，这里0表示群$\psi$的单位元。对于任何正整数常量c及任意$x \in \psi$，cx表示$x \oplus \ldots \oplus x$（c次）。任取$h \in \tau$，$h^c$表示h.....h（c次）。

三步认证协议实际上就是一种交互式零知识证明：P知道证据$x \in \psi$，满足

$h = f(x)$，这里$h \in \tau$是公共输入，P要向V证明他知道证据x，但又不能向V泄漏任何有关x的知识。协议的具体执行流程如图所示，三步认证协议也是采用“询问一响应”模式：P首先向V发送一个承诺a，V随机选择c作为询问发送给P，其中t是安全参数，P计算响应：再发送给V，V验证等式$f(r) \otimes h^c = a$是否成立，如果成立则说明P知道证据x 。

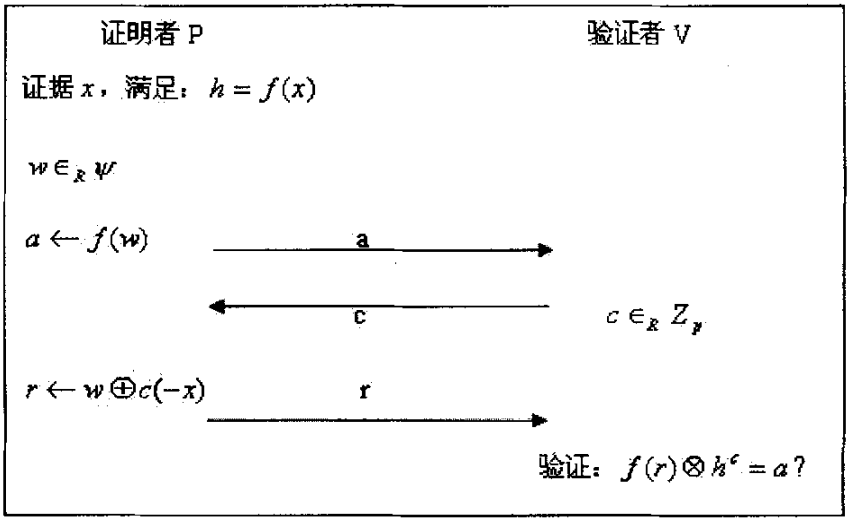

图5-1 三步认证协议

交互式知识证明的形式化证明最先由Feige，Fiat和Shamir[26]以及Tompa和wol1[26]分别提出。下面我们从完备性、合理性、证据不可区分性和证据保密性这四个方面来证明三步认证协议。对这些特性的一般描述如下所述：

1)完备性：如果p知道证据$x \in \psi$，$h \in \tau$，则P能以极大的概率使V信服。事实上，如果P知道某个$x \in \psi$，他就能正确计算r，这样必然有：

$f(r) \otimes h^c = f(r) \otimes (f(x))^c = f(r) \otimes f(cx) = f(r \oplus cx)$

$= f(\omega \oplus c(-x) \oplus cx) = f(\omega \oplus c(-x \oplus x)) = f(\omega \oplus 0) = f(\omega) = a$

从而，验证必然通过。

2)合理性：如果p不知道任何满足$h = f(x)$的证据x，则他只能以可忽略不计的概率使V信服。

3)证据不可区分性：即使V知道所有的证据也不能辨认出p用的是哪一个据。

4)证据保密性：V应该不能从与P的交互中获得关于证据的任何信息，知识证

明系统的这一特性称为证据保密性[27]。如果在协议执行前V不知道关于输入h的证据，则即使她参与到具体的协议中也无法求解出新的证据。

Feige, Fiat和Shami:对完备性和合理性给出了正式的定义[26]。关于证据不可区分性和证据保密性的正式定义由Feige和Shami:给出[27]。

5.2.3 表示问题的知识证明

1)表示问题的知识证明

表示问题的知识证明即为:证明者P向验证者V证明他知道$y = g_1^{a_1} g_2^{a_2}$，但是又不向V揭示a_1和a_2。该证明采用一种零知识证明的方法，具体流程如图5-2所示。

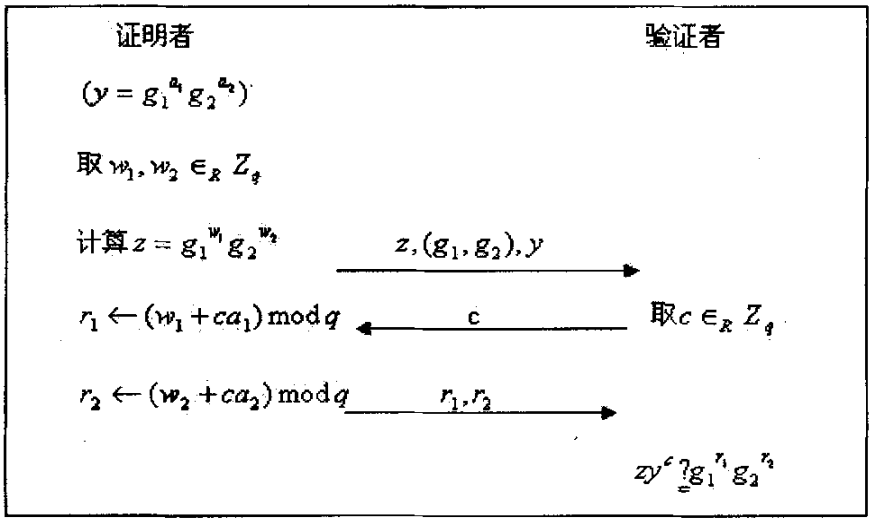

图5-2表示问题的知识证明

5.3 数字签名技术

5.3.1 数字签名方案

在电子支付过程中，为了保证电子商务活动的安全性，必须对交易主体的身份进行认证，在电子环境下能够实现手工签名功能的数字签名技术应运而生，数字签名技术能够比较完美地实现手工签名的基本功能，具有以下特点:可信性、不可伪造性、不可重用性、不可更改性、不可抵赖性。在我们的电子支付中，会在很多地方用到数字签名技术。本节主要介绍论文中将会用到的几种签名方案:签名方案和 Schnorr 签名算法。

Schnorr 签名方案

(1) 体制参数

G_q 是阶为 q 的有限循环群，$g \in G_q$ 是 G_p 的生成元。签名者的私钥是 x，签名者的公钥为 $y = g^x$，散列函数为 $H:\{0,1\}^* \rightarrow Z_q$，在 G_q 中计算离散对数问题是困难的。

(2) 签名的产生过程

对于待签字的信息 m，签名者执行以下步骤：

- 选择随机数：$r \in_R Z_q$，计算 g^r。
- 计算 $c=H(m \| g^r)$。
- 计算 $s \equiv r-cx \pmod q$。

以(c,s)作为产生的数字签名。

(3) 签名验证过程

- 接收方在收到消息 m 和数字签名(c,s)后，先计算 $g^s y^c$，然后计算 $H(g^s y^c \| m)$,并按下式验证

$Ver(y,(c,s),m)=true \Leftrightarrow H(m \| g^s y^c)=c$

其正确性可由下式证明：

$g^s y^c \equiv g^{s+xc} \equiv g^{r-xc+xc} \equiv g^r$ 。

5.3.2 盲数字签名

盲数字签名是具有下列两个特性的一种数字签名方案：(1)消息的内容对签名者是盲的；(2)在签名被接收者泄露后，签名者不能追踪签名。

盲数字签名在签名时，接收者首先将被签名的消息进行盲变换，把变换后的消息(称为盲消息)发送给签名者，签名者对盲消息进行签名并把消息发送还给接收者，接收者对签名再做逆盲变换，得出的消息即为原消息的盲签名。这个过程如下所示：

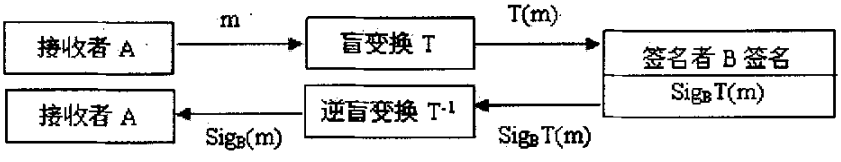

图 5-3 盲数字签名的签名过程

盲变换实现了盲数字签名的特性(1)要实现盲数字签名的特性(2)必须要求当签名者后来看到盲签名时不能与盲消息联系起来。

schnorr 盲签名方案

运用 Okamoto 和 Ohta 提出的可转移的零知识证明，可以根据基于交互式零知识身份识别方案的签名方案来构造盲数字签名方案，其中较典型的是最早由

Okamoto 提出的 Schnorr 盲签名方案。

(1) 体制参数

Schnorr 盲签名方案的系统设置、密钥产生、签名验证和 Schnorr 签名相同。设 G 是阶为 q 的有限循环群，$g \in G$ 是 G 的生成元，在 G 中计算离散对数是困难的。签名者的私钥是 x，公钥是 $y=g^x$。散列函数为 $H:\{0,1\}^* \to Z_q$，其中消息 $m \in \{0,1\}^*$，产生的签名为 $(c,s) \in Z_q \times Z_q$。

(2) 签名的产生过程

- 签名者随机选取 $\tilde{r} \in_R Z_q^*$，计算 $\tilde{t} = g^{\tilde{r}}$，并将 $\tilde{t}$ 发送给接收者。
- 接收者随机选取 $\gamma, \delta \in_R Z_q^*$ 计算 $t=\tilde{t}\, g^{\gamma} y^{\delta}$，$c=H(m \| t)$，$\tilde{c}=c-\delta \pmod q$，并将 $\tilde{c}$ 发送给签名者。
- 签名者计算 $\tilde{s}=\tilde{r}-\tilde{c}\, x \pmod q$，并将 $\tilde{s}$ 发送给接收者。
- 最后，接收者计算 $s=\tilde{s}+\gamma \pmod q$。

(3)验证过程

- 验证方程为 $c=H(m \| g^s y^c)$，证明如下。

该签名的不可伪造性由 Schnorr 签名方案的安全性保证。该签名还具有统计盲性：假设 $(m,(c,s))$ 是任意一次签名协议产生的消息 / 签名对，$(\tilde{r},\tilde{t},\tilde{c},\tilde{s})$ 是任意一次签名协议中签名者的协议信息，则签名者可以计算盲因子 $\gamma=s-\tilde{s} \pmod q$ 和 $\delta=c-\tilde{c} \pmod q$，由于 $\tilde{s}=\tilde{r}-\tilde{c}\, x \pmod q$，所以有：$g^s y^c = g^{\tilde{s}+\gamma} y^{\tilde{c}+\delta} = g^{\tilde{s}+\tilde{c}x} g^{\gamma} y^{\delta} = \tilde{t}\, g^{\gamma} y^{\delta} = t$，即 $(m,(c,s))$ 能够通过签名验证，这就说明对签名者来说任意一个通过验证的消息 / 签名对可能由任意一次签名会话产生。

5.4 知识的签名问题

知识的签名是与给定消息m唯一对应的一种构造：除了在知道秘密的某方的帮助下以外，任何人都无法得到该消息，这些秘密例如：给定的$y \in G$基于g的离散对数$(G=\langle g \rangle)$。

知识的证明是：某人让其他人相信他知道某些事实，但是实际上又不揭示该事实的一种方法。在知识的签名中，签名者将他对一个秘密的知识绑定到签名的消息中。使用知识的签名的目的有两个：对消息签名和证明一个秘密的知识。文献[28]中提出的所有的知识的签名都可以在随机预言模式下证明是安全的，且它们的交互版本是零知识的。

为了构建知识的盲签名，我们更改了文献[28]中提出的知识的签名的一些构造，适应该文献的对安全性的证明也适应于我们的知识签名。

下面我们给出在本文中将要用到的几个知识的签名及其盲签名。

定义1 离散对数的知识签名：设二元组$(c, r) \in \{0,1\}^k \times Z_n^*$满足下列等式：

$$c = H(m \| g \| h \| g^r h^c)$$

则称(c, r)是$h \in G$基于g的离散对数的知识对消息m的签名，记为：

$$SKLOG[\alpha \mid h = g^{\alpha}]$$

在随机预言模式下可以证明：如果签名者不知道$h \in G$基于g离散对数，就无法构造出满足上述等式的二元组(c, r)，下面的其它几个知识的签名也可以同样证明。

如果签名者知道一个整数、满足$x = \log_g h$，则可以按照如下步骤计算出此签名：

1)选取：$s \in_R Z_n^*$，计算$h' = g^s$；

2)计算$c = H(m \| g \| h \| h')$；

3)计算$r = (s - cx) \bmod n$。

定义2 表示问题的知识签名：设三元组$(c, r_1, r_2) \in \{0,1\}^k \times Z_n^* \times Z_n^*$；满足下列等式：

$$c = H(m \| g_1 \| g_2 \| h_1 \| g \| h \| g_1^{r_1} g_2^{r_2} h_1^c \| g_1^{r_1} h^c)$$

则称(c, r_1, r_2)为$h_1 \in G$关于底g_1，g_2的表示，且$h_1 \in G$关于g，g_1的指数与$h \in G$关于底g的离散对数相等的知识，对消息$m \in \{0,1\}^*$的签名，记为：

$$SKREP\{(\alpha, \beta) \mid h_1 = g_1^{\alpha} g_2^{\beta} \wedge h = g^{\alpha}\}(m)。$$

签名者如果知道两个整数x和y满足$h_1 = g_1^x g_2^y$和$x = \log_g h$，则可以按照如下步骤计算出此签名：

1)选取$a_1, a_2 \in_R Z_n^*$，计算$h' = g_1^{a_1}$，$h_1' = g_1^{a_1} g_2^{a_2}$

2)计算$c = H(m \| g_1 \| g_2 \| h_1 \| g \| h \| h_1' \| h')$；

3)计算$r_1 = a_1 - cx \bmod n$和$r_2 = a_2 - cy \bmod n$。

第六章 一种基于ECDLP的Brands受限盲签名的设计与实现

6.1 盲签名技术

在普通的数字签名方案中，通常是由接收者选择一个消息发送给签名者，并和签名者执行交互式签名，这种协议实际上是一种公钥证书分发协议。由于签名者知道自己签署的消息内容，他就可以将消息和签名行为联系起来。而电子现金系统的显著特点之一就是要保证用户的匿名性，也就是说，要求银行在日后无法将自己签署的电子现金与用户的身份对应起来。如果采用普通数字签名，银行可以存储签名消息(电子现金)与用户身份的对应关系，当商家在银行处存储电子现金时，银行可以将电子现金与特定的提取行为匹配，从而可以掌握用户使用电子现金的情况，用户毫无隐私可台。所以普通的数字签名不适用于电子现金支付协议，为了保护用户的隐私权，必须保证签名者(银行)对用户提交的消息进行匿名签名，即所谓“盲签名”。通常对签名进行盲变换，使得签名者在日后可以识别自己的签名，但无法将该签名和当时的签名行为相对应。

Chaum最先提出了盲签名[29]的概念及其具体实现[30]，Camenisch，Piveteau和Stadler提出了基于DSA和Nyberg-Rueppel数字签名方案的盲签名协议[31]. Stadler，Piveteau和Camenisch将盲签名的思想引入到公平盲签名中[32]，从而使得签名者和可信的第三方联合起来可以将消息和对应的签名联系起来。

盲签名是具有如下两个特性的一种数字签名方案:一是“盲性”，即消息的内容对签名者是盲的(不可见的);二是“不可追踪性”，即在签名被接收者公开后，签名者不能追踪签名。盲签名包括一个签名方案以及对签名者隐藏签名消息和签名的方法。和普通签名方案不同的是，其签名通过签名者和接收者之间的交互协议产生。

定义 1 盲签名方案:一个算法的三元组(gen，IP，ver)，其中gen是概率型算法，IP是签名者S和接收者R之间的交互协议，ver是确定型验证算法。gen 的输入是系统参数，输出是签名者S的私钥和公钥h。交互协议IP中S的输入是s，R的输入是消息m和公钥h，R的输出是m的签名σ。ver的输入是消息m、签名σ和S的公钥h,输出是true或false。

盲签名方案具有如下性质:

1)正确性:如果R和S都正确执行IP，则签名满足验证算法。

2)不可伪造性:任何人不知道私钥就不能产生正确的签名。

3) 盲性:签名者的协议信息和消息-签名对是不可链接的，即给定若干次签名会话的协议信息和若干个消息-签名对，S不能确定协议信息和消息签名对的对应关系。盲签名方案的盲性有两种:如果消息-签名对和签名者的协议信息是统计独立的，则称为统计盲性；如果链接消息-签名对和签名者的协议信息需要签名者解决计算困难问题(如离散对数问题)，则称为计算盲性。

6.2 Brands 受限盲签名方案

在电子现金方案中使用完全盲签名协议会带来一个很大的问题，即恶意用户可能会让银行在匿名情况下签署一个巨额现金。为了解决这个问题，Chaum采用“分割选择技术”[29]，但其效率非常低。Brands在盲签名协议中增加了“受限”特性，即把接受者的身份编码到要签署的消息中去，极大地提高了提取协议的执行效率。

Brands提出的受限盲签名的原理实际上很简单，我们可以用一个“两点确定一条直线”的定理来类比阐述，如图6-1所示。在消息中使用两个变量x和y，将接受者的身份作为直线的斜率:I=y/x，根据“两点确定一条直线”的定律，只有执行两次支付，才能够确定直线的斜率，也就是用户身份。

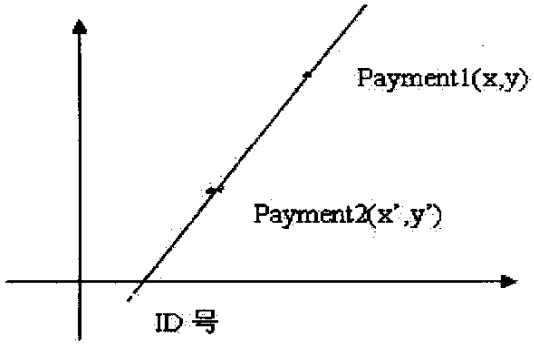

图 6-1 Brands 受限盲签名原理

Brands 受限盲签名协议是由三步认证协议、Fiat-shamir 数字签名协议、Schnorr 数字签名协议、Chaum-pedersen 数字签名协议发展而来的，其中，三步认证协议和 Schnorr 签名协议前面已经介绍过了，其它的签名协议由于论文篇幅所限，不再介绍了，下面直接介绍 Brands 受限盲签名协议。

签名者的私钥为 x，公钥为 $h=g^x$，m 为需要签名的消息，将 g,h 公开。$m'=m'\ g^{t'}$，$m\in Gq$，其中 t,t' 是接收者随机选取的，m 和 $z=m^x$ 是签名者和接收者都知道的知识。

1) 签名者 S 随机选择 $w\in_R Z_q$，计算 $a\leftarrow g^w, b\leftarrow m^w, z\leftarrow m^x$，并将 a,b,z 发送

给接收者 R；

2) 接收者随机选择 $s,t,u,v \in_R Z_q$，分别对 m,a,b,z 进行盲变换得：

$m' \leftarrow m^s g^t$， $a' \leftarrow a^u g^v, b' \leftarrow a^{ut} b^{us} (m')^v$， $z' \leftarrow z^s h^t$，取哈希运算得：

$c' \leftarrow \mathrm{H}(m' \| z' \| a' \| b')$，$\mathrm{c} \leftarrow c'/\mathrm{u}$，将询问 c 发送给签名者；

3) 签名者计算应答 $r \leftarrow (w+\mathrm{c}) \bmod \mathrm{q}$，并将其发送给验证者；

4)验证者验算两个等式 $h^c a = g^r$ 和 $z^c b = m^r$ 是否成立，如果成立，则签名成功，计算 $r' \leftarrow (ur+v) \bmod \mathrm{q}$，则签名为四元组：sign=$(z', a', b', r')$。

本协议中，接收者将 m,a,b,c,z 变换为 m',a',b',c',z' 即为一种盲变换。

为了得到 m 的盲变换 $m' = m^t g^t$ 的签名，接收者按如下方式根据 $z = m^x$ 可以得到 $z' = (m')^x$。

接收者计算作为询问的 Hash 函数 $\mathrm{c} = \mathrm{H}(m \| z \| a \| b)$，而不是由签名者产生随机询问。在发送询问 c' 给签名者前，用盲因子 u 将其变换为盲询问 c。最后，接收者得到关于 m' 的签名。

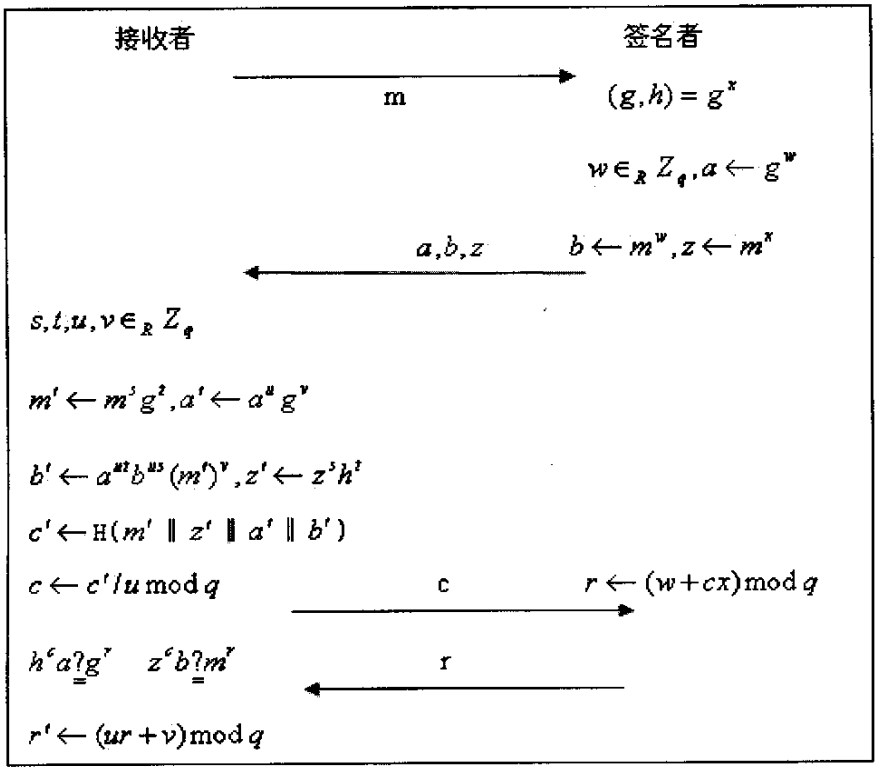

图 6-2 Brands 受限盲签名

6.3 基于 ECDLP 的改进的 Brands 受限盲签名协议

与 Brands 的受限盲签名协议相比较，我们提出的改进协议主要作了以下两

点改进:

(1)在第二步中，对消息 m 的盲变换改进为 $m' \leftarrow m^s$，而在Brands受限盲签名协议中，该盲变换为 $m' \leftarrow m^s g'$，其中 $t \in_R Z_q$。

因为，Brands在文献[33]中第9节对盲变换的分析，盲变换所应满足的条件为: $m' = m^{t_1} g^{t_2} (g')^{t_3}$，其中 $t_1, t_2, t_3 \in_R Z_q$，如果 $t_3 \neq 0$，还必须知道 g'，关于 (m, g) 的表示。在本文中对消息 m 的盲变换是取 t_2 和 t_3 同时为0，此时，可得 $m' \leftarrow m^s$。又因为离散对数与表示问题的安全性级别相同，所以不会降低协议的安全性，但是可以降低计算复杂度，提高在线执行的效率。

(2)在第二步中， a' 的计算由 $a' = a^u g^v$ 变为 $a' = a g^v h^u$,前者必须在线进行 a 的模指数运算，而由于 g^v 和 h^u 由接收者确定，而不依赖签名者，所以可以提前计算，这样在线的模指数运算由原来的一次简化为零次。b' 的计算由 $b' = a^{ut} b^{us} (m')^v$ 变为 $b' = (b m^v z^u)^s$，同样的道理，$m^{vs} z^{us}$ 可以提前计算，所以在线的模指数运算由两次简化为一次。

可见，改进后的协议可以提高在线处理的效率。

表 6-1 DLP 和 ECDLP 中的算术操作比较

	DLP	ECDLP
所用集合	F_q^*	F_q
基本运算	F_q 上的乘法	E 上点的加法
主要运算	模幂运算	倍点运算
基础运算	生成元 g	E 上基点 G
基元的阶	素数 P	素数 P
私有密钥	整数 $a \bmod p$	整数 $a \bmod p$
公有密钥	$w = g^a \in F_q$	E 上的点 $W = aG$

根据参考文献[2]中，所描述的表 6-1，如上。

下面我们介绍基于 ECDLP 的 Brands 受限盲签名协议，此方案实际上是上面提到的改进 Brands 受限盲签名协议在椭圆曲线上的模拟，使得该协议具有更高的安全性和健壮性。在本协议中，我们规定 m 为接收者发送给签名者的消息，d 为签名者私钥，$Q = dG$ 为签名者公钥。将 $(q, FR, a, b, G, n, h, Q, SHA-1)$ 公开。记号 ‖ 表示两个比特串的级联，$R_x(A)$ 表示取 A 点的 x 坐标，其中:

1)q是有限域 $GF(q)$ 中元素的个数，这里 $q = p$ 或 $q = 2^m$;

2) FR 是有限域中元素的表示方法，例如多项式表示或者正规基表示等;

3) $a,b \in GF(q)$, $GF(q)$ 上的椭圆曲线: $y^2 = x^3 + ax + b \quad p > 3$, $y^2 + xy = x^3 + ax^2 + b \quad p = 2$;

4) $h = \#E(GF(q))/n$ 称为余因子，h 远小于 n，可以利用 h 来计算基点;

5) $d \in_R Z_n^*$ 是银行签名私钥，$Q = dG$ 是银行签名公钥:

6) $SHA-1: \{0,1\}^* \to \{0,1\}^{160}$ 是美国NIST和NSA设计的一种安全Hash算法，输入信息长度一般小于 2^{64} bit。

盲签名协议具体执行如图 6-3:

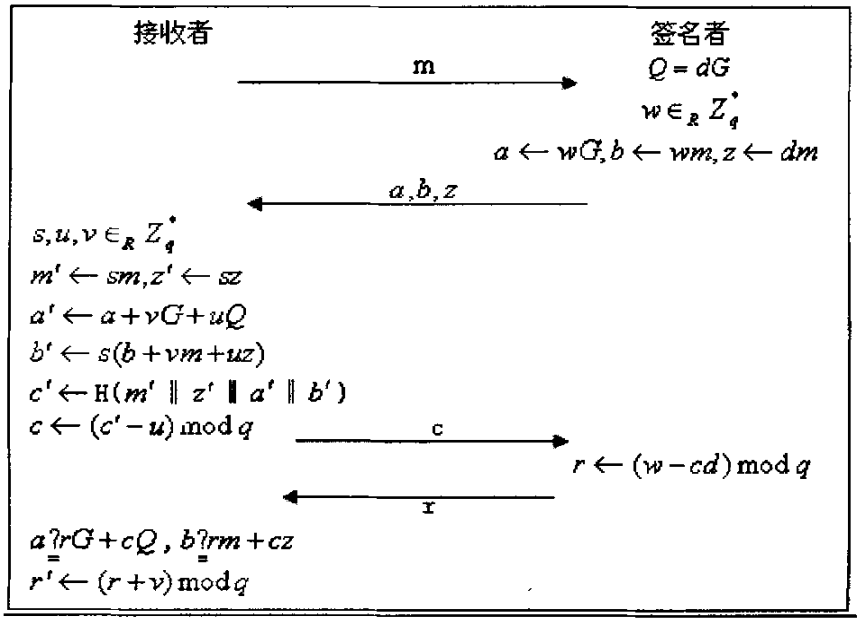

图 6-3 基于 ECDLP 的 Brands 受限盲签名协议

1)签名者 S 随机选择 $w \in_R Z_q^*$，计算 $a \leftarrow wG, b \leftarrow wm, z \leftarrow dm$，并将 a,b,z 发送给接收者 R，这一步没有任何变化;

2) 接收者随机选择 $s,u,v \in_R Z_q^*$，分别对 m,z,a,b 进行盲变换得: $m' \leftarrow sm, z' \leftarrow sz$，$a' \leftarrow a + vG + uQ$，$b' \leftarrow s(b + vm + uz)$，取哈希运算得: $c' \leftarrow H(m' \| z' \| a' \| b')$，$c \leftarrow (c' - u) \bmod q$，将询问 c 发送给签名者;

3)签名者计算应答 $r \leftarrow (w - cd) \bmod q$，并将其发送给验证者;

4)验证者验算两个等式 $a \stackrel{?}{=} rG + cQ$，$b \stackrel{?}{=} rm + cz$ 是否成立，如果成立，则签名成功，计算 $r' \leftarrow (r + v) \bmod q$，则签名为四元组: Sign=$(z', a', b', r')$。

第七章 基于ECDLP的安全离线电子现金协议设计实现

7.1 电子支付系统的模型及描述

在电子现金的支付模型中，协议涉及的三方为银行、用户和商家。电子现金协议主要包括三个过程:提取、支付和存款。用户和商店在银行有开设有账户。系统操作过程如下:

1)取款:用户和银行在认证过的可信信道上执行取款协议，从账户中取出电子现金;

2)支付:用户和商家在匿名信道上执行支付协议，花费电子现金;

3)存款:商家和银行执行存款协议，将用户的电子现金存入商家账户;

在完整的系统中还包括系统设置协议、商店设置协议和用户设置(开户)协议等。

这些协议完成系统的初始化，如系统参数设置、密钥的产生和发布、用户和商家账户的设立等。

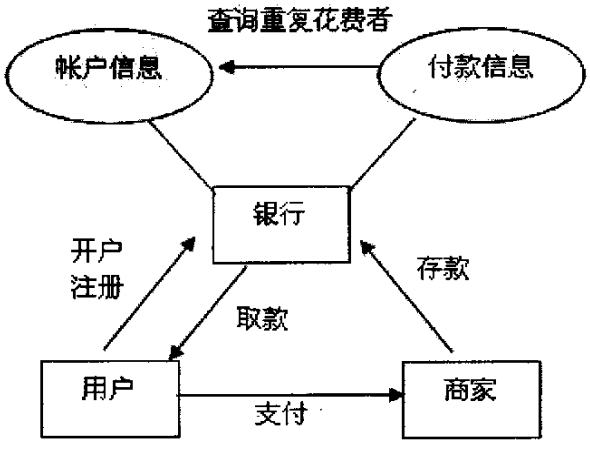

图7-1 电子现金系统协议框架

图7-1给出了本电子现金系统采用的协议框架。银行维护两个数据库:账户信息数据库和付款信息数据库。由银行产生系统所需的参数。

本协议涉及的主要业务为开户注册、取款、支付和存款四大流程，用户和商家需要在注册协议中在银行处开设账户才能提取和接受电子现金。商家的注册

基本与传统的业务流程类似，不同之处在于商家需要产生用于证明其身份的公私钥对，并将公钥发送给银行。银行则在账户数据库中新添一条记录，并保存

商家的公钥。

用户的注册分两步进行：预注册和在线注册。首先用户需亲自到银行预注册一个账号，银行向用户颁发私钥，可以使用智能卡或 USB 盘等作为载体，同时在账户数据库中新添一条记录，并记录用户的私钥及用户预注册时的口令的 Hash 值，并置用户的账户为锁定状态。在一段时间内，用户可以通过因特网向银行申请进行在线注册。银行解锁用户账户。

用户只有通过注册激活他在银行开设的账户并在其上存有一定数量的现金，才能通过取款协议提取电子现金。在取款阶段，银行先向用户证明其身份，再验证用户的身份，这样，只有拥有银行颁发的合法私钥的用户才能执行随后的提取协议。用户产生电子现金的公私钥，并盲化公钥后发送给银行。银行用发行电子现金的私钥进行盲签名回送给用户。用户通过去盲处理得到电子现金。

在本系统中，银行充当认证中心的角色。如果用户没有在本地查找到所欲交易的商家的公钥，则向银行提出查询请求，银行发送经过签名的商家的公钥。用户验证银行签名后保存在本地数据库中，在下一次与该商家交易时不必再向银行申请查询。用户在支付中是匿名的，只须用户验证商家的身份。商家一一检验用户发送的电子现金的合法性(银行的盲签名的正确性)后，产生一份付款请求给用户。用户用电子现金的私钥对付款请求签名。商家验证签名后保存电子现金及有关的支付信息，并发送经商家签名的收条。

经过一段交易时间后，商家将收集到的电子现金(的价值)一起转移到其传统现金账户上。银行要逐一验证欲存款的电子现金的合法性，其支付时产生的签名的正确性。随后银行查询付款信息数据库，以核实商家没有重复存储电子现金，用户没有重复花费电子现金。如验证都通过，则对商家的账户进行转账，同时保存电子现金及相关的支付信息。如检测到了欺骗行为，银行锁定相应的账户。

7.2 基于 ECDLP 的安全离线电子现金协议设计与实现

7.2.1 系统初始化

有限域 $GF(q)$ 上椭圆曲线的有理数点的个数 $\#E(GF(q))$ 可以被一个大素数 $n(n>2^{160}, n>4\sqrt{q})$ 整除，有限域 $GF(q)$ 的特征为 p，基点 $G, G_1, G_2 \in EE(GF(q))$ 将 d 保密，并将 $(q, FR, a, b, G, n, h, Q, SHA-1)$ 公开。记号 $\|$ 表示两个比特串的级联，$R_x(A)$ 表示取 A 点的 x 坐标，其中：

1) q是有限域 $GF(q)$ 中元素的个数，这里 $q=p$ 或 $q=2^m$；

2) FR 是有限域中元素的表示方法，例如多项式表示或者正规基表示等；

3) $a,b \in GF(q), GF(q)$ 上的椭圆曲线: $y^2 = x^3 + ax + b \quad p > 3$,

$y^2 + xy = x^3 + ax^2 + b \quad p = 2$;

4) $h = \#E(GF(q))/n$ 称为余因子，h 远小于 n，可以利用 h 来计算基点;

5) $d \in_R Z_n^*$ 是银行签名私钥，$Q = dG$ 是银行签名公钥:

6) $SHA-1: \{0,1\}^* \to \{0,1\}^{160}$ 是美国NIST和NSA设计的一种安全Hash算法，输入信息长度一般小于 2^{64} bit。

7.2.2 开户协议

1)用户选取 $u_1 \in_R Z_n^*$，计算 $I_u = R_x(u_1 G_1)$ 并将其发送给银行；银行在其用户数据库中存储用户的身份识别信息以及 I_u，账号 I_u 与用户的身份必须一一对应，这样，在用户进行双重花费后，银行通过计算可以得到该用户账号，就能确定其身份。

2)商家选择 $u_2 \in_R Z_n^*$，计算 $I_s = R_x(u_2 G_1)$ 并将其发送给银行，银行存储商家账号。

7.2.3 提取协议

当用户想要从银行处自己的账户上提取电子现金时，就和银行一起执行提取协议，如图 7-2 所示。该提取协议实际上就是一个受限盲签名协议，其中的消息为 $m = I_u + R_x(G_2)$。

银行收到询问c后，计算响应 $r \leftarrow (k - cd) \bmod q$，将其发送给用户，并从用户的账户中减去相应数目的金额。用户收到r后，验证是否满足 $a \stackrel{?}{=} rG + cQ$ 和 $b \stackrel{?}{=} rm + cz$。

如果满足，则计算 $r' \leftarrow (r + v) \bmod q$，并存储 $Sign(pk_1, pk_2) = (z', a', b', r')$。

因此，六元组 $coin = (pk_1, pk_2, Sign(pk_1, pk_2))$ 就是一个合法的电子现金，只有用户知道该现金的一个表示。

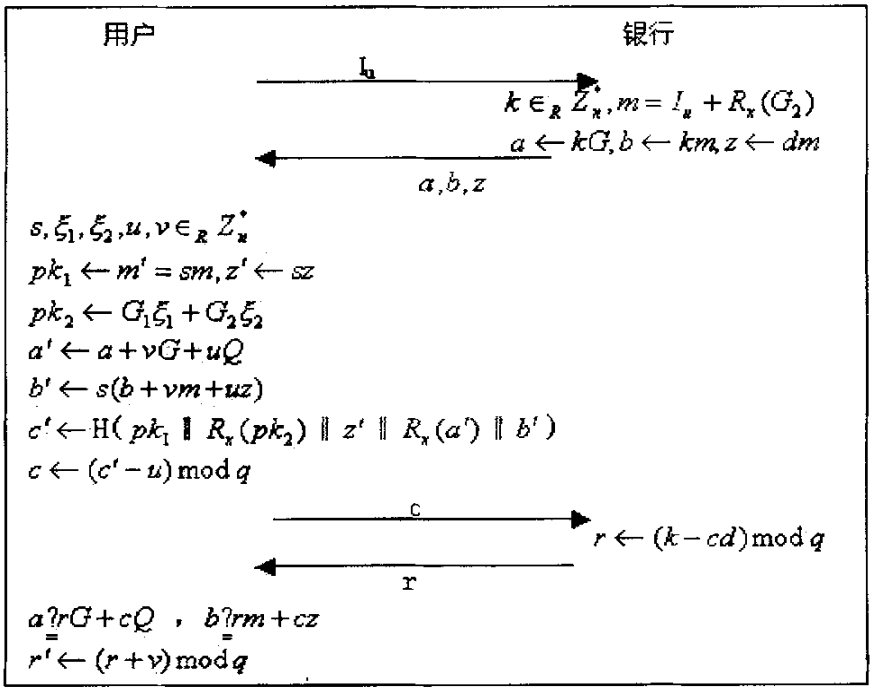

图 7-2 基于 ECDLP 的安全离线电子现金协议的提取协议

下面，是我们对提取协议中的一些等式进行推导：

1）根据等式 $r \leftarrow (k - cd) \bmod q$，可以推导得出用户需要验证的两个等式一定是成立的：

$rG + cQ = G(k - cd) + cdG = Gk = a, rm + cz = (k - cd)m + cdm = km = b$。

2）根据等式：$k' = k + v + ud$，$a = kG, b = mk, m' = ms, z = md$，$Q = dG$，和可以推出：

$a' = Gk' = G(k + v + ud) = a + vG + uQ, b' = m'k' = (ms)(k + v + ud) = s(b + vm + uz)$

3）如果接收者接受了该协议，也就是说，接收者已经验证了下列条件：$a = rG + cQ$ 和 $b = rm + cz$。而

$r'G + c'Q = (r + v)G + (c + u)Q = (r + cd)G + vG + uQ = a + vG + uQ = a'$

$r'm' + c'z' = (r + v)sm + (c + u)sz = s((r + cd)m + vm + uz) = s(b + vm + uz) = b'$

从而等价说明了等式 c'=H($pk_1 \| R_x(pk_2) \| z' \| R_x(a') \| b'$)成立，即，签名Sign(pk_1, pk_2)是合法签名。

7.2.4 支付协议

当用户在任何时间在商家处进行购物时，和商家一起执行支付协议。支付协议的具体流程如图7-3所示。记 $msg = I_s \| amount \| t_p$，，其中 I_s 为商家在银行处的账号，标识商家的身份，$amount$ 为交易金额，t_p 为交易时间。

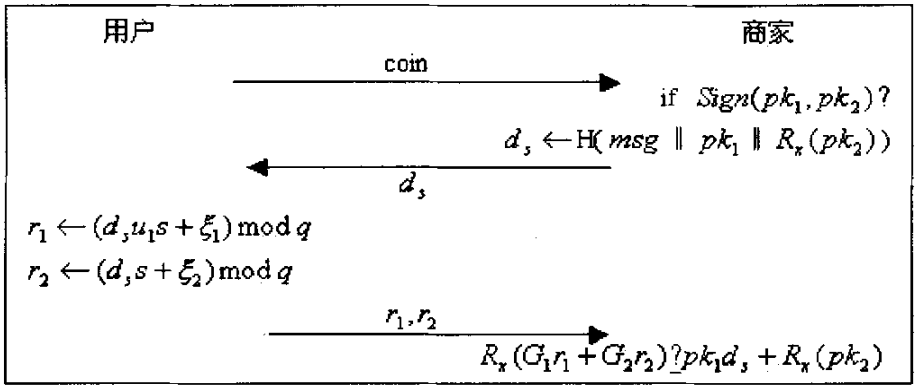

图 7-3 基于 ECDLP 的安全离线电子现金协议的支付协议

用户计算并发送响应 r_1 和 r_2 给商家，商家首先要判断 $Sign(pk_1, pk_2)$ 为合法签名，并验证等式 $R_x(G_1 r_1 + G_2 r_2) = pk_1 d_s + R_x(pk_2)$ 成立，具体推导如下：

等式左边：$R_x(G_1 r_1 + G_2 r_2) = R_x(G_1(d_s u_1 s + \xi_1) + G_2(d_s s + \xi_2))$

$$= R_x(G_1 \xi_1 + G_2 \xi_2) + d_s s R_x(G_1 u_1 + G_2)$$

$$= R_x(pk_2) + d_s s R_x(G_1 u_1 + G_2)$$

等式右边：$pk_1 = sm = s(I_u + R_x(G_2)) = s(R_x(G_1 u_1) + R_x(G_2))$

$$= s R_x(G_1 u_1 + G_2)$$

因此满足：

$$R_x(G_1 r_1 + G_2 r_2) = pk_1 d_s + R_x(pk_2)$$

只有同时满足上述条件，商家才接受该电子现金，并给用户提供相应的商品。

7.2.5 存储协议

存储协议比较简单：经过一段固定的交易周期后，商家将收到的电子现金到银行处批量进行存储。商家将在支付协议中得到的电子现金的一个副本 $\{coin, r_1, r_2, msg\}$ 传递给银行，银行验证电子现金 $coin$ 的有效性，如果验证不通过，则拒收该电子现金；否则，就继续在银行的电子现金数据库中搜索该电子现金，如果搜索失败，则说明此电子现金有效，银行就在数据库中录入该电子现金和 (r_1, r_2, msg)，并在其账目数据库中为商家入账；如果搜索成功，则说明用户或者商家存在欺诈企图，银行拒绝接收此电子现金。

7.3 基于 ECDLP 的安全离线电子现金协议的安全性分析

要使人们完全接纳一种新的电子支付方式，不仅要求这种方式使用起来更方便、成本更低廉、服务更周全，更重要的是该系统能够很好地保护交易各方的合

法利益不受侵害。实现电子支付的安全对于交易各方来说具有举足轻重的地位。如果电子现金系统缺乏必要的安全性，那么它永远不会得到实际的应用。

参照Franklin和Yung的定义[34]，离线电子现金系统的安全要求主要包括四个方面：不可重复花费电子现金；不可伪造电子现金；从n个合法电子现金不可得到第n+1个有效电子现金；对用户支付活动的不可跟踪性。

具体来讲，可从以下八个方面进行严格的定义：

1)完备性：在提取协议中，如果用户按照协议正确执行，并最后接受了该协议，那么六元组$(pk_1, pk_2, Sign(pk_1, pk_2))$就是一个合法的电子现金。

2)用户匿名性：在提取协议中，如果用户按照协议正确执行，那么银行即使拥有无限的计算能力也不能获得关于(pk_1, pk_2)的签名(z', a', b', r')的任何有用信息。

3)不可伪造性：在提取协议中，如果用户不知道自己的身份信息u_1，则他(或她)就不可能获得正确的电子现金。

4)证据真实性：在提取协议中，如果用户和银行按照协议正确执行，那么当用户使用电子现金$coin = (pk_1, pk_2, Sign(pk_1, pk_2))$在商家处购物时，商家可以确定支付协议中产生的证据一定成立。

5)公正性(Soundness)：在提取协议中，如果银行不知道Q关于G的表示d，用户无法获得合法的电子现金。

6)证据隐藏性(Witness Hiding)：在提取协议中，即使用户知道所有信息并具有无限的计算能力，也无法知道Q关于G的表示d.

7)不可重用性：在支付协议中，如果用户使用同一个电子现金进行两次正常花费，当银行收到这两个支付记录后能够揭示该用户身份。

8)不可追踪性：银行即使与商家合作也不可能将电子现金的提取过程与其付款过程联系起来。

接下来，我们就从以上八个方面对基于ECDLP的安全离线电子现金协议进行证明，以保证协议的安全性。

- 完备性证明：

要证明六元组$(pk_1, pk_2, Sign(pk_1, pk_2))$就是一个合法的电子现金，也就是等价要证明$Sign(pk_1, pk_2) = (z', a', b', r')$是$(pk_1, pk_2)$的正确的盲签名。在假设$SHA-1(\cdot)$为碰撞自由杂凑函数的情况下，对于上述命题的证明等价于需要证明等式$c' = \mathrm{H}(pk_1 \| R_x(pk_2) \| z' \| a' \| b')$成立，也等价于需要证明$a' = r'G + c'Q$且$b' = c'z' + r'm'$。如果协议正确执行，说明用户接受了该协议，也即表明用户验证了$a = rG + cQ$和$b = cz + rm$成立

$$r'G + c'Q = (r + v)G + (c + u)Q = (r + cd)G + vG + uQ = a + vG + uQ = a'$$

$r'm'+c'z'=(r+v)sm+(c+u)sz=s((r+cd)m+vm+uz)=s(b+vm+uz)=b'$

所以$c'=\mathrm{H}(pk_1 \| R_x(pk_2) \| z' \| g^{r'}h^{c'} \| (z')^{c'}(m')^{r'})$成立，所以本协议满足完备性。

- 用户匿名性证明：

在提取协议执行成功以后，用户获得的信息为(m',a',b',c',r')；银行能够获得的信息为：(m,z,a,b,c,r)，满足$a=rG+cQ$和$b=cz+rm$可以证明：对于签名对(m',a',b',c',r')以及(m,z,a,b,c,r)，恰好存在唯一的一组随机数$s,u,v\in_R Z_q$。使得下列等式成立：

$$\begin{cases} m'=sm \\ a'=a+vG+uQ \\ b'=s(b+vm+uz) \\ c'=(c+u)\bmod q \\ r'=(r+v)\bmod q \end{cases} \qquad (*)$$

根据等式$m'=sm$，知道s可以被唯一确定为$s=m'/m$；同时，u和v也可以由等式$c'=(c+u)\bmod q$和$r'=(r+v)\bmod q$唯一确定为$u=(c'-c)\bmod q$和$v=(r'-r)\bmod q$。下面证明(s,u,v)满足等式$a'=a+vG+uQ$和$b'=s(b+vm+uz)$

因为

$a'=r'G+c'Q=(r+v)G+(c+u)Q=(rG+cQ)+vG+uQ=a+vG+uQ$

$b'=c'z'+r'm'=(c+u)zs+(r+v)ms=s((rm+cz)+vm+uz)=s(b+vm+uz)$

故随机数组(s,u,v)满足上述所有等式，并且是唯一确定的。由于(s,u,v)从集合Z_n^*中随机均匀选取，所以银行通过猜测攻击，同时猜中三个数的概率为$(1/n)^3$，从而银行在计算上不可能获得关于盲消息m'的签名(z',a',b',r')任何有用的消息，所以用户匿名性也是满足的。

- 不可伪造性证明：

假设用户（身份信息为u_1）冒用其它用户（身份信息为u_2）的名义和银行成功执行提取协议，获得电子现金$coin=(pk_1,pk_2,Sign(pk_1,pk_2))$，则有$pk_1=ms=(R_x(u_2G_1)+R_x(G_2))s$。当他在使用该电子现金进行支付时，由于只知道$u_1$，因此只能将$r_1=d_su_1s+\xi_1$和$r_2=d_ss+\xi_2$发送给商家，商家验证

$$\begin{aligned} R_x(G_1r_1+G_2r_2) &= R_x(G_1(d_su_1s+\xi_1)+G_2(d_ss+\xi_2)) \\ &= R_x(G_1\xi_1+G_2\xi_2)+d_ssR_x(G_1u_1+G_2) \\ &= R_x(pk_2)+d_ssR_x(G_1u_1+G_2) \end{aligned}$$

又因为，此时$pk_1=sR_x(G_1u_2+G_2)$

所以 $R_x(G_1r_1+G_2r_2)\neq R_x(pk_2)+pk_1d_s$

因此该用户不能获得正确的电子现金，所以不可伪造性得证。

● 证据真实性证明：

在提取协议执行成功以后， 如果用户获得的电子现金为 $coin=(pk_1,pk_2,Sign(pk_1,pk_2))$，则当用户使用该现金与商家执行支付协议时，商家需要判断的证据为：是否满足等式 $R_x(G_1r_1+G_2r_2)=pk_1d_s+R_x(pk_2)$

根据完备性证明，如果等式 $c'=\mathrm{H}(pk_1 \| R_x(pk_2) \| z' \| g^{r'}h^{c'} \| (z')^{c'}(m')^{r'})$ 成立，则证明电子现金是合法的， 因此有：$pk_1=s(u_1G_1+G_2)$，$pk_2=(\xi_1G_1+\xi_2G_2)$ 可以推导如下：

$R_x(G_1r_1+G_2r_2)=pk_1d_s+R_x(pk_2)$，因此证据真实性也是成立的。

● 公正性证明：

在提取协议中，假设银行公布的 Q 满足 $Q=d\ G$，即 d 为正确的银行签名私钥，但是假设银行不知道 d，因此在向用户发送响应时，计算响应：$r=k-cd'$，但是 $d\neq d'$，则当用户验证等式 $a\stackrel{?}{=}rG+cQ$ 和 $b\stackrel{?}{=}rm+cz$ 是否成立时，有

$rG+cQ=(k-cd')G+cdG=kG+(d-d')cG\neq a$，同理，$b\neq mr+cz$。因此，用户就会拒绝接收该非法电子现金。所以满足公正性要求。

● 证据隐藏性证明：

在提取协议中，银行公布其签名公钥 Q 满足 $Q=d\ G$，但是对该私钥 d 保密，

在协议执行过程中，银行泄漏给用户与 d 有关的信息只有两条：$z=dm$ 和 $r=(k-cd)\bmod q$ 根据基于椭圆曲线的离散对数困难问题，用户不可能根据：$z=dm$ 求出的 d 值；由于k和 d 均为银行随机选取，而 r 和c 是用户所知的数值，所以，可以将等式 $r=(k-cd)\bmod q$ 看成关于变量 k 和 d 的二元一次方程，显然，该方程具有无穷多个解，用户也无法计算得出其解。因此，证据隐藏性得证。

● 不可重用性证明：

在离线电子现金系统中，银行通过查询数据库可以离线判断双重花费行为，进而通过计算可以找出该用户。假设用户的有效电子现金为 $coin=(pk_1,pk_2,Sign(pk_1,pk_2))$ 在使用同一个电子现金进行两次不同支付的过程中，商家计算的 d_2 不同，相应地，用户 (r_1,r_2) 也不同，设两次花费的记录分别为 (r_1,r_2,d_s) 和 (r_1',r_2',d_s')。因为该记录能够通过商家的验证，即满足：$R_x(G_1r_1+G_2r_2)=pk_1d_s+R_x(pk_2)$ 和 $R_x(G_1r_1'+G_2r_2')=pk_1d_s'+R_2(pk_2)$，那么，可以很容易得出 $pk_1=(R_x(G_1r_1+G_2r_2)-R_x(G_1r_1'+G_2r_2'))/(d_s-d_s')$

又因为 $pk_1=ms=s(I_u+R_x(G_2))$，$r_2=d_ss+\xi_2, r_2'=d_s's+\xi_2$，从而可得：$R_x(G_1(r_1-r_1'))/(d_s-d_s')=sI_u$，即 $R_x(G_1(r_1-r_1'))/(r_2-r_2')=I_u$

从而说明，银行可以找出进行双重花费的恶意用户。

● 不可追踪性证明：

在离线电子现金协议中，如果三个子协议都成功执行，则在提取协议中，用户获得的信息为 (m',z',a',b',r',c')，银行获得的信息为：(w,m,z,a,b,c,r)；在支付

子协议中，用户获得的信息为 (d_s, r_1, r_2)，商家获得的信息为：$(pk_1, pk_2, z', a', b', r', d_s, r_1, r_2, I_s, date/time)$；在存储协议中，商家将支付记录 $(pk_1, pk_2, z', a', b', r', r_1, r_2, date/time)$ 发送给银行。因此银行与商家合作共同知道的信息为：$(pk_1, pk_2, z', a', b', r', r_1, r_2, date/time, w, m, z, a, b, c, r, h, x)$ 不知道的信息为：$(u_1, s, u, v, \xi_1, \xi_2, c')$ 。这些信息满足下列关系：

$$\begin{cases} m' = sm \\ a' = a + vG + uQ \\ b' = s(b + vm + uz) \\ c' = (c + u) \bmod q \\ r' = (r + v) \bmod q \\ pk_1 = ms \\ pk_2 = \xi_1 G_1 + \xi_2 G_2 \\ R_x(G_1 r_1 + G_2 r_2) = pk_1 d_s + R_x(pk_2) \end{cases}$$

下面证明：存在唯一的一组参数 (u_1, s, u, v, x_1, y_1)，使得上述关系成立。我们在用户匿名性证明中已经证明，恰好存在唯一的一组随机数 $s, u, v \in_R Z_n$。使得等式(*)成立，因此我们只需要进一步证明，恰好存在唯一的一组随机数 $u_1, \xi_1, \xi_2 \in_R Z_n$，使得下列等式成立

$$\begin{cases} pk_1 = ms \\ pk_2 = \xi_1 G_1 + \xi_2 G_2 \\ R_x(G_1 r_1 + G_2 r_2) = pk_1 d_s + R_x(pk_2) \\ r_1 = d_s u_1 s + \xi_1 \\ r_2 = d_s s + \xi_2 \end{cases}$$

我们令 $\xi_1 = r_1 - d_s u_1 s, \xi_2 = r_2 - d_s s$，$R_x(u_1 G_1) = \sqrt{pk_1} - R_x(G_2)$，从而可以唯一确定 (ξ_1, ξ_2, u_1)，下面证明它们也满足剩下的两个等式，对于 $pk_2 = \xi_1 G_1 + \xi_2 G_2$ 显然是成立的，下面验证 $R_x(G_1 r_1 + G_2 r_2) = pk_1 d_s + R_x(pk_2)$

$$\begin{aligned} R_x(G_1 r_1 + G_2 r_2) &= R_x(G_1(\xi_1 + d_s u_1 s) + G_2(\xi_2 + d_s s)) \\ &= R_x(d_s s(G_1 u_1 + G_2)) + (G_1 \xi_1 + G_2 \xi_2)) \\ &= pk_1 d_s + R_x(pk_2) \end{aligned}$$

上述证明说明，存在唯一的一组参数 (u_1, s, u, v, x_1, y_1) 使得等式成立。同时，由于 (u_1, s, u, v, x_1, y_1) 是随机取自 $Z_n (n > 2^{160})$，所以银行联合商家通过猜测获得成功的概率仅为 $(1/n)^6$，从而不可追踪性得证。

通过对上述命题的证明可以说明，我们的基于ECDLP的安全离线电子现金协议是安全的。

7.4 基于 ECDLP 的安全离线电子现金协议性能分析

从1983年Chaum提出电子现金协议至今已是整整二十年时间，在这二十年里，为了将电子现金系统真正推向实用，诸多学者对于如何实现电子现金的公平性、可分性和可转移性[35][36]等扩展特性进行了广泛的研究。但是，由于目前实用的电子现金系统还不多，而且由于技术保密的原因，在公开发表的论文中鲜见专门针对电子现金系统的性能进行研究的文章。但是，要真正将电子现金应用于实践，性能问题是一个不容忽视、不能回避的重要问题。

为此，本节就对基于ECDLP的安全离线电子现金协议的效率问题进行一下简单的探讨，从以下两个方面进行具体的阐述。

1）首先，通过对传统的Brands受限盲签名协议的改造，使其降低了计算复杂度，从而提高了在线提取现金的效率。与乘法、加法等运算相比，模指数运算的计算量要大得多，而Brands受限盲签名协议中将会用到大量模指数运算，所以我们通过简化盲变换表达式，可以降低在线提取的计算量。首先，将 $m' = m^{t_1} g^{t_2} (g^r)^{t_3}$，（其中 $t_1, t_2, t_3 \in_R Z_q$）中的 t_2, t_3 同时取零，从而得到 $m' = m^s$ 与原来的 $m' = m^s g^t$ 相比，减少了模指数运算。然后，将原来的 w 的盲变换表达式 $w' = uw + v$ 转变为 $w' = w + v + xu$ 使得 a 的盲变换没有幂指数运算，b 的幂指数运算形式也比以前要简单，所以也可以提高在线处理的效率。

2）然后，将传统的电子现金协议模拟到椭圆曲线上，将基于离散对数的数学难题转变为基于椭圆曲线的离散对数的数学难题，使得在不降低安全性的前提下，密钥长度有所减小，从而提高了电子现金的执行效率。数学家们研究椭圆曲线已有一百多年历史，直到 20 世纪 90 年代，Koblitz 和 Miller 才开始将其应用到密码领域中。椭圆曲线密码体制的数学基础就是利用椭圆曲线上的点构成的从 Abelian 加法群构造的离散对数的计算复杂性。椭圆曲线密码体制与基于离散对数的传统公钥密码体制，如 RSA 相比有两个优点：密钥长度较短和安全性更高[2]，如表

表 7-1 ECC 与 RSA 的安全性对照表

ECC 密钥长度	RSA 密钥长度	解密代价年(每秒100万条指令)
160	1024	1E+12
320	5120	1E+36
600	21000	1E+72
1200	120000	1E+168

7.5 模块设计

本系统的实现选择的是基于 windows 的开发平台，采用客户机/服务器运行模式，网络通信基于 winsock 套接字。用户、商家、银行分别进行编程，以下是选用的开发工具：JAVA、Microsoft SQL Server 2000、GNU Multiple Precision Arithmetic Library 4.2 等。随机数采用 GMP 自带的伪随机数发生器。

本系统包括银行、商家和用户端三部分的软件，三者均存在相似的功能。每一方均有数据库模块。用户的数据库存储已提取而未花费的电子现金、商家收条以及本地商家公钥表等。商家的数据库存储已收集但尚未存储到银行的电子现金，商品的货物 ID 及价格，银行转账的收条。对银行的数据库设计来说，它包括账户信息、支付信息和已注册的商家的公钥表。三方的数据库设计均要求有插入、删除、查询和修改等操作，所以我们另设一个通用的数据类。

通信交互时，银行扮演服务器的角色，用户扮演客户机的角色；而商家同时具有服务器和客户机的功能，对用户而言，商家是服务器，对银行而言，它是客户机。服务器的设计均为多进程并发模式，在资源许可的情况下，尽可能满足多个客户的服务要求。此外，每一方的通信还要有初始化配置工作，每一方的密钥交换我们把它归到算法模块。

算法模块主要有 Diffie-Helman 密钥交换和 Schnorr 身份认证和签名算法。另外，我们把以 GMP 大数处理库为基础，将系统参数的产生和倍点，倍乘归为操作模块。如下给出了了本系统的模块组织图

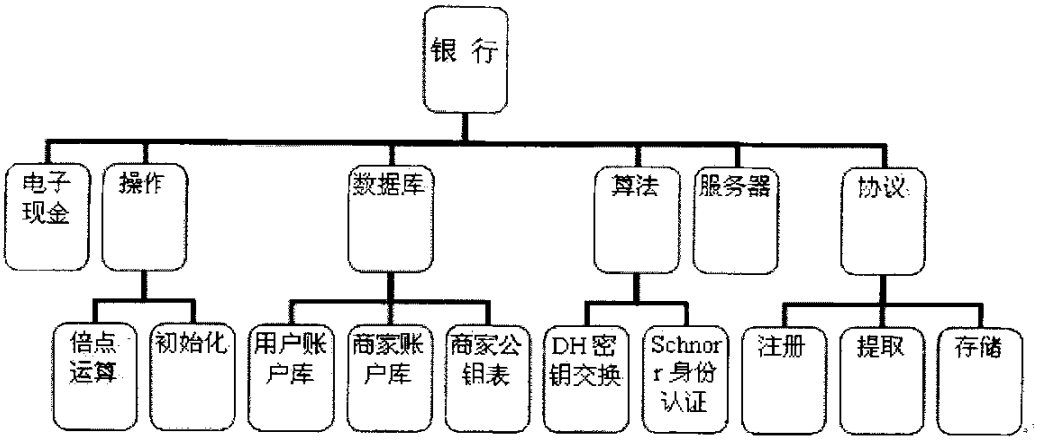

图7-4 银行的模块组织图

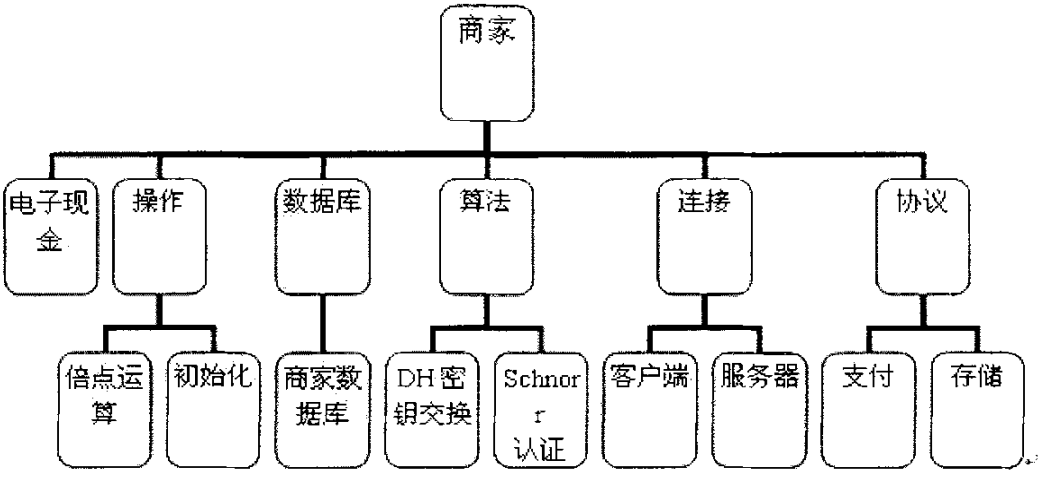

图7-5 商家的模块组织图

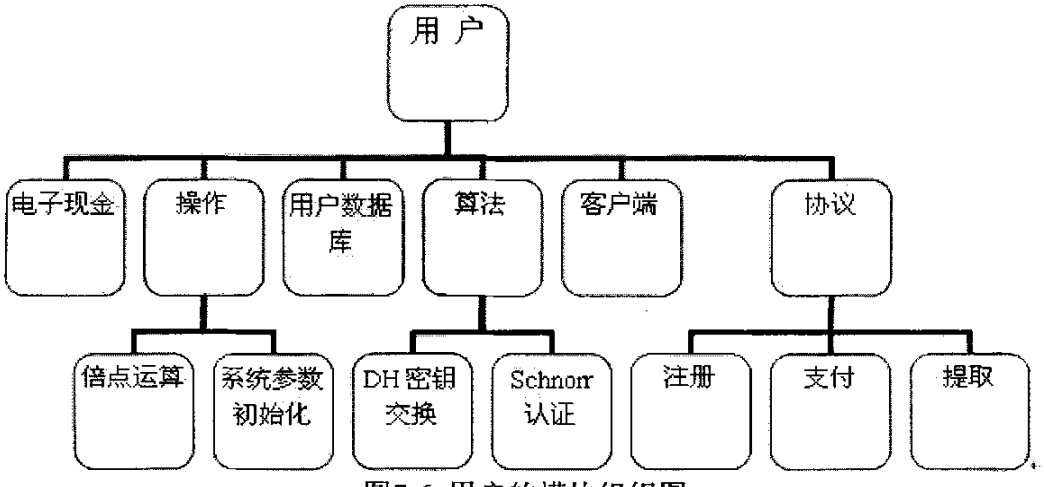

图7-6 用户的模块组织图

7.6 系统实现详述

7.6.1 系统初始化

1)选取有限域$GF(q)$上椭圆曲线的表达式为$y^2+xy=x^3+ax^2+b \quad p=2$；q是有限域$GF(q)$中元素的个数，取有限域个数为$GF(2^{10})$，$FR$是有限域中元素的表示方法，用正规基表示。

2)银行随机选择13个基点，表示为$(G_1,G_2,G_3,Q_0 \sim Q_9) \in E(GF(2^{10}))$。

3)电子现金面额记为n,则将n表示成二进制数，取位为1对应$Q_0 \sim Q_9$的基点相乘即得到表示电子现金面额的基点n_c。本系统支持的最大面额为1024元，最

小面额为1元。

4) $SHA-1:\{0,1\}^{*}\rightarrow\{0,1\}^{160}$ 是美国NIST和NSA设计的一种安全Hash算法，输入信息长度一般小于2^{64} bit。

7.6.2 注册阶段

在本系统中，为了模拟现实生活，我们将用户注册分为预注册和注册两个步骤：首先，用户亲自到银行进行注册，用户生成身份认证私钥和公钥，并把公钥发给银行。银行核对用户身份后对用户的身份证号 ID 和注册口令的 hash 值签名，并在帐户数据库中添加一条记录，并置为冻结状态。用户随后可以在任何时候通过因特网与银行进行远程注册。银行与用户之间双向身份认证，并确认用户帐号记录为冻结。用户的计算机随机生成公私钥(u_1,I_u)，并将公钥发送给银行以生成电子现金，最后将用户的身份证号 ID 与该公钥相对应，并存储到帐户数据库中。

商家注册比较简单，只需要法人代表携带个人身份证到银行开户，并产生商家的公私钥，银行在其帐户数据库中增加一条记录，同时记录商家法人代表的身份证号及其公钥。

7.6.3 身份认证阶段

交易双方在必要的身份认证通过后，随后的通信消息均采用会话密钥加密后再传输。消息到达另一端后用会话密钥解密后进行运算处理。下面简单介绍一下 Diffie-Hellman 算法。设 p 是大素数，a 是 p 的生成元，a 和 p 是公开的。用户 A 选择一保密的随机整数 X_A，并将 $Y_A=a^{X_A} \bmod p$ 发送给 B，同样的，用户 B 把 $Y_B=a^{X_B} \bmod p$ 发送给 A，然后 A 和 B 用自己的私钥分别对 Y_A 和 Y_B 进行加密得到 K，则 K 就是共享密钥，这是因为：

$Y_B^{X_A} \bmod p=(a^{X_B} \bmod p)^{X_A} \bmod p=(a^{X_B})^{X_A} \bmod p=a^{X_BX_A} \bmod p=Y_A^{X_B} \bmod p$

又因为 X_A,X_B 是保密的，第三者只能知道 p,a,Y_A,Y_B，要想知道 K，必须知道 X_A,X_B 中的一个，而，这就意味着求解离散对数难题，所以第三者求 K 是不可行的。

在用户、商家和银行三个参与方分别执行提取协议、支付协议和存储协议，在交易之前双方必须进行双向身份认证，一证明对方的真实身份，由于本系统中没有使用 PKI，所以使用了 Schnorr 身份认证协议。用户成功注册后，在执行取款协议时首先要进行双向身份认证，而在执行支付协议时，用户的身份是隐匿的，用户首先检索本地的商家公钥表，如果没有找到，则想银行提出查询要求，此时，

不需要进行双向身份认证。商家用私钥和 Schnorr 身份认证协议向用户证明自己的身份。

商家与银行执行存款协议时，也要进行双向身份认证。商家和银行分别使用自己的私钥及 Schnorr 身份认证协议向用户证明自己的身份。

7.6.4 提取协议

用户必须先在银行开户并存有一定数量现金后，才能提取小于该数额的电子现金。用户与银行执行取款协议时，首先进行双向身份认证，在确认对方身份后，再产生会话密钥。然后，用户构造电子现金的公私钥(sk, pk)，并将个人身份信息I_u嵌入到公私钥中，银行对其进行盲签名后即得电子现金。协议详细过程见图 7-2。

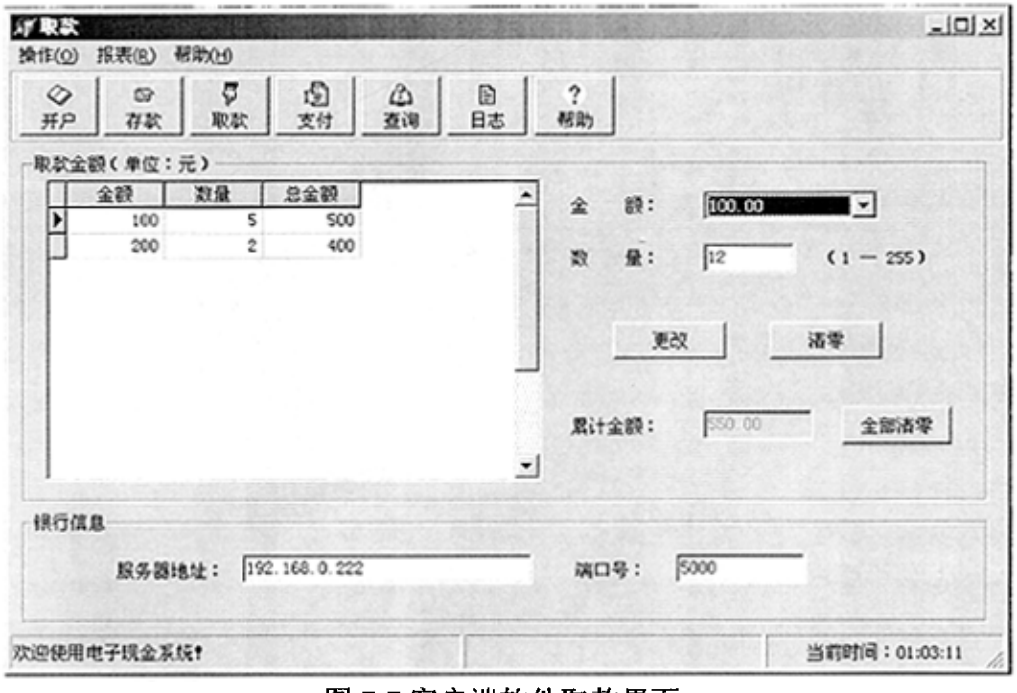

图 7-7 客户端软件取款界面

7.6.5 支付协议

用户首先从本地或银行获取商家的公钥，然后提出支付请求。商家证明自己的身份及双方产生的会话密钥后，用户传送电子现金及想要购买的商品的标识。商家首先验证银行对该电子现金公钥和盲签名，如通过验证，则说明该电子现金是合法的。然后商家构造一条付款要求，包括交易的时间、日期、交易额、商家身份及一个随机数。用户收到此付款要求后，核对除随机数外的各项，如正确，则用电子现金的私钥对该付款要求进行签名。商家验证此签名正确后，保存电子

现金、支付信息和用户签名，并产生收条表明商家接收了用户的电子现金，随后发送货物。

协议详细过程见图 7-3，支付界面如下图 7-8。

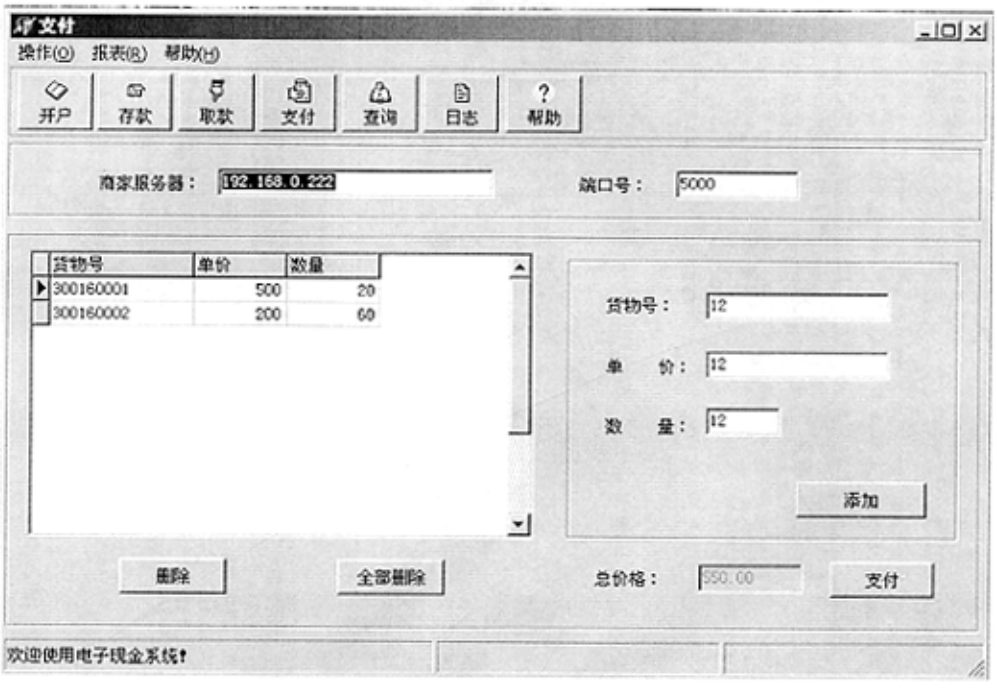

图 7-8 客户端软件支付界面

7.6.6 存款协议

商家经过一段时间的电子现金收集，然后将电子现金及其相应的支付信息发送给银行要求存款，即将电子现金所代表的价值转移到他在银行开设的帐户上。银行对收到的电子现金和支付信息逐一检验。银行需要验证每一笔交易的付款要求中嵌入了商家的身份标识及交易金额不大于该交易的电子现金的面额。然后银行按商家同样的验证方法验证每一电子现金的有效性以及电子现金对应的付款要求签名的正确性。最后银行查询付款信息数据库，确保没有发生重复存储和重复花费。如果付款信息数据库中存在某条记录，其付款要求对应饿随机数与商家提供要求存款的付款要求中包含的随机数相同，则银行拒绝对该电子现金进行转帐；如果该记录对应的电子现金部分与商家提供要求存款的付款要求中包含的电子现金部分相同，则银行根据该记录与商家提供的电子现金及支付信息计算出重复花费者的身份，商家因受骗遭到的损失由不诚实的用户进行补偿。

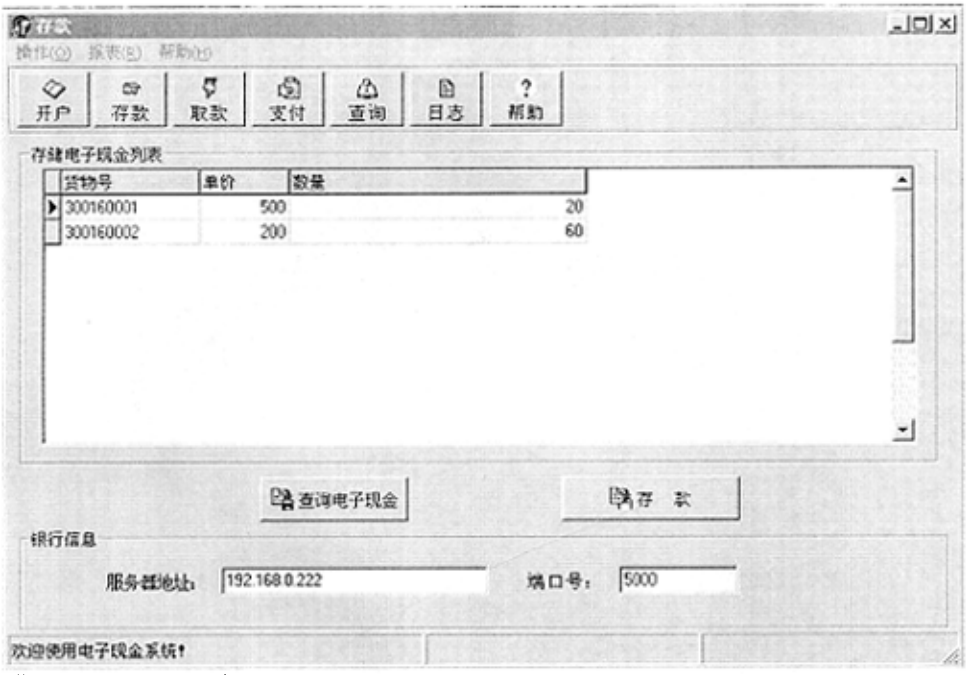

图 7-9 商家端存款界面

7.6.7 部分代码实现

\\这是商家用来处理订单的 EntityBean 的 Home 接口

Public interface MemberorderProcHomeint extends EJBHome

{

public MeberOrderProcRemoteint create(String meberid,int totalprice,ArrayList commodityorder) throws RemoteException, CreateException;

public MeberOrderProcRemoteint findByPrimaryKey(String orderid) throws FinderException, RemoteException ;

public Collection findAll() throws FinderException,RemteException;

public Collection findByMemberid(String memberid) throws FinderException,RemoteException;

}

\\EntityBean 的 Remote 接口

Public interface MemberOrderProcRemoteint extends EJBObject {

Public void setTotalprice(int totalprice) throws RemoteException;

Public void setCommodityorder(Arraylist commodityorder) throws RemoteException;

Public Arraylist getCommoditOrder() throws RemoteException;

```
Public String getMemberid() throws RemoteException ;
Public String getOrderid() throws RemoteException ;
//Bean Class 中的 Business 方法
Public ArrayList getCommodityOrder()
{   return commodityorder;   }
Public String getMemberid()
{   return memberid;}
Public int gerTotalprice()
{return totalprice }
Public String getOrderid()
{ return ordered;}
//ShopCommodityProcRemoteint.java 代码
Package NetCommodityOrder.scejb;
Import java.util.*;
Import javax.ejb.*;
Import java.rmi.RemoteException;
Import NetCommodityOrder.ejbtools.*;
//这是 EntityBean(shopCommodityProcEjb)的一个 Remote 接口
//这个 EntityBean(shopCommodityProcEjb)用来处理订单的事项
//它是一个 Container managed persistence EntityBean
Public interface ShopCommodityProcRemoteint extends EJBObject{
//建立 3 个 business 方法，这 3 个 business 方法
//必须与 Bean Class 中的 business 方法相对应
Public void setCommodityInformation(String commodityname,int
unitprice)throws RemoteException;
Public void setUnitprice(int unitprice)throws RemoteException;
Public void setCommodityname(String commodityname)throws
RemoteException;
//建立四个 business 方法，这四个 business 方法必须与 Bean Class 中的
business 方法相对应
Public ShopCommodity getCommodityInfomation()throws RemoteException;
Public int getUnitprice() throws RemoteException;
Public String getCommodityname() throws RemoteException;
}
```

```
//ShopCommodityProcEJavaBean.java 代码
Package NetCommodityOrder.scejb;
Import java.util.*;
Import javax.ejb.*;
Import javax.sql.*;
Import javax.naming.*;
Import NetCommodityOrder.ejbtools.*;
//这是 EntityBean(ShopCommodityProcEJB)的 Bean Class 类
Public class ShopCommodityProcEJavaBean implements EntityBean
{
Public String commodityid=null;
//定义回调方法
Public void setEntityContext(EntityContext context)
{ this.entitycontext=entitycontext;}
Public void unsetEntityContext()
{entitycontext=null};
Public String ejbCreate(String commodityid)throws
DuplicateKeyException,CreateException
{this.commodityid=commodityid;
This.commodityname=""
Return null;}
Public String ejbCreate(String commodity,String commodityname,int
unitprice)throws DuplicateKeyException,CteateException;
{ this.commodityid=commodityid;
This.commodityname=commodityname;
Return null;}
Public void ejbActivate()
{  commodityid=(String)entitycontext.getPrimaryKey;}
Public void ejbPassivate()
{ commodityid=null;
Commodityname=null;
Nuitprice=0;
}
Public void ejbRemote(){}
```

```
//定义 business 方法
Public void setCommodityname(String commodityname)
{this.commodityname=commodityname;}
.....
Public String getCommodityname()
{return commodityname}
```

7.7 进一步工作及结论

1)采用更好的椭圆曲线上的快速实现算法,可以进一步提高电子现金协议的在线执行的效率。

椭圆曲线公钥密码实现在效率在于椭圆曲线上的运算速度,常用的运算有点的倍乘和加法运算,其核心计算是点的倍乘。对于倍乘运算,常用的方法有四种:

(1)二进制取幂方法

椭圆曲线上一个点P被一个大整数n乘,这个问题的标准算法是二进制取幂算法,它的一个推广是每次迭代执行K指数比特的K-ary方法,滑动窗口法是K-ary方法的进一步推广。

(2)加减方法

加减方法是椭圆曲线纯量乘积的基本技术。首先定义系数n的非相邻(NAF):一个具有无两个连续系数是非零性质的有符号二进制展开。有几种从n的二进制表示中构造NAF(n)的方法,这里选用的是重复用2除。一个整数的二进制表示可以通过被2除,存储剩余,用商重复这个过程而求得。

(3)使用影射坐标

求一次域元素的逆仍然比一次域乘法要费时的多,使用影射坐标可除去二次点相加时所需要的逆运算。

(4)Montgomery 方法

寻找快速计算椭圆曲线倍乘的新方法仍然是椭圆曲线公钥密码的研究热点。

2)本电子现金协议要求所有商家和用户必须使用同一银行,而从长远来看,这必定会阻碍电子现金的广泛推广,所以多银行电子现金系统是未来电子现金系统发展的方向。

本章介绍了基于 ECDLP 的安全离线电子现金协议方案,它是基于椭圆曲线密码机制的。随着椭圆曲线密码机制的相应标准的制定和采用,基于椭圆曲线密码机制的电子现金将有更广的应用前景。

参考文献

[1] 南湘浩，陈钟. 网络安全技术概论. 北京：国防工业出版社. 2003.

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

[3] 冯登国，裴定一. 密码学导引. 北京：科学出版社. 1999

[4] 杨波. 现代密码学. 北京：清华大学出版社. 2003

[5] 白国强，黄谆等. 基于椭圆曲线的代理数字签名. 电子学报. 2003. 11(11):1659~1662

[6] 罗浩，乔秦宝. 椭圆曲线签名方案. 武汉大学学报. 2003. 49(1):95~98

[7] 吕皖丽，钟诚. 一种安全的椭圆曲线多重数字签名方案. 计算机工程. 2004. 30(50):126~128

[8] 秦晓东，辛运维. 基于椭圆曲线的数字签名系统的设计与实现. 计算机工程与应用. 2003. (28):156~159

[9] 蔡满春，杨义先. 基于椭圆曲线密码体制的一种电子现金方案. 北京邮电大学学报. 2004. 27(2):44~47

[10] 张雁，林英. 椭圆曲线公钥密码体制的研究热点综述. 计算机工程. 2004. 30(3):127~130

[11] 夏先智，赵毅. 基于椭圆曲线加密算法技术优势的讨论. 计算机科学. 2003. 30(10):181~183

[12] 唐文，南湘浩. 基于椭圆曲线密码系统的组合公钥技术. 计算机工程与应用. 2003. 21:1~3

[13] 王文龙，王泽成. 一种基于椭圆曲线数字签名的可认证密钥分配方案. 2003. 31:179~182

[14] 罗涛，易波. 关于椭圆曲线数字签名算法研究. 计算机工程与应用. 2003. 29:184~188

[15] 周先存. 单向函数在公开密钥密码系统中的应用. 皖西学院学报. 2004. 20(2):64~66

[16] 王泽成，苏晓萍. 一个基于椭圆曲线的代理签名和代理盲签名方案. 青海大学学报. 2002. 20(3):36~38

[17] 王泽成，周振江. 基于知识签名的若干代理签名方案. 高性能计算技术. 2002. 159:31~33

[18] 郭涛，李之棠. 基于椭圆曲线的盲签名与离线电子现金协议. 通信学报. 2003. 24(9):142~147

[19] 谭运猛，杨宗凯. 电子现金支付协议的研究. 通信学报. 2002. 23(11). 8~13

[20] 徐小平. 一种改进的椭圆曲线算法及在电子商务中的应用. 微电子学与计算机. 2004. 21(4):74~78

[21] 罗新星，江景佼，汪晓. 电子支付安全技术及其应用的研究. 株洲工学院学报. 2003. 17(2):67~69

[22] 常晓燕，崔泽永. 安全电子支付系统探析. 电子商务. 2004. 1

[23] 李继国，曹珍富，李建中. 电子现金技术. 计算机科学. 2004. 31(1):5~10

[24] 郭涛，李之棠. 一种改进的离线电子现金方案. 华中科技大学. 2003. 31(5):14~16

[25] S. Goldwasser, S. Micali, C. Racko. The knowledge complexity ofinteractive proof systems. Providence, Rhode Island, U. S. A.: ACM Press. 1985. 291~304

[26] U. Feige, A. Fiat, A. Shamir. Zero-knowledge proofs of identity, Proc. 19th ACM Symp. Theory of Computing and Cryptology. 1988. 10(2):77~94

[27] U. Feige, A. Shamir. Witness indistinguishable and witness hiding protocols. in: Baruch Awerbuch, editor. Proceedings of the Twenty Second annualACM Symposium on Theory of Computing. Baltimore, Maryland: ACM Press. 1990. 416~426

[28] Camenisch, Markus, Stadler. Efficient group signatures for large groups. In Proc. CRYPT097, Springer-Verlag, Lecture Notes in Computer Science. 1997. 10~42

[29] D. Chaum. Blind signatures for untraceable payments. Advances in cryptology—Crypto' 82. 1983. 199~203

[30] D. Chaum. Security Without Identification:Transaction Systems to Make Big Brother Obsolete. Communications of Association for Comput- ing Machiner, 16 of 18 An Anonymous Electronic Voting Protocol For Voting Over The Internet. 1985. 28(10): 1030~1044

[31] Sirbu, J. Douglas Tygar. Netbill: an electronic commerce systems optimized for network delivered information and services. Proc. IEEE Compcon' 95. San Francisco. 1995

[32] M. Stadler, M. Piveteau, J. Camenisch. Fair blind signatures. In L. C. Guillou and J. Quisquater, editors, Advances in Cryptology-EUROCRYPT' 95, volume 921 of Lecture Notes in Computer Science. Springer-Verlag. 1995. 209~219

[33] S. Brands. An efficient off-line electronic cash system based on the representation problem. Report CS-R9323, CWI (Center for Mathematics

and Computer Science). Amsterdam. 1993

[34] Matthew K. Franklin, Moti Yung. Secure and efficient off-line digital money. In:eds.. Automata, Languages Colloquium. volume 700 of Lecture Notes in Computer Science. Sweden:Springer-Verlag. July, 5-9 1993. 265~27

[35] Y. Frankel, Y. Tsiounis, M. Yung. Indirect discourse proofs: achieving efficient fair off-line E-Cash. In Advances in Cryptology, Proc. Of Asiacrypt'96(Lecture Notes in Computer Science 1163). South Korea: Springer-Verla. 1996. 3~7

[36] T. Okamoto, K. Ohta. Universal electronic cash. Advances in Cryptology-Crypto'91(Lecture Notes in Computer Science). Springer-Verlag. 1992. 324-337

发表论文和参加科研情况说明

1.《一种新型的 Diff Over MPLS 的设计与实现》发表在《微型电脑应用》2004 年 11 月

2.《MIS 货运系统的软件开发过程》发表在《微机发展》2005 年 5 月

致谢

本文能够顺利完成，首先要感谢我的导师万振凯教授。论文的选题、研究、实现，直至最后的修改完善，都是在他的精心指导下完成的。万老师一直关注着论文的进展情况，并给予了许多及时、必要的指导，使我深受启迪。在攻读硕士学位的两年多的时间里，他严谨的治学态度、诲人不倦的良师风范、忘我的工作作风使我十分钦佩和敬仰。

此外，我要感谢网络中心的李静东、韩清、苏华等几位老师，在课题的研究过程中，他们给我提供了很多宝贵的意见和良好的实验条件，为本文的顺利完成打下了坚实的基础。