摘要

电子商务是在现代信息技术与经营管理活动相结合的背景下应运而生的一种新型动态商务活动，它将参与商务交易的各方即商家、顾客、金融机构以及政府等利用计算机网络联系起来，实现了交易的电子化。企业对消费者（B2C）电子商务模式是以Internet为主要手段，由商家或企业通过网站向消费者提供商品和服务的一种商务模式，是我国最早产生的电子商务模式。从长远来看，B2C电子商务将取得快速发展并最终在电子商务领域占据重要地位。然而，由于B2C电子商务的交易模式和安全技术方面存在着种种不足，使得诚信、支付和配送逐渐成为阻碍我国B2C电子商务发展的三大瓶颈。如何通过商务模式创新和安全技术的完善来解决这些瓶颈问题，促进我国电子商务快速、稳定的发展，成为当务之急。

本文简要介绍了电子商务的基本概念以及当前发展趋势，通过对B2C电子商务模式的分析，找出制约我国B2C电子商务发展的瓶颈问题存在的根源，并引入“安全电子交易中心”改进原有的商务交易模式，从体制上提出瓶颈问题的解决方案。同时本文深入分析了安全电子支付协议(SET)的工作原理、SET协议涉及的安全技术，阐述了基于SET的电子商务交易流程，分析其安全性。从技术的角度分析瓶颈问题存在的原因，并结合改进后的B2C电子商务模式，针对SET协议在实际应用中存在的某些不足，对SET协议进行了扩展及完善，明确了解决方案的交易流程。从而确定了一个体制和技术相结合的、全面的、系统的缓解我国B2C电子商务发展瓶颈的解决方案。

分析表明，改进的商务模式加上完善后的SET协议，能有效地缓解B2C电子商务所面临的瓶颈问题，促进我国电子商务快速、稳定的发展。

关键词： B2C 电子商务　瓶颈问题　商务模式　安全电子支付协议

Abstract

An new kind of dynamic commercial activity which electronic commerce is under which latter-day information technology and the management activity will unify the background arises at the historic moment, it participates in the commercial activity all quarters,the merchant,the customer,the financial organ and the government and so on using the computer network unifies,will realize on thoroughly the transaction electrification.An kind of electronic commerce model that corporation to Customer (Business to Customer,B2C) ,which using internet as its primary instrumentality through merchant or corporation provide consumer with merchandise and servings,it's the first arisen electronic commercial model in china at the same time. In the long term,B2C electronic commerce will achieved double-quick development and occupied the main position of electronic commerce realm finally. However, the faithfulness, secure payment and the logistics have become the three bottleneck problems which affect the development of B2C electronic commerce in chianl,due to some deficiency exist in the trading model and secure technology of B2C electronic commerce.How to solve these problems by the innovation of business models and the amelioration of secure technology, accelerate the rapid and steady development of electronic commerce in china is very exigent.

This article briefly introduce the electronic commerce basic concept and the current development tendency, through the analysis of B2C electronic commerce model, find the causation which cause the bottleneck problems that affect the development of B2C electronic commerce in chianl to be exist,then ameliorate the quondam commerce trading model wich a bring-in Secure Electronic Transaction Center,bring forward the institutional project to solve the bottleneck problems.At the same time,this article provides a further research on the operating rules and the encryption technologies used by SET(Secure Electronic Transaction) protocol,while the study explores the electronic commerce transaction process on the basis of SET and its concerning security. Find the technical causation which cause the bottleneck problems to be exist on the other side,then unite with the ameliorated commerce model,with regard to some deficiencies in practical use of SET protocol,some development and improvement are made to SET, the transaction process of new project is maken certain.An comprehensive project which is united with institution and technology to solve the bottleneck problems is framed in conclusion.

It's prove up to the hilt that the comprehensive project which is united with innovation of business models and the amelioration of secure technology can availably

solve the bottleneck problems that exist in the B2C electronic commerce , accelerates the rapid and steady development of electronic commerce in china.

Keywords: B2C Electronic Commerce Bottleneck problems Business Models Secure Electronic Transaction protocol

目录

第一章 绪论

1.1 研究背景

随着互联网络技术和信息技术的日趋成熟，互联网络规模日益扩大以及网络用户数量急剧增加，互联网络的应用已逐步渗入到社会的各行各业之中，与人们的日常工作和生活紧密地联系在一起。互联网络技术在全球的广泛使用，标志着人类社会开始进入网络经济时代，而网络经济时代一个最显著的特征就是信息技术在传统商业领域的应用，即电子商务。目前，电子商务正以其高效益、低成本的优势，逐步成为新兴的商业模式和理念。

B2C(Business to Customer B2C)电子商务是以Internet为主要手段,由商家或企业通过网站向消费者提供商品和服务的一种商务模式，是我国最早产生的电子商务模式。目前，在Internet上遍布了各种类型的B2C商务网站，向顾客提供从鲜花、图书到计算机、汽车等各种消费品和服务。由于各种因素的制约，目前以及未来比较长的一段时间内，这种模式的电子商务还只能占据比较小的比重。但是，从长远来看，企业对消费者的电子商务必将取得快速的发展，并将最终在电子商务领域占据重要地位。在整个电子商务中，B2C是最基础的一环，如果没有B2C，也就失去了B2B（Business to Business）最终发展的目标。互联网络规模的高速度增长为我国开展电子商务应用奠定了必要的信息网络基础。如何把握机遇，冲破种种障碍，大力发展我国的电子商务应用，是政府部门、各大中小型企业及信息技术专家都在考虑的问题，也是电子商务领域研究的重要课题。

电子商务在发展的过程中遇到了许多制约因素，由于电子商务中交易双方是不见面的，将会产生许多传统商务模式中不会出现的问题，本质上就是交易的安全性问题。从安全和信任的角度来看，传统的买卖双方是面对面的，因此较容易保证交易过程的安全性，同时交易双方便于通过交易建立起彼此的信任关系。但在电子商务的交易过程中，买卖双方是通过网络来联系的，由于网络本身的开放性、动态性等特征，使得交易双方很难在保障交易安全的基础上建立起相互间的信任关系。换句话说，电子商务交易双方(商家和消费者)都面临着安全威胁。同时，物流作为商务活动中不可缺少的一个环节，在电子商务环境下被赋予了更深的定义和内涵。作为一种特殊的 “商品”，物流将与实际商品一交付到消费者手中。然而，应运用何种商务模式或技术对此种特殊商品的交易过程及商品质量进行控制，成为电子商务发展过程中一个不可回避的问题。

可见，诚信、支付和配送已逐渐成为制约我国电子商务发展的三大关键性因素，如何通过商务交易模式的创新以及安全技术的改进增强电子商务交易的安全性，解决所面临的问题，已成为中国B2C电子商务发展的迫切需求。

1.2 电子商务概述

1.2.1 电子商务的定义及特点

一、电子商务的定义

电子商务，顾名思义是利用现代的信息技术所进行的商务活动。这些商务活动不仅包括与购销直接有关的网上广告、网上洽谈、订货、收款、客户服务、货物递交等活动，还包括网上市场调查、财务核算、生产安排等利用计算机网络开发的商业活动[1]。

电子商务的定义有广义和狭义之分。狭义的电子商务也称作电子交易(E-commerce)，主要是指利用网络提供的通信手段在网上进行的交易。而广义的电子商务，则是包括电子交易在内的利用网络进行的全部商业活动，如市场调查分析、客户联系、物资调配等等，也称为电子商业(E-business)[2]。

二、电子商务的特点

电子商务与传统的商务相比，除了具有一般商务的基本特征之外，还因为与信息技术的结合而被赋予了以下一些新的特征：

(1) 对网络的依赖性

电子商务以计算机网络作为商务信息传播、交流的重要手段。离开了网络，电子商务也就失去了其基本的通信功能，所以电子商务对网络有极强的依赖性。

(2) 开放性

由于电子商务是基于Internet的，而Internet是一个全球连接的庞大互联网络，所以电子商务轻易地跨越了地域的限制，使得商务活动可以在开放的空间中广泛地进行。

(3) 快捷性

信息技术的发展在改变信息交换方式的同时大大提升的信息传递的速度，电子商务使用现代信息技术来处理商务信息，使商务通信的处理速度大大加快，人们几乎可以用“思维的速度”来进行商务活动。

(4) 集成性

电子商务以计算机网络为主线，对商务活动的各种功能进行了高度的集成，同时也对参加商务活动的主体各方进行了高度的集成。集成性使电子商务的效率的到了进一步提升。

(5) 安全性

Internet是电子商务重要的交易平台，由于Internet的全球性、开放性、共享性、动态性等特征，使电子商务面临着许多安全威胁，从而对电子商务安全性提出了更新更高的要求。安全性是电子商务发展的重要保证。

1.2.2 电子商务的分类

电子商务有多种分类方法，通常可以从支付方法、参与主体、商务形式等不同的角度来对电子商务分类。

一、按支付方法对电子商务进行分类

从支付角度来分，电子商务业务可以分为支付型电子商务业务和非支付型电子商务业务。

二、按电子商务参与主体进行分类

根据电子商务参与主体和应用对象的不同，可将电子商务分为5类，即企业内部、企业对企业(Business to Business B2B)、企业对消费者(Business to Customer B2C)、企业对政府机构(Business to Government B2G)和消费者对政府机构(Customer to Government C2G)的电子商务，如图1.1所示。

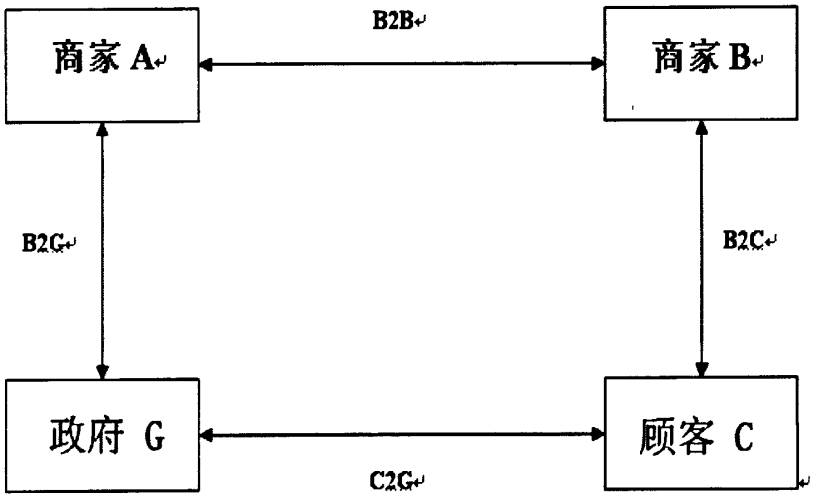

图1.1电子商务分类示意图

三、按商务形式对电子商务进行分类

电子商务从商务形式来分类，可以有邮购、零售、网上信息销售、电子商厦、预定、网上拍卖、文书传递等多种形式的电子商务。

1.2.3 电子商务的现状及发展趋势

电子商务是应用现代信息技术，通过计算机网络进行的商务活动。作为一种崭新的商务运营模式，电子商务有着独特的优势：它减少了许多繁琐的中间环节，大大降低了交易成本；它能快速准确地传递交易市场的需求信息，在极短的时间内完成交易手续；它可以大幅降低商品库存，缩短生产周期，加快市场开发；它可以不受时间和地域的限制，在全球范围内全天候地运行等等。正是因为这些优势，使电子商务在世界范围内得以迅速的发展。

据调查，1994年全球电子商务销售额为12亿美元，1997年达到26亿美元，增长了一倍多，1998年销售额达500亿美元，比1997年增长近20倍。联合国最近发表的一份报告表明，2000年全球电子商务的交易额已达到3770亿美元，2010年交易额可达10000亿美元，未来10年1/3的全球国际贸易将以网络贸易的形式来完成。专家预言，电子商务是21世纪经济增长的引擎。

电子商务在中国的发展可分为四个阶段:培育阶段(1998-2002年)；成长阶段(2003-2005年)；快速发展阶段(2006-2010年)；成熟阶段(2010年以后)。其中2005年是中国电子商务从成长阶段步入快速发展阶段的关键期。如今我国电子商务的发展已步入到了快速发展阶段，如图1.2所示。

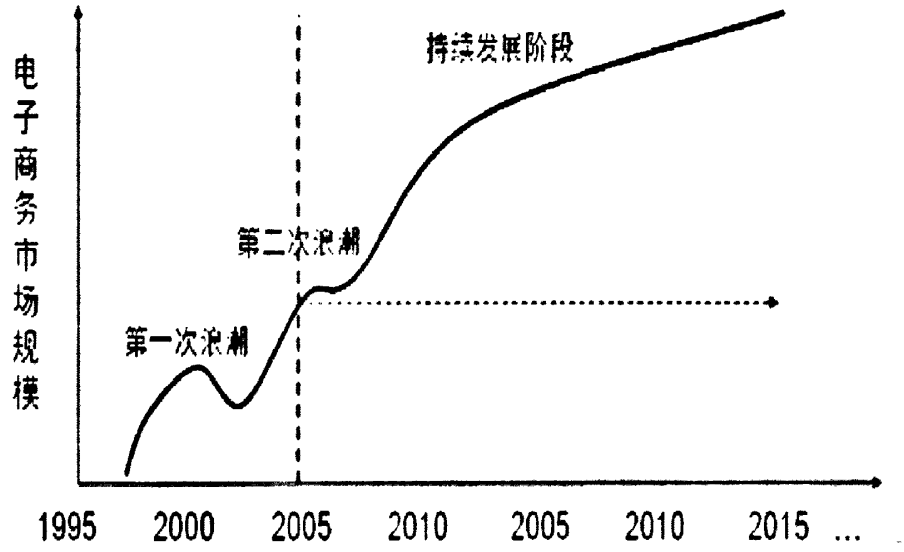

图1.2 未来电子商务发展趋势

据调查表明中国电子商务之所以有近年来的蓬勃发展，主要是由于以下三方面的巨大潜力得到了发挥[3]:

(1)不断增强的中国经济以及网络建设。

(2)不断增长的网民数量及上网公司。

(3)不断提升的电子商务相关服务。

但是，由于目前国内网络消费环境尚不完善，网上购物立法匮乏，与传统的购物环境相比，网上购物在在线支付、售后服务、质量保证等方面仍然难以让消费者放心，所以电子商务发展中的瓶颈问题依然存在，并制约着我国电子商务发展的速度。

1.3 制约中国电子商务发展的因素

在我国电子商务发展过程中还存在许多问题，如网络基础设施薄弱、电子交易安全存在漏洞、网上支付手段不健全、物流配送体系滞后、相关法律不完善、

信用体制不健全、企业信息化程度低、电子商务人才缺乏以及电子商务缺乏宏观调控、发展不平衡等。其中，诚信、支付和配送是严重制约我国B2C电子商务发展的三大核心瓶颈问题[4]。

一、诚信问题

在电子商务交易过程中，企业、消费者、银行、物流等任何一方诚信缺失，交易就不能顺利进行。不诚信的交易对象会对电子商务的安全造成极大的威胁，这些威胁主要表现为以下几种情况：

(1)欺诈，即假冒者冒用合法商家站点进行网上销售欺诈，或者假冒者冒用别人的信用卡进行支付欺诈等。

(2)信息被窃听和拦截，即一些与交易有关的商业或私人信息被非法的获取或阻截，从而影响交易的正常进行，给交易方带来损失。

(3)信息被篡改，即交易信息在传输中可能会被修改、重放或删除，在这些信息中商品信息、信用卡号信息以及物流信息等都是受攻击的对象。

(4)抵赖，即信息发送方否认曾经发送过某信息，或者信息接收方否认曾经收到过某信息。

由于这些诚信风险的存在，让交易的参与者对彼此的诚信问题心存疑虑，从而给电子商务的发展带来极大的影响。

二、支付安全问题

实现电子支付是电子商务成功运转的一个重要环节。电子商务如果缺失了相应的电子支付手段，就将大大降低电子商务交易的效率。电子支付是电子商务得以顺利发展的基础条件，同时它也是电子商务中安全性要求最高的一个环节。然而，由于体制和技术上的种种原因，让许多人感觉网上支付总是那么不安全，这是阻止很多人网上购物的原因。应通过何种电子支付方式安全公平地完成整个交易，增强电子商务交易的安全性，已成为我国电子商务发展过程中必须面对的重要问题。

三、配送问题

配送问题也就是商务活动中的物流问题，它是交易过程中不可缺少的一个过程。目前，对于网上的一笔交易，结算机构并不能获取物流的状态、控制物流的行为。用户对物流公司的身份无法认证，物流活动的质量处于非受控状态。物流作为一种特殊的商品，其产品质量与安全只能由自我监督来保证。一旦物流过程发生纠纷，发货方、承运方、接收方的责任将纠缠不清。退货、退款、退运费等权益的维护将要依靠漫长的法律途径去实现。所以，电子商务的物流问题同样成为了阻碍我国电子商务发展的瓶颈问题。

1.4 研究内容及意义

1.4.1 研究内容

随着全球信息化进程的不断深入，Internet得以迅速发展和广泛普及，基于Internet的电子商务已成为21世纪新的经济增长点。然而，由于Internet的全球性、开放性、动态性、共享性等原因，促使Internet的安全非常脆弱。同时，由于现有的B2C电子商务模式及其安全技术中存在着种种不足，致使诚信问题、安全支付问题和配送问题成为阻碍我国B2C电子商务发展的三大瓶颈，影响并制约了我国电子商务的发展。为了缓解这三大瓶颈，本文从对现有的B2C电子商务模式及安全技术的分析入手，结合商务模式的创新和电子商务安全协议的改进，提出了一个系统的，全面的问题解决方案。主要工作有：

1、B2C电子商务模式分析

本文简要介绍了我国B2C电子商务发展的现状，指出制约其发展的瓶颈问题，并对B2C电子商务模式进行分析、研究，从商务交易模式上分析“瓶颈”存在的原因。

2、B2C电子商务交易模式改进

结合商务模式分析的结论，引入“安全电子交易中心”对原有的B2C电子商务交易模式进行改进，并定义了安全电子交易中心的功能职责，从而从体制上提出缓解我国B2C电子商务发展瓶颈的解决方案。

3、电子商务安全技术研究

对B2C电子商务的安全技术进行分析，研究，从安全技术的角度分析“瓶颈”存在的原因，为下一步SET协议的研究及改进提供技术理论支持。同时确定技术解决方案设计的目标及原则。

4、SET协议扩展及完善

对安全支付协议SET进行了分析，研究。针对SET协议在实际应用中存在的某些不足，结合新的B2C电子商务交易模式对其进行了扩展及完善，从而从体制和技术两方面完善了缓解我国B2C电子商务发展瓶颈的解决方案。对SET协议的改进工作有：

1）SET协议对借记卡的支持，增强解决方案的适用性。

2）SET安全控制分级模型，增强解决方案的针对性。

3）SET协议的安全性及物流监控性增强，结合新商务交易模式，引入物流作为交易实体，定义安全电子交易中心的技术职能，确定了新交易模式的交易流程。

1.4.2 研究意义

电子商务是在现代信息技术与经营管理活动相结合的产物，换句话说，电子商务=电子+商务。商务模式创新和信息技术的变革是它发展的源动力，同时也是问题出现的根源。所以，如果仅从安全技术或商务模式一个方面入手去解决电子商务发展时所带来的问题的话，这样的解决方案是片面的。本文结合电子商务模式的创新及安全协议的修改，全面、系统地提出了缓解我国B2C电子商务发展瓶颈问题的解决方案，对于解决电子商务安全性问题和推动电子商务的进一步发展有着重要的学术和实用意义。同时也将对SET协议在我国的普及和推广提供参考和借鉴。

1.5 本章小结

本章主要介绍了电子商务的基本概念、发展状况、未来发展趋势及发展电子商务面临的主要问题；同时对本文研究背景进行阐述；最后介绍了本文所研究的主要内容及研究意义。

第二章 B2C 电子商务模式分析及改进

B2C电子商务是企业与消费者之间的电子商务，它是以Internet为主要商务手段，实现公众消费和服务，并保证与其相关的付款方式电子化的一种商务模式。本章将通过对B2C电子商务模式的分析，找到阻碍我国B2C电子商务发展的瓶颈问题存在的根源。同时，针对分析的结果改进B2C电子商务交易模式，从而从制度上提出缓解电子商务发展瓶颈的解决方案。

2.1 B2C 电子商务模式的基本内涵

电子商务模式(e-Business Model)是电子商务的商业模式(The Business Model for e-Business)的简称，是企业运作电子商务、创造价值的具体表现形式，它直接、具体的体现了电子商务的生存状态和生存规律。同时，电子商务模式也是一种关于企业产品流（服务流）、资金流、信息流及价值创造过程的运作机制，它包括三个要素：

（1） 产品、资金和信息流的体系结构。

（2） 不同商业角色在商务运作中获得的利益和收入来源。

（3） 企业在商务模式中创造和体现的价值。

随着Internet和电子商务应用的发展，出现了许多成功的电子商务模式，如按照参与电子商务交易的实体类型的B2B、B2C、C2C、B2G等电子商务，其中B2C电子商务是以Internet为主要手段,由商家或企业通过网站向消费者提供商品和服务的一种商务模式，是我国最早产生的电子商务模式，以8848网上商城(http://www.8848.net.cn/)正式运营为标志。在这种商务模式中，企业通过互联网为消费者提供一个新型的购物环境——网上商店，消费者通过网络在网上购物、网上支付等操作参与到商务活动中。目前虽然B2C电子商务的交易额在整个零售市场中所占比重较小，但其影响力和发展潜力是十分巨大的。针对于传统交易形式和其它电子商务模式而言，B2C电子商务模式拥有以下三点特征：

（1）交易金额小

目前消费者网上购物大多以日用消费品和娱乐服务为主，所以与B2B电子商务相比，B2C电子商务的交易金额相对较小；

（2）交易范围广阔

相对于B2B、C2C电子商务模式而言，B2C电子商务在具有电子交易地域广阔性的同时还具有商品种类的广阔性特征。

（3）个性化服务

在B2C电子商务中，卖方往往会按照客户要求的不同将商品做出精细的分类，而且由于数字产品具有可变形性，易于修改、重新组织和编辑，这些产品往往还可随各层次用户的不同要求而定制，因此B2C电子商务更多地体现为一种个性化的服务；

根据以上论述，B2C电子商务基本上等同于电子化的零售商务。目前在Internet上已遍布了各种类型的商业中心、虚拟商店和虚拟企业，向消费着提供各种商品或服务。

2.2 B2C 电子商务的现状及发展

随着Internet技术的不断发展应用，电子商务得以超常数发展，同时，电子商务的交易额的增长也十分迅猛。北美在线零售额以每年翻三番的速度增长。欧洲的电子商务虽然比美国起步晚了18个月，但也不甘落后，奋起直追。据Forrester Research 的报告预测：从2000年到2004年，欧洲国家的电子商务交易额将以每年100%的速度增长，并在四年内达到贸易总额16000亿欧元的水平，约占欧洲贸易总额的6%。同时，亚太地区信息产业发达的国家，电子商务也在迅速的发展。

目前在我国商务网站中以网上购物类为数最多，占商务网站总数的60%左右。在B2C网站中不仅有商品种类齐全的综合类网上购物商城——新浪商城、8848网上超市，还出现了许多销售某类产品的网上专卖店，如专门销售图书音像商品的卓越网、当当网上书店，专门销售女性家居、生活用品的伊族网，专门销售鲜花礼品的玫瑰花坊，专门销售IT产品的中关村在线等。目前网上商店所销售的商品种类集中在计算机软硬件、图书、音像制品、家用电器、通讯器材、礼品、服装服饰等。各类购物网站的比例大概是综合商城36%，图书音像14%，鲜花礼品12%，其他电脑通信、服装、家用电器等购物网站比例为38%。

中国互联网协会DCCI数据中心公布的第四届互联网调查数据表明，电子商务三种模式——B2B、B2C和C2C在2007年获得了快速的增长，未来还将保持高增长速度。2007年中国互联网B2C电子商务市场保持健康增长，B2C网站总收入为52.2亿元，同比增长33.5%。预计2008年B2C电子商务营收规模将超过70.9亿元，2009年有望达到98.6亿元。随着网络购物环境的好转，未来两年B2C电子商务交易模式将更受欢迎，用户数和年平均消费金额均会提高。

B2C电子商务系统是企业和消费者在“边交易边学习”方法的基础上逐步建立起来的，目前我国还处于市场经济体系有待进一步完善的时期，电子商务也还属于相对较新的交易模式，政府还需密切关注电子商务的发展方向，及时给予有关的政策支持，以减少交易规则形成过程中的不确定性。

2.3 B2C 电子商务模式分析

2.3.1 B2C 电子商务的主要经营模式

可以从不同角度对 B2C 的商务模式进行分类和分析。从企业和消费者买卖关系的角度分析 B2C 的商务模式主要分为卖方企业—买方个人的电子商务及买方企业—卖方个人的电子商务两种模式[5]。根据交易的客体分析可把 B2C 电子商务分为无形商品和服务的电子商务模式、有形商品和服务的电子商务模式以及综合模式。

一、无形产品和服务的电子商务模式

计算机网络本身具有信息传输和信息处理功能，无形商品和服务（如电子信息、计算机软件、数字化视听娱乐产品等）一般可以通过网络直接提供给消费者。无形商品和服务的电子商务模式主要有网上订阅模式、付费浏览模式、广告支持模式和网上赠予模式。

1、网上订阅模式

网上订阅模式指的是企业通过网页安排向消费者提供网上直接订阅，消费者直接浏览信息的电子商务模式。网上订阅模式主要被商业在线机构用来销售报刊杂志、有线电视节目等。

2、付费浏览模式

付费浏览模式指的是企业通过网页安排向消费者提供计次收费性网上信息浏览和信息下载的电子商务模式。付费浏览模式让消费者根据自己的需要，在网址上有选择地购买一篇文章、一章书的内容或者参考书的一页。在数据库里查询的内容也可付费获取。另外一次性付费参与游戏娱乐将会是很流行的付费浏览方式之一。例如统计报告、电子书、电子杂志、收费下载服务等都是付费浏览的实例。

3、广告支持模式

广告支持模式是指在线服务商免费向消费者或用户提供信息在线服务，而营业活动全部用广告收入支持。此模式是目前最成功的电子商务模式之一。由于广告支持模式需要上网企业的广告收入来维持，因此该企业网页能否吸引大量的广告就成为该模式能否成功的关键。而能否吸引网上广告又主要靠网站的知名度，知名度又要看该网站被访问的次数。广告网站必须对广告效果提供客观的评价和测度方法，以便公平地确定广告费用的计费方法和计费额。

4、网上赠与模式

网上赠与模式是一种非传统的商业运作模式，是企业借助于国际互联网用户遍及全球的优势，向互联网用户赠送软件产品，以扩大企业的知名度和市场份额。通过让消费者使用该产品，让消费者下载一新版本的软件或购买另外一个相关的

软件。由于所赠送的是无形的计算机软件产品，而用户是通过国际互联网自行下载，因而企业所投入的分拨成本很低。因此，如果软件确有其实用特点，那么是很容易让消费者接受的。比如，卡巴斯基、360 安全卫士等杀毒软件服务提供商经常提供网上赠与模式，从而提高企业的品牌形象，开发客户潜在价值。

二、有形商品的电子商务模式

有形商品是指传统的实物商品，采用这种模式，有形商品和服务的查询、订购、付款等活动将在网上进行，这种电子商务模式也叫在线销售。目前，企业实现在线销售主要有两种方式：一种是在网上开设独立的虚拟商店；另一种是参与并成为网上购物中心的一部分。网上实物商品销售的特点主要是网上在线销售在市场扩大的同时减少了交易中的摩擦，提高了交易效率。与传统的店铺市场销售相比，即使企业的规模很小，网上销售也可以将业务伸展到世界各个角落。例如，中国的名族特产放在互联网上，可以将产品卖到全世界去，其中，美国占20%、欧洲占35%，这样以来，产品的国际化门槛越来越低，国际消费者也不必跑到国外市场去买需要的产品。此外，戴尔电脑的直销也是一个很好的例子，戴尔创始人41岁的Michael Dell因为公司的迅速增长其个人净资产至2006年已达到117亿美元，跃居美国福布斯杂志2006年全球亿万富豪榜第十一位。取得这样的成绩来源于自己坚持和正确实施电子商务的B2C模式。同时，网上商店不需要象一般的实物商店那样保持很多的库存，如果是纯粹的虚拟商店，则可以直接向厂家或批发商订货，省去了商品存储的阶段，从而大大节省了库存成本。

三、综合模式

实际上，多数企业网上销售并不是仅仅采用一种电子商务模式，而往往采用综合模式，即将各种模式结合起来实施电子商务。Golf Web 就是一家有 3500 页有关高尔夫球信息的网站。这家网站采用的就是综合模式。其中 40%的收入来自于订阅费和服务费，35%的收入来自于广告，还有 25%的收入是该网址专业零售点的销售收入。该网址已经吸引了许多大公司的广告，如美洲银行、美国电报电话公司等。专业零售点开始两个月的收入就高达 10 万美元。综合模式也是 B2C 电子商务发展的一种趋势。

2.3.2 B2C 电子商务交易模式闭环

B2C 电子商务是指商家把有形或无形的商品通过互联网销售到顾客手中的过程。包括商家自建网站购物平台，以及去网上商城申请一个“铺面”开店两种方式。要完成一次网上购物交易，买卖双方必须经历以下 5 步过程：

（1）确定购买商品的内容

互联网在传递与处理信息方面有着无可比拟的优势，购物站点的 Web 程序能

与顾客在线交互，提供诸如购物车、比较购物、商品检索、在线议价等服务。这些服务是传统购物商场无法比拟的，是网络购物的优势所在。

在大家熟悉的网站购物车/订单模式下，选择商品，确认规格参数，确定订购数量，确定送货要求之后，就完成了购物的第一步——订单。

（2） 确定商品配送的方式

已经填写完成的订单下面要进入第 2 步，选择配送方式。有形商品的配送，也就是物流，这是一个让所有商家都会头痛的问题，它牵涉到整个社会的物流基础。通常 B2C 购物网站所提供的配送方式有平邮、快递送货上门、国内特快专递 EMS 等。消费者将从中选择一种配送方式，以便快速、安全的得到需要的物品。

（3） 确定付款的方式

配送方式选定之后，物流费用已经确定，整张订单的总金额也已经确定下来，交易双方下一步需要确定付款方式。通常有三种付款方式可供选择:

1、直接交易，款到发货。

这种付款方式要求买方先付款，买方收到货款后向买方发货。在款到发货模式下，顾客面临着极大的安全威胁。要求款到发货是许多网络欺诈者的常用手法。由于是直接交易，欺诈者能立即收到货款，一旦收到款之后，欺诈者就销声匿迹，给消费者带来极大的损失。同时，如果出现商品与买方的要求不符，或是在运输的过程中出现了破损、丢失等情况，所带来的经济损失也将直接附加在买方身上。

2、直接交易，货到付款。

这种付款方式要求卖方先发货，买方收到货物后付款结算。货到付款也存在风险，买家有可能毁约拒付。卖方不仅损失双程运输费用，还面临货物运输破损、变质、丢失的风险，以及生产资金被占用、要处理库存货品等压力。

3、引入第三方监管模式。

在这种付款方式下，买方先将购物款交给交易的第三方监管，等到收到货物后并确定其质量后，第三方从购物款中扣除相应的监管费后交给卖方，完成交易。当然，这种付款方式也存在一下一些不足之处:

首先，引入的第三方自身的公信力如何保证。第三方是对交易的资金流和物流进行监管的重要机构，它的公信力是交易顺利进行的重要保障，如果缺失了其公信力，第三方很有可能成为交易过程中的另一个欺诈者。

其次，第三方无法对交易各方的诚信进行正确的判断，也无法对物流的质量进行控制。目前，第三方比较流行的做法是，只要买家不投诉，在一段时间之后，第三方就会认为交易已经成功，并向卖家支付货款。

最后，引入第三方将增加了交易的总体成本，因为多进行了一次电子支付，买家首先将货款支付给第三方，然后由第三方再支付给卖方。而且在监管期内，资金还被第三方占用了一段时间，增加了卖方的资金周转压力。

（4）执行付款

买方选定了付款方式后，会根据选择的付款方式将购物款支付给卖方，完成交易的支付过程。支付与结算这一环节是电子商务整个流程中安全性最高的一个环节，因为它涉及到顾客、商家、银行等多个实体的信息安全。目前，常见的支付方式有三种：

1、传统的支付方式，包括 ATM 柜员机转账；去银行柜台汇款、异地账号存/取款，邮局汇款等。

2、通过金融机构的支付网关支付，这些支付网关包括各家银行、银联提供的在线支付网关、银联 ePOS 和第三方支付网关等。

3、电子钱包方式支付，它是由经营第三方支付网关业务的公司提供的一种支付方式。买卖双方先到同一家服务商处申请一个电子钱包账户，然后买方汇款给服务商，给自己的钱包账户充值，然后买方转账到卖方的钱包。服务商在卖方在提出结算请求时，把现金汇入卖方指定的银行账户。这类支付方式比较适合于小额支付。

（5）商品配送

在完成了以上四个步骤后，就进入了 B2C 电子商务交易的最后一个环节——商品配送。无论是有形商品还是无形商品，最终都要根据第 2 步所确定的配送方式配送到消费者的手中，完成整个交易过程，形成如图 2.1 所示的 B2C 交易闭环[6]。

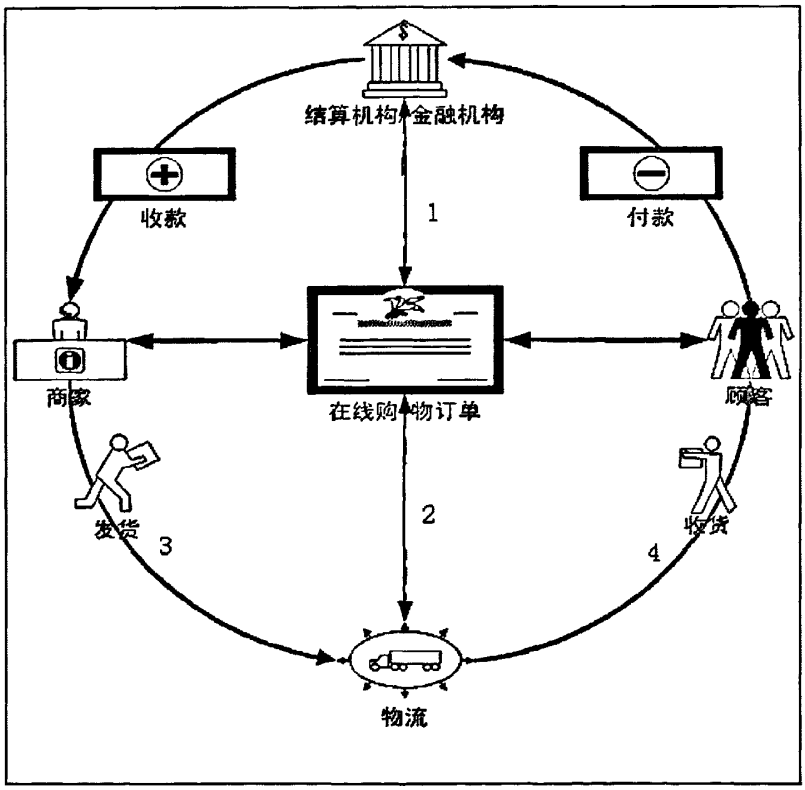

图2.1 B2C电子商务交易流程

2.3.3 B2C 电子商务发展瓶颈的体制成因分析

在图 2.1 所示的 B2C 交易闭环中，参与交易的参与方分别是商家、顾客、金融机构及物流。交易环中间水平线以上的半圆部分反映的是资金流，流向是从顾客流向商家，中间的参与方是金融机构。水平线以下的半圆部分（线 3 和线 4，图 2.1 所示）是物流，其流向是从商家流向顾客，中间参与方是物流公司。中间水平线则代表了信息流，其流向是双向的。

在 B2C 电子商务交易模式中，一张简单的购物订单将参加交易的各方联系起来，完成整个交易。如图 2.1 所示，虽然四个交易实体间的信息通信是畅通的，然而，任何一个交易实体都无法通过简单的信息通信确定与其交易的实体的真实身份，更无法对其诚信度作出准确的判断。使得商家、顾客、金融机构及物流在交易的过程中都面临着欺诈、信息窃取、抵赖等安全威胁。这是诚信问题成为制约我国 B2C 电子商务发展瓶颈的成因。

同时，在当前的电子商务体系中，普遍缺乏纵向的控制,即缺乏图中所示垂直的两条线(线 1 和线 2，图 2.1 所示)。由于线 1 的缺失，使得资金流在流通的过程中存在着窃取、篡改、重放等威胁。同时，由于线 2 的缺失，将导致线 3 与线 4 的收、发货过程实际也处于非受控状态。也就是说，顾客、银行并不能获取物流的状态、控制物流的行为，物流活动的质量处于非受控状态。这是支付安全问题、配送问题成为制约我国 B2C 电子商务发展瓶颈的成因。

由于以上交易控制环节的缺失，大大降低了 B2C 电子商务的安全性，同时也带来了不可避免的交易纠纷。一旦出现了交易纠纷，就意味着消费者、商家、金融机构或是物流公司需通过复杂且漫长的法律途径来解决纠纷，维护各自的合法权义。这极大地打击了交易各方参与电子商务的积极性，阻碍了 B2C 电子商务的发展步伐。

所以，不难看出，缺乏认证及信用评价体系、缺乏对支付安全及物流服务的监管控制是使得诚信问题、支付安全问题、配送问题成为制约中国 B2C 电子商务发展瓶颈的根本原因。要缓解这些瓶颈，应从健全认证体系、加强对支付安全及物流服务监管的控制的角度出发，针对 B2C 电子商务交易模式存在的问题对其进行改进，增强 B2C 电子商务的安全性，同时应确定合理快捷的交易纠纷解决机制，从而从体制改进的角度解决 B2C 电子商务发展所面临的瓶颈问题。

2.4 B2C 电子商务交易模式改进

业界称2005年是在线支付元年，2006年则是在线购物普及年，2007—2008年则是电子商务快速发展年，一些购物网站在诚信体系、支付与物流这三方面尝试新模式。本文认为，要解决我国电子商务发展的三大“瓶颈”，需要在原商务交

易模式中引入“安全电子交易中心”，以便其在完成交易各方身份认证的基础上合理的对支付安全及物流服务监管进行控制[7-10]，增强B2C电子商务交易的安全性，使物流服务的过程与质量得到有效的控制。同时，通过安全电子交易中心建立一个交易纠纷在线解决平台，以便合理、快捷地解决B2C电子商务交易过程中出现的交易纠纷。如图2.2所示，该中心主要的职能有：

1、交易各方身份的认证以及诚信度评价[11]

在交易过程中安全电子交易中心的第一个职能是对交易各方身份的认证，以次保证交易的真实性，从而承担起CA认证中心的工作职责，即解决电子商务交易中参与各方身份和资信的认定，维护交易活动的安全，从根本上保障电子商务交易活动顺利进行 。它通过对电子商务各参与方发放并管理数字证书，来确定各方

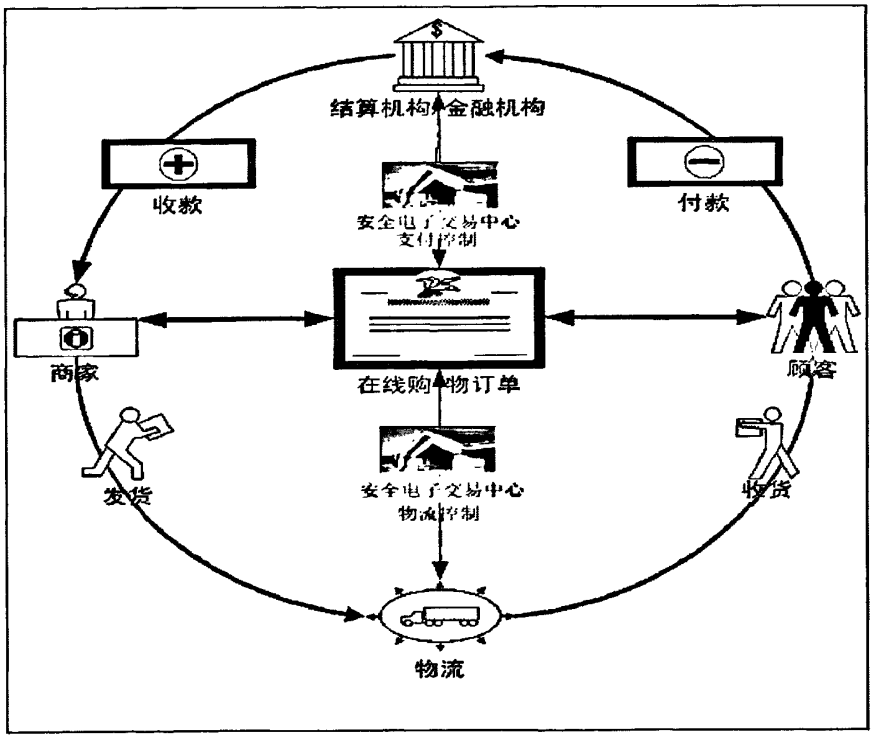

图2.2 改进后的B2C电子商务交易流程

的身份，并保证在 Internet 及内部网上传送数据的安全以及电子支付的安全。值得一提的是，在以往的交易模式中，物流被视为交易的一个过程，没有参与认证。在新的交易模式中，物流将作为交易的参与方而进行认证，从而保障物流身份的真实性。

除了完成身份认证的职责外，安全电子交易中心还必须通过对以往交易过程中数据的保存，建立诚信档案，准确评价交易各方的诚信度。以便于参与交易的各个实体可根据对彼此诚信度的判断，做出交易的选择。目前，我国有许多大型 B2C 电子商务交易平台采用站内买卖双方互评的方法来确定交易双方的诚信度。例如，淘宝网、eBay 易趣和拍拍网都采用信用评价的方式来保障本网站的诚信安

全。信用评价的方式、管理办法基本相同。具体措施有： (1)交易后，双方对本次交易做出评价，分“好”“中”“差”三等。并累计各种评价的个数，对参与者的评价可供查询。(2)根据反馈评价，通过数学模型得出对不同参与者的不同诚信等级，并对不同诚信等级做出相应的交易限制。这种诚信评价机制在激励诚实可靠的参与者累积良好的诚信度并长期留在交易市场的同时，也将淘汰不诚实者，从而减少非诚信行为的发生。当然，目前我国所有的诚信评价机制中并没有涉及对物流的诚信度评价，这也是此诚信评价机制的一个弊端。安全电子交易中心完全可以引用并健全此诚信评价机制，对参与交易的各方（包括物流及金融机构）的诚信度进行正确的评价后建立诚信档案，解决交易过程中的非诚信问题。

2、二次结算控制

在商家与顾客直接交易的模式下，不存在二次结算的问题。在由多个商家入驻 B2C 电子商务平台的多用户网上商城模式下，要能把顾客在这一平台上支付的款项结算给每一个商家，这一过程称为二次结算。

在 B2C 的交易闭环中，我们明显地看到，在款项的支付过程中，经历了结算机构这一环。买家直接付款给商家会面临诚信风险，因此，安全电子交易中心担任起了第三方结算控制的职能。其主要职能之一是管理的收与付，其二是对交易的结果做出确认，结算过程如图 2.3 所示。

用户通过支付网关将货款信息及对货物和物流服务的满意度交到安全电子交易中心，中心根据用户的满意情况将货款和物流费用交付到对应的商家和物流公司。这样可以降低买家所面临的诚信风险，同时也能对物流的质量进行控制，增强交易的安全性。

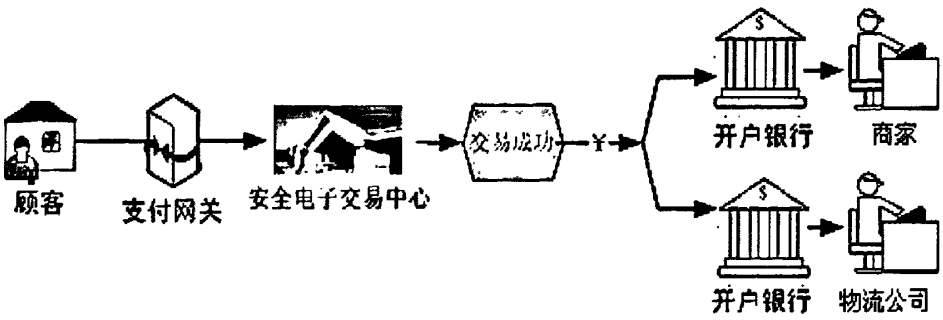

图2.3 B2C电子商务二次结算流程

值得说明的是，安全电子交易中心是二次结算的控制机构，而不是实际执行机构。它与目前电子商务交易过程中出现的第三方支付（比如：支付宝）不同，也就是说，用户的货款并不会交付给交易中心。交易中心的二次结算控制基于文中第四章要介绍的一种“资金冻结”机制，既在交易未完成前，交易中心会将用户帐户中的购货款冻结，待交易结束后再根据对交易结果的判断将用户帐户中的

冻结款项作出相应的分配。具体交易流程本文将在第四章中详细说明。

3、物流监控

安全电子交易中心除完成上述的身份的认证和二次结算功能以外，还需完成交易过程中的物流监控功能。

首先是物流费用计算，这是当前 B2C 网上购物流程断开的一环，通行的做法是由购物平台或商家定义了一组公式来计算物流费用。这一过程缺乏实际物流公司的在线参与。所以应在安全电子交易中心建立物流费用的产生机制。目标是：由实际的物流公司对某一票货的物流费用进行报价，该价格将作为物流商承运之后进行结算的依据。用户则可通过中心挑选符合自己需求的物流公司及其物流服务。

其次是收发货的过程监控。安全电子交易中心应担负起调度商家与物流公司工作进程的责任。首先是通知商家备货，然后由商家对完成备货的状态做出确认。这个确认是在 B2C 平台内完成的，商家要去点一下完成按钮。这个按钮一点，信息将流向物流公司环节。在物流公司打印出的提货单上，有相关的详细信息，例如有提货地址、货品明细、提货时间、包装规格等信息。物流公司拿着打印出的提货单到商家指定地点收货，如果货、单不符，物流公司有权拒收货物。物流公司的责任就是安全、按时把货物完好无损地送到指定地点，而中心则需对物流的质量进行监控，并将监控结果与用户满意情况相结合作为物流费用支付的依据。

4、在线交易纠纷解决[12]

安全电子交易中心完成上述三点主要职责后，可完善电子商务交易过程中的认证、安全支付、物流监控等环节。然而在商务交易过程中，交易纠纷是不可避免的。在传统的交易纠纷解决过程中，我国《消费者权益保护法》第 34 条规定了五种争议解决途径，即“消费者和经营者发生消费者权益争议时，可以通过下列途径解决：(一)与经营者协商和解；(二)请求消费者协会调解；(三)向有关行政部门申诉；(四)根据与经营者达成的仲裁协议提请仲裁机构仲裁；(五)向人民法院提起诉讼。” 这些解决途径针对 B2C 电子商务而言是极为不便的，同时也会降低用户参与电子商务的热情。因此安全电子交易中心应提供在线交易纠纷解决机制，在合法保护交易各方利益的前提下，灵活快速地解决 B2C 交易纠纷。在线交易解决机制的主要处理方式有：

（1）在线协商

在这种解决方式下，安全电子交易中心应向对交易过程有争议的各方提供一个在线交流的平台。各争议方可通过此平台交换各自的观点和请求，加强沟通，并最终达成一个确定的解决方案，并将其交付给安全电子交易中心，由中心负责下一步的执行，以最快的速度，最小的经济成本解决交易纠纷。

（2）在线调解

当一项争议发生时，争议的各方以在线的方式提交争议，然后由安全电子交易中心调解员调解。调解员按照规定的程序以及公平原则，帮助争议双方分析争议焦点，明确双方的利益，找出可能的解决途径，帮助当事人之间达成自己的解决方案。在整个争议解决过程中，调解员并不评价争议双方的对错，也不由调解员做出调解协议。调解员必须具有相关的专业知识或技能。如果调解成功，一般会有一份和解协议。最后，由安全电子交易中心负责和解协议的监督执行，解决交易纠纷。

（3）在线仲裁

在线仲裁是比较正式的一种纠纷解决方式。当交涉，调解无效时，安全电子交易中心可按照相关的法律法规，审查相关的交易事实和证据进行裁决。并通过“二次结算”的资金冻结机制执行仲裁。

当然，安全电子交易中心应在具有：中立性、合法性、易用性、低成本、透明性这五个基本原则的基础上完成交易纠纷的解决工作，以此增强 B2C 电子商务的可信性、安全性和稳定性，大力推动电子商务在我国的发展。

2.5 改进后的商务模式分析

在原有的 B2C 电子商务交易模式中引入了安全电子交易中心后，成功地完成了对交易过程中信息流、资金流及物流的监管与控制。同时，通过对安全电子交易中心的职责功能定义，增强了交易的安全性，解决了物流活动处于非受控状态的问题。

首先，对交易中心身份认证及诚信度评价的职能定义，使得交易各方容易通过身份的核实及诚信的判断建立起相互间的信任关系，减少交易所面临的欺诈、抵赖等安全威胁，保障交易的顺利进行。从而缓解了制约 B2C 电子商务发展瓶颈中的诚信问题。

其次，对交易中心交易中二次结算的职能定义，减少买家直接付款给商家所面临的支付风险，加强对交易过程中的资金流的控制，增强了支付安全性。同时为安全电子交易中心的物流控制职能以及一个隐身职能——“仲裁”奠定了基础，从而缓解了制约 B2C 电子商务发展瓶颈中的支付安全问题。

再次，对交易中心交易中物流控制的功能定义，在物流公司身份得以认证的基础上，通过对物流费用的计算以及对收发货过程的监控，使得物流的行为、物流活动的质量得到了很好的控制，提高了物流服务的质量。从而缓解了制约 B2C 电子商务发展瓶颈中的配送问题。

同时，对交易中心交易在线纠纷解决功能的定义，为 B2C 电子商务交易过程中的交易纠纷解决提供了一个公平、公开的解决平台和解决渠道，使得一些小的

交易纠纷可以得到快速、方便的解决，提高了广大用户参与电子商务积极性。

综上所述，改进后的 B2C 电子商务交易模式能有效的缓解电子商务发展瓶颈中的诚信问题、支付安全问题和配送问题。需要说明的是，以上对电子商务交易模式的该进仅仅是从体制上提出的一种解决方案，需要相关电子商务安全技术的支持。接下来本文将通过对电子商务安全技术的分析研究完善解决方案的技术支持，并通过对安全电子交易协议 SET 的修改，确定新交易模式的交易流程，并予于安全电子交易中心新的技术职能，从而完善缓解 B2C 电子商务瓶颈的解决方案。

2.6 本章小结

本章主要对 B2C 电子商务模式进行分析，找出我国 B2C 电子商务发展瓶颈的体制成因。针对分析的结论，引入安全电子交易中心并对其功能职责进行定义，改进原 B2C 电子商务交易模式，从体制上完成了缓解 B2C 电子商务瓶颈的解决方案设计。

第三章 B2C 电子商务安全技术研究

电子商务运用其商务构架为我们构建起了一个电子世界，在构架中有一个非常重要的支撑点——安全技术，电子商务的安全与否，决定着电子商务的成败。本章将对B2C电子商务的安全技术进行研究。从安全技术的角度分析"瓶颈"存在的原因，为下一步SET协议的研究及改进提供技术理论支持，同时确定技术解决方案设计的目标及原则。

3.1 电子商务安全

由于Internet的全球性、开放性、动态性、共享性及其它原因，使得Intemet安全非常脆弱。从而，影响和制约了电子商务的发展和普及。如何保障电子商务交易的安全和顺利进行，即如何实现电子商务的机密性、完整性、可鉴别性、不可伪造性和不可抵赖性是目前电子商务安全领域研究的热点。

3.1.1 电子商务面临的安全威胁

当前网络技术的飞速发展，新的威胁和脆弱点不断出现，从而对网络安全技术提出了更高的要求。电子商务在这样的环境中，时时处处受到安全的威胁。其安全威胁可分为以下四大类[13-14]:

(1)信息的截获和窃取:如没有采取加密措施或加密强度不够，攻击者可采用各种手段非法获得用户机密的信息。

(2)信息的篡改:攻击者利用各种技术和手段对网络中的信息进行中途修改，并发往目的地，从而破坏信息的完整性。这种破坏手段有三种:

篡改 ：改变信息流的次序。

删除 ：删除某个消息或消息的某些部份。

插入 ：在消息中插入一些无用的信息，让接收方读不懂或接收错误的信息。

(3)信息假冒:攻击者通过掌握网络信息数据规律或解密商务信息后，假冒合法用户或发送假冒信息来欺骗其用户。

(4)交易抵赖:指交易单方或双方否认曾进行的交易行为。

3.1.2 电子商务的安全需求

电子商务面临的威胁导致了对电子商务安全的需求[15-17]。 电子商务安全需求主要包括:机密性、完整性、认证性、不可抵赖性、不可拒绝性、访问控制性、匿名性、原子性等安全需求，如图3.1所示。

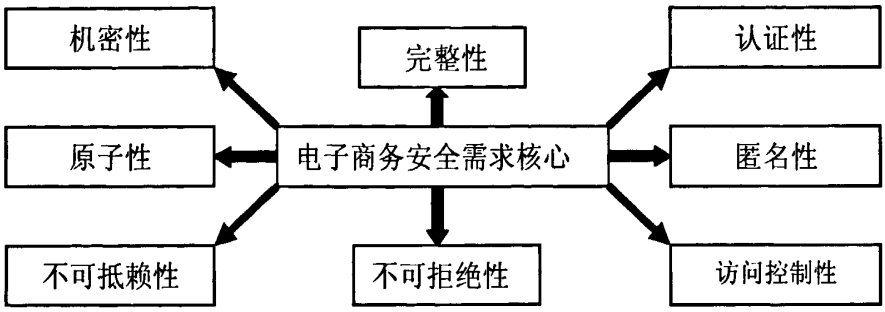

图3.1 电子商务的安全需求

1、机密性

机密性又叫保密性，是指信息在传送或存储的过程中不被他人窃取、不被泄露或披露未经授权的人或组织，或者经过加密伪装后，使未经授权者无法了解其内容。机密性一般通过密码技术对保密的信息进行加密处理来实现。

2、完整性

完整性又叫真实性，是保护数据不被未授权者修改、建立、嵌入、删除、重复传送或由于其他原因使原始数据被更改。完整性一般可通过提取信息消息摘要的方式来获得。

3、认证性

认证性也称为身份合法性，是指参与交易的各个实体在交易前相互确认对方的身份。在电子商务中，认证性一般都通过证书机构CA和证书来实现。

4、不可抵赖性

不可抵赖性又叫不可否认性，是指信息的发送方不能否认已发送的信息，接收方不能否认已收到的信息，这是一种法律有效性要求。不可抵赖性可通过对发送信息进行数字签名来获得。

5、不可拒绝性

商务服务的不可拒绝性又叫有效性，或可用性，是保证授权用户在正常访问信息和资源时不被拒绝，即保证为用户提供稳定的服务。

6、访问控制性

访问控制性是指在网络上限制和控制通信链路对主机系统和应用的访问，用于保护计算机系统的资源(信息、计算和通信资源)不被未经授权人或未授权方式接入、使用、修改、破坏、发出指令或植入程序等。

7、匿名性

匿名性指发送者匿名性、接收者匿名性、发送者与接收者之间的无连接性。其包含三个方面含义:信息分离、防勾结和匿名度。其中，匿名度是将匿名性从绝对隐藏、可能暴露、到暴露分为若个等级，用来衡量网络支付协议所达到的匿名

程度。

8、原子性

原子性是指整个支付协议(一般包括初始化阶段、订购阶段、支付阶段、清算阶段等)看作一个事务，保证要么全部执行，要么全部取消。原子性包括:钱原子性、商品原子性、确认发送原子性。

3.1.3 电子商务安全的特征

电子商务安全具有以下四大特性:

(1)电子商务安全是一个系统概念；电子商务安全问题不仅仅是个技术性问题，更重要的是管理问题，而且它还与社会道德、行业管理以及人们的行为模式都紧密地联系在一起。所以，电子商务安全是一个系统的概念，任何单方面通过技术手段或交易管理手段去解决电子商务安全问题的方法都是片面的，不完整的。

(2)电子商务安全具有针对性的；由于电子商务交易形式及交易商品的多样性，导致不同类型的电子商务对其安全性有不同的要求。一种安全机制或技术不可能适用于所有的电子商务商务形式和商品，所以电子商务安全具有针对性。

(3)电子商务安全是有代价的；电子商务交易活动中，其安全性与效率是一对矛盾体。如注重安全，就必定要以牺牲速度作为代价，反之亦然。所以电子商务的安全性的提高是以牺牲效率为代价的。

(4)电子商务安全是发展的、动态的；社会在不断发展，技术在不断地进步，没有一劳永逸的安全，也没有一蹴而就的安全。

3.2 B2C 电子商务安全体系结构

电子商务的安全控制体系结构是保证电子商务交易安全的一个完整的逻辑结构。主要有 5 个部分组成:即网络服务层、加密技术层、安全认证层、安全协议层、应用系统层。其中，上层是下层的扩展与递进；下层是上层的基础，为上层提供技术支持。各层次之间相互依赖、相互关联构成统一整体。各层通过各自的安全控制技术，实现各层的安全策略，保证电子商务系统的安全[18-19]。如图 3.2 所示。

电子商务系统是依赖网络实现的商务系统，需要利用 Internet 基础设施和标准，所以构成电子商务安全框架的底层是网络服务层，它提供信息传送的载体和用户接入的手段，是各种电子商务应用系统的基础，为电子商务系统提供了基本、灵活的网络服务。通过 Internet 网络层的安全机制(如入侵检测、安全扫描、防火墙等)保证网络层的安全[20]。

为确保电子商务系统全面安全，必须建立完善的加密技术和认证机制，加密

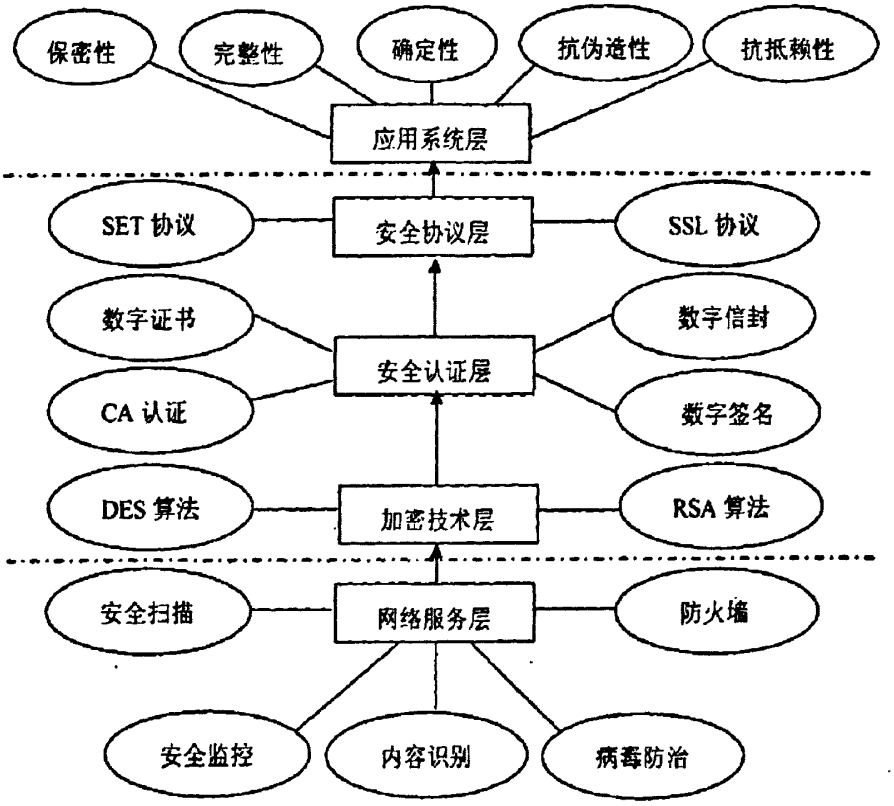

图3.2 电子商务安全技术框架体系结构图

技术层、安全认证层和安全协议层，即为电子交易数据的安全而构筑。其中，安全协议层是加密技术层和安全认证层的安全控制技术的综合运用和完善。

3.3 加密技术层

加密技术是电子商务采取的基本安全措施，贸易方可根据需要在信息交换的阶段使用。其基本功能是提供机密性服务。而且使用其它安全技术时也会使用加密技术[21]。加密算法通过扰频来保护信息。这样，只有信息所有者才能够阅读。

3.3.1 对称加密技术

对称加密又称为对称密钥加密、专用密钥加密。对称加密技术要求消息发送者和接收者共享同一密钥——用来加密和解密一个消息的一小块秘密消息。这样，除了发送者和接收者外，其他人都不能读出正确的消息。

DES 算法是对称密钥加密算法的代表[22-25]。DES 算法最初由 IBM 在 1970 年左右开发，在 1977 年经 NIST 提议把它选为国家标准后，它就成了美国政府的标准。以前，美国政府每隔几年就对 DES 算法重新作一次证明，但 1998 年，美国政府宣布不再证明 DES 了。对于 DES，一直有许多争论，最大的问题是它可能有一个未知的弱点，或者是只为 NSA 所掌握的弱点。原来 DES 建议的密钥长度为 64 位，但在它被批准成为标准前被减少到 56 位，于是有人认为减少密钥长度使得美

国政府可以使用 NSA 功能强大的计算机系统破译密码。56 位密钥空间的 DES 算法已经被认为是经不起攻击的了。

图 3.3 描述了 DES 算法的工作原理.基本上说，DES 算法所做的就是 16 次的迭代，把各块明文交织起来并与从密钥中获得的值混合.下面以 56 位的 DES 算法为例，简要地阐述一下 DES 算法的整个工作流程:

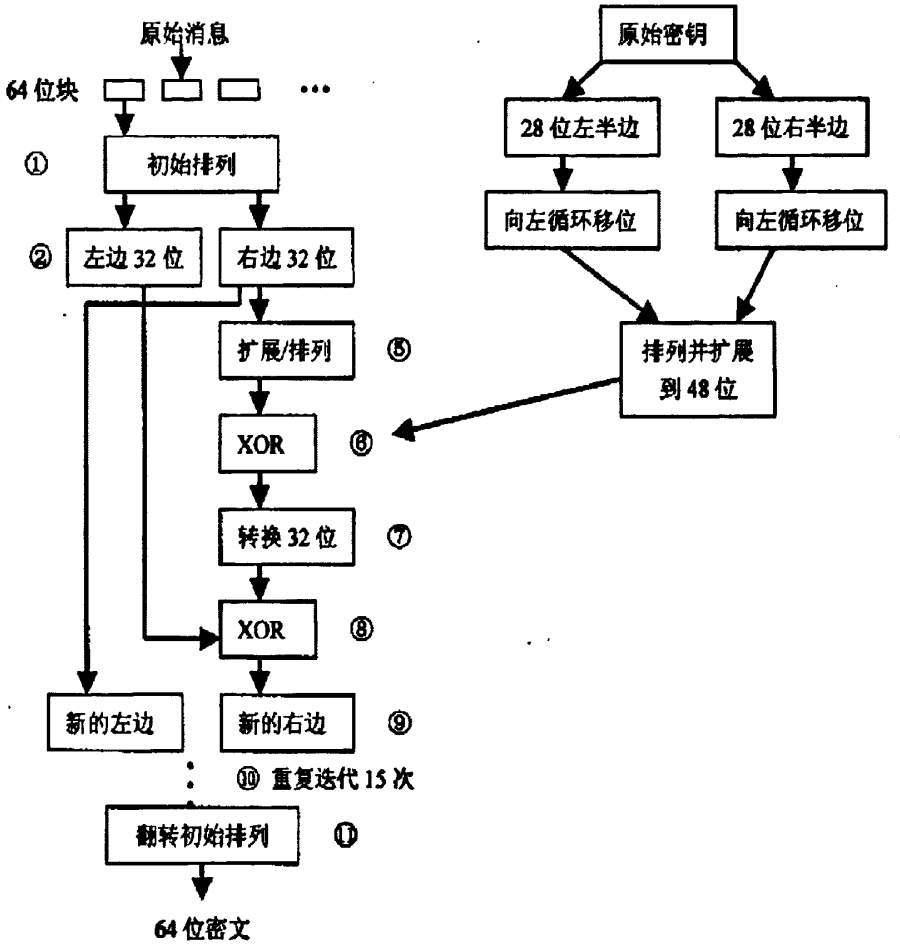

图3.3 DES加密过程

(1) 在左边，64 位的明文被修改(排列)以改变位的次序；

(2) 把明文分成两个 32 位的块；

(3)在图中密码一侧，原始密钥被分成两半；

(4)密钥的每一半向左循环移位，然后重新合并、排列，并扩展到 48 位，分开的密钥仍然保存起来供以后的迭代使用；

(5)在图的明文一边，右侧 32 位块被扩展到 48 位，以便与 48 位的密钥进行异或(XOR)操作，在这一步后还要进行另一次排列；

(6)把第三步和第五步的结果(明文与密钥)进行 XOR 操作；

(7)使用置换函数把第 6 步的结果转换 32 位；

(8)把第 2 步创建的 64 位值的左边一半与第 7 步的结果进行 XOR 操作；

(9) 第 8 步的结果和第 2 步创建的块的右半部分共同组成一个新块，前者在右边，后者在左边；

(10) 从第 4 步开始重复这个过程，迭代 16 次(连上之前的一次共 16 次)；

(11)完成最后一次迭代后，对这个 64 位块进行一次翻转，得到一个 64 位的密文。对原始明文中的下一个 64 位块重复整个过程，直到把原始消息加密完毕。

3.3.2 非对称加密技术

非对称加密又称为公开密钥加密。利用该方案实现机密信息交换的基本过程是；贸易方甲生成一对密钥并将其中的一把作为公开密钥向其他贸易方公开；得到该公开密钥的贸易方乙使用该密钥对机密信息进行加密后再发送给贸易方甲；贸易方甲再用自己保存的另一把私有密钥对加密后的信息进行解密。

一、RSA 加密算法

RSA 算法是非对称加密领域内最为著名的算法[26-27]，同时 RSA 也是当前最广泛流行的公开密钥加密系统。不同于 DES, RSA 使用两个密钥:一个公开的密钥(公钥)和一个秘密的密钥(私钥)。公钥被用于加密消息，而私钥用于解密消息。当然也可以反过来使用。一般地，公钥有两大类用途:

1、用于验证数字签名:消息接收者使用发送者的公钥对消息的数字签名进行验证。

2、用于加密消息:消息发送者使用接收者的公钥加密用于加密消息的密钥(如 DES 对称密钥)，进行数据加密密钥的传递。

RSA 算法的强度是基于一个非常大的数的因子分解的困难程度。RSA 算法的数学理论来自于“模与整数”的数论特性，RSA 利用了欧拉(Euler)函数中 $\Phi(n)$ 的特性。一个数的欧拉函数被定义为比这个数小且与这个数互素的整数的个数。

RSA 算法使用这个被 Euler 发现的数论特性是:对于任意的整数 i 和 n，且 i 和 n 互素，则有:

$$i^{\Phi(n)} \bmod n \equiv 1 \tag{3-1}$$

假设 e 和 d 是随机整数，并且:

$$e \times d \equiv 1 \bmod \Phi(n) \tag{3-2}$$

另一个被 Euler 发现的数论特性指出:如果 M 是任何与 n 互素的整数，则有:

$$(M^e)^d \bmod n \equiv M \text{ 以及} (M^d)^e \bmod n \equiv M \tag{3-3}$$

将这个特性用于密码技术时，如果 M 是消息的一个部分，我们就可以用函数

$$s \equiv M^e \bmod n \tag{3-4}$$

对它编码。同时用函数

$$M \equiv s^{d} \bmod n \tag{3-5}$$

对它解码。

利用上述 Euler 数论特性，RSA 密钥生成的步骤是:

（1）选取两个大素数 p 和 q，通常要求 p×q 均大于 10^{100}；

（2）计算 n= p×q 和 z=(p-1) ×(q-1);

（3）找出一个小于 n 的数 e，使 e 与 z 互素;

（4）另找一数 d，使满足(e×d) mod z ≡1 ；

（5）(n, e)即公钥，(n, d)即私钥。

为了加密一个消息 m，我们把 m 划分为一些比 n 小的固定长度的整数，然后对每一个信息段 M，计算它的编码: $S \equiv M^{e} \bmod n$，S 是密文块。如果采用专门的硬件或是使用特殊算法的软件，这个计算可以很快完成。这些密文块连接起来就是信息 m 的密文 s 。

要解密一个密文 s，将它划分成相应的信息段 S，用算法 $M \equiv S^{d} \bmod n$ 对每一小段密文解密，拼起来就是完整的明文 m 了。

在实际应用中，RSA 常常使用数百位长的十进制，所以计算起来非常费时间，当前的 RSA 应用的设计要点是尽量减少 RSA 的计算量。

二、椭圆曲线加密算法

椭圆曲线可以定义在任意的有限域上，主要在有域 Zp(p 为素数)和特征为 2 的有限域 F2m。(m≥1)上。椭圆曲线密码体制的加密原理基于有限域上椭圆曲线离散对数问题(ECDLP)的困难性。下面以定义在奇特征域上的椭圆曲线为例，说明椭圆曲线密码体制的加密原理[28]。

设 GF(p)是一个 P≠2，3 的奇特征有限域，定义在 GF(P)上的椭圆曲线是指满足 Weierstrass 方程：y2=x3+ax+b(a，b∈GF(p)，且满足 4a3+27b2≠0)的所有解，(x，y)∈GF(p)*GF(p)与无穷远点 O 构成的非空集合。设 P 是椭圆曲线 E（a，b）(GF(p))上的一个点，则 E 上关于户的椭圆曲线离散对数问题为：给定一点 Q∈E（a，b）(GF(p))，求解整数 x(x∈GF(p))，使 xP=Q。如果这样的数，存在，就是椭圆曲线离散对数。也就是说选取该椭圆曲线上的一个点 P 作为基点，给定一个整数 x，求解 xP=Q 是容易的。但是要从 Q 点和 P 点推导出整数 x，则是非常困难的。

基于椭圆曲线的密码体制操作都包含由一些椭圆曲线域参数所确定的有限域上椭圆曲线的算术运算。通常，将有限域上椭圆曲线域参数 T 定义为一个六元组：T=(p，a，b，C，n，h)。其中 p，a，b 的意义同上；G(xCG，yG)是椭圆曲线上的一个基点，G≠O，使 nG=O 的最小正整数 n 称为点 C 的阶，记为 n=ord(G)；整数

h 是余因子，$h \neq E(GF(p)) / n$。由以上参数可以惟一地确定一个椭圆曲线。在[1，n-1]之间随机地确定一个整数 d，计算 Q=dG，由此就确定了密钥对(d，Q)，其中：d 是私钥，需要保密，Q 是公钥，可以公开。而六元组 T 也要完全公开。

三、椭圆曲线与 RSA 的比较

椭圆曲线密码算法相对于 RSA 系统而言，其离散对数的困难性在计算复杂度上达到了全级指数。而 RSA 所基于的大整数因子分解问题只是亚指数级，因此对于椭圆曲线密码算法来说，只需要 180 位左右的密钥就可以达到 1024 位 RSA 算法提供的安全等级。所以，在 SET 协议中使用椭圆曲线密码的加密和签名算法代替 RSA 算法，在相同等级的安全条件下，将使网络交易的性能和速度获得显著的提高。

3.4 安全认证层

目前，仅有加密技术不足以保证电子商务中的交易安全，身份认证技术是保证电子商务安全不可缺少的又一重要技术手段。认证的实现包括数字签名技术、数字证书技术和智能卡技术等。

3.4.1 数字摘要

数字摘要是个特殊函数，称为单向散列函数[29-30]。单向散列函数 H( )作用于一任意长度的消息 M,它返回一固定长度的散列值 h: h=H(M)。其中 h 的长度为 m。单向散列函数拥有如下特性:

1) 给定 M,则很容易计算 h。

2) 给定 h ，根据 H(M) = h 逆计算 M 不可能或非常困难。

3) 给定 M,要找到另一消息 M' 并满足 $H(M)=H(M')$不可能或非常困难。

单向散列函数是公开的，也无需密钥，它的安全性即它的单向性。一般而言，输入值的单个位的改变将引起散列值中一半以上的位改变。

3.4.2 数字签名

数字签名是非对称机密技术中的一种技术[31-32]。其主要方式为：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)，接着荐用发送方的公歼密钥来对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并实现不可否认性。

3.4.3 数字时间戳

同传统商务一样，日期和时间是商务文件中的重要内容之一，需要加以确认与保护。同样，在电子商务中，也需对交易文件的日期和时间信息采取安全措施。数字时间戳服务（DTS）是网上安全服务项目，由专门的机构提供。时间戳(time-stamp)是一个经加密后形成的凭证文档，它包括三个部分:

1)需加时间戳的文件的摘要(digest)；

2)DTS 收到文件的日期和时间；

3)DTS 的数字签名。

时间戳产生的过程为:用户首先将需要加时间戳的文件用哈希编码加密形成摘要，然后将该摘要发送到 DTS, DTS 在加入了收到文件摘要的日期和时间信息后再对该文件加密(数字签名)，然后送回用户。需要强调的是，书面签署文件的时间是由签署人自己写上的，而数字时间戳则不然，它是白认证单位 DTS 签署的，以 DTS 收到文件的时间为依据。因此，时间戳也可作为科学家的科学发明文献的时间认证。

3.4.4 数字证书

数字证书技术与公钥基础设施息息相关，从字面上去理解，公钥基础设施(Public Key Infrastructure,PKI) 就是利用公钥密码理论技术建立的提供安全服务的基础设施。所谓基础设施，就是在某个大环境下普遍使用的系统和准则[33]。

PKI 是一种遵循标准的密钥管理平台，主要包括五个模块:CA (Certification Authority，认证中心)、证书库(Certificate Database)、密钥管理(生成、备份、恢复和更新)系统(Key Manage System)、证书撤销管理系统(Certificate Revocation List Manage System)和 PKI 应用接口系统(PKI ApplicationIn terface System)PKI 平台总体框架结构如图 3.4 所示:

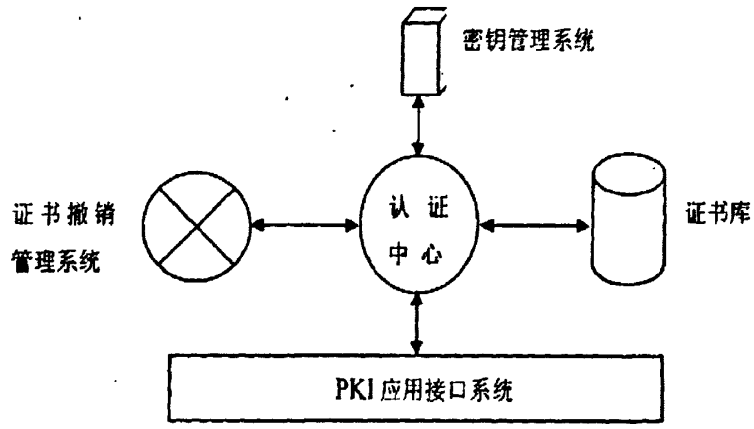

图3.4 PKI总体结构图

通常来说 ，CA 是证书的签发机构，它是 PKI 的核心。CA 通过对电子商务各参与方发放并管理数字证书，来确定各方的身份，并保证在 Internet 及内部网上传送数据的安全以及电子支付的安全。一个典型的 CA 系统包括安全服务器、注册机构 RA (Register Authority)、CA 服务器、LDAP(L ightweight Directory Access Protocol，轻量目录访问协议)、目录服务器和数据库服务器等。它的结构如图 3.5 所示。

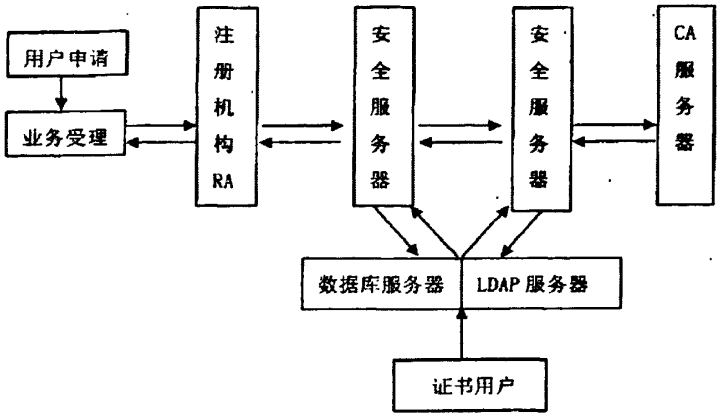

图3.5 典型CA结构图

对于一个大型的应用环境，CA 往往采用一种多层次的分层结构，各级的 CA 类似于各级行政机关，上级 CA 负责签发和管理下级 CA 的证书，最后一级的 CA 直接面向最终的用户。CA 主要功能包括证书的颁发、证书的更新、证书的查询、证书的作废以及证书的归档。

数字证书又称为数字凭证，是公开密钥体系的一种密钥管理媒介。它是一种权威性的电子文档，形同网络计算环境中的一种身份证，用于证明某一主体(如人、服务器等)的身份以及其公开密钥的合法性，又称为数字 ID。数字证书的内部格式是由 CCITTX. 509 国际标准所规定的，包含以下内容：证书拥有者的姓名、证书拥有者的公共密钥、公共密钥的有效期、颁发数字证书的单位、数字证书的序列号。数字证书的使用涉及到数字认证中心 CA。

目前，数字证书有个人证书、企业证书、软件证书，其中前两类较为常用。

个人证书(Personal Digital ID)：仅仅为某单个用户提供凭证，用以帮助其个人在网上进行安全交易操作。

企业凭证(Server ID)：通常为网上的某个 Web 服务器提供凭证，拥有 Web 服务器的企业就可以用具有凭证的互联网站点(Web Site)来进行安全电子交易。

3.5 安全协议层

网络安全是实现电子商务的基础，而一个通用性强，安全可靠的网络协议则是实现电子商务安全交易的关键技术之一。目前，比较成熟的协议有 SET, SSL, iKP

等基于信用卡的交易协议；NetBill,NetCheque 等基于支票的交易协议；Digicash, Netcash 等基于现金的交易协议，匿名原子交易协议[34-36]。

3.5.1 SSL 协议

安全套接字层协议 SSL(Secure Socket Layer)是 Netscape 公司于 1996 年推出的安全协议。SSL 协议的实现属于 SOCKET 层，位于传输层和应用层之间，由 SSL 记录协议(SSL Record Protoc0l)和 SSL 握手协议(SSL Handshake Protoc01)和 SSL 警报协议(SSL Alter Protoc0l)组成的，其结构如图 3.6 所示。

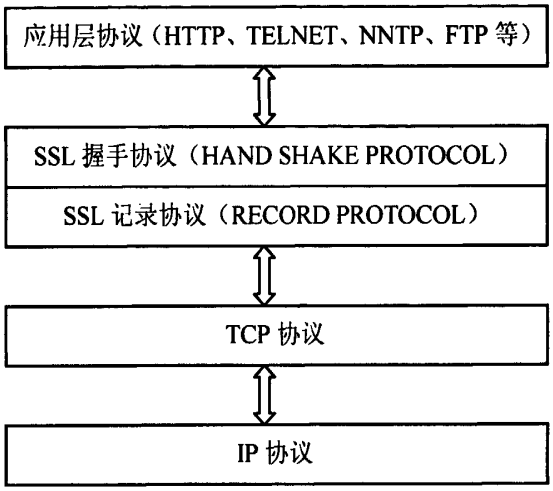

图3.6 SSL在TCP/IP网络分层结构模型中的位置

SSL 握手协议被用来在客户与服务器真正传输应用层数据之前建立安全机制。当客户与服务器第一次通信时，双方通过握手协议在版本号、密钥交换算法、数据加密算法和 HASH 算法上达成一致，然后互相验证对方身份，最后使用协商好的密钥匙交换算法产生一个只有双方知道的秘密信息，客户和服务器各自根据此秘密信息产生数据加密算法和 Hash 算法参数。SSL 记录协议根据 SSL 握手协议协商的参数，对应用层送来的数据进行加密、压缩、计算消息鉴别码 MAC(Message Authentication Code)，然后经网络传输层发送给对方。SSL 警报协议用来在客户和服务器之间传递 SSL 出错信息。

3.5.2 SET 协议

SET 协议(Secure Electronic Transaction)是为了在 Internet 上进行在线交易时保证信用卡支付的安全而设计的一个开放的规范，它是由维萨国际组织(VISA)和万事达(MasterCard)两大信用卡公司于 1997 年 5 月联合推出的能保证通过开放网络进行安全支付的技术标准，内容包括 SET 的交易流程、程序设计规格和 SET 协议完整性描述三个部分。它采用 RSA 公开密钥体系对交易双方进行认证，利用 DES 对

称加密方法进行信息的加密传输，并用 Hash 算法鉴别消息真伪、有无篡改。

SET 支付系统主要由持卡人、商家、发卡银行、收单银行、支付网关及认证机构等六个部分组成，由 CA 根据 X.509 标准发布和管理证书，提供了保密、数据完整、用户和商家身份认证及顾客不可否认等功能。本文将于第四章对 SET 协议的工作原理、交易流程等进行详细论述。

3.5.3 SSL 与 SET 协议的比较

1、在认证要求方面，早期的 SSL 并没有提供商家身份认证机制，虽然在 SSL3.0 中可以通过数字签名和数字证书可实现浏览器和 Web 服务器双方的身份验证，但仍不能实现多方认证；相比之下，SET 的安全要求较高，所有参与 SET 交易的成员（持卡人、商家、发卡行、收单行和支付网关）都必须申请数字证书进行身份识别。

2、在安全性方面，SET 协议规范了整个商务活动的流程，从持卡人到商家，到支付网关，到认证中心以及信用卡结算中心之间的信息流走向和必须采用的加密、认证都制定了严密的标准，从而最大限度地保证了商务性、服务性、协调性和集成性。而 SSL 只对持卡人与商店端的信息交换进行加密保护，可以看作是用于传输的那部分的技术规范。从电子商务特性来看，它并不具备商务性、服务性、协调性和集成性。因此 SET 的安全性比 SSL 高。

3、在网络层协议位置方面，SSL 是基于传输层的通用安全协议，而 SET 位于应用层，对网络上其他各层也有涉及。

4、在应用领域方面，SSL 主要是和 Web 应用一起工作，而 SET 是为信用卡交易提供安全，因此如果电子商务应用只是通过 Web 或是电子邮件，则可以不要 SET。但如果电子商务应用是一个涉及多方交易的过程，则使用 SET 更安全、更通用些。

总之，SSL 协议比较简单，应用较广，但安全性较差；SET 协议十分复杂，价格昂贵，加密环节多，推广较难，但安全性较高。

3.6 B2C 电子商务发展瓶颈的技术成因分析

除了以上所介绍的安全技术外，病毒防范技术、防火墙技术等等也是电子商务中常用的安全技术。由于当前网络技术的飞速发展，新的威胁和脆弱点不断出现，这使得基于计算机网络的 B2C 电子商务面临着许多安全威胁，从而增加了电子商务的安全需求。所以不难看出，加强电子商务安全技术的可靠性、安全性，满足电子商务的安全需求是解决 B2C 电子商务发展瓶颈的技术根本。同时，结合新的 B2C 电子商务交易模式，技术解决方案因注意以下三个方面的技术性要求：

1）适用性

在电子商务交易过程中，由于交易模式、交易对象、交易的商品等交易条件的不同，将对电子商务的技术提出不同的要求，应针对这些不同的要求完善技术方案的设计，提高安全技术的适用性。

2）针对性

电子商务的安全是有代价的，其安全性与效率是一对矛盾体，每一种安全技术都对应着安全性和效益间的一个平衡点。由于交易规模、交易商品、顾客的要求等交易因素的不同，其对安全性和效率的要求也不同。方案设计时应针对这些不同的要求寻找平衡点，提高技术方案的针对性。

3）安全性

安全性是技术解决方案的根本，要求技术方案应满足机密性、完整性、认证性、不可抵赖性、不可拒绝性、访问控制性、匿名性、原子性等 B2C 电子商务安全需求，为缓解我国 B2C 电子商务发展瓶颈的解决方案提供可靠的技术支持。

3.7 本章小结

本章对 B2C 电子商务的安全技术进行了分析，研究。从安全技术的角度分析“瓶颈”存在的原因，为下一步 SET 协议的研究及改进提供技术理论支持，同时确定了技术解决方案设计的目标及原则。

第四章 SET 协议的分析及完善

电子商务安全协议是完成信息安全交换的共同约定的逻辑操作规则，是保证网上交易的机密性、数据完整性、身份的合法性和抗否认性的重要技术。本章将对安全支付协议 SET 进行分析，研究。针对 SET 协议在实际应用中存在的某些不足，结合新的 B2C 电子商务交易模式对其进行改进并确定交易流程，从体制和技术两方面完善缓解我国 B2C 电子商务发展瓶颈的解决方案。

4.1 SET 协议概述

4.1.1 SET 协议介绍

在 Interne 上开发对所有公众开放的电子商务系统，从技术角度讲，关键的技术问题有两个:一是信息传递的准确性；二是信息传递的安全可靠性。前者是各种数据交换协议已经解决了的问题，后者则是目前学术界、工商界和消费者最为关注的问题。为此，西方学者和企业界在这方面投入了大量的人力、物力。Visa 和 Mastercard 以及其他一些业界的主流厂商通过多年的研究，于 1996 年提出了安全电子交易协议 SET，并在 1997 年 5 月正式发布了 SET1.0 标准。这个标准自推出之后，得到了 IBM, Netscape, Microsoft, Oracl。等众多厂商的支持。SET 协议是应用层的协议，是一种基于消息流的协议，它是面向 B2C 模式的，完全针对信用卡来制定，涵盖了信用卡在电子商务交易中的交易协议信息保密、资料完整等各个方面。

在 SET 协议中主要定义了以下内容:

① 加密算法的应用；

② 证书消息和对象格式；

③ 购买消息和对象格式；

④ 请款消息和对象格式；

⑤ 参与者之间的消息协议。

SET 协议确保了网上交易所要求的保密性、数据的完整性、交易的不可否认性和交易的身份认证。

4.1.2 SET 协议实现的目标

SET 协议是一个基于可信的第三方认证中心的方案，其主要的实现目标是[37]:

① 保证电子商务参与者信息的相互隔离。持卡人的资料加密或打包后到达银行，商家看不到持卡人的帐户和密码信息，银行看不到持卡人的购物信息。

② 保证信息在因特网上安全传输，防止数据被黑客或被内部人员窃取。

③ 解决多方认证问题，不仅要对消费者的信用卡认证，而且要对在线商店的信誉程度认证，同时还有消费者、在线商店与银行间的认证，保证付款的安全。

④ 保证网上交易的实时性，实现在线支付。

⑤ 提供一个开放式的标准，规范协议和消息格式，促使不同厂家开发的软件具有兼容性和互操作功能，并且可以在不同的硬件和操作系统平台上运行。

4.2 SET 交易过程

4.2.1 SET 交易的参与方介绍

SET 改变了支付系统中各个参与者之间交互的方式。在面对面的零售交易或邮购交易中，电子处理过程始于商家或付款银行；而在 SET 交易中，电子支付始于持卡人。SET 交易的参与方包括持卡人、商家、发卡银行、收单银行、支付网关和数字证书认证中心 CA[38]。

1） 持卡人

SET 交易是在开放的 Internet 中进行的，交易双方互不见面，无法使用现金，而是使用信用卡，所以在 SET 协议中将购物者既买方称为持卡人。持卡人要参加 SET 交易，首先必须要拥有一台能够上网的计算机，保障畅通的信息通信；其次还必须到发卡银行去申请并取得一套 SET 交易专用的持卡人软件(即电子钱包)，然后安装在自己的计算机上；第三，必须上网去向数字证书认证中心申请一张数字证书。这样持卡人就可以开始安全地进行网上交易了。

2）商家

商家要参与 SET 交易，首先必须要开设网上商店，在网上提供商品或服务；其次商家的网上商店必须集成 SET 交易商户软件，顾客在网上购物时，由网上商店提供服务，购物结束进行支付时，由 SET 交易商户软件进行服务；第三，商家必须到接收网上支付业务的收单银行申请并且必须在该银行设立帐户；第四，同持卡人一样，还必须上网申请一张能证明自己合法身份的数字证书。

3）发卡银行

发卡银行是负责为持卡人建立帐户并发放支付卡的金融机构。发卡银行在分理行和当地法规的基础上保证信用卡支付的安全性。

4）收单银行

收单银行是商家建立帐户并处理支付卡认证和支付的金融机构。

5）支付网关

SET 交易中买卖双方进行交易，必须通过银行进行支付，但由于 SET 交易是在开放的 Intemet 上进行的，而银行的计算机主机及银行专用网络是不能盲接与

Internet 相联的，为了能接收从 Internet 上传来的支付信息，在银行与 Internet 之间必须有一个专用系统，负责接收处理从商家传来的扣款信息，并通过专线送给银行；银行对支付信息的处理结果再通过这个专用系统反馈回商家。这个专用系统就称为支付网关。

6）数字证书认证中心(Certificate Authority 简称 CA)

为了保证 SET 交易的安全，SET 协议规定参加交易的各方都必须持有数字证书，在交易过程中，每次交换信息都必须向对方出示自己的数字证书，而且都必须验证对方的数字证书。CA 的主要工作是负责 SET 交易数字证书的发放、更新、废除、建立证书黑名单等各种证书管理。参与 SET 交易的各方(包括持卡人、商家、支付网关)在参加交易前必须到 CA 处申请数字证书。在证书到期时还必须去 CA 处更换一张新的证书。同时，CA 还要随时掌握哪些证书已经被废除，要将这些证书写入证书黑名单，作为交易时验证对方证书的依据。

4.2.2 SET 工作原理

SET 协议工作原理如图 4.1 所示:

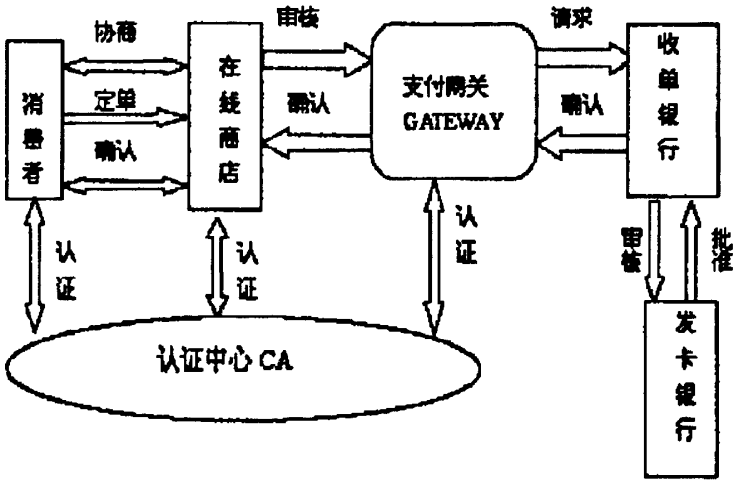

图 4.1 SET 协议工作原理

其具体工作流程如下:

① 持卡人通过浏览器选择在线商店里自己需要的商品，放入购物车。

② 持卡人填写订单信息，并选择支付方式。

③ 持卡人将订单信息和支付信息发送给商家，这里订单信息和支付指令由消费者进行数字签名，同时利用双重签名技术保证商家看不到消费者的账号信息及银行看不到消费者的订单信息。

④ 商家接受订单量信息后，与支付网关进行通信，请求授权认证。

⑤ 支付网关通过收单银行向持卡人的发卡银行请求进行支付确认。

⑥ 发卡银行同意支付，将确认信息通过支付网关返回给商家。

⑦ 商家发送订单确认信息给持卡人，持卡人端软件可记录交易日志以备将来查询。

⑧ 商家发送货物或提供服务。

⑨ 商家向持卡人的发卡银行请求支付，即实现支付获取、完成清算。

在处理过程中，通信协议、请求信息的格式、数据类型的定义等，SET 都有明确的规定。在操作的每一步，消费者、商家、支付网关都将通过 CA 来验证通信主体的身份，以确保通信的对方不是冒名顶替。

4.2.3 SET 交易过程

SET 交易过程包括持卡人注册、商家注册、购买请求、支付授权、付款清算等过程。

1）持卡人注册[39]

持卡人在发卡银行申请登记并得到持卡人软件后，还必须上网向 CA 申请数字证书，即持卡人必须注册。持卡人注册的全过程，有 7 个基本步骤:

①持卡人初始化注册

② CA 发出响应

③持卡人接收到响应并请求注册表

④ CA 处理注册表请求并签发注册表

⑤持卡人接收注册表并请求证书

⑥CA 处理请求和产生证书

⑦持卡人接收证书

2）商家注册[40]

商家在收单银行申请登记并已安装 SET 商家软件后，还必须上网向 CA 申请数字证书，即必须进行注册。商家注册包括四个基本步骤:

①商家发出注册表请求

②CA 发出响应

③商家接收到响应并请求注册表

④CA 处理请求并发出商家证书

3）购买请求[41]

在 SET 协议中，购买请求的步骤如下:

①持卡人初始化请求

②商家发送初始化响应及证书

③持卡人接收初始化响应并发送购买请求

④商家处理购买请求

⑤持卡人接收购买响应

4）支付授权

商家在向持卡人发送商品前，首先向支付网关查询持卡人是否具有支付能力。支付网关通过发卡银行证实持卡人确实具有支付能力后，商家才向持卡人发送货物。其支付授权过程如下:

①商家请求授权

②支付网关处理授权请求

③商家处理授权响应

5）付款清算

一个购物过程完成以后，商家为了得到货款向支付网关发出扣款请求，支付网关通过金融网络将货款转入商家所在收单银行的帐户中实现一次付款过程。其过程如下:

①商家请求付款

②支付网关处理付款请求

③商家接收付款响应

通过以上的分析可以看到，SET 定义了一个完整的电子交易流程，它较好地解决了电子交易中各方之间复杂的信任关系和安全连接，确保了电子交易中信息的真实性、保密性、完整性和不可否认性。

4.3.4 SET 交易过程分析

从 SET 交易过程可以看出，SET 设计严密，对每一过程都考虑得比较周密，解决了客户资料的安全性问题，商家看不到客户的信用卡帐号，银行看不到客户的订货信息;解决了用户与商家、用户与银行、商家与银行之间的多方认证问题，能够有效的防止假冒问题的发生；所有的交易过程都是在线的，保证了网上交易的实时性；利用加密技术、Hash 算法、数字签名、数字信封、第三方机构 CA 等技术，确保了电子商务交易信息的安全。

SET 交易过程中对证书处理、数字签名、信息加密的统计如表 4.1、表 4.2 及表 4.3 所示[42]:

表 4.1 SET 证书处理操作统计表

参与方	证书传递次数	证书验证次数
持卡人	1（持卡人签名证书）	3（商家签名证书 2，网关加密证书 1）
商家	5（持卡人证书 1，网关证书 1，商家加密证书 1，商家签名证书 2）	3（持卡人签名证书 1，网关加密证书 1，网关签名证书 1）
支付网关	1（网关签名证书 1）	3（持卡人签名证书 1，商家签名证书 1，商家加密证书 1）

表 4.2 SET 签名处理操作统计表

参与方	签名次数	验证次数
持卡人	1	2（商家签名证书 2）
商家	3	2（持卡人签名证书 1，网关签名证书 1）
支付网关	1	2（持卡人签名证书 1，商家签名证书 1）

表 4.3 SET 加密操作统计表

参与方	加密次数		解密次数	
	对称	非对称	对称	非对称
持卡人	1（商家，网关）	1（商家，网关）		
商家	1（网关）	1（网关）	2(持卡人,网关)	2(持卡人,网关)
支付网关	2（商家）	2（商家）	2(持卡人,商家)	2(持卡人,商家)

从以上统计可以看出，SET 交易过程非常复杂，完成一个 SET 交易的过程，需传递证书 7 次，验证数字证书 9 次，进行 5 次数字签名，验证数字签名 6 次， 4 次对称加解密和 4 次非对称加解密，所以完成一个 SET 交易过程需要花费较长的时间。由此可知，SET 协议使用麻烦，价格昂贵，操作复杂，且只适合信用卡交易，目前，在中国的广泛应用还比较困难。

4.3 SET 协议的扩展及完善

SET 协议由美国两家信用卡公司联合设计，公布之后引起了相关厂家的高度重视，并逐渐成为国际信用卡支付的标准。SET 协议是通过 Internet 进行在线交易的一个安全协议标准，是为了解决用户、商家和银行之间通过信用卡进行支付而设计的，以保证支付信息的机密性，支付过程的完整性，以及各参与方身份的合法性、交易行为的不可否认等。尽管 SET 协议有许多优点，但是，同时也暴露出了一些问题[43-44]，主要体现在:

(1)SET 只支持信用卡消费。SET 协议主要传输持卡者的主帐户信息，没有个人密码 PIN 的使用。但在我国，主要使用借记卡。所以这一问题阻碍了 SET 协议在我国的推广使用。

(2)SET 协议过于复杂，要求安装的软件包太多，处理速度慢，价格昂贵。对于小型交易来说，高安全性带来的低效率与高费用代价是不值得的。同时，SET 涉及的实体较多，不同实体间复杂的交易联系也是 SET 协议交易效率低的原因之一。

(3)协议没有担保“非拒绝行为”且 SET 协议不满足“商品原子性”及“确认

发送原子性”；即当商家从支付网关得到客户正确支付后，SET 协议不能保证商家一定会发货给客户，也不能保证发给客户的商品就是客户订购的商品。同时 SET 协议并没有体现对物流服务的管理，也没有明确交易结束后，交易数据应如何保存或销毁。

本章节将针对以上的问题提出，结合新的 B2C 交易模式对 SET 协议进行改进，增强其适用性、针对性及安全性。具体的改进措施有：对借记卡的支持、SET 安全控制分级模型、SET 协议的安全性及物流监控性增强。

4.4.1 对借记卡的支持

原有的 SET 协议是基于信用卡交易来设计的，而中国社会的信用体制不健全，与国外发达国家相比，我国没有统一的个人信用制度管理，因此无法建立以信用为基础的电子支付。我国目前在电子商务在线支付中信用卡的使用不普及，多是借记卡。借记卡和信用卡的主要区别是信用卡支持信用制度可以透支，而借记卡在使用时支付金额不可大于卡内金额数且需要个人密码的支持。因此，若要在改进的 B2C 电子商务交易模式中使用 SET 协议，首先应该解决其实用性问题，既对助记卡的支持。具体改进方案如下：

一、PIN 数据项的扩展

因为目前国内进行借记卡支付时都要输入个人密码 PIN，而 SET 1.0 标准主要针对信用卡,只需要输入主帐户 PAN 信息(主要是信用卡卡号)，没有定义 PIN 的处理方法。在 SET 协议中，持卡者的身份出持卡者的证书和支付卡的主帐户 PAN 唯一确定。可见，主帐户 PAN 是持卡者最关键的数据，而 PIN 应该和 PAN 具有同等的安全要求，所以可以考虑对 PIN 使用相同的加密处理方法[39]。

在线 PIN 加密机制如图 4.2 所示，PIN 通过键盘或其它设备输入到持卡人的计算机中。PIN 数据放在 SET 协议中的 RSA/OAEP 块中，采用支付网关公钥和对称加密保护，在 SET 协议中加密的 PIN 通过商家传输到支付网关，支付网关使用私钥解开信封，再用对称密钥解出 PIN 数据，如果需要，可以将 PIN 数据转换为其它的 PIN 块格式，采用对称密钥重新加密，然后将重新加密的 PIN 数据发送到支付卡网络。

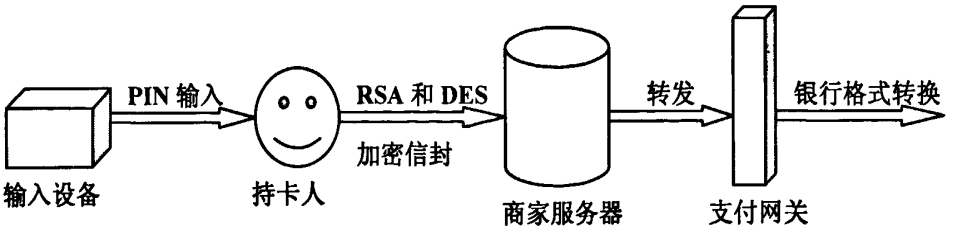

图 4.2 PIN 加密流程

PIN 的格式应遵循 IS09564-1 FormatO,PIN 块使用 8 个字节，格式化操作时将一个明文的 PIN 数据区和一个账号号码数据区进行二进制异或，异或的目的是增强 PAN 和 PIN 数据的关联性，防止替换攻击。明文的 PIN 格式如图 4.3 所示。

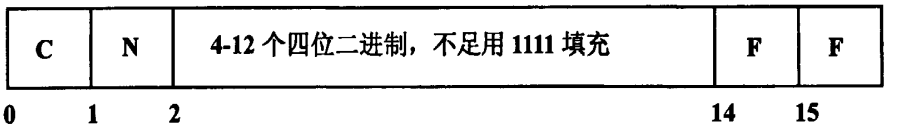

图 4.3 PIN 格式

C=控制数据，一般为 0000 表示“Format 0”编码。

N= PIN 长度，4bit 二进制数 0100(4)到 1100(12)。

PIN 值为 4 到 12 个数字,每个数字代表 4 位二进制数，从左排列，不足的填充二进制 1111。F =填充数字，C，N，PIN 区使用 PIN 明文的前 14 个数字，剩下的 2 个数字设置为二进制 1111。账号号码数据区的格式如图 4.4 所示，前 4 个 4bit 数字每个包含二进制 0000，其它 12 个二进制数字以右边为准排列，是主帐户号码，不足从左开始用二进制 0 来填充。

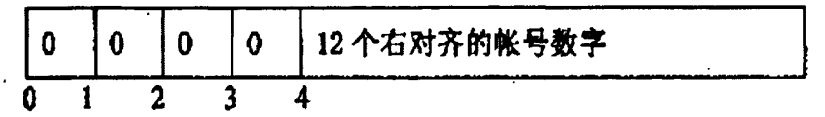

图 4.4 帐号号码格式

二、持卡人和支付网关对 PIN 的支持

为了使持卡人知道某一张卡是否需要 PIN,需要在 SET 的证书中增加一个扩展项，来标示是否要输入 PIN。如果需要输入，则利用输入设备得到 PIN，建立明文的 PIN 数据域，并与 PAN 数据域求异或后用用随机产生的对称密钥加密，在用支付网关的公钥加密发送给支付网关。支付网关解密得到 PAN 及对应的 PIN 数据项

后送银行验证，执行支付。持卡人对 PIN 数据项处理如下：

(1) 在用户选择了支付的卡后，通过该卡对应证书的扩展项来判断该卡是否要求 PIN 输入。

(2)如需要，则利用输入设备得到 PIN，建立明文的 PIN 数据域。

(3) 建立帐号数据区，异或明文的 PIN 数据和账号数据区。

(4)用随机生成的对称密钥，加密异或后的 PIN 数据区。

(5) 用支付网关的 RSA 公开密钥，加密对称密钥。

支付网关处理的过程如下：

(1)执行标准的 RSA/OAEP 的过程，这将解开对称加密密钥。

(2)用对称加密密钥解密 PIN 加密数据。

(3)重新建立 PAN 的数据区，并与 PIN 数据块异或，得到 PIN。

(4)根据需要将 PIN 数据经过格式的转换，送去银行效验。

三、即时付款的支持

中国借记卡 SET 支付的方式主要采用“当时授权批准并且转账”付款模式，该功能对借记卡是必须的。如需“即时付款”，商家产生授权请求消息 AuthReq 时，需要在该消息中设置“即时付款”标志；由支付网关将此信息发送给开卡银行。开卡银行判断持卡人账户余额，完成交易，其支付的流程如下:

(1)在购物过程进入支付阶段时，持卡者首先向商家发出购买请求消息 PReq。

(2)商家接收到 PReq 消息并确认持卡者身份后，向支付网关发出授权请求消息 AuthReq。

(3)商家产生授权请求消息 AuthReq 时，需要在该消息中设置“即时付款”标志。

(4)支付网关接收到 AuthReq 后，因为要求当时付款，所以支付网关通过银行内部网络连接发卡行和收单行，发卡行首先确认持卡者身份，然后检查持卡者账户资金余额是否小于要付款的金额，然后将资金从发卡行转到收单。

(5)在交易完成后，如果需要退款，可以使用退款请求消息来处理。

4.4.2 SET 安全控制分级模型

SET 是一种基于网上信用卡支付的安全电子交易协议，交易前，它要求持卡人、商家、支付网关等参与方均需安装相应的软件和均需向 CA 申请自己的数字证书；交易过程中，要进行多次证书的传递和验证，以及进行多次加密、解密和数字签名等。操作复杂且价格昂贵，运行效率较低，针对性和适应性较差。没有根据持卡人、商家的实际情况或具体需求进行分别考虑，而是不管交易金额的多或少，以及商家规模的大或小，支付过程都一个样。由于这些问题的存在，阻碍了

SET 协议在我国电子商务中的应用和推广。因此，在改进后的 B2C 电子商务交易模式中应用 SET 协议时应考虑其针对性改进的问题，既根据不同的商务规模，有针对性地建立相应得交易类型供用户选择。为此，应该在 SET 协议中建立安全控制分级模型。

一、安全控制分级模型原理

安全控制分级模型的基本原理就是将 SET 的安全控制分为不同的安全级别，每种安全级别的安全性及执行效率都不相同。不同的消费者可以根据不同的交易情况和自身需求来选择相应的安全级别。如果消费者所购商品的交易额较小，而且他对银行、商家又充分的信任，为了提高交易速度，他就可以选择安全级别较低的交易模式；反之，如果消费者所购商品的交易额较大，为了确保交易的安全，他就可以选择安全级别较高的交易方式。级别越低，安全性就越差，但加解密的次数减少，完成整个 SET 交易的效率提高；反之，级别越高，安全性就越高，其加解密的次数增多，完成整个 SET 交易的速度减慢，交易效率降低。

由于电子商务主要使用的协议标准是 SSL 协议和 SET 协议，从之前的分析可以看出 SET 比 SSL 更安全，而 SSL 协议比 SET 协议又更快捷。因此，不同等级的界限可以以 SSL 和 SET 为定界线来进行划分：安全性比 SSL 差的定义为 A 级；安全性等同于 SSL 的定义为 B 级；安全性比 SSL 高，但又比 SET 低的定义为 C 级；D 级是未改进的 SET 协议；E 级则是改进后的 SET 协议。同时，结合改进后的 B2C 交易模式，不同级别的安全控制赋予了安全电子交易中心不同的技术职责。

安全控制分级模型各级别安全控制内容如下所述：

①A 级

A 级是安全级别最低交易类型，主要用于交易金额额较小(如小商品之类)、对安全要求不高的交易，其目的在于简化操作程序、提高交易的效率。其安全控制如下：

1) 各参与方之间充分信任，不需要进行相互身份的验证。

2) 交易过程中仅对持卡人的支付信息进行短密钥加密，而其它交易信息则不需要加密。此级别只对持卡人的支付信息进行保密，不提供完整性、真实性和不可否认性服务。由于该级别不用进行数字证书的传递、证书的验证，不用进行数字签名和签名的验证，因此减少了加密解密的次数，简化了操作流程、节约了时间、提高了交易的效率，但其安全性是最低的。

②B 级

安全性等同于 SSL 协议，主要用于交易额稍大(如高档衣服之类)、对信息传输过程中的安全要求相对较高的商务交易，其目的是简化操作、提高交易效率。其安全控制如下：

1) 各参与方之间传送的信息必须用中等长度的密钥进行加密。

2) 持卡人与商家之间需要进行身份认证，其它参与方则不需进行身份认证。

3) 发送的信息需生成消息摘要，需进行完整性鉴别，但持卡人发送的订单信息和支付信息不进行双重签名，因此商家可以知道持卡人的帐号信息，而支付网关可以知道持卡人的订单信息。

该级别提供保密性、完整性服务，只在持卡人与商家之间提供真实性服务，在各参与者之间都不提供不可否认性服务。由于此级别在交易的过程中只在持卡人客户端与商家服务器端进行身份认证，而持卡人与银行之间、商家与银行之间不进行身份认证，而且在各参与者之间不用进行数字签名，因此，简化了操作流程，交易效率得到提升。

③C 级

安全性高于 B 级，该级别类似于在持卡人与商家之间实现 SSL 协议，在商家与银行之间实现 SET 协议。主要用于交易额较大(如家用电器之类)，对安全性要求较高，而消费者又不想操作过于复杂的交易。其目的仍然是简化操作流程、提高工作效率，保证信息传输和支付的安全性。其安全控制如下：

1) 持卡人和商家之间需进行身份认证，商家和支付网关之间同样需进行身份认证。

2) 持卡人和商家之间不需进行数字签名，但商家与支付网关之间需要进行数字签名。

3) 各参与方之间传送的信息均需进行完整性检验和加密，加密密钥长度较长。

该级别提供保密性、完整性、部分真实性和部分不可否认性服务。由于该级别在持卡人与商家之间实现的是类似于 SSL 协议，而 SSL 协议比 SET 协议的实现要简单、效率要高。因此，该级别的交易效率仍然高于 SET 协议。

④D 级——未改进的 SET 协议

该级别的安全性要求比 C 级要高，主要适应于交易额大(如批量采购大件之类)、的交易，能够提供信息的保密性、完整性、真实性和不可否认性等服务，但操作复杂、速度慢。其安全控制如下：

1) 持卡人、商家、支付网关必须有自己的证书，相互间必须进行证书的验证，确保对方的真实身份。

2) 各参与方之间传送的信息必须进行加密、数字签名，保证信息的机密性和不可否认性。

3) 持卡人对订单信息和支付信息进行双重签名后，发送给商家，保证信息的完整性和持卡人的局部信息的保密性。

⑤E 级——改进后的 SET 协议

此级别安全性最高，不但能保证信息的机密性、完整性、真实性和不可否认性，而且加、解密方式不受限制、比较灵活，还可以较好地解决持卡人与商家或

是物流公司之间的纠纷问题，解决有效交易的日期、时间问题及有效交易信息由谁来保存的问题，增加了 SET 协议的物流控制管理功能。主要适用于交易额大(如上万甚至几十万)的交易。但交易过程比 D 级稍复杂、交易效率相对 D 级有所降低。其安全控制如下：

1) 持卡人、商家、支付网关、以及物流都必须有自己的证书，相互间必须进行证书的验证，确保对方的真实身份。

2) 在对信息进行加密时，先用有自主知识产权的算法进行加密，再用 SET 默认的加密方法进行加密，既进行信息的嵌套加密，以增加信息的安全强度。

3) 增加发卡银行的仲裁功能，对纠纷进行裁决，对每一次有效交易都加盖数字时间戳后进行保存；为了解决纠纷，发卡银行收到支付请求时，并不立即将持卡人的购物款项划入商家或物流在收单银行的帐户中，而是将款项划入一个冻结帐户，保存 T 天，等待持卡人收到货物后的意见，以备交易纠纷的解决。

二、安全控制分级模型的实现

具体实现步骤如下：

①持卡人通过浏览在线商店的主页选购自己需要的商品，填写订单并选择相应的支付方式。

②持卡人根据需要选择一种安全控制级别，以后的交易将按照这个安全控制级别进行。

③持卡人将安全控制级别、订单信息和支付信息一起发送给商家。

④商家收到持卡人发来的信息后，按照持卡人选择的安全控制级别进行操作，生成支付请求，其中包括持卡人发给支付网关的支付信息，然后发送给支付网关。

⑤支付网关收到商家发来的支付请求后，按照选择的安全控制级别进行处理，并将支付请求发送给收单银行。

⑥收单银行收到支付网关的支付请求后，转发给发卡银行；发卡银行按照选择的安全控制级别来处理支付请求。如果是 E 级，发卡银行并不立即将持卡人的购物款项划入收单银行，而是将购物款项冻结，看是否有纠纷发生，以便解决。

4.4.3 SET 协议安全性及物流监控性增强

一、问题分析

SET 安全协议存在的问题:

(1) SET 协议没有担保“非拒绝行为”，在线商家无法证明订单是不是由签署证书的消费者发出的。

(2) SET 协议不满足“商品原子性”及“确认发送原子性”；SET 协议不能保证商家一定会发货给客户，也不能保证发给客户的商品就是客户订购的商品。一

旦出现消费者对商家提供的商品不满意时，责任问题无法落实。

(3) SET 协议并没有体现对物流服务的监管,物流在协议中被视为一个过程而不是一个实体，物流的身份认证及支付过程在协议并中没用涉及。同时，SET 协议也没有明确事务处理结束后，如何安全地保存或销毁交易数据，这些漏洞可能使这些数据以后受到潜在的攻击。

因此,应结合改进的B2C 电子商务交易模式对 SET 协议的交易流程进行改进，在增强其安全性的同时，体现其对物流的监管作用，并进一步丰富“安全电子交易中心”的技术职能，完善解决方案设计。

二、SET 协议安全性改进

针对 SET 安全协议的几个缺陷，将新 B2C 商务模式中的安全电子交易中心引入 SET 协议中，在新的支付模型中，安全电子交易中心处于核心位置，如图 4.5 所示。为了实现交易过程的安全性，应该在技术领域赋予安全电子交易中心以下几种技术职能:

1、区域 CA 职能:实现对持卡人、商家、物流等参与实体的身份认证。如果对签发证书的 CA 本身不信任，则需要沿信任树向上追溯验证 CA 的身份，直到一个公认可信的组织一根 CA 为止。

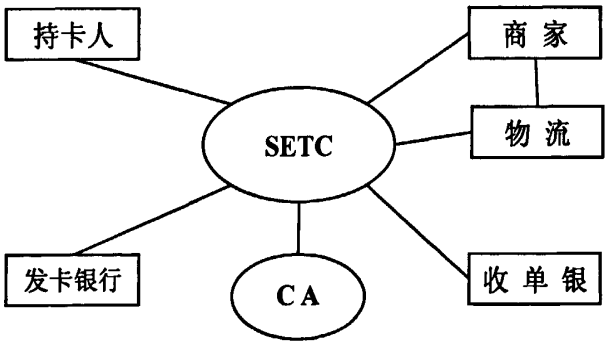

图 4.5 改进的 SET 支付模型

2、第三方交易数据保存:使得交易过程可审查监督，并为其可能的“交易纠纷解决”提供必要的证明数据。传统的 SET 模型中，交易数据分散保存在持卡人、商家和银行，不利于信息安全。若将这些信息保存在交易中心，不仅安全可靠，防止被恶意篡改或删除，而且可以为将来的审查或仲裁提供证据。

3、数字时间戳服务：电子商务交易中的时间，比如订购时间、授权时间、交易撤消时间等对支付安全十分关键，因此，交易中心可提供数字时间戳服务，对相关信息进行 Hash 编码形成摘要，加盖时间戳，并进行数字签名，确保交易的时效性。

4、仲裁:在网上购物时持卡人与商家可能产生纠纷，比如商品规格不符或质

量问题，因而产生退货、拒绝付款等。SET 协议中用授权撤消 AuthRev 和捕获撤消 CapRev 来取消授权请求和获款请求，但这要求发生在每天日终的批处理之前。为了保护持卡人利益，交易中心应通知银行从持卡人账户中扣下应支付款项，并暂时冻结若干天，而不是立即划转到商家或物流公司的账户上。等持卡人对商品签收之后，再将冻结款划给商家和物流公司。当出现争议时，由交易中心执行其在线交易纠纷解决功能，并根据解决的结果进行仲裁。如商品符合要求，则按原规定处理；否则将冻结款项划回持卡人账户。

基于以上 4 点安全交易中心工作职能，本文对 SET 安全协议流程作如下修改，并以此确定了改进的 B2C 商务模式的交易流程：

(1) 消费者 C 向商家 M 发出采购请求。

(2) 商家 M 向消费者 C 提供商品目录清单。

(3) 消费者 C 同意报价，确定购物订单 Order，并对 Order 进行数字签名，然后连同数字证书用商家 M 的公钥加密：

$$CM1 = E_{pkm}\ (\ D_{skc}\ (\ Order)\ ,\ Cert_c\ ) \qquad (4\text{-}1)$$

然后将 CM1 发给商家 M。

(4) 商家 M 对 CM1 进行解密得：

$$D_{skm}\ (CM1)=(\ D_{skc}(\ Order)\ ,\ Cert_c\ ) \qquad (4\text{-}2)$$

得到 C 的公钥证书 $Cert_c$，然后用 C 的公钥解密：

$$Order = E_{pkc}\ (\ D_{skc}\ (\ Order)) \qquad (4\text{-}3)$$

确认 Order 为消费者 C 所发。

（5）商家 M 从 Order 中确定消费者需要商品的数目及几交货的时间、地点等信息，先用签名后再用物流的公钥匙加密的：

$$E_{pkw}\ (D_{skm}\ (Pay^1)\ ) = Pay^2 \qquad (4\text{-}4)$$

将 Pay^2发给物流 W。

物流 W 用对 Pay^2解密：

$$Pay^1 = E_{pkm}\ (\ (D_{skw}\ (Pay^2)\ ) \qquad (4\text{-}5)$$

确定是商家 M 发来的信息，并对其物流费用进行核对计算得到支付信息 Pay^3，同对其进行数字签名后连同自己的数字证书 $Cert_w$ 用商家 M 的公钥进行加密后得到 pay′，发送给商家 M。

$$pay'= E_{pkm}\ (\ D_{skw}\ \ (\ Pay^3)\ ,\ Cert_w\ ) \qquad (4\text{-}6)$$

商家M得到pay′后用其私钥对其解密得(D_{skw} (Pay^3), $Cert_w$),再用 $Cert_w$ 解密得到 Pay^3，并确定是物流 W 发送的信息，随后对 Pay^3及商品信息进行计算得到总的付款要求 Pay。

商家 M 对自己的数字证书 $Cert_m$ 、物流 W 的数字证书 $Cert_w$ 、支付网关的数字证书 $Cert_p$ 以及付款要求 Pay 进行数字签名，并将信息发送给消费者 C。

$$MC2= D_{skm} (Cert_m , Cert_p , Cert_w , Pay) \quad (4\text{-}7)$$

付款要求 Pay 包括物品名称、数量、应付款数（包括商品费用和物流费用）、消费者 C 和商家 M 以及物流 W 的身份,同时包括交货时间、地点、方式等信息。

(6)消费者 C 对收到的 MC2 进行解密：

$$E_{pkc} (MC2) = (Cert_m , Cert_p , Cert_w , Pay) \quad (4\text{-}8)$$

确认为商家 M 所发，确认商家 M、物流 W 和支付网关 P 的身份。核对物品名称、数量、应付款数等信息。

消费者 C 按要求生成支付命令 PI，并进行数字签名：

$$PI^1 = D_{skc}(PI) \quad (4\text{-}9)$$

消费者 C 随机生成一个对称密钥 K，由 K 对 PI^1进行加密：

$$PI^2 = E_k (PI^1) \quad (4\text{-}10)$$

用支付网关 P 的公钥对消费者 C 的帐户信息 PANIC 的姓名、信用卡号等 K 用密钥 K 进行加密：

$$PI= E_{pkp} (PAN，K) \quad (4\text{-}11)$$

消费者 C 对 PI^2, PI 及 MC2 进行签名：

$$CCA3 = D_{skc} (PI^2 , PI , MC2 , Cert_c , Cert_m) \quad (4\text{-}12)$$

然后发送给电子交易中心。

(7) 电子交易中心对收到的 CCA3 进行解密：

$$E_{pkc} (CCA3) = (PI^2 , PI , MC2 , Cert_c , Cert_m) \quad (4\text{-}13)$$

将用商家 M 的公钥解密 MC2 得到：

$$E_{pkm} (MC2) = (Cert_m , Cert_p , Cert_w , Pay) \quad (4\text{-}14)$$

电子交易中心 CA 将 $Cert_m$, $Cert_p$, $Cert_w$, Pay 记录在数据库中。同时对 $Cert_m$, $Cert_c$, $Cert_w$, $Cert_p$, PI^2, PI 进行数字签名：

$$CAP4= D_{skCA} (Cert_m , Cert_c , Cert_w , Cert_p , PI^2 , PI) \quad (4\text{-}15)$$

然后发送给支付网关 P。

(8)支付网关 P 对 CANP4 进行解密：

$$E_{pkCA}(CANP4) = (Cert_m, Cert_c, Cert_w, Cert_p, PI^2, PI) \quad (4\text{-}16)$$

确认为电子交易中心 CA 所发。

同时对 PI 进行解密，确认为消费者 C 所发：

$$D_{skp}(PI) = (PAN, K) \quad (4\text{-}17)$$

利用得到的对称密钥 K 对 PI^2 进行解密：

$$PI^1 = D_k(PI^2) \quad (4\text{-}18)$$

再对 PI，用消费者 C 的公钥解密：

$$PI = E_{pkc}(PI^1) \quad (4\text{-}19)$$

得到曾由消费者 C 签发的支付命令 PI，将支付命令 PI 经由安全的金融网发给发卡行 I。

(9) 发卡行 I 在数据库中查找消费者 C 的帐号，确认其帐户中有足够金额，即消费者 c 有能力支付后，将此笔款项存入一冻结帐户，然后由金融网通知支付网关 P 此款项已经扣除。

(10) 支付网关 P 向商家 M 发出可以交货的通知:

$$Msg' = D_{skp}(Msg) \quad (4\text{-}20)$$

(11) 商家 M 对 Msg，进行解密，确认为支付网关 P 所发：

$$Msg = D_{skp}(Msg') \quad (4\text{-}21)$$

则商家 M 可用同样的方式转告物流向消费者 C 发货。

(12)冻结帐户时间有一定的规则，假设为 T 天，如果在 T 天内，消费者 C 对商家 M、物流公司 W 提供的商品和服务反应有以下两种情况：

①电子交易中心 CA 未收到消费者 C 的任何异议，则发卡行 I 自动将冻结款项拨入商家 M 和物流 W 在各自收单银行的帐户。收单银行通知商家 M 和物流 W 款项到位。电子交易中心 CA 将交易日志记为交易成功。

②如果消费者 C 对收到的商品或享受的服务有异议，可在指定时间 T 内向交安全电子交易中心提出异议，要求交易中心进行交易纠纷解决并执行仲裁。交易中心根据在第六步中收到的关于物品名称、单价、数量、质保、交货方式、地点、时间等信息作出判断，是商家 M 未履行承诺，或是物流 W 服务质量有问题，还是

消费者 C 恶意欺诈等等。在仲裁结果未出来时，电子交易中心 CA 通知发卡银行 I 继续冻结此款项，如果是商家 M 的过错，则按一定规章制度对消费者 C 进行赔偿或是退货，取消此笔交易。如果是物流的服务质量问题，同样按照一定规章制度要求物流公司对商家或是消费者作出相应的赔偿。如果是消费者 C 的恶意欺诈，则交易中心将在消费者 C 的信用记录上记录此次恶意行为。一旦仲裁结果出来，电子交易中心 CA 就通知发卡行 I 具体该如何操作：

1.如果是商家 M 过错时，无论是进行赔偿或退货。电子交易中心 CA 要求商家 M 和消费者 C 协商并对处理意见进行共同签名。然后根据共同签名的内容，通知发卡行 I 将其中一部分冻结款项划回消费者 C 帐户作为赔偿或是全部划回消费者 C 帐户进行退货。发卡行 I 通知电子交易中心 CA 划拨成功。则电子交易中心 CA 将如何处理事情争纷记入交易日志，标志此交易完成。

2.如果是物流公司的问题，同样电子交易中心 CA 要求物流 W 和消费者 C 协商并对处理意见进行共同签名。然后根据共同签名的内容，通知发卡行 I 将其中一部分冻结的物流款项划回消费者 C 帐户作为赔偿或是全部划回消费者 C 帐户。发卡行 I 通知电子交易中心 CA 划拨成功。则电子交易中心 CA 将如何处理事情争纷记入交易日志，标志此交易完成。

3.如果是消费者 C 的恶意攻击，则交易中心 CA 通知发卡行 I 将全部款项拨入商家 M 和物流 W 各自的帐户中，并将消费者 C 的恶意行为记入消费者 C 的信誉档案中，修改消费者 C 的诚信度。

4.4.4 改进后的 SET 安全协议分析

结合 B2C 电子商务交易模式对 SET 协议进行改进后，使 SET 协议的适用性、针对性及安全性都得到了提高。同时，也赋予了 SET 协议一个全新的特性，既对物流的监控性。这些改变主要体现在以下几个方面：

(1) 根据我国目前 B2C 电子商务发展的现状，针对我国目前在电子商务在线支付中信用卡的使用不普及，多是借记卡的特殊性，对 PIN 数据项进行扩展，为 SET 协议在我国的推广与使用提供了一个实际且可行的方法，增强了 SET 协议在我国的适用性。

(2)安全控制分级模型是从具体的实际出发，根据交易的性质、交易额的大小以及消费者对交易的效率和安全等方面的要求，来选择不同的安全级别，满足了不同的消费对象对交易安全性的不同需求。具有灵活性、实用性、可控性和操作容易等特点，较好地提高了 SET 的针对性。

(3) 通过安全电子交易中心保存交易日志，一旦以后发生纠纷，交易中心可出示交易日志作判决。避免了交易数据放在商家 M、物流 W 或消费者 C 的数据库里

受到攻击或篡改，同时健全了诚信档案的建设，完善了交易中心诚信度判断的职能。

(4) 引入交易中心参与交易，交易中心可起监督作用。保证消费者 C 付款，就可得到商家 M 的商品或服务。且交易中心记录的关于商品数量、单价、质保、交货时间、地点等信息，确保商家 M 提供的商品及物流服务的质量得到彼此的确认。这样满足了钱原子性、商品原子性和确认发送原子性，增强了 SET 协议的安全性。

(5) 物流 W 作为交易的一个实体而不是一个过程参与到了交易的认证和支付过程中，从技术上实现了对物流过程及其质量的控制，解决了物流处于非受控状态的实际瓶颈问题。

4.4 本章小结

本章对安全支付协议 SET 进行分析、研究，针对 SET 协议在实际应用中存在的某些不足，结合新的 B2C 电子商务交易模式对其进行了扩展及完善，增强了 SET 协议的适用性、针对性、安全性及物流监控性。同时在定义“安全电子交易中心”的技术职能的基础上，确定了新交易模式的交易流程。从而从体制和技术两方面完善了缓解我国 B2C 电子商务发展瓶颈的解决方案设计。

第五章 结束语

21 世纪是一个以数字化、网络化与信息化为特征，以网络通信为核心的信息时代。电子商务作为信息技术与经营管理活动的融合，以其独特的方式改变着人们的思维方式、经济活动方式、工作方式和生活方式。商务模式的创新和信息技术的变革是电子商务发展的源动力，同时也是问题出现的根本原因。目前，由于电子商务模式存在着种种不足以及广大用户对电子商务安全性需求的不断增长，促使诚信问题、支付安全问题、配送问题成为了制约我国 B2C 电子商务发展的三大核心瓶颈，严重阻碍了我国电子商务的发展。

为了缓解这三大核心瓶颈，促进我国 B2C 电子商务的快速发展，本文从对现有的 B2C 电子商务模式及安全技术的分析入手，结合商务模式的创新和电子商务安全协议的改进，提出了一个系统的，全面的问题解决方案。分析表明，该解决方案具有以下特性：

1、全面性

电子商务是一个系统的概念，它是商务活动和信息技术完美的结合体。当系统出现问题时，如果仅仅从某个组成部分去解决的话，这样的解决方案是片面的。本文所提出的解决方案包括商务模式的创新和安全技术的完善，具有问题解决的全面性。

2、适用性

方案设计在 SET 协议完善的过程中，针对我国目前在电子商务在线支付中信用卡的使用不普及，多是借记卡的特殊性，对 PIN 数据项进行扩展，在解决 SET 协议对助记卡的支持的同时，增强了解决方案在我国 B2C 电子商务环境下的适用性。

3、针对性

在电子商务交易中，由于交易规模、交易商品、顾客的要求等交易因素的不同，其对安全性和效率的要求也不同。交易的安全性和效率是一对矛盾体，针对不同类型的电子商务交易而言，需要有不同的平衡点。方案中 SET 安全控制分级模型将这些平衡点罗列到了用户面前，用户可根据不同的交易需求选择相应的安全级别，针对性地解决交易过程中出现的问题。

4、物流监控性

无论在体制方案还是在技术方案中，物流都被视为交易的一个实体而不是一个过程参与到了交易的认证和支付过程中，物流的过程和质量得到了较好的监控，合理地解决了 B2C 电子商务交易中，物流处于非受控状态的问题。

5、安全性

通过在 B2C 电子商务模式中引入安全电子交易中心，赋予其相应的功能职责和技术职能，完善 SET 协议确定交易流程后，使得交易各参与方的身份得到有效认证的同时，满足了交易过程中钱原子性、商品原子性和确认发送原子性，增强了解决方案的安全性。

电子商务系统是一个由多方参与的、经营管理和技术相结合的社会系统，本文所提出的解决方案仅仅局限于从技术上支持一种创新的商务模式。下一步的研究应从以下几方面予于解决方案新的内涵，从而更好地解决制约我国 B2C 电子商务发展的瓶颈问题。

1、电子商务相关法律法规的健全

新的商务模式的运行与推广除了技术的支持外还必须从法律的角度出发，确定商务模式中各个实体的权与责，从而保障其交易的合法性。

2、在线交易纠纷解决机制的完善

解决方案中对于交易纠纷的处理仅局限于一些简单的，便于调解的交易纠纷。对于不断发展的 B2C 电子商务而言，应进一步完善交易纠纷解决机制的设计与实现，从而可便捷合理地处理因交易环境改变而出现的新的交易纠纷。

3、交易效率的提高

新的商务模式中，SET 协议的安全性增强的同时降低了交易的效率。接下来研究应对交易效率的提高予于考虑。

致谢

本文从选题到定稿，历时一年的时间。在本论文完成之际，首先要向我的导师鱼滨老师致以诚挚的谢意。鱼老师学识渊博、治学严谨，平易近人，在论文选题、资料查阅、研究方法、论文撰写等诸多方面都给予了我悉心的指导和帮助。同时他对工作的踏实负责、有条不紊、实事求是的态度，给我留下了深刻的印象，使我受益非浅。在此我谨向鱼老师表示衷心的感谢和深深的敬意。

同时，我要感谢曾给我授课的所有老师，正是由于他们的传道、授业、解惑，让我学到了专业知识，并从他们身上学到了求知、治学、做人、处事的方法和准则。我也要感谢西安电子科技大学，学校良好的学风和教风给我留下的永久的烙印，为我以后的教育生涯留下了宝贵的财富。

我还要感谢我的同学董建刚、原民民、徐万锦、孙建永以及其他同学，在我毕业论文写作中，与他们的探讨交流使我受益颇多；同时，在西电学习期间，他们也给了我很多无私的帮助和支持，我在此深表谢意。

参考文献

[1] 黄敏学. 电子商务. 2004 年 2 月第二版. 北京:高等教育出版社. 2006，12. P3.

[2] 王春. 电子商各交易平台安全架构的研究与应用[硕士学位论文]. 汕头大学. 2002, 5. P6.

[3] 田仲富. B2B 电子商务模式及安全在线支付系统的研究[硕士学位论文]. 东北林业大学. 2006, 6. P2-3.

[4] 沈扬. 我国电子商务发展的瓶颈问题及对策研究[硕士学位论文]. 南昌大学. 2007, 12. P23-27.

[5] 罗汉洋. B2C 电子商务模式分析与策略建议. 情报杂志. 2004, 2. 第 23 卷第 2 期. P10-11.

[6] 李庭春. B2C 电子商务交易流程浅析. 长沙大学学报. 2008, 5. 第 22 卷第 3 期. P29-30.

[7] 邵浩侠. 电子商务模式比较和创新探析. 新西部（下半月）. 2007 年第 12 卷 24 期. P139-140.

[8] 张婷，朱邦毅. 中国 B2C 电子商务的三种类别的分析研究. 商场现代化. 2009, 2. 第 5 卷第 566 期. P141-142.

[9] 梁静坤，金欣，郝敏钗. 谈 B2C 电子商务的优劣. 商场现代化. 2007, 3. 第 7 卷第 496 期. P94.

[10] 刘少涛，凌捷. 数据加密算法与大素数的生成及运算. 广东工业大学学报. 2001, 4. 第 18 卷第 5 期. P25-29.

[11] 桂学勤. 电子商务诚信安全对策探究. [硕士学位论文]. 华中师范大学. 2007, 5. P30.

[12] 吴热生. B2C 电子商务交易纠纷解决机制研究[硕士学位论文]. 安徽大学. 2006,10. P25-28.

[13] 丁宏，郭艳华. 一种安全有效的小公钥 RSA 加密协议. 小型微型计算机系统. 2003, 5. 第 24 卷第 5 期. P943-944.

[14] Daemen J, Rijmen V Rijndael. The advanced encryptionst andard. Dr. D obb'Joumal. 2001, 26 (3) . P137-139.

[15] Daemen J, Knudsen L R, Rijmen V. The block Cipher Square. Fast Software Encrytion, Springer-Verlag, 1997, 23 (4). P149-165.

[16] 韩宝明, 杜鹏, 刘华. 电子商务安全与支付. 2003 年 6 月第 1 版. 北京:人民邮电出版社. 2003, 6. P27-125.

[17] 陈海卫. 电子商务安全技术综述. 网络世界. 2003, 3.

[18] 唐作莉. 电子商务安全技术研究[硕士学位论文]. 贵州大学. 2008, 3. P20-23.

[19] 肖德琴. 电子商务安全保密技术与应用. 华南理工大学出版社. 2003, 6. P5-9, 46-47, 75-76.

[20] William Stallings. 密码编码学与网络安全—原理与实践. 2006年11月第四版. 北京：电子工业出版社. 2006, 11.

[21] 卢开澄. 计算机密码学[Ml. 第1版. 北京:清华大学出版社, 1998. P25-70.

[22] Biham E, Shamir A. Digerential Cryptanalysis of the Data Encryption Standard[R]. Springer-Verlag, 1993, 6.

[23] Biham E, Shamir A. Diferential Cryptanalysis of DES-like Cryptosystems [R]. Advances Cryptology-CRYPTO'90 Proceedings Springer-Verlag. 1991, 7. P2-21.

[24] (美)Derek Atkins. Intemet 网络安全. 第1版. 北京:机械工业出版社. 严伟, 刘晓丹, 王千样等译. 1998, 9. P430-449.

[25] E. Fujisaki, T. Okamoto, D. Pointcheval, J. Stern. RSA-OAEP Is Secure under the RSA Assumption. Journal of Cryptology. 2002, 17(2). P81-104.

[26] [RSA78]H . D obbertin, A . Bo sselaers, B . Pr ennel, RI PEMD-160:astrengthened version of RIPEMD, Fast Software Encryption, LNCS 1039, D. Golhnan, Ed. Springer-Verlag, 1996.

[27] 王学理, 裴定一. 椭圆与超椭圆曲线公钥密码的理论与实现. 2006 年 12 月第一版. 北京:科学出版社. 2006, 12. P5-15.

[28] 胡凯. 基于网络环境的电子商务系统认证和安全交易技术的研究[硕士学位论文]武汉理工大学. 2003, 3. P17-18.

[29] Secure Hash Standard. National Bureau of Standards FIPS Publican-on180. 1993. P15-20.

[30] Rivest R . L, Shamir A , Adleman L . On a Method for Obtaining Digital Signatures and Public Key Cryptosystems:Communications of the ACM. 1978(21). P120-126.

[31] Preneel B, Govaerts R, Vandewalle Disinformation Authentication. Hash Functions and Digital Signatures. Computer Security and Industrial Cryp-tography . Srpinger-Verlag. 1993. P87-131.

[32] 郑连清. 网络安全概论. 北京:清华大学出版社. 2004, 5. P71-73.

[33] 陈语林. 电子商务中安全问题的研究[硕士学位论文]中南大学. 2004, 5. P11-12.

[34] 陈如刚，杨小虎. 电子商务安全协议. 2000 年 7 月第一版. 浙江：浙江大学出版社. 2000, 7. P1-9.

[35] Cox B, Tygar J D, Sirbu M. Netbill Security and T ransaction Protocol. In:Proceedings of the 1st USENIX Workshop on Electronic Commerce. 1995. P77-78.

[36] 王卓. 电子商务安全支付协议的研究[硕士学位论文]长春理工大学. 2008, 4. P30-32.

[37] 童光才. 电子商务中安全协议的研究—SET 协议的完善与改进[硕士学位论文] 重庆大学. 2004, 5. P34-38.

[38] 鄂旭. 电子商务安全问题的研究[硕士学位论文]. CNKL. 2001. P28-32.

[39] 韩宝明, 杜鹏, 刘华. 电子商务安全与支付. 2003 年 7 月第 1 版. 北京:人民邮电出版社 2003, 7. P27 -125.

[40] 陆首群. 剖析 SET 协议. 中国计算机报. 1999. 7. 133-135.

[41] 何国斌. 安全电子交易 SET 协议的研究[硕士学位论文]. CNKL . 2003. 3. P32-33.

[42] 陈凡, 许先斌. SET 协议的分析与改进措施. 计算机应用研究. 2000. 第 6 期. P42-47.

[43] 王蝉. 姚赤丹. SSL/SET 协议比较与改进模型. 现代计算机. 2002. 8 总第 145 期. P16-18.

[44] 张宁. 电子商务安全性分析[硕士学位论文]. 北京邮电大学. 2007, 3. P36-40.

研究成果

发表的论文：

[1] 王俊洁,王俊鑫.浅谈产生式系统在人工智能中的应用.楚雄师范学院报.2007 年第 22 卷第 6 期.

[2] 王俊洁,王俊鑫，桂林斌.人工智能中感知问题的求解技术——约束满足法.楚雄师范学院学报. 2008 年第 23 卷第 3 期.

[3] 王俊洁,王俊鑫，黄青松.基于数据仓库的毕业生就业预测系统设计和实现.楚雄师范学院学报.2009 年第 24 卷第 3 期.

[4] 王俊鑫,王俊洁.K-Means 聚类算法在毕业生就业系统分析中的实现.楚雄师范学院学报.2009 年 第 9 期.