摘要

电子商务是当前各国研究的热点。电子商务是以协议为构成框架的，电子商务协议的安全性是决定电子商务发展的关键因素。安全电子商务协议，是使用了密码学方法的协议，其目的就是为了在复杂的、不安全的网络环境中为参加电子商务活动的主体提供各种安全服务。安全电子商务协议的目的是保证信息的安全，但是如果协议本身存在漏洞，攻击者就会利用这些漏洞，对合法通信者造成危害。因此需要对安全协议进行分析和验证，来检查安全电子商务协议是否能够达到其预期的目标。

Kailar 逻辑和卿-周逻辑是常见的安全电子商务协议形式化分析方法，但是它们只能分析协议的有限性质，并且在遇到重放攻击时 Kailar 逻辑和卿-周逻辑不能正确分析主体的责任性。本文在深入研究安全电子商务协议形式化分析方法理论的基础上，做了以下几个方面的工作：

（1）深入了解了安全电子商务协议的安全性质，尤其是原子性、可追究性与公平性。

（2）熟悉针对安全电子商务协议的常见攻击方法，用重放攻击分析了 IBS 协议和 CMP 协议，并对后者提出了改进方案。

（3）分析 Kailar 逻辑和卿-周逻辑的不足，提出了一种改进的逻辑分析方法，并给出了验证实例。

关键词：安全电子商务协议，Kailar 逻辑，卿-周逻辑，原子性，可追究性，公平性

ABSTRACT

Currently, electronic commerce is the heat point of the research and development in each country. Electronic commerce protocol is the comprising framework of electronic commerce, and its security is the key factor to decide the development of electronic commerce. Security electronic commerce protocol which uses the cryptographic methods for network communication, its goal is to provide security services in the complex and insecure environment. The purpose of the security electronic commerce protocol is to ensure the security of the information. But if there are some leaks in the protocol itself, attackers will use the leaks to cause harm to the legitimate communications. Hence we need to analyze and test the protocol to verify that the protocol is expected to achieve its security goals.

Kailar logic and Qing-Zhou logic have been proved to be the very useful formal methods for analyzing security electronic commerce protocols, but there are still some limitations. And they can not rightly analyze the accountability when the replay attack happens. We have made the following aspects of work on the basis of the study of the formal methods :

(1) We have studied the security property of the security electronic commerce protocols, in particular the atomicity、the accountability and the fairness.

(2) We have studied the common attacks to the security electronic commerce protocols. This paper analyses IBS and CMP when the replay attack happens, and gives the scheme of the improving CMP.

(3) This paper analyses the limitations of Kailar logic and Qing-Zhou logic. An improved logic is put forward to analyze security electronic commerce protocols. At last, two abstracted protocols are especially analyzed and verified completely by the improved logic.

Keywords: security electronic commerce protocol, Kailar logic , Qing-Zhou logic,

atomicity, accountability , fairness

第一章 绪论

1.1 研究背景

电子商务是客户(customer)、商家(merchant)和各方所信任的第三方认证机构 (CA)之间的信息流、资金流和物流的交互关系，各方通过遍及全球的、开放的但不安全的Internet相互联系[1]。如图1所示。

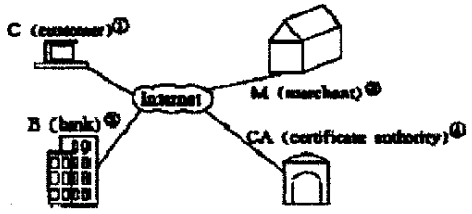

图 1.1 电子商务模型

协议是两个或两个以上的参与者为完成某项特定任务而采取的一系列动作步骤。这个定义包含三层含义：

(1) 协议自始至终是有序的过程，每一个步骤必须执行，在前一步没有执行完之前，后面的步骤不能执行；

(2) 协议至少需要两个参与者(称为协议实体或主体)；

(3) 通过协议必须能够完成某项任务。

协议还具有如下特点：

(1) 协议中每个实体都必须了解协议，并预先知道所要完成的所有步骤。

(2) 协议中的每个诚实实体都必须同意并遵循它。

(3) 协议不能模糊，每一步都必须明确定义且不会引起误解。

(4) 协议必须是完整的，对每种可能情况必须规定具体的动作。

电子商务协议是建立在密码体制基础上的一种协议，它运行在计算机通信网或分布式系统中，借助于密码算法来进行电子商务活动，协议自始至终是有序的过程，每一个步骤必须执行，在前一步没有执行完之前，后面的步骤不能执行；每个通信步骤将消息从一个主体传给另一个主体，计算步骤用于更新主体的内部状态。总之，它是为了完成电子商务活动而设计的协议。

电子商务由于方便、快捷而开展得如火如荼。据不完全统计，2005年我国电子商务交易额达7400亿元，比上年增长50%；网上购物用户数量达2200万户，比上年增加600万户。但电子商务的安全问题也越来越突出。万事达信用卡集团于2005年6月17日称，大约4000万信用卡顾客账户被一名黑客利用电脑病毒侵入，黑客可能将用户账号信息用作欺诈行为，而且多家银行的顾客账户都遭到了入侵。信用卡账户等信息的泄漏，将带给人们最直接的损失。此外，AC尼尔森公司的调查表明：安全性是网上购物者用信用卡支付的主要顾虑。

安全的电子商务协议是保证电子商务活动正常开展的基础。电子商务中的客户之间必须通过安全的、可信赖的协议才能建立起相互之间的信任关系。协议的缺陷可能会使客户间传送的数据遭到恶意修改而不被客户发现，从而使客户受到严重损失。因此，电子商务协议的安全性是电子商务安全的重要环节，也是电子商务发展的瓶颈。

安全的电子商务协议不但应当具备传统的安全协议所具备的全部功能，还必须具备一些特殊的性质来确保交易的有效性。例如，电子商务协议必须保证货币在交易过程中守恒；顾客和商家能够出示证据显示交易商品的内容；在交易过程中不泄漏主体的身份；参与协议的主体不能否认曾经参加过会话，等等。但电子商务协议在并行环境中运行，非常复杂且容易出错。经过精心设计的协议往往存在安全上的漏洞，仅凭人的直觉判断很难把错误找出来。如：kerberos协议及基础Needham_Schroeder协议起初被认为是安全的，17年后才被证实有可怕的漏洞[2]。因此对电子商务协议安全性的分析是一个重要的问题。

分析电子商务协议的困难性在于[3]：(1) 安全目标本身的微妙性；(2) 协议运行环境的复杂性。当协议运行在一个十分复杂的公开环境时，攻击者处处存在。必须形式化地刻画协议的运行环境，这是一项艰巨的任务；(3) 攻击者模型的复杂性。必须形式化地描述攻击者的能力，对攻击者和攻击行为进行分类和形式化分析。因此，一个电子商务协议在设计出来之后，需要从多方面对其各种性质进行分析，协议分析正是揭示电子商务协议是否存在缺陷的重要途径。为此，本文对电子商务协议安全性质的分析进行了初步的研究和探讨。

1.2 研究现状

近年来，国内外研究人员利用形式化方法分析安全协议并取得了一系列成果。如在定理证明方面，Meadows的NRL协议分析器[4]发现了许多已知的和未知的安全协议漏洞；Paulson提出了基于归纳的定理证明方法[5]，他研制的定理证明器Isabelle可用归纳的方法分析安全协议；文献[6]用归纳证明的方法分析了SET协议的安全性质。

在模型检测方面使用最广的是CSP理论。1996年Lowe首先采用CSP(通信顺序模型)和CSP模型校验工具FDR分析NSPK协议，发现了一个近17年来未知的攻击[2]。之后，Roscoe提出CSP+FDR可用于分析不可靠环境下电子商务协议的确认发送原子性[7]、原子性[8]及可追究性。另外，Standford大学的Mitchell等人[9]使用Murphi分析了一些复杂协议，如Kerberos协议、SSL协议等。文献[10]用模型检测工具SMV分析了Digicash协议和Netbill协议的原子性。文献[11]用自动验证工具UPPAAL验证了带时间约束的简单网络支付协议的原子性，文献[12]用UPPAAL验证了TLS握手协议，等等。

逻辑分析方法是迄今为止影响最大，应用最为广泛的协议分析方法。最先出现的协议分析方法是1989年，美国DEC公司的研究人员提出的一种基于信仰的逻辑—BAN逻辑[13]，并用来说明和验证密码协议。BAN逻辑成功地对NS、Kerberos等著名协议进行分析并找到了其中的漏洞。随后人们在使用BAN逻辑分析密码协议时，发现BAN逻辑存在着缺陷[14][15][16]，为此许多文献对BAN逻辑进行改进或扩展，这些都统称为BAN类逻辑（如GNY逻辑、AUTLOG逻辑、AT逻辑），但是它们都没有最初的BAN逻辑简单、易用。SVO逻辑[17]是在总结BAN逻辑、NY逻辑、AUTLOG逻辑、AT逻辑和VO逻辑的基础上发展而成的，它可用于分析电子商务协议的不可否认性[18]；后来，Kailar在BAN 逻辑基础上提出了用于分析电子商务协议可追究性的Kailar逻辑[19]，并用来分析了当时几个著名的电子商务协议。1999年，白硕等提出了非单调动态逻辑NDL[20][21][22]，但它也有自己的缺陷。周典翠、卿斯汉和周展飞等人随后也发现了Kailar逻辑的缺陷[23]并提出了一种分析电子商务协议的新工具[24]，文献[25]将Kailar逻辑和LPC结合来分析电子商务协议，等等。

1.3 本文工作

上述方法都能较好地分析协议的某些属性，但也有一定的局限性。如文献[6]用基于归纳的方法分析SET协议，证明过程较为繁琐；BAN逻辑可对交易主体的消息和信仰建模，但不能对行为建模；Kailar逻辑可对交易主体的消息和责任建模，从而可分析可追究性，但需要初始假设及对协议进行理想化[23][26]，而这正是Kailar逻辑的最大缺陷[23]；Kailar逻辑和卿-周逻辑[24]不能分析电子商务协议的原子性并且在受到重放攻击时不能正确分析主体的责任性，等等。

本文提出了一种改进的逻辑分析方法，它可用于分析电子商务协议的原子性、可追究性、公平性，并且弥补了 Kailar 逻辑和卿-周逻辑的不足。

本文通过对安全电子商务协议理论的深入分析研究，所作的工作主要包括以下几个方面：

（1）深入了解了安全电子商务协议的安全性质，尤其是原子性、可追究性与公平性。

（2）熟悉针对安全电子商务协议的常见攻击方法，用重放攻击分析了 IBS 协议和 CMP 协议，并对后者提出了改进方案。

（3）分析 Kailar 逻辑和卿-周逻辑的不足，提出了一种改进的逻辑分析方法，并给出了验证实例。

本文章节安排如下：

第一章 绪论，介绍研究背景、现状和本文所作的工作。

第二章 介绍安全电子商务协议的基本知识。并简单介绍几个典型的安全电子商务协议。

第三章 介绍了针对电子商务协的几种常见攻击，用重放攻击分析了 NewIBS 协议和 CMP 协议，并对后者提出了改进方案。

第四章 介绍电子商务协议的安全性质和分析方法，并分析了 Kailar 逻辑和卿-周逻辑的缺陷。

第五章 具体介绍一种改进的逻辑分析方法，并给出验证实例。

第六章 对全文工作进行了总结，并对下一步的工作进行了展望。

第二章 安全电子商务协议综述

电子商务发展经历了两个主要的发展阶段：第一个阶段主要是基于专用网的传统电子商务发展阶段；第二个阶段主要是基于因特网的现代电子商务发展阶段。

传统电子商务所采用的方式主要有：电子文件交换（EDI）、传真通信、文电处理系统（MHS）、电子金融交易（EFT）、自动支付机（ATM）、信用卡等。这些方式大多采用基于增值网的专用消息网的多存储转发方式，缺点是耗时多、成本高、互通性差。

现代电子商务以因特网为基础，比增值网的成本低、效率高，实时性和互通性好。但是，为了在因特网上方便、安全地进行电子商务，必须采用一系列信息安全技术保障措施。其中，安全电子商务协议是最重要的一种安全手段。

2.1 安全电子商务协议的基本概念

2.1.1 安全电子商务协议的基本需求

保密性、完整性、原子性、认证性和非否认性是安全电子商务协议的基本性质。

可追究性（accountability）是与非否认性密切相关的另外一个重要性质，是安全电子商务协议必须满足的基本要求。可追究性指协议主体应当对自己的行为负责，在发生交易纠纷时，主体可以提供必要的证据保护自身的利益。可追究性是通过发方非否认证据和收方非否认证据来实现的，即正确地执行完协议后，应当保证发送方收到POR(proof-of-receipt)并且接收方收到POO (proof-of-origin)。

除了上述要求外，安全电子商务协议还应当满足下述公平性要求。

公平性（fairness）包含两层含义。首先，正确地执行完协议后，应当满足可追究性，即保证发送方收到POR且接收方收到POO。其次，如果协议异常终止，协议应当保证通信双方都处于同等地位，任何一方都不占任何优势。

安全电子商务协议的另外一个基本要求是隐私性，即在协议的执行过程中，不应该泄露参与协议的主体的私有信息。除此之外，安全电子商务协议还应当满足实用性的需求，例如，没有冗余性、效率高、可靠性好等。

2.1.2 安全电子商务协议的基本结构

通常的安全电子商务协议的基本结构[27]如下。参与协议的主体有3个：

用户：安全地从服务提供方获得服务，然后通过金融机构安全地向服务提供方付费。

服务提供方：安全地向用户提供服务，并通过金融机构安全地向用户索取费用。

金融机构：负责向用户和服务提供方提供证据，然后从用户方帐户安全地提取资金，并将资金安全地支付给服务提供方帐户。

电子商务协议主要由以下3个步骤组成。

确定价格(price assurance)：用户和服务提供方通过执行协议，协商并确定价格。

提供服务(service provision)：服务提供方向用户安全地提供服务。

传递证据（invoice delivery）：金融机构向交易双方传递一个消息，表明已经从用户帐户安全地提取资金，并将资金安全地支付给服务提供方帐户。

2 .1.3 安全电子商务协议的分类

安全电子商务协议可以有多种分类方法。例如，根据功能分类，可分为安全电子支付协议、安全电子合同签订协议、电子邮件认证协议等。

根据协议中信息交换的不同，可以将安全电子商务协议分为以下两类：

（1）逐步交换协议（gradual exchange protocol），即参与协议的主体只有两个，它们通过许多步骤一步一步地暴露所交换的信息。此外，还有一类协议可以实现所谓“概率公平性”。这类协议类似于逐步交换协议：第一，它无须第三方参与；第二，通过许多回合一步一步地交换信息。

（2）可信第三方协议，即协议主体通过可信第三方交换信息，保证实现协议的各种安全目标，例如原子性、非否认性、可追究性、公平性、隐私性等。

对逐步交换协议，通常需要对它们做一种不合理的假设，即参与协议的两个主体具有相同的计算能力。此外，实现这类协议需要进行大量的信息交换，因此效率很低。基于以上原因，目前主流的电子商务协议都采用可信第三方协议方法。逐步交换协议在现实中很少应用，它们只有理论上的研究价值。

2.1.4 安全电子商务协议的运行环境及语义

电子商务协议在一个分布式环境中运行，这个环境包含3类主体：发送方A、接收方B和可信第三方TTP，其中TTP可以是一个或多个主体。在这个环境中，A和B之间可以直接通信，也可通过TTP转发。环境包含两方面：交易实体是否诚实和通信信道是否可靠[24]。协议的各种属性与运行环境密切相关。

假设通信信道不可靠，电子商务协议语句根据中断性可分为三类[24]：

(1) 协议语句A|B→B|A|TTP:M若A，B都是诚实的且通信信道是可靠的，则是不可中断的；否则是可中断的，因为A或B是不诚实的，它可能因对自己有利而不执行这条协议语句。

(2) 在信道可靠的情况下，协议语句TTP→B|A:M是不可中断的。因为TTP是诚实的，他肯定会执行这条协议语句，TTP发送的消息会被A或B正确地接收。在信道不可靠的情况下，TTP发送的消息有可能会丢失，第2类协议语句是可中断的。

(3) 协议语句A|B←→TP:M在信道可靠或不可靠的条件下都是不可中断的。因为TTP是诚实的，他使M可被ftp[28]操作取得。A或B可以通过这一操作获得对自己有用的消息，A或B不会放弃这一操作。即使在信道不可靠的条件下，A或B仍然可以通过多次ftp操作取得M。

2.2 典型的安全电子商务协议

常见的电子商务协议有：自动解决争论的公平交换协议[29]，安全套接层协议SSL (secure socket layer)[30]，安全电子交易协议SET (secure electronic transaction)[31]，匿名原子交易协议 (anonymous atomic transaction protocol)[32]，Franklin/Reiter协议[33]，基于公钥体制的IBS协议[34](internet billing service protocol)，可证实电子邮件协议CMP[35](certified electronic mail

protocol)等。下面简单介绍几个典型的安全电子商务协议。它们当中有一些简单的、示例性的协议是本文进行形式化分析的“试验床”。

1. 基于公钥体制的IBS协议

IBS协议(internet billing service protocol) 是由卡内基-梅隆大学开发的电子商务协议，该协议分为如下3 个部分

确定价格

(1) E →S: $\{Price\,Request\}_{K_e^{-1}}$

(2) S →E: $\{Price\}_{K_s^{-1}}$

在确定价格的过程中，用户E首先向服务提供方S发送一个用它的私有密钥K_e^{-1}签名的价格咨询消息。 如果服务提供方S同意这个价格，他就发送一个用他的私有密钥K_s^{-1}签名的价格同意消息。

提供服务

(3) E →S: $\{\{Price\}_{K_s^{-1}}, Price\}_{K_e^{-1}}$

(4) S →Invoice: $\{\{Price\}_{K_s^{-1}}, Price\}_{K_e^{-1}}$

(5) S →E: $\{Service\}_{K_s^{-1}}$

(6) E →S: $\{ServiceAcknowledge\}_{K_e^{-1}}$

(7) S →Invoice: $\{\{ServiceAcknowledge\}_{K_e^{-1}}\}_{K_s^{-1}}$

在提供服务协议中，第1条消息用户E向服务提供方S发送一个服务请求，服务提供方S把这条消息复制到发票上，并发送一条签名的服务消息给用户E。用户E收到服务后，发送一个签名的服务认可消息给服务提供方S，服务提供方S把它复制到发票上。

传递发票

(8) E →S: $\{Invoice\,Request\}_{K_e^{-1}}$

(9) S →B: $\{\{Invoice\}_{K_b}\}_{K_s^{-1}}$

(10) B →S: $\{\{Invoice\}_{K_s}\}_{K_b^{-1}}$

(11) B →E: $\{\{Invoice\}_{K_s}\}_{K_b^{-1}}$

在传递发票协议中,用户E给服务提供方S发送一个发票请求。服务提供方S向银行机构B发送一张先用银行机构的公开密钥加密，然后用他的私有密钥签名的发票。银行验证发票后，进行相应的转帐处理，将发票用他们的公开密钥加密后再用银行机构的私有密钥签名，然后分别发送给用户和服务提供方。

2. 可证实电子邮件协议CMP

可证实电子邮件协议CMP (certified electronic mail protocol)是由Robert Deng 和Li Gong等人提出的认证电子邮件协议。它运行在X.400定义的消息处理系统上,为电子邮件传输提供非否认服务。CMP的模型有两个:CMP1和CMP2。这两者的区别是：在CMP1中，加密的信息和密钥发送给第三方TTP，而在CMP2中，只有经过TTP的公钥加密后的密钥发送给TTP，由电子邮件接收者B进行解密。CMP1协议如下：

K_a，K_b，K_{ttp}分别为协议参与者 A，B 以及可信第三方 TTP 的公开密钥；

K_a^{-1}，K_b^{-1}，K_{ttp}^{-1}分别为协议参与者 A ,B 以及可信第三方 TTP 的秘密密钥；

h(m)为对消息 m 进行哈希运算得到的摘要；

$\{m\}_K$表示以K为会话密钥用对称密码体制加密消息m。

(1) A→B: A,B,TTP,h(m),$\{K\}_{K_{ttp}}$,$\{\{m\}_{K_a^{-1}}\}_K$

(2) B→TTP: $\{h(m)\}_{K_b^{-1}}$, $\{K\}_{K_{ttp}}$,$\{\{m\}_{K_a^{-1}}\}_K$

(3) TTP→B: $\{\{m\}_{K_a^{-1}}\}_{K_{ttp}^{-1}}$

(4) TTP→A: $\{\{h(m)\}_{K_b^{-1}},(B,m)\}_{K_{ttp}^{-1}}$

第(1)步，A选择一个会话密钥K，然后把消息m的摘要h(m)、消息m签名后用K加密的密文$\{\{m\}_{K_a^{-1}}\}_K$和加密的会话密钥$\{K\}_{K_{ttp}}$发送给B。第(2)步，B对h(m)签名，并连同后两部分转发给TTP。TTP收到后，通过解密获取$\{m\}_{K_a^{-1}}$，并校验A签名的有效性。同时，TTP对$\{h(m)\}_{K_b^{-1}}$校验B签名的有效性。然后，TTP通过由$\{\{m\}_{K_a^{-1}}\}_K$获得的m计算摘要h(m)，并与$\{h(m)\}_{K_b^{-1}}$中的h(m)比较。如果一致，在第(3)步，TTP

将$\{m\}_{K_A^{-1}}$用自己的私有密钥签名后传送给B，在第(4)步将B签过名的摘要和(B,m)用自己的私有密钥签名后传送给A。

3. 匿名原子交易协议

匿名原子交易协议(Anonymous Atomic Transactions)是由J.Camp和J.D.Tygar于1996年提出的，首次解决了电子商务协议中原子性与匿名性之间的矛盾，对推动电子商务发展起着至关重要的作用。该协议描述如下：

1. C→M: order;

2. M→C: $(n, contract, (goods)_K)_{K_M^{-1}}$;

3. C→B: $(n, timeout, M, L, coin)_{K_C^{-1}}$;

4. B→M: $(n, timeout, M, L, value)_{K_B^{-1}}$;

5. M→L: $(n, timeout, K)_{K_M^{-1}}$;

6. C←→L: $(commit, K, n)_{K_C^{-1}}$;

7. B←→L: $(commit, n)_{K_L^{-1}}$;

8. M←→L: $(commit, n)_{K_L^{-1}}$ 。

顾客发送商品订单给商家，商家收到后，发送已签名的交易号n、商品描述contract及用对称密钥K加密的goods给顾客。顾客在第三步向银行发送签过名的消息，银行检验coin是否有效及是否被重用；在第四步银行通知商家准备提交，商家确认n、L、timeout（value为coin的币值）。第五步中商家向交易日志L发送K、timeout和n进行提交，L验证是否超时。第六、七、八步中，C、B、M分别通过ftp操作从L处获得提交成功的证据。

4. Franklin/Reiter协议

Franklin/Reiter协议也是一个重要的公平交换协议，它在参与者X和Y之间通过第三方Z交换秘密。协议描述如下：

1. X --> Y: Xsecret1;

2. Y --> X: Ysecret1;

3. X --> Z: Xsecret2correct 或 Xsecret2incorrect;

4. Y --> Z: Ysecret2correct 或 Ysecret2incorrect;

5. Z --> X: Ysecret2correct 或 ExchangeAbort;

6. Z --> Y: Xsecret2correct 或 ExchangeAbort。

在该协议中，参与者X与Y相互交换秘密，第三方Z控制两个参与者或者接收或者均得不到彼此的秘密。X、Y把各自的秘密分为两部分。第一二步，两者各自把秘密的第一部分传给对方；三四步中，各自把秘密的第二部分传给第三方Z。在实际的FR协议的第四步之后，Z对X和Y秘密的第二部分进行基于HASH函数的检验。之后，Z要么把秘密的第二部分正确传送，要么通知X、Y交换失败。

第三章 针对电子商务协议的攻击

协议在日常生活中大量存在，协议是一系列的规则和协定，它们被用于定义两个或两个以上的参与者之间的一个通信框架。由此可知安全电子商务协议至少应该具有以下基本性质：

1) 安全电子商务协议的参与者不能少于两个，一个人可以通过执行一系列的步骤来完成一项任务，但它不构成协议；

2) 安全电子商务协议包含一系列的消息接收和消息发送行为，参与者还可能会对消息进行内部处理；

3) 安全电子商务协议是有目的的事件，参与各方希望通过执行安全电子商务协议达到一个目的，可能是传送电子产品，也可能是网上支付等；

4) 安全电子商务协议的成功依赖于参与各方遵守规则的参与执行，任何一方破坏规则都将导致协议无法顺利完成。

安全电子商务协议运行过程之中的参与者，称为主体，这里的主体的概念很广泛，可能是人，也可能是一个程序，或者是一个服务器。协议的运行由一些相互独立的有先后顺序的动作序列和步骤构成，这种独立的动作序列被称为一个角色或者身份。每个角色的功能是独立的，但相互之间是关联的和交互的，比如发起者、响应者等等。在协议中，主体与角色的概念是不尽相同的，一个主体可能就代表一个角色，同样也可能扮演多个角色和身份。从发起者发起一个协议开始，到最终协议的结束，称为协议的一轮运行。一轮协议的运行当中所涉及到的参与者的数目，或者角色不一定恰好符合安全协议的规定，其中那些破坏协议的正常运行，或者不遵守协议规定步骤的参与者称为攻击者(或者叫做攻击者角色)，其他的参与者称为诚实参与者(或者叫做诚实角色)。协议的一个参与者 A 向另外一个参与者 B 传递一个消息，称 A 的动作为发送，B 的动作为接收，A 称为消息的发送者，B 称为消息的接收者。一个安全电子商务协议 P 在运行过程中，假如有攻击者 I 存在，并且没有被系统或者诚实角色所察觉，同时攻击者 I 在参与过程之中并没有利用任何密码学上的漏洞，称安全电子商务协议 P 被攻破，即安全电子商务协议 P 存在设计上的漏洞。安全电子商务协议是一门艺术的科学，设计安全电子商务协议绝非简单的工作，它需要精确的和复杂的科学思维。

针对协议的弱点存在不同的攻击方法。了解入侵者的知识和能力以及常见的对电子商务协议的攻击方法对于如何避免这些攻击，如何证明协议的正确性，如何设计有效的形式化分析方法具有重要的意义。本章简单介绍了这方面的知识并给出了两个对协议进行重放攻击的例子。

3.1 入侵者的知识和能力

密码学是安全电子商务协议的学科基础，如果密码体制被破解则安全协议将会随之被破解而变得毫无意义。一般情况下我们认为在安全电子商务协议中使用的加密算法是安全的、不会被破破解的，加密算法对于安全电子商务协议而言被看作是一个黑盒子，它提供对通信协议信息处理环节的加密解密操作。

(1)入侵者知识

入侵者知识包括入侵者运行协议前的初始知识;以及在协议运行过程中增加的知识，构成历史知识集，以作为入侵者下次协议运行的初始知识。具体包括如下:

① 熟悉现代密码学，知道协议中用到的公开的密码算法和密码技术;

② 知道参与协议运行的各实体名及其公钥;

③ 拥有自己的加密密钥和解密密钥;

④ 拥有前次协议运行的所有网上消息(明文和密文)及这些消息经分解、合成后得到的知识;

⑤ 拥有网上消息经入侵者可能的加密、解密、散列等密码操作后得到的知识。

(2)入侵者能力

假设入侵者完全控制了通信网络，即:协议所有的消息都要经过入侵者，入侵者能够读取、修改、重定向任何消息。具体包括如下:

①可窃听、拦截系统中传送的任何消息;

②每窃听或收到一个消息，即增加自己的知识;

③可解密用他自己加密密钥加密的消息;

④可在系统中插入新的消息;

⑤即使不知道加密部分的内容，也可重放他所看到的任何消息(可改变其中

的明文部分)；

⑥可运用他知道的所有知识(如临时值等)，并可产生新的临时值；

⑦可分解、组合他所知道的知识，并产生新的知识；

⑧可对已有的知识进行加密、解密、散列等密码操作，并产生新的知识。

3.2 电子商务协议的常见攻击

在设计和分析电子商务协议时，必须对攻击对手有全面和深刻的认识，所设计的电子商务协议至少应当抵抗已知的各种攻击。 电子商务协议的常见攻击[36]如下：

• 假冒攻击(impersonation attack)：入侵者冒充协议的一方诚实主体与另一方进行协议运行，被假冒方甚至根本没有参与此次协议运行。入侵者可以假冒协议发起方，也可以假冒响应方，或是服务器方。入侵者一般是利用以前(或当前)协议运行中获得的有关消息或秘密的相关知识发起这种攻击。

• 篡改攻击(tampering attack)：入侵者篡改消息内容而发起的攻击。

• 重放攻击(replay attack)：入侵者复制协议(包括当前协议或其他协议)中的消息(或消息成分)并作为当前运行的协议中的消息(或消息成分)重新发送。依据消息接收者的不同，重放攻击又包括直接重放(消息被转发给预定的接收者，但具有一定的延迟)、转移重放(消息被转发给第三者)、反射转发(消息被回发给发送者)。

• 密钥泄露攻击(known-key attack)：入侵者利用各种类型密钥的泄露(包括旧的会话密钥泄露和长期密钥泄露)而发起的对当前协议的主动(如假冒)和被动(如泄露新的会话密钥)攻击，设置这种攻击的目的是测试协议是否符合完善的前向保密性 (perfect forward secrecy)。密钥泄露攻击也叫已知密钥攻击。

• 反射攻击(reflection attack)：入侵者截获来自发送方的消息，经篡改后直接返回给原消息发送方，类似于消息重放中的反射转发。这种攻击产生的原因常常是因为协议中密文消息结构具有相似性。

• 重置攻击(reset atack)[37]：对于认证协议，入侵者以认证方(verifier)的角色与被认证方(prover)进行多次并行交互，把被认证方的状态重新置回到初始条件(或后退到某一状态)后再次执行协议。该攻击的目的是希望获得更多的知

识以便将来能假冒被认证方。

• 选择文本攻击（chosen-text attack）：在挑战——响应协议中，入侵者策略地选择挑战消息以诈取协议发起方的长期密钥信息。选择文本攻击包括选择明文攻击(如果要求协议发起方对挑战进行加密、签名、或MAC运算)、选择密文攻击(如果要求协议发起方对挑战进行解密)。

• 前向搜索攻击（forward search attack）：类似于字典攻击，用于从密文消息中识别出明文。

• 并行攻击(interleaving atack)：入侵者利用协议的两次或多次并行运行，用某一次协议运行中的消息来形成另一次运行中的消息，从而对协议发起攻击。

• 串通攻击(conspiracy attack)：入侵者与其他主体串通在一起发起的攻击。

3.3 针对 NewIBS 协议的重放攻击

在IBS协议(internet billing service protocol)的传递发票阶段，将发票Invoice 分解成发票号和除了发票号之外的信息Invoice＇，将传递发票阶段的协议修改为（将修改后的协议记为NewIBS）：

(1) E →S: $\{Invoice'\mathrm{Re}quest\}_{K_e^{-1}}$

(2) S →B: $\{\{Invoice'\}_{K_b}\}_{K_s^{-1}}$

(3) B →S: $\{\{Invoice'\}_{K_s}\}_{K_b^{-1}}$

(4) B →E: $\{\{Invoice'\}_{K_e}\}_{K_b^{-1}}$

NewIBS协议存在如下的重放攻击[38]：

(1) E →S: $\{Invoice'\mathrm{Re}quest\}_{K_e^{-1}}$

(2) S →B: $\{\{Invoice'\}_{K_b}\}_{K_s^{-1}}$

(2＇) I(S) →B: $\{\{Invoice'\}_{K_b}\}_{K_s^{-1}}$

(3) B →S: $\{\{Invoice'\}_{K_s}\}_{K_b^{-1}}$

(3＇) B →I(S): $\{\{Invoice'\}_{K_s}\}_{K_b^{-1}}$

(4) B →E: $\{\{Invoice'\}_{K_e}\}_{K_b^{-1}}$

(4 ') B →I(E): $\{\{Invoice'\}_{K_e}\}_{K_b^{-1}}$

在第（2）步中，S向B传送发票之后，入侵者I窃听到这个发票消息，并在（2 ' ）中冒充S将该发票消息转发给B，在第（3 ' ）和（4 ' ）中入侵者分别拦截B转发给E和S的消息。这样，攻击成功。此时，银行收到两张发票。银行B两次向商家S 转账，从而导致客户E必须支付双倍TotalPrice的货款，却只收到一次价值TotalPrice的服务。

3.4 针对 CMP 协议的重放攻击

CMP 协议存在如下攻击：

（1） A→B: A,B,TTP,h(m),$\{K\}_{K_{ttp}}$,$\{\{m\}_{K_a^{-1}}\}_K$

（2） B→TTP: $\{h(m)\}_{K_b^{-1}}$, $\{K\}_{K_{ttp}}$,$\{\{m\}_{K_a^{-1}}\}_K$

(2 ') I(B)→TTP: $\{h(m)\}_{K_b^{-1}}$, $\{K\}_{K_{ttp}}$,$\{\{m\}_{K_a^{-1}}\}_K$

（3）TTP→B: $\{\{m\}_{K_a^{-1}}\}_{K_{ttp}^{-1}}$

(3 ') TTP→I(B): $\{\{m\}_{K_a^{-1}}\}_{K_{ttp}^{-1}}$

（4） TTP→A: $\{\{h(m)\}_{K_b^{-1}},(B,m)\}_{K_{ttp}^{-1}}$

（4 ' ） TTP→I(A): $\{\{h(m)\}_{K_b^{-1}},(B,m)\}_{K_{ttp}^{-1}}$

在第 2 步中，B 向 TTP 发送消息后，入侵者 I 窃听到这个消息，并在第(2 ')步中冒充 B 将该消息转发给 TTP，TTP 将它作为新一轮的协议来响应，在第(3 ')步和(4 ')步中入侵者分别拦截 TTP 转发给 B 和 A 的消息。这样，攻击成功。因为在第(2 ')和第(2)步中，TTP 收到的消息是一样的，所以在第(3 ')步中 TTP 给 B 而实际被入侵者拦截的消息就是协议第(3)步中发送给 B 的内容，入侵者 I 用 A 和 TTP 的公钥 K_a、 K_{ttp}解密$\{\{m\}_{K_a^{-1}}\}_{K_{ttp}^{-1}}$，这样入侵者就得到了客户之间发送的消息 m 而 TTP 却以为是执行了两轮协议。显然原协议不能抵御重放攻击，未满足机密性。

针对上述缺陷，我们对协议进行分析并做了一定的改进。

改进后的CMP协议如下：

K_a，K_b，K_{ttp}分别为协议参与者A，B以及可信第三方TTP的公开密钥；

K_a^{-1}，K_b^{-1}，K_{ttp}^{-1}分别为协议参与者A，B以及可信第三方TTP的秘密密钥；

h(m)为对消息m进行哈希运算得到的摘要；

$\{m\}_K$表示以K为会话密钥用对称密码体制加密消息m；

A←→TTP：m 表示主体A通过多次ftp操作，从TTP处获得了消息m。

$EOO=\{A,B,TTP,\{m\}_{K_b}\}_{K_a^{-1}}$

$EOR=\{A,B,TTP,h(\{m\}_{K_b})\}_{K_b^{-1}}$

$EOD=\{B,\{m\}_{K_b},EOR\}_{K_{ttp}^{-1}}$

① $A\rightarrow B: A,B,TTP,h(\{m\}_{K_b})$，$\{K\}_{K_{ttp}}$，$\{EOO\}_K$

② $B\rightarrow TTP: EOR$，$\{K\}_{K_{ttp}}$，$\{EOO\}_K$

③ $B\longleftrightarrow TTP:\{EOO\}_{K_{ttp}^{-1}}$

④ A←→TTP: EOD

协议开始执行时，A把消息m用B的公钥K_b加密，生成发送m的非否认证据EOO；随之选择一个会话密钥K，并用K将EOO加密；接下来再计算消息$\{m\}_{K_b}$的摘要$h(\{m\}_{K_b})$、应用K_{ttp}加密会话密钥K；然后将消息①发送给B。第②步，B收到后生成收到满足$h(\{m\}_{K_b})$的消息的非否认证据EOR，并将消息②发给可信第三方TTP。TTP收到后，通过解密获得EOO，并校验A签名的有效性。同时，TTP对EOR校验B签名的有效性。然后，TTP用由EOO获得的$\{m\}_{K_b}$计算摘要$h(\{m\}_{K_b})$，并与EOR中的$h(\{m\}_{K_b})$比较。如果一致，在第③与第④步，B和A分别通过ftp操作从TTP处获得消息③和④，即使在信道不可靠的条件下，A或B仍可通过多次ftp操作取得消息。

我们对协议进行分析，当发生如前面所述的重放攻击时，入侵者从EOO得到的是加密的消息$\{m\}_{K_b}$，入侵者并不知道B的私钥K_b^{-1}，因而也无法解密出消息明

文m，这种改进有效地抵御了重放攻击。

IBS协议的提供服务阶段，我们对其进行分析发现它存在和CMP协议同样的缺陷，可以采用类似的办法对其进行改进，在此不再详述。

3.5 小结

在设计安全的电子商务协议时，必须对攻击对手有全面和深刻的认识，所设计的协议至少应当抵抗已知的各种攻击。本章描述了入侵者的知识和能力，并简单介绍了重放攻击、密钥泄露攻击、选择文本攻击等攻击方法。重放攻击是最基本、最常用、危害性最大的一种攻击形式，因此本章最后给出了针对NewIBS协议的重放攻击和针对CMP协议的重放攻击，并且提出了对CMP协议进行改进的方案和详细分析。

第四章 电子商务协议的安全性

电子商务协议的安全性是一个很难解决的问题，电子商务协议的运行不是独立的，而是处于某种不安全的环境之中的，因而它是容易出错的，并且错误很难完全由人工识别。许多事例已经向我们表明，即使在设计一个安全协议时对运行环境做了最为充分的估计，并且很小心仔细地进行了设计，而且使用了很多年，但依然包含一些微妙的漏洞没有被发现。造成这种现象的原因有很多，但最主要的还是因为协议的设计者对安全需求定义研究的不够彻底，并且对设计出来的协议也没有进行足够的安全性分析。

安全电子商务协议分析的困难性在于：

1)安全目标本身的微妙性和不确定性。例如，表面上十分简单的“认证性目标”就十分微妙。关于认证性的定义，至今存在各种不同的观点。

2)协议运行环境的复杂性。实际上，当安全电子商务协议运行在一个十分复杂的公开环境时，攻击者处处时时都存在。我们必须形式化地刻画安全电子商务协议的运行环境，这当然是一项艰巨的任务。

3)攻击者模型的复杂性。我们必须形式化地描述攻击者的能力，对攻击者和攻击行为进行分类和形式化的分析。

4)安全电子商务协议在实际运行中的异常复杂性。因为在很多时候，多轮协议是并发执行的，同一个主体在这些安全电子商务协议中又会充当不同的角色。

以上四点原因使得安全电子商务协议的分析和设计变得更加复杂并具有挑战性。从安全电子商务协议的分析和设计角度来看，我们必须要对协议的安全性作出理论的分析，并借助于一些自动化的工具来完成安全电子商务协议安全性的分析和证明。多年来为了应对这一挑战，科学家们投入了大量的精力设计开发了不同种类的研究理论与方法，比如形式化方法、可证明安全理论、零知识证明理论等等，其中以形式化分析方法的成果最为显著和突出，其发展前景被安全领域的专家们普遍看好。

本章将介绍电子商务协议的安全性质和设计准则以及分析方法，并通过对一个实例的分析发现了 Kailar 逻辑和卿-周逻辑的缺陷。

4.1 电子商务协议的安全性质

电子商务协议验证就是验证协议的安全属性能否得到保证。常见的属性主要有机密性、完整性、认证性、非否认性、可追究性、公平性、原子性等。介绍如下：

（1） 有效性（availability）

电子商务以电子形式取代纸张，那么如何保证这种电子形式的贸易信息的有效性则是开展电子商务的前提。电子商务作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此，要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻和确定的地点是有效的。

（2） 机密性（confidentiality）

电子商务作为贸易的一种手段，其信息直接代表着个人、企业或者国家的商业秘密，传统的纸面贸易都是通过邮寄信封的信件或者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。电子商务是建立在一个较为开放的网络环境上的（尤其Internet是更为开放的网络），维护商业机密是电子商务全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。

（3）不可否认性(non-repudiation)：

不可否认性是指贸易双方对其所作的动作不可抵赖，换句话说就是，会话结束后，会话各方都没有能力否认其参加会话的事实。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。这也就是人们常说的“白纸黑字”。因此，要通过网络进行交易，就必须在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。

（4）认证性（authenticity）

认证性是指信息的接收者能确认信息的真实来源。电子商务可能直接关系到贸易双方的商业交易，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则是保证EC顺利进行的关键。在无纸化的电子商务方式下，通过手写签名和印章进行贸易方的认证已是不可能的。

（5）可追究性(accountability)

可追究性指协议主体应当对自己的行为负责，在发生纠纷时，主体可以提供必要的证据保护自身的利益。可追究性通过发方非否认证据 (POO)和收方非否认证据(POR)实现，即正确执行完后，应当保证发送方收到POR且接收方收到POO。

（6）公平性(fairness)

公平性保证参加协议的各方在协议执行的任何阶段都处于同等地位，当协议执行完后或者各方得到各自所需的或者什么也得不到。它包含两层含义：首先，正确地执行完协议后保证发送方收到POR且接收方收到POO；其次，如果协议异常终止，协议应保证通信双方都处于同等地位，任何一方都不占优势。

（7） 原子性[39] (atomicity)

原子性分为三级，呈向上兼容，后者包含前者。

货币原子性(Money Atomicity)：电子商务交易发生前后资金守恒，资金在电子支付中既不会创生也不会消失，顾客货币的减少等于商家货币的增加。

商品原子性(Goods Atomicity)：协议一定满足货币原子性且保证顾客收到商品当且仅当对应商家获得付款。

确认发送原子性(Certified Delivery)：首先，协议一定满足货币原子性和商品原子性；其次，需对顾客从商家购得的商品和商家付给顾客的商品分别确认，保证客户得到他所订购的商品。如有争议，拥有仲裁依据证实交易商品的内容。

（8）完整性（integrity）

电子商务简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商业信息的完整、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、信息重复或者信息传送的次序差异也会导致贸易各方信息的不同，贸易各方信息的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。因此，要预防对信息的丢失和重复并保证信息传送次序的统一。

4.2 电子商务协议的分析前提

在分析协议安全性时，常用的方法是对其各种可能的攻击，测试其安全度。这些攻击的目标通常分为三种：

（1）协议中常用的密码算法

（2）算法和协议中采用的密码技术

（3）协议本身

对于前两种的研究不是本文的主题，协议本身才是我们要研究的对象，但是有一点要强调的是，在分析电子商务协议时，我们通常做以下基本假设：

(1) 协议所采用的加密算法足够强壮。

(2) 密码系统是完善的(perfect)，即任意的加密消息块只能被拥有解密密钥的主体理解，并认为在有限时间和空间内，或者加密消息失去价值之前是不会被攻击者理解的。

(3) 无加密项冲突，即加密数据无碰撞性假定。无碰撞包含3层意思：任意两条不同的明文消息使用相同的密钥加密后不会产生相同的密文消息，任意两条不同的明文消息使用任意两个不相同的密钥加密后不会产生相同的密文消息，相同的明文消息使用任意两个不相同密钥加密后不会产生相同的密文消息。

(4) 哈希函数是抗碰撞的。

(5) 加密数据完整独立性假定。假定认为一个加密消息块无法被拆分成数个小的加密块，同样一个加密消息块无法由数个小的加密块连接拼凑而成，而且一条消息中的两个加密块可以被区分开来，被认为是两次分别到达。

(6) 攻击者具有对消息进行加密和解密运算的能力，还具有对连接消息项进行拆分的能力；此外，攻击者了解协议的运行规则，可以根据已知的知识合理推导隐藏知识。一般而言，攻击者还可以得到协议运行中参与主体之间传递的消息，并可以参与到协议的运行当中。

(7) 诚实的主体遵循协议规定执行协议，不诚实的主体不会完全遵守协议。

这种假设是必要的，因为它有利于我们关注协议本身，而不考虑过多的细节，这也是我们分析电子商务协议的一个重要前提。

4.3 电子商务协议的设计准则

在电子商务协议的设计过程中，一方面要求协议具有足够的复杂性以抵抗各种攻击；另一方面，又要求协议尽可能地经济和简单，以利于实现。当然，要满足的性质越多，所设计的协议就会越复杂，归纳起来可以提出以下电子商务协议的设计准则：

（1）尽量采用一次性随机数（Nonce）和挑战（Challenge），而不是时戳（Timestamp）。

在已经设计的一些协议里，人们采用了时戳以保证消息的新鲜性，但这需要个实体之间严格保持一个同步时钟或者专门有一个时戳服务器。这个条件与环境的实现有时并不容易，且容易受到干扰，故建议采用 Nonce 或 Challenge 来代替 Timestamp。SET 协议就是其中一例。

（2）用公认强壮安全的密码算法

协议必须采用具有代表性的密码算法，如 AES、三重 DES、IDEA、RSA 等，这些是经过大量研究证明具有较高安全强度的。这条准则的提出是因为电子商务协议的安全性是以密码算法的强度为基础的。

（3）方便扩展

协议要具有一定的灵活性，其中之一便是允许对信息的组成与结构进行扩展，在 SET 协议中几乎每一条消息都含有扩展域。

（4）最小的初始化假设

在进行协议设计前，通常需要对网络环境做出分析，提出合适的初始化假设。例如：CA 是可信赖或信道是可信赖的，或者各实体都拥有自己的证书，等等。但是，初始化假设并非越多越好，因为有些假设可能本身存在着不确定因素，或者根本经不起严格推理，所以应尽可能减少初始化假设的数目。

（5）根据协议目标选择适当密码技术

在电子商务协议中，加密、签名等密码技术经常用到。但它们同时也是耗时且提高成本的，所以在用它们之前，要明确使用它们的原因，否则可能造成消息的冗余，而不正确使用，甚至可能会导致错误的产生。

（6）消息应具有明确的意义

协议中每一条消息都有其意义和作用，对消息的解释应依赖于消息本身。即使有一种合适的形式化语言可以描述某条消息，那么也应该可以用一句话来描述其内容，即可以将消息由符号转换为更易理解的语句。

4.4 电子商务协议的分析方法简介

目前电子商务协议的分析方法主要有非形式化方法和形式化方法。

非形式化方法是利用现在已知的攻击方法对协议进行攻击,以攻击是否有效判断协议是否安全或者是直接观测协议有无漏洞。这种方法显的不够严密,不能深入实质;由于实际中还存在许多未知的攻击方法,因此无法检测在未知攻击下协议是否存在缺陷;直观检测则必须在协议实现之后才能实行,这有可能导致人力物力的巨大浪费。

安全电子商务协议涉及大量数学和逻辑学领域的知识,安全电子商务协议目标的精确和标准的定义必须要借助于数学和逻辑学语言的描述和刻画,对安全电子商务协议的分析同样必须借助数学和逻辑学的模型和手段。

形式化的分析方法是采用各种形式化的语言或者模型,为安全协议建立模型,并按照规定的假设和分析、验证方法证明协议的安全性。简而言之,形式化分析的目的就是为证明系统的安全属性提供一种严格的、彻底的方法。安全协议的多样性决定了需要应用不同的分析方法。形式化分析方法主要包括定理证明、模型检测和逻辑分析。

模型检验(ModelChecking)是一种自动分析和验证技术,是形式化验证中很重要的一种方法。它是一种面向有限状态系统的验证技术。所以模型检验适用于一定范围的协议,速度比较快,而且便于实现自动化。只要计算机处理能力和时间足够,模型检验过程总能终止并给出待检验性质的真、假值的回答。但是状态空间爆炸的问题限制了它的应用,使它不能用来分析过于复杂的协议。

形式化逻辑推理可以在安全协议实现之前,对其进行逻辑分析,即进行协议分析,就像证明数学命题一样,逻辑严密,并且它不受协议规模的限制,因此这种方法成了当今人们研究的热点问题。

形式化分析方法有如下优点:

(1) 形式化分析方法除去了在非形式化说明中不可避免的大部分含糊不清的描述,这种精确性为开发人员与用户对需求的一致性理解,及需求的正确执行提供了更大的可能性,不会产生误解;

(2) 形式化分析方法能够精确的验证协议所做的假设和环境是否满足协议的属性;

(3) 形式化分析方法能够提供一个协议优点和缺点的完整内幕;

(4) 形式化分析方法通过对需求分析中所描述的系统行为提供逻辑的精确

论证是非常系统的、彻底的；

（5）形式化分析方法在系统描述阶段以及具体实施阶段都提供了相应的工具。

形式化分析方法能全面深刻地检测到协议中的细小漏洞，并能发现现有的攻击手段对协议造成的威胁，甚至能发现新的攻击方法。形式化分析方法以其严谨、简洁的特点而成为分析安全电子商务协议的重要方法，是电子商务领域研究的热点。

用形式化方法分析电子商务协议，首先要对协议及其必须满足的性质进行形式化描述，然后用某种方法（定理证明、模型检测或逻辑分析）分析协议。需要指出的是：用形式化方法分析电子商务协议，只是保证协议安全性的必要条件而非充分条件。

本文主要用逻辑分析方法分析电子商务协议的安全性质，而Kailar逻辑是所有逻辑分析方法中框架最自然的，下面简单介绍Kailar逻辑和在Kailar逻辑基础上形成的卿-周逻辑。

4.5 Kailar 逻辑和卿-周逻辑简介

4.5.1 Kailar 逻辑简介

Kailar 逻辑是 Rajashekar Kailar 于 1995 年提出的一种用于分析电子商务协议或其他需要可追究性的协议的形式化逻辑语言。正确设计电子商务协议是可以清除协议缺乏可追究性这一漏洞的，Kailar 逻辑就是用来分析协议是否具有可追究性的，利用它，经过推理，就可以知道参与协议的任何一方主体在协议完毕后，是否能提供充分的证据以解决以后可能出现的争议。如果能，则说明此协议具有可追究性；如果不能，则不具有可追究性，说明协议的设计有问题，有待改进。

Kailar 逻辑主要用于分析电子商务协议的可追究性。它由下述 6 个构件组成。

(1) 强证明构件：A CanProve x。对于任何主体 B，主体 A 能执行一系列操作使得通过这些操作以后，A 使 B 相信公式 x 而不泄漏任何关于 y（y!=x）的秘

密给 B。

(2) 弱证明构件：A CanProve x to B。对于特定主体 B，主体 A 能执行一系列操作使得通过这些操作以后，A 使 B 相信公式 x 而不泄漏任何关于 y（y!=x）的秘密给 B。

显然，强证明可推出弱证明。

(3) 签名验证构件： K_a Authenticates A。密钥 K_a 用于验证主体 A 的数字签名。

(4) 消息解释构件：x in m。x是m中一个或几个可被理解的域，与具体的协议相关。

(5) 声明构件：A Says x。主体A声明公式x，并对x以及x能推导出的公式负责。

(6) 消息接收构件：A Receives m SignedWith K^{-1}。主体A收到一个用 K^{-1} 签名的消息m。

(7) 信任构件：A IsTrustedOn x。 主体A对公式x有管辖权。通常，这种表达形式用于表示关于密钥认证权威（如CA）或解释由权威机构发行的证书的信任假设上。

这种信任程度分有两种：

（1）全球化信任：即A如果具有这种信任度，则所有主体B相信A所做的陈述x。

（2）非全球化信任：表示为 A is TrustedOn by B。即：特定主体B相信A所做的陈述x。

Kailar逻辑共有以下4个推理规则。

（1）连接规则

$$\frac{A \text{ CanProve } x,\ A \text{ CanProve } y}{A \text{ CanProve } (x \wedge y)}$$

如果 A 能够证明公式 x，并且 A 能够证明公式 y，那么 A 就能够证明公式 x∧y。

（2）推理规则

$$\frac{A \text{ CanProve } x,\ x \Rightarrow y}{A \text{ CanProve } y}$$

如果A能够证明公式x，并且公式x能推导出公式y，那么A能够证明公式y。

（3） 签名规则

$$\frac{\text{A Receives(m SignedWith } K^{-1}),x \text{ in m, A CanProve(K Authenticates B)}}{A\ Can\ Prove\ (B\ \text{Says x})}$$

如果A收到用私钥K^{-1}签名的消息m，m中包含了x，并且A能够证明公钥K能够验证B的身份，那么A就能够证明B对公式x负责。

（4） 信任规则

$$\frac{\text{A CanProve(B Says x), A CanProve(B IsTrustedOn x)}}{\text{A CanProve x}}$$

如果A能够证明B声明了公式x，并且A能够证明B对x有管辖权，那么A就能够证明公式x。

应用Kailar逻辑来分析电子商务协议分为以下5个步骤：

（1）标明协议要达到的步骤；

（2）解释协议的语句，并将它们转换为逻辑公式。在这一步中，只对那些包含签过名的明文信息和分析可追究性相关的语句进行解释；

（3）标明分析协议时所需要的初始化假设；

（4）应用推理规则对协议进行逻辑分析；

（5）得结论，若分析结果与目标不一致，则说明协议可能会有可追究性方面的问题。

Kailar 逻辑的提出开辟了形式化逻辑方法发展的另一条道路，即从信念逻辑中走出来，专门针对协议的可追究性的分析而提出了这种逻辑，并且可以探测和消除协议中存在的信息冗余。正是由于其专门性，因此才导致了 Kailar 逻辑应用的局限性。因为有各种各样的协议（包括电子商务协议）往往不仅要求协议具有可追究性，还要有公平性、信用等其他性质，这就需要对 Kailar 逻辑进行扩展。另外，Kailar 逻辑本身应该说构造并不复杂，推理起来甚至比 BAN 逻辑还容易，并且比较灵活，尤其是在确定协议分析目标方面，可以依照不同协议列举出协议应该或者是想达到的目标，而不像 BAN 逻辑那样，固定形式化。总的说来，Kailar 逻辑要比 BAN 逻辑好，更自然，尤其是语义方面。

然而，Kailar 逻辑自身也存在一定的缺陷，同 BAN 逻辑一样，Kailar 逻辑

在对参与协议的各个主体进行初始化假设时，也是非形式化的，这就使得我们容易犯错，导致分析失败，即使责任可追究性不全的协议也可能被误认为其在这一性质上是全面的。还有，在 Kailar 逻辑中，公式 A CanProve x 要求主体 A 向任何主体 B 证明公式 x 时不泄露任何秘密 y(y!=x)给 B,这就使得 Kailar 逻辑在解释分析协议语句时，只能解释分析那些签过名的明文消息，这就限制了它的使用范围。

4.5.2 卿-周逻辑简介

卿-周逻辑是Kailar逻辑的改进、增强和扩充，可同时分析安全电子商务协议的可追究性和公平性。在这个新的形式化分析方法中，每个主体在协议运行前拥有一个初始拥有集合，它由一些公式组成。随着协议分析的进行，主体的拥有集合不断扩大，到协议运行结束时，每个主体拥有一个最终拥有集合。

协议的可追究性是通过发方非否认和接收方非否认两个基本目标实现的。在这个新的形式化分析方法中，通过验证POO(proof-of-origin)属于接收方的最终拥有集合，并且POR(proof-of-receipt)属于发送方的最终拥有集合是否成立，验证协议的可追究性。

协议的公平性包含两层含义：首先，协议正常完成后，保证发送方收到POR且接收方收到POO；其次，如果协议异常终止，协议应保证通信双方都处于同等地位，任何一方都不占有优势。或者等价地说，消息接收方收到POO当且仅当消息发送方收到POR。在新的形式化分析方法中，当协议在任何一步异常终止时，验证协议是否满足公平性的方法是POO属于接收方的集合是否当且仅当POR属于发送方的拥有集合。

下面简单介绍卿-周逻辑中用到的部分基本符号：

|：“或”运算符；

P：主体变量；

P∋X：主体 P 拥有公式 X,它和 $x \in O_P$ 等价，O_P 是 P 的拥有集合；

P≻ X：主体 P 能够证明公式 X；

P→X：主体 P 对公式 X 负有责任；

$\xrightarrow{K_P} P$：密钥 K_P 可以用于验证主体 P 的身份。

在卿-周逻辑中，每个主体在协议运行前拥有一个初始拥有集合，它由一些公式组成。随着分析的进行，主体的拥有集合不断扩大，到协议运行结束时，每个主体拥有一个最终拥有集合。假设协议由n条语句组成。在协议开始之前，主体P的初始拥有集合记为O_p^0，它包含环境分配给P的密钥和P能证明的公式。当协议的第i条语句执行完毕后，主体P的拥有集合记为O_p^i。当协议经过n步运行终止时，用O_p记P的最终拥有集合。

卿-周逻辑共有6条推理规则：

R1. 签名规则

$$\frac{P \ni \{x\}_{K_q^{-1}}, P \succ \xrightarrow{K_q} Q}{P \succ (Q \rightarrow x)}$$

如果主体 P 拥有用K_q^{-1}签过名的公式 x，并且 P 能够证明K_q可用于验证主体 Q 的身份，那么 P 可以证明主体 Q 对公式 x 负有责任。

R2. 连接规则

$$\frac{P \succ Q \rightarrow (x,y)}{P \succ Q \rightarrow x; P \succ Q \rightarrow y}$$

$$\frac{P \succ Q \rightarrow x; P \succ Q \rightarrow y}{P \succ Q \rightarrow (x,y)}$$

$$\frac{P \succ x; P \succ y}{P \succ (x,y)}$$

$$\frac{P \succ (x,y)}{P \succ x; P \succ y}$$

如果主体 P 能够证明主体 Q 对某一公式的连接或并负有责任，那么 P 能够证明 Q 对这个公式的各个部分负有责任。反之，P 能够证明 Q 对几个公式负有责任，那么 P 能够证明 Q 对这几个公式的连接或并负有责任。

R3. 密文理解规则

$$\frac{P \succ Q \rightarrow \{X\}_K, P \succ Q \ni K}{P \succ Q \rightarrow x}$$

这条规则用于理解签过名的加密消息，以弥补 Kailar 逻辑的不足。如果主体

P 能够证明主体 Q 对某个用 K 加密过的公式 x 负有责任,并且 P 能够证明 Q 拥有加密密钥 K(也是解密密钥),那么 P 能够证明 Q 对 x 负有责任。

R4. 拥有规则

$$\frac{x \in O_p^0}{\forall Q, Q \succ P \ni x}$$

如果 P 的初始拥有集合中包含某个公式 x,那么任何一个其他的主体 Q 都能证明 P 拥有这个公式 x。

R5. 传递规则

$$\frac{A \succ TTP \rightarrow m}{A \succ B \ni m}$$

$$\frac{B \succ TTP \rightarrow m}{B \succ A \ni m}$$

假设 A,B 是通信双方,A 与 B 通过 TTP 交换消息。如果通信的一方 A 或者 B 能够证明 TTP 对消息 m 负责的话,那么它能够证明对方 B 或者 A 拥有这条消息。

R6. 电子证书规则

$$\frac{P \succ CA \rightarrow (K_q, Q)}{P \succ \xrightarrow{K_q} Q}$$

这条规用于解释电子证书机构(certification authority)在协议中的作用。假设 P 是一个主体,CA 是电子证书机构,CA 可以由 TTP 兼任。那么,如果 P 能够证明电子证书机构 CA 对某个公式(K_q,Q)负责,那么 P 能够证明 K_q 可用于验证主体 Q 的身份。

应用卿-周逻辑分析电子商务协议时，分4个步骤。前3个步骤是对协议可追究性的分析，第4个步骤是对协议公平性的分析：

(1) 列出初始拥有集合 O_A^0 和 O_B^0，它们是协议运行的初始状态。

(2) 列出POO和POR。在协议中，POO和POR是协议设计者明确定义了的。假定 POO$\in O_B$，POR$\in O_A$ 成立，并分析POO$\in O_B$，POR$\in O_A$ 是否可推导出协议满足可追究性目标。

(3) 验证协议结束时，POO$\in O_B$ 和POR$\in O_A$ 是否成立；

(4) 协议满足公平性等价于对于任何第i条可中断的协议语句，$POO \in O_B^{i-1}$ 当且仅当$POR \in O_A^{i-1}$。

概括起来，卿-周逻辑与Kailar逻辑相比较主要有以下三个优点：

(1) 卿-周逻辑能有效地分析公平性。在进行公平性分析时，它考虑了两个环境因素：主体是否诚实和通信信道是否可靠。

(2) 卿-周逻辑增加了密文理解规则，它能有效地分析“先加密后签名”的消息。

(3) 卿-周逻辑中的初始拥有集合只依赖于环境，不需要人为地引入初始假设，因而是一个更为严格的形式化分析方法。

4.6 Kailar 逻辑和卿-周逻辑的缺陷

Kailar 逻辑以及在 Kailar 逻辑基础上发展得来的卿-周逻辑虽然有很多优点，但是在分析重放攻击时却有一个共同的缺点，就是不能正确分析各方的责任性，它们存在一个机制性的缺陷，并且它们都不能分析协议的原子性，具体分析如下。

本节以 3.3 节介绍的 NewIBS 协议为例来分析 Kailar 逻辑和卿-周逻辑的缺陷。

用Kailar逻辑对NewIBS协议进行分析发现Kailar逻辑存在缺陷[38]，当发生重放攻击时，它不能正确分析各方的责任性。

在传递发票阶段协议的设计目标为：

(1) E CanProve (B从E的帐户中划拨了总数为TotalPrice的资金给S)

(2) S CanProve (B从E的帐户中划拨了总数为TotalPrice的资金给S)

(3) B CanProve (S请求从E的帐户中划拨了总数为TotalPrice的资金给S)

NewIBS所需要的初始化假设为：

S, E CanProve (K_E Authenticates E) (5)

B, E CanProve (K_S Authenticates S) (6)

S, E CanProve (K_B Authenticates B) (7)

(B Says invoice ') $\Rightarrow$ B从E的帐户中划拨了TotalPrice资金给S) (8)

（S Says invoice＇）⇒ S请求从E的帐户中划拨TotalPrice资金给S） （9）

协议分析过程如下：

由协议第（2）式和初始化假设（6）及签名规则可得如下关系：

B CanProve（S Says invoice＇） （10）

由（10）式和初始假设（8），可得协议设计目标（3）

由协议第（3）式和初始化假设（6）及签名规则可得如下关系：

S CanProve（B Says invoice＇） （11）

由（11）式和初始假设（7）可得协议设计目标（2）

由协议第（4）式和初始化假设（8）及签名规则可得如下关系：

E CanProve（S Says invoice＇） （12）

由（12）式和初始假设（7）可得协议设计目标（1）

这样，我们可用Kailar逻辑验证了NewIBS协议符合设计的责任性要求。

然而，当发生第三章所描述的重放攻击时，用Kailar逻辑进行分析，银行能够证明S仍然应该对第二张发票invoice＇负责，而实际上第二张发票invoice＇是由入侵者I重放过来的，S不应该再对它负责。这就导致了客户E支付双倍TotalPrice的货款，却只收到一次价值TotalPrice的服务，显然这样违反了电子商务协议的原子性。即Kailar逻辑不能分析协议是否能够抵御重放攻击。

用卿-周逻辑对NewIBS协议进行分析。当发生第三章所描述的重放攻击时，对于第（2）步中银行收到的第1张发票，S能对其负责。对于第（2＇）步中银行B收到的第2张发票，按照卿-周逻辑中的签名规则，我们可以得到 $B \triangleright S \rightarrow Invoice'$。而实际上第2张发票invoice＇是由入侵者I重放过来的，S不应该再对它负责。可以看出 $B \triangleright S \rightarrow Invoice'$ 只能说明S曾经能够对invoice＇负责，但并不能保证B收到invoice＇时S一定能够对invoice＇负责。在以后的分析中，卿-周逻辑不再检测消息invoice＇是否新鲜，从而导致B认为S应该对这两张发票负责，其后果是银行B两次向商家S转账，从而导致客户E必须支付双倍TotalPrice的货款，却只收到一次价值TotalPrice的服务，这样就违反了电子商务协议的原子性。

实际上，由签名规则所得到的 $B \triangleright S \rightarrow Invoice'$ 中的 $S \rightarrow Invoice'$ 只能确保主体S在发送invoice＇的时刻能够对invoice＇负责，但不能确保在B接收到

invoice ' 的时刻，S一定能够对invoice ' 负责，因为invoice ' 在信道传输过程中可能会被其他主体重放，而卿-周逻辑在分析过程中没有检测消息在信道传输过程中是否被其他主体重放，从而致使发生重放攻击时，卿-周逻辑不能正确分析各方的责任性。

4.7 小结

本章介绍了电子商务协议的诸多安全性质并归纳了电子商务协议的各种分析方法。由于Kailar逻辑和卿-周逻辑的简单性和有效性，使它成为目前对安全电子商务协议进行形式化分析的主要工具。但是我们通过分析发现当发生重放攻击时，它们不能正确分析各方的责任性，它们存在一个机制性的缺陷，并且不能分析协议的原子性。下一章我们将提出一种改进的逻辑分析方法来解决这个问题。

第五章　一种改进的逻辑分析方法

形式化分析是设计和验证一个安全的协议的常用办法。Kailar 逻辑和卿-周逻辑扩展了信念逻辑的分析范围，在形式化分析安全协议的正确性方面得到广泛应用。但是，它们存在机制上的缺陷，使得当发生重放攻击时，它们不能正确分析各方的责任性，并且不能分析协议的原子性。本章在卿-周逻辑的基础上对其进行了改进和扩充。改进的逻辑分析方法引入新鲜性机制，增加了两条关于主体的拥有集合的生成规则和三条协议的推理规则，对原逻辑中一条推理规则的使用附加了限制条件，并对关于可追究性的实现条件分三类进行了重新定义，最后增加了对原子性的分析。在本章的第三部分，我们给出了两个验证实例，和第四章的分析结果进行对比，这种改进的逻辑分析方法是有效的。

5.1 改进的逻辑分析方法的语法

本章介绍的这种逻辑分析方法是卿-周逻辑的改进、增强和扩充，可以同时用于分析安全电子商务协议的可追究性、公平性和原子性，并且弥补了上章所述两种逻辑机制上的缺陷，使得在发生重放攻击时能正确分析各方的责任性。在改进的逻辑分析方法中，每个主体在协议运行前拥有一个初始拥有集合，它由一些公式组成。当收到表示新鲜性的信息时，执行一个将消息标记为新鲜的动作，随着协议分析的进行，主体的拥有集合不断扩大，到协议运行结束时，每个主体拥有一个最终拥有集合。

协议的可追究性根据参与协议的主体是两方还是三方有不同的实现方法。

协议的公平性包含两层含义：首先，协议正常完成后，保证发送方收到POR且接收方收到POO；其次，如果协议异常终止，协议应保证通信双方都处于同等地位，任何一方都不占有优势。或者等价地说，消息接收方收到POO当且仅当消息发送方收到POR。在新的形式化分析方法中，当协议在任何一步异常终止时，验证协议是否满足公平性的方法是POO属于接收方的集合是否当且仅当POR属于发送方的拥有集合。

5.1.1 基本符号

现列举本文用到的基本符号：

A：消息发送方。

B：消息接收方。

M：消息，是A通过电子商务协议最终发给B的消息或电子货物。

|：“或”运算符，例如，A|B表示主体A或者B。

P：主体变量，表示主体A或者B之一，但不同于Q。

Q：主体变量，表示主体A或者B之一，但不同于P。

TTP：可信任第三方(trusted third party)。

CA：电子证书权威，负责为主体颁发电子证书，可以由TTP担任。

K_a：A的公开密钥，用于验证A的数字签名。K_a^{-1}是与K_a对应的A的私有密钥。

k_a：对称密钥体制中A的密钥。

k，K：会话密钥。

K_{ab}：A与B的共享密钥。

$(x)_K$：公式x用密钥K加密后的密文。

X in M：x是M中一个或几个可被理解的域，它的含义是由协议设计者明确定义的。可被理解的域通常是明文或者主体拥有密钥的加密域。

P∋x：主体P拥有公式或消息x。

P|~x：主体P能够证明公式或者消息x。

P→x：主体P对公式或者消息x负有责任。

$P \succ_{ftp} x$：主体P通过ftp方式获得消息x。

#x：消息x是新鲜的。

N_a：主体A表示新鲜性的一个临时值。

LINK（N_a）：用于联系一个响应与一个请求。当银行Bank或可信第三方TTP收到主体A的临时值N_a时，将公式LINK（N_a）加入到自己的拥有集合中。

$\xrightarrow{K_P} P$：密钥K_P可以用于验证主体P的身份。

(x, y)：由公式 x 和公式 y 组合而成的公式。

5.1.2 概念和定义

协议运行于一个分布式环境中，这个环境包含 3 个主体：发送方 A、接收方 B 和可信任第三方 TTP 或银行 Bank，其中 TTP 或 Bank 可以是一个或多个主体。在这个环境中，A 和 B 之间可以直接通信，或者通过 TTP 或 Bank 进行转发。环境是协议运行的具体环境的抽象，它只包含协议设计者和协议分析者考虑的因素，而屏蔽了其他因素。在本文中，环境包含主体是否诚实和通信信道是否可靠这两方面的因素。本文总假设 A 和 B 是不诚实的，TTP 和 Bank 是诚实公正的。通信信道可以是可靠的，也可以是不可靠的。

协议是一个分布式算法。它是由有限个协议语句组成的有序集，每个协议语句定义了主体在这一轮中应接收和发送什么消息。每条协议语句都是以下三种形式之一：

P→Q| TTP| Bank:M——表示主体 P 向主体 Q 或者 TTP 或者 Bank 发送消息 M。

TTP| Bank→P:M——表示主体 TTP 或 Bank 向主体 P 发送消息 M。

P←→TTP| Bank:M——表示主体 P 通过一次或多次 ftp 操作[28]从主体 TTP 或 Bank 取得消息 M。这一基于 ftp 的方法是由 ZhouJianying 和 DieterGollman 提出的[40]。即在通信信道不可靠的条件下，主体通过多次向 TTP 进行 ftp 操作获取他所需要的消息，以弥补通信信道不可靠的不足。

假设协议由 n 条协议语句组成。在协议开始之前，主体 P 的初始拥有集合记为 O_p^0，它包含环境分配给 P 的密钥和 P 能证明的公式。当协议的第 i(1≤i≤n)条语句执行完毕以后，主体 P 的拥有集合记为 O_p^i。当协议经过 n 步运行结束时，用 O_p 记 P 的最终拥有集合，$O_p=O_p^n$。

O_p^i 按如下规则递归生成：

(1)如果协议的第 i 条语句为 P→Q: M，不妨设 M=($\{M'\}_{K'}$, $\{M''\}_{K''}$, ...)，其中 $\{M'\}_{K'}$, $\{M''\}_{K''} \notin O_p^{i-1}$, $K' \in O_p^{i-1}$, $K'' \in O_p^{i-1}$，即 M 由若干个不在 O_p^{i-1} 中出现的加密消息如 $\{M'\}_{K'}$, $\{M''\}_{K''}$（它们的加密密钥 K′，K″ 在 O_p^{i-1} 中出现）和一

些其他消息复合而成，那么$O_p^i=O_p^{i-1}\cup\{M',M'',M\}$。

(2)如果第 i 条协议语句为 Q→P: M 或者 P←→TTP| Bank: M，那么$O_p^i=O_p^{i-1}\cup\{M\}$。

(3)如果第 i 条协议语句为 Q→TTP| Bank: M，或者 TTP| Bank→Q: M，或者 Q←→TTP: M，那么$O_p^i=O_p^{i-1}$。

(4)如果$(x,y)\in O_p^i$，那么$x\in O_p^i$且$y\in O_p^i$。反之，如果$x\in O_p^i$且$y\in O_p^i$，那么$(x,y)\in O_p^i$。

(5)如果$\{x\}_K\in O_p^i$且$K\in O_p^i$，那么$x\in O_p^i$。反之，如果$x\in O_p^i$且$K\in O_p^i$，那么$\{x\}_K\in O_p^i$。

(6)如果协议的第 i 条语句为 P→Q: $\{M\}_K$，其中$\{M\}_K\notin O_Q^{i-1}$，$\tilde{K}\in O_Q^{i-1}$，在这里，我们用$\tilde{K}$表示 K 的对偶密钥。如果 K 表示对称密钥，则$\tilde{K}$=K；如果 K 表示公钥密钥，则$\tilde{K}$就是其对应的公钥或者是私钥。那么$O_Q^i=O_Q^{i-1}\cup\{M\}\cup\{\{M\}_K\}$。

(7)如果协议的第 i 条语句为 P→TTP| Bank: $\{M\}_K$，其中$\{M\}_K\notin O_{TTP|Bank}^{i-1}$，对偶密钥$\tilde{K}\in O_{TTP|Bank}^{i-1}$，并且 M 中包含表示消息新鲜性的临时值 N_a。如果 LINK(N_a)$\notin O_{TTP|Bank}^{i-1}$，那么$O_{TTP|Bank}^i=O_{TTP|Bank}^{i-1}\cup\{\{M\}_K\}\cup\{\#M\}\cup\{LINK(N_a)\}$；否则$O_{TTP|Bank}^i=O_{TTP|Bank}^{i-1}\cup\{M\}-\{\#M\}$。

可追究性是指参与通信的双方均能向第三方证明对方对某个消息负有责任。在这个改进的形式化逻辑方法中，我们对协议的可追究性分为三类进行了重新定义。我们用记号 P→x 表示主体 P 对公式 x 负有责任。

（一）在没有第三方参与的协议中，可追究性是这样达到的：

(1)发送方非否认是由 A 将 POO(proof-of-origin)通过环境传送给 B 来达到的。POO 是协议设计者定义的一个公式，它包含使 A 不可抵赖的证据。这个公式由 A 产生，或者由 A 和 TTP 共同产生，通过环境最终传送给 B，并且由$POO\in O_B$可

以推导出 B$\triangleright$ A$\rightarrow$m 。

(2)接收方非否认是由 B 将 POR(proof-of-receipt)通过环境传送给 A 来达到的。POR 是协议设计者定义的一个公式,它包含使 B 不可抵赖的证据。这个公式由B产生,或者由B和TTP共同产生,通过环境最终传送给A,并且由POR$\in O_A$可以推导出 A$\triangleright$ B$\rightarrow$m 。

(二) 假设发送方 A 通过环境将消息或电子货物 m 传送给接收方 B,则可追究性是这样达到的:

(1)发送方非否认是由A将POO(proof-of-origin)通过环境传送给B来达到的。POO 是协议设计者定义的一个公式,它包含使 A 不可抵赖的证据。这个公式由 A 产生,或者由 A 和 TTP 共同产生,通过环境最终传送给 B,并且由 POO$\in O_B$可以推导出 B$\triangleright$ A$\rightarrow$m 。

(2)接收方非否认是由 B 将 POR(proof-of-receipt)通过环境传送给 A 来达到的。POR 是协议设计者定义的一个公式,它包含使 B 不可抵赖的证据。这个公式由B产生,或者由B和TTP共同产生,通过环境最终传送给A,并且由POR$\in O_A$可以推导出 A$\triangleright$ B$\rightarrow$m 。

(3)可信第三方 TTP 必须能够证明发货请求是由接收方提出,即 TTP$\triangleright$ B$\rightarrow$m,以免发生重放攻击时主体责任性不能得到保证。

(三) 假设发送方 A 和接收方 B 通过 Bank 进行转帐,则可追究性是这样达到的:

(1)发送方非否认是由 A 或 Bank 将 POO 通过环境传送给 B 来达到的。POO 是协议设计者定义的一个公式,它包含使 A 不可抵赖的证据。这个公式由 A 和 Bank 共同产生,通过环境最终传送给 B,并且由 POO$\in O_B$可以推导出 B$\triangleright$ Bank$\rightarrow$ invoice。

(2)接收方非否认是由 B 或 Bank 将 POR 通过环境传送给 A 来达到的。POR 是协议设计者定义的一个公式,它包含使 B 不可抵赖的证据。这个公式由 B 和 Bank 共同产生,通过环境最终传送给 A,并且由 POR$\in O_A$可以推导出 A$\triangleright$ Bank$\rightarrow$ invoice。

(3)银行 Bank 必须能够证明支付收据是由发送票据方提出,即 Bank$\triangleright$ A$\rightarrow$

invoice，以免发生重放攻击时主体责任性不能得到保证。

原子性分为三级。货币原子性是指电子商务交易发生前后资金守恒，顾客货币的减少量等于商家货币的增加。商品原子性则要求协议一定满足货币原子性且保证顾客收到商品当且仅当对应商家获得付款。确认发送原子性则要求协议首先满足货币原子性和商品原子性，其次，需对顾客从商家购买的商品和商家付给顾客的产品分别确认，如有争议，拥有仲裁证据证实交易商品的内容。

协议语句的一个重要属性是可中断性。如果一个协议语句受环境影响，可能未被执行或未被正确执行，那么这条语句是可中断的。按照可中断性，协议语句分为以下3类：

(1)第1类协议语句A|B→B|A|TTP| Bank :M是可中断的。因为A或B是不诚实的，他可能因为对自己有利而不执行这条协议语句。

(2)在信道可靠的情况下，第2类协议语句TTP| Bank→A|B:M是不可中断的。因为TTP和Bank是诚实的，他肯定会执行这条协议语句，因为TTP或Bank发送的消息会被A或B正确地接收到。在信道不可靠的情况下，TTP和Bank发送的消息有可能会发生丢失，第2类协议语句是可中断的。

(3)第三类语句A|B←→TTP| Bank:M在信道可靠或信道不可靠的条件下都是不可中断的。因为TTP和Bank是诚实的，他使M可被ftp操作取得。A或B可以通过这一操作获得对自己有用的信息，他不会放弃这一操作。即使在信道不可靠的条件下，A或B仍可通过多次ftp操作来取得M。

因此，协议的公平性是指，协议除了满足可追究性外，还满足以下条件："当协议的执行在任何第i条语句中断时，$POO \in O_B^{i-1}$ 当且仅当 $POR \in O_A^{i-1}$"。协议的执行在哪些步可能异常终止要取决于环境。

5.1.3 推理规则

R1.签名规则

$$\frac{P \ni \{x\}_{K_q^{-1}}, P \succ \xrightarrow{K_q} Q}{P \succ (Q \rightarrow x)}$$

如果主体P拥有用 K_q^{-1} 签过名的公式x，并且P能够证明 K_q 可用于验证主体

Q 的身份，那么 P 可以证明主体 Q 对公式 x 负有责任。在这个改进的逻辑中我们对这个公式引入一个限制条件，就是主体 P 是除 TTP 或者 Bank 之外的任何主体，因为对 TTP 和 Bank 的责任性分析应该有更加严格的条件。

R2. 连接规则

$$\frac{P \succ Q \rightarrow (x,y)}{P \succ Q \rightarrow x; P \succ Q \rightarrow y}$$

$$\frac{P \succ Q \rightarrow x; P \succ Q \rightarrow y}{P \succ Q \rightarrow (x,y)}$$

$$\frac{P \succ x; P \succ y}{P \succ (x,y)}$$

$$\frac{P \succ (x,y)}{P \succ x; P \succ y}$$

如果主体 P 能够证明主体 Q 对某一公式的连接或并负有责任，那么 P 能够证明 Q 对这个公式的各个部分负有责任。反之，P 能够证明 Q 对几个公式负有责任，那么 P 能够证明 Q 对这几个公式的连接或并负有责任。

R3. 密文理解规则

$$\frac{P \succ Q \rightarrow \{x\}_K, P \succ Q \ni K}{P \succ Q \rightarrow x}$$

这条规则用于理解签过名的加密消息，以弥补 Kailar 逻辑的不足。如果主体 P 能够证明主体 Q 对某个用 K 加密过的公式 x 负有责任，并且 P 能够证明 Q 拥有加密密钥 K(也是解密密钥)，那么 P 能够证明 Q 对 x 负有责任。

R4. 拥有规则。这条规则主要包括三条分规则，最后一条分规则是新引入的：

$$\frac{x \in O_p^0}{\forall Q, Q \succ P \ni x}$$

如果 P 的初始拥有集合中包含某个公式 x，那么任何一个其他的主体 Q 都能证明 P 拥有这个公式 x。

$$\frac{P \succ Q \rightarrow x}{P \succ Q \ni x}$$

文献[41]提出了这条规则，若P能证明Q对消息x负责，那么他能证明Q拥有x。

$$\frac{P \ni x}{x \in O},$$

若主体 P 拥有某个公式 x，则公式 x 一定在 P 的拥有集合中。

R5. 传递规则

$$\frac{A \succ TTP \rightarrow x}{A \succ B \ni x}$$

$$\frac{B \succ TTP \rightarrow x}{B \succ A \ni x}$$

假设 A, B 是通信双方，A 与 B 通过 TTP 交换消息。如果通信的一方 A 或者 B 能够证明 TTP 对消息 x 负责的话，那么它能够证明对方 B 或者 A 拥有这条消息。

$$\frac{A \succ B \rightarrow x, B \succ C \rightarrow x}{A \succ C \rightarrow x}$$

文献[41]提出了这条规则，如果主体A能证明主体B对消息x负责，同时B能证明C对x负责，则A能证明C对x负责。

R6. ftp 获取规则

$$\frac{P \succ_{ftp} x}{P \ni x}$$

文献[41]介绍了这条规则，若P通过ftp方式获得消息x，则P一定能得到x。

R7. 子消息新鲜性规则

$$\frac{\#x, x_1 \in x, x_2 \in x}{\#x_1, \#x_2}$$

这条规则是新引入的，如果消息 x 是新鲜的，且 x_1 和 x_2 是消息 x 的子消息，则子消息 x_1 和 x_2 也是新鲜的。这个规则反映了下述事实：如果一个消息是新鲜的，则该消息的任何子消息都是新鲜的。

R8.Bank 规则和 TTP 规则

$$\frac{P \ni \{x\}_{K_q^{-1}}, \#x, P \xrightarrow{K_q} Q}{P \succ (Q \rightarrow x)}$$

这条规则是新引入的，用于分析新鲜性。因为和银行 Bank 或 TTP 之间传送的消息一般都牵涉到转账或发货之类重要的信息，所以对它们引入新鲜性检测机制。只有当主体 P 为银行 Bank 或 TTP 时才能使用此规则。如果主体 P 拥有用 K_q^{-1}

签过名的消息 x,且 x 是新鲜的，并且 P 能够证明 K_q 可用于验证主体 Q 的身份，那么 P 可以证明主体 Q 对消息 x 负有责任。

R9. 电子证书规则

$$\frac{P \succ CA \rightarrow (K_q, Q)}{P \succ \xrightarrow{K_q} Q}$$

这条规用于解释电子证书机构(certification authority)在协议中的作用。假设 P 是一个主体,CA 是电子证书机构,CA 可以由 TTP 兼任。那么,如果 P 能够证明电子证书机构 CA 对某个公式(K_q,Q)负责,那么 P 能够证明 K_q 可用于验证主体 Q 的身份。

5.2 协议分析步骤

改进的形式化方法分析协议分为以下5个步骤.前4个步骤是对协议可追究性和公平性的分析,第5步是对协议原子性的分析。

(1) 列出初始拥有集合 O_A^0 和 O_B^0，它们是协议运行的初始状态。

(2) 列出POO和POR。在协议中，POO和POR是协议设计者明确定义了的。假定 POO$\in O_B$,POR$\in O_A$ 成立，并分析POO$\in O_B$，POR$\in O_A$ 是否可推导出协议满足可追究性目标。

(3) 验证协议结束时，POO$\in O_B$ 和POR$\in O_A$ 是否成立以及TTP$\succ$B$\rightarrow$m或者 Bank$\succ$A$\rightarrow$invoice是否成立。

(4) 协议满足公平性等价于对于任何第i条可中断的协议语句，POO$\in O_B^{i-1}$ 当且仅当POR$\in O_A^{i-1}$。

(5) 验证协议结束时是否满足原子性目标。列出原子性目标 GA_1 和 GA_2，在协议的每步执行中，均判断是否满足原子性目标；若满足，检查交易双方终态的消息集，若双方得到交换的信息，则满足原子性。

5.3 验证实例

5.3.1 IBS 协议的逻辑验证

本节以IBS协议为例分析协议性质。

首先列举初始化拥有集合：

$O_E^0=\{K_e,K_e^{-1},K_s,K_b\}, O_S^0=\{K_s,K_s^{-1},K_e,K_b\}, O_B^0=\{K_e,K_b^{-1},K_s,K_b\}$,

$S\succ(\xrightarrow{K_e}E,\xrightarrow{K_b}B), E\succ(\xrightarrow{K_s}S,\xrightarrow{K_b}B), B\succ(\xrightarrow{K_e}E,\xrightarrow{K_s}S)$。

在确定价格协议中：

（1）列举发方非否认证据和收方非否认证据如下：

$POO=\{Price\ Request\}_{K_e^{-1}}$, $POR=\{Price\}_{K_s^{-1}}$

现在假定$POO\in O_S$,即$\{Price\ Request\}_{K_e^{-1}}\in O_S$，则$S\ni\{Price\ Request\}_{K_e^{-1}}$成立。

由$S\ni\{Price\ Request\}_{K_e^{-1}}$与初始化假设$S\succ\xrightarrow{K_e}E$，利用签名规则得：

$S\succ E\rightarrow$Price Request。同理可证$E\succ s\rightarrow Price$。

因此，协议设计者对POO 和POR 的设计满足可追究性。

（2）这一步将验证当协议运行结束时，是否可以确保E和S取得相应的证据。

由于$O_E^2=O_E^1\cup\{\{Price\}_{K_s^{-1}}\}$，$\{Price\}_{K_s^{-1}}\in O_E^2\in O_E$，即$POR\in O_E$。

当协议运行结束时，消息发送者E可以取得POR。类似地可以验证当协议运行结束时，消息接收者S可以取得POO。

因此确定价格协议满足可追究性。

（3）在信道不可靠的情况下，协议语句（1）与（2）是可中断的。协议是公平的等价于下面的命题成立：

$POO\in O_S^i$当且仅当$POR\in O_E^i$（i=0, 1, 2）。

$O_E^1=O_E^0\cup\{\{Price\ Request\}_{K_e^{-1}}\}$，$O_S^1=O_S^0\cup\{\{Price\ Request\}_{K_e^{-1}}\}$。

由于O_E^1中不含有公式$\{Price\}_{K_s^{-1}}$，因此$POR\in O_E^1$不成立。然而O_S^1中含有公式$\{Price\ Request\}_{K_e^{-1}}$，因此$POO\in O_S^1$成立。

以上证明了在信道不可靠的情况下，确定价格协议是非公平的。

在提供服务协议中：

（4）列举发方非否认证据和收方非否认证据。

POO=（$\{\{Price\}_{K_t^{-1}}, Price\}_{K_t^{-1}}$，$\{ServiceAcknowledge\}_{K_t^{-1}}$），POR=$\{Service\}_{K_t^{-1}}$。

假定POO$\in O_S$ 成立，则：

（$\{\{Price\}_{K_t^{-1}}, Price\}_{K_t^{-1}}$，$\{ServiceAcknowledge\}_{K_t^{-1}}$）$\in O_S$

即$O_S \ni \{\{Price\}_{K_t^{-1}}, Price\}_{K_t^{-1}}$与$O_S \ni \{ServiceAcknowledge\}_{K_t^{-1}}$。

由初始化假设$S \succ \xrightarrow{K_t} E$和签名规则得：

$S \succ E \rightarrow$（$\{Price\}_{K_t^{-1}}$，Price）与$S \succ E \rightarrow$\{Service Acknowledge\}

再由连接规则得：

$S \succ E \rightarrow$（$\{\{Price\}_{K_t^{-1}}$，Price\}，\{Service Acknowledge\}）

假定POR$\in O_E$成立，则$\{Service\}_{K_t^{-1}} \in O_E$。由初始化假设$E \succ \xrightarrow{K_t} S$和签名规则得：$E \succ s \rightarrow Service$。因此协议设计者对POO 和POR 的设计满足可追究性。

（5）这一步将验证当协议运行结束时，是否可以确保E和S取得相应的证据。

由于$O_S^7 = O_S^6 = O_S^5 \cup \{\{ServiceAcknowledge\}_{K_t^{-1}}\}$，且$\{\{Price\}_{K_t^{-1}}, Price\}_{K_t^{-1}} \in O_S^3 \subset O_S$，即POO$\in O_S$。当协议运行结束时消息接收者可以取得POO。类似地可以验证当协议运行结束时，消息发送者可以取得POR。

因此提供服务协议满足可追究性。

（6）在信道不可靠的情况下，协议语句（3），（4），（5），（6），（7）是可中断的。协议是公平的等价于下面的命题成立：

POO$\in O_S^i$当且仅当POR$\in O_E^i$，i=0，3，4，5，6。

由于$O_S^5 = O_S^0 \cup \{\{\{Price\}_{K_t^{-1}}, Price\}_{K_t^{-1}}, \{Service\}_{K_t^{-1}}\}$且$\{ServiceAcknowledge\}_{K_t^{-1}} \in O_S^5$不成立，因此POO$\in O_S^5$不成立。而$\{Service\}_{K_t^{-1}} \in O_E^5$，即POR$\in O_E^5$成立。

以上证明了在信道不可靠的情况下，提供服务协议是非公平的。

在传递发票协议中：

（7）列举发方非否认证据和收方非否认证据。

POO=$\{\{Invoice\}_{K_s}\}_{K_b^{-1}}$，POR=$\{\{Invoice\}_{K_s}\}_{K_b^{-1}}$。假定POR$\in O_E$ 成立，即 E$\ni \{\{Invoice\}_{K_s}\}_{K_b^{-1}}$，由初始化假设和签名规则得E$\succ B \rightarrow \{Invoice\}_{K_s}$。

又B$\ni K_s$，由密文理解规则得E$\succ$B$\rightarrow$Invoice，因此POR 满足可追究性。

假定POO$\in O_S$，即$\{\{Invoice\}_{K_s}\}_{K_b^{-1}} \in O_S$。由初始化假设S$\succ \xrightarrow{K_b} B$和由签名规则得：S$\succ B \rightarrow \{Invoice\}_{K_s}$。又B$\ni K_s$，由密文理解规则得S$\succ$B$\rightarrow Invoice$，因此POO满足可追究性。

（8）这一步将验证当协议运行结束时，是否可以确保E与S取得相应的证据。

由于$O_S^{11} = O_S^{10} = O_S^9 \cup \{\{\{Invoice\}_{K_s}\}_{K_b^{-1}}\}$，$\{\{Invoice\}_{K_s}\}_{K_b^{-1}} \in O_S$，即 POO$\in O_S$。当协议运行结束时，消息接收者可以取得POO。类似地可以验证当协议运行结束时，消息发送者可以取得POR。

协议的第（9）条语句为$S \rightarrow B:\{\{Invoice\}_{K_b}\}_{K_s^{-1}}$，$Invoice$中有表示消息新鲜性的临时值$N_a$，即表示交易的序列号ID，根据$O_P^i$生成规则（7），$O_B^9 = O_B^0 \cup \{\{\{Invoice\}_{K_b}\}_{K_s^{-1}}\} \cup \{\#\{Invoice\}_{K_b}\} \cup \{$ LINK（N_a） $\}$，即B$\ni \{\{Invoice\}_{K_b}\}_{K_s^{-1}}$由初始化假设B$\succ \xrightarrow{K_s} S$和Bank规则得：B$\succ S \rightarrow \{Invoice\}_{K_b}$。

又S$\ni K_b$，由密文理解规则得B$\succ$S$\rightarrow Invoice$。

因此传递发票协议满足可追究性。

（9）在信道不可靠的情况下，（8）、（9）语句是可中断的。协议的公平性等价于下面的命题成立：

POO$\in O_S^i$当且仅当POR$\in O_E^i$（i=8，9）。

$O_S^8 = O_S^7 \cup \{\{Invoice\,Request\}_{K_s^{-1}}\}$，而$\{\{Invoice\}_{K_s}\}_{K_b^{-1}} \notin O_S^8$，POO$\in O_S^8$因此不成立。$O_S^9 = O_S^8 \cup \{\{\{Invoice\}_{K_b}\}_{K_s^{-1}}\}$，而$\{\{Invoice\}_{K_s}\}_{K_b^{-1}} \notin O_S^9$，所以，POO$\in O_S^9$也不成立。同理可证POR$\in O_E^i$不成立。

因此在信道不可靠的情况下，传递发票协议是公平的。

综上所述IBS 协议整体上满足可追究性，但是不满足公平性。

接下来，我们来分析协议的原子性。

首先分析货币原子性目标。

在协议执行的第九步中，货币从顾客E通过银行流至服务提供方S。由于银行是可信的，因此货币在协议执行过程中保持守恒，故协议满足货币原子性。

下面分析商品原子性目标。

在该协议中，商品原子性目标表示为：GA_1= Service$\notin O_E^i$ $\wedge$InvoiceRequest$\notin O_S^i$ ，GA_2= Service$\in O_E^i$ $\wedge$InvoiceRequest$\in O_S^i$。

当协议语句（1）执行后，$O_E^1 = O_E^0 \cup \{\{PriceRequest\}_{K_t^{-1}}\}$，$O_S^1 = O_S^0 \cup \{\{PriceRequest\}_{K_t^{-1}}\}$。

从而，Service$\notin O_E^i$ $\wedge$InvoiceRequest$\notin O_S^i$，故此时满足商品原子性。

同样地，当协议语句（2）执行后，有Service$\notin O_E^i$ $\wedge$InvoiceRequest$\notin O_S^i$；当协议语句（3）执行后，有Service$\notin O_E^i$ $\wedge$InvoiceRequest$\notin O_S^i$；当协议语句（4）执行后，仍然有Service$\notin O_E^i$ $\wedge$InvoiceRequest$\notin O_S^i$。

但是，当协议语句（5）执行后，$O_S^5 = O_S^0 \cup \{\{\{Price\}_{K_t^{-1}}, Price\}_{K_t^{-1}}, \{Service\}_{K_t^{-1}}\}$，可见InvoiceRequest $\in O_S^5$不成立，然而$\{Service\}_{K_t^{-1}} \in O_E^5$，所以有 Service$\in O_E^5$ $\wedge$InvoiceRequest$\notin O_S^5$；从而可知协议不满足商品原子性。

综上所述IBS协议不满足原子性目标。

5.3.2 NewIBS 协议的逻辑验证

下面，我们用这种改进的形式化方法分析NewIBS协议。

（1）列举发方非否认证据和收方非否认证据。

POO=$\{\{Invoice'\}_{K_t}\}_{K_b^{-1}}$，POR=$\{\{Invoice'\}_{K_t}\}_{K_b^{-1}}$。假定POR$\in O_E$ 成立，即 E$\ni \{\{Invoice'\}_{K_t}\}_{K_b^{-1}}$，由初始化假设和签名规则得 $E \succ B \rightarrow \{Invoice'\}_{K_t}$。

又B∋ K_e，由密文理解规则得E≻B→ *Invoice'*，因此POR 满足可追究性。

假定POO∈ O_S，即 $\{\{Invoice'\}_{K_s}\}_{K_b^{-1}} \in O_S$。由初始化假设S≻ $\xrightarrow{K_b} B$ 和由签名规则得：S≻ $B \rightarrow \{Invoice'\}_{K_s}$ 。又B∋ K_s，由密文理解规则得S≻B→ *Invoice'*，因此POO满足可追究性。

（2）这一步将验证当协议运行结束时，是否可以确保E与S取得相应的证据。

由于 $O_S^4 = O_S^3 = O_S^2 \cup \{\{\{Invoice'\}_{K_s}\}_{K_b^{-1}}\}$，$\{\{Invoice'\}_{K_s}\}_{K_b^{-1}} \in O_S$，即 POO∈ O_S。当协议运行结束时，消息接收者可以取得POO。类似地可以验证当协议运行结束时，消息发送者可以取得POR。

协议的第（2）条语句为 $S \rightarrow B:\{\{Invoice'\}_{K_b}\}_{K_s^{-1}}$，*Invoice'* 中没有表示消息新鲜性的临时值N_a，即表示交易的序列号ID，根据 O_P^i 生成规则（6），$O_B^2 = O_B^0 \cup \{\{\{Invoice'\}_{K_b}\}_{K_s^{-1}}\} \cup \{\{Invoice'\}_{K_b}\}$，没有表示新鲜的消息，因此不能用Bank规则，也就无法得出B≻S→ *Invoice'*。

因此NewIBS协议不满足可追究性。

因为公平性和原子性要求协议首先得满足可追究性，所以NewIBS协议不满足公平性和原子性。

综上所述，NewIBS协议不满足可追究性、公平性和原子性。

这种扩展和改进的逻辑分析方法发现和验证了Kailar逻辑和卿-周逻辑针对责任性分析的一个错误，实验结果说明了这种逻辑分析方法是有效的。

5.4 小结

前人在安全协议的逻辑验证方面做了许多重要的工作，Kailar逻辑扩展了信念逻辑分析的范围，作为一种“可证明性”逻辑它适于分析电子商务协议的可追究性。卿-周逻辑是Kailar逻辑的改进、增强和扩充，可以同时用于分析安全电子商务协议的可追究性和公平性，但它们都有缺陷。本章在卿-周逻辑的基础上对它进行了扩充和改进，并详细介绍了这种扩充和改进的逻辑方法的语法和对协议分析的步骤，最后给出了两个验证实例。希望本章对协议属性的分析方法，能够在电子商务协议的研究方面提供一点帮助。

第六章 总结与展望

电子商务协议是电子商务的构成框架，它为高层应用提供了技术基础。电子商务协议规定了电子商务的具体流程、消息格式以及运用的密码技术，从而使得实现的电子商务能满足相应的性质。然而，如何在具体的电子商务实现以前验证其是否具有特定的安全性质以降低成本并让用户放心，则是许多研究者正在研究的课题。从逻辑角度出发验证电子商务协议便是一种比较方便实用的方式。形式化逻辑推理可以在安全协议实现之前，对其进行逻辑分析，即进行协议分析，就像证明数学命题一样，逻辑严密，但这种方法还很不完善。

本文首先以研究电子商务安全出发，对电子商务协议的基本知识及常见攻击进行了介绍，在此基础上模拟了两个对协议的攻击并对其中一个提出了改进方案；电子商务协议的设计与分析是当前研究的热点，本文明确了电子商务协议的要求或者各种属性，说明了 Kailar 逻辑和卿-周逻辑分析协议的方法、步骤并分析了其缺陷；在此基础上，作者尝试着提出了一种分析电子商务协议的改进的逻辑分析方法，并用它来分析了两个电子商务协议，分析结果表明此逻辑更有效并且弥补了 Kailar 逻辑和卿-周逻辑的缺陷。

待解决的问题

关于电子商务协议的逻辑分析方法的研究还有很多值得研究的问题，这里列出一些：

1. 电子商务协议的设计及实现；

2. 在语法分析的同时进行语义分析；

3. 逻辑语言的改进与完善，使其随着电子商务安全协议的发展有方便的扩展性；

4. 电子商务协议中密码技术的设计和使用。

致谢

在本文完成之际，我要衷心感谢我的导师周清雷教授三年来对我的帮助和教育。他以战略家的眼光给我的研究生三年的学习生活进行了方向性的指导。为师者，传道、授业解惑。周老师严谨的治学态度、渊博的学识、忘我的工作精神，给了我有力的鞭策和激励，他不仅让我在研究生阶段学到了大量的专业知识，树立了正确的治学态度，而且让我学会了宽厚待人和谦逊、乐观、积极、热情的生活态度。这一切都使我受益终生。

深深感谢信息工程学院各位给我授课及给予我帮助的老师们，正是由于他们的悉心教诲，让我学到了丰富的专业知识。

同时感谢和我一起度过三年的每一位同学，感谢王峰、周颜、赵琳、马中良、文娟娟、吕静、张莉，你们对我学习、生活等各方面给予了很好的帮助与关爱。有了你们我的生活才更加的丰富多彩，与你们在一起的日子将是我记忆中的珍宝。

感谢我的家人，我的一切都与您们的支持与关爱是分不开的。最后，谨向百忙中抽出时间来参加我的论文答辩的各位专家表示衷心的感谢。

参考文献

1. 周龙骧. 电子商务协议研究综述. 软件学报, 2001, 12(7): 1015-1031.

2. Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In: itshape Proceedings of TACAS, LNCS 1055, Springer-Verlag, 1996, 147-166.

3. 卿斯汉. 安全协议20年研究进展. 软件学报, 2003, 14(10): 1740-1752.

4. Meadows C. The NRL protocol analyzer: An overview. Journal of Logic Programming, 1996, 26(2): 113-131.

5. Paulson LC. The inductive approach to verifying cryptographic protocols. Journal of Computer Security, 1998, (6): 85-128.

6. Giampaolo Bella, Fabio Massacci, and Lawrence C. Paulson. Verifying the SET registration protocols. IEEE Journal on Selected Areas in Communications, 2003, 21(1): 77–87.

7. Ray I, Ray I. Failure analysis of an e-commerce protocol using model checking. In: Proceedings of the 2nd International Workshop on Advanced Issues of E-Commerce and Web-based Information Systems, San Jose: CA, June 2000, 176-183.

8. Xu S, Yung M, Zhang G, Zhu H. Money conservation via atomicity in fair offline e-cash. In: Proceedings of the 2nd Int. Workshop of Information Security, Lecture Notes in Computer Science, Springer-Verlag, 1999, 14-31.

9. John C. Mitchell, Mark Mitchell, Ulrich Stern. Automated analysis of cryptographic protocols using Murphi. In: proceedings of IEEE Symposium on Security and Privacy, 1997.

10. 董荣胜,郭云川,古天龙. 一种电子商务协议原子性的模型检验分析方法.计算机科学, 2005, 32(4): 184-186.

11. Zhang Z, Ma H. Modeling and Verification of a Simple Network Payment Protocol. In: Proceedings of ICCT, 2003, 1670-1673.

12. Gregorio Díaz, Fernando Cuartero, Valentín Valero Ruiz, Fernando L. Pelayo. Automatic verification of the TLS handshake protocol. SAC 2004, 789-794.

13. Burrows M, Abadi M, Needham R. A logic of authentication. Research report 39, digital systems research center. February 1989. In: Proceedings of the Royal Society of London A, 1989, 426: 233-271.

14. Oorschot PV.An Alternate Explanation of two BAN-Login "Failures" In Advances in Cryptology-EUROCRPT 93，Vol 765 of Lecture Notes in Computer Science[c]. Berlin: Springer-Verlag,1993.443-447.

15. Boyd c. Man Wenbo. On a Limitation of BAN Login. In Advances in Crypto-EUROCRYPT 93, Vol 765 of Lecture Notes in Computer Science.Berlin: Springer-Verlag,1993.240-247.

16. 张玉清，李继红，肖国镇，密码协议分析工具——BAN逻辑及其缺陷，西安电子科技大学学报，1996，26（3）.

17. Syverson P F, van Oorschot P C. On unifying some cryptographic protocol. In: Proceedings of the IEEE 1994 Computer Society Symposium in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1994, 14-28.

18. Zhou J, Gollmann D. Towards verification of non-repudiation protocols. In: International Refinement Workshop and Formal Methods. Berlin: Springer-Verlag, 1998, 370-380.

19. Kailar R. Accountability in electronic commerce protocols. IEEE Transaction on Software Engineering, 1996, 22(5): 313-328.

20. 陈庆锋，白硕，王驹等，电子商务安全协议及其非单调动态逻辑验证. 软件学报，2001，11（2）：240-250.

21. 白硕, 隋立颖, 陈庆锋等. 安全协议的逻辑验证. 软件学报,2000, 11(2): 213-221.

22. 陈庆锋，王驹，白硕等，电子商务安全协议的逻辑验证. 软件学报,2000, 11(3): 346-362.

23. 周典萃, 卿斯汉, 周展飞. Kailar逻辑的缺陷. 软件学报, 1999, 10(12)：1238-1245.

24. 周典萃,卿斯汉,周展飞. 一种分析电子商务协议的新工具.软件学报,2001,12(9): 1318-1328.

25. 王彩芬,葛建华. 一种分析电子商务协议的新方法.计算机学报, 2004, 27(4): 507-515.

26. Boyd C， Mao W. On a limitation of BAN logic. In： Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science, Springer-Verlag, 1993, 240-247.

27. 卿斯汉. 安全协议. 2005,3, 第一版,351-352.

28. Postel J, Reynolds J. File transfer protocol RFC 959,1985。

29. Ray I, Ray I, Narasimhamurthi N. A fair-exchange protocol with automated dispute resolution. In: Proceedings of the 14th Annual IFIP WG 11.3 Working Conference on Database Security. The Netherlands: Schoorl, 2000, 27-38.

30. Frier A, Karlton P, Kocher P. The SSL 3.0 Protocol. Netscape Communication Corp, 1996.

31. http://www.setco.org/set_specifications.html.

32. Camp L J, Harkavy M, Tygar J D, Yee B. Anonymous Atomic Transactions. In: Proceedings of the 2nd USENI Workshop on Electronic Commerce, 1996, 123-133.

33. Franklin M, Reiter M. Fair exchange with a semi-trusted third party. In: Proceedings of the 4th ACM conference on computer and communication security. Switzerland: ACM Press, 1997, 1-5.

34. O'Toole K R. The Internet billing server transaction protocol alternatives. IN I TR 1994 - 1, Carnegie Mellon University: Information Net working Institute. 1994

35. Robert H Deng, Li Gong ,Aurel A Lazar, WeiguoWang. Practical protocols for certified electronic mail〔J 〕. Journal of Network System Manager, 1996, 4 (3) : 279 ~ 297

36. A.J.Menezes,P.C.Oorschot,S.A.Vanstone.Handbook of Applied Cryptography. NewYork:CRC Press, 1997 .

37. M.Bellare, M.Fischlin, S.Goldwasser, S.Micali. Identification Protocols Secure against Reset Atacks. Advances in Cryptology EUROCRYPT2 001, International Conference on the Theory and Application of Cryptographic Techniques. Innsbruck, Austria,pages4 95-511,2001.

38.石曙东，李之棠.Kailar逻辑的缺陷及改进.计算机工程与设计，2004,25(6):853-883.

39. Tygar J D. Atomicity in electronic commerce. In: Proc of the 15th Annual ACM Symposium on Principles of Distributed Computing, 1996: 8-26.

40.Zhou,Jian-ying,Gollman,D.Afairnon-repudiationprotocol.In:Proceedings of the 1996 IEEE Symposiumon Securityand Privacy. Los Alamitos,CA: IEEE Computer Society Press,1996.55～61.

41.郭华.基于模型检测的电子商务协议形式化验证方法研究.郑州大学硕士研究生学位论文，2006年10月.

附录 1 攻读硕士期间发表和完成的论文

1. 席琳，赵东明. CMP协议的缺陷与改进. 微计算机信息. 2007，11.
2. 席琳，周清雷.CMP协议的改进与形式化分析. 计算机应用研究（增刊）.2007.9-11.