基于 ATL 的公平电子商务协议形式化分析

文静华[①②③] 李 祥[①] 张焕国[②] 梁 敏[③] 张 梅[③]

[①](贵州大学计算机软件与理论研究所 贵阳 550025)

[②](武汉大学计算机学院 武汉 430072)

[③](贵州财经学院信息学院 贵阳 550004)

摘 要：针对传统时序逻辑 LTL，CTL 及 CTL*等把协议看成封闭系统进行分析的缺点，Kremer 博士(2003)提出用一种基于博弈的 ATL(Alternating-time Temporal Logic)方法分析公平电子商务协议并对几个典型的协议进行了公平性等方面的形式化分析。本文讨论了 ATL 逻辑及其在电子商务协议形式化分析中的应用，进一步扩展了 Kremer 博士的方法，使之在考虑公平性等特性的同时能够分析协议的安全性。最后本文用新方法对 Zhou 等人(1999)提出的 ZDB 协议进行了严格的形式化分析，结果发现该协议在非保密通道下存在两个可能的攻击：保密信息泄露和重放攻击。

关键词：电子商务协议；公平性；安全性；形式化分析；ATL

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2007)04-0901-05

Formal Analysis of Fair E-Commerce Protocols Based on ATL

Wen Jing-Hua[①②③] Li Xiang[①] Zhang Huan-guo[②] Liang Min[③] Zhang Mei[③]

[①](*Institute of Software and Theory*, *Guizhou University*, *Guiyang* 550025, *China*)

[②](*School of Computer*, *Wuhan University*, *Wuhan* 430072, *China*)

[③](*Information Institute*, *Guizhou Financial Institute*, *Guiyang* 550004, *China*)

Abstract: Aiming at the shortcoming that traditional temporal logic such as LTL,CTL and CTL* regards protocols as close system to analyze, Dr Kremer(2003) proposes an ATL(Alternating-time Temporal Logic) logical method based on game to analyze fair E-commerce protocols, and analyses formally several typical protocols on their fairness and other properties. In this paper, ATL logical and its applications in formal analysis of E-commerce protocols are discussed, and Dr Kremer' approach is ulteriorly extended to analyze security of protocols besides fairness. Finally, the strict formal analysis is made for ZDB protocol(1999)proposed by Zhou *et al*. With this new method, as a result there exists 2 possible attacks in the ZDB protocol under non-secrecy channels: leakiness of secret information and reply attacks.

Key words: E-commerce protocols; Fairness; Security; Formal analysis; ATL

1 引言

电子商务协议是面向电子商务的密码协议，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，这类协议的基本属性包括安全性、保密性、完整性、可认证性、非否认性及公平性等[1]。与其它密码协议一样，电子商务协议的建模和形式化分析研究非常重要，对于已有成熟的密码协议分析和验证技术可以直接应用到电子商务协议中去。目前在各种电子商务协议形式化分析方法研究中，有影响的方法主要有BAN逻辑方法、Kailar逻辑方法、串空间方法、进程代数方法及基于时序逻辑的方法等[1–3]。其中，时序逻辑方法能够通过建立数学模型来描述协议系统，可提供相应的模型检测工具对协议性质进行自动验证，对状态空间有限的并发协议系统分析尤为成功，已成为对电子商务协议进行形式化分析的主要工具之一。

基于时序逻辑[2, 4]的密码协议(包括电子商务协议)形式化分析方法已成为一个研究热点，其中，Emerson等人提出的线性时序逻辑LTL方法[4]具有很强的描述能力，可以对协议系统进行形式化建模分析；Clarke和Emerson在LTL基础上提出了计算树逻辑CTL[2]的方法能够对协议的并发性质进行更为准确的描述。这些传统时序逻辑方法由于把协议看成封闭式并发系统进行研究，不太适合日益复杂的电子商务协议和大型游戏协议的描述和分析。Kremer博士提出一种新的基于博弈的ATL[5, 6](Alternating-time Temporal Logic)逻辑分析方法可有效地解决上述问题，能够对协议主体间的合作与竞争关系，协议内部与外部环境的关系等进行有效描

2005-08-30 收到，2006-01-11 改回

国家自然科学基金(40261009)和贵州省科学技术基金(20052111)资助课题

述[7, 8]。本文讨论了ATL逻辑及其在电子商务协议形式化分析中的应用，进一步扩展了Kremer博士的方法使之在考虑公平性等特性的同时能够分析协议的安全性。本文利用新方法对ZDB协议[9]进行了严格的形式化分析，发现了该协议的潜在缺陷。

2 ATL逻辑

交替转换系统ATS与时间交替时序逻辑ATL是Alur等人提出的适合于描述开放分布式系统的逻辑描述工具[5, 6]，其相应模型检测工具为MOCHA。

交替转换系统 (Alternating Transition Systems，ATS)

ATS是我们用来对电子商务协议建模的形式化工具。ATS是普通Kripke结构的一个带博弈变量的扩展，其定义如下：

定义1 一个交替转换系统是一个六元组 $S=\langle \Pi,\Sigma,Q,Q_0,\pi,\delta\rangle$。其中 Π 是命题集，Σ 是参与者集，Q 是状态集，$Q_0\subset Q$ 是初始状态集，$\pi:Q\to 2^{\Pi}$ 是从状态到命题集的映射，$\delta:Q\times \text{鈦}\to 2^{2^Q}\setminus\{\ \}$ 是一个从{状态×参与者}到非空的选择集合的转换函数，这里的每个选择是一个可能的下一个状态集合(可能包含一些约束)。当系统在状态 q 时，每个参与者选择一个集合 $Q_a\in\delta(q,a)$，这样，一个参与者 a 保证系统的下一个状态包含在它的选择 Q_a 中，具体选择其中的哪一个状态还要看系统中其它参与者的选择，因为 q 的后继存在于所有参与者选择的交集 $\bigcap_{a\in\Sigma}Q_a$ 里面。必须保证转换函数是无阻塞的而且所有参与者共同选择唯一的下一个状态，即：如果 $\sum=\{a_1,\cdots,a_n\}$，那么对每个状态 $q\in Q$ 和集合 $Q_1,\cdots,Q_n$，$Q_1\bigcap\cdots\bigcap Q_n$ 是唯一的。若 $q_0\in Q_0$ 是一个初始状态，由状态构成的无限序列 $q_0,q_1,\cdots,q_n,\cdots$ 是一个计算。

时间交替时序逻辑(Alternating-time Temporal Logic，ATL)

ATL是与交替转换系统ATS对应的逻辑系统，下面给出ATL公式定义：

定义2 一个ATL公式有如下形式：

(1) p，其中，命题 $p\in\Pi$；

(2) $\neg\varphi$ 或 $\varphi_1\vee\varphi_2$，其中，φ_1 和 φ_2 是ATL公式；

(3) $\langle\langle A\rangle\rangle\circ\varphi$，$\langle\langle A\rangle\rangle\Box\varphi$，$\langle\langle A\rangle\rangle\varphi_1\bigcup\varphi_2$，

其中 $A\in\sum$ 是参与者集合，φ，φ_1 和 φ_2 是ATL公式，$\langle\langle\rangle\rangle$ 是路径量词，$\circ$(下一个)，$\Diamond$(可能)，$\Box$(必然)，$\bigcup$(直到)是时态算子，其具体定义可参见文献[5]，其它 $\neg$，$\wedge$，$\cup$ 等与普通逻辑学中含义相同。

定义3 策略：一个参与者的策略是一个映射：$f_a:Q^+\to 2^Q$，使得对所有 $\lambda\in Q^*$ 和所有 $q\in Q$，$f_a(\lambda\cdot q)\in\delta(q,a)$ 成立。

关于ATL和ATS的语法及语义的详细定义可以参见文献[5]。

3 公平电子商务协议的要求和ATL分析

公平电子商务协议既要求满足非否认性、公平性及适时终止性等特性，同时要有足够的安全性，能够抵御重放等攻击。要用 ATL 逻辑进行公平电子商务协议分析，首先必须对协议系统进行建模，为了简化建模过程，本文不用直接建立系统的 ATS 模型，而是沿用 Dijkstra 类型保护命令语言[10](guarded command language)的方法进行建模，每个参与者 a 对应一个形如 guard → update 的保护命令集。一个计算步骤定义为：每个参与者选择它自己的命令集中 guard 取值为真的一个命令，所有参与者选择的命令中 update 部分相交得到的结果就是下一个状态。用保护命令语言建立系统的ATS模型，用ATL公式描述待验证的系统性质并输入到模型检测工具MOCHA[6]中运行，即可根据输出结果分析系统性质。

下面沿用文献[7，8]中的标记方式对公平电子商务协议上述性质进行一般描述，另外本文增加了一个入侵者 i。

3.1 基本假设

考虑到电子商务协议的一般情况，同时为了简化特定协议分析过程，本文对一些比较有共性的内容作一个基本假设，特定协议另有说明的除外。

通道：假定协议参与各方之间的通道是不可靠的，即其传输的信息可能延迟、丢失；而协议参与各方与可信第三方之间的通道是可恢复的，即其传输的信息可能延迟，但最终会在有限时间内到达目的地。

协议主体：协议参与各方都可能是不诚实的，而可信第三方是诚实可靠的。

入侵者：假定对入侵者 i 对信道有完全的控制能力，入侵者能够偷听、拦截、存储、插入、删除、生成、转发、重放消息。

3.2 保密性及安全性

电子商务协议的保密性与其它密码协议的要求一致：协议外的攻击者不能通过各种攻击方法非法得到协议参与各方的交换信息与参与协议的证据，用ATL公式可以描述如下：

$$\neg\langle\langle i\rangle\rangle\Diamond(m\vee \text{item}_A\vee \text{item}_B)$$

其中 m 是协议参与各方的交换信息，item_A，item_B 是协议参与各方参与协议的证据。协议的安全性与保密性基本相同，对具体协议中的区别，我们将在具体例子中进行分析。

3.3 非否认性

定义4 非否认性：协议参与双方在协议运行结束后都不能否认参与协议的行为，这主要通过交换发方非否认证据 NRO 与收方非否认证据 NRR 来实现。

如果协议双方都是诚实的，而且通道配合协议正常运行，B 拥有一个策略可以得到 A 参与协议的证据 item_A，同

时 A 也拥有可以得到 B 参与协议的证据 item_B 的策略，用ATL公式可以描述如下：

$$\langle\langle A_h, B_h, \text{Com}\rangle\rangle\Diamond(\langle\langle B\rangle\rangle\text{item}_A \wedge \langle\langle A\rangle\rangle\text{item}_B)$$

3.4 公平性

定义5　公平性：电子商务协议被称为是公平的。 如果满足以下两个条件:

(1) 在协议结束时,能够分别给发信方和接收方提供有效的NRR和NRO证据；

(2) 协议中止在任何阶段时，不会造成任何一方处于较另一方更为优势的地位，或者说协议双方要么得到了各自期望的东西，要么都得不到任何有利信息。

A 没有一个策略可以通过控制通道使得系统到达这样一个状态：在该状态 A 得到 B 参与协议的证据 item_B 而没有策略可以得到 A 参与协议的证据 item_A，即协议对 B 应该是公平的，用ATL公式可以描述如下：

$$\neg\langle\langle A, \text{Com}\rangle\rangle\Diamond(\text{item}_B \wedge \neg\langle\langle B_h\rangle\rangle\Diamond\text{item}_A)$$

协议对 A 是公平的可以描述如下：

$$\neg\langle\langle B, \text{Com}\rangle\rangle\Diamond(\text{item}_A \wedge \neg\langle\langle A_h\rangle\rangle\Diamond\text{item}_B)$$

3.5 适时终止性

定义6　电子商务协议如果在不失公平性的前提下，能够保证协议的任何一方可以单方地促使一个交易结束，那么这个非否认协议就是适时终止的。

适时终止性表明诚实的协议参与方可以在有限时间到达协议的一个状态，使得自己在该状态可以在保证协议公平性的前提下终止协议：

$$\langle\langle A_h\rangle\rangle\Diamond(\text{stop}_A \wedge \neg\text{item}_B \rightarrow \neg\langle\langle B\rangle\rangle\Diamond\text{item}_A)$$

$$\langle\langle B_h\rangle\rangle\Diamond(\text{stop}_B \wedge \neg\text{item}_A \rightarrow \neg\langle\langle A\rangle\rangle\Diamond\text{item}_B)$$

4　应用实例

4.1 ZDB协议简介

ZDB协议[9]是Zhou 等人提出的公平非否认协议，下面首先对其进行简要描述。

基本记号： M 为A发给B的消息； K 为A定义的A，B间会话密钥； $C = eK(M)$ 为对M用K加密后得到的密文； $L = H(M,K)$ 为唯一标识； $f_i(i = 1,2,\cdots)$ 为用来描述一条消息的目的； $\text{EOO}\_C = sS_A(f_1,B,L,C)$ 为对密文 C 的发信证据(Evidence Of Origin)； $\text{EOR}\_C = sS_B(f_2,A,L,\text{EOO}\_C)$ 为对密文C的收信证据(Evidence Of Receipt)； $\text{EOO}\_K = sS_A(f_3,B,L,K)$ 为对密钥K的发信证据(Evidence Of Origin)； $\text{EOR}\_K = sS_B(f_4,A,L,\text{EOO}\_K)$ 为对密钥K的收信证据(Evidence Of Receipt)； $\text{sub}\_K = sS_A(f_5,B,L,K,\text{TTP},\text{EOO}\_C)$ 为 A 提交K的证明； $\text{con}\_K = sS_{\text{TTP}}(f_6,A,B,L,K)$ 为 TTP 发布的对 K 的确认证据(evidence of confirmation)； $\text{abort} = sS_{\text{TTP}}(f_8,A,B,L)$ 为TTP 发布的对一个交易的中止证据(evidence of abort)； P_{TTP} 为TTP的公开密钥。

ZDB协议包括交换子协议、中止子协议与决议子协议3个部分，下面我们分别对其各个进行简要描述。

交换子协议Exchange：

(1) $A \rightarrow B : m_1 = f_1, f_5, B, L, C, \text{TTP}, eP_{\text{TTP}}(K), \text{EOO}\_C, \text{sub}\_K$

IF B gives up THEN quit ELSE goto (2)

(2) $B \rightarrow A : m_2 = f_2, A, L, \text{EOR}\_C$

IF A gives up THEN abort ELSE goto (3)

(3) $A \rightarrow B : m_3 = f_3, B, L, K, \text{EOO}\_K$

IF B gives up THEN resolve ELSE goto (4)

(4) $B \rightarrow A : m_4 = f_4, A, L, \text{EOR}\_K$

IF A gives up THEN resolve

中止子协议Abort：

(1) $A \rightarrow \text{TTP} : f_7, B, L, sSA(f_7, B, L)$

IF resolved THEN

(2) $\text{TTP} \rightarrow A : f_2, f_6, A, B, L, K, \text{con}\_K, \text{EOR}\_C$

ELSE

(3) $\text{TTP} \rightarrow A : f_8, A, B, L, \text{abort}$

决议子协议Resolve如下，其中的U可以是A或B。

(1) $U \rightarrow \text{TTP} : f_2, f_5, A, B, L, \text{TTP}, eP_{\text{TTP}}(K), \text{sub}\_K, \text{EOO}\_C, \text{EOR}\_C$

IF aborted THEN

(2) $\text{TTP} \rightarrow U : f_8, A, B, L, \text{abort}$

ELSE

(3) $U \rightarrow \text{TTP} : f_2, f_6, A, B, L, K, \text{con}\_K, \text{EOR}\_C$

需要说明的是，Zhou等人在协议中对通道的假设是：TTP与各通信主体A，B之间的通道是可复原的，符合本文3.1节的基本假设；而其对通信主体A，B之间的通信信道则假定是私密的。我们认为这个前提要求太高，在本文中将按照3.1节的基本假设进行分析，即通信主体A，B之间的通道是可复原但非保密的，同时入侵者对信道有完全的控制能力。由于减弱了协议前提假设，因而本文的分析结果与文献[9]有一些区别。

4.2 ZDB协议的建模

对协议建模的关键在于刻画出协议各主体的基本行为转换关系，主要包括协议发起者、协议响应者和可信第三方。同时要对不诚实的协议参与者、可能存在的入侵者的行为进行描述，还要对通信信道进行合理的假设。在下述图1~图3中，m_1~m_4含义见Exchange协议，其余符号含义如下：

Ar为A发给TTP的abort请求；Rr为A或B发给TTP的resolve请求；A为TTP发给A或B的abort确认；R为TTP发给A或B的resolve确认。

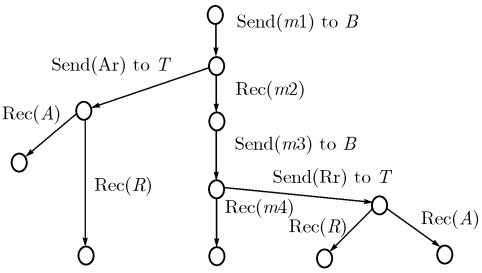

图1 协议参与者A的基本行为图

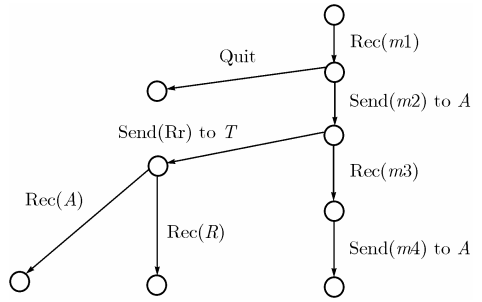

图2 协议参与者B的基本行为图

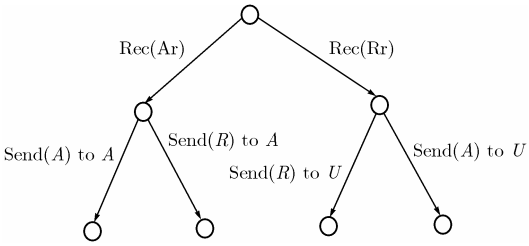

图3 可信第三方TTP的行为图

图1是协议参与者A在正常状态下的行为转换图，若A是不诚实的，它可以尝试与图1不同的行为以获取利益。如不按协议规定启动Abort，Resolve子协议，窃听B与TTP之间的通信内容等。B同样可以尝试类似的行为以获取利益，下面省略。

假设入侵者对信道有完全的控制能力，入侵者能够偷听、拦截、存储、插入、删除、生成、转发、重放消息，在协议运行中，入侵者将不依照协议的要求，而是根据自己拥有知识的情况，向所有的主体进行截获、生成、插入消息等。

除了对ZDB协议的上述主要模块建模外，我们还要对不诚实的协议主体(参与者)、通道行为(按基本假设)、入侵者的各种可能的入侵行为等进行建模，然后将这些模型转化成MOCHA可以接受的保护命令语言[10](guarded command language)输入MOCHA系统进行验证，根据ATL公式是否成立来判断系统是否满足某个性质。与SMV等模型检测工具不同，MOCHA系统在ATL公式不成立时并不输出对应反例，因而还需要对协议进行详细分析以找出其满足该性质的具体原因。

4.3 ZDB协议性质的ATL描述和分析

根据前面对ZDB协议的描述可以定义协议双方的非否认证据。

发方非否认证据：

$$\mathrm{NRO} = B.\mathrm{knows}(\mathrm{EOO}.C) \wedge (B.\mathrm{knows}(\mathrm{EOO}.K) \vee B.\mathrm{knows}(\mathrm{Con}.K)),$$

收方非否认证据：

$$\mathrm{NRR} = A.\mathrm{knows}(\mathrm{EOR}.C) \wedge (A.\mathrm{knows}(\mathrm{EOR}.K) \vee A.\mathrm{knows}(\mathrm{Con}.K))。$$

下面将用ATL公式分别对ZDB协议的保密性、安全性、非否认性、公平性及适时终止性等性质进行描述，并利用MOCHA工具进行验证。

保密性：对本协议来说，协议双方通信的内容 m，发方非否认证据 NRO 与收方非否认证据 NRR 都属于机密信息，入侵者 i 应该不能重放等手段获取，即如果协议双方 A 和 B 是诚实的，那么即使 i 可以控制通信信道 com，它也无法获取协议双方通信的内容 m，发方非否认证据 NRO 与收方非否认证据 NRR，但其中最为关键的机密信息应为 m。为简单起见，保密性可以用以下ATL公式描述如下：

$$\neg\langle\langle i,\mathrm{com}\rangle\rangle\Diamond(m)$$

通过利用MOCHA工具对上述公式进行验证可知，ZDB协议不满足保密性。分析可知在主协议Exchange中的第(1)步和第(2)步，A直接将密文C和密钥K发送给B，入侵者 i 可以通过偷听获取密文C和密钥K进而得到m的内容。当然按照原协议中Zhou等人对A，B之间的通信信道假定是私密的，就不会存在这样的攻击。

安全性：主要检验入侵者 i 能否通过重放等方法欺骗A或B使其在不知情的状况下以为是与合法协议主体(B或A)完成协议。经检验，下述公式不成立：

$$\neg\langle\langle i,\mathrm{com},B_h\rangle\rangle\Diamond(\mathrm{stop}\wedge\langle\langle i\rangle\rangle\Diamond\mathrm{NRR})$$

分析可知在协议中入侵者 i 可以通过偷听等手段获取以前某次协议的信息实施重放攻击而欺骗B：

(1) $I \to B : f_1, f_5, B, L, C, \mathrm{TTP}, eP_{\mathrm{TTP}}(K),$ $\mathrm{EOO\_}C, \mathrm{sub\_}K$

(2) $B \to A : f_2, A, L, \mathrm{EOR\_}C$ (入侵者 i 拦截)

(3) $I \to B : f_3, B, L, K, \mathrm{EOO\_}K$

(4) $B \to A : f_4, A, L, \mathrm{EOR\_}K$ (入侵者 i 拦截)

上述攻击中，若 B 不保留以往通信副本，则入侵者 i 可以成功实现重放攻击，使得诚实的 B 以为是 A 发起的一个新的通信过程(如新合同等)而在其上签署收到的不可否认证据。由于入侵者 i 只能使用 A，B 以前成功进行的一个协议副本才能进行攻击，因此本文并不认为它造成了对 B 的不公平，而是对整个协议的安全性构成威胁。因而在随后分析协议的非否认性、公平性等性质时本文并不考虑这个攻击的影响，另外可以通过加盖时间戳的方式有效地防止这种重放攻击。

非否认性：如果协议双方都是诚实的，而且通道配合协议正常运行，B 拥有一个策略可以得到 A 参与协议的证据

NRO，同时 A 也拥有可以得到 B 参与协议的证据 NRR 的策略：

$$\langle\langle A_h, B_h, \mathrm{Com}\rangle\rangle\Diamond(\langle\langle B\rangle\rangle\mathrm{NRO} \wedge \langle\langle A\rangle\rangle\mathrm{NRR})$$

经过验证可知，ZDB协议满足非否认性。

公平性：A 没有一个策略可以通过控制通道使得系统到达这样一个状态：在该状态 A 得到 B 参与协议的证据 item_B 而没有策略可以得到 A 参与协议的证据 item_A，即协议对 B 应该是公平的：

$$\neg\langle\langle A, \mathrm{Com}\rangle\rangle\Diamond(\mathrm{NRR} \wedge \neg\langle\langle B_h\rangle\rangle\Diamond\mathrm{NRO})$$

协议对 A 是公平的可以描述如下：

$$\neg\langle\langle B, \mathrm{Com}\rangle\rangle\Diamond(\mathrm{NRO} \wedge \neg\langle\langle A_h\rangle\rangle\Diamond\mathrm{NRR})$$

通过利用MOCHA工具对上述公式进行验证可知协议对 A 是公平的。

适时终止性：适时终止性表明诚实的协议参与方可以在有限时间到达协议的一个状态，使得自己在该状态可以在保证协议公平性的前提下终止协议，根据这个可知，协议如果不公平就不可能满足适时终止性，对ZDB协议本身，以下ATL公式：

$$\langle\langle A_h\rangle\rangle\Diamond(\mathrm{stop}_A \wedge \neg\mathrm{NRR} \rightarrow \neg\langle\langle B\rangle\rangle\Diamond\mathrm{NRO})$$

$$\langle\langle B_h\rangle\rangle\Diamond(\mathrm{stop}_B \wedge \neg\mathrm{NRO} \rightarrow \neg\langle\langle A\rangle\rangle\Diamond\mathrm{NRR})$$

成立，因而协议也满足适时终止性。

5　结束语

本文研究并扩展了Kremer等人提出的的基于博弈的ATL逻辑方法，能够对协议主体之间的对抗和合作关系进行准确的描述，是有效的针对复杂电子商务协议的形式化分析方法。通过对一个典型的公平电子商务协议ZDB协议进行了严格的形式化分析并用MOCHA工具验证，发现在非保密信道下存在两个可能的攻击，结果表明了新方法的正确性和实用性。

与Kremer[7,8]及其他人[11–14]的工作相比，本文的分析方法不仅可以对复杂电子商务协议的非否认性、公平性及适时终止性进行有效描述和分析，还针对协议的安全性引入了入侵者模型以分析各种主要攻击方式，因而更为符合复杂电子商务协议的形式化分析的需要。

参 考 文 献

[1] Asokan N. Fairness in electronic commerce. [PhD thesis], University of Waterloo, May 1998.

[2] Clarke E M and Emerson E A. Design and synthesis of synchronization skeletons using branching time temporal logic. In Logic of Programs, volume 131 of Lecture Notes in Computer Science, Springer- Verlag, 1981: 52–71.

[3] Schneider S A. Formal analysis of a non- repudiation protocol. In 11th IEEE Computer Security Foundations Workshop, Massachusetts, USA, 1998: 54–65.

[4] Emerson E A. Temporal and modal logic. In J. van Leeuwen, editor, Handbook of Theoretical Computer Science, vol B: Formal Models and Semantics, chapter 16. Elsevier Publishers B.V, 1990: 995–1072.

[5] Alur R, Henzinger T A, and Kupferman O. Alternating-time temporal logic. In 38th Annual Symposium on Foundations of Computer Science, Miami Beach, IEEE Computer Society Press, 1997: 100–109.

[6] Alur R, Henzinger T A, Mang F, Qadeer S, Rajamani S, and Tasiran S. MOCHA: Modularity in model checking. In Proc. CAV '98, Vancouver, BC, Canada, 1998: 512–525.

[7] Kremer S and Raskin J F. A game-based verification of non-repudiation and fair exchange protocols. *Journal of Computer Security*, 2003, 11(3): 399–429.

[8] Kremer S and Raskin J F. Game analysis of abuse-free contract signing. In Proceedings of the 15th IEEE Computer Security Foundations Workshop (CSFW'02), Cape Breton, Nova Scotia, Canada, June 2002, IEEE Computer Society Press, 2002: 206–220.

[9] Zhou J Y, Deng R H, and Bao F. Evolution of fair non-repudiation with TTP. In ACISP: Information security and privacy: Australasian Conference, volume 1587 of Lecture Notes in Computer Science, Springer-Verlag, 1999: 258–269.

[10] Henzinger T, Majumdar R, Mang F, and Raskin J F. Abstract interpretation of game properties. In Proc. SAS '00, Santa Barbara, USA, 2000: 220~239.

[11] Mahimkar A and Shmatikov V. Game-based analysis of denial-of-service prevention protocols. in 18th IEEE Computer Security Foundations Workshop (CSFW), Aix-en-Provence, France June 2005: 151–166.

[12] Schunter M. Optimistic fair exchange.[PhD thesis], Technische Fakult¨at der Universit at des Saarlandes, Saarbr¨ucken, October 2000.

[13] Zhou J and Gollmann D. An efficient non-repudiation protocol. Proceedings of 10th IEEE Computer Security Foundations Workshop[C]. Rocport , Massachusetts : IEEE Computer Society Press, June 1997: 126–132.

[14] Garay J A, Jakobsson M, and MacKenzie P D. Abuse-free optimistic contract signing. In Advances in Cryptology —Crypto 1999, volume 1666 of Lecture Notes in Computer Science, Springer-Verlag, 1999: 449–466.

文静华：　男，1975 年生，博士后，主要从事信息安全、协议分析研究.

李　祥：　男，1942 年生，教授，博士生导师，研究方向为可计算性理论、密码学与网络安全.

张焕国：　男，1945 年生，教授，博士生导师，主要从事密码学与网络安全研究.

梁　敏：　女，1980 年生，硕士生，从事电子商务安全研究.

张　梅：　女，1974 年生，博士生，从事计算机视觉研究.