一种分析电子商务安全协议的新逻辑

陈 莉
(河南财经学院计算中心 郑州 450002)

摘 要 针对典型电子商务安全协议逻辑分析方法存在的问题,如安全属性分析存在局限性、缺乏形式化语义、对混合密码原语的处理能力不强等,提出了一种新的逻辑分析方法。新逻辑能够分析电子商务安全协议的认证性、密钥保密性、非否认性、可追究性、公平性及原子性。以匿名电子现金支付协议 ISI 作为分析实例,证明了新逻辑方法的有效性。分析找出了该协议的安全漏洞和缺陷:不满足商家的非否认性、密钥保密性、可追究性、公平性以及原子性,客户面临商家恶意欺骗的潜在威胁。

关键词 逻辑分析方法,安全属性,密钥保密性,原子性,混合密码原语,逻辑构件

New Logic of Analyzing Electronic Commerce Security Protocols

CHEN Li
(Computer Center, Henan University of Finance and Economics, Zhengzhou 450002, China)

Abstract The paper researched the typical logic analysis methods of electronic commerce security protocols and pointed out their limitations in analyzing security properties. Most of them are lack of formal semantics and ability of analyzing hybrid cryptography-based primitives. In response on the above-mentioned problems, the paper proposed a new logic analysis method, which can analyze most of the known security properties of the electronic commerce protocols, such as authentication, secrecy of key, non-repudiation, accountability, fairness and atomicity. The validation of the new logic was verified by analyzing the anonymous e-cash payment protocol ISI. The analysis reveals the security vulnerabilities and flaws of the protocol, which cannot satisfy non-repudiation of merchants, secrey of key, accountability, fairness and atomicity, moreover, the customers face malicious cheat of the merchants.

Keywords Logic analysis method, Security property, Secrey of key, Atomicity, Hybrid cryptography-based primitives, Logic sentences

1 引言

目前,典型的电子商务安全协议逻辑分析方法被广泛应用于协议的安全属性分析,而且发现了一些典型电子商务安全协议的缺陷或存在的安全漏洞。本文研究发现,典型逻辑分析方法[1-7]存在以下问题:(1)有些逻辑方法没有给出其形式化语义[3-7],无法判断其推理规则的正确性[8,9];(2)对混合密码原语的处理能力有待提高;(3)安全属性分析存在一定的局限性,多数方法仅能分析3种以内的安全属性,在一定程度上限制了其自身的发展;基于对比较典型的电子商务安全协议逻辑分析方法的研究可以得出,大多数逻辑方法的初衷是针对一种安全属性进行分析,如 SVO 逻辑[1]和 KAILAR 逻辑[2]。为了拓宽这些逻辑的分析范围,研究人员提出了一些能分析2种或3种安全属性的改进方法,如能分析可追究性和公平性的卿-逻辑方法[3]、KPBHS 方法[4]和 LPC 与 KAILAR 逻辑结合法[5],能够分析认证性、非否认性、原子性的王-杨方法[6],能够分析认证性、非否认性、时限性的黎-罗方法[7]。因此,提高现有典型电子商务安全协议逻辑方法的分析能力,是目前逻辑方法研究的热点和趋势。

基于对典型电子商务安全协议逻辑分析方法的研究,本文提出了一种能够分析电子商务安全协议的认证性、密钥保密性、非否认性、可追究性、公平性及原子性的新逻辑分析方法。综合上述安全属性的特点,提出了新逻辑涉及的逻辑构件、公理和推理规则。通过增加与 Hash 函数和加密 Hash 函数等密码原语相关的逻辑谓词、公理和推理规则,使新逻辑方法不仅具有分析基于对称密码体制和公钥密码体制的协议的能力,而且具有分析高效 Hash 函数密码原语的能力。本文对使用新逻辑对匿名电子现金支付协议 ISI[10]的安全目标进行了严格的形式化验证,发现了其存在以下安全漏洞和缺陷:不满足商家的非否认性、可追究性、公平性和原子性,客户面临商家恶意欺骗的潜在威胁,以及不满足密钥保密性。并验证了新逻辑的有效性。

鉴于篇幅,本文没有给出新逻辑的形式化语义分析。

2 新逻辑

2.1 新逻辑的语法

在新逻辑中,把不同类型的对象分为4类:主体 *principal*、密钥 *key*、消息 *message* 以及公式 *formula*,其中公式是

到稿日期:2009-11-18 返修日期:2010-01-29 本文受国家高技术研究发展计划(863计划)(2007AA01Z471),国家自然科学基金项目(60473021),河南省重点科技攻关项目(072102210029),河南省科技攻关项目(0624260017)资助。

陈 莉(1968—),女,博士,副教授,主要研究方向为信息安全、安全协议和电子商务,E-mail:chlit123@yahoo.com.cn。

消息的子类。新逻辑的语法结构包括有限个常量项、变量项、n 元函数、n 元动作、原子公式、复合公式、逻辑连接符、量词和时态操作符。

主体：指交易的参与者，包括诚实主体、非诚实主体、可信第三方和攻击者。通常用大写字母表示，例如，P,Q,R,TTP,I 等。

消息：指通信的内容，用小写字母表示。存在 3 种消息类型：原子消息、组合消息和加密消息。其中原子消息分别是主体标识、密钥、新鲜数(包括随机数和时间戳)。

定义 1 消息语言抽象为一个二元组(M,K)，其中 $K\subseteq M$，则其满足下列条件：

逆钥：若 $k\in K$，则 $k-1\in K$。

组合：若 $m_1,m_2,\cdots,m_n\in M$，则$(m_1,m_2,\cdots,m_n)\in M$。

分解：若$(m_1,m_2,\cdots,m_n)\in M$，则 $m_1,m_2,\cdots,m_n\in M$。

加密：若 $k\in K$ 且 $m\in M$，则 $E(m,k)\in M$。

解密：若 $k\in K$ 且 $E(m,k)\in M$，则 $m\in M$。

签名：若 $k^{-1}\in K$ 且 $m\in M$，则 $S(m,k^{-1})\in M$。

Hash：若 $m\in M$，则 $H(m)\in M$。若 $k\in K$ 且 $m\in M$，则 $H(m,k)\in M$。

在此假定：

(1)若 $E(m_1,k_1)=E(m_2,k_2)$，则 $m_1=m_2$ 且 $k_1=k_2$。

(2)若$(m_1,m_2,\cdots,m_n)=(m_1',m_2',\cdots,m_{n'}')$，则 $n=n'$ 且对于 $1\leqslant i\leqslant n, m_i=m_i'$。

动作：主体的通信操作，主要包括发送消息、接收消息，格式如下：

$send(P,Q,m)$：表示主体 P 刚发送消息 m 给主体 Q。这里，Q 为可选项。

$receive(P,m)$：表示主体 P 接收到消息 m。

$transmit(P,Q,FTP)$：表示主体 P 采用 FTP 方式传递消息 m 给主体 Q。

函数：定义在消息空间上的映射关系。主要函数有：

$E(m,k)$：表示用密钥 k 对消息 m 进行加密。

$D(m,k)$：表示用密钥 k 对消息 m 进行解密。

$S(m,k^{-1})$：表示用密钥 k^{-1} 对消息 m 进行签名。

$H(m,k)$：表示对比特串(m,k)的单向 Hash 运算，这里 k 是可选项。

$F(m_1,m_2)$：表示 F 为一般函数，用于密钥协商运算。

$Od(P)$：表示主体 P 的订单信息。

$Pc(P)$：表示主体 P 的信用卡号。

$Pi(P)$：表示主体 P 的支付指令。

$Tid(P)$：表示主体 P 的本次交易标识。

谓词：表示各种信任关系、证明关系及消息状态。主要有以下谓词：

$believe(P,m)$：表示主体 P 相信消息 m。

$possess(P,m)$：表示主体 P 拥有消息 m。

$control(P,m)$：表示主体 P 对消息 m 有管辖权。

$canprove(P,m)$：表示主体 P 能证明消息 m。

$claim(P,m)$：表示主体 P 对消息 m 负责。

$say(P,m)$：表示主体 P 声明消息 m。

$Pk(P,k)$：表示 k 是主体 P 公钥，用于消息解密或验证签名。

$Sk(P,k^{-1})$：表示 k^{-1} 是主体 P 的私钥，用于数据加密或签名。

$share(P,Q,k)$：表示 k 是主体 P 与主体 Q 之间"好的"共享密钥。

$share(P,Q,k-)$：表示 k 是 P 的、适合于与 Q 通信的非确认共享密钥(*unconfirmed key*)，即 $share(P,Q,k-)$相当于 $share(P,Q,k)\wedge possess(P,k)$。

$share(P,Q,k+)$：表示 k 是 P 的、适合于与 Q 通信的确认共享密钥(*confirmed key*)，即 $share(P,Q,k+)$相当于 $share(P,Q,k)\wedge possess(P,k)\wedge Send(P,k)$。

$authenticate(k,P)$：表示密钥 k 能用于验证主体 P 的身份。

$fresh(m)$：表示消息 m 是新鲜的。

$match((m,k),h(m,k))$：用于校验由消息 m 和密钥 k 连接而成的比特串(m,k)与其摘要 $h(m,k)$的一致性。这里参数 k 为可选项。

$verify(m_1,k^{-1},m_2)$：表示使用密钥 k^{-1} 能验证 m_2 是 m_1 的签名，即 $m_2=S(m_1,k^{-1})$。

$verify(m_1,k,m_2)$：表示使用密钥 k 能验证 m_2 是 m_1 的密文，即 $m_2=E(m_1,k)$。

$in(m_1,m_2)$：表示消息 m_1 包含于消息 m_2 中。若 m_2 为集合，则表示前者属于后者。

$equal(m_1,m_2)$：表示消息 m_1 与消息 m_2 相同。

时态操作符$\diamondsuit$：表示某个动作发生在过去的某个时刻。

时态操作符$\textcircled{t}$：表示某个动作发生在 t 时刻。

量词：沿用数理逻辑中的符号，包括全称量词 $\forall$ 和存在量词 $\exists$。

逻辑连接符：沿用数理逻辑中的符号，包括逻辑并 $\wedge$、逻辑或 $\vee$、逻辑蕴涵 $\rightarrow$、逻辑等价 $\leftrightarrow$ 等。

定义 2 原子公式语言 F 是由以下规则生成的最小语言：

(1)若 $x\in M$ 且 P 为主体，则 $believe(P,x)$，$possess(P,x)$，$control(P,x)$，$canprove(P,x)$，$claim(P,x)$，$say(P,x)$，$send(P,x)$，$receive(P,x)$，$transmit(P,Q,x)$，$fresh(x)\in F$。

(2)若 P、Q 为主体且 $k,k^{-1}\in K$，则 $share(P,Q,k)$，$share(P,Q,k-)$，$share(P,Q,k+)$，$Pk(P,k)$，$Sk(P,k^{-1})$，$authenticate(k,P)$，$possess(P,k)\in F$。

(3)若 $x,y\in M$ 且 $k\in K$，则 $verify(x,k^{-1},y)$，$verify(x,k,y)\in F$。

上述原子公式亦称为逻辑构件。

复合公式：由原子公式、量词、逻辑连接符以递归的形式构造而成。

2.2 新逻辑的公理与推理规则

新逻辑包含以下公理：

(1)信任公理

AB1 $believe(P,x)\wedge believe(P,y)\leftrightarrow believe(P,x\wedge y)$

AB2 $believe(P,x)\wedge believe(P,x\rightarrow y)\rightarrow believe(P,y)$

AB3 $believe(P,x)\rightarrow believe(P,believe(P,x))$

(2)消息来源公理

ASA1 $share(P,Q,k)\wedge receive(R,E(x,k))\rightarrow\diamondsuit send(Q,x)\wedge possess(Q,k)$

ASA2 $Sk(Q,k^{-1})\wedge receive(R,x)\wedge verify(x,k,y))\rightarrow\diamondsuit send(Q,y)$

(3)密钥协商公理

AKA1 $Pk(P,k) \wedge Pk(Q,k) \rightarrow share(P,Q,k)$

AKA2 $equal(x, F_0(k_P, k_Q)/F_0(k_Q, k_P))$

(4)消息接收公理

AMR $receive(P,(x_1,x_2,\cdots,x_n)) \rightarrow receive(P,x_i)$

(5)密文理解公理

ACC1 $receive(P,E(x,k)) \wedge possess(P,k^{-1}) \rightarrow receive(P,x)$

ACC2 $receive(P,S(x,k^{-1})) \rightarrow receive(P,x)$

ACC3 $receive(P,(x_1,H(x_2,k))) \wedge believe(P,share(P,Q,k)) \rightarrow believe(P,\ominus send(Q,x_1))$

(6)消息拥有公理

AMP1 $receive(P,x) \rightarrow possess(P,x)$

AMP2 $possess(P,(x_1,x_2,\cdots,x_n)) \rightarrow possess(P,x_i)$

AMP3 $possess(P,x_1) \wedge possess(P,x_2) \wedge \cdots \wedge possess(P,x_n) \rightarrow possess(P,F(x_1,\cdots,x_n))$

(7)消息理解公理

AMC $believe(P,possess(P,F(x))) \rightarrow believe(P,possess(P,x))$

(8)消息发送公理

AMS1 $\ominus send(P,(x_1,x_2,\cdots,x_n)) \rightarrow \ominus send(P,x_i) \cdots possess(P,x_i)$

AMS2 $send(P,(x_1,x_2,\cdots,x_n)) \rightarrow \ominus send(P,(x_1,x_2,\cdots,x_n)) \wedge send(P,x_i)$

AMS3 $send(P,E(x,k)) \wedge possess(P,k) \rightarrow send(P,x)$

(9)管辖公理

AC $control(P,x) \wedge send(P,x) \rightarrow true(x)$

(10)消息新鲜性公理

AMF1 $fresh(x_i) \rightarrow fresh(x_1,\cdots,x_n)$

AMF2 $fresh(x_i) \rightarrow fresh(F(x_1,x_2,\cdots,x_n))$

(11)临时值验证公理

ANV $fresh(x) \wedge \ominus send(P,x) \rightarrow send(P,x)$

(12)“好的”共享密钥对称性公理

ASG $share(P,Q,k) \rightarrow share(Q,P,k)$

新逻辑包含以下推理规则：

(1)分离规则 MPR

$true(x) \wedge (x \rightarrow y) \leftrightarrow true(y)$

(2)必然规则 NER

$true(x) \rightarrow true(believe(P,x))$

(3)连接规则 LR1－LR4

$canprove(P,x_1) \wedge canprove(P,x_2) \wedge \cdots \wedge canprove(P,x_n) \rightarrow anprove(P,x_1 \wedge x_2 \wedge \cdots \wedge x_n)$

$canprove(P,x_1 \wedge x_2 \wedge \cdots \wedge x_n) \rightarrow canprove(P,x_1) \wedge canprove(P,x_2) \wedge \cdots \wedge canprove(P,x_n)$

$canprove(P,claim(Q,x_1)) \wedge canprove(P,claim(Q,x_2)) \wedge \cdots \wedge canprove(P,claim(Q,x_n)) \rightarrow canprove(P,claim(Q,x_1 \wedge x_2 \wedge \cdots \wedge x_n))$

$canprove(P,claim(Q,x_1 \wedge x_2 \wedge \cdots \wedge x_n)) \rightarrow canprove(P,claim(Q,x_1)) \wedge canprove(P,claim(Q,x_2)) \wedge \cdots \wedge canprove(P,claim(Q,x_n))$

(4)推理规则 RR

$canprove(P,x) \wedge canprove(P,x \rightarrow y) \rightarrow canprove(P,y)$

(5)信任规则 BR

$canprove(P,say(Q,x)) \wedge canprove(P,control(Q,x)) \rightarrow canprove(P,x)$

(6)签名规则 SR1－SR2

签名规则 SR1：

$possess(P,S(x,k^{-1})) \wedge canprove(P,authenticate(k,Q)) \rightarrow canprove(P,claim(Q,x))$

签名规则 SR2：

$believe(P,receive(P,S(m,k^{-1}))) \wedge believe(P,authenticate(k,Q)) \rightarrow believe(P,send(Q,m))$

(7)密文理解规则 CCR1－CCR2

密文理解规则 CCR1：

$canprove(P,claim(Q,E(x,k))) \wedge canprove(P,possess(Q,k)) \wedge canprove(P,verify(x,k,E(x,k))) \rightarrow canprove(P,claim(Q,k))$

密文理解规则 CCR2：

$canprove(P,claim(Q,E(x,k))) \wedge canprove(P,claim(Q,k)) \wedge canprove(P,verify(x,k,E(x,k))) \rightarrow canprove(P,claim(Q,x))$

(8)拥有规则 PR

$in(x,S_P^0) \rightarrow \forall Q, canprove(Q,possess(P,x))$

(9)传递规则 TR1－TR2

$canprove(P,claim(TTP,m)) \rightarrow canprove(P,possess(Q,m))$

$canprove(Q,claim(TTP,m)) \rightarrow canprove(Q,possess(P,m))$

(10)FTP 获取规则 GR1－GR2

$transmit(P,Q,m,FTP) \rightarrow receive(Q,m)$

$transmit(Q,P,m,FTP) \rightarrow receive(P,m)$

(11)身份证明规则 IAR1－IAR3

身份证明规则 IAR1：

$canprove(P,claim(TTP,(k,Q))) \rightarrow canprove(P,authenticate(k,Q))$

身份证明规则 IAR2：

$canprove(P,authenticate(k_{TTP},TTP)) \wedge possess(P,S((k_Q,Q),k_{TTP}^{-1})) \wedge possess(P,k_{TTP}) \rightarrow canprove(P,authenticate(k_Q,Q))$

身份证明规则 IAR3：

$believe(P,possess(P,S((k_Q,Q),k_{TTP}^{-1})) \wedge possess(P,k_{TTP}) \rightarrow believe(P,authenticate(k_Q,Q))$

3 新逻辑分析协议的步骤

在使用新逻辑对电子商务安全协议的安全属性进行形式化分析之前，首先需要完成以下准备工作：

任务 1：给出协议的形式化描述。

任务 2：列举协议的初始假设或初始化集合。

根据协议运行环境和协议运行的初始状态，分别列举协议主体的初始假设(集合)、拥有集合以及接收消息集合。

任务 3：列举发方非否认证据 EOO 和收方非否认证据 EOR。

接着，针对协议的某一具体安全属性，使用新逻辑按以下步骤做进一步分析：

步骤 1　使用逻辑语言给出此安全属性的形式化定义。

步骤 2　运用初始集合(或初始假设)、新逻辑的公理及推理规则对协议进行形式化推理分析。

如果推理结果不满足安全属性描述的安全目标,则说明协议存在缺陷或安全漏洞。

4　应用实例

本节将使用新逻辑方法对匿名电子现金支付协议 ISI 进行形式化分析,说明新逻辑方法的有效性。

4.1　匿名电子现金支付协议 ISI

ISI 协议[10]是由 Medvinsky 和 Neuman 提出来的匿名电子现金支付协议,协议涉及 3 个参与者:客户 A、商家 B 以及双方都信任的货币服务方 CS。其目的是客户 A 通过货币服务方 CS 向商家 B 付款,B 给 A 提供付款收据。在整个付款过程中,客户 A 保持匿名。ISI 协议描述如下:

(1)$A\rightarrow B:K_{AB}$

(2)$B\rightarrow A:\{K_B\}K_{AB}$

(3)$A\rightarrow B:\{\{coins\}K_{CS}^{-1},SK_A,K_{\_SES},S_{\_ID}\}K_B$

(4)$B\rightarrow CS:\{\{coins\}K_{CS}^{-1},SK_B,transaction\}K_{CS}$

(5)$CS\rightarrow B:\{\{new\_coins\}K_{CS}^{-1}\}SK_B$

(6)$B\rightarrow A:\{\{amount,Tid,date\}K_B^{-1}\}SK_A$

在 ISI 协议中,K_{AB} 表示 A 和 B 之间的会话密钥,K_A,K_B,K_{CS},K_{CS}^{-1} 分别表示客户 A、商家 B 的公钥以及货币服务方 CS 的公钥和私钥,$\{coins\}K_{CS}^{-1}$ 表示 A 的电子货币(货币均由 CS 签发),SK_A,SK_B 分别表示 A 与 B 共享的密钥,$K_{\_SES}$ 表示想获得的服务的密钥;$S_{\_ID}$ 表示想获得的服务的标识符,$transaction$ 表示具体事务处理。

4.2　ISI 协议形式化分析

本节对 ISI 协议的密钥保密性、非否认性、可追究性、公平性和原子性进行分析。

协议分析的准备工作如下。

任务 1:给出协议的形式化描述。

使用新逻辑对 ISI 协议进行形式化描述如下:

(1)$receive(B,K_{AB})$

(2)$receive(A,E(k_B,K_{AB}))$

(3)$receive(B,E((S(coins,K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),K_B))$

(4)$receive(CS,E((S(coins,K_{CS}^{-1}),SK_B,transaction),K_{CS}))$

(5)$receive(B,E(S(new\_coins,K_{CS}^{-1}),SK_B))$

(6)$receive(A,E((S(amount,Tid,date),K_B^{-1}),SK_A))$

任务 2:列举协议的初始化集合。

根据协议运行环境和协议运行的初始状态,分别列举协议主体的初始假设集合、拥有集合以及接收消息集合。

设协议主体 A、B、仲裁方 ADJ 和攻击者 I 的初始假设集合分别为 INI_S_A,INI_S_B,INI_S_{ADJ} 和 INI_S_I,他们的初始拥有集合分别为 POS_A^0,POS_B^0,POS_{ADJ}^0 和 POS_I^0,A 和 B 的接收消息集合分别为 REV_A 和 REV_B。

$INI\_S_A=\{canprove(A,authenticate(K_{CS},CS))\}$

$POS_A^0=\{SK_A,K_{CS},K_{AB},K_A,K_A^{-1}\},REV_A=\{\}$

$INI\_S_B=\{believe(B,authenticate(K_{CS},CS)),canprove(B,authenticate(K_{CS},CS))\}$

$POS_B^0=\{SK_B,K_{CS},K_A,K_B,K_B^{-1}\},REV_B=\{\}$

$INI\_S_{ADJ}=\{believe(ADJ,authenticate(K_{CS},CS))\}$

$POS_{ADJ}^0=\{K_{CS},K_A,K_B\}$

$INI\_S_I=\{\neg(in(K_{CS}^{-1},POS_I)\wedge in(K_A^{-1},POS_I)\wedge in(K_B^{-1},POS_I))\},POS_I^0=\{K_{CS},K_A,K_B\}$

任务 3:列举发方非否认证据 EOO 和收方非否认证据 EOR。

$EOO=S(new\_coins,K_{CS}^{-1})$

$EOR=S((amount,Tid,date),K_B^{-1})$

4.2.1　密钥保密性分析

步骤 1　给出密钥保密性的形式化定义。

使用新逻辑可以将密钥保密性目标形式化定义为:

$G\neg(in(K_{AB},POS_I)\wedge in(SK_A,POS_I)\wedge in(K_{\_SES},POS_I)\wedge in(SK_B,POS_I)\wedge in(K_{CS}^{-1},POS_I)\wedge in(K_A^{-1},POS_I)\wedge in(K_B^{-1},POS_I))$

步骤 2　验证密钥保密性目标。

使用新逻辑的公理和推理规则,在每一条协议语句执行之后,分析攻击者获取合法协议主体的密钥信息的情况,并以此判断密钥保密性目标是否满足。

证明:首先,分析在协议第(1)条语句执行之后,攻击者获取密钥信息的情况。

由于电子商务交易的网络环境是开放的,因此在第(1)条语句执行之后,不仅协议合法主体 B 能收到他与主体 A 之间的会话密钥 K_{AB},而且攻击者 I 也能获得 K_{AB},即以下公式成立:

$$believe(B,receive(B,K_{AB})) \tag{1}$$

$$believe(I,receive(I,K_{AB})) \tag{2}$$

由式(2)可得:

$$in(K_{AB},POS_I) \tag{3}$$

由式(3)和密钥保密性形式化定义可以得出,ISI 协议不满足密钥保密性目标。

证毕。

4.2.2　非否认性分析

步骤 1　给出非否认性的形式化定义。

使用新逻辑可以将非否认性目标形式化定义为:

G1　$believe(ADJ,send(A,EOO))$

G2　$believe(ADJ,send(B,EOR))$

步骤 2　验证非否认性目标。

利用新逻辑的公理和推理规则,证明 ISI 协议是否满足上述所给的非否认性目标 G1 和 G2。

1)验证发方非否认性。

证明:假设仲裁方 ADJ 收到了发方非否认证据 EOO,可知

$$believe(ADJ,receive(ADJ,EOO)) \tag{4}$$

即

$$believe(ADJ,receive(ADJ,S(new\_coins,K_{CS}^{-1}))) \tag{5}$$

根据 ADJ 的初始假设集合 INI_S_{ADJ} 可知:

$$believe(ADJ,authenticate(K_{CS},CS)) \tag{6}$$

由式(5)、式(6)和新逻辑的信任公理 AB1 可得

$$believe(ADJ,receive(ADJ,S(new\_coins,K_{CS}^{-1}))\wedge authenticate(K_{CS},CS)) \tag{7}$$

由式(7)和新逻辑的签名规则 SR2,可得:

$believe(ADJ, send(CS, new\_coins))$ (8)

由于 ISI 协议是匿名支付协议，而且协议主体不可能进行不利于自己的欺骗，因此对于仲裁方来说，只需要证明付款有效即可。因此，协议满足发方非否认性目标。

证毕。

2)验证收方非否认性。

证明：假设仲裁方 ADJ 收到了发方非否认证据 EOR，可知：

$believe(ADJ, receive(ADJ, EOR))$ (9)

即

$believe(ADJ, receive(ADJ, S((amount, Tid, date), K_B^{-1})))$ (10)

由于仅凭商家 B 提供的公钥 K_B 不能作为其身份证明，因此 ISI 协议不满足收方非否认性目标。

证毕。

4.2.3 可追究性分析

步骤 1 给出可追究性的形式化定义。

使用新逻辑可以将可追究性目标形式化定义为：

G1 $canprove(B, claim(A, new\text{-}coins))$

G2 $canprove(A, claim(B, (amount, Tid, date)))$

G3 $in(EOO, POS_B)$

G4 $in(EOR, POS_A)$

步骤 2 验证可追究性目标。

1)假定 $in(EOO, POS_B)$ 和 $in(EOR, POS_A)$ 成立，验证 G1 和 G2 是否成立。

证明：假定 $in(EOO, POS_B)$ 成立，即得：

$in(S(new\_coins, K_{CS}^{-1}), POS_B)$ (11)

由式(11)可知

$possess(B, S(new\_coins, K_{CS}^{-1}))$ (12)

由 B 初始假设集合 INI_S_B 可知：

$canprove(B, authenticate(K_{CS}, CS))$ (13)

由式(12)、式(13)和新逻辑的签名规则 SR2 可得：

$canprove(B, claim(CS, new\_coins))$ (14)

由于 ISI 协议是匿名支付协议，因此对于收款方 B 而言，只需证明付款有效，即可认为实现了可追性目标 G1。

假定 $in(EOR, POS_A)$ 成立，即：

$in(S((amount, Tid, date), K_B^{-1}))$ (15)

由式(15)可知：

$possess(A, S((amount, Tid, date), K_B^{-1}))$ (16)

由于 A 不能证明式(17)成立，

$authenticate(k_B, B)$ (17)

因此，就无法推导出式(18)成立，

$canprove(A, claim(B, (amount, Tid, date)))$ (18)

即收款人 B 的非否认证据 EOR 的设计不能满足其非否认目标，因此，可追究性目标 G2 不成立。

2)验证协议运行结束时 G3 和 G4 是否成立。

由于目标 G2 不成立，就可得出协议不满足可追究性目标，因此无需再判断 G3 和 G4 是否成立。

证毕。

4.2.4 公平性分析

步骤 1 给出公平性的形式化定义。

1)协议正常结束时，使用新逻辑可以将公平性目标形式化定义为：

G1 $in(EOO, POS_B)$

G2 $in(EOR, POS_A)$

2)协议第 i 条语句中断执行时，使用新逻辑可以将公平性目标形式化定义为：

G3 $\neg in(EOO, POS_B^{i-1})$(这里 $i=1,2,3,4,5$)

G4 $\neg in(EOR, POS_A^{i-1})$ (这里 $i=1,2,3,4,5$)

步骤 2 验证公平性目标。

证明：根据本文 4.2.3 节中的分析结果，可以得知协议不满足可追究性。由于满足公平性的前提是必须满足可追究性，因此协议不满足公平性目标。

下面讨论在协议不满足公平性的情况下，交易双方中的哪一方占据优势。

假定通信信道是可靠的，参与交易的双方是不诚实的。

当 $i=1$ 时，

$$POS_B^1 \xrightarrow[\text{接收消息(1)}]{\text{初始拥有}} POS_B^0 \cup \{K_{AB}\}$$

$$= \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}\} \cup \{K_{AB}\}$$

$$= \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}, K_{AB}\}$$

当 $i=2$ 时，$POS_B^2 = POS_B^1 = \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}, K_{AB}\}$

当 $i=3$ 时，

$$POS_B^3 \xrightarrow{\text{接收消息(3)}} POS_B^2 \cup \{E((S(coins, K_{CS}^{-1}), SK_A, K\_SES, S\_ID), K_B)\} = \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}, K_{AB}\} \cup \{E((S(coins, K_{CS}^{-1}), SK_A, K\_SES, S\_ID), K_B)\} = \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}, K_{AB}, E((S(coins, K_{CS}^{-1}), SK_A, K\_SES, S\_ID), K_B)\} \xrightarrow{\text{解密}} \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}, K_{AB}, S(coins, K_{CS}^{-1}), SK_A, K\_SES, S\_ID\}$$

当 $i=4$ 时，

$POS_B^4 = POS_B^3 = \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}, K_{AB}, S(coins, K_{CS}^{-1}), SK_A, K\_SES, S\_ID\}$

当 $i=5$ 时，

$$POS_B^5 \xrightarrow{\text{接收消息(5)}} POS_B^4 \cup \{E(S(new\_coins, K_{CS}^{-1}), SK_B)\} = \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}, K_{AB}, S(coins, K_{CS}^{-1}), SK_A, K\_SES, S\_ID\} \cup \{E(S(new\_coins, K_{CS}^{-1}), SK_B)\} = \{SK_B, K_{CS}, K_{AB}, K_A, K_B, K_B^{-1}, K_{AB}, S(coins, K_{CS}^{-1}), SK_A, K\_SES, S\_ID, E(S(new\_coins, K_{CS}^{-1}), SK_B)\} \xrightarrow{\text{解密}} \{SK_B, K_{CS}, K_A, K_B, K_B^{-1}, K_{AB}, S(coins, K_{CS}^{-1}), SK_A, K\_SES, S\_ID, S(new\_coins, K_{CS}^{-1})\}$$

因此，可以得出，当 $i=5$ 时，满足

$in(S(new\_coins, K_{CS}^{-1}), POS_B^5)$

即 $in(EOO, POS_B^5)$ (19)

对 A 而言，

当 $i=1$ 时，$POS_A^1 = POS_A^0$

当 $i=2$ 时，

$$POS_A^2 \xrightarrow[\text{接收消息(2)}]{\text{初始拥有}} POS_A^0 \cup \{E(K_B, K_{AB})\}$$

$$= \{SK_A, K_{CS}, K_{AB}, K_A, K_A^{-1}\} \cup \{E(K_B, K_{AB})\}$$

$$= \{SK_A, K_{CS}, K_{AB}, K_A, K_A^{-1}, E(K_B, K_{AB})\}$$

$$\xrightarrow{\text{解密}} \{SK_A, K_{CS}, K_{AB}, K_A, K_A^{-1}, K_B\}$$

当 $i=3,4,5$ 时，

$POS_A^3 = POS_A^4 = POS_A^5 = POS_A^2 = \{SK_A, K_{CS}, K_{AB}, K_A,$

$K_A^{-1}, K_B\}$

很显然，当 $i=5$ 时，

$\neg in(S((amount, Tid, date), K_B^{-1}), POS_A^5)$

即 $\neg in(EOR, POS_A^5)$ (20)

由式(19)和式(20)得出，如果收款方 B 不执行协议第(6)步，则收款方 B 占优势，而付款方 A 处于劣势。

证毕。

4.2.5 原子性分析

步骤 1 给出原子性的形式化定义。

使用新逻辑可以将原子性目标形式化定义为

G A1 $\vee$ A2

A1 $in(new\text{-}coins, REV_B) \wedge in((amount, Tid, date), REV_A)$(当协议正常结束时)

A2 $\neg in(new\text{-}coins, REV_B) \wedge \neg in((amount, Tid, date), REV_A)$(当协议异常终止时)

步骤 2 验证原子性目标。

利用新逻辑的公理和推理规则，分别分析协议主体 A 和 B 每一步接收的消息，判断是否包含所交换的信息，用以验证原子性目标。

证明：1)在通信信道可靠的情况下，协议将正常结束。

由于协议前 4 条语句中不含原子性目标中所含的内容，因此，只需分析协议语句(5)和语句(6)。

首先，分析协议语句(5)。

$believe(B, receive(B, E(S(new\_coins, K_{CS}^{-1}), SK_B)))$ (21)

由 B 的初始拥有集合 $POS_B^0 = \{SK_B, K_{CS}\}$ 可知：

$possess(B, SK_B)$ (22)

由式(21)、式(22)和新逻辑的密文理解规则 CCR1 可得：

$believe(B, receive(B, S(new\_coins, K_{CS}^{-1})))$ (23)

由 B 的初始拥有集合 $POS_B^0 = \{SK_B, K_{CS}\}$ 可知：

$possess(B, K_{CS})$ (24)

由式(23)、式(24)和新逻辑的签名规则 SR1 可得，

$believe(B, receive(B, new\_coins))$ (25)

即 $in(new\text{-}coins, REV_B)$ (26)

接下来，分析协议语句(6)。

$believe(A, receive(A, E(S((amount, Tid, date), K_B^{-1}), SK_A)))$ (27)

由 A 的初始拥有集合 $POS_A^0 = \{SK_A, K_{CS}, K_{AB}\}$ 可知：

$possess(A, SK_A)$ (28)

由式(27)、式(28)和新逻辑的密文理解规则 CCR1 可得：

$believe(A, receive(A, S((amount, Tid, date), K_B^{-1})))$ (29)

由 A 的拥有集合 $POS_A^5 = POS_A^0 \cup \{K_B\}$ 可知：

$possess(A, K_B)$ (30)

由式(29)、式(30)和新逻辑的签名规则 $SR2$ 可得：

$believe(A, receive(A, (amount, Tid, date)))$ (31)

即

$in((amount, Tid, date), REV_A)$ (32)

由式(26)和式(32)可得出，原子性目标的子目标 A1 成立。

2)在通信信道不可靠的情况下，当协议前 5 条语句中的任何一条语句中断时，都不会执行协议语句(5)和语句(6)，因此可得出，交易双方都得不到所交换的信息，即原子性目标的子目标 A2 成立。

因此，结合情况 1)和 2)可得出，在最好情况下，即通信信道是可靠的，语句不会中断执行，并且交易双方都是诚实主体；或者在通信信道不可靠，但是只有在协议前 4 条语句中的任何一条出现中断执行的情况下，协议的原子性目标才成立。

同理可以分析，下述 3 种情况，协议不满足原子性。

情况 1：通信信道不可靠，交易双方都是诚实的，但是第 6 条语句中断执行，即出现网络故障，协议异常终止，协议无法满足原子性。

情况 2：通信信道可靠，但是付款方 B 不诚实，即 B 不执行协议第(6)步，则协议无法实现原子性。

情况 3：通信信道不可靠，交易双方也不诚实。

很显然，这是最坏的情况，协议不可能满足原子性。

证毕。

结束语 本文在对现有典型电子商务安全协议逻辑分析方法研究的基础上，提出了一种新的逻辑分析方法。该逻辑方法不仅在一定程度上弥补了现有典型逻辑分析方法在安全属性分析方面的局限性，而且能够分析多种电子商务安全协议安全属性。此外，新逻辑进一步增强了对密码原语的分析能力，具有分析基于混合密码原语体制的电子商务安全协议的能力。

由于电子商务协议具有多种安全属性，而且随着电子商务和网络信息技术的发展，新的安全需求还会不断增加，因此需要进一步提高本文所提出的新逻辑分析方法的分析能力。同时必须认识到，对电子商务安全协议形式化分析方法的研究任重而道远。

参 考 文 献

[1] Kailar R. Accountability in Electronic Commerce Protocols [J]. IEEE Transactions on Software Engineering, 1996, 22(5): 313-328

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

[3] 卿斯汉. 一种电子商务安全协议形式化分析方法[J]. 软件学报, 2005, 16(10): 1757-1765

[4] 王彩芬. 电子商务安全协议的形式分析与设计[D]. 西安：西安电子科技大学, 2002

[5] 王彩芬，葛建华. 一种分析电子商务安全协议的新方法[J]. 计算机学报, 2004, 27(4): 507-515

[6] 王茜，杨德礼. 一种基于 SVO 逻辑的新形式化验证方法[J]. 计算机集成制造系统, 2004, 10(3): 342-351

[7] 黎波涛，罗军舟. 不可否认协议时限性的形式化分析[J]. 软件学报, 2006, 17(7): 1510-1516

[8] Knowledge S P. belief, and semantics in the analysis of cryptographic protocols[J]. Journal of Computer Security, 1992, 1(3): 317-334

[9] Carnap R. Meaning And Necessity-A Study in Semantics and Modal logic[M]. Clarke Press, 2007

[10] Medvinsky G, Neuman B C. Netcash: a design of practical electronic currency on the Internet [A]// Proceedings of the First ACM Conference on Computer and Communications Security [C]. USA: ACM Press, 1993: 102-106