一种分析电子商务协议的新工具*

周典萃，卿斯汉，周展飞

(中国科学院 软件研究所,北京 100080);
(中国科学院 信息安全技术工程研究中心,北京 100080)
E-mail: qsihan@yahoo.com
http://www.ercist.ac.cn

摘要：提出了一种新的形式化分析方法,可用于分析电子商务协议.与Kailar逻辑相比,它有3个优点:(1)能够有效地分析协议的公平性,在进行公平性分析时充分考虑了通信信道的可靠性;(2)初始化拥有集合只依赖于环境,不需要人为地引入初始化假设;(3)增加了密文理解规则,能够有效地分析包含有签过名的加密公式的消息.

关键词：可追究性;电子商务;公平性;逻辑分析;协议
中图法分类号：TP309 **文献标识码**：A

近年来,通过设计和发展电子商务协议来开展网上交易逐渐成为一个热点.一个设计正确的电子商务协议必须遵循可追究性和公平性两个重要原则.可追究性是指电子商务协议必须具备这一机制,它迫使交易双方对自己的行为负责.如果缺乏可追究性,交易双方则容易引起争议.公平性是指如果交易成功,交易双方应该获得他们要取得的电子货物;或者,如果交易失败,交易双方谁也不能获得要取得的电子货物.

Kailar[1]提出了一种用于分析电子商务协议的可追究性的形式化分析方法,简称Kailar逻辑.它是目前电子商务协议形式化分析的主要工具.经过研究,我们发现Kailar逻辑存在3个缺陷[2]:(1)不能分析协议的公平性;(2)列举初始化假设是非形式化的,不当地引入初始化假设会导致协议分析的失败;(3)无法理解包含签过名的密文的协议语句.

本文提出了一种新的形式化方法,用于分析电子商务协议的可追究性和公平性.在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化拥有集合,它由一些公式组成.随着协议语句的执行,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收方非否认两个基本目标[3]来达到的.发方非否认是指电子商务协议提供给接收方一个不可抵赖的证据,这个证据可以证明接收方接收到的消息的内容和发送方发送的消息的内容是相同的.通常用POO(proof-of-origin)表示发方非否认证据.收方非否认是指电子商务协议提供给发送方一个不可抵赖的证据.这个证据可以证明接收方接收到的消息的内容与发送方发送的消息的内容是相同的.通常用POR(proof-of-receipt)表示收方非否认证据.在新的形式化分析方法中,通过验证POO属于接收者的最终拥有集合并且POR属于发送者的最终拥有集合是否成立来验证协议的可追究性.

* 收稿日期：1999-06-29；修改日期：2000-04-21
基金项目：国家自然科学基金资助项目(60083007);国家重点基础研究发展规划973资助项目(G1999035810)
作者简介：周典萃(1971-),男,湖南邵阳人,工程师,主要研究领域为信息安全基础理论;卿斯汉(1939-),男,湖南邵阳人,研究员,博士生导师,主要研究领域为信息安全理论和技术;周展飞(1959-),男,江苏苏州人,博士,副研究员,主要研究领域为密码理论,应用数学.

协议的公平性包含两层含义: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,任何一方都不占有优势,或者说,消息接收者收到了POO当且仅当消息发送者收到了POR.在新的形式化分析方法中,通过验证协议的执行在任何一步异常终止时,POO属于接收者的拥有集合是否当且仅当POR属于发送者的拥有集合来验证协议的公平性.

1 新的形式化分析方法

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,SK: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.

$P \ni X$: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.

$P \succ X$:主体P能够证明公式X.

$\xrightarrow{K_P} P$: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.

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,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,或者通过TTP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两种形式之一:

$P \rightarrow Q|TTP:M$——表示主体P向主体Q或者TTP发送消息M.

$TTP \rightarrow P:M$——表示主体 TTP 向主体 P 发送消息 M.

$P \longleftrightarrow TTP:M$——表示主体 P 通过一次或多次 ftp 操作[4]从主体 TTP 取得消息 M. 这一基于 ftp 的方法是由 Zhou Jianying 和 Dieter Gollman 提出的[5]. 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 $i(1 \leqslant i \leqslant n)$ 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 $P \rightarrow Q:M$,不妨设 $M = (\{M'\}_{K'}, \{M''\}_{K''}, \ldots)$,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 $Q|TTP \rightarrow P:M$ 或者 $P \longleftrightarrow TTP:M$,那么 $O_p^i = O_p^{i-1} \cup \{M\}$.

(3) 如果第 i 条协议语句为 $Q \rightarrow TTP:M$,或者 $TTP \rightarrow Q:M$,或者 $Q \longleftrightarrow TTP:M$,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 $\{x\}_K \in O_p^i$.

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. 我们用记号 $P \rightarrow x$ 表示主体 P 对公式 x 负有责任. 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 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 $B > A \rightarrow m$.

(2) 接收方非否认是由 B 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 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 $A > B \rightarrow m$.

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 $A|B \rightarrow B|A|TTP:M$ 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 $TTP \rightarrow A|B:M$ 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,因为 TTP 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 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 $A|B \longleftrightarrow TTP:M$ 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 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,$POO \in O_B^i$ 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.

1.3 协议分析的步骤

新的形式化方法分析协议分为以下4个步骤.前3个步骤是对协议可追究性的分析,第4步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.下面列举用于推导的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.

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

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

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

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

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.

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

这条规则是新引入的,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 对密钥 K 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.

$$\frac{A\succ TTP\rightarrow M}{A\succ A\ni M}$$

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

这条规则是新引入的,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.

$$\frac{P \succ CA \rightarrow (K_b, B)}{P \succ \xrightarrow{K_b} B}$$

这条规则是新引入的,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.

(3) 验证在协议结束时,$POO \in O_B$ 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,$POO \in O_B^{-1}$ 当且仅当 $POR \in O_A^{-1}$.

2 协议分析的例子

本节利用上一节提出的新形式化方法对 3 个协议进行分析,并把分析结果与 Kailar 逻辑的分析结果进行比较.

2.1 ISI 支付协议的分析

以下的支付协议是由 Medvinsky 和 Neuman 提出来的[6],其目的是付款人 A 向收款人 B 付款,A 保持匿名.

(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) $B \rightarrow A: \{\{amount, Tid, date\}_{K_b^{-1}}\}_{SK_a}$.

在协议的(1)、(2)步,A 取得 B 的公开密钥,在第(3)步,A 把电子货币、想获得的服务的标识号 S_id和密码 K_ses 用 B 的公开密钥加密后传送给 B.使用 K_{cs},B 可以验证电子货币的有效性.然后,B 通过第(4)步将电子货币传送给货币服务方 CS(currency server),如果这笔钱尚未花掉,CS 通过第(5)步支付给 B.最后,B 将收据传送给 A.

在利用Kailar 逻辑分析本协议时,我们发现它不满足可追究性[2].利用新的形式化方法可以发现,本协议除了不满足可追究性以外,它还是非公平的.

协议的分析过程如下:

(1) 列举初始化拥有集合如下.在协议运行的初始状态中,K_{cs}可以用于验证主体 CS 的身份,交易双方 A 和 B 拥有 CS 的公开密钥 K_{cs}.

$$O_A = \{K_{cs}\}$$

$$O_B = \{K_{cs}\}$$

$$A \succ \xrightarrow{K_{cs}} CS$$

$$B \succ \xrightarrow{K_{cs}} CS$$

(2) 然后,列举发方非否认证据和收方非否认证据如下:

$$Proof\_of\_A=\{new\_coins\}_{K_{cs}^{-1}},$$

$$Proof\_of\_B=\{amount,Tid,date\}_{K_b^{-1}}.$$

现在假定 $Proof\_of\_A\in O_B$ 成立,即 $\{new\_coins\}_{K_{cs}^{-1}}\in O_B$, $B\ni\{new\_coins\}_{K_{cs}^{-1}}$,再由 $B\succ\xrightarrow{K_{cs}}CS$,利用签名规则可得

$$B\succ CS\rightarrow new\_coins. \tag{G_1}$$

由于本协议是一个匿名支付协议,对于收款人 B 来说,他只需要证明付款是有效的.因此,式(G_1)满足付款人 A 非否认目标.

现在假定 $Proof\_of\_B\in O_A$ 成立,$\{amount,Tid,date\}_{K_b^{-1}}\in O_A$,即

$$A\in\{amount,Tid,date\}_{K_b^{-1}}, \tag{$*$}$$

但是无法证明 $A\succ\xrightarrow{K_b}B$,因此 A 无法推导出 $A\succ B\rightarrow\{amount,Tid,date\}$.协议设计者设计的收款人(即 B)非否认证据 $Proof\_of\_B$ 不能达到收款人非否认目标.新的形式化方法发现了 ISI 支付协议不满足可追究性.

本协议第(1)、(2)步的目的是付款人 A 获得收款人 B 的公开密钥 $K\_\{b\}$,但实际上 A 获得的 K_b 不能用于验证 B 的电子签名.所以,可将原协议的第(1)、(2)步修改如下:

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

(2) $B\rightarrow A:\{\{K_b,B\}_{K_{CA}^{-1}}\}_{K_{ab}}$.

对于修改过的协议,现在仍然假定 $Proof\_of\_B\in O_A$ 成立,即公式($*$)成立,那么由于 $K_{ab}\in O_A^1\subset O_A$ 和 $\{\{K_b,B\}_{K_{CA}^{-1}}\}_{K_{ab}}\in O_A^2\subset O_A$,所以 $\{\{K_b,B\}_{K_{CA}^{-1}}\}\subset O_A$,即 $A\in\{\{K_b,B\}_{K_{CA}^{-1}}\}$.

由签名规则可知,$A\succ CA\rightarrow(K_b,B)$成立,再运用电子证书规则,$A\succ\xrightarrow{K_b}B$ 成立.

由以上公式和公式($*$),运用签名规则,$A\succ B\rightarrow\{amount,Tid,date\}$,所以,修改过的协议对收款人 B 非否认证据 $Proof\_of\_B$ 的设计达到了收款人非否认的目标.

(4) 下面我们对改进过的协议进行公平性分析.考虑最好的情况,假定通信信道是可靠的.由于参与交易的双方 A 和 B 是不诚实的,那么协议语句(1)、(2)、(3)、(4)、(6)是可中断的.

协议是公平性的,等价于以下命题成立:

$$Proof\ of\ A\in O_B^i \quad 当且仅当 \quad Proof\_of\_B\in O_A,\ i=0,1,2,3,4,5.$$

现在来看 O_B^5.

$$O_B^5=O_B^4\cup\left\{\left\{\{new\ \ coins\}_{K_{cs}^{-1}}\right\}_{SK_b}\right\},$$

$$O_B^4=O_B^3\cup\left\{\left\{\{coins\}_{K_{cs}^{-1}},SK_b,transaction\right\}_{K_{cs}}\right\},\ SK_b\in O_B^4\subset O_B^5,$$

所以 $\{new\ \ coins\}_{K_{cs}^{-1}}\in O_B^5$,即 $\$\ proof\ \ of\ \ A\in O_B^5$.再来看 O_A^5.

$$O_A^2=\{K_{cs},K_b\},$$

$$O_A^5=O_A^3=O_A^2\cup\left\{\left\{\{coins\}_{K_{cs}^{-1}},SK_a,K_{\_ses},S_{\_id}\right\}_{K_b}\right\}=\{K_{cs},K_b,\{coins\}_{K_{cs}^{-1}},SK_a,K_{\_ses},S_{\_id}\}.$$

O_A^5 中不包含 K_b^{-1} 及任何用 K_b^{-1} 签过名的公式,显然 $Proof\_of\_B\in O_A^5$ 不成立.

所以,本协议是非公平的.收款人 B 可以不执行协议语句(6)而使协议的执行终止,这样,B 能够证明 A 的付款是有效的,而 A 无法证明 B 应提供相应的服务.

2.2 CMP1 协议的分析

以下的 CMP1 协议是由 Robert Deng 和 Li Gong 等人提出的认证电子邮件协议[7]. 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.

(1) $A\rightarrow B: h(m), \{k\}_{K_{TPP}}, \{\{m\}_{K_a^{-1}}\}_k$.

(2) $B\rightarrow A: \{h(m)\}_{K_b^{-1}}, \{k\}_{K_{TPP}}, \{\{m\}_{K_a^{-1}}\}_k$.

(3) $TTP\rightarrow B: \{\{m\}_{K_a^{-1}}\}_{K_{TPP}^{-1}}$.

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

其中 k 是 A 与 TTP 共享的会话密钥.

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 $\{k\}_{K_{TPP}}$ 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 $\{m\}_{K_a^{-1}}$,然后在第(3)步将它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.

Kailar 逻辑在分析本协议时由于引入了不当的初始化假设而认为它满足可追究性[2]. 新的形式化方法发现本协议有两个弱点:第一,它只满足较弱的可追究性;第二,它在通信信道不可靠的条件下是非公平的. 协议的分析过程如下:

(1) 首先,列举初始化拥有集合.

$$O_A^0=\{K_a^{-1}, K_a, K_b, K_{TTP}\},$$

$$O_B^0=\{K_a, K_b^{-1}, K_b, K_{TTP}\},$$

$$A\succ(\xrightarrow{K_b}B, \xrightarrow{K_{TTP}}TTP),$$

$$B(\xrightarrow{K_a}B, \xrightarrow{K_{TTP}}TTP).$$

(2) 然后,列举发方非否认证据和收方非否认证据如下:

$$POO=\{m\}_{K_a^{-1}},$$

$$POR=\{\{h(m)\}_{K_b^{-1}}, (b,m)\}_{K_{TTP}^{-1}}.$$

现在假定 $POO\in O_B$ 成立,即 $\{m\}_{K_a^{-1}}\in O_B$, $B\ni\{m\}_{K_a^{-1}}$. 再由 $B\succ\xrightarrow{K_a}A$,利用签名规则可得

$$B\succ A\rightarrow m. \tag{G1}$$

消息接收者 B 可以证明消息发送者 A 对消息 m 负有责任. 协议设计者设计的发方非否认证据 POO 满足可追究性目标.

现在假定 $POR\in O_A$ 成立,即 $\{\{h(m)\}_{K_b^{-1}}, (B,M)\}_{K_{TTP}^{-1}}\in O_A$. 由于 $K_{TTP}\in O_A^0\subset O_A$,所以 $\{h(m)\}_{K_b^{-1}}\in O_A$.

由 $A\succ\xrightarrow{K_b}B$,利用签名规则可得

$$A\succ B\rightarrow h(m). \tag{G2a}$$

再由 $\{\{h(m)\}_{K_b^{-1}}, (B,m)\}_{K_{TTP}^{-1}}\in O_A$ 和 $A\succ\xrightarrow{K_{TTP}}TTP$,利用签名规则可得 $A\succ TTP\rightarrow(\{h(m)\}_{K_b^{-1}}, (B,m))$,于是 $A\succ TTP\rightarrow(B,m)$.

由于 TTP 在协议中担任传递者的角色,利用传递规则可得

$$A\succ B\ni m. \tag{G2b}$$

由(G2a)和(G2b)连接得到

$$A\succ(B\rightarrow h(m))\wedge(B\ni m). \tag{G2}$$

消息发送者 A 能够证明消息接收者 B 对 $h(m)$ 负有责任和 B 拥有 m,(G2)是一种较弱的可追究性,它比可追究性目标 $A\succ B\rightarrow m$ 要弱一些.在未检查 $h(m)$ 和 m 的一致性之前,无法认为协议设计者设计的收方非否认证据 POR 满足可追究性目标.

(3) 这一步将验证当协议运行结束时,是否可以确保 A 和 B 取得相应的证据.

由于 $O_B^3=O_B^0\cup\{\{\{m\}_{K_a^{-1}}\}_{K_{TTP}^{-1}}\}$,所以 $\{\{m\}_{K_a^{-1}}\}_{K_{TTP}^{-1}}\in O_B^3\subset O_B$.

又 $K_{TTP}\in O_B^0\subset O_B$,所以 $\{m\}_{K_a^{-1}}\in O_B$.

即 $POO\in O_B$,当协议运行结束时,B 可以取得 POO.

由于 $O_A^4=O_A^3\cup\{\{\{h(m)\}_{K_b^{-1}},(B,m)\}_{K_{TTP}^{-1}}\}$,

$$\{\{h(m)\}_{K_b^{-1}},(B,m)\}_{K_{TTP}^{-1}}\in O_A$$

即 $POR\in O_A$,当协议运行结束时,A 可以取得 POR.

(4) 在信道不可靠的条件下,协议语句(1)~(4)是可中断的.协议是公平性的,等价于下面的命题成立:$POO\in O_B^i$ 当且仅当 $POR\in O_A^i$,$i=1,2$.

现在来看 O_B^3.

$$O_B^5=O_B^2\cup\{\{\{m\}_{K_a^{-1}}\}_{K_{TTP}^{-1}}\},\{\{m\}_{K_a^{-1}}\}_{K_{TTP}^{-1}}\in O_B^3.$$

又 $K_{TTP}\in O_B^0\subset O_B^3$,所以 $\{m\}_{K_a^{-1}}\in O_B^3$.

即 $POO\in O_B^3$ 成立.

再来看 O_B^3.

$$O_A^3=O_A^4=\{K_a^{-1},K_a,K_b,K_{TTP},k,\{m\}_{K_a^{-1}}\},$$

显然 $POR\in O_A^5$ 不成立.

所以,在信道不可靠的条件下,本协议是非公平的.

2.3 非否认协议(Zhou-Gollman)的分析

下面介绍 J. Zhou 和 D. Gollman 提出的非否认协议[5],它适用于在信道不可靠的条件下签订电子合同.

(1) $A\rightarrow B:\{M\}_K,\{\{M\}_K\}_{K_a^{-1}}$

(2) $B\rightarrow A:\{\{M\}_K\}_{K_b^{-1}}$

(3) $A\rightarrow TTP:\{K,\{K\}_{K_a^{-1}}\}_{K_{a,TTP}}$

(4) $B\longleftrightarrow TTP:K,\{K\}_{K_{TTP}^{-1}}$

(5) $A\longleftrightarrow TTP:\{K\}_{K_{TTP}^{-1}}$

其中 $k_{a,ttp}$ 是 A 与 TTP 共享的密钥.

第(1)、(2)步,A 选择一个密钥 K 对 M 进行加密,然后连同他对 $\{M\}_k$ 的签名发送给 B.B 对 $\{M\}_k$ 签名后返回给 A.第(3)步,A 把密钥 K 连同他对 K 的签名用他与 TTP 的共享密钥加密后发送给 TTP.第(4)、(5)步,B 通过 ftp 操作从 TTP 获取 K 和 TTP 对 K 的签名.A 通过 ftp 操作从 TTP 获得 TTP 对 K 的签名.

由于 Kailar 逻辑无法分析那些签名的加密消息,所以它不能正确分析本协议[2].利用新的形式化方法可以证明本协议满足可追究性,并且在信道不可靠的条件下是公平的,达到了协议设计者期待的目标.

协议的分析过程如下：

(1) 首先，列举初始化拥有集合. 在协议运行的初始状态中，$k_{a,ttp}$是 A 与 TTP 共享的密钥.

$$O_A^0=\{K_a^{-1},K_a,K_b,K_{TTP}\},$$

$$O_B^0=\{K_a,K_b^{-1},K_b,K_{TTP}\},$$

$$A\succ(\xrightarrow{K_b}B,\xrightarrow{K_{TTP}}TTP),$$

$$B\succ(\xrightarrow{K_a}A,\xrightarrow{K_{TTP}}TTP).$$

(2) 然后，列举发方非否认证据和收方非否认证据如下：

$$POO=(\{\{m\}_K\}_{K_a^{-1}},\{K\}_{K_{TTP}^{-1}}),$$

$$POR=(\{\{m\}_K\}_{K_b^{-1}},\{K\}_{K_{TTP}^{-1}}).$$

现在假定 $POO\in O_B$ 成立，即$(\{\{m\}_K\}_{K_a^{-1}},\{K\}_{K_{TTP}^{-1}})\in O_B$，则 $B\ni\{\{m\}_K\}_{K_a^{-1}}$ 和 $B\ni\{K\}_{K_{TTP}^{-1}}$ 成立.

由 $B\ni\{K\}_{K_{TTP}^{-1}}$和 $B\succ\xrightarrow{K_{TTP}}TTP$，利用签名规则可得

$$B\succ TTP\rightarrow K.$$

由于 TTP 在协议中担任传递者的角色，利用传递规则可得

$$B\succ A\ni K. \tag{1}$$

由 $B\ni\{\{m\}_K\}_{K_a^{-1}}$和 $B\succ\xrightarrow{K_a}A$，利用签名规则可得

$$B\succ A\rightarrow\{m\}_K. \tag{2}$$

由式(1)和式(2)，利用密文理解规则，

$$B\succ A\rightarrow m.$$

类似地，假定 $POR\in O_A$ 成立，可以证明：

$$A\succ B\rightarrow m.$$

因此，协议设计者对 POO 和 POR 的设计满足可追究性.

(3) 这一步将验证当协议运行结束时，是否可以确保 A 和 B 取得相应的证据.

由于 $O_A^2=O_A^1\cup\{\{\{m\}_K\}_{K_b^{-1}}\},\{\{m\}_K\}_{K_b^{-1}}\in O_A^2\subset O_A$.

又 $O_A^5=O_A^4\cup\{\{K\}_{K_{TTP}^{-1}}\},\{K\}_{K_{TTP}^{-1}}\in O_A^2\subset O_A$.

所以，$(\{\{m\}_K\}_{K_b^{-1}},\{K\}_{K_{TTP}^{-1}})\in O_A$.

即 $POR\in O_A$，当协议运行结束时，消息发送者 A 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 B 可以取得 POO.

(4) 在信道可靠的条件下，协议语句(1)～(3)是可中断的. 协议是公平性的，等价于以下命题成立：

$$POO\in O_B^i \quad \text{当且仅当} \quad POO\in O_A^i,i=0,1,2.$$

$$O_A^2=O_A^0\cup\{\{m\}_K,\{\{m\}_K\}_{K_a^{-1}},\{\{m\}_K\}_{K_b^{-1}}\}.$$

由于 O_A^2 中不含有公式$\{K\}_{K_{TTP}^{-1}}$，因此 $POR\in O_A^2$ 不成立.

$O_A^1\subset O_A^2,O_A^0\subset O_A^2$，故 $POR\in O_A^i,i=0,1,2$ 均不成立.

类似地，可以验证 $POO\in O_B^i,i=0,1,2$ 均不成立.

以上证明了在信道不可靠的条件下,本协议是公平的.

(5) 在利用新的形式化方法对本协议的分析过程中,我们发现协议语句存在冗余.以协议语句(1)为例.

$$O_B^1=O_B^0 \cup \{\{m\}_K,\{\{m\}_K\}_{K_A^{-1}}\}$$

由于 $K_a \in O_B^0$,因此 $\{m\}_K \in O_B^0 \cup \{\{\{m\}_K\}_{K_a^{-1}}\}$.

$$O_A^1=O_A^0 \cup \{\{m\}_K,\{\{m\}_K\}_{K_a^{-1}}\}$$

由于 $K_a \in O_A^0$,同样地,$O_A^1=O_A^0 \cup \{\{m\}_K,\{\{m\}_K\}_{K_a^{-1}}\}$.

协议语句(1)可优化为

$$A \rightarrow B:\{\{m\}_K\}_{K_a^{-1}}.$$

对于协议语句(1)优化后,协议的拥有集合 O_A^1 和 O_B^1 与原协议是完全相同的.根据新的形式化方法,可以认为优化后的协议语句(1)与原协议语句(1)是等价的.

此外,在协议运行的初始状态中,需要假定 A 与 TTP 之间有一个共享密钥 $K_{a,\mathrm{ttp}}$,而 $K_{a,\mathrm{ttp}}$ 仅在协议语句(3)中运用过一次,其目的是 A 把公式 $\{K,\{K\}_{K_a^{-1}}\}$ 加密传送给 TTP,使 B 和其他主体不能截获这一公式.在协议语句(3)中,我们建议用 K_{TTP} 替代 $K_{a,\mathrm{ttp}}$,因为只有 TTP 拥有 K_{TTP} 的解密密钥 K_{TTP}^{-1},同样可以防止 B 和其他主体截获这一公式.这样,在协议运行的初始状态中,不再需要假定 A 与 TTP 之间有一共享密钥 $K_{a,\mathrm{ttp}}$.建议将这一协议修改如下:

(1) $A \rightarrow B:\{\{m\}_K\}_{K_a^{-1}}$;

(2) $A \rightarrow B:\{\{m\}_K\}_{K_a^{-1}}$;

(3) $A \rightarrow TTP:\{\{K\}_{K_a^{-1}}\}_{K_{\mathrm{TTP}}}$;

(4) $B \longleftrightarrow TTP:\{K\}_{K_{\mathrm{TTP}}^{-1}}$;

(5) $A \longleftrightarrow TTP:\{K\}_{K_{\mathrm{TTP}}^{-1}}$.

利用新的形式化方法可以验证,修改过的协议的所有拥有集合和最终拥有集合与原协议是相同的.因此,两个协议等价.

3 结 论

与 Kailar 逻辑相比,新的形式化方法主要有 3 个优点:

(1) 新方法能够有效地进行公平性分析.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) 新方法增加了密文理解规则,它能够有效地分析包含签过名的加密公式的消息.

(3) 新方法中的初始化拥有集合只依赖于环境,不需要人为地引入初始化假设,因而是一个更为严格的形式化分析方法.

References:

[1] Kailar, R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, 1996,2(5):313~328.

[2] Zhou, Dian-cui, Qing, Si-han, Zhou, Zhan-fei. Limitations of Kailar logic. Journal of Software, 1999,10(12):1238~1245 (in Chinese).

[3] ISO/IEC 3rd CD 13888-1. Information technology---security techniques Part 1: general model. ISO/IEC JTC11/SC24 N1274, 1996.

[4] Postel, J., Reynolds, J. File transfer protocol. RFC 959, 1985.

[5] Zhou, Jian-ying, Gollman, D. A fair non-repudiation protocol. In: Proceedings of the 1996 IEEE Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1996. 55~61.

[6] Medvinsky, G., Neuman, B.C. Netcash: a design of practical electronic currency on the Internet. In: Denny, D., Pyle, R., eds. Proceedings of the ACM Conference on Computer and Communication Security. New York: ACM Press, 1993. 76~83.

[7] Deng, R.H., Gong, L.. Practical protocols for certified electronic mail. Journal of Network and Systems Management, 1996,4(3):279~297.

附中文参考文献:

[2] 周典萃,卿斯汉,周展飞. Kailar 逻辑的缺陷. 软件学报,1999,10(2):1238~1245.

A New Approach for the Analysis of Electronic Commerce Protocols*

ZHOU Dian-cui, QING Si-han, ZHOU Zhan-fei

(*Institute of Software, The Chinese Academy of Sciences, Beijing* 100080, *China*);
(*Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing* 100080, *China*)
E-mail: qsihan@yahoo.com
http://www.ercist.ac.cn

Abstract: In this paper, a new framework is proposed for the analysis of electronic commerce protocols. Comparing to the framework proposed by Kailar, it has three major improvements. Firstly, it can analyze fairness of protocols efficiently. In the analysis of fairness, it takes the reliability of communication channels into consideration. Secondly, the initial possesion set depends on environment in stead of human beings. At last, by introducing the cipher text understanding rule the new framework can analyze the message which includes signed cipher text.

Key words: accountability; electronic commerce; fairness; logical analysis; protocol

* Received June 29, 1999; accepted April 21, 2000
Supported by the National Natural Science Foundation of China under Grant No. 60083007; the National Grand Fundamental Research 973 Program of China under Grant No. G1999035810