一种电子商务协议形式化分析方法*

卿斯汉[1,2+]

[1](中国科学院 软件研究所 信息安全技术工程研究中心,北京 100080)

[2](北京中科安胜信息技术有限公司,北京 100080)

A Formal Method for Analyzing Electronic Commerce Protocols

QING Si-Han[1,2+]

[1](Engineering Research Center for Information Security Technology, Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

[2](Beijing ZhongkeAnsheng Corporation of Information Technology, Beijing 100080, China)

+ Corresponding author: Phn: +86-10-62635150, Fax: +86-10-62635150, E-mail: qsihan@ercist.iscas.ac.cn

Received 2004-05-25; Accepted 2005-06-22

Qing SH. A formal method for analyzing electronic commerce protocols. *Journal of Software*, 2005,16(10): 1757−1765. DOI: 10.1360/jos161757

Abstract: A formal method which can be used to analyze security properties such as accountability and fairness in electronic commerce protocols is presented. Compared with the previous work, the main contributions are the following. Firstly, a formal definition is given to the possession set of each protocol participant, and the initial possession set depends only on the environment. Secondly, the set of initial state assumptions is divided into three categories: basic assumptions, trust assumptions, and protocol comprehension assumptions, in order to avoid analysis errors caused by informal initial state assumptions. Thirdly, the set of trust assumptions is articulated by formal specification at a lower level of granularity, exposing the essence of the protocol. Fourthly, establishing an axiom system makes the new approach more rigorous and expressive.

Key words: formal analysis; electronic commerce protocol; accountability; fairness; TTP

摘 要: 提出了一种新颖的形式化方法,可以用于分析电子商务协议的安全性质,例如可追究性和公平性.与以前的工作相比较,主要贡献在于:(1) 对协议主体的拥有集合给出了形式化定义,且主体的初始拥有集合只依赖于环境;(2) 将协议的初始状态假设集合分为 3 类:基本假设集合、可信假设集合和协议理解假设集合,避免了因非形式化的初始假设而产生的分析错误;(3) 对可信假设作细粒度的形式化规范,揭示协议的内涵;(4) 建立公理系统,使新方法更为严格与合理.

关键词: 形式化分析;电子商务协议;可追究性;公平性;可信第三方

中图法分类号: TP309 文献标识码: A

* Supported by the National Natural Science Foundation of China under Grant Nos.60083007, 60573042 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973)); the Beijing Natural Science Foundation of China under Grant No.4052016 (北京市自然科学基金)

作者简介: 卿斯汉(1939−),男,湖南隆回人,研究员,博士生导师,主要研究领域为信息系统安全理论和技术.

近年来,电子商务的交易量迅猛增加,因而电子交易的安全性问题日益受到重视.除公开密钥基础设施 PKI 是保障电子商务安全的重要工具之外,安全的电子商务协议是安全地进行电子交易的基础.以往,安全协议的研究重点是认证协议.认证协议的设计是一个众所周知的难题,常因一些细微的问题产生安全缺陷[1,2].为此,一些分析认证协议的形式化工具应运而生,其中 BAN 逻辑方法[3]与 BAN 类逻辑方法[4]最为著名.BAN 类逻辑是一种模态逻辑,通过主体信念集合的演化推断认证协议的正确性与安全性.

电子商务协议比认证协议更为复杂,它不仅需要满足认证协议的安全需求,还需要考虑认证协议中未涉及到的若干安全性质,其中最重要的是可追究性与公平性.所谓可追究性,是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以保护自身的利益.所谓公平性,是指协议在运行的任何一步终止时,参与协议的主体都处于同等的地位,任何一方都不占据优势.

BAN 逻辑不能分析电子商务协议的可追究性,因为它用于证明主体相信某个公式.相反,证明可追究性,则需要向第三方证明另一个主体对某个公式负有责任.因此,Kailar 提出了一种新的逻辑分析方法[5],扩展了信念逻辑的分析范围,可以用于分析电子商务协议的可追究性.虽然 Kailar 逻辑仍然是形式化分析电子商务协议的主要工具之一,但是,Kailar 逻辑也有一些不足之处[6].文献[7]对 Kailar 逻辑进行改进,提出了一种新的逻辑分析方法,可以同时分析电子商务协议的可追究性与公平性.

本文提出了一种新颖的电子商务协议形式化分析方法,与其他相关工作相比较,该方法的特点是:(1) 以公理系统为基础,由一个推理规则和 8 个公理组成.(2) 对协议主体的拥有集合给出了形式化定义.(3) 将协议的初始状态假设细粒度化,将它们分为 3 类:基本假设、可信假设与协议理解假设,避免因非形式化的初始假设而产生的分析错误.(4) 对 TTP 的信任程度进行细粒度的形式化规范,揭示协议的内涵.(5) 分析步骤与过程简明、清晰.

1 新的形式化分析方法

本文作了如下基本假设:

1. 通信信道是安全的,亦即攻击者无法通过窃听获得通过通信信道交换的消息.
2. 协议所采用的密码算法是“完善”的.亦即,除非获得正确的解密密钥,无法通过密文还原为明文.
3. TTP 和一般主体之间的通信信道是可恢复信道,下文将作进一步解释.
4. 协议主体不进行合谋欺骗,也不进行不利于自己的欺骗.

以上基本假设 1~假设 3 是标准的,亦即,在大多数安全电子商务协议的设计与分析中,都采用类似的假设.这些假设被公认是合理的理论上的简化,并符合实际应用的需求.基本假设 4 说明,本文不讨论主体合谋的问题.

以下,为行文简捷起见,我们简称电子商务协议为协议.

1.1 基本符号

(m,n):表示消息 m 与消息 n 进行级连;

K_a:主体 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 的秘密密钥;

$\widetilde{K}$:密钥 K 的对偶密钥.如果 K 是非对称密钥,则 $\widetilde{K}=K^{-1}$.如果 K 是对称密钥,则 $\widetilde{K}=K$.

$h(m)$:应用于消息 m 的单向散列函数.

EOO(evidence-of-origin):发方非否认证据,是指电子商务协议向接收方提供的不可抵赖证据,用于证明发送方发送过某个消息.

EOR(evidence-of-receipt):收方非否认证据,是指电子商务协议向发送方提供的不可抵赖证据,用于证明接收方收到发送方发送的某个消息.

f_X:字段名,其中下标表示字段的含义,用于标识消息交换的目的.例如, f_{EOO} 表示 EOO 字段,说明该条消息发送 EOO 证据.

1.2 概念与定义

1.2.1 协议与环境

协议是一个分布式算法,在分布式环境中运行.本文将环境抽象为二元组,亦即环境由参与协议的主体和通信信道构成: $Environment=\langle Principle, Channel\rangle$.

协议主体集合 $Principle=\{\mathrm{TTP}, A,B,C,...,P,Q,R,...\}$,其中 $A,B,\ldots,Q,R,\ldots$等是参与协议消息交换的主体.他们既可以是诚实的,也可以是不诚实的.亦即,他们可以服从协议的执行,也可以不服从协议的执行.一般地,我们总假设这些主体是不诚实的.特别地,他们可以随意中断协议的执行.TTP 是特殊的主体,被参与协议的主体视为公正的第三方.对 TTP 的信任程度与具体的协议和运行环境有关.

环境的另外一个重要组成部分是通信信道.通信信道既可以是可靠的,也可以是不可靠的,依赖于具体的运行环境.通常,假设一般主体之间的通信信道是不可靠的,TTP 与一般主体之间的通信信道是"可恢复的",亦即该通信信道不可能永远瘫痪,最终消息可以传输成功.

1.2.2 协议语句

协议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协议的当前回合中应该接收和发送什么消息.协议语句具有以下两种形式之一:

$A\to B:m$ 表示主体 A 向主体 B 发送消息 m.

$A\leftarrow B:m$ 表示主体 A 主动从主体 B 处取到 m.

在下列两种情形下,主体 A 可以主动从主体 B 处取到 m:(1) 通过一次或多次 *ftp* 操作从主体 B 取得消息 m.这一基于 *ftp* 的方法是 Zhou 和 Gollman 提出来的[8],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,以弥补通信信道的不可靠性.(2) 当任意主体 B 公开消息 m 时,A 可以从 B 处取到 m.注意,这里"公开"也有两种情形:(a) 任意主体 B 向公众公开消息 m;(b) 协议主体 B 仅向参与协议的主体公开消息 m.

1.2.3 协议主体的拥有集合

假设协议由 n 条语句组成,A 为参与协议的任意主体.协议开始时,主体 A 的初始拥有集合为 O_a^0.协议执行第 i 步后,A 的拥有集合为 O_a^i.此外,我们将 $O_a=O_a^n$ 记为 A 的最终拥有集合.当协议运行一步后,A 的拥有集合包含其上一步的拥有集合和 A 在本回合接收和发送的消息.随着协议的继续运行,主体 A 的拥有集合单调增加,直至 $O_a=O_a^n$ 时为止.

下面给出主体 A 的拥有集合的形式化定义.为此,我们需要"可构造消息集合"这一概念.

定义 **1**. 可构造消息.

设 m 为消息,M 为消息集合.称 m 是由 M 可构造的,记为 $m\hat{\in}M$;当且仅当

$$\begin{aligned}&(m\in M)\vee\\&((m=(m_1,m_2))\wedge(m_1\hat{\in}M)\wedge(m_2\hat{\in}M))\vee\\&(((m=m_1)\vee(m=m_2))\wedge((m_1,m_2)\hat{\in}M))\vee\\&((m=f(m_1,...,m_n))\wedge(m_1\hat{\in}M)\wedge(m_2\hat{\in}M)\wedge\ldots\wedge(m_n\hat{\in}M)).\end{aligned}$$

其中,f 是元记号,表示实际上可计算的任意函数.

定义 **2**. 可构造消息集合.

设 m 为消息,M 为消息集合.称 $\hat{M}$ 为 M 的可构造消息集合,当且仅当

$$\hat{M}=\{m\mid m\hat{\in}M\}.$$

定义 **3**. 主体 A 的拥有集合.

假设协议由 n 条语句组成.主体 A 的拥有集合 O_a^i $(i=0,1,...,n)$是 O_a^i 的可构造消息集合 $\hat{O}_a^i$.

为行文简捷起见,以下除特别强调之外,我们不区分 $\hat{O}_a^i$ 与 O_a^i,而是将 O_a^i 理解为 $\hat{O}_a^i$.

当协议由第 i–1 步执行到第 i 步时,主体 A 的拥有集合由 O_a^{i-1} 到 O_a^i $(i=1,2,...,n)$的改变,遵循以下规则:

(1) 如果协议的第 i 条语句为 $A\to B:m$,m 为 A 新生成的消息,亦即 $m\notin O_a^{i-1}$,则 $O_a^i=O_a^{i-1}\cup\{m\}$, $i=1,2,...,n$.

如果 m 不是 A 新生成的消息,则有: $m \hat{\in} O_a^{i-1}$.

(2) 如果协议的第 i 条语句为 $B \to A: m$,或者 $A \leftarrow B: m$,且 $m \notin O_a^{i-1}$,则 $O_a^i = O_a^{i-1} \cup \{m\}$, $i = 1,2,...,n$.

(3) 其余情形, $O_a^i = O_a^{i-1}$, $i = 1,2,...,n$.

1.3 逻辑构件

我们的方法包含以下 8 个逻辑构件:

(1) A Can Prove x :对于任何主体 B,A 可以通过执行一系列操作,使 B 相信公式 x,且不向 B 泄漏任何秘密 $y \neq x$.

(2) A Claims x :A 声明对公式 x(以及所有 x 蕴涵的公式)负责.在分析过程中,下述蕴涵式成立:

$$A \text{ Claims } (x, y) \Rightarrow A \text{ Claims } x ,$$

亦即,如果 A 声明对公式(x,y)负责,则 A 声明对公式 x 负责.

(3) A Controls x :A 对公式 x 具有管辖权,即参与协议的主体都相信 A 所声明的公式 x 是正确的.

(4) A Has m :A 拥有消息 m.

(5) A Received m :A 收到消息 m.在分析过程中,下述蕴涵式成立:

$$A \text{ Received } (m,n) \Rightarrow A \text{ Received } m ,$$

亦即,如果 A 收到 (m,n) ,则 A 收到 m.

(6) $PK(A,K)$:K 是 A 的公开密钥,用于验证 A 用 K^{-1} 签名的消息.

(7) A Fetched m :A 主动取到消息 m.

(8) A Generated m :A 在协议回合中新生成消息 m.

1.4 公理系统

我们的公理系统由 1 个推理规则和 8 个公理组成.

推理规则如下:

$$(\vdash \varphi) \wedge (\vdash (\varphi \Rightarrow \psi)) \Rightarrow \vdash \psi .$$

上述推理规则说明,由 $\vdash \varphi$ 和 $\vdash (\varphi \Rightarrow \psi)$ 可以得到 $\vdash \psi$.这里,$\vdash$ 是元语言符号. $\Gamma \vdash \varphi$ 表示由公式集合 Γ (以及公理集合)可以推导出 φ . $\vdash \varphi$ 表示 φ 为定理,亦即由公理本身可以推导出 φ .因此,上述推理规则表示:如果 φ 是定理,且 φ 蕴涵 ψ ,则 ψ 也是定理.

公理集合中的 8 个公理分别为:

A1. 连接公理

$$A \text{ CanProve } x \wedge A \text{ CanProve } y \Rightarrow A \text{ CanProve } (x \wedge y) .$$

如果 A 既能够证明公式 x 又能够证明公式 y,则 A 能够证明公式 $x \wedge y$.

A2. 蕴涵公理

$$A \text{ CanProve } x \wedge (x \Rightarrow y) \Rightarrow A \text{ CanProve } y .$$

如果 A 能够证明公式 x,且公式 x 蕴涵公式 y,则 A 能够证明公式 y.

A3. 签名公理

$$(A \text{ Has } \{m\}_{K^{-1}}) \wedge A \text{ CanProve } PK(B,K) \Rightarrow A \text{ CanProve } (B \text{ Claims } m) .$$

如果 A 拥有用 K^{-1} 签名的消息 m,且 A 能够证明 K 可以用于验证 B 的身份,则 A 能够证明 B 对消息 m 负责.

A4. 管辖公理

$$A \text{ CanProve } (B \text{ Controls } x) \wedge A \text{ CanProve } (B \text{ Claims } x) \Rightarrow A \text{ CanProve } x .$$

如果 A 能够证明 B 对公式 x 具有管辖权,且 A 能够证明 B 对公式 x 负责,则 A 能够证明公式 x 成立.

A5. 密文理解公理

$$A \text{ CanProve } (B \text{ Claims } \{m\}_K) \wedge A \text{ CanProve } (B \text{ Claims } K) \Rightarrow A \text{ CanProve } (B \text{ Claims } m) .$$

如果 A 能够证明 B 对密文消息 $\{m\}_K$ 负责,且 A 能够证明 B 对对称密钥 K 负责,则 A 能够证明 B 对消息 m 负责.

A6. 拥有公理

$$A\,\text{Received}\,m \vee A\,\text{Fetched}\,m \vee A\,\text{Generated}\,m \Rightarrow A\,\text{Has}\,m\,.$$

如果 A 收到消息 m,或者 A 主动取到消息 m,或者 A 新生成消息 m,则 A 拥有消息 m.

A7. 接收公理

$$A\,\text{Received}\,\{m\}_K \wedge A\,\text{Has}\,\widetilde{K} \Rightarrow A\,\text{Received}\,m\,.$$

如果 A 收到用密钥 K 加密或签名的消息 $\{m\}_K$,且 A 拥有 K 的对偶密钥 $\widetilde{K}$,则 A 收到消息 m.

A8. 取到公理

$$A\,\text{Fetched}\,\{m\}_K \wedge A\,\text{Has}\,\widetilde{K} \Rightarrow A\,\text{Fetched}\,m\,.$$

如果 A 主动取到用密钥 K 加密或签名的消息 $\{m\}_K$,且 A 拥有 K 的对偶密钥 $\widetilde{K}$,则 A 取到消息 m.

1.5 协议分析的步骤

协议分析由以下 3 个步骤组成.

(1) 协议分析准备

(i) 列出协议主体的初始拥有集合;

(ii) 列出初始状态假设集合

(a) 基本假设;

(b) 可信假设;

(c) 协议理解假设;

(iii) 列举 EOO 与 EOR;

(2) 可追究性分析

(i) 列举可追究性目标;

(ii) 分析 EOO 与 EOR 的设计是否符合可追究性要求;

(iii) 分析协议是否达到可追究性目标,亦即,协议正常结束时, $EOO \in O_b \wedge EOR \in O_a$ 是否成立;

(3) 公平性分析

分析协议是否达到公平性目标,亦即协议在第 $i(1 \le i \le n)$ 步终止执行时,是否满足 $EOO \in O_b^{i-1}$ 当且仅当 $EOR \in O_a^{i-1}$.

2 协议分析的例子之一

2.1 CMP1协议

1995 年,Deng 等人提出了一种挂号电子邮件协议[9]方案,称为 CMP1 和 CMP2 . CMP1 和 CMP2 的主要区别在于, CMP2 具有邮件加密的功能,而 CMP1 则没有.下面,我们介绍 CMP1 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.

(1) $A \to B: A, B, \text{TTP}, h(m), \{k\}_{K_{ttp}}, \{\{A, B, \text{TTP}, m\}_{K_a^{-1}}\}_k$.

(2) $B \to \text{TTP}: \{A, B, \text{TTP}, h(m)\}_{K_b^{-1}}, \{k\}_{K_{ttp}}, \{\{A, B, \text{TTP}, m\}_{K_a^{-1}}\}_k$.

(3) $\text{TTP} \to B: \{\{A, B, \text{TTP}, m\}_{K_a^{-1}}\}_{k_{ttp}^{-1}}$.

(4) $\text{TTP} \to A: \{\{A, B, \text{TTP}, h(m)\}_{K_b^{-1}}, B, m\}_{k_{ttp}^{-1}}$.

协议开始时,A 用其秘密密钥 K_a^{-1} 对 $\{A, B, \text{TTP}, m\}$ 进行签名,然后生成一个会话密钥 k,并用 k 加密 A 的签名消息.最后,A 计算邮件 m 的摘要 $h(m)$,将 k 用 TTP 的公开密钥加密,并将消息(1)发送给 B.其中,消息(1)的明文部分,亦即 A,B,TTP,$h(m)$是邮件标识符,记为 mid.通过邮件标识符 mid,B 获得如下信息:"A 准备向 B 发送由邮局 TTP 挂号递交的,其摘要为 $h(m)$的邮件.如果 B 希望接收这个邮件,请向 TTP 提交接收邮件 m 的请求".

收到消息(1)后,B 可以有两种选择.如果 B 对这个邮件不感兴趣,可以不对消息(1)进行响应,此时协议异常终

止,对双方都没有影响.如果 B 愿意接收这个邮件,就用 B 的秘密密钥 K_b^{-1} 对 mid 进行签名,连同消息(1)的其余部分一起发送给 TTP.

收到消息(2)后,TTP 首先用 B 的公开密钥 K_b 校验 B 对 mid 签名的有效性.其次,TTP 用自己的秘密密钥 K_{ttp}^{-1} 解密 $\{k\}_{K_{ttp}}$,并获得会话密钥 k.然后,TTP 用 k 解密 $\{\{A, B, \text{TTP}, m\}_{K_a^{-1}}\}_k$,获得 $\{A, B, \text{TTP}, m\}_{K_a^{-1}}$,并用 A 的公开密钥 K_a 校验 A 签名的有效性.最后,TTP 通过由 $\{A, B, \text{TTP}, m\}_{K_a^{-1}}$ 获得的 m 计算摘要 $h(m)$,并与 $\{A, B, \text{TTP}, h(m)\}_{K_b^{-1}}$ 中的 $h(m)$进行比较.如果二者一致,则 TTP 断定"A 希望发送给 B 的邮件内容为 m,且 B 愿意接收 m".在这种情形下,TTP 向 B 发送消息(3),亦即"A 发送邮件 m 的非否认证据"——EOO:

$$EOO = \{\{A, B, \text{TTP}, m\}_{K_a^{-1}}\}_{k_{ttp}^{-1}}.$$

同时,TTP向A发送消息(4),亦即"TTP向B递交邮件m的非否认证据"——EOD:

$$EOD = \{\{A, B, \text{TTP}, h(m)\}_{K_b^{-1}}, B, m\}_{k_{ttp}^{-1}}.$$

2.2 CMP1协议的分析

分析前,我们引入谓词 $match$,用于校验任意消息 m 与其摘要 $h(m)$的一致性,亦即

$$match(m, h(m)) = \text{true}$$

当且仅当对 m 应用单向散列函数 h 时,其结果为 $h(m)$.

协议的分析过程如下:

(1) 协议分析准备

(i) 列出初始拥有集合:

$$O_a^0 = \{K_a^{-1}, K_a, K_b, K_{ttp}\};\ O_b^0 = \{K_a, K_b^{-1}, K_b, K_{ttp}\}.$$

(ii) 列出初始状态假设集合:

(a) 基本假设:

B1 A CanProve $PK(B, K_b)$

B2 B CanProve $PK(A, K_a)$

B3 A, B CanProve $PK(TTP, K_{ttp})$

(b) 可信假设:

T1 A, B CanProve (TTP Controls (将 m 发送给 B))

T2 A, B CanProve (TTP Controls $match(m, h(m))$)

T3 TTP Claims (将 m 发送给 B) $\Rightarrow$ TTP Claims $match(m, h(m))$

(c) 协议理解假设:

C1 (将 m 发送给 B) $\Rightarrow$ B Has m

C2 B Claims $h(m) \wedge B$ Has $m \wedge match(m, h(m)) \Rightarrow B$ Claims m

C3 TTP Claims $(B, m) \Rightarrow$ TTP Claims (将 m 发送给 B)

(iii) 列举 EOO 与 EOR:

我们注意到,CMP1 协议的 EOO 与 EOR 的设计存在冗余.事实上,令 $EOO = \{A, B, \text{TTP}, m\}_{K_a^{-1}}$,$EOR = \{A, B, \text{TTP}, h(m)\}_{K_b^{-1}}, \{B, m\}_{K_{ttp}^{-1}}$ 即可满足要求.根据以上分析,我们得到协议理解假设 C3.

去掉冗余性以后,CMP1 协议的第(3)和第(4)步如下,第(1)步与第(2)步不变.我们将对修改后的 CMP1 协议进行形式化分析.

(第3步) $\text{TTP} \rightarrow B: \{A, B, \text{TTP}, m\}_{K_a^{-1}}$

(第4步) $\text{TTP} \rightarrow A: \{A, B, \text{TTP}, h(m)\}_{K_b^{-1}}, \{B, m\}_{k_{ttp}^{-1}}$

(2) 可追究性分析

(i) 列举可追究性目标:

(G1) B CanProve (A Claims m)

(G2) A CanProve (B Claims m)

(ii) 分析 EOO 与 EOR 的设计是否符合可追究性要求:

假定 $EOO \in O_b$ 成立,即 $\{A, B, \text{TTP}, m\}_{K_a^{-1}} \in O_b$.

由 B Has $\{A, B, \text{TTP}, m\}_{K_a^{-1}}$,B2 与 A3 可得:

$$B \text{ CanProve } (A \text{ Claims } m) \tag{G1}$$

假定 $EOR \in O_a$ 成立,即 $\{A, B, \text{TTP}, h(m)\}_{K_b^{-1}} \in O_a$, $\{B, m\}_{K_{ttp}^{-1}} \in O_a$.

由 A Has $\{A, B, \text{TTP}, h(m)\}_{K_b^{-1}}$,B1 与 A3 可得:

$$A \text{ CanProve } (B \text{ Claims } h(m)) \tag{1}$$

由 A Has $\{B, m\}_{K_{ttp}^{-1}}$,B3 与 A3 可得:

$$A \text{ CanProve } (\text{TTP Claims } (B, m)).$$

由上式,C3 与 A2 可得:

$$A \text{ CanProve } (\text{TTP Claims } (\text{将 } m \text{ 发送给 } B)) \tag{2}$$

由上式,T1 与 A4 可得:

$$A \text{ CanProve } (\text{将 } m \text{ 发送给 } B).$$

由上式,C1 与 A2 可得:

$$A \text{ CanProve } (B \text{ Has } m) \tag{3}$$

由式(2),T3 与 A2 可得:

$$A \text{ CanProve } (\text{TTP Claims } match(m, h(m))).$$

由上式,T2 与 A4 可得:

$$A \text{ CanProve } match(m, h(m)).$$

由上式,式(3)与 A1 可得:

$$A \text{ CanProve } ((B \text{ Has } m) \wedge match(m, h(m))).$$

由上式,式(1)与 A1 可得:

$$A \text{ CanProve } ((B \text{ Claims } h(m)) \wedge (B \text{ Has } m) \wedge match(m, h(m))).$$

由上式,C2 与 A2 可得:

$$A \text{ CanProve } (B \text{ Claims } m) \tag{G2}$$

因此,改进后的 CMP1 协议的 EOO 与 EOR 的设计满足可追究性要求.

(iii) 分析协议是否达到可追究性目标:

因为, $O_b^3 = O_b^2 \cup EOO$, $O_a^4 = O_a^3 \cup EOR$.我们有: $EOO \in O_b^3 \subseteq O_b$ 和 $EOO \in O_a^4 \subseteq O_a$.

因此,协议达到可追究性目标.

(3) 公平性分析

协议达到公平性目标等价于下述命题成立:

$$EOO \in O_b^{i-1} \text{ 当且仅当 } EOR \in O_a^{i-1}, i = 1,2,3,4.$$

已知 $EOO \in O_b^3$,现考查 O_a^3.由于 $O_a^3 = O_a^1$,且 $(\{A, B, \text{TTP}, h(m)\}_{K_b^{-1}}, \{B, m\}_{K_{ttp}^{-1}}) \notin \hat{O}_a^1$,因此 $EOR \hat{\in} O_a^3$ 不成立.

所以,在信道不可靠的条件下,本协议是非公平的.

3 协议分析的例子之二

3.1 Zhou-Gollmann协议

以下是 Zhou-Gollmann 协议[8],它可以用于在信道不可靠的条件下签订电子合同.

$c=\{m\}_K$ $l=h(m,K)$

$\overline{EOO}=\{f_{\overline{EOO}},B,l,c\}_{K_a^{-1}}$ $\overline{EOR}=\{f_{\overline{EOR}},A,l,c\}_{K_b^{-1}}$

$sub\_K=\{f_{SUB},B,l,K\}_{K_a^{-1}}$ $con\_K=\{f_{CON},A,B,l,K\}_{K_{ttp}^{-1}}$

(1) $A\rightarrow B$: $f_{\overline{EOO}},B,l,c,\overline{EOO}$

(2) $B\rightarrow A$: $f_{\overline{EOR}},A,l,\overline{EOR}$

(3) $A\rightarrow$ TTP : f_{SUB},B,l,K,sub_K

(4) $B\leftarrow$ TTP : f_{CON},A,B,l,K,con_K

(5) $A\leftarrow$ TTP : f_{CON},A,B,l,K,con_K

其中,m 是 A 向 B 发送的消息;K 是 A 随机生成的密钥;c 是用 K 加密 m 的加密消息;表示 A 向 B 发送消息 m 的承诺; sub_K 是 A 提交密钥 K 的证据; con_K 是 TTP 确认已经交付密钥 K 的证据. $l=h(m,K)$ 是协议中唯一的标记,表示这个协议回合中交换的消息是 m.

在协议的第(1)步,A 向 B 发送 $\overline{EOO}$ 与 c.第(2)步,B 向 A 发送 $\overline{EOR}$.第(3)步,A 向 TTP 发送 K 与 sub_K .这里,K 是明文传送的,因此,B 有可能在 TTP 得到 K 之前获得消息 m.为保证协议的公平性,协议假设 A 与 TTP 之间的通信信道是“可恢复的”.亦即,B 不可能永远阻止 TTP 收到 A 发送的消息(3).收到消息(3)之后,TTP 生成 con_K, 并在其目录上公布证据 con_K ,供公众进行只读访问.第(4)步与第(5)步,B 和 A 分别从 TTP 处取到证据 con_K.

3.2 Zhou-Gollmann协议的分析梗概

受篇幅所限,本文仅给出该协议的分析梗概.首先,引入谓词 *verify* 如下:

$$verify(c,K,m)=\text{true}$$

当且仅当对密文消息 c 应用对称密钥 K 解密时,其结果为明文消息 m.

协议的可信假设是:

T1 TTP Claims $K\Rightarrow A$ Claims K

T2 TTP Claims $K\Rightarrow$ TTP Claims $verify(c,K,m)$

T3 A,B CanProve (TTP Controls $verify(c,K,m)$)

协议理解假设是:

C1 TTP Claims $K\Rightarrow$ TTP Claims (公布con_K)

C2 TTP Claims (公布con_K) $\Rightarrow B$ Has con_K

C3 B Claims $c\wedge B$ Has $con\_K\wedge verify(c,K,m)\Rightarrow B$ Claims m

该协议的 EOO 与 EOR 是:

$$EOO=\overline{EOO},con\_K=\{f_{\overline{EOO}},B,l,c\}_{K_a^{-1}},\{f_{CON},A,B,l,K\}_{K_{ttp}^{-1}},$$

$$EOR=\overline{EOR},con\_K=\{f_{\overline{EOR}},A,l,c\}_{K_b^{-1}},\{f_{CON},A,B,l,K\}_{K_{ttp}^{-1}}.$$

通过类似于第 2.2 节中的分析,不难证明:Zhou-Gollmann 协议的 EOO 与 EOR 的设计满足可追究性要求:

$$B \text{ CanProve } (A \text{ Claims } m) \quad \text{(G1)}$$

$$A \text{ CanProve } (B \text{ Claims } m) \quad \text{(G2)}$$

并且,协议达到可追究性目标.此外,由于可恢复信道的假设,不难证明该协议也满足公平性的要求.

4 结 论

通过上述分析,可以发现某些协议的冗余性,并揭示了协议的某些内涵.为了保证协议的可追究性与公平性,在 CMP1 协议中,TTP 必须做到:将 m 发送给 B,并在发送前检查 m 与 $h(m)$的一致性.类似地,在 Zhou-Gollmann 协议中,TTP 必须做到:公布证据 con_K;TTP 声明负责的密钥 K 是 A 提交的密钥;并且对该密钥进行了 c 与 m 的一致性验证.

注意,公理 A6~A8 可用于建立主体的拥有集合.因篇幅所限,本文省略了它们的应用.

应用本文提出的方法,可以分析范围很广的电子商务协议,例如,文献[10,11]中的一些协议.

近年来,对于公平交换协议,提出了一些新的概念.例如,对公平性提出了时效性、不可滥用性等要求;为了减少可信第三方的参与,提出了乐观公平交换协议等[12,13].全面分析这些复杂的协议,需要应用更为复杂的形式化工具,例如我们提出的一种新方法[14].尽管如此,本文提出的方法仍然具有简单、实用、应用广泛等特点.特别地,在设计复杂协议时,可以首先应用本方法分析和检查协议的各种安全性质.

References:

[1] Qing SH. Cryptography and Computer Network Security. Beijing: Tsinghua University Press, 2001 (in Chinese).

[2] Qing SH. Design and logical analysis of security protocols. Journal of Software, 2003,14 (7):1300−1309 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1300.htm

[3] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Trans. on Computer Systems, 1990,8(1):18−36.

[4] Syverson PF, van Oorschot PC. On unifying some cryptographic protocol logics. In: Proc. of the 1994 IEEE Computer Society Symp. on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1994. 14−28. http://chacs.nrl.navy.mil/publications/CHACS/1994/1994syverson-sp.pdf

[5] Kailar R. Accountability in electronic commerce protocols. IEEE Trans. on Software Engineering, 1996,22(5):313−328.

[6] Zhou DC, Qing SH, Zhou ZF. Limitations of Kailar logic. Journal of Software, 1999,10(12):1238−1245 (in Chinese with English abstract).

[7] Zhou DC, Qing SH, Zhou ZF. A new approach for the analysis of electronic commerce protocols. Journal of Software, 2001,12(9): 1318−1328 (in Chinese with English abstract).

[8] Zhou J, Gollman D. A fair non-repudiation protocol. In: Proc. of the 1996 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1996. 55−61. http://citeseer.ist.psu.edu/62704.html

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

[10] Qing SH. The TTP roles in electronic commerce protocols. Journal of Software, 2003,14(11):1936−1943 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1936.htm

[11] Qing SH. Security Protocols. Beijing: Tsinghua University Press, 2005 (in Chinese).

[12] Asokan N, Shoup V, Waidner M. Optimistic fair exchange of digital signatures. In: Nyberg K, ed. Advances in Cryptology: Proc. of the Eurocrypt'98. LNCS 1403, Springer-Verlag, 1998. 591−606.

[13] Asokan N, Schunter M, Waidner M. Optimistic protocols for fair exchange. Research Report, RZ 2858, IBM Research, 1996.

[14] Qing SH, Li GC. A formal model of fair exchange protocols. Science in China (E), 2005,35(2):161−172 (in Chinese with English abstract).

附中文参考文献:

[1] 卿斯汉.密码学与计算机网络安全.北京:清华大学出版社,2001.

[2] 卿斯汉.安全协议的设计与逻辑分析.软件学报,2003,14(7):1300−1309. http://www.jos.org.cn/1000-9825/14/1300.htm

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

[7] 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.

[10] 卿斯汉.电子商务协议中的可信第三方角色.软件学报,2003,14(11):1936−1943. http://www.jos.org.cn/1000-9825/15/1936.htm

[11] 卿斯汉.安全协议.北京:清华大学出版社,2005.

[14] 卿斯汉,李改成.公平交换协议的一个形式化模型.中国科学(E 辑),2005,35(2):161−172.