计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200500072

基于进程代数的 Otway-Rees 协议的形式化验证

蔡雨桐[1]　王　勇[1]　王然然[1]　姜正涛[2]　代桂平[3]
1 北京工业大学信息学部计算机学院　北京 100124
2 中国传媒大学计算机与网络空间安全学院　北京 100024
3 北京工业大学信息学部人工智能与自动化学院　北京 100124
(1241282400@qq.com)

摘　要　Otway-Rees 协议的目的是完成发起者和响应者之间的双向认证,并且分发服务器产生的会话密钥。该协议的特点是简单实用,没有使用复杂的同步时钟机制或双重加密,仅用少量的信息提供了良好的时效性。此协议允许通过一个网络的个别通信认证自己的身份,还可以阻止重放攻击和窃听,允许修改检测。对安全协议的分析是信息时代无法回避的关键问题,事实证明,形式化方法是安全协议分析更为可靠和有效的途径。此协议的形式化验证对于工程实施具有重要意义。对 Otway-Rees 协议进行抽象处理,得到抽象模型,在此基础上给出基于进程代数的形式化描述,并进行形式化验证。验证结果表明,此协议形式的并行系统展现出了期望的外部行为。

关键词:Otway-Rees;安全协议;协议验证;形式化;进程代数
中图法分类号　TP301.2

Formal Verification of Otway-Rees Protocol Based on Process Algebra

CAI Yu-tong[1],WANG Yong[1],WANG Ran-ran[1],JIANG Zheng-tao[2] and DAI Gui-ping[3]
1 College of Computer Science and Technology,Faculty of Information Technology,Beijing University of Technology,Beijing 100124,China
2 School of Computer Science and Cybersecurity,Communication University of China,Beijing 100024,China
3 College of Artificial Intelligence and Automation,Faculty of Information Technology,Beijing University of Technology,Beijing 100124,China

Abstract　Otway-Rees protocol is to complete the two-way authentication between the initiator and the responder,and to distribute the session key generated by the server. The feature of this protocol is simple and practical. It does not use complicated synchronous clock mechanism or double encryption,and provides good timeliness with only a small amount of information. This protocol allows individual communications to be authenticated through a network,while also preventing replay attacks and eavesdropping,as well as modifying detection. The analysis of security protocols is a key issue that cannot be avoided in the information age. Formal method,which is based on strict mathematical and mechanical methods,is an important method to improve and ensure the quality of computing system. Its model,technology and tools have become an important carrier of computing thinking. The formal method can accurately reveal all kinds of logic rules,make corresponding logic rules,and make all kinds of theoretical systems more rigorous. Formal method is a mathematical description of what a program does,a description of the function of a program written in a formal language with precise semantics. It is not only the starting point of designing and programming,but also the basis of verifying whether a program is correct,so as to improve the reliability and robustness of the design. By abstracting the Otway-Rees protocol,we can get the abstract model. On this basis,the formal description based on process algebra is given and the formal verification is carried out. The verification results show that the parallel system in the form of this protocol shows the expected external behavior.

Keywords　Otway-Rees,Security protoco,Protocol verification,Formalization,Process algebra

随着计算机网络通信技术的高速发展以及分布式计算的普及,并发系统的建模与分析已成为计算机技术的主流方向之一。并发模型与其他传统模型的顺序计算不同,具有其固有的复杂性,进程代数是通过代数模型来描述并发计算的一种数学模型,它能够刻画并发现象,即多个计算进程同时活动,通过交换信息(通信)来协作完成预期的特定计算任务。由于其具有良好的代数性质以及规范简洁的语法和语义,进程代数成为了众多并发模型中最具有代表性的模型。

Otway 和 Rees 研究所得的 Otway-Rees 协议是于 1987 年提出的一种早期认证协议。此协议是一个基于服务器的协议,该协议的目的是完成发起者和响应者之间的双向认证,并且通过可信服务器为通信双方分配会话密钥[1]。参加的主题是通信双方 A、B 和认证服务器 C。该协议的特点是非常简单且实用性强,不需要采用复杂的系统时钟所提供的同步时

基金项目:广西密码学与信息安全重点实验室研究课题(GCIS201808)
This work was supported by the Guangxi Key Laboratory of Cryptography and Information Security Research Project(GCIS201808).
通信作者:王勇(wangy@bjut.edu.cn)

钟机制，仅用少量的信息提供了良好的时效性。Otway-Rees 协议是专为在不安全网络上使用进而设计的网络认证协议。此协议允许通过一个网络个别通信认证自己的身份，还可以阻止重放攻击和窃听，允许修改检测。

证明具有所需安全属性的协议是相当困难的，需要的是一个理论上能够描述和推理的密码协议[2]。针对此问题，本文结合进程代数的知识[3]对此协议进行了形式化分析。首先，采用进程代数 ACP 对证明系统及协议进行建模，并给出了待验证问题的形式化定义对此协议进行形式化验证，最后对 Otway-Rees 协议进行了严格的理论推导。理论分析结果表明，此协议形式的并行系统展示了期望的外部行为。本文研究结果为 Otway-Rees 协议的有效实施提供了坚实的理论基础。

1 ACP 基础

进程代数是通过代数模型来描述并发计算的一种数学模型，它能够刻画并发现象，即多个计算进程的活动，通过交换信息(通信)来协作完成预期任务的特定计算现象。由于其具有良好的代数性质以及规范简洁的语法和语义，进程代数成为了众多并发模型中最具代表性的模型。

进程代数面向行为，更贴近人的思维分析模式，可以对并发和交互的进程进行严格的数学推理。进程代数提出了许多演算模型，20 世纪 70 年代后期，英国学者 Milner 提出了通信系统演算和通信顺序进程 CCS[4]，Hoare 等提出的通信顺序进程 CSP[5]是面向分布式系统的程序设计语言，开创了用代数方法研究通信并发系统的先河。随着时间的发展，演算系统得到了快速的完善，本文主要研究的是通过 Bergstra 等于 1984 年提出的 ACP 理论[6]进行的形式化理论的验证。该理论针对反应式、并行式和分布式系统，描述了两个系统之间的交互行为。ACP 是在 BPA 的基础上加入了互模拟等价的概念，并引入了并行算子以及死锁 δ 和封装 ∂_H 分析工具，具有很强的描述并发系统的能力。

2 Otway-Rees 协议

该协议的核心思想是使用一个可信任的服务器，发起者和响应者两人各和可信服务器共享一个秘密密钥，这些密钥只用于密钥分配过程中，而不应用于加密发起者和响应者之间的实际消息。协议完成后，双方之间就拥有了会话密钥，从而能够进行通信。发起者、响应者及可信服务器的 Otway-Rees 协议如图 1 所示。其中，EA 表示用发起者与可信服务器的共享密钥进行的加密操作，EB 表示用响应者与可信服务器的共享密钥进行的加密操作，DA 表示用发起者与可信服务器的共享密钥进行的解密操作，DB 表示用响应者与可信服务器的共享密钥进行的解密操作，g 表示生成随机数操作，T 表示匹配操作，T' 表示不匹配操作。*Alice* 代表发起者，*Bob* 代表响应者，*Carl* 代表可信任的服务器。

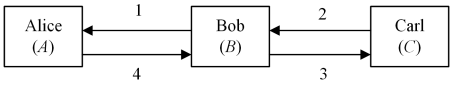

图 1 发起者、响应者及可信服务器的 Otway-Rees 协议

Fig. 1 Otway-Rees protocol for initiator, responder and trusted server

(1)A 产生消息，此消息包括一个索引号 I、他的名字 A、B 的名字 B 和随机数 N_A，用他和 C 共享的密钥对此消息加密，并将索引号、他的名字和 B 的名字与他加密的消息一起发送给 B。$A->B: I, A, B, E_A(N_A, I, A, B)$，该消息记为 m_1。

(2)B 产生消息，此消息包括一个新的随机数 N_B、索引号 I、A 的名字 A 和 B 的名字 B。用他与 C 共享的密钥对此消息加密，并将 A 的加密消息、索引号、A 的名字、B 的名字与他加密的消息一起发送给 C。$B->C: I, A, B, E_A(N_A, I, A, B), E_B(N_B, I, A, B)$，该消息记为 m_2。

(3)C 产生随机会话密钥 K，然后产生两个消息，一个用他与 A 共享的密钥对 A 的随机数和会话密钥加密，另一个用与 B 共享的密钥对 B 的随机数和会话密钥加密。他将这两个消息与索引号一起发送给 B。$C->B: I, E_A(N_A, K), E_B(N_B, K)$，该消息记为 m_3。

(4)B 将用 A 的密钥加密的消息连同索引号一起发送给 A。$B->A: I, E_A(N_A, K)$，该消息记为 m_4。

(5)另外，将 (N_A, I, A, B) 消息记为 m_5，将 (N_B, I, A, B) 消息记为 m_6，将 (N_A, K) 消息记为 m_7，将 (N_B, K) 消息记为 m_8。

(6)A 解密消息，恢复出他的密钥和随机数，然后确认协议中的索引号和随机数都没有改变。假设所有随机数都匹配，并且按照这种方法索引号没有改变，A 和 B 现在互相确认对方的身份，他们就有一个用于通信的秘密密钥。

3 Otway-Rees 协议的形式化分析

(1)协议抽象

对图 1 所示的 Otway-Rees 协议进行抽象处理，得到如图 2 所示的抽象模型。发起者 A 和响应者 B 之间的连接通道(包括通道 B,E)以及响应者 B 和可信任服务器 C 之间的连接通道(包括通道 C,D)为内部通道，B 通道为发起者 A 向响应者 B 发送信息的通道，E 通道为响应者 B 向发起者 A 发送信息的通道，C 通道为响应者 B 向可信任服务器 C 发送信息的通道，D 通道为可信任服务器 C 向响应者 B 发送信息的通道；而通道 A 和通道 F 分别为发起者 A 接受外部信息 d 的通道和响应者 B 输出结果消息 dr 的通道。发起者 A、响应者 B 和可信任服务器 C 作为一个封闭的系统，即通道 B,C,E,D 为内部通道，而通道 A,F 为外部通道。

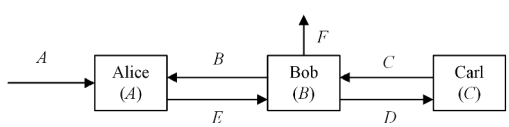

图 2 Otway-Rees 协议的抽象模型

Fig. 2 Abstract model of Otway-Rees protocol

通过某个通道发送消息的行为由两个原子动作组成，在消息的发送方需要执行 send 操作(简写为 s)，在消息的接收方需要执行 read 操作(简写为 r)。

(2)ACP 描述

ACP 建立在等式逻辑(equational logic)的基础上，具有一个严格的公理系统，它由以下部分组成：

1)定义有限进程的基本算子 A，+，·；

2)使得原子动作进行通信的并行算子 ‖，|，⌊以及死

锁 δ 和封装 ∂_H；

3）使得内部计算不可见的静默步骤 τ 和抽象算子 τ_I；

4）捕捉正则进程的受保护线性递归 $\langle X|E\rangle$。

发起者 A 的状态变迁的 ACP 描述如下：

$A=\sum_{d\in\Delta} r_A(d)\cdot A_1$

$A_1=g(N_A)\cdot A_2$

$A_2=E_A(m_5)\cdot A_3$

$A_3=s_B(m_1)\cdot A_4$

$A_4=r_E(m_4)\cdot A_5$

$A_5=D_A(m_7)\cdot A_6$

$A_6=T(N_A)\cdot A+T'(N_A)\cdot A_1$

其中，A_i 为 A 所处的状态，Δ 为 A 和用户之间输入数据 d 和输出数据 d_r 的集合。

响应者 B 的状态变迁的 ACP 描述如下：

$B=r_B(m_1)\cdot B_1$

$B_1=g(N_B)\cdot B_2$

$B_2=E_B(m_6)\cdot B_3$

$B_3=s_C(m_2)\cdot B_4$

$B_4=r_D(m_3)\cdot B_5$

$B_5=D_B(m_8)\cdot B_6$

$B_6=T(N_B)\cdot B_7+T'(N_B)\cdot B_1$

$B_7=s_E(m_4)\cdot B_8$

$B_8=\sum_{d_r\in\Delta} s_F(d_r)\cdot B$

可信任服务器 C 的状态变迁的 ACP 描述如下：

$C=r_C(m_2)\cdot C_1$

$C_1=D_A(m_5)\cdot C_2$

$C_2=D_B(m_6)\cdot C_3$

$C_3=E_A(m_7)\cdot C_4$

$C_4=E_B(m_8)\cdot C_5$

$C_5=s_D(m_3)\cdot C$

在同一信道上同一数据的读取和发送操作可以彼此进行通信，其他原子操作之间的通信导致死锁 δ。其中，γ 为通信函数：

$\gamma(s_B(m_1),r_B(m_1))\overset{\triangle}{=}C_B(m_1)$

$\gamma(s_C(m_2),r_C(m_2))\overset{\triangle}{=}C_C(m_2)\gamma(s_D(m_3),r_D(m_3))\overset{\triangle}{=}C_D(m_3)$

$\gamma(s_E(m_4),r_E(m_4))\overset{\triangle}{=}C_E(m_4)$

通过把 A，B 和 C 并行化，封装通过内部信道 B，C，D，E 进行的 send 操作和 read 操作，并抽象掉通过上述内部通道的通信操作，从而得到期望的并行系统，用下文的进程项表示该系统：

$\tau_I(\partial_H(A\parallel B\parallel C))$

其中：

$H=\{s_B(m_1),r_B(m_1),s_C(m_2),r_C(m_2),s_D(m_3),r_D(m_3),s_E(m_4),r_E(m_4)|m_1,m_2,m_3,m_4\in\Delta_2\}$

$I=\{C_B(m_1),C_C(m_2),C_D(m_3),C_E(m_4),g(N_A),g(N_B),T(N_A),T'(N_A),T(N_B),T'(N_B),E_A(m_5),D_A(m_5),E_A(m_7),D_A(m_7),E_B(m_6),D_B(m_6),E_B(m_8),D_B(m_8)\}$

（3）形式化分析

命题 1 Otway-Rees 系统具有期望的外部行为，即 $\tau_I(\partial_H(ABC))$ 具有期望的外部行为。

证明：

令 $A\parallel B=Z$，则 $A\parallel B\parallel C=Z\parallel C$

$A\parallel B\overset{M_1}{\rightleftharpoons}A\llcorner B+B\llcorner A+A|B\overset{RDP}{\rightleftharpoons}(\sum_{d\in\Delta} r_A(d)\cdot A_1)\llcorner B+(r_B(m_1)\cdot B_1)\llcorner A+(\sum_{d\in\Delta} r_A(d)\cdot A_1)|(r_B(m_1)\cdot B_1)\overset{LM_5,CM_8}{\rightleftharpoons}\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B)+r_B(m_1)\cdot(B_1\parallel A)+\gamma(\sum_{d\in\Delta} r_A(d)\cdot r_B(m_1))\cdot(A_1\parallel B_1)\overset{CM_8,A_7}{\rightleftharpoons}\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B)+r_B(m_1)\cdot(B_1\parallel A)+\delta\overset{A_6,A_7}{\rightleftharpoons}\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B)+r_B(m_1)\cdot(B_1\parallel A)$

$Z\parallel C\overset{M_1}{\rightleftharpoons}Z\llcorner C+C\llcorner Z+Z|C\overset{RDP}{\rightleftharpoons}(\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B)+r_B(m_1)\cdot(B_1\parallel A)\llcorner C+(r_C(m_2)\cdot C_1)\llcorner Z+(\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B)+r_B(m_1)\cdot(B_1\parallel A)|(r_C(m_2)\cdot C_1)\overset{CM_6}{\rightleftharpoons}(\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B))\llcorner C+(r_B(m_1)\cdot(B_1\parallel A))\llcorner C+r_C(m_2)\cdot(C_1\parallel Z)\overset{LM_3}{\rightleftharpoons}\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B\parallel C)+r_B(m_1)\cdot(B_1\parallel A\parallel C)+r_C(m_2)\cdot(C_1\parallel Z)$

$\partial_H(A\parallel B\parallel C)\overset{RDP}{\rightleftharpoons}\partial_H(\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B\parallel C)+r_B(m_1)\cdot(r_C(m_2)\cdot(C_1\parallel Z))\cdot(C_1\parallel Z))\overset{D_4}{\rightleftharpoons}\partial_H(\sum_{d\in\Delta} r_A(d)\cdot(A_1\parallel B\parallel C))+\partial_H(r_B(m_1)\cdot(B_1\parallel A\parallel C))+\partial_H(r_C(m_2)\cdot(C_1\parallel Z))\overset{D_5}{\rightleftharpoons}\partial_H(\sum_{d\in\Delta} r_A(d))\cdot\partial_H(A_1\parallel B\parallel C)+\partial_H(r_B(m_1))\cdot\partial_H(B_1\parallel A\parallel C)+\partial_H(r_C(m_2))\cdot\partial_H(C_1\parallel Z)\overset{A_6,A_7,D_1,D_2}{\rightleftharpoons}\sum_{d\in\Delta} r_A(d)\cdot\partial_H(A_1\parallel B\parallel C)$

同理可得：

$\partial_H(A_1\parallel B\parallel C)=g(N_A)\cdot\partial_H(A_2\parallel B\parallel C)$

$\partial_H(A_2\parallel B\parallel C)=E_A(m_5)\cdot\partial_H(A_3\parallel B\parallel C)$

$\partial_H(A_3\parallel B\parallel C)=C_B(m_1)\cdot\partial_H(A_4\parallel B_1\parallel C)$

$\partial_H(A_4\parallel B_1\parallel C)=g(N_B)\cdot\partial_H(A_4\parallel B_2\parallel C)$

$\partial_H(A_4\parallel B_2\parallel C)=E_B(m_6)\cdot\partial_H(A_4\parallel B_3\parallel C)$

$\partial_H(A_4\parallel B_3\parallel C)=C_C(m_2)\cdot\partial_H(A_4\parallel B_4\parallel C_1)$

$\partial_H(A_4\parallel B_4\parallel C_1)=D_A(m_5)\cdot\partial_H(A_4\parallel B_4\parallel C_2)$

$\partial_H(A_4\parallel B_4\parallel C_2)=D_B(m_6)\cdot\partial_H(A_4\parallel B_4\parallel C_3)$

$\partial_H(A_4\parallel B_4\parallel C_3)=E_A(m_7)\cdot\partial_H(A_4\parallel B_4\parallel C_4)$

$\partial_H(A_4\parallel B_4\parallel C_4)=E_B(m_8)\cdot\partial_H(A_4\parallel B_4\parallel C_5)$

$\partial_H(A_4\parallel B_4\parallel C_5)=C_D(m_3)\cdot\partial_H(A_4\parallel B_5\parallel C)$

$\partial_H(A_4\parallel B_5\parallel C)=D_B(m_8)\cdot\partial_H(A_4\parallel B_6\parallel C)$

$\partial_H(A_4\parallel B_6\parallel C)=T(N_B)\cdot\partial_H(A_4\parallel B_7C)+T'(N_B)\cdot\partial_H(A_4\parallel B_1\parallel C)$

$\partial_H(A_4\parallel B_7\parallel C)=C_E(m_4)\cdot\partial_H(A_5\parallel B_8\parallel C)$

$\partial_H(A_5\parallel B_8\parallel C)=D_A(m_7)\cdot\partial_H(A_6\parallel B_8\parallel C)$

$\partial_H(A_6\parallel B_8\parallel C)=T(N_A)\cdot\partial_H(A\parallel B_8\parallel C)+T'(N_A)\cdot\partial_H(A_1\parallel BC)$

$\partial_H(A\parallel B_8\parallel C)=\sum_{d\in\Delta} s_F(d_r)\cdot\partial_H(A\parallel B\parallel C)$

令 $\partial_H(AB\parallel C)=\langle X_1|E\rangle$，$E$ 表示以下的线性递归定义：

$\{X_1=\sum_{d\in\Delta} r_A(d)\cdot X_2$，

$X_2=g(N_A)\cdot X_3$，

$X_3=E_A(m_5)\cdot X_4$,
$X_4=C_B(m_1)\cdot X_5$,
$X_5=g(N_B)\cdot X_6$,
$X_6=E_B(m_6)\cdot X_7$,
$X_7=C_C(m_2)\cdot X_8$,
$X_8=D_A(m_5)\cdot X_9$,
$X_9=D_B(m_6)\cdot X_{10}$,
$X_{10}=E_A(m_7)\cdot X_{11}$,
$X_{11}=E_B(m_8)\cdot X_{12}$,
$X_{12}=C_D(m_3)\cdot X_{13}$,
$X_{13}=D_B(m_8)\cdot X_{14}$,
$X_{14}=T(N_B)\cdot X_{15}+T'(N_B)\cdot X_5$,
$X_{15}=C_E(m_4)\cdot X_{16}$,
$X_{16}=D_A(m_7)\cdot X_{17}$,
$X_{17}=T(N_A)\cdot X_{18}+T'(N_A)\cdot X_2$,
$X_{18}=\sum_{d\in\Delta}s_F(d_r)\cdot X_1\}$

对$\langle X_1|E\rangle$应用抽象操作符τ_I可得下列式子：

$$\begin{aligned}\tau_I(\langle X_1|E\rangle)&=\tau_I(\langle(\sum_{d\in\Delta}r_A(d)\cdot X_2)|E\rangle)\\&=\tau_I(\sum_{d\in\Delta}r_A(d)\langle X_2|E\rangle)\\&=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_2|E\rangle)\end{aligned}$$

$$\begin{aligned}&\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_2|E\rangle)\\&=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle(g(N_A)\cdot X_3)|E\rangle)\\&=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(g(N_A)\langle X_3|E\rangle)\\&=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_3|E\rangle)\end{aligned}$$

$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_3|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_4|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_4|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_5|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_5|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_6|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_6|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_7|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_7|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_8|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_8|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_9|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_9|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{10}|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{10}|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{11}|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{11}|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{12}|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{12}|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{13}|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{13}|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{14}|E\rangle)$$

$$\begin{aligned}&\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_{14}|E\rangle)\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau_I(T(N_B))\cdot\tau_I(\langle X_{15}|E\rangle)+\tau_I(T'(N_B))\cdot\tau_I(\langle X_5|E\rangle)]\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_I(\langle X_{15}|E\rangle)+\tau\cdot\tau_I(\langle X_5|E\rangle)]\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_I(\langle X_5|E\rangle)+\tau\cdot\tau_I(\langle(C_E(m_4)\cdot X_{16})|E\rangle)]\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_I(\langle X_5|E\rangle)+\tau\cdot\tau_I(\langle X_{16}|E\rangle)]\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_I(\langle X_5|E\rangle)+\tau\cdot\tau_I(\langle X_{17}|E\rangle)]\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_I(\langle X_5|E\rangle)+\tau\cdot([\tau_I(T(N_A))\cdot\tau_I(\langle X_{18}|E\rangle)+\tau_I(T'(N_A)\cdot\tau_I(\langle X_2|E\rangle)])]\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_I(\langle X_5|E\rangle)+\tau\cdot\tau_I(\langle X_2|E\rangle)+\tau\cdot\tau_I(\langle X_{18}|E\rangle)]\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_I(\langle X_5|E\rangle)+\tau\cdot\tau_I(\langle X_2|E\rangle)+\tau\cdot\tau_I(\sum_{d_r\in\Delta}s_F(d_r)\cdot\langle X_1|E\rangle)]\\&=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_I(\langle X_5|E\rangle)+\tau\cdot\tau_I(\langle X_2|E\rangle)+\tau\cdot\sum_{d_r\in\Delta}s_F(d_r)\cdot\tau_I(\langle X_1|E\rangle)]\\&=\sum_{d\in\Delta}r_A(d)\cdot\sum_{d_r\in\Delta}s_F(d_r)\cdot\tau_I(\langle X_1|E\rangle)\end{aligned}$$

由此可得：

$\tau_I(\partial_H(A\parallel B\parallel C))=\sum_{d\in\Delta}r_A(d)\cdot\sum_{d_r\in\Delta}S_F(d_r)\cdot\tau_I(\partial_H(A\parallel B\parallel C))$，证毕。

结束语 本文基于进程代数ACP对Otway-Rees协议进行了形式化验证，验证结果表明此协议抽象构成的形式系统展示了期望的外部行为。但是，本文所作的形式化分析并没有包括安全性分析。

参 考 文 献

[1] ZAJAC B P. Applied cryptography: Protocols, algorithms, and source code in C[J]. Computers & Security, 1994, 13(3): 217-218.

[2] OROS H, BOIAN F. Spi calculus analysis of Otway-Rees protocol[J]. International Journal of Computers, Communications & Control (IJCCC), 2008, 3(3): 427-432.

[3] Fokkink. Introduction to Process Algebra[J]. Texts in Theoretical Computer Science An Eatcs, 2000: 1-163.

[4] VAGLINI G. Communication and concurrency: R Milner Prentice Hall (1989) 260pp 17. 95 softback[J]. Information and Software Technology, 1991, 33(6): 462.

[5] HOARE T, O'HEARN P. Separation Logic Semantics for Communicating Processes[J]. Electronic Notes in Theoretical Computer Science, 2008, 212: 3-25.

[6] BERGSTRA J A, KLOP J W. Algebra of communicating processes with abstraction[J]. Theoretical Computer Science, 1985, 37(85): 77-121.

[7] 王勇，许荣强，任兴田，等. 可信计算中信任链建立的形式化验证[J]. 北京工业大学学报，2016，42(3)：73-78.

[8] 王勇，方娟，任兴田，等. 基于进程代数的TCG远程证明协议的形式化验证[J]. 计算机研究与发展，2013(2)：103-109.

CAI Yu-tong, born in 1996, postgraduate. Her main research interests include big data and deep learning.