计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200500074

基于进程代数的 Yahalom 协议正确性的形式化验证

王然然[1]　王　勇[1]　蔡雨桐[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
(1092526108@qq.com)

摘　要　通信过程中为了使得通信双方之间的对话过程是安全传输的,在引入可信第三方的基础上,Yahalom 协议借助于可信第三方为通信双方分配"好"的会话密钥,利用该共享密钥加密对话内容保证双方对话的安全。Yahalom 协议的形式化验证具有很重要的意义。为了使可信第三方在通信双方之间安全地分配会话密钥,文中对通信过程进行理论化形式的验证。文中基于可信平台的随机会话密钥分配过程进行了抽象化的处理,给出了抽象模型中各个实体状态及状态变迁的操作语义描述,建立了 Yahalom 协议结构化的操作语义并发计算模型,主要通过 ACP 公理系统对 Yahalom 协议的状态变迁系统进行了形式化的验证,验证结果表明 Yahalom 协议系统地展示了期望的外部行为,从理论上证明了基于进程代数的 Yahalom 协议是可行的。

关键词:Yahalom 协议;进程代数;形式化的验证;可信第三方;ACP 公理系统
中图法分类号　TP301.2

Formal Verification of Yahalom Protocol Based on Process Algebra

WANG Ran-ran[1],WANG Yong[1],CAI Yu-tong[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　In the process of communication,in order to make the conversation between the two sides safe,Yahalom protocol uses the trusted third party to distribute the "good" conversation key to the two sides of communication,and uses the shared key to encrypt the conversation content to ensure the security of the conversation between the two sides. The formal verification of Yahalom protocol is of great significance. In order to make the trusted third party distribute the session key safely between the two sides of communication,this paper makes a theoretical verification of the communication process. In this paper,the process of random session key distribution based on trusted platform is abstracted,the operational semantic description of each entity's state and state transition in the abstract model is given,and the structural operational semantic concurrent computing model of Yahalom protocol is established. The formal verification of Yahalom protocol's state transition system is mainly carried out through ACP public system. The results show the expected external behavior,and theoretically proves that Yahalom protocol based on process algebra is feasible.

Keywords　Yahalom protocol,Algebra process,Formal verification,Trusted third party,ACP axiom system

随着计算机通信技术的迅速发展,人们对计算机网络安全性的要求越来越高。Yahalom 协议作为建立在密码体制基础上的一种交互通信的协议,借助于密码学算法来安全地完成通信双方密钥的分配,并完成通信双方之间的身份认证。作为一种基于单钥体制的经典认证协议,Burrow 等提出的 Yahalom 协议[1]可以利用可信第三方 Trent 完成通信双方之间的会话密钥的分配任务。假设两个通信主体都相信 Trent 可以为他们分发好的会话密钥,二者之间通过可信第三方完成了会话密钥分发的任务[2],"好"的会话密钥确保通信数据传输的安全可靠性。本文结合进程代数的知识[3],用数学的方式对 Yahalom 协议进行了描述和刻画,用 ACP 的公理系统对 Yahalom 协议进行了形式化的验证,通过严格的数学推理证明得出的 Yahalom 协议是正确的。

1　ACP 基础知识

进程代数是描述并发和通信系统的数学工具,适合对复杂系统进行模型分析。进程代数在计算机系统性能评价方面产生了一些较好的分析方法,对复杂系统进行模型的简化,相比其他性能评价方法具有其独特的优势。进程代数提供了结构化的操作语义,能够将代数项映射到带标号的变迁系统,具有自然的合成和抽象能力,从形式上可以对复杂系统进行形式化正确性的判断,提供了一种系统性能评价的新思路。

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,文献[14]提出了通信系统演

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)

算和通信顺序进程 CCS，Hoare 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 等在 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 Yahalom 协议

Yahalom 协议是由 Burrow 等于在 1990 年提出的一种基于单钥体制的经典认证协议。它是计算机安全界研究人员分析的最重要的密钥建立协议之一。参加协议的主体是通信双方 Alice，Bob 和可信第三方 Trent。在可信第三方 Trent 的参与下，且不使用时间戳的前提下，该协议可以实现两个通信双方建立会话密钥的任务。其中，Alice 和 Bob 分别同可信第三方共享一个秘密密钥。Yahalom 协议的核心思想是通过可信第三方 Trent 为通信双方安全地产生并分配会话秘钥；假设可信第三方能得到通信双方的信任，并且有能力生成好的会话秘钥。图 1 给出了 Yahalom 协议的工作流程图。假设 Alice 和 Bob 都与可信第三方 Trent 有一个共享密钥，且彼此都握有这个密钥。本文将 Alice 和 Trent 的秘钥记作 Kat，将 Bob 和 Trent 的秘钥记作 Kbt，将 Alice 和 Bob 生成的随机会话秘钥记作 Kab。Alice，Bob 同可信第三方的通信过程如下，其中 Alice 记为主体 A，Bob 简记为主体 B，可信第三方 Trent 简记为可信第三方 T。

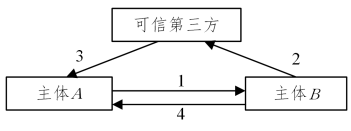

图 1 Yahalom 协议流程图

Fig. 1 Yahalom protocol flow chart

第一步 Alice 产生一个随机数 N_a，该原子操作记为 $g(N_a)$。Alice 将该随机数和自己的名字作为消息 $M_1(A, N_a)$ 发给通信的另一方 Bob。

第二步 Bob 将自己的名字作为消息 M_2(B)。Bob 在读取消息 M_1 后，也产生一个随机数 N_b，该原子操作记为 $g(N_a)$，随后 Bob 将 Alice 的名字、Alice 的随机数 N_a 以及自己的随机数 N_b 用自己与可信第三方的共享秘钥加密，该原子操作为 $e_{bt}(A, N_a, N_b)$，将加密的结果作为消息 $M_3(\{A, N_a\}k_{bt})$。Bob 将消息 M_2 和 M_3 发给可信第三方 Trent。

第三步 可信第三方读取消息 M_2 和 M_3 后，用它和 Bob 的共享密钥解密消息 M_3，该原子操作记为 $d_{bt}(M_3)$，为通信双方 Alice 和 Bob 分配随机会话秘钥 Kab，并产生两条消息，第一个消息是将 Bob 的名字、Bob 的随机数 N_b、Alice 的随机数 Na 和通信两方的随机会话秘钥 Kab 用 Alice 和可信第三方的共享秘钥 Kat 加密，并将消息简记为 $M_4(\{B, N_a, N_b, K_{ab}\}K_{at})$，加密消息的原子操作记为 $e_{at}(B, N_a, N_b, K_{ab})$，第二个消息是将 Bob 的随机数用可信第三方和 Bob 的共享秘钥 Kbt 加密作为消息 $M_5(\{N_b\}K_{bt})$，将 M_4 和 M_5 发送给 Alice。

第四步 Alice 利用自己与可信第三方的共享秘钥对收到的消息 M_4 进行解密，该操作记为 $d_{at}\{M_4\}$，验证自己收到的两个随机数是否与自己发给 Bob 的随机数是一致的。若收到的随机数与 Alice 之前发给 Bob 的随机数不一致，该原子操作记为 $t'\{N_a\}$，则 Alice 回到第一步，重新发起与 Bob 的通信请求。若随机数一致，该原子操作记为 $t\{N_a\}$，则确认从消息 M_4 中提取的自己的和 Bob 的会话密钥 K_{ab} 是由可信第三方分配的会话密钥，确认自己与 Bob 进行通信操作是安全的。Alice 将发送给 Bob 两条消息。用 Alice 和 Bob 的会话秘钥加密 Bob 的随机数 N_b 作为消息 $M_6(\{N_b\}k_{ab})$，该操作记为 $e_{ab}\{N_b\}$，第二条是它把自己收到的由可信第三方和 Bob 的共享秘钥加密的内容消息 M_5 原封不动地再发给 Bob。

第五步 Bob 用他与 Trent 的密钥解密，对接收的消息 M_5 进行解密操作，该操作记为 $d_{bt}\{M_5\}$，得到可信第三方 Trent 为他与 Alice 分配的会话秘钥，在用得到的会话密钥 K_{ab} 解密消息 M_6，验证从消息 M_6 中得到的随机数是否与自己在第二步产生的随机数一样。若收到的随机数与 Bob 之前发给 Trent 的随机数不一致，该原子操作记为 $t'\{N_b\}$，则 Bob 回到第二步再次生成新的随机数，向可信第三方发送消息，请求分配与 Alice 会话密钥的通信请求。若随机数一致，该原子操作记为 $t\{N_b\}$，则确认自己和 Alice 的会话密钥是 K_{ab}，确定通过 Trent 分配的会话密钥是安全的、可靠的。

最后，经过彼此 Alice 和 Bob 的互相验证确定自己是在同通信的另一方进行会话。

3 Yahalom 协议的形式化分析

3.1 协议抽象

对 Yahalom 协议进行抽象处理，得到如图 2 所示的协议模型。其中，通信双方 Alice 和 Bob 简记为 A 和 B，可信第三方简记为 T。通道 A 和通道 F 是外部通道，通道 B, C, D, E 为协议的内部信道。

主体三方之间的信息交互过程抽象为图 2 所示的模型。

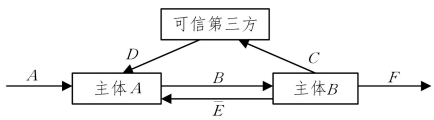

图 2 Yahalom 协议抽象模型

Fig. 2 Yahalom protocol abstract model

其中，M_1, M_2, M_3, M_4 消息的具体内容抽象为如下的符号：

$A->B: M_1(A, N_a)$

$B->T: M_2(B)M_3(\{A, N_a\}k_{bt})$

$T->A: M_4(\{B, N_a, N_b, k_{ab}\}k_{at})M_5(\{N_b\}k_{bt})$

$A->B: M_5(\{N_b\}k_{bt})M_6(\{N_b\}k_{ab})$

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

3.2 ACP 描述

ACP 是建立在等式逻辑的基础上的，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 $\|$，$|$，$\llcorner$，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 τ_I；

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

通信方 Alice 的状态变迁 ACP 描述如下：

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

$A_1=g(N_a)\cdot A_2$

$A_2=s_B(M_1)\cdot A_3$

$A_3=r_D(M_4,M_5)\cdot A_4$

$A_4=d_{as}(M_4)\cdot A_5$

$A_5=t'(N_a)\cdot A+t(N_a)\cdot A_6$

$A_6=e_{ab}(M_6)\cdot A_7$

$A_7=S_E(M_5,M_6)\cdot A$

其中，A_i 为 Alice 所处的不同状态，Δ 为 A 从外界输入的数据 d 和 B 向外界输出的数据d_r的集合。

通信方 Bob 的状态变迁 ACP 描述如下：

$B=r_B(M_1)\cdot B_1$

$B_1=g(N_b)\cdot B_2$

$B_2=e_{bt}(M_3)\cdot B_3$

$B_3=S_C(M_2,M_3)\cdot B_4$

$B_4=r_E(M_5,M_6)\cdot B_5$

$B_5=d_{bt}(M_5)\cdot B_6$

$B_6=d_{ab}(M_6)\cdot B_7$

$B_7=t'(N_b)\cdot B_1+t(N_b)\cdot B_8$

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

可信第三方 Trent 的状态变迁 ACP 描述如下：

$T=r_C(M_2,M_3)\cdot T_1$

$T_1=d_{bt}(M_3)\cdot T_2$

$T_2=e_{at}(M_4)\cdot T_3$

$T_3=e_{bt}(M_5)\cdot T_4$

$T_4=S_D(M_4,M_5)\cdot T$

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：

$\gamma(s_B(M_1),r_B(M_1))\triangleq C_B(M_1)$

$\gamma(s_C(M_2,M_3),r_C(M_2,M_3))\triangleq C_C(M_2,M_3)$

$\gamma(s_D(M_4,M_5),r_D(M_4,M_5))\triangleq C_D(M_4,M_5)$

$\gamma(s_E(M_5,M_6),r_E(M_5,M_6))\triangleq C_E(M_5,M_6)$

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

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

其中：

$H=\{s_B(M_1),r_B(M_1),s_C(M_2,M_3),r_C(M_2,M_3),s_D(M_4,M_5),r_D(M_4,M_5),s_E(M_5,M_6),r_E(M_5,M_6)\mid M_1,M_2,M_3,M_4,M_5,M_6\in\Delta_2\}$

$I=\{C_B(M_1),C_C(M_2,M_3),C_D(M_4,M_5),C_E(M_5,M_6),g(N_a),g(N_b),d_{at}(M_4),d_{bt}(M_3),d_{bt}(M_5),d_{ab}(M_6),e_{at}(M_4),e_{bt}(M_3),e_{bt}(M_5),e_{ab}(M_6)\}$

3.3 形式化分析

命题 1 直接证明 Yahalom 系统具有期望的外部行为。$\tau_I(\partial_H(A\parallel B\parallel T))$具有期望的外部行为[7]。

$A\parallel B\parallel T=(A\parallel B)\parallel T\xrightleftharpoons{M_1}(A\parallel B)\between T+T\between(A\parallel B)+(A\parallel B)\mid T$

令 $AB=Z$，则 $A\parallel B\parallel T=Z\parallel T$

$A\parallel B\xrightleftharpoons{M_1}A\between B+B\between A+A\mid B$

$\xrightleftharpoons{RDP}(\sum_{d\in\Delta}r_A(d)\cdot A_1)\between B+(r_B(M_1)\cdot B)\between A+(\sum_{d\in\Delta}r_A(d)\cdot A_1)\mid(r_B(M_1)\cdot B)$

$\xrightleftharpoons{LM_3,CM_8}\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B)+r_B(M_1)\cdot(B_1\parallel A)+\gamma(\sum_{d\in\Delta}r_A(d)\cdot r_B(M_1))\cdot(A_1\parallel B_1)$

$\xrightleftharpoons{CM_6,A_7}\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B)+r_B(m_1)\cdot(B_1\parallel A)+\delta$

$\xrightleftharpoons{A_6,A_7}\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B)+r_B(m_1)\cdot(B_1\parallel A)$

$Z\parallel T\xrightleftharpoons{M_1}Z\between T+T\between Z+Z\mid T$

$\xrightleftharpoons{RDP}(\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B)+r_B(M_1)\cdot(B_1\parallel A))\between T+(r_C(M_2,M_3)\cdot T_1)\between Z+(\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B)+r_B(M_1)\cdot(B_1\parallel A))\mid(r_C(M_2,M_3)\cdot T_1)$

$\xrightleftharpoons{LM_3,LM_4,CM_9}(\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B))\between T+(r_B(M_1)\cdot(B_1\parallel A))\between T+r_C(M_2,M_3)\cdot(T_1\parallel Z)+(\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B))\mid(r_C(M_2,M_3)\cdot T_1)+r_B(M_1)\cdot(B_1\parallel A)\mid(r_C(M_2)\cdot T_1)$

$\xrightleftharpoons{A_7,CM_9,CM_{13}}(\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B))\between T+(r_B(M_1)\cdot(B_1\parallel A))\between T+r_C(M_2,M_3)\cdot(T_1\parallel Z)+\delta+\delta$

$\xrightleftharpoons{LM_3}\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B\parallel T)+(r_B(M_1)\cdot(B_1\parallel A\parallel T)+r_C(M_2,M_3)\cdot(T_1\parallel Z)$

$\partial_H(A\parallel B\parallel T)$

$\xrightleftharpoons{LM_3}\partial_H(\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B\parallel T)+(r_B(M_1)\cdot(B_1\parallel A\parallel T)+r_C(M_2,M_3)\cdot(T_1\parallel Z))$

$\xrightleftharpoons{D_4}\partial_H(\sum_{d\in\Delta}r_A(d)\cdot(A_1\parallel B\parallel T))+\partial_H((r_B(M_1)\cdot(B_1\parallel A\parallel T))+\partial_H(r_C(M_2,M_3)\cdot(T_1\parallel Z))$

$\xrightleftharpoons{D_5}\partial_H(\sum_{d\in\Delta}r_A(d))\cdot\partial_H(A_1\parallel B\parallel T)+\partial_H(r_B(M_1))\cdot\partial_H(B_1\parallel A\parallel T)+\partial_H(r_C(M_2,M_3))\cdot\partial_H(T_1\parallel Z)$

$\xrightleftharpoons{D_1,D_2,A_4,A_7}\sum_{d\in\Delta}r_A(d)\cdot\partial_H(A_1\parallel B\parallel T)$

同理可得：

$\partial_H(A_1\parallel B\parallel T)=g(N_a)\cdot\partial_H(A_2\parallel B\parallel T)$

$\partial_H(A_2\parallel B\parallel T)=C_B(M_1)\cdot\partial_H(A_3\parallel B_1\parallel T)$

$\partial_H(A_3\parallel B_1\parallel T)=g(N_b)\cdot\partial_H(A_3\parallel B_2\parallel T)$

$\partial_H(A_3\parallel B_2\parallel T)=e(M_3)\cdot\partial_H(A_3\parallel B_3\parallel T)$

$\partial_H(A_3\parallel B_3\parallel T)=C_C(M_2,M_3)\cdot\partial_H(A_3\parallel B_4\parallel T_1)$

$\partial_H(A_3\parallel B_4\parallel T_1)=d_{bt}(M_3)\cdot\partial_H(A_3\parallel B_4\parallel T_2)$

$\partial_H(A_3\parallel B_4\parallel T_2)=e_{at}(M_4)\cdot\partial_H(A_3\parallel B_4\parallel T_3)$

$\partial_H(A_3\parallel B_4\parallel T_3)=e_{at}(M_5)\cdot\partial_H(A_3\parallel B_4\parallel T_4)$

$\partial_H(A_3\parallel B_4\parallel T_4)=C_D(M_4,M_5)\cdot\partial_H(A_4\parallel B_4\parallel T)$

$\partial_H(A_4\parallel B_4\parallel T)=d_{at}(M_4)\partial_H(A_5\parallel B_4\parallel T)$

$\partial_H(A_5\parallel B_4\parallel T)=t'(N_a)\cdot\partial_H(A\parallel B\parallel T)+t(N_a)\cdot\partial_H(A_6\parallel B_4\parallel T)$

$\partial_H(A_6\parallel B_4\parallel T)=e_{ab}(M_6)\cdot\partial_H(A_7\parallel B_4\parallel T)$

$\partial_H(A_7\parallel B_4\parallel T)=C_E(M_5,M_6)\cdot\partial_H(A\parallel B_5\parallel T)$

$\partial_H(A\parallel B_5\parallel T)=d_{bt}(M_5)\cdot\partial_H(A\parallel B_6\parallel T)$

$\partial_H(A\parallel B_6\parallel T)=t'(N_b)\cdot\partial_H(A_3\parallel B_1\parallel T)+t(N_a)\cdot\partial_H(A\parallel B_8\parallel T)$

$\partial_H(A\parallel B_8\parallel T)=\sum_{d_r\in\Delta}S_F(d_r)\cdot\partial_H(A\parallel B\parallel T)$

令$\partial_H(A\parallel B\parallel T)=\langle X_1\mid E\rangle$，$E$ 表示以下的线性递归定义：

$$\{X_1=\sum_{d\in\Delta}r_A(d)\cdot X_2$$
$$X_2=g(N_a)\cdot X_3$$
$$X_3=C_B(M_1)\cdot X_4$$
$$X_4=g(N_b)\cdot X_5$$
$$X_5=e(M_3)\cdot X_6$$
$$X_6=C_C(M_2,M_3)\cdot X_7$$
$$X_7=d_{bt}(M_3)\cdot X_8$$
$$X_8=e_{at}(M_4)\cdot X_9$$
$$X_9=e_{at}(M_5)\cdot X_{10}$$
$$X_{10}=C_D(M_4,M_5)\cdot X_{11}$$
$$X_{11}=d_{at}(M_4)\cdot X_{12}$$
$$X_{12}=t'(N_a)\cdot X_1+t(N_a)\cdot X_{13}$$
$$X_{13}=e_{ab}(M_6)\cdot X_{14}$$
$$X_{14}=C_E(M_5,M_6)\cdot X_{15}$$
$$X_{15}=d_{bt}(M_5)\cdot X_{16}$$
$$X_{16}=d_{ab}(M_6)\cdot X_{17}$$
$$X_{17}=t'(N_b)\cdot X_4+t(N_a)\cdot X_{18}$$
$$X_{18}=\sum_{d_r\in\Delta}S_F(d_r)\cdot X_1\}$$

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

$$\tau_I(\langle X_1|E\rangle)=\tau_I(\langle\sum_{d\in\Delta}r_A(d)\cdot X_2|E\rangle)$$
$$=\tau_I(\sum_{d\in\Delta}r_A(d)\cdot\langle X_2|E\rangle)$$
$$=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_2|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_2|E\rangle)$$
$$=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle g(N_a)\cdot X_3|E\rangle)$$
$$=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(g(N_a)\cdot\langle X_3|E\rangle)$$
$$=\sum_{d\in\Delta}r_A(d)\cdot\tau_I(\langle X_3|E\rangle)$$

同理可得：

$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_3|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_4|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_4|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_5|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_5|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_6|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_6|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_7|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_7|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_8|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_8|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_9|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_9|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_{10}|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_{10}|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_{11}|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_{11}|E\rangle)=\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_{12}|E\rangle)$$
$$\sum_{d\in\Delta}r_A(d)\cdot\tau_1(\langle X_{12}|E\rangle)$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau_1(t'(N_a)\cdot\tau_1(\langle X_1|E\rangle))+\tau_1(t(N_a)\cdot\tau_1(\langle X_{13}|E\rangle))]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1(\langle X_{13}|E\rangle)]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1((\langle e(M_6)\cdot X_{14}\rangle|E\rangle)]=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1(\langle X_{14}|E\rangle)]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1(\langle X_{15}|E\rangle)]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1(\langle X_{16}|E\rangle)]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1(\langle X_{17}|E\rangle)]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot([\tau_1(t'(N_b))\cdot\tau_1(\langle X_4|E\rangle)+\tau_1(t(N_b))\cdot\tau_1(\langle X_{18}|E\rangle])]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1(\langle X_4|E\rangle)+\tau\cdot\tau_1(\langle X_{18}|E\rangle)]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1(\langle X_4|E\rangle)+\tau\cdot\tau_1(\sum_{d_r\in\Delta}s_F(d_r)\cdot\tau_1\langle X_1|E\rangle)]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot[\tau\cdot\tau_1(\langle X_1|E\rangle)+\tau\cdot\tau_1(\langle X_4|E\rangle)+\tau\cdot\sum_{d_r\in\Delta}s_F(d_r)\cdot\tau_1(\langle X_1|E\rangle)]$$
$$=\sum_{d\in\Delta}r_A(d)\cdot\sum_{d_r\in\Delta}s_F(d_r)\cdot\tau_1(\langle X_1|E\rangle)$$

由此可得：

$$\tau_I(\partial_H(A\|B\|T))=\sum_{d\in\Delta}r_A(d)\cdot\sum_{d_r\in\Delta}S_F(d_r)\cdot(\partial_H(A\|B\|T))$$

通过形式化验证，得到 Yahalom 协议系统具有期望的外部行为。

结束语 本文利用进程代数的数学符号对 Yahalom 协议进行了刻画和描述，在结构化的操作语义基础下，用代数项将该协议映射到带标号的变迁系统，模拟 Yahalom 协议的工作流程。以 ACP 公理系统为基础，对 Yahalom 协议为通信双方分配会话密钥的过程进行了一系列的形式化推导，基于进程代数对 Yahalom 协议系统进行形式化的验证，验证的结果表明 Yahalom 协议系统具有期望的外部行为[8]，明确指出了该协议是正确的。

参 考 文 献

[1] CHOO K K R. A Proof of Revised Yahalom Protocol in the Bellare and Rogaway (1993) Model[J]. The Computer Journal, 2007, 50: 591-601.

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

[3] FOKKINK W. 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, HEARN P O. Separation Logic Semantics for Communicating Processes[J]. NULL, 2008, 212: 3-25.

[6] BERGSTRA J A, KLOP J W. Algebra of communicating processes with abstraction[J]. Theoretical Computer Science, 1985, 37: 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.

WANG Ran-ran, born in 1996, postgraduate. Her main research interests include big data and deep learning.