基于离线可信第三方的公平电子合同签署协议

丁振国[1],刘多峥[1],刘美玲[2]
(1.西安电子科技大学 计算机学院,陕西 西安 710071;
2.西安电子科技大学 软件工程研究所,陕西 西安 710071)

摘 要:电子合同签署是电子商务中的一个重要领域,公平电子合同签署协议是公平交换协议的一种应用模型,然而已有的公平电子合同签署协议存在各种安全缺陷。设计了一种新的基于离线可信第三方的公平电子合同签署协议,该协议能够解决已有协议的缺陷,并且提高了协议的执行效率。对协议的安全性进行了分析和证明,结果表明,本协议保证了交换活动的公平进行,从而为电子商务提供了完整的安全保障。

关键词:公平交换协议;电子合同签署协议;可信第三方;计算机网络安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2009)06-0171-04

A Fair Electronic Contract Signing Protocol Based on Off-Line Trusted Third Party

DING Zhen-guo[1], LIU Duo-zheng[1], LIU Mei-ling[2]
(1. College of Computer Science, Xidian University, Xi'an 710071, China;
2. Software Engineering Institute, Xidian University, Xi'an 710071, China)

Abstract: Electronic contract signing is an important issue in electronic commerce, while fair electronic contract signing protocol is an application model of fair exchange protocol, but there were defects in traditional fair electronic contract signing protocols. Presents a new fair electronic contract signing protocol based on the off-line trusted third party. The protocol effectively prevents all kinds of security attacks, and improves the efficiency of the implementation. The security of the newly devised scheme is also examined and proved. It is showed that fair processes of exchange activities are guaranteed in this protocol.

Key words: fair exchange protocol; electronic contract signing protocol; trusted third party; computer network security

随着网络技术的发展,电子商务已经得到相当广泛的应用。然而网络固有的不安全性给通过网络进行安全可靠的商务活动带来了新的挑战,其中最重要的基础问题之一就是公平性。所谓公平性是指在交换过程结束后,参与交换的各方或者都得到了自己想要的东西,或者都没有得到任何有用的东西。公平交换协议可以满足公平性需求,使得参与交换的双方以公平的方式交换信息。目前,公平交换协议的研究主流是使用离线可信第三方(trusted third party,TTP)优化的公平交换协议[1,2],在没有出现异常问题的情况下,TTP不需要参与交易的任何一个环节,由于这类离线TTP协议克服了以前协议的所有缺陷,因此被称为优化的或乐观的公平交换协议。公平电子合同签署协议便是公平交换协议的一种应用模型。

公平电子合同签署协议[3]是针对以下场景提出的:Alice与Bob要签署一份已达成共识的合同,协议目的是保证协议结束后,双方都能得到对方签署的合同文件;若失败,则双方都得不到任何有效文件。Micali在PODC2003上提出了几个简单的乐观公平交换协议[4],但是其中的公平电子合同签署协议(即ECS1协议)已经被Feng Bao等人证明是不安全的[5]。

文中设计出一个安全的基于离线的可信第三方的公平电子合同签署协议,并进一步对该协议的安全性进行了讨论,说明该协议满足公平交换协议最重要的公平性以及其它重要的性质。

1 公平交换协议的设计原则

公平交换协议是安全协议的一种,但是与传统的安全协议不完全相同,因此,在设计公平交换协议时需

收稿日期:2008-09-19;**修回日期**:2008-12-04
基金项目:国家863计划项目(2004AAS1Z2520-1);装备技术基础项目(2006QB1070)
作者简介:丁振国(1959-),男,陕西三原人,教授,硕士生导师,研究方向为计算机网络与信息处理。

考虑的问题也有差异[6,7]。

(1)明确公平交换协议要求的信道质量。

在传统安全协议中,通常假设协议在不安全的信道上进行,攻击者完全控制通信,所有在信道上传输的消息都有可能被拦截、篡改、重放。而在公平交换协议中,有时需要对信道有更高的要求。1999 年,Pagnina 和 Gartner 证明了没有可信第三方的存在,就不可能有真正公平的公平交换协议[8]。这就说明,如果协议只在不可靠信道上进行,也不可能建立真正的公平交换协议。因此,在设计乐观公平交换协议时,需要给出合适的信道质量的假设。

(2)明确公平交换协议面临的攻击者能力。

在传统的安全协议中,通常假设协议在攻击者可以完全控制的网络环境中运行,诚实参与者互相信任,他们想要通过合作获得共同目标。在公平交换协议中,由(1)知道,在有 TTP 参与的协议中,攻击者不能完全控制信道。因为在公平交换协议中,参与协议的各方没有共同的利益和目标,在某种意义上,参与者总是在和攻击者运行协议。因此,除了考虑外部入侵者以外,恶意的一方可以是参与协议的实体中的一个。传统的安全协议必须对外部入侵者是安全的,公平交换协议甚至对恶意的参与者也是安全的。

(3)确保协议执行过程的唯一性。

在传统的安全协议中,一般不存在子协议,协议一般是按固定的顺序执行。而在公平交换协议中,往往存在多个子协议,协议的运行通常没有唯一的路径,在不同情况下可能存在不同的执行顺序。协议设计者必须使得协议在任何情况下都只能选择一种路径,否则有可能破坏协议的安全性。

2 公平电子合同签署协议设计

下面首先介绍将用到的符号、概念及系统假设,然后构造我们的公平电子合同签署协议。该协议包括交换子协议和争端解决子协议两部分。

2.1 符号、概念及系统假设

文中将用到的符号和记号表示如下:

* $H(x)$:对消息 x 的安全的单向抗碰撞的杂凑函数;

* 协议发起者 Alice 的身份标识记为 A,协议响应者 Bob 的身份标识记为 B,参与协议的双方互不信任,但双方都信任离线 TTP P_t,同意由 P_t 在他们不能完成公平交换时介入,帮助他们完成交换。假设协议的每一方以及 TTP 均应用如 Goldwasser 等人[9] 所定义的抗自适应选择明文攻击的非对称密码算法,都有各自的公钥和私钥,可以用于对消息的加密/解密或签名/验证;

* C:系统中双方要签署的电子合同;

* D:电子合同 C 的单向抗碰撞的杂凑函数;

* $R_i(i = A, B)$:i 选择的一次性随机数;

* $E_{P_i}(x), D_{P_i}(x)$:分别是应用 P_i 的公/私钥对消息 x 进行加密/解密;

* $\mathrm{SIG}_i(x)$ $(i = A, B)$:应用 i 的私钥对消息 x 进行签名;$\mathrm{VAL}_i(x)(i = A, B)$:应用 i 的公钥对消息 x 进行验证;

* X, Y:消息 X 和消息 Y 的逐比特连接;

* 发送端不可否认性:接收方必须能够证明接收到的信息确实是来自发送方。目的端不可否认性:发送方必须能够证明接收方确实收到了其发送的信息。

* 假定整个签名交换过程任何通信双方之间都使用了安全的通信协议(例如 SSL/TLS 协议等),用于满足信道质量要求,即在该信道上传输的消息在一定时间后总可以到达,攻击者不能拦截。

2.2 交换子协议

在交换子协议中,A 发起与 B 之间的公平交换。当参与交换的双方都非常诚实,公平交换成功完成时,用户之间的消息交换过程如图 1 所示。

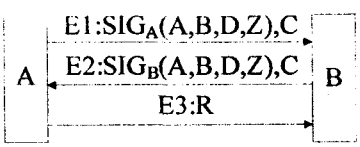

图 1 交换过程

公平交换过程包括以下 3 个步骤(E1) ~ (E3):

(E1):$A \rightarrow B$:$\mathrm{SIG}_A(A, B, D, Z), C$。

A 首先产生随机数 R,然后计算 $Z = E_{P_t}(A, B, D, R)$ 和数字签名 $\mathrm{SIG}_A(A, B, D, Z)$ 将 $\mathrm{SIG}_A(A, B, D, Z)$ 和数字合同 C 发送给 B。该数字签名作为合同签署协议的发起端不可否认的证据。

(E2):$B \rightarrow A$:$\mathrm{SIG}_B(A, B, D, Z), C$。

B 在收到 A 发来的信息后,对数字签名进行验证,验证过程如(V1)。

(V1):用 A 的公钥解密 $\mathrm{SIG}_A(A, B, D, Z)$ 得到四元组 $(A, B, D, Z) = \mathrm{VAL}_A(\mathrm{SIG}_A(A, B, D, Z))$,并确认 A 和 B 分别为协议发起方和响应方,$D = H(C)$。

如果(V1)验证未通过,则 B 请求 A 重新发送消息(E1)或终止协议的执行。否则,B 产生 (A, B, D, Z) 的数字签名 $\mathrm{SIG}_B(A, B, D, Z)$,并将其和数字合同 C 一起发送给 A。该数字签名作为合同签署协议的响应端不可否认的证据。

(E3):$A \rightarrow B$:R。

A 在接收到 B 发来的消息后,对数字签名进行验

证,验证过程如(V2)。

(V2):用 B 的公钥解密 $SIG_B(A,B,D,Z)$ 得到四元组 (A,B,D,Z),并确认 A 和 B 分别为协议发起方和响应方,$D = H(C)$,同时判断得到的 Z 是否与自己发送的相等。

如果(V1)验证未通过,则 A 请求 B 重新发送消息(E2)或终止协议的执行。否则,A 将本次协议的随机数 R 发送给 B。

B 在收到 R 后,对 R 进行验证,验证过程如(V3)。

(V3):用 P_t 的公钥加密四元组 (A,B,D,Z) 得到 Z',与从(E1)的信息中得到的 Z 进行比较,即验证 $Z' = Z$。

若(V3)验证通过,则公平交换过程成功完成。在这个过程中,B 得到了 A 的合同签署的承诺:$SIG_A(A,B,D,Z)$ 和 R,而 A 也得到了 B 的承诺:$SIG_B(A,B,D,Z)$ 和 R,协议结束。

若(V3)验证不通过或在一定时限内 B 未收到 A 发来的随机数,则 B 向 P_t 提出仲裁请求,进入争端解决过程。

2.3 争端解决子协议

当 B 在一定时限内没有接收到 A 的随机数,或者接收到的 R 无效时,B 与 P_t 联系,执行如图 2 所示的争端解决过程。

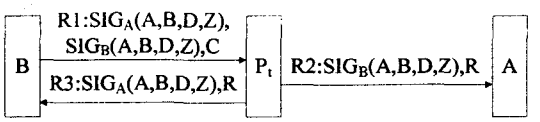

图 2　争端解决过程

争端解决过程包括以下 3 个步骤(R1) ~ (R3):

(R1):$B \rightarrow P_t$:$SIG_A(A,B,D,Z)$,$SIG_B(A,B,D,Z)$,C。

B 将 $SIG_A(A,B,D,Z)$,$SIG_B(A,B,D,Z)$,C 发送给 P_t,P_t 在接收到 B 的争端解决请求后,对所收到的信息进行验证,验证过程如(V4)。

(V4):分别用 A 和 B 的公钥解密 $SIG_A(A,B,D,Z)$ 和 $SIG_B(A,B,D,Z)$ 得到对应的四元组,并确认两个四元组的前两项 A 和 B 分别为协议发起方和响应方,第三项 $D = H(C)$,检验第四项中两个 Z 是否相等,若以上验证不通过,P_t 停止争端解决过程。若检验通过,P_t 用自己的私钥解密 Z,得到四元组 $(A,B,D,R) = D_{P_t}(Z)$,检验其中的前三项是否与前面得到的信息对应相等,若以上验证不通过,P_t 停止争端解决过程。否则,P_t 分别将 A 和 B 的合同签署承诺发给另一方。

(R2):$P_t \rightarrow A$:$SIG_B(A,B,D,Z)$,R。

P_t 将消息 $SIG_B(A,B,D,Z)$,R 发送给 A,这保证 A 得到了 B 对电子合同签署的承诺。

(R3):$P_t \rightarrow B$:$SIG_A(A,B,D,Z)$,R。

P_t 将消息 $SIG_A(A,B,D,Z)$,R 发送给 B,这保证 B 得到了 A 对电子合同签署的承诺。

在文献[5]中,由于电子合同的全部信息的长度不定,且比其他信息元素大很多,因此在进行签名和验证时需要进行大量运算。在计算 Z 的时候,为减小 Z 的长度,将电子合同信息用其单项散列函数的输出信息替代,同时也可提高计算 Z 的效率。在协议中,将电子合同信息全部由其单项散列函数的输出信息 D 替代。因为协议签订双方在签订合同前都已明确所要签署的协议内容,即 C 是已知的,由单项散列函数的性质可知,想要寻找一个 C' 使其单项散列函数等于 D,这在理论上不可能的,因此对 C 的签名等同于对 D 的签名。目前通常采用的单项散列函数的算法执行效率要比非对称密码算法高很多,因此采用这样的策略可以有效提高协议的执行效率。

3 安全性分析

下面来分析文中提出的公平电子合同签署协议的安全性。

3.1 公平性

若用户双方都诚实,交换过程成功完成,A 和 B 分别得到了对方对指定合同的签署承诺,满足公平性要求。若(V3)验证不通过或在一定时限内 B 未收到 A 发来的随机数,则 B 向 P_t 提出仲裁请求,进入争端解决过程。P_t 在(V4)验证通过后,从 Z 中解密出该协议的随机数 R,并将 $SIG_B(A,B,D,Z)$,R 发送给 A,将消息 $SIG_A(A,B,D,Z)$,R 发送给 B,依然满足公平性要求。

考虑 A 和 B 的各种欺骗攻击(A1) ~ (A4),如下所示。

(A1):假设 B 通过在(E2)中拒绝发送签名或发送错误的签名 $SIG_B(A',B',D',Z')$ 给 A,并向 P_t 请求进行争端解决,来进行攻击。如果 A 在一定时限内未收到 B 的签名,或对错误签名进行验证(V2)但结果失败,A 将终止该交换子协议。此时 A 没有得到 B 的合同签署的承诺,然而 B 虽然得到了 A 的签名,但是没有得到随机数 R,同样没有得到 A 的合同签署的承诺。于是 B 向 P_t 提出争端解决请求,若 B 提供正确的信息 $SIG_A(A,B,D,Z)$,$SIG_B(A,B,D,Z)$,C,P_t 在通过验证后,在(R2),(R3)中分别将正确的合同签署承诺发送出去,此时 A 和 B 均得到了承诺;若 B 提供错误的

信息，将无法通过 P_t 在(V4)中的验证，双方均得不到合同签署的承诺。

(A2)：假设 A 通过在(E3)中拒绝发送随机数或发送错误的随机数 R' 给 B 来进行攻击。如果 B 在一定时限内未收到 A 的随机数，或对 R' 进行验证(V3)但结果失败，B 将终止该协议，并向 P_t 提出争端解决请求，B 向 P_t 提供正确的请求信息 $SIG_A(A,B,D,Z)$，$SIG_B(A,B,D,Z)$，C，P_t 在验证通过后，在(R2)，(R3)中分别将正确的合同签署承诺发送出去，此时 A 和 B 均得到了承诺。

(A3)：假设 A 通过在(E1)中发送假签名进行攻击。A 也只能对签名消息中的 Z 做些改变，因为其它的信息都是 B 可以检验的。A 可以把其中的身份标识 A，B 换成别的用户的身份识别码或者用随机数代替，或者把 D 换成某个随机数，即 $Z' = E_{P_t}(A',B',D',R)$，其中 A'，B'，D' 中至少有一个是错误信息。B 虽然在此不能验证 Z' 的正确性，但是在进行到(E3)后，B 得到了随机数 R，当进行(V3)时验证失败，$Z' \neq Z$，B 将终止该协议，并向 P_t 提出争端解决请求，B 向 P_t 提供请求信息 $SIG_A(A,B,D,Z')$，$SIG_B(A,B,D,Z')$，C，，P_t 在(V4)中解密 Z' 时发现 A'，B'，D' 中存在错误的信息，验证不通过，P_t 终止该子协议。此时 A 得到的信息为 $SIG_B(A,B,D,Z')$，R，B 为 $SIG_A(A,B,D,Z')$，R，然而其中的 $Z' \neq E_{Pt}(A,B,D,R)$，不能作为本次合同签署的承诺。

(A4)：假设 B 与外部攻击者 F 合谋想要获得 A 对合同的承诺，却不想让 A 获得自己对合同的承诺。对这种攻击进行分析是因为在本协议中存在不诚实参与者与外部攻击者合谋的情况。在 B 收到 A 发来的正确的签名后，只能与 F 合谋试图获得 R，而不能通过欺骗 A 和 P_t 来获得，原因如(A1)所述。但是 R 与 A，B 和 D 联系在一起，即与每次协议的发起方、响应方和所签署的合同都有关系。P_t 在解决争端时，通过(V4)进行验证，要检验 Z 中的 A 和 B 是否分别是发起方和相应方，这将使 B 与 F 的合谋攻击失败，具体合谋攻击过程如图3所示。首先 B 获得 A 的正确签名，验证后获得其中的四元组，将对四元组进行调整并重新封装后的信息 $SIG_B(F,B,D,Z)$，C 发送给 F，F 返回应答信息 $SIG_F(F,B,D,Z)$，C。B 将 $SIG_F(F,B,D,Z)$，$SIG_B(F,B,D,Z)$，C 发送给 P_t，在(V4)中对双方签名的验证都正确。当解密 Z 后，得到的信息为 (A,B,D,R)，其中的发起方与签名的发起方不一致，根据争端解决协议说明，P_t 将终止协议的进行。这样，B 仍然得不到 R。

因此，提出的公平电子合同签署协议对于 A 和 B 的各种欺骗攻击都是公平的。

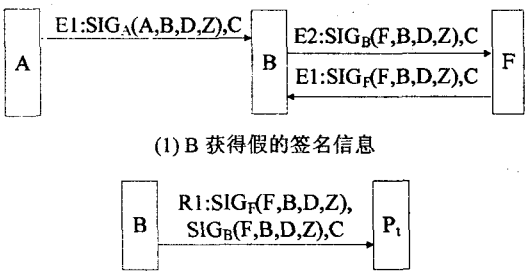

图 3 B 和 F 合谋攻击过程

3.2 不可否认性与不可伪造性

发起端不可否认性：在本协议中，A 提供对四元组的签名 $SIG_A(A,B,D,Z)$。B 和 P_t 分别在(E1)和(R1)中获得该签名，并对其进行检验，这保证了 A 的不可否认性。响应端不可否认性：B 提供对四元组的签名 $SIG_B(A,B,D,Z)$。A 和 P_t 分别可以在(E2)或(R1)中获得该签名，并对其进行验证，这保证了 B 的不可否认性。由于文中各方的私钥均为秘密信息，并不公开，而公钥为公开信息，攻击者无法得到用户的私钥，因此协议双方的签名满足不可伪造性。

3.3 TTP 可恢复性

A 和 B 分别产生对合同签署的承诺，其中 Z 是用 P_t 的公钥进行加密而得到的。P_t 在(R1)中接收到双方的签名信息，在(V4)中已经证明，P_t 可以从 Z 中恢复出随机数，并与双方的签名信息组成合同签署的承诺。因此，本协议具有 TTP 的可恢复性。

3.4 签名的保密性

由于假定整个签名交换过程任何通信双方之间都使用了安全的通信协议(例如 SSL/TLS 协议等)，因此能够满足消息保密性要求。

4 结束语

虽然网络技术已经得到广泛的应用，但网络应用本身仍然具有安全缺陷。在安全可靠的电子商务活动中，公平性显得尤其重要。公平电子合同签署协议是安全电子商务的基石，保证参与合同签署的双方都得到对方的承诺，或都得不到对方的任何承诺。文中提出了一种带有离线可信第三方的公平电子合同签署协议，能够保证交换活动公平的进行，为电子商务提供了完整的安全保障。

参考文献：

[1] Ray I, Ray I. Fair exchange in E-commerce[J]. ACM SIGecom Exchanges, 2002, 3(2): 9-17.

(下转第 178 页)

URL 地址访问，可在 WEB 服务器上建立一个访问数据库的页面用户权限表，在页面的开始位置通过程序代码进行用户合法性检查，以防止非法用户入侵到系统的核心数据库中。

(2)视图。

视图是由行和列组成的虚拟表格，是一个数据结果集，用户通过这个虚拟表查看自己感兴趣的数据，而数据的物理存放位置依然在基表。创建视图后，要保证视图发布的安全[6,7]，可针对视图对不同的用户授予不同的访问权限，而不必给作为视图表基础的基表授予权限。利用视图，可以限制用户只看到表中的某些行和指定的列，它通过限制访问表的特定行和特定列来保证数据的安全，实现行级或列级的安全性。如图 4 所示。

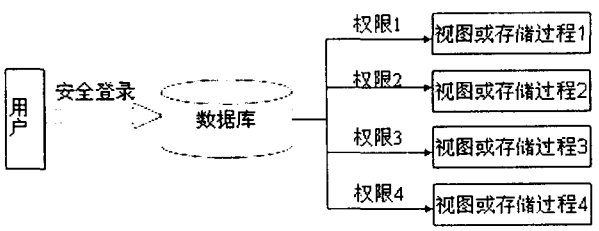

图 4 视图与存储过程的安全性

(3)存储过程。

存储过程是一组完成特定功能的 SQL 语句集，经编译后存储在数据库中，用户通过指定存储过程的名字并给出参数来执行它。

它的安全性主要体现在以下几个方面：

一是通过向用户授予对存储过程而不是基础表的访问权限来提供对特定数据的访问；

二是可以防止某些类型的 SQL 插入攻击，如使用运算符(如 AND 或 OR)将命令附加到有效输入参数值的攻击，从而解决代码安全问题；

三是当应用程序受到攻击时，它可以隐藏业务规则的实现等等，如图 4 所示。

3 结束语

从网络系统层次、OS 层次、DBMS 层次、应用程序层次分别阐述了网络数据库安全体系的构建方法，在实际实用中，需灵活处理。如在安全性要求不很高时，防火墙可选用代理服务型；数据库审计功能可选择关闭；数据库加密方法宜采用属性加密等。而对于安全性要求非常严格的网络数据库，除高要求选用文中所用方法外，还需加强系统管理员的管理，可将它们分为数据库管理员、数据库安全管理员、数据库审计员三类，做到三权分立、各司其职、相互制约，同时为了尽量消除推理通道(即用户根据低密级的数据和模式的完整性约束推导出高密级的数据)，应加强推理控制研究[8]。

参考文献：

[1] 郝文江.基于防火墙技术的网络安全防护[J].通信技术，2007,40(7):24-26.

[2] 林 庆,王 飞,吴 旻,等.基于专家系统的入侵检测系统的实现[J].微计算机信息,2007,23(3):61-63.

[3] 李 斓,冯登国,徐 震.多级安全 OS 与 DBMS 模型的信息流及其一致性分析[J].计算机学报,2005,28(7):1123-1129.

[4] Ferraiolo D, Sandhu R, Gavrila S, et al. A proposed standard for role based access control[J]. ACM Transactions on Information and System Security, 2001,4(3):224-274.

[5] 竹 勇,叶水生.Oracle9i 数据库的安全管理机制[J].计算机技术与发展,2006,16(6):142-144.

[6] Sweeney L. A model for protecting privacy[J]. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems,2002,10(5):557-570.

[7] Ahalevy. Answering queries using views: A survey[J]. VLDB Journal,2001,10(4):270-294.

[8] 严和平,汪 卫,施伯乐.安全数据库的推理控制[J].软件学报,2006,17(4):108-116.

(上接第 174 页)

[2] 刘永杰,李 芳,周玉洁.一种安全的三方公平电子合同方案[J].计算机应用研究，2007,24(1):170-173.

[3] 徐 明,张祥德.电子支付研究综述[J].计算机技术与发展,2007,17(9):213-216.

[4] Micali S. Simple and Fast Optimistic Protocols for Fair Electronic Exchange[C]//Proc. of Symposium on Principles of Distributed Computing. Boston:[s.n.],2003:12-19.

[5] Bao Feng, Wang Guilin, Zhou Jianying, et al. Analysis and Improvement of Micali's Fair Contract Signing Protocol[C]// Proc. of ICANN'04. Sydney:[s.n.],2004:176-187.

[6] 王芷玲,张玉清,杨 波.公平交换协议设计原[J].中国科学院研究生院学报,2006,23(4):555-560.

[7] 莫 燕,张玉清,李学干.关于安全协议设计原则的研究[J].计算机工程,2005,31(24):183-185.

[8] Pagnia H, Gartner C. On the Impossibility of Fair Exchange Without a Trusted Third Party[R]. Darmstadt: Darmstadt University of Technology,1999.

[9] Goldwasser S, Micali, S, Rivest R. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attack[J]. SIAM Journal of Computing,1988,17(2):281-308.