一种交换协议的理性模型及其公平机制设计*

牛翠翠[1a,1b,2]，彭长根[1b,1c,2†]，李 新[1a,1b,2]

(1. 贵州大学 a. 理学院；b. 密码学与数据安全研究所，c. 计算机科学与技术学院；贵阳 550025；2. 贵州省公共大数据重点实验室，贵阳 550025)

摘 要：理性交换协议是解决小额支付的有效方法，但是由于参与者的自利性，理性交换协议的公平性较难满足。对理性交换过程中的集体利益进行形式化定义，并基于占优策略构建理性参与者模型，以及基于占优策略和集体利益建立理性交换协议的公平性模型，基于激励相容理论设计理性交换协议的公平机制，基于理性交换协议的公平机制和扩展式博弈构建理性交换协议的理性博弈模型，并基于理性交换协议的博弈模型设计了一个理性交换协议。基于相关博弈方法证明所设计的协议满足正确性和理性公平性，并用一个案例说明方案的可行性。

关键词：博弈论；理性交换协议；激励相容；机制设计；理性公平性

中图分类号：TP393.09 **文献标志码**：A **文章编号**：1001-3695(2017)05-1504-05

doi:10.3969/j.issn.1001-3695.2017.05.052

Rational model of exchange protocol and its mechanism design on fairness

Niu Cuicui[1a,1b,2], Peng Changgen[1b,1c,2†], Li Xin[1a,1b,2]

(1. *a. College of Science, b. Institute of Cryptography & Data Security, c. College of Computer Science & Information, Guiyang* 550025, *China*; 2. *Guizhou Provincial Key Laboratory of Public Big Data, Guiyang* 550025, *China*)

Abstract: Rational exchange protocol is the efficient method to solve the micropayments, however, rational exchange protocol is difficult to satisfy the fairness because of the self-interest of the participants. First, the paper formally defined the collective interests during the rational exchange and constructed the rational participants model based on the dominant strategy, and established a rational exchange protocol fairness model on the basis of collective interests and dominant strategy. Then, the paper designed a rational exchange protocol fairness mechanism based on the theory of incentive compatibility, and constructed a rational exchange protocol's rational game model based on the rational exchange protocol fairness mechanism and extensive form game, and designed a rational exchange protocol on the basis of exchange protocol fairness mechanism and extensive form game. Finally, the paper proves that the protocol satisfies the correctness and rational fairness based on the related game method and demonstrates the feasibility with a case.

Key words: game theory; rational exchange protocol; incentive compatibility; mechanism design; rational fairness

0 引言

在电子商务的快速发展之下，对电子商务协议的研究也逐渐成为热点。交换协议是电子商务协议的重要组成部分，尤其是公平交换协议。公平交换协议通过在协议的执行过程中加入可信第三方来实现公平性。2011 年，Shi 等人[1]提出了一种由几种技术结合的新的公平交换协议，实现了在电子商务的公平交换。同年，Liu 等人[2]提出一种改进的乐观公平交换协议，在该协议中，参与者除了可信第三方，不需要相信其他任何人，以保证协议的公平性。2012 年，Huang 等人[3]提出一种新的基于原始密码的乐观公平交换，并且其安全性是不依赖于随机预言模型的。同年，Zhao 等人[4]提出一种基于可公开验证秘密共享的分布式公平交换，通过设计一个分布式第三方来保证协议的公平性，不同于传统的第三方，该第三方是动态的。2013 年，Htun 等人[5]提出一种公平性不依赖于发起者的可更改参与者的多方公平交换协议。同年，Camacho[6]提出一种基于新的零知识交互式证明而不依赖可信第三方的公平交换协议。2014 年，Jayasinghe 等人[7]通过减少可信第三方的使用，在电子商务中通过匿名的方法保证交换的强公平性。同年，Djuric 等人[8]提出了公平交换网上支付协议(FEIPS)。该 FEIPS 协议通过使用可信第三方来保证支付实物和落入实物的公平交换。Ganjavi 等人[9]通过使用可追踪环签名(TRS)，实现了协议的问责性。针对乐观公平交换协议中验证者可以将签名者的签名向别人展示，而使签名者处于不利地位的问题，2015 年，Huang 等人[10]提出了模糊乐观公平的概念，使验证者不能让签名者生成部分签名，并证明模糊乐观公平交换的通用结构，基于强 Diffie-Hellman 假设与决策线性假设在无随机预言模型是可证明安全的。同年，Rajasree 等人[11]通过比较部分收到的签名进行验证，并降低可信第三方的参与以确保交易的安全。

对于小额支付而言，为保证公平性而加入可信第三方的代价要比小额支付本身的代价高得多，为解决交换协议中可信第

收稿日期：2016-03-22；**修回日期**：2016-06-02 **基金项目**：国家自然科学基金资助项目(61262073,61363068)；贵州省普通高等学校创新人才团队项目(黔教合人才团队字 2013-09)；全国统计科研重点项目(2013LZ46)；贵州省统计科学研究课题项目(201511)

作者简介：牛翠翠(1991-)，女，山西吕梁人，硕士研究生，主要研究方向为可信计算与信息安全；彭长根(1963-)，男(侗族)(通信作者)，贵州锦屏人，教授，博导，博士，主要研究方向为密码学与信息安全(peng_stud@163.com)；李新(1991-)，男，安徽蚌埠人，硕士研究生，主要研究方向为可信计算与信息安全.

三方产生的瓶颈,不需要可信第三方的理性交换协议的研究逐渐受到国内外学者的关注。1998 年,Asokan[12] 提出将博弈论应用于公平交换协议设计中,并给出了一个两方的数字签名协议。同年,Syverson[13] 提出了理性交换协议,在 Syverson 的理性交换协议中,为了使参与者不得不遵守协议,引入惩罚机制,当有参与者不遵守协议时,就会对该参与者进行惩罚,而且这个惩罚值远远大于他违背协议后的收益值,以此约束参与者使其不得不遵守协议,而后继续在文献[14 ~ 16]中基于博弈论对 Syverson 理性交换进行研究。Alcaide 等人[17] 提出了多方理性交换协议,设计了一个三方的理性交换协议,并结合密码技术和启发式搜索技术,实现了三方理性交换协议的自动生成。Buttýan[18] 基于逐比特交换设计了一个理性支付协议,该协议虽然不满足公平性,但是参与者却没有偏离协议执行的动机。2014 年,吕桢等人[19] 在完全不完美动态博弈中,基于信息熵原理解决理性交换协议中理性参与者的行为推断问题。2015 年,Campos 等人[20] 在完全不完美信息的非合作博弈中提出多方理性信息交换中的均衡情况,主要构建了一个广义纳什均衡模型,分析了在保证信息的公平、点对点以及隐私的保护同时发生时的均衡情况。

但是由于理性参与者的自利性,使理性交换协议难以满足公平性。所以本文基于机制设计,旨在设计一种公平机制,以此设计理性交换协议,并用博弈方法分析其满足公平性。机制设计通过构造具有一定规则的博弈,使得该博弈的均衡解是社会目标,主要包含个人理性和激励相容两个方面的内容。激励相容是指在给定机制的约束下,真实汇报自己的类型是参与者的占优策略均衡。本文基于激励相容机制设计理性交换协议的公平机制,通过定义交换协议过程中的集体利益和理性交换协议公平机制中的支付函数约束理性参与者的行为。在该机制的基础上设计一个两方的理性交换协议,且该协议满足正确性,用博弈论对该协议的公平性进行分析,证明该协议满足理性公平性,解决了理性交换协议公平性难以满足的问题。

1　基础知识

在这里将介绍机制设计[21] 和博弈论[22] 中的一些相关概念等基础知识。

1.1　机制设计

标准的机制是一个二元组 $M=(f,\Theta)$。其中:

a) 社会选择函数 $f:(\Theta_1\times\Theta_2\times\cdots\times\Theta_n)\to O$,$O$ 表示所有参与者 P 在不同策略下的所有可能结果,P 为参与者集合;

b) $\Theta:\Theta=(\Theta_1\times\Theta_2\times\cdots\times\Theta_n)$ 表示各个参与者类型的集合,其中,$\theta_i\in\Theta_i$ 表示参与者的私人类型;理性参与者 $i(i\in P)$ 在机制 M 的约束下选择策略 s 的效用函数为

$$u_i(s)=v_i(o(s),\theta_i)-p_i(s)$$

其中,$v_i(o(s),\theta_i)$ 表示参与者 $i(i\in P)$ 在类型为 θ_i 时选择策略 s 时对结果 o 的估值;$p_i(s)$ 表示参与者 $i(i\in P)$ 在选择策略 s 时的支出。

1.2　扩展式博弈

1) 扩展式博弈

以动态博弈理论为基础,扩展式博弈是一个七元组 $\langle P,Q,(I_i)_{i\in P},c,D,U_i(q),r\rangle$,其中:

P:参与者集合 $P=\{1,2,\cdots,n\}$;

Q:参与者的行动序列集,满足下列性质:

a) 空序列 $\varnothing\in Q$;

b) 如果 $q=(d_k)_{k=1}^{\omega}\in Q$,并且 $0<\nu<\omega$(ν 和 ω 是自然数),那么 $q'=(d_k)_{k=1}^{\nu}\in Q$;

c) 如果对任意正整数 ν,对于无穷序列 $(d_k)_{k=1}^{\infty}$,满足 $(d_k)_{k=1}^{\nu}\in Q$,那么 $(d_k)_{k=1}^{\infty}\in Q$。

对于任意的行动 d,$q.d$ 表示行动序列 q 后的行动为 d,如果行动序列 $q\in Q$ 是无限的或者它的后续行动是 $\varnothing$,则称其为终端,本文一般用 Z 来表示其终端行动序列组成的集合。

$(I_i)_{i\in P}$:参与者 $i\in P$ 的信息集,它表示参与者在获得一些信息之后进行行动的选择。

D:可选行动集合,它表示各个参与者的可选行动集的并集。

c:参与者函数,$\{O\backslash Z\}\to P$,它表示非终端行动序列到参与者的一个映射。

$U_i(q)$:效用函数,$Z\to R$,它表示参与者 $i\in P$ 在终端行动序列 $q\in Z$ 通过计算给定的一个实数值。其中,$u_i(q)$ 的定义同上述(*)式定义。

r:轮计数器值。

2) 策略

用函数 s_i 表示参与者 $i(i\in P)$ 的策略,其中,$s_i:Q\backslash Z\to D_i(q)$,它表示参与者 $i\in P$ 在非终端行动序列根据其信息集从其可选行动集中选择行动。$S_i=\{s_i\}$ 是参与者 $i(i\in P)$ 的策略集,策略组合 $(s_j,(s_i)_{i\in P\backslash\{j\}})$ 表示每个参与者从策略集 S_i 选择其中一个策略 s_i 所组成的向量组。

3) 占优策略均衡

s_i^* 称做参与人 $i(i\in P)$ 的占优策略,如果对应所有的 s'_i、s_i^* 是 $i(i\in P)$ 的严格最优选择,即 $u_i(s_i^*,s_{-i})>u_i(s'_i,s_{-i})$,$\forall s_{-i},s'_i\neq s_i^*$;如果对于所有的参与者 $j(j\in P)$,s_j^* 是 $j(j\in P)$ 的占优策略,那么策略组合 $S^*=(s_1^*,s_2^*,\cdots,s_n^*)$ 称为占优策略均衡。s_{-i} 表示除去参与者 $i(i\in P)$ 的其他参与者策略的集合。

2　公平交换协议的理性模型

本章首先对集体利益作形式化定义,然后构建理性参与者和理性公平性模型,基于激励相容原理设计两方理性交换协议的公平机制,再将两方理性交换协议的公平机制与扩展式博弈结合构建两方理性公平交换协议模型。

2.1　相关定义

为了对理性交换协议进行分析,主要考虑构建两方理性交换协议模型。首先对理性交换过程中的集体利益作形式化定义,然后分别对理性参与者和理性公平性建模。

定义 1　集体利益是指在理性交换结束后各个参与者的效用函数的总和,即 $U=\sum_{i=1}^{n}u_i$。

定义 2　激励相容是指在一种机制 M 的约束下,使理性参与者在追寻个人利益最大化的同时实现集体利益最大化。即当参与者 $i(i\in P)$ 的个人收益 u_i 最大时,集体利益 U 也实现最大。

定理 1　在理性交换协议中,由于参与者 $i(i\in P)$ 都是理性的,在执行协议的过程当中,会最大化自己的收益。即当 $u_i(s_i^*)>u_i(s'_i)$,则参与者 $i(i\in P)$ 选择执行策略 s_i^*。

定理 2　若策略组合 $S^*=(s_1^*,s_2^*,\cdots,s_n^*)$ 是一个占优策略均衡,理性交换协议满足公平性当且仅当协议执行结束后个

人利益和集体利益同时实现最大,即对于任意的理性参与者 i $(i\in P)$,有 $u_i(s_i^*,s_{-i})>u_i(s'_i,s_{-i})$,$\forall s_{-i},s'_i\neq s_i^*$ 和 $U'\leqslant U^*$ 成立。

2.2 两方理性公平交换协议的公平机制

理性交换协议公平机制 $M_{RE}=(S_i,p)$ 是一个二元组。其中:

a)S_i 表示参与者 $i(i\in P)$ 的策略集合。

b)$p=(p_1,p_2,\cdots,p_n)$ 是理性交换协议公平机制根据理性参与者在协议执行过程中所选策略的支付函数。其中,p_i 表示理性参与者 $i(i\in P)$ 在协议结束后的总共支出,且满足

$$p_i=\begin{cases}p'_i+fv_i(o(s_i),\theta_d), s_i\in S_i, S_i\cap \mathrm{send}(m_i^*)\neq\varnothing & f>1\\ p'_i-M_r, S_i\cap \mathrm{send}(m_i^*)=\varnothing & M_r>0\end{cases}$$

其中:p'_i 表示理性参与者 $i(i\in P)$ 在协议结束后的应该支出。简单地说,理性交换协议公平机制 M_{RE} 是指当理性参与者 $i(i\in P)$ 遵守协议执行时,理性参与者在原有收益的基础上会增加 M_r(M_r 的值会非常小),并且随着其交换次数的增多(增加到一定数量后便不再增加),其额外收益也会增加;反之,若理性参与者 $i(i\in P)$ 偏离协议的执行,则理性参与者 $i(i\in P)$ 将会对理性交换协议公平机制 M_{RE} 进行支付,支付金额为其收益的 $f(f>1)$ 倍。

定理 3 理性交换协议公平机制 M_{RE} 是激励相容机制。

证明 先假设参与者 $i(i\in P)$ 的类型为两种,诚实的和不诚实的,即 θ_h 和 θ_d,s 表示参与者偏离协议执行时的策略,s' 表示参与者遵守协议执行时的策略;所以当参与者 $i(i\in P)$ 偏离协议执行时,理性参与者的效用函数为

$$u_i(s)=v_i(o(s),\theta_d)-p'_i-fv_i(o(s),\theta_d)$$

当参与者 $i(i\in P)$ 遵守协议执行时,理性参与者的效用函数为

$$u_i(s')=v_i(o(s'),\theta_h)-p'_i+M_r$$

因为 $f>1$,所以 $u_i(s)<0$,所以 $u_i(s)<u_i(s')$。又由于参与者 $i(i\in P)$ 是理性的,会选择最大化自己的收益,所以在机制 M_{RE} 下,理性参与者 $i(i\in P)$ 会选择遵守协议执行,即真实地汇报自己的类型。所以理性交换协议公平机制 M_{RE} 是激励相容机制。

2.3 两方理性公平交换协议的形式化模型

根据理性交换协议的公平机制和扩展式博弈,构建两方理性公平交换协议的模型为七元组$\langle P,Q,(I_i)_{i\in P},c,D,U_i(q),r\rangle$

a)理性交换协议的参与者集合 $P=\{A,B\}$;

b)理性交换协议的行动序列集合:

$$\begin{aligned}Q=\{&\varnothing,\mathrm{quit}_A,\mathrm{send}_A(m_1^*).\mathrm{quit}_B,\mathrm{send}_A(m_1^*).\\&\mathrm{send}_B(m_2).\mathrm{send}_A(m_3),\mathrm{send}_A(m_1^*).\mathrm{send}_B(m_2).\\&\mathrm{send}_A(m_3^*),\mathrm{send}_A(m_1).\mathrm{quit}_B,\mathrm{send}_A(m_1).\mathrm{send}_B(m_2).\\&\mathrm{quit}_A,\mathrm{send}_A(m_1).\mathrm{send}_B(m_2).\mathrm{send}_A(m_3^*),\mathrm{send}_A(m_1).\\&\mathrm{send}_B(m_2).\mathrm{send}_A(m_3),\mathrm{send}_A(m_1).\mathrm{send}_B(m_2).\mathrm{send}_A(m_3^*)\}\end{aligned}$$

其中,$\varnothing$ 表示参与者双方不执行任何行动;quit_i 表示参与者 $i(i\in P)$ 不执行任何行动,$\mathrm{send}_i(m)$ 表示参与者 $i(i\in P)$ 执行发送消息 m,$m_i(i=1,2,3)$ 表示第 i 轮的正确消息;m_i^* $(i=1,2,3)$ 表示第 i 轮的垃圾消息。

c)参与者的信息集,其中,

参与者 A 的信息集合为

$$I_A=\{\varnothing,\mathrm{send}_A(m_1^*).\mathrm{send}_B(m_2),\mathrm{send}_A(m_1).\mathrm{send}_B(m_2)\}$$

参与者 B 的信息集合为

$$I_B=\{\mathrm{send}_A(m_1^*),\mathrm{send}_A(m_1)\}$$

d)可选行动集合,其中,

参与者 A 的可选行动集合为

$$D_A=\{\mathrm{send}(m_1^*),\mathrm{send}(m_1),\mathrm{send}(m_3),\mathrm{send}(m_3^*),\mathrm{quit}_A\}$$

参与者 B 的可选行动集合为

$$D_B=\{\mathrm{send}(m_2),\mathrm{quit}_B\}$$

e)参与者函数 c

$$c(\varnothing)=c(\mathrm{send}_A(m_1^*).\mathrm{send}(m_2))=c(\mathrm{send}_A(m_1).\mathrm{send}(m_2))=A$$

$$c(\mathrm{send}_A(m_1^*))=c(\mathrm{send}_A(m_1))=B$$

f)如图 1 所示,参与者 A 关于终端序列的效用为

$$M_1>0^+>0>-v+M_1>(1-f)v>-fv$$

如图 1 所示,参与者 B 关于终端序列的效用为

$$M_1>0>-v+M_1$$

2.4 两方理性公平交换协议的博弈树模型

根据上述理性交换协议模型的建立,整个协议的动态博弈过程可以表示为一棵博弈树,如图 1 所示。

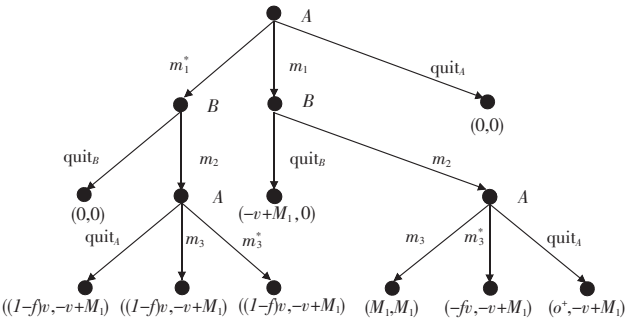

图 1 三轮扩展式博弈树

协议从理性参与者 A 开始,在第一轮,参与者 A 的可选行动集合为 $\{\mathrm{send}_A(m_1),\mathrm{send}_A(m_1^*),\mathrm{quit}_A\}$,参与者 A 执行行动完毕,第一轮结束。第二轮从参与者 B 开始,此时,参与者 B 的可选行动集合为 $\{\mathrm{send}_B(m_2),\mathrm{quit}_B\}$,若在第一轮参与者 A 选择执行行动 quit_A,双方博弈结束,参与者 B 不做任何行动,参与者 A 选择执行行动 $\mathrm{send}_A(m_1)$ 或 $\mathrm{send}_A(m_1^*)$,参与者 B 不能判断参与者 A 在第一轮的行动;若参与者 A 选择执行行动 $\mathrm{send}_A(m_1^*)$,B 选择行动 quit_B,则双方收益均为 0;若参与者 A 选择执行行动 $\mathrm{send}_A(m_1)$,B 选择行动 quit_B,参与者 A 和 B 的最终收益分别为 $-v+M_1$ 和 0,若 B 选择行动 $\mathrm{send}_B(m_2)$,则第二轮结束。第三轮由参与者 A 开始,此时,参与者 A 的可选行动集为 $\{\mathrm{send}_A(m_3),\mathrm{send}_A(m_3^*),\mathrm{quit}_A\}$,若参与者 A 在第一轮选择执行行动 $\mathrm{send}_A(m_1^*)$,则根据理性交换协议的公平机制 M_{RE},其最终收益均为 $(1-f)v$,参与者 B 的最终收益为 $-v+M_1$,参与者 A 在第一轮执行行动 $\mathrm{send}_A(m_1)$,在第三轮选择执行行动 $\mathrm{send}_A(m_3^*)$ 或 quit_A,则其最终收益为 $-fv$ 和 0^+,0^+ 表示参与者的支出与收益等价,0 表示参与者无支出也无收益,若参与者 A 选择执行行动 $\mathrm{send}_A(m_3)$,则第三轮结束,参与者 A 和 B 的最终收益均为 M_1。即整个博弈也结束。

3 一种两方理性公平交换协议

本章首先基于理性交换协议的公平机制,设计了一个两方的理性交换协议。然后对协议的正确性和公平性进行分析。最后通过一个实例说明所设计的协议是满足正确性和公平性

的。

3.1　协议描述

在理性交换协议中,理性参与者在交换物品时有先后顺序,显然,先发送物品的理性参与者较后发送物品的理性参与者具有一定的劣势。故本文为消除这种先发送物品参与者的劣势,基于激励相容原理设计两方理性交换协议的公平机制有效的约束理性参与者的自利性行为,并基于该机制和两方理性公平交换协议模型设计一个两方的理性交换协议,使其满足公平性。

由于传统的公平交换协议是通过可信第三方实现的,使得公平交换协议的执行效率较低,而且考虑小额支付中参与者的收益远远小于对可信第三方的支付。为了解决这一问题,理性交换受到越来越多的关注,本文基于两方理性交换协议的公平机制设计了一个两方理性交换协议,所设计的理性交换协议如下:

$$A\rightarrow B:M_{RE}(m_1)=(B,\mathrm{desc}_{\mathrm{item}_A},\mathrm{enc}(k,\mathrm{item}_A),\sigma_1)$$
$$\sigma_1=\mathrm{sig}(K_A^{-1},(B,\mathrm{desc}_{\mathrm{item}_A},\mathrm{enc}(k,\mathrm{item}_A)))$$
$$B\rightarrow A:M_{RE}(m_2)=(A,\mathrm{item}_B,m_1,\sigma_2)$$
$$\sigma_2=\mathrm{sig}(K_B^{-1},(A,\mathrm{item}_B,m_1))$$
$$A\rightarrow B:M_{RE}(m_3)=(B,k,m_2,\sigma_3)$$
$$\sigma_3=\mathrm{sig}(K_A^{-1},(B,k,m_2))$$

A 和 B 为两个协议的理性参与者,分别拥有各自的私钥 K_A^{-1} 和 K_B^{-1}。协议假设在协议开始之前,A 和 B 已对交换过程达到共识,且 item_A 和 item_B 为参与者 A 和 B 交换的东西,特别地,参与者 A 和 B 同意 item_A 和 item_B 是等价的。$\mathrm{desc}_{\mathrm{item}_A}$是对 item_A 的一个描述(由于该协议是一个支付协议,item_B 对 item_A 的一个支付,故不需要对 item_B 进行描述)。更进一步,$\mathrm{sig}(K_i^{-1},m)$是指用私钥 K_i^{-1} 对消息 m 进行签名,$\mathrm{enc}(k,m)$是指用密钥 k 对消息 m 进行加密。$M_{RE}(m_i)$ 指消息 m_i 是在机制 M_{RE} 下发送的。

下面基于前文的两方理性公平交换协议模型和两方理性公平交换协议的博弈树模型,给出方案的正确性和公平性分析。

3.2　协议的正确性分析

定理 4　基于 M_{RE} 机制,理性交换协议是正确的。

证明　根据协议的协定,在理性交换协议执行的过程当中,首先理性参与者 A 向理性参与者 B 发送消息 m_1,在消息 m_1 中包含对物品 item_A 的一个描述和用密钥 k 对物品 item_A 的加密,并有理性参与者 A 用私钥 K_A^{-1} 对其进行签名,因此当参与者 B 收到消息 m_1 时,可以确认消息 m_1 为参与者 A 发送。然后,参与者 B 将消息 m_2 发送给参与者 A,消息 m_2 中包含消息 m_1 和物品 item_B 以及用私钥 K_B^{-1} 对消息 m_2 的签名,前两轮执行完毕后,参与者 A 收到消息 m_2 时,A 可以确认消息 m_2 为参与者 B 发送,并且 B 已经收到消息 m_1。在前两轮执行完之后,参与者 A 和 B 已经实现了相互认证。接下来进入第三轮,参与者 A 向 B 发送消息 m_3,消息 m_3 中包含消息 m_2、密钥 k 以及用 K_A^{-1} 对消息 m_3 的签名。参与者 B 获得密钥 k 之后,对密文 $\mathrm{enc}(k,\mathrm{item}_A)$解密,获得物品 item_A。即在协议结束后理性参与者 A 和 B 均能获得自己想要的物品 item_A 和 item_B。

在协议的执行过程中,由于参与者是理性的,参与者 A 可能会选择行动 $\mathrm{send}_A(m_1^*)$ 和 $\mathrm{send}_B(m_3^*)$ 以获得更大的收益。但是在理性交换协议的公平机制 M_{RE} 下,参与者若偏离协议执行,则会获得自己收益的 f 倍惩罚,若参与者遵守协议执行时,则会在自己收益的基础上获得 M_r 的收益,并且该额外收益会因交易次数的增加而增加。因此,在 M_{RE} 机制下,由于参与者是理性的,会最大化自己的收益,所以会选择遵守协议来执行。所以该理性交换协议在 M_{RE} 机制下,是满足正确性的。

3.3　协议的理性公平性分析

对理性参与者 A 来说,其收益值的大小关系为 $M_1>0^+>0>-v+M_1>(1-f)v>-fv$,对理性参与者 B 来说,其收益值的大小关系为 $M_1>0>-v+M_1$。应用逆推归纳法先分析第三轮参与者 A 的选择,因为有 $M_1>0^+>0>-v+M_1>(1-f)v>-fv$,所以一旦博弈进行到该阶段,结果必然是参与者 A 选择发送消息 m_3,双方得益为(M_1,M_1),此时上述的三阶段博弈就与图 2 中的两轮博弈是完全等价的。然后分析图 2 中第二轮参与者 B 的选择,因为有 $M_1>0>-v+M_1$,所以一旦博弈进行到该阶段,结果必然是参与者 B 选择发送消息 m_2。以此类推,可知道$(\mathrm{send}_A(m_1).\mathrm{send}_A(m_3),\mathrm{send}_B(m_2))$是纳什均衡,且$(\mathrm{send}_A(m_1).\mathrm{send}_A(m_3),\mathrm{send}_B(m_2))$为最优策略,所以$(\mathrm{send}_A(m_1).\mathrm{send}_A(m_3),\mathrm{send}_B(m_2))$为占优策略均衡。又因为此时的集体利益为 $U=M_1+M_2$,该集体利益在该博弈的过程当中,显然是最大的。

所以该协议在理性交换协议公平机制 M_{RE} 下是满足理性公平性的。

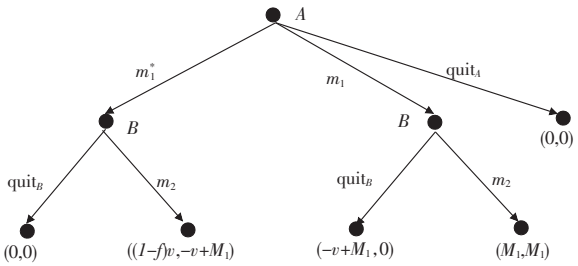

图 2　与图 1 等价的两轮扩展式博弈树

3.4　实例分析

现有消费者 B 想向服务提供商 A 购买价值为 $p'=28$ 元的商品 SERVICE,在交易顺利的情况下,服务提供商 A 会获得 28 元现金,消费者 B 会获得价值为 28 元的商品。现服务提供商对商品进行促销,并规定若消费者成功购买商品,并推荐其他的消费者购买成功或该消费者多次购买,则该消费者就会享有一定的优惠,且服务提供商承诺自己的商品假一赔十。具体情况如表 1 所示。

消费者 B 向服务提供商 A 购买商品,首先服务提供商 A 向消费者 B 发送商品信息,消费者 B 选定商品之后,生成订单信息,并向服务提供商 A 发送支付信息,服务提供商 A 经过验证之后发送商品。具体交易过程如下:

a)服务提供商 A 用自己的私钥对商品 SERVICE 的描述和对商品 SERVICE 用密钥 k 加密后进行签名,并发送给消费者 B。

b)消费者 B 收到服务提供商 A 的签名后,对商品 SERVICE 进行支付,并将支付信息用自己的私钥签名后发送给服务提供商 A。

c)服务提供商 A 收到消费者 B 的支付订单后,将商品 SERVICE 的解密密钥发送给消费者 A。

表 1 服务提供商和消费者的收益情况

件数(买/卖)	折扣	A 的总收益(u_A)	B 的平均支出(p_B)
1	100%	28	28
2	99%	55.44	27.72
3	98%	83.32	27.44
4	97%	108.64	27.16
5	96%	134.4	26.88
6	95%	159.6	26.6
7	95%	186.2	26.6

在交易过程当中,服务提供商 A 向消费者 B 的承诺,以及服务提供商的承诺假一赔十的约束就相当于是一个激励相容机制 M_{RE}。可以看到,在该过程中,$M_{RE}=\{S_i,p\}$(其中 $i=\{A,B\}$),A 的策略有 $S_A=\{s_1,s_2\}$(其中 s_1 表示 A 向 B 发送假冒伪劣产品,s_2 表示 A 向 B 发送正品),若 A 选择策略 s_1,但由于在承诺(机制 M_{RE})的约束下,A 将受到其收益 10 倍的惩罚,即 $f=10$,此时,A 的支付函数为 $p_A=28+10\times28=308$(元),则其效用函数显然为负,因此在该机制的约束下,A 只会向 B 发送正品,即选择策略 s_2。B 的策略有 $S_B=\{s_3,s_4\}$(其中 s_3 表示 B 向 A 购买产品,s_4 表示 B 不向 A 购买产品)。若 A 选择策略 s_2,则 B 显然选择 s_3 对 B 是最有利的。此时,在机制 M_{RE} 的约束下,B 会享有优惠,如表 1 所示,即 B 的支付函数 p_B 在减少,而 A 的收益 u_A 在增加。即在诚实地进行交易时,在承诺(机制 M_{RE})的约束下,A 和 B 都会有额外收益 M_r,而服务提供商 A 和消费者 B 都是理性的,会最大化自己的收益。因此,最终 A 和 B 都会诚实地进行交易,即该交易是满足公平性和有效性的。

4 结束语

本文基于激励相容机制构建了一个理性交换协议公平机制 M_{RE},并在该机制下设计了一个两方的理性交换协议。文章基于 M_{RE} 机制对理性参与者通过惩罚和奖励两种方法约束理性参与者正确地执行协议,而奖励值会随着交易次数的增加而增大。长时间正确执行协议,会提升参与者的信誉,因此理性参与者在执行协议时无论从眼前利益还是长远利益考虑都不会选择偏离协议。本文对理性交换协议的公平性建模时同时考虑了个人利益和集体利益,使该模型更符合实际情况。最后基于博弈论中的逆向归纳法证明所设计的协议是满足公平性的,并通过在协议中加入参与者的身份来保证协议的安全性。然而通过奖励制度约束理性参与者的行为,也适用于参与者的长远利益。在所设计机制下,通过一个实例表明正确性和有效性,并且满足公平性。因此,在下一步的研究中,将通过构建合理的机制设计一个多方的理性交换协议,将奖励制度与信誉机制结合,同时考虑理性参与者的眼前利益和长远利益构建理性交换协议的公平性模型。

参考文献:

[1] Shi Q, Zhang N, Merabti M. Achieving autonomous fair exchange in ubiquitous network settings[J]. Journal of Network and Computer Applications, 2011, 34(2): 653-667.

[2] Liu Yi, Hu Hongli. An improved protocol for optimistic multi-party fair exchange[C]//Proc of International Conference on Electronic and Mechanical Engineering and Information Technology. 2011: 4864-4867.

[3] Huang Qiong, Yang Guomin, Wong D S. *et al*. A new efficient optimistic fair exchange protocol without random oracles[J]. International Journal of Information Security, 2012, 11(1): 53-63.

[4] Zhao Yang, Qin Zhiguang. An optimistic protocol for distributed fair exchange[C]//Proc of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. 2012: 395-399.

[5] Htun N C, Kyaw K K K. Analysis and improvement on a single unit cyclic fair exchange protocol for multi-party[J]. International Journal of Advanced Research in Computer Engineering & Technology, 2013, 2(5): 1901-1903.

[6] Camacho P. Fair exchange of short signatures without trusted third party[C]//Proc of the 13th International Conference on Topics in Cryptology. Berlin: Springer-Verlag, 2013: 34-49.

[7] Jayasinghe D, Markantonakis K, Mayes K. Optimistic fair-exchange with anonymity for bitcoin users[C]//Proc of the 11th IEEE International Conference on e-Business Engineering. 2014: 44-51.

[8] Djuric Z, Gasevic D. FEIPS: a secure fair-exchange payment system for internet transactions[J]. The Computer Journal, 2015, 58(10): 2537-2556.

[9] Ganjavi R, Asaar M R, Salmasizadeh M. An ambiguous optimistic fair exchange protocol with traceability[C]//Proc of the 7th International Symposium on Telecommunications. 2014: 919-924.

[10] Huang Qiong, Yang Guomin, Wong D S, *et al*. Ambiguous optimistic fair exchange: definition and constructions[J]. Theoretical Computer Science, 2015, 562: 177-193.

[11] Rajasree R S, Pede S V. An abuse-free optimistic signature exchange protocol using block cipher[C]//Proc of International Conference on Computing Communication Control and Automation. 2015: 256-260.

[12] Asokan N. Fairness in electronic commerce[D]. Waterloo: University of Waterloo, 1998.

[13] Syverson P. Weakly secret bit commitment: applications to lotteries and fair exchange[C]//Proc of the 11th IEEE Computer Security Foundations Workshop. 1998: 2-13.

[14] Alcaide A, Estevez-Tapiador J M, Hernandez-Castro J C, *et al*. An extended model of rational exchange based on dynamic games of imperfect information[M]//Emerging Trends in Information and Communication Security. Berlin: Springer, 2006: 396-408.

[15] Estevez-Tapiador J M, Alcaide A, Hernandez-Castro J C, *et al*. Bayesian rational exchange[J]. International Journal of Information Security, 2008, 7(1): 85-100.

[16] Buttyán L, Hubaux J P, Capkun S. A formal model of rational exchange and its application to the analysis of Syverson's protocol[J]. Journal of Computer Security, 2004, 12(3/4): 551-587.

[17] Alcaide A, Estevez-Tapiador J M, Hernandez-Castro J C, *et al*. A multi-party rational exchange protocol[C]//On the Move to Meaningful Internet Systems 2007: OTM 2007 Workshops. Berlin: Springer, 2007: 42-43.

[18] Buttyán L. Removing the financial incentive to cheat in micropayment schemes[J]. Electronics Letters, 2000, 36(2): 132-133.

[19] 吕桢, 彭长根, 刘海, 等. 基于极大熵原理的理性公平交换协议[J]. 计算机应用研究, 2014, 31(2): 563-567.

[20] Campos F A, Pham V. Rational information exchange model: a new optimization approach for equilibrium computing[C]//Pro of the 6th International Conference on Modeling, Simulation, and Applied Optimization. 2015: 1-6.

[21] Mierendorff K. Optimal dynamic mechanism design with deadlines[J]. Journal of Economic Theory, 2016, 161: 190-222.

[22] Nisan N, Roughgarden T, Tardos E, *et al*. Algorithmic game theory[M]. Cambridge: Cambridge University Press, 2007.