

混合策略下的理性交换协议模型

丁洪^{1,2}, 彭长根^{1,2}, 邱青青^{1,2}

(1. 贵州大学理学院, 贵州 贵阳 550025;
2. 贵州大学密码学与数据安全研究所, 贵州 贵阳 550025)

摘要: 在小额支付的交换协议中, 通过 TTP 保证协议公平性所需代价往往高于协议本身价值, 在这种情况下, 理性交换协议是一种合适的选择。应用扩展式博弈混合策略理论对交换协议进行了建模, 引入熵函数对交换过程中的公平性进行了描述; 在保证过程公平性原则的前提下, 运用混合策略纳什均衡概念形式化定义了理性公平性, 并在此模型基础上构造了一个新的理性交换协议; 对协议的可追究性、理性公平性进行了证明, 结果表明该协议能达到混合策略纳什均衡。该协议无须可信第三方, 实现了理性公平性并对惩罚值进行了优化, 具有更好的适应性。

关键词: 理性交换协议; 混合策略; 过程公平; 纳什均衡

中文分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00016

Rational exchange protocol model based on mixed strategy

DING Hong^{1,2}, PENG Chang-gen^{1,2}, KUANG Qing-qing^{1,2}

(1. College of Science, Guizhou University, Guiyang 550025, China;
2. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China)

Abstract: In the exchange of micropayment protocol, the cost of ensuring fairness by TTP is higher than the value of protocol, in this case the rational exchange protocol is a appropriate choice. Exchange protocol was modeled by extensive mixed strategy game and the entropy function was introduced to discuss the fairness in the process of exchange. In addition, the rational fairness was formally defined by using the concept of mixed strategy Nash equilibrium under the principle of the fairness in the process, and on the basis of this model to construct a new rational exchange protocol. The protocol's accountability and rational fairness were proved, the results show that the proposed protocol can achieve mixed strategy Nash equilibrium. Without the participation of the trusted third party, the protocol can achieve rational fairness and optimize the penalty values, it is beautifully adapted to the real environment.

Key words: rational exchange protocol, mixed strategy, process fairness, Nash equilibrium

收稿日期: 2015-11-11; 修回日期: 2016-01-09. 通信作者: 彭长根, peng_stud@163.com

基金项目: 国家自然科学基金资助项目 (No.61262073); 全国统计科学研究计划基金资助项目 (No.2013LZ46); 贵州省统计科学研究课题基金资助项目 (No.201511)

Foundation Items: The National Natural Science Foundation of China(No.61262073), The National Statistical Scientific Research Project (No.2013LZ46), The Guizhou Provincial Statistical Science Research Project(No.201511)

1 引言

交换协议被广泛应用在电子合同签署、电子邮件认证和网络支付服务等领域，如何保证交换过程中各方参与者的公平性是交换协议的一个重要问题，目前，主要依赖于公平交换原则和理性交换原则来解决。传统的公平交换协议通常以可信第三方（TTP, trusted third party）或复杂的通信为代价来保证公平性的实现，可信第三方容易成为瓶颈。理性交换不需要可信第三方，在实现理性公平性的同时提高了效率，因此理性交换逐渐成为研究热点。在微支付协议中，保证强公平性的代价往往高于支付协议本身的价值，从而强公平性不再适用于这类协议，而理性交换能提供更合适的解决方法。

1998年，Asokan^[1]首次将博弈论应用到公平交换协议的分析设计中，同年 Syverson^[2]首次提出了理性交换的概念，即在交换过程中，参与者的不诚实行为可能会对其他参与者的利益造成损失，但是参与者不会因不诚实行为而获利。换言之，理性交换不能完全保证公平性，但理性参与者没有理由偏离协议。2001年，Buttayan等^[3]运用博弈论的方法给出了公平性的形式化定义，基于扩展式博弈对交换协议进行了建模并对 Syverson 协议进行了分析。针对 Syverson 协议中的不足，Alcaide等^[4-6]应用不完全信息动态博弈理论，在交换协议中引入信念，建立了贝叶斯博弈下的理性交换协议模型，使理性交换更加符合现实应用环境。在文献[7]中，作者基于极大熵原理设计了一个新的理性交换协议，并对协议的安全性和公平性进行了证明。上述研究成果都只对交换协议的结果公平性进行了讨论，并未涉及过程公平性的分析。而本文考虑用信息论中的熵理论^[8]对过程公平性进行描述，并探讨过程公平原则下的理性公平性。

本文应用扩展式博弈下的混合策略^[9]对理性交换协议进行建模，给出此模型下的混合策略纳什均衡定义；通过引入熵理论对过程公平性进行描述，给出过程公平性的定义；在过程公平性原则下，利用博弈树对整个交换过程进行分析并给出协议的可追究性^[10]、理性公平性

的证明。结果表明该协议能达到混合策略纳什均衡。协议交换过程无须可信第三方，该协议实现了理性公平性并对惩罚值进行了优化，具有更好的适应性。

2 理性交换协议的混合策略模型

博弈论是研究决策问题的理论。在博弈过程中，参与者会极力猜测对方如何选择，同时又不想让对方猜到自己的选择，在这样的情况下，参与者往往会随机选择自己的策略。混合策略解释了一个参与者对其他参与者所采取行动的不确定性，它描述了参与者在给定信息下以某种概率分布随机地选择不同的行动或策略。可以通过引用熵对这样的不确定性进行描述。

在小额支付协议中，选择可信第三方来保证公平性所需的代价往往高于支付协议本身。在这种情况下，理性交换协议是一种合适的选择。而协议参与者进行信息交互的过程可以看作一个混合策略扩展式博弈过程，因此可以利用混合策略扩展式博弈理论对其进行建模。

2.1 基础知识

1) 混合策略

在一个给定的有限 n 人策略式博弈 $G = \langle \Gamma; S_1, \dots, S_n; u_1, \dots, u_n \rangle$ 中，对任一参与者 i ，设 $S_i = \{s_i^1, \dots, s_i^K\}$ 为参与者 i 的策略集，则参与者 i 的一个混合策略为定义在 S_i 上的一个概率分布 $\sigma_i = (\sigma_i^1, \dots, \sigma_i^K)$ ，其中 $\sigma_i^j (j=1, \dots, K)$ 表示参与者 i 选择策略 s_i^j 的概率，即 σ_i^j 满足： $0 \leq \sigma_i^j \leq 1$ 且 $\sum_{j=1}^K \sigma_i^j = 1$ 。

2) 用 $\sum_i$ 表示参与者 i 的混合策略空间，其中 $\sigma_i \in \sum_i$

$\sigma = (\sigma_1, \dots, \sigma_n)$ 为混合策略组合，表示博弈中每个参与者 $i (i=1, 2, \dots, n)$ 采取混合策略中相应策略 σ_i 的一种博弈情形。给定策略组合 $\sigma = (\sigma_1, \dots, \sigma_n)$ ，用 $\sigma_{-i} = (\sigma_1, \dots, \sigma_{i-1}, \sigma_{i+1}, \dots, \sigma_n)$ 表示除参与者 i 以外的其他参与者的混合策略组合，因此， $\sigma = (\sigma_i, \sigma_{-i})$ 。

3) 期望效用

用 $v_i(\sigma) = v_i(\sigma_i, \sigma_{-i})$ 表示参与者 i 在混合策略组合 $\sigma = (\sigma_i, \sigma_{-i})$ 下的期望效用； $v_i(s_i, \sigma_{-i})$ 表示

参与者在其他参与者选择混合策略 σ_{-i} 的情况下, 选择纯策略 s_i 的期望收益。

4) 混合策略 Nash 均衡

定义 1 在一个给定的有限 n 人策略式博弈 $G = \langle \Gamma; S_1, \dots, S_n; u_1, \dots, u_n \rangle$ 中, 混合策略组合 $\sigma^* = (\sigma_1^*, \sigma_2^*, \dots, \sigma_n^*)$ 为一个 Nash 均衡, 当且仅当 $\forall i \in \Gamma, \forall s_i \in S_i$ 时, 有

$$v_i(\sigma_i^*, \sigma_{-i}^*) \geq v_i(s_i, \sigma_{-i}^*)$$

定义 2 在一个给定的有限 n 人策略式博弈 $G = \langle \Gamma; S_1, \dots, S_n; u_1, \dots, u_n \rangle$ 中, 混合策略组合 $\sigma^* = (\sigma_1^*, \sigma_2^*, \dots, \sigma_n^*)$ 为一个 Nash 均衡, 当且仅当 $\forall i \in \Gamma, \forall s_i \in S_i$ 时, 有

$$v_i(\sigma_i^*, \sigma_{-i}^*) \geq v_i(s_i, \sigma_{-i}^*)$$

2.2 混合策略下的交换协议模型

下面将一个交换协议记为 π , 其执行的过程看作一个混合策略扩展式博弈进行的过程, 则可以将交换协议描述为与扩展式博弈类似的七元组 $\pi = \langle T, A, Q, P, (I_i)_{i \in T}, (\geq_i)_{i \in T}, (H_i(\cdot))_{i \in T} \rangle$, 其中各元素的含义如下。

1) T : 参与者集合。

2) A : 参与者可选择的行动集合。一般用 a_i 表示参与者 $i \in T$ 的一个行动, $A_i = \{a_i\}$ 表示参与者 i 的可选行动集合, 从而 $A = \cup A_i$ 。

3) Q : 对于任意动作 a , $q.a$ 表示在非终点行动序列 q 后的动作 a , $A_i(q)$ 表示参与者 i 在非终点行动序列 q 后的可选行动集合。若 $q.a$ 为终点行动序列, 则表示协议执行完毕。

4) P : 参与者函数, 用于计算非终点行动序列的下一个参与者。表示为 $P: \{Q \setminus Z\} \rightarrow T$, 对于任意非终点行动序列 q , $P(q)$ 表示非终点行动序列 q 后的下一个参与者。

5) $(I_i)_{i \in T}$: 参与者 i 的信息集合。对于任何非终点行动序列 q 和 q' , 只要 $P(q) = P(q')$ 且 $A(q) = A(q')$, 则 q 和 q' 属于参与者 i 的同一个信息集。

6) $(\geq_i)_{i \in T}$: 参与者 i 在其混合策略集上的偏好关系。

如果 $v_i(\sigma_i^*, \sigma_{-i}^*) \geq v_i(\sigma_i, \sigma_{-i}^*)$, 则混合策略 σ_i^* 优于混合策略 σ_i , 记为 $\sigma_i^* \geq_i \sigma_i$ 。

如果 $v_i(s_i^*, \sigma_{-i}^*) \geq v_i(s_i, \sigma_{-i}^*)$, 则策略 s_i^* 优于策略 s_i , 记为 $s_i^* \geq_i s_i$ 。

7) $(H_i(\cdot))_{i \in T}$: 参与者 i 在每轮中其可选行动集上的混合策略熵函数, 若参与者 i 在第 r 轮中的可选行动集为 $A_i = (a_i^1, \dots, a_i^K)$, 其在可选行动集上的混合策略为 $\sigma_i = (\sigma_i^1, \dots, \sigma_i^K)$, 则 $H_i(r) = -\sum_{j=1}^K \sigma_i^j \lg \sigma_i^j$ 。

在对收益值进行计算的过程中, 加入一个惩罚函数 F 。在协议执行的每一轮中, 只要参与者采取某种不诚实行为, 就在他的收益值上减去相应的惩罚函数。在计算最终收益时将每一轮的惩罚值都算入收益结果中。

2.3 混合策略下的理性公平性

定义 3 过程公平性原则。在协议执行过程中, 若每个参与者在每个自己的可选行动集上的策略熵函数 $H_i(r)$ 相等, 即 $H_i(\cdot) = H_j(\cdot)$, 则该交换协议是过程公平的。

定义 4 混合策略 Nash 均衡。将有 2 个参与者的交换协议记为 π' , 将交换协议看为一个博弈, 2 个参与者分别为 A 和 B , 参与者的混合策略集分别记为 $\sum_A$ 和 $\sum_B$, 若一个交换协议是混合策略 Nash 均衡公平的, 则其存在一个混合策略组合 $\sigma^* = (\sigma_A^*, \sigma_B^*)$, 满足

$$v_A(\sigma_A^*, \sigma_{-A}^*) \geq v_A(s_A, \sigma_{-A}^*)$$

$$v_B(\sigma_B^*, \sigma_{-B}^*) \geq v_B(s_B, \sigma_{-B}^*)$$

定义 5 若一个交换协议在保证过程公平的前提下, 能满足混合策略 Nash 均衡公平性, 则称该协议为一个理性交换协议。

3 一种新的理性交换协议

3.1 理性交换协议的构造

在以上的混合策略博弈模型的基础上, 构建一个新的理性交换协议。假设进行通信的网络是可靠的, 使用的加密方法是安全的, 在保证过程公平的基础上, 通过对收益函数进行调整, 最终达到混合策略 Nash 均衡点, 从而实现理性公平交换。

协议中有 2 个参与者 A 、 B , A 是商家, B 是顾客。他们要交换的物品分别为 $item_A$ 、 $item_B$, 假设他们用于交换的物品是等价的, 即若协议正常执行, 则参与者 A 、 B 的收益均为 0。协议中用到弱秘密承诺函数 $w(k)$, 在一定的时间内, 该函数无法破解。构造的协议如图 1 所示。

$$\begin{aligned}
A \rightarrow B: & m_1 = E_{p_A}(\alpha_1, B, dsc_A, E_{k_A}(item_A), w(k_A)) \\
B \rightarrow A: & m_2 = E_{p_A}(\alpha_2, A, dsc_B, E_{k_B}(item_B), E_{k_A}(item_A), w(k_B)) \\
A \rightarrow B: & m_3 = E_{p_A}(B, E_{S_A}(k_A), E_{S_A}(m_2), t) \\
\text{其中, } & \alpha_1 = sig_{S_A}(B, dsc_A, E_{k_A}(item_A), w(k_A)) \\
& \alpha_2 = sig_{S_B}(A, dsc_B, E_{k_B}(item_B), w(k_B))
\end{aligned}$$

图1 理性交换协议交互过程

其中, dsc_A 是对所要交换的物品 $item_A$ 的描述, 参与者 A 随机选择对称密钥 k_A 对 $item_A$ 进行加密, 得到 $E_{k_A}(item_A)$; $w(k_A)$ 是弱秘密承诺函数, 能在一定时间内对密钥 k_A 进行有效保护; α_1 、 α_2 分别为参与者 A 、 B 用自己的私钥 S_A 、 S_B 对所发消息进行的数字签名, 并用对方的公钥 P_B 、 P_A 对所发的消息、数字签名进行加密; t 为时间戳。

步骤1 参与者 A 遵循一定的概率分布选择发送正确的消息 m_1 或虚假消息 m_1^* 。如果一开始 A 就发送虚假的消息, 那在第三轮中, B 能通过收到的 k_A 发现 A 欺骗了他。而在消息 m_1 中有 A 的签名, 这时 A 就不能为自己的欺骗行为进行辩解, 从而接受惩罚。 A 发送 m_1^* 的惩罚值为 F_{A_1} , F_{A_1} 的值大于交换物品本身的价值, $F_{A_1} > u_A^+$ 。

步骤2 参与者 B 能观察到参与者 A 选择发送消息的概率分布, 为了保证过程公平性, B 采取与 A 相同的概率分布选择自己要发送的消息。假设参与者 B 是诚实且理性的, 他可以选择发送的信息为 $quit_B$ 、 m_2 。

步骤3 参与者 A 使用与第一步相同的概率分布去选择发送消息 m_3 或 $quit_A$, 若 A 在第三轮中没有发送消息 m_3 , 则在一定的时间后, B 能提起申诉, 这时 A 受到惩罚 F_{A_2} ; 若 B 收到了 m_3 却对 A 提起申诉, 则 A 可以用时间戳 t 为自己辩解。

3.2 理性交换协议的分析

下面从正确性、可追究性、公平性的角度对以上的理性交换协议进行分析。首先, 分析了在混合策略下该理性交换协议的正确性; 其次, 用 Kailar 逻辑对该协议进行了可追究性分析; 最后, 在过程公平性的原则下, 基于博弈树对整个协议过程进行了描述, 探寻了其混合策略 Nash 均衡的存在性。

1) 正确性

定理1 当交换协议正常执行完毕时, 若协议主体 A 和 B 分别能够获得所交换的物品 $item_A$ 和 $item_B$, 则上述基于混合策略下的理性交换协议是正确的。

证明 通过协议的执行过程, 可以看到, 当协议完成后, 参与者 A 能够获得消息 m_2 , 并且 A 可以利用自己的私钥 S_A , 通过解密算法 $D_{S_A}(E_{P_A}(\alpha_2, A, dsc_B, E_{k_B}(item_B), w(k_B)))$ 获得 $E_{k_B}(item_B)$ 和 $w(k_B)$, 经过一定的时间后, 通过弱秘密承诺函数 $w(k_B)$ 得到 k_B , 从而通过计算 $D_{k_B}(E_{k_B}(item_B))$ 得到想要交换的商品 $item_B$ 。

协议正常执行完毕后, 参与者 B 能够获得消息 m_1 和 m_3 , 通过解密算法 $D_{S_B}(m_1)$ 得到 $E_{k_A}(item_A)$ 、 $w(k_A)$, 并通过 m_3 中获得的 k_A , 通过解密算法 $D_{k_A}(item_A)$ 得到 $item_A$ 。

综上, 当协议正常执行完毕时, 各方参与者都能得到自己想要交换的商品 $item_A$ 、 $item_B$, 即该混合策略下的理性交换协议是正确的。

2) 可追究性

可追究性要求任何交易方必须为自己的行为负责, Kailar 逻辑是专门针对电子商务可追究性进行分析的逻辑。其有如下基本原理。

$$\begin{aligned}
\text{连结: } & \frac{A \text{ CanProve } x; A \text{ CanProve } y}{A \text{ CanProve } x \wedge y} \\
\text{推断: } & \frac{A \text{ CanProve } x; x \Rightarrow y}{A \text{ CanProve } y} \\
\text{签名: } & \frac{A \text{ Received}(m \text{ SignedWith } K^{-1}); x \text{ in } m}{A \text{ CanProve}(K \text{ Authenticates } B)} \\
& \frac{A \text{ CanProve}(K \text{ Authenticates } B)}{A \text{ CanProve}(B \text{ Says } x)} \\
& \frac{A \text{ CanProve}(B \text{ Says } x)}{A \text{ CanProve}(B \text{ IsTrustedOn } x)} \\
\text{信任: } & \frac{A \text{ CanProve}(B \text{ IsTrustedOn } x)}{A \text{ CanProve } x}
\end{aligned}$$

用 Kailar 逻辑对上述协议进行形式化分析, 若协议能满足一定的目标, 则说明该协议在 Kailar 逻辑下满足可追究性。

定理2 在给定的初始状态假设下, 该协议在 Kailar 逻辑下具有可追究性。

证明 根据 Kailar 逻辑的定义, 该协议保证可追究性必须满足的目标如下。

$$G1: A \text{ CanProve}(B \text{ Received } item_A)$$

G2: $B \text{ CanProve}(A \text{ Sent } item_A)$

G3: $B \text{ CanProve}(A \text{ Received } item_B)$

G4: $A \text{ CanProve}(B \text{ Sent } item_B)$

对于协议目标的推导有关的部分语句解释如下。

① $B \text{ Received}(B, dsc_A, E_{k_A}(item_A), w(k_A)) \text{ Signed With } S_A$

② $A \text{ Received}(A, dsc_B, E_{k_A}(item_A), E_{k_B}(item_B), w(k_B)) \text{ Signed With } S_B$

③ $B \text{ Received}(B, E_{S_A}(k_A), m_2, t) \text{ Signed With } P_B$

引入如下初始状态假设。

A1: $A \text{ CanProve}(P_B \text{ Authenticates } B)$

A2: $B \text{ CanProve}(k_B \text{ Authenticates } B)$

A3: $B \text{ CanProve}(P_A \text{ Authenticates } A)$

A4: $A \text{ CanProve}(k_A \text{ Authenticates } A)$

A5: $A \text{ Says } E_{k_A}(item_A) \Rightarrow A \text{ Sent } item_A$

A6: $B \text{ Says } E_{k_A}(item_A) \wedge (k_A \text{ Authenticates } A) \Rightarrow$

$B \text{ Received } item_A$

A7: $B \text{ Says } E_{k_B}(item_B) \Rightarrow B \text{ Sent } item_B$

A8: $A \text{ Says } E_{k_B}(item_B) \wedge (k_B \text{ Authenticates } B) \Rightarrow$

$A \text{ Received } item_B$

根据上述假设, 利用 Kailar 逻辑进行如下推理。

当 B 收到消息①时, 可得

$B \text{ Received } E_{k_A}(item_A) \text{ Signed With } S_A$

由假设 A3 和签名原理得

$B \text{ CanProve}(A \text{ Says } E_{k_A}(item_A))$

再由假设 A5 和推断原理得

$B \text{ CanProve}(A \text{ Sent } item_A)$

即满足 G2。

当 A 收到消息②时, 可得

$A \text{ Received } E_{k_A}(item_A) \text{ Signed With } S_B$

由假设 A1 和签名原理得

$A \text{ CanProve}(B \text{ Says } E_{k_A}(item_A))$

在由假设 A4 和连结原理得

$A \text{ CanProve}(B \text{ Says } E_{k_A}(item_A) \wedge (k_A \text{ Authenticates } A))$

最后, 由假设 A6 和推断原理得

$A \text{ CanProve}(B \text{ Received } item_A)$

即满足 G1。

同理可证目标 G3、G4 能被满足。

因此, 该协议在 Kailar 逻辑下具有可追究性。

3) 公平性

根据上述建立的模型, 利用博弈树对整个协议过程进行描述, 如图 2 所示。

第一轮由参与者 A 开始选择行动。 A 的可选行动集为 $A_A^1 = \{m_1, m_1^*\}$, A 在 A_A^1 上的混合策略为 $\sigma_A^1 = \{\theta, 1-\theta\}$, 即参与者 A 以概率 θ 选择行动 m_1 , 以概率 $1-\theta$ 选择行动 m_1^* 。这时的混合策略熵函数 $H_A(1) = -\theta \lg \theta - (1-\theta) \lg (1-\theta)$ 。 A 执行完毕后, 协议进入第二轮。

第二轮由参与者 B 开始选择行动。参与者 B 不能够区分 A 发送的消息是 m_1 还是 m_1^* , 但是, B 能够观察到 A 在可选行动集上的概率分布。此时参与者 B 的信息集 $I_B = \{m_1, m_1^*\}$ 。为了达到过程公平, 即参与者 B 不想让参与者 A 通过自己的行动推测到更多的信息, B 选择以和 A 相同的概率分布选择自己的行动。此时 $A_B^1 = \{m_2, quit_B\}$, B 在 A_B^1 上的混合策略为 $\sigma_B^1 = \{\beta, 1-\beta\}$, 混合策略熵函数 $H_B(2) = -\beta \lg \beta - (1-\beta) \lg (1-\beta)$ 。若参与者 B 选择行动 $quit_B$, 则博弈终止; 若 B 选择 m_2 , 第二轮结束进入第三轮, 双方受益待定。

第三轮由参与者 A 开始, 若在第二轮中 B 选择 $quit_B$, 则 A 不做任何动作, 博弈终止。若 B 选择了 m_2 , 则 A 的可选行动集 $A_A^2 = \{m_3, quit_A\}$, A 在 A_A^2 的混合策略为 $\sigma_A^2 = \{\alpha, 1-\alpha\}$ 。当 A 选择 m_3 或 $quit_A$ 后, 博弈终止。

下面分析此交换协议的公平性。在博弈过程中, 每个参与者会极力猜测对方如何选择, 同时又不能让对方猜到自己的选择, 为了使对方猜不透自己的选择, 会随机选择自己的策略, 即以一定的概率分布去选择自己的策略。通过分析, 可以知道如下信息。

参与者 A 的纯策略集为

$$S_A = (m_1 quit_A, m_1 m_3, m_1^* quit_A, m_1^* m_3)$$

相应的混合策略为

$$\sigma_A = (\theta(1-\alpha), \theta\alpha, (1-\theta)(1-\alpha), (1-\theta)\alpha)$$

参与者 B 的纯策略集为

$$S_B = (m_2, quit_B)$$

相应的混合策略为

$$\sigma_B = (\beta, 1-\beta)$$

则可以得到如图 3 所示的收益矩阵。

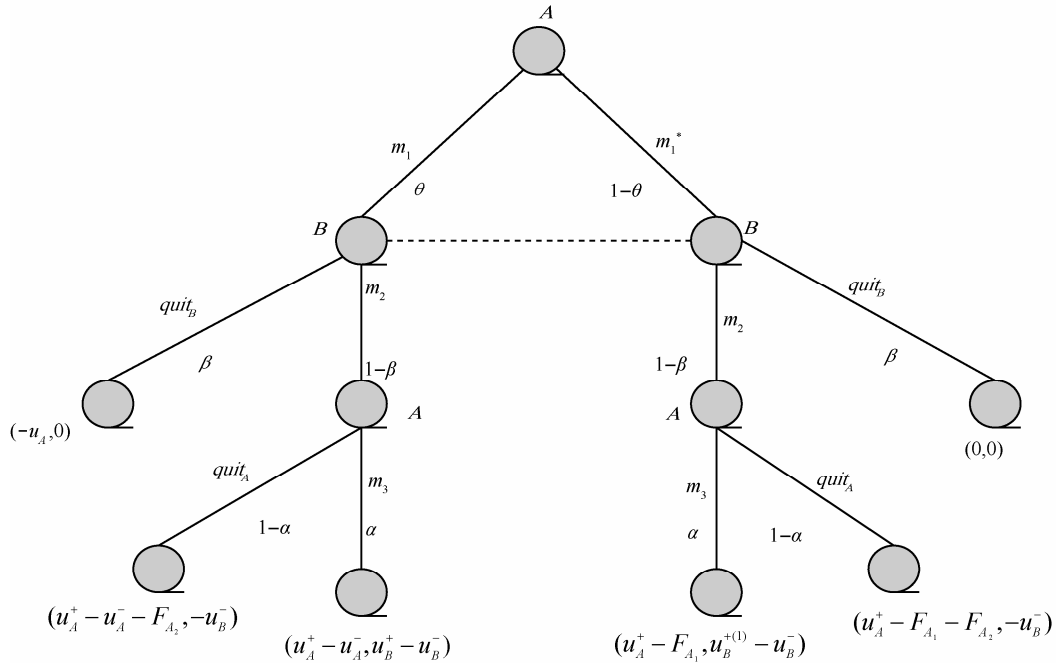


图2 交换协议的博弈树描述

			$\theta\alpha$ $m_1 m_3$	$\theta(1-\alpha)$ $m_1 quit_A$	$(1-\theta)\alpha$ $m_1^* m_3$	$(1-\theta)(1-\alpha)$ $m_1^* quit_A$
B	β	m_2	$(u_A^+ - u_A^-, u_B^+ - u_B^-)$	$(u_A^+ - u_A^- - F_{A_1}, -u_B^-)$	$(u_A^+ - F_{A_1}, u_B^{+(1)} - u_B^-)$	$(u_A^+ - F_{A_1} - F_{A_2}, -u_B^-)$
	$1-\beta$	$quit_B$	$(-u_A^-, 0)$	$(-u_A^-, 0)$	$(0, 0)$	$(0, 0)$

图3 收益矩阵

下面讨论在什么条件下混合策略组合

$$\sigma = (\sigma_A, \sigma_B) = ((\theta(1-\alpha), \theta\alpha, (1-\theta)(1-\alpha), (1-\theta)\alpha), (\beta, 1-\beta))$$

为混合策略 Nash 均衡。

在过程公平的原则下，为了保证每一轮中的混合策略熵函数不变，假设 $\theta = \alpha = \beta$ 。所以，参与者 A 在混合策略组合 (σ_A, σ_B) 下的期望收益为

$$\begin{aligned} v_A(\sigma_A, \sigma_B) &= \theta^3(u_A^+ - u_A^-) + \theta^2(1-\theta)(-u_A^-) + \\ &\theta^2(1-\theta)(u_A^+ - u_A^- - F_{A_2}) + \theta(1-\theta)^2(-u_A^-) + \\ &\theta^2(1-\theta)(u_A^+ - F_{A_1}) + \theta(1-\theta)^2(u_A^+ - F_{A_1} - F_{A_2}) \\ &= \theta^3(u_A^+ - u_A^-) + \theta^2(1-\theta)(-u_A^- + u_A^+ - u_A^- - F_{A_2} + u_A^+ - F_{A_1}) + \\ &\theta(1-\theta)^2(-u_A^- + u_A^+ - F_{A_1} - F_{A_2}) \\ &= \theta^3(u_A^+ - u_A^-) + \theta^2(1-\theta)(2u_A^+ - 2u_A^- - F_{A_1} - F_{A_2}) + \\ &\theta(1-\theta)^2(u_A^+ - u_A^- - F_{A_1} - F_{A_2}) \end{aligned}$$

当参与者 B 选择混合策略 σ_B 时，A 选择各个纯策略的期望收益为

$$v_A(m_1 m_3, \sigma_B) = \theta(u_A^+ - u_A^-) + (1-\theta)(-u_A^-)$$

$$v_A(m_1 quit_A, \sigma_B) = \theta(u_A^+ - u_A^- - F_{A_2}) + (1-\theta)(-u_A^-) < 0$$

$$v_A(m_1^* m_3, \sigma_B) = \theta(u_A^+ - F_{A_1}) < 0$$

$$v_A(m_1^* quit_A, \sigma_B) = \theta(u_A^+ - F_{A_1} - F_{A_2}) < 0$$

由定义 2 可知，当 $v_A(\sigma_A, \sigma_B) \geq v_A(S_A, \sigma_B)$ 时， σ_A 为参与者 A 的最优混合策略，则有 $v_A(\sigma_A, \sigma_B) \geq v_A(m_1 m_3, \sigma_B)$ 。令 $x = u_A^+ - u_A^-$ ， $F = F_{A_1} + F_{A_2}$ ，可得

$$\begin{aligned} &\theta^3 x + 2\theta^2(1-\theta)x + \theta(1-\theta)^2 x - \theta^2(1-\theta)F - \theta(1-\theta)^2 F \\ &\geq \theta(u_A^+ - u_A^-) + (1-\theta)(-u_A^-) \theta(u_A^+ - u_A^-) - (\theta - \theta^2)F \\ &\geq \theta u_A^+ - u_A^- \end{aligned}$$

$$\frac{1-\theta}{\theta - \theta^2} \geq \frac{F}{u_A^-}$$

$$\text{即 } \theta \leq \frac{u_A^-}{F}.$$

同理，可以对参与者 B 在混合策略

$$\sigma = (\sigma_A, \sigma_B) = ((\theta\alpha, \theta(1-\alpha), (1-\theta)\alpha, (1-\theta)(1-\alpha)), (\beta, 1-\beta))$$

下的期望收益进行讨论。

在过程公平的原则下，即 $\theta = \alpha = \beta$ ，参与者 B 在混合策略组合 (σ_A, σ_B) 下的期望收益为

$$\begin{aligned} v_B(\sigma_A, \sigma_B) &= \theta[\theta^2(u_B^+ - u_B^-) + \theta(1-\theta)(-u_B^-) + \\ &\quad \theta(1-\theta)(u_B^{+(1)} - u_B^-) + (1-\theta)^2(-u_B^-)] \\ &= \theta^3 u_B^+ + \theta^2 u_B^{+(1)} - \theta^3 u_B^{+(1)} - \theta u_B^- \end{aligned}$$

当参与者 A 选择混合策略 σ_A 时，参与者 B 选择纯策略 m_2 、 $quit_B$ 的期望收益为

$$\begin{aligned} v_B(\sigma_A, m_2) &= \theta^3 u_B^+ + \theta^2 u_B^{+(1)} - \theta^3 u_B^{+(1)} - \theta u_B^- \\ v_B(\sigma_A, quit_B) &= 0 \end{aligned}$$

由定义2可知，当 $v_B(\sigma_A, \sigma_B)$ 满足

$$\begin{aligned} v_B(\sigma_A, \sigma_B) &\geq v_B(\sigma_A, m_2) \\ v_B(\sigma_A, \sigma_B) &\geq v_B(\sigma_A, quit_B) \end{aligned}$$

时， σ_B 为参与者 B 的最优混合策略，即 $\theta^3 u_B^+ + \theta^2 u_B^{+(1)} - \theta^3 u_B^{+(1)} - \theta u_B^- \geq 0$ 。又因为 $u_B^+ > u_B^{+(1)}$ ，则有

$$\begin{aligned} \theta^3 u_B^+ + \theta^2 u_B^{+(1)} - \theta^3 u_B^{+(1)} - \theta u_B^- &> \theta^3 u_B^{+(1)} + \\ \theta^2 u_B^{+(1)} - \theta^3 u_B^{+(1)} - \theta u_B^- &= \theta^2 u_B^{+(1)} - \theta u_B^- \end{aligned}$$

则只需证明 $\theta^2 u_B^{+(1)} - \theta u_B^- \geq 0$ ，即 $\theta \geq \frac{u_B^-}{u_B^{+(1)}}$ 。

综上，当 θ 满足 $\frac{u_B^-}{u_B^{+(1)}} \leq \theta \leq \frac{u_A^-}{F}$ 时，混合策略组合 $\sigma = (\sigma_A, \sigma_B)$ 为混合策略 Nash 均衡。

通过以上分析可以看到，在所构造的新的理性交换协议中，惩罚值并非越大越好。参与者遵守协议的概率与惩罚值和交换物品本身的价值之比有关。在这样的情况下，可以通过对惩罚值的设定控制参与者遵守协议的概率分布，从而更好地促使参与者遵守协议。

3.3 实例分析

现在商家 A 要和顾客 B 交换的商品价值 $u_A^- = 10$ ，在交换正常进行的情况下， B 将会得到该价值的物品，即 $u_B^+ = 10$ 。现商家进行促销，对所售商品进行打折销售，且设定惩罚值 $F = u_A^-$ ，则可以得到 θ 和 u_B^- 之间的变化关系，如表1所示。

表1 成本与选择概率之间的关系

u_B^-	θ
9	[0.9, 1]
8	[0.8, 1]
7	[0.7, 1]
6	[0.6, 1]
5	[0.5, 1]

可以看到，随着商家给出折扣的升高，顾客 B 在得到实惠的同时，所面临风险的不确定度也在增大。此时商家的报价越接近商品的实际价值，则协议正常执行的概率就越大。而这时若随意改动惩罚值，则有可能找不到满足条件的 θ 。那么，原有的协议博弈在没有均衡解的情况下，很难保证协议的正常进行。而对于惩罚值的设定，并非越高越好。在所提出的模型中，过高的惩罚值反而会降低 θ 最大值的取值，让商家望而却步，从而降低了商家诚信参与协议的概率。

4 结束语

本文在假设加密方法安全、网络通道可靠的前提下，引入熵理论对协议交换过程中的不确定性进行描述，进而给出过程公平的定义，并在保证过程公平的原则下，应用扩展式博弈下的混合策略理论对理性交换协议进行建模。结合所建模型和博弈论中混合策略 Nash 均衡的定义，本文对理性交换协议做了形式化的定义，并构造了一个新的理性交换协议。而当网络不一定可靠以及过程不一定严格公平时，如何建立一个基于扩展博弈的协议博弈模型，在这样的模型中交换协议是否依然满足理性公平将是进一步研究的方向。

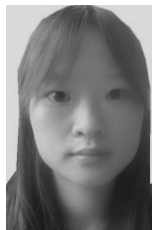
参考文献:

- [1] ASOKAN N. Fairness in electronic commerce[D]. Waterloo: University of Waterloo, 1998.
- [2] SYVERSON P. Weakly secret bit commitment: applications to lotteries and fair exchange[C]//The 11th IEEE Computer Security Foundations Workshop. c1998: 2-13.
- [3] BUTTYAN L. Building blocks for secure services: authenticated key transport and rational exchange protocols[D]. Lausanne: Ecole Polytechnique Federale de Lausanne, 2001.

- [4] ALCAIDE A, ESTEVEZ-TAPIADOR J M, HERNANDEE-CASTRO J C, et al. An extended model of rational exchange based on dynamic games of imperfect information[C]//International Conference on Emerging Trends in Information and Communication Security. c2006: 396-408.
- [5] ALCAIDE A. Rational exchange protocols[D]. Leganés: Universidad Carlos III de Madrid, 2008.
- [6] ESTEVEZ-JAPIADOR J M, ALCAIDE A, HERMANDEZ-CASTRO J C, et al. Bayesian rational exchange[J]. International Journal of Network Security, 2008, 7(1): 85-100.
- [7] 吕桢, 彭长根, 刘海. 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.
LV Z, PENG C G, LIU H. Rational fairness exchange protocols based on maximum entropy principle[J]. Application Research of Computers, 2014, 31(2):563-567.
- [8] 陈运. 信息论与编码[M]. 北京: 电子工业出版社, 2007.
CHEN Y. Information theory and coding[M]. Beijing: Publishing House of Electronics Industry, 2007.
- [9] 朱·弗登博格, 让·梯若儿. 博弈论[M]. 黄涛, 译. 北京: 中国人民大学出版社, 2010.
FUDENBERG D, TIROLE J. Game theory[M]. Translated by HUANG T. Beijing: China Renmin University Press, 2010.
- [10] 王可心, 韩芳溪. Kailar 逻辑推理中初始状态假设[J]. 大连理工大学学报, 2003, 43(1): 193-196.
WANG K X, HAN F X. Initial state assumptions in Kailar logic reasoning[J]. Journal of Dalian University of Technology,

2003, 43(1): 193-196.

作者简介:



丁洪(1991-), 女, 贵州安顺人, 贵州大学硕士生, 主要研究方向为密码学理论与工程。



彭长根(1963-), 男, 侗族, 贵州锦屏人, 博士, 贵州大学教授、博士生导师, 主要研究方向为密码学、信息安全。



邝青青(1988-), 男, 贵州安顺人, 贵州大学硕士生, 主要研究方向为密码学理论与工程。