有限理性公平数据交换协议的设计与仿真

陆正福 普艳红 倪盛斌 许辰铭 杨春尧
(云南大学数学与统计学院 昆明 650500)

摘 要 理性交换协议(REP)因使用了理想化的理性假设,在现实中有可能失效。为解决此协议失效的问题,基于与现实更为接近的有限理性假设(BRH),定义了有限理性公平概念,并首次基于 BRH 设计了有限理性公平数据交换协议(FDEP-BR)。理论分析表明,与 REP 相比,FDEP-BR 虽然牺牲了一定效率(轮复杂度为 $O(l*v)$),但具有容错性和有限理性公平性,能够抵抗非合作攻击。对 FDEP-BR 构造自动机模型,并改进经验加权吸引(EWA)学习模型的决策方式,设计了 EWA 学习决策算法;在此基础上,基于 Jade-Repast 集成平台对 FDEP-BR 进行了仿真,仿真结果表明 FDEP-BR 的均衡状态与预期具有一致性。

关键词 有限理性,有限自动机,有限理性公平,公平数据交换协议,协议仿真
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.017

Design and Simulation of Fair Data Exchange Protocol with Bounded Rationality

LU Zheng-fu PU Yan-hong NI Sheng-bin XU Chen-ming YANG Chun-yao
(School of Mathematics and Statistics, Yunnan University, Kunming 650500, China)

Abstract Rational exchange protocol may fail in reality because of the use of the idealized rationality hypothesis. In order to solve the protocol failure problem, based on bounded rationality hypothesis which is more consistent with the reality, the concept of bounded rational fairness was defined and fair data exchange protocol with bounded rationality (FDEP-BR) was designed for the first time. The theoretical analysis shows that the FDEP-BR can resist non-cooperative attack because of its fault-tolerance and bounded rationality fairness at the cost of round complexity $O(l*v)$ compared with the rational exchange protocol. A finite automata model for FDEP-BR was constructed, the decision-making method for experiential weighted attraction (EWA) learning model was improved, and the EWA learning decision algorithm was designed. Then the FDEP-BR was simulated on the Jade-Repast integration platform. The simulation results show that the equilibrium state of the FDEP-BR is consistent with expectations.

Keywords Bounded rationality, Finite automata, Bounded rational fairness, Fair data exchange protocol, Protocol simulation

1 引言

1998 年,Asokan[1]在欧洲密码学会上首次提出了基于博弈论来设计公平交换协议的思想,并设计了两方公平数字签名交换协议。同年,Syverson[2]首次提出理性交换(Rational Exchange,RE)的概念,并基于弱比特承诺函数设计了两方理性交换协议(Rational Exchange Protocol,REP),为理性交换协议的设计奠定了基础。之后,Buttyán 等基于逐步交换的思想设计了理性支付协议,研究了理性公平与公平交换之间的关系,指出公平性能推导出理性,而理性却不能推导出公平性[3-5];进一步地,Buttyán 等还基于博弈论框架对理性交换进行了形式化建模,并将其用于分析 Syverson 协议[6-7]。Alcaide 等[8-10]分析了 Syverson 协议的缺陷并对其进行改进,基于博弈论框架对理性交换协议进行形式化研究,提出了一种扩展模型并设计了自动生成的三方理性交换协议。Campos 等[11]于 2015 年基于完全但不完美信息的非合作博弈研究了多方理性信息交换协议中的均衡问题。Tao 等[12]于 2016 年以大数据、物联网和云计算数据交换为背景,为了验证和保证数据交换机制的公平性,基于不完全信息扩展博弈提出了具体的分析模型,分析了交换中的合理性和公平性。国内对理性交换协议的研究主要集中于文献[13-17],其中文献[13-15]基于信息熵、过程公平性原则和激励相容机制分别设计了满足理性公平的理性交换协议;文献[16]基于博弈论对理性交换协议进行了形式化建模和分析;文献[17]基于理性秘密

到稿日期:2018-06-22 返修日期:2018-08-28 本文受国家自然科学基金项目(10861012),云南省教育厅科学研究基金项目(09Y0347),云南大学理(工)科校级科研基金项目(YNUY201368),云南大学中青年骨干教师培养计划专项经费基金项目(XT412003)资助。
陆正福(1965-),男,教授,主要研究方向为信息安全、协议工程和网络计算等,E-mail:zhflu@ynu.edu.cn(通信作者);**普艳红**(1992-),男,硕士生,主要研究方向为信息安全;**倪盛斌**(1987-),男,硕士,主要研究方向为信息安全;**许辰铭**(1987-),男,硕士,主要研究方向为信息安全;**杨春尧**(1986-),男,硕士,工程师,主要研究方向为信息安全。

共享设计了多方理性交换协议。

总体来看，自 1998 年 Syverson 开创性地设计了 Syverson 协议以来，虽然国内外很多学者都基于博弈论的不同模型研究了理性交换协议，但他们均以理性假设(Rationality Hypothesis，RH)为前提，这样的主体假设过于理想化，偏离了现实，并不能很好地解释现实中的很多现象，因此早在 20 世纪中期就有学者对 RH 提出了质疑。经济学家 Simon 于 1955 年提出了有限理性假设[18](Bounded Rationality Hypothesis，BRH)，对 RH 发出了挑战，继而也有学者对 RH 提出质疑[19-20]，以 1978 年 Simon 获得诺贝尔经济学奖为契机，有限理性假设(BRH)确立了它在学术界的地位。

传统的公平交换协议的主体假设是两极假设(即要么是诚实的，要么是恶意的)，诚实的参与者总是遵守协议，而恶意的参与者总是偏离协议。随着理性交换协议被学者提出，公平交换协议的主体假设进入了 RH 阶段，协议参与者能根据具体收益做出最优决策。到目前为止，在设计公平交换协议时均是基于 RH 的，但 RH 过于理想化而偏离了现实，并不能很好地解释现实中的很多现象[19-20]，故有必要将协议的主体假设引入 BRH。

本文基于 BRH 研究了有限理性公平数据交换协议(Fair Data Exchange Protocol with Bounded Rationality，FDEP-BR)的设计。首先，对交换场景的有限理性做出合理假设，证明了 REP 在 BRH 下存在一定的失效概率且不能抵抗非合作攻击，并基于概率公平定义了强于理性公平的有限理性公平(见第 3 节)。其次，设计了惩罚机制 M_{RE}^{δ} 来约束有限理性参与者的行为，基于机制 M_{RE}^{δ} 和理性秘密共享思想设计了 FDEP-BR，证明了其具有正确性、有限理性公平性，能抵抗非合作攻击，并与经典的理性交换协议进行了对比分析(见第 4 节)。最后，对 FDEP-BR 建模，设计仿真算法，并基于此在 Jade-Repast 集成平台上对 FDEP-BR 进行仿真，验证其均衡状态与预期是否具有一致性(见第 5 节)。

2 预备知识

本节主要介绍博弈论、机制设计、自动机理论、理性秘密共享[21]和理性交换协议[4]的相关知识。

2.1 博弈论知识

定义 1(基本博弈模型) 一个基本博弈模型 $G=[P,S,U]$是一个三元组，其中：

(1)$P=\{P_1,P_2,\cdots,P_n\}$为参与者集合，满足$|P|=n$。P_i表示第$i(1\leqslant i\leqslant n)$个参与者，$P_{-i}$表示除了参与者 P_i 外的其余所有参与者的集合。

(2)$S=\{S_1,S_2,\cdots,S_n\}$是策略集合。记参与者 P_i 的策略为$s_i,s_i\in S_i$，其中 S_i为参与者P_i 可选择的策略组成的策略集合，n 个参与者各选择一个策略形成的向量 $s=\{s_1,s_2,\cdots,s_n\}$称为策略组合。记 P_i 的对手 P_{-i}所采取策略的组合为s_{-i}。

(3)U 是参与者在不同策略组合下的效用函数。$U=\{u_1,u_2,\cdots,u_n\}$，$u_i:S\rightarrow R$(R 为实数空间)表示参与者 P_i 在不同策略组合下所得到的收益。

定义 2(纳什均衡) 在 n 人的非合作博弈中，策略组合$s=(s_1,s_2,\cdots,s_n)$构成了一个纳什均衡，当且仅当：对于任意一个参与者$i(i=1,2,\cdots,n)$，其策略s_i是策略组合s 中的其他参与者策略 s_{-i}的最优回应，即对于任意 $s_i'\in S_i$，$u_i(s_i,s_{-i})\geqslant u_i(s_i',s_{-i})$。

定义 3(机制设计) 机制 $M=(o,p)$是一个二元组，其中：

(1)$o(\cdot)$是输出函数，对于$\forall i\in[1,n]$，参与者 P_i 选择的策略构成策略组合$a=(a_1(\theta_1),\cdots,a_n(\theta_n))$，机制 M 以策略 a 为输入，$a=o(a)$为输出(θ_i为理性参与人 P_i 的类型)。

(2)$p=\{p_1,\cdots,p_n\}$是支付集合，机制 M 根据每个理性参与人 P_i 选择的策略$a_i(\theta_i)$支付其额外收益 $p_i=p_i(a)\in p$。

2.2 有限自动机理论

定义 4(有限状态自动机) 有限状态自动机 $FA=\langle Q,\Sigma,\delta,q_0,F\rangle$是一个五元组，其中：

(1)Q 是一个有限状态的集合；

(2)Σ 是字母表，是输入带上的字符构成的集合；

(3)$q_0\in Q$，表示开始状态；

(4)$F\subseteq Q$，是接收状态(终止状态)集合；

(5)$\delta:Q\times\Sigma\rightarrow Q$，是状态转移函数。

2.3 密码学知识

定义 5(双变量单向函数) 若 $E=f(x,y)$满足以下性质，则称其为双变量单向函数：

(1)已知 x,y，则计算 $C=f(x,y)$是容易的；

(2)已知 x,C，则计算 y 是不可行的；

(3)未知 y 时，对于$\forall x$，则计算 $C=f(x,y)$是困难的；

(4)给定 y，找到两个不同的 x_1,x_2，使得等式 $f(x_1,y)=f(x_2,y)$成立是困难的；

(5)已知 y,C，则计算 x 在计算上是不可行的；

(6)已知 x_1和 $f(x_1,y)$，计算 $f(x_2,y)$是困难的。

定义 6(理性秘密共享) 理性秘密共享是将博弈论应用于解决密码学领域内一些关键问题的标志性研究，在赋予参与者理性假设后，参与者具有自利性和排他性。Halpern 等[21]于 2004 年在设计理性秘密共享时给出了理性参与者的效用假设，即 $U^+>U>U^->U^{--}$，其中：

(1)U^+表示 P_i 独得秘密；

(2)U 表示 P_i 和 P_{-i}均获得秘密；

(3)U^-表示 P_i 和 P_{-i}均未获得秘密；

(4)U^{--}表示 P_i 未获得秘密而 P_{-i}获得秘密。

定义 7(理性交换协议) Syverson[2]于 1998 年首次提出了理性交换的概念，并设计了一个两方理性交换协议，该协议保证了参与者偏离协议不会带来额外的收益，即让参与者没有偏离协议的动机。

协议 1 Syverson 理性交换协议

$A\rightarrow B:m_1=(desc_{item_A},E_k(item_A),w(k),\sigma_1)$

$B\rightarrow A:m_2=(item_B,m_1,\sigma_2)$

$A\rightarrow B:m_3=(k,m_2,\sigma_3)$

其中：$\sigma_1=sig(k_A^{-1},(desc_{item_A},E_k(item_A),w(k)))$，$\sigma_2=sig(k_B^{-1},(item_B,m_1))$，$\sigma_3=sig(k_A^{-1},(k,m_2))$。

协议 1 中，$item_A$和 $item_B$分别表示参与方 A 和 B 要交换的项目内容；$desc_{item_A}$是对项目$item_A$的描述；$E_k(item_A)$表示用对称加密密钥 k 对$item_A$进行加密；k 是随机选择的密钥；

$w(\cdot)$是一个弱密码承诺函数，$w(k)$表示如果能在 t 时间内破解比特串 k，那么 t 处于可接受的最低值和最高值之间；σ_1 和σ_3分别表示参与者 A 用其私钥 k_A^{-1} 对其发送的消息 m_1 和 m_3 进行数字签名，σ_2 表示参与者 B 用其私钥 k_B^{-1} 对其发送的消息 m_2 进行数字签名。

3　基于 BRH 分析 REP

3.1　有限理性分析

在错综复杂的网络环境中，互不信任的节点之间需要安全和公平地交换有价值的数据或信息，在交换开始之前，由于信息不完全，交换双方的理性程度只能达到有限理性。虽然参与者仍具有自利性和排他性，但在决策刚开始时不具有稳定的偏好，也无法做出最优决策。以博弈论为理论基础，对公平数据交换场景中参与者的有限理性进行合理化假设（即参与者具备如下有限理性特征）。

假设 1　交换参与者具有自利性和排他性。

假设 2　交换参与者知道所有待交换对手。

假设 3　交换参与者具有完全策略集。

假设 4　交换参与者具有不完全收益信息。

假设 5　交换参与者具有不完全策略序。

以上 5 条假设表明，在交换之前参与者均能确定自己的交换对象（交换最基本的条件）；能明确知道自己和交换对象的所有可选策略（即发送策略和不发送策略，或遵守协议和偏离协议）；没有确定的收益函数，在交换博弈开始之前均不知道自己和对手可选策略的具体收益，只能在每一轮交换结束后不断更新策略的收益信息；不知道发送策略和不发送策略的具体序关系，只有在交换过程中通过不断更新策略的收益信息来明确策略之间的序关系。下文中的有限理性假设（BRH）均是指以上 5 条假设描述的有限理性。

3.2　REP 有效性分析

在分析 REP 的有效性之前，首先介绍一个定义。受文献[22]中秘密共享的非合作攻击启发，定义在公平数据交换中的非合作攻击。

定义 8（非合作攻击）　参与者在执行公平数据交换协议时提供他们伪造的数据或不提供数据。

Syverson 协议是开创性的、最具代表性的理性交换协议，绝大多数学者在设计理性交换协议时均继承了 Syverson 协议中的交互方式。因此，下面分析 BRH 对采用 Syverson 固定交互方式的理性交换协议的影响（BRH 指 3.1 节描述的有限理性）。

命题 1　非合作攻击下，固定交互方式的 REP 将失效。

证明：在以 Syverson 协议为代表的具有固定交互模式的理性交换协议中（如协议 1 所示，交换双方共发送 3 次信息），当 A 在第一步选择不发送或发送伪造信息时，B 在第二步选择支付则利益受损，选择不支付则交换失败；当 A 在第三步选择不发送或发送伪造信息时，则 B 利益受损；当 B 在第二步选择发送支付的伪造信息或不支付时，虽然 A 的利益不受损但交换失败。因此，在以上 3 步中只要任意一方采取非合作攻击就无法达成公平交换，REP 失效。综上，结论得证。

下面进一步证明在 BRH 下 REP 失效的概率。

命题 2　在 BRH 下，当交换双方选择发送策略（遵守协议）的概率分别为 p_1 和 p_2 时，REP 失效的概率为 $1-p_1*(p_2)^2$ 或 $1-p_2*(p_1)^2$。

证明：在 BRH 下，交换的前几轮中交换双方均不知道发送策略和不发送策略的具体收益，无法确定两种策略的具体偏好，在决策时表现为以不同的概率选择两种策略。因此，当交换双方选择发送策略的概率分别为 p_1 和 p_2 时，理性交换协议要能成功执行就需要在交互中双方均选择发送正确的信息（共 3 条消息），则协议成功执行的概率为 $p_1*(p_2)^2$ 或 $p_2*(p_1)^2$，具体成功执行协议的概率与交换顺序有关，从而协议失效的概率就为 $1-p_1*(p_2)^2$ 或 $1-p_2*(p_1)^2$。例如，当交换双方选择两种策略的概率均为 0.5 时（相当于随机选择两种策略），理性交换协议能成功执行的概率只有 $(1/2)^3=1/8$，协议失效的概率达到了 7/8。由此可知，当交换双方无法确定发送策略和不发送策略的具体偏好时，协议将有极大的概率失效。综上，结论得证。

3.3　有限理性公平

公平性是在设计交换协议时追求的重要属性，但是在 BRH 下，在协议执行中参与者可能会因为理性不足多次偏离协议，即使在某几轮遵守了协议，之后也可能再次偏离，在这样的情形下理性公平性并不能满足参与者的需求，即偏离协议不会带来额外收益的条件对有限理性的参与者无约束力。因此，有必要对理性公平进行适当修正，让其适用于有限理性交换场景。

定义 9（可忽略函数）　令函数 $\mu(\cdot)$ 是可忽略函数，如果对于任意的正多项式 $p(\cdot)$ 和足够大的正数 k，均有 $\mu(k)<1/p(k)$ 成立。

定义 10（概率公平）　设交换双方为 A 和 B，所拥有的待交换项目分别为 $item_A$ 和 $item_B$，则称交换协议 π 是概率公平的，如果在交换过程中下面两个条件同时成立：

(1)$\Pr[A \text{ acquire } item_B \mid B \text{ acquire } item_A]=1$ 且 $\Pr[B \text{ acquire } item_A \mid A \text{ acquire } item_B]=1$；

(2)$\Pr[A \text{ acquire } item_B \mid B \text{ not acquire } item_A]<\mu(k)$ 且 $\Pr[B \text{ acquire } item_A \mid A \text{ not acquire } item_B]<\mu(k)$。

即当交换参与者 A 和 B 中有一方获得对方的项目时，另一方同样可以获得对方的项目；同时，在对方未获得自己的项目时，自己获得对方的项目的概率是可忽略的。若同时满足以上条件，则称交换协议是概率公平的。

特别地，若同时满足：

$\Pr[A \text{ acquire } item_B \mid B \text{ not acquire } item_A]=0$

$\Pr[B \text{ acquire } item_A \mid A \text{ not acquire } item_B]=0$

则称交换协议是完全公平的。

定义 11（有限理性公平）　令 π 是两方有限理性交换协议，称 π 是有限理性公平的，如果同时满足以下两个条件：

(1)当参与者为理性时，协议 π 能保证理性公平；

(2)当参与者为有限理性时，协议 π 能保证概率公平。

下面分析有限理性公平与理性公平之间的关系。

命题 3　有限理性公平强于理性公平。

证明：理性公平是要求协议满足参与者偏离协议不会带来额外的收益，但是不能保证诚实遵守协议的参与者的利益

不遭受损失。而有限理性公平要求参与者偏离协议不会带来额外的收益，同时要求诚实遵守协议的参与者的利益遭受损失的概率是可忽略的。显然，有限理性公平强于理性公平，结论得证。

注：需特别注意，理性假设强于有限理性假设，而理性公平弱于有限理性公平。

4 有限理性公平数据交换协议的设计

4.1 惩罚机制的设计

不论是因自利性和排他性，还是因理性不足，均可能会导致参与者偏离协议。因此，协议应具有倾向调整机制，以约束和调整参与者的行为。

令策略 $s_t^{q(1)}$ 表示的参与者 P_t 在第 q 轮数据交换博弈中遵守协议，选择发送正确的子秘密，策略 $s_t^{q(2)}$ 则相应地表示偏离协议，不发送或发送错误的子秘密；历史 h_0^q 表示第 q 轮博弈开始前已构成的策略组合，h_1^q 表示第 q 轮有一个参与者做出决策后构成的策略组合（主要针对异步通信情形，参与者非同时做出决策），h_2^q 表示第 q 轮博弈结束后构成的策略组合，且有 $h_2^q=h_0^{q+1}$，则惩罚机制的定义如下。

定义 12（惩罚机制） 惩罚机制 $M_{\mathrm{RE}}^{\delta}=(h_t^q,p^q)$ 是二元组，其中：

（1）h_t^q 是在第 q 轮数据交换博弈中参与者 P_{-t} 决策之前已完成决策构成的策略组合。

（2）$p^q=\{p_1^q,p_2^q\}$ 是机制根据参与者在第 q 轮数据交换博弈中的策略选择所支付的额外收益集合。其中，p_t^q 表示参与者 P_t 在 q 轮博弈中所获得的额外收益：

$$p_t^q=\begin{cases}\delta*0^+, & \text{if } s_t^q=s_t^{q(1)}\\ \delta*0^-, & \text{if } s_t^q=s_t^{q(2)}\end{cases}$$

其中，$s_t^q\in h_t^q$ 表示参与者 P_t 在第 q 轮真实选择的策略；δ 为惩罚系数。在机制中，用“0^+”表示参与者因遵守协议而获得的优势，用“0^-”表示参与者因偏离协议而失去的优势，“0^+”和“0^-”虽然不会改变博弈的最终收益，但是可以提高或降低参与者在交换过程中的风险。因此，在加入惩罚系数 δ 后，可选择不同的 δ 值来调整惩罚力度，以降低遵守协议参与者的风险，提高偏离协议参与者的风险。

为了方便在交换协议中使用机制 M_{RE}^{δ}，用参数 m_t^n（$m_t^n\geqslant 0$）来表示参与者 $P_t(t\in[1,2])$ 在第 n 轮交换的惩罚值，即 P_t 散失的后手优势。P_t 的惩罚值由 P_{-t} 进行更新，则 P_t 在第 n 轮的更新规则如下：

$$m_t^n=\begin{cases}m_t^{n-1}-e_1*\delta, & \text{if } s_t^n=s_t^{n(1)}\\ m_t^{n-1}+e_2*\delta, & \text{if } s_t^n=s_t^{n(2)}\end{cases}$$

其中，参数 $e_i\in R(i\in\{1,2\})$ 用来控制不同策略的惩罚力度，即在实际应用场景下根据不同需求可以设置惩罚值系数。在协议执行中，每一轮交换均通过比较参与者的惩罚值大小来确定首先发送份额的参与者，由惩罚值较大的参与者首先发送份额，当惩罚值相等时则随机选择。

4.2 FDEP-BR 的设计

有限理性公平数据交换协议（FDEP-BR）由两个阶段组成：初始化阶段和交易阶段。初始阶段完成参数的初始化，交易阶段完成公平交换。

（1）初始化阶段

参与者为 $P=\{P_1,P_2\}$，拥有唯一、公开且不可篡改的身份标识 $\{id_1,id_2\}$，分发者 D 需完成如下初始化操作：

1）P_1 与 P_2、P_1 与 D 以及 P_2 与 D 通过安全的密钥协商协议完成密钥协商：$E_{1,2}$，$E_{1,D}$，E_{2D}。

2）D 随机选取 3 个随机整数 r，h 和 v，满足 $h<v$，并利用公钥密码体制随机生成 $l\times v$ 的密钥对矩阵 $\{(PK_1,SK_1),(PK_2,SK_2),\cdots,(PK_v,SK_v)\}$，满足 $l=poly(k)$，k 为安全参数，保证 $1/l$ 为可忽略的，对于 $\forall i,j\in[1,v]$，$i\neq j$，有 $(PK_i,SK_i)\neq(PK_j,SK_j)$。由公钥构成公钥矩阵 $PK=\{PK_1,PK_2,\cdots,PK_v\}$，将矩阵 PK 每一列中元素的顺序随机打乱构成 PK'，并在公告牌上公开 PK'，l，v。

3）D 选择密钥对矩阵中的私钥构成私钥矩阵 SK（维数为 $l\times v$），并选择随机数对 SK 的后 $v-h$ 列进行替换得到 SK'，满足 $\forall i,j\in[1,v]$，$i\neq j$ 时，有 $SK_i'\neq SK_j'$ 成立。同时，以 SK' 中 $l*v$ 个私钥为常数项构造一次多项式，将参与者的身份标识 $\{id_1,id_2\}$ 分别代入多项式，计算每个参与者的份额矩阵：$S_1=\{S_1^1,S_2^1,\cdots,S_v^1\}$ 和 $S_2=\{S_1^2,S_2^2,\cdots,S_v^2\}$。

4）D 对 S_1，S_2 和 SK' 的每一列向量按相同规则随机重置顺序，形成新的 S_1'，S_2' 和 SK''，然后选择随机数对 SK'' 第 1 列的前 $r_1(r_1<l)$ 个私钥进行替换得到新的 SK'''，使用单向承诺函数 $C(\cdot)$ 计算 S_1'，S_2' 和 SK''' 的承诺信息 $C(s_{i,j}^1\oplus j)$，$C(s_{i,j}^2\oplus j)$ 和 $C(sk_i^j\oplus j)$，从而得到承诺信息矩阵 $C(S_1')$，$C(S_2')$ 和 $C(SK''')$。在公告牌上公开 $C(\cdot)$，$C(S_1')$，$C(S_2')$ 和 $C(SK''')$，将 $E_{t,D}(S_t')$ 发送给 $P_t(t\in[1,2])$，其中 $C(sk_i^j\oplus j)=C(s_{i,j}^1\oplus j)\oplus C(s_{i,j}^2\oplus j)$。

5）P_t 接收到 D 发送的份额矩阵后验证份额矩阵中的份额是否正确，若正确则向 D 发送成功验证消息，否则让 D 重新发送。

6）当 D 接收到两个参与者的验证成功消息后，分别告知两个参与者秘密分发完成，并销毁所有生成的数据，然后退出协议；否则，返回步骤 1）。

在成功执行以上 6 个步骤后参数初始化完成，参与者 P_1 和 P_2 获得各自的份额矩阵和承诺信息，分发者 D 销毁所有生成的数据并退出协议。

（2）交易阶段

假设 P_1 和 P_2 想要交换的电子物品分别为 $item_A$ 和 $item_B$，则 P_1 和 P_2 需执行如下步骤：

1）P_1 和 P_2 从公钥矩阵 PK' 的每一列中协商选择一个公钥，得到 $1\times v$ 维的公钥向量 $pk=\{pk_{l_1}^1,pk_{l_2}^2,\cdots,pk_{l_v}^v\}$。

2）$P_t(t\in[1,2])$ 用公钥向量 pk 加密 $item_t$，得到 $pk(item_t)=\{pk_{l_1}^1(item_t),\cdots,pk_{l_v}^v(item_t)\}$，并向 P_{-t} 发送 $message_t=(P_{-t},desc_{item_t},pk(item_t),\sigma_t)$，其中 $\sigma_t=sig(k_t^{-1},(P_{-t},desc_{item_t},pk(item_t)))$。

3）交换双方接收到对方发送的信息后进入份额交换，假设当前为第 n 轮交换。从公告牌上可以查询 P_1 和 P_2 的惩罚值 m_1^{n-1} 和 m_2^{n-1} 的大小，若相等则随机确定首先发送份额的参与者，否则由惩罚值最大的参与者首先发送份额。假设第 n 轮由参与者 P_t 首先发送份额。

4) P_{-t} 等待接收 P_t 发送的信息 $message_t$，若超时未收到 $message_t$，或使用 $C(\cdot)$ 验证 $C'(s_{i,j}^t \oplus j)) = C(s_{i,j}^t \oplus j))$ 和 $C(sk_i^j \oplus j) = C'(s_{i,j}^1 \oplus j) \oplus C'(s_{i,j}^2 \oplus j)$ 未同时成立，则令 $m_t^n = m_t^{n-1} + e_2 * \delta$，并判断 m_t^n 是否超过 r，若超过则终止协议，未超过则令 $n=n+1$，并返回步骤 3)。如收到 $message_t$ 且验证通过，则发送自己的份额 $s_{i,j}^t$ 信息给 P_{-t}，并令 $m_t^n = m_t^{n-1} - e_1 * \delta$，进入下一步。

5) P_t 等待接收 P_{-t} 发送的信息 $message_{-t}$，若超时未收到 $message_{-t}$，或使用 $C(\cdot)$ 验证 $C'(s_{i,j}^{-t} \oplus j)) = C(s_{i,j}^{-t} \oplus j))$ 和 $C(sk_i^j \oplus j) = C'(s_{i,j}^1 \oplus j) \oplus C'(s_{i,j}^2 \oplus j)$ 未同时成立，则令 $m_{-t}^n = m_{-t}^{n-1} + e_1 * \delta$，并判断 m_{-t}^n 是否超过 r，如超过则终止协议，未超过则令 $n=n+1$，并返回步骤 3)。如收到 $message_{-t}$ 且验证通过，则发送自己的份额 $s_{i,j}^{-t}$ 信息给 P_t，并令 $m_{-t}^n = m_{-t}^{n-1} - e_2 * \delta$，进入下一步。

6) P_t 和 P_{-t} 分别使用 Lagrange 插值法恢复 sk_i^j，并验证 $C'(sk_i^j \oplus j) = C(sk_i^j \oplus j)$ 是否成立，如成立则进入下一步，否则超过协议容忍极限 h，终止协议。

7) P_t 和 P_{-t} 分别使用 sk_i^j 解密 $pk_{l_1}^j$ ($item_A$) 和 $pk_{l_1}^j$ ($item_B$)，如成功则完成交换并终止协议，否则令 $n=n+1$ 并返回步骤 3)。

注：$C'(\cdot)$ 表示交换双方用公式 $C(\cdot)$ 计算得到的承诺信息。

综上所述，协议中参数 r 的意义在于给有限理性参与者一定的犯错机会，使其有机会调整自己的策略，但又不是无限制的；参数 h 的意义在于让参与者更倾向于尽快达成交换，因为越往后交换成功的机会就越小；参数 v 的意义在于协议的总执行次数是固定的常数，即保证协议在有限次执行后能停止，让协议具有时效性；参数 r_1 的意义在于让参与者不会在前 r_1 轮就欺骗成功(可理解为测试轮)，即使前 r_1 轮所有参与者均选择偏离协议，也不会让任何一方遭受损失，且任意一方参与者均不知道参数 r_1 的具体取值；参数 $l = poly(k)$ 选取的意义在于当参与者执行 l 轮交换协议后，保证任意一方遭受损失的概率不超过 $1/l$，是可忽略的，即从概率角度保证遭受损失的概率是可以忽略的。

4.3　协议正确性和公平性分析

下面对 FDEP-BR 的正确性和公平性进行分析。

命题 4　FDEP-BR 具有正确性。

证明：如果参与者 P_t 和 P_{-t} 均诚实遵守协议，则至多在第 $2l$ 轮就能恢复出 $sk_{l_1}^1$ 或 $sk_{l_2}^1$。因为在份额矩阵前 2 列至少有一个正确的私钥，如第 1 列私钥位于 r_1 行之后，则前 2 列有两个正确的私钥，参与者 P_t 可通过以下解密过程获得 P_{-t} 的交易项目：

$$item_{-t} = sk_{l_j}^1(pk_{l_j}^1(item_{-t})), j \in [1,2]$$

因此，协议具有正确性。

命题 5　在 FDEP-BR 的交易阶段协议执行之前，每个参与者能猜对真正子秘密位置的概率为 $1/(e_2\delta l)$，其中 $l = poly(k)$，$e_2\delta$ 为偏离协议的惩罚值。

证明：根据准备阶段协议和交易阶段协议之前的协商过程可知，在准备阶段，协议分发者 D 会给参与者 P_t 发送 $l \times v$ 维的份额矩阵 S_t'，并公布份额承诺信息：$C(S_t')$，$C(S_{-t}')$，$C(S''')$，以及公钥矩阵 PK'。但在此阶段未取定加密公钥向量，故每个参与者均无法确定对应的解密私钥；在交易阶段协议执行之前的协商中，参与者对 $l \times v$ 维公钥矩阵 PK' 的每一列随机选取公钥，从而获得 v 维公钥向量 $pk = \{pk_{l_1}^1, pk_{l_2}^2, \cdots, pk_{l_v}^v\}$。一方面，因私钥矩阵 S''' 的每一列被随机重置，所以参与者 P_t 无法从所选取的加密公钥的具体位置推知私钥的位置，从而也无法推知份额矩阵 S_t' 中真正子秘密的位置；另一方面，虽然参与者 P_t 知道双方的份额承诺信息中矩阵 $C(S_t')$ 和 $C(S_{-t}')$，但是由于承诺函数的单向性，P_t 也无法从份额承诺信息恢复 P_{-t} 的份额矩阵 S_{-t}'。因此，在交换协议未结束前，没有参与者能从份额承诺信息中获得对手的份额信息。

因此，一方面，只需保证 $l \times v$ 维公钥 PK' 和私钥矩阵 S''' 对应位置的随机性；另一方面，对偏离协议的参与者进行惩罚，使其丧失 $e_2\delta$ 轮的“后手优势”，即让参与者在 l 轮交换中至多有 $l/(e_2\delta)$ 次欺骗或偏离协议的机会。因此，参与者 P_t 能成功猜对子秘密在自己份额矩阵 S_t' 中具体位置的概率为 $C_l^{l/e_2\delta}(1/l) = 1/(e_2\delta l)$，由于 $l = poly(k)$，k 为安全参数，$1/l$ 为可忽略函数，因此 $1/(e_2\delta l)$ 也为可忽略函数。综上，结论得证。

命题 6　在 RH 下，机制 M_{RE}^{δ} 是激励相容机制。

证明：假设理性参与者为 P_1 和 P_2，参与者在第 q 轮遵守协议时执行策略 $s_t^{q(1)}$，偏离协议时执行策略 $s_t^{q(2)}$。在任意第 q 轮共享中，不失一般性，假设由 P_t 首先发送份额，而由命题 5 可知，当参与者未获得双方的份额信息时，参与者无法从份额承诺信息矩阵 $C(S_t')$ 和 $C(S_{-t}')$ 中恢复出真正的密钥，且参与者猜对真正密钥在份额矩阵中位置的概率是可忽略的。因此，理性的参与者 P_t 在第 q 轮中选择策略 $s_t^{q(1)}$ 的偏好评估为 (U^- 表示交换双方均未获得秘密)：

$$\nu_t(s_t^{q(1)}) = \begin{cases} U^-, & q = K \\ U^-, & q \neq K \end{cases}$$

其中，K 表示真正密钥隐藏轮。当参与者 P_t 在第 q 轮选择策略 $s_t^{q(2)}$ 时，参与者 P_{-t} 可以通过份额承诺信息检测出参与者 P_t 偏离协议并拒绝发送份额，因此策略 $s_t^{q(2)}$ 的偏好评估为：

$$\nu_t(s_t^{q(2)}) = \begin{cases} U^-, & q = K \\ U^-, & q \neq K \end{cases}$$

又因为当理性参与者 P_t 选择策略 $s_t^{q(1)}$ 和 $s_t^{q(2)}$ 时会收到额外收益：

$$p_t^q = \begin{cases} \delta * 0^+, & \text{if } s_t^q = s_t^{q(1)} \\ \delta * 0^-, & \text{if } s_t^q = s_t^{q(2)} \end{cases}$$

所以，参与者 P_t 的最终收益为：

$$u_t(s_t^{q(1)}) = U^- + \delta * 0^+, u_t(s_t^{q(2)}) = U^- + \delta * 0^-$$

显然，$u_t(s_t^{q(1)}) > u_t(s_t^{q(2)})$，因此参与者 P_t 只会选择遵守协议策略 $s_t^{q(1)}$。故在任意第 q 轮共享中，首先发送份额的参与者总是会选择遵守协议，而最后发送份额的参与者猜对密钥具体轮数的概率也是可忽略的，为了不提高自己的风险，其也会选择遵守协议。当每个参与者在任意 q 轮共享中均遵守协议时，每一轮将随机决定首先发送份额的参与者。因此，此时交换双方将具有相同的最低风险，遵守协议策略成为双方的最优选择，故机制 M_{RE}^{δ} 是激励相容机制。

命题 7 在 RH 下，FDEP-BR 具有理性公平性。

证明：由定理 6 可知，当参与者为理性参与者时，在 FDEP-BR 中的机制 M_{RE}^{δ} 是激励相容机制。显然，当惩罚机制 M_{RE}^{δ} 是激励相容机制时，遵守协议策略组合 $(s_t^{q(1)}, s_{-t}^{q(1)})$ 构成了纳什均衡。因此，FDEP-BR 在理性假设下具有理性公平性。综上，结论得证。

命题 8 FDEP-BR 在非合作攻击下是概率公平的。

证明：FDEP-BR 的交易阶段协议，本质上是理性秘密共享方案的扩展，在 $l\times v$ 维的份额矩阵 S_t' 中，每一列 l 维的份额向量的共享（交换）相当于执行一次理性秘密共享协议，v 个 l 维的份额向量相当于执行了 v 次理性秘密共享，且 v 个 l 维的份额向量之间是相互独立的。因此，只需证明参与者在执行一列 l 维的份额向量的共享在非合作攻击下是公平的。

在 FDEP-BR 中，参与者均知道双方的份额承诺信息矩阵 $C(S_1')$ 和 $C(S_2')$，因此，在交易阶段，协议的任何参与者发送错误份额信息都将会被对方检测到。对于 $i=1,2,\cdots,l$，下面分两种情况来进行证明。

(1)第 i 轮没有参与者发送错误秘密份额。此时显然是公平的，即 $\Pr[A \text{ acquire } item_B \mid B \text{ acquire } item_A]=\Pr[A \text{ acquire } item_B \mid B \text{ acquire } item_A]=1$，对于 $i\in[1,l]$，如果第 i 轮没有参与者采取欺骗行为。

(2)第 i 轮有参与者发送错误秘密份额。根据交易阶段协议可知，没有参与者能共享错误秘密份额而不被检测到。因此，如果协议进行到第 i 轮，意味着前 $i-1$ 轮交换中所有参与者均发送了正确的秘密份额。如果真正子秘密位于第 i 轮以前，则共享已经完成，协议已结束；如果真正子秘密位于第 i 轮或第 i 轮之后，根据命题 5，参与者能欺骗成功的概率不超过 $1/e_2\delta l$，即 $\Pr[A \text{ acquire } item_B \mid B \text{ not acquire } item_A]<\mu(k)$ 且满足 $\Pr[B \text{ acquire } item_A \mid A \text{ not acquire } item_B]<\mu(k)=1/l$，若 $l=poly(k)$，k 为安全参数，则 $1/l$ 和 $1/(e_2\delta l)$ 均为可忽略函数。综上所述，结论得证。

命题 9 FDEP-BR 是有限理性公平的。

证明：由有限理性公平性定义 11 可知，协议是有限理性公平的，如果同时满足：当参与者的理性程度达到理性时，协议具有理性公平；当参与者的理性程度还未达到理性时，协议具有概率公平。命题 7 和命题 8 分别保证了 FDEP-BR 满足以上两条，因此具有有限理性公平性。

4.4 协议协议进行对比与效率分析

本节将 FDEP-BR 与最具代表性的文献[9]中的 Syverson 协议和文献[15]协议进行对比，主要从协议是否具有有限理性公平(Bounded Rational Fairness，BRF)、理性公平(Rational Fairness，RF)和容错性(Fault Tolerance，FT)、协议的轮复杂度(Round Complexity，RC)以及是否能抵抗非合作攻击(Non-Cooperative Attack，NCA)等角度进行对比分析，如表 1 所列。

表 1 协议对比

Table 1 Comparison of protocols

协议	BRF	RF	Fault Tolerance	Round complexity	NCA
文献[9]协议	No	Yes	No	O(1)	No
文献[15]协议	No	Yes	No	O(1)	No
FDEP-BR	Yes	Yes	Yes	$O(l*v)$	Yes

与文献[9,15]中的协议相比，FDEP-BR 具有如下优点：更广泛的适用场景，能适用于有限理性和理性假设下的交换场景；达到有限理性公平，即能在概率意义下保证交换的一方不会因为另一方由于理性不足偏离协议而遭受损失；交换双方在交换过程中对交换消息进行了加密，具有安全性；协议具有容错性，不会因为交换双方少数几次的偏离协议而导致交换失败，而文献[9,15]中的协议不允许在交换过程中任意一方有偏离协议的行为，否则将会导致交换失败。

但是，为了让 FDEP-BR 具备容错性、有限理性公平性，能抵抗 NCA，牺牲了一定效率，协议执行轮数从文献[9,15]中固定的 3 轮增加到至多要执行 $l*v$ 轮，即轮复杂度从 O(1) 增加到了 $O(l*v)$。其中，l 表示交换的份额矩阵行数，v 表示交换的份额矩阵列数。在交换阶段，每个交换参与者需存储 $l\times v$ 维的份额矩阵，而在每一轮交换结束后交换双方通过单向承诺函数 $C(\cdot)$ 计算承诺信息来验证份额的正确性，当验证通过后，使用(2,2)-Shamir 门限秘密共享方案中的恢复函数来计算共享的私钥，故参与者在协议执行中所需的计算量非常小，而所需存储空间的大小与份额矩阵的大小有关。

FDEP-BR 为了保证交换的公平性，一方面使参数 l 的选取满足 $l=poly(k)$，k 为安全参数，$1/l$ 是可忽的；另一方面应用了定义 12 设计的惩罚机制 M_{RE}^{δ} 来约束有限理性参与者的行为，促进其理性进化。因此，FDEP-BR 的公平性与参数 l 和机制 M_{RE}^{δ} 中惩罚值 $e_2\delta$ 的选取有关，参与者非合作攻击(NCA)成功的概率也与 l 和 $e_2\delta$ 的取值有关，满足 $Pr_{NCA}=(1/l)*(l/le_2\delta)=1/(le_2\delta)$。表 2 列出了 l 和 $e_2\delta$ 的部分取值所对应的非合作攻击成功的概率 Pr_{NCA}。

表 2 NCA 成功的概率

Table 2 Probability of successful noncooperative attack

$e_2\delta$	$l=10$	$l=20$	$l=50$	$l=100$	$l=500$
3	0.03	0.017	0.0067	0.0033	0.0007
5	0.02	0.01	0.004	0.002	0.0004
10	0.01	0.005	0.002	0.001	0.0002

由 $Pr_{NCA}=1/(le_2\delta)$ 可知，Pr_{NCA} 与 l 和 $e_2\delta$ 的取值成反比例关系，即 l 和 $e_2\delta$ 取值越大，参与者攻击成功的概率越低，协议就越公平。因此，在实际应用场景中，可根据安全参数 k 来选取 l 和 $e_2\delta$。特别地，当 k 取固定值时，在保证 $e_2\delta<l$ 的条件下，适当降低 l 并增加 $e_2\delta$ 可降低协议的存储复杂度和轮复杂度。

5 FDEP-BR 仿真

5.1 FDEP-BR 建模

FDEP-BR 中参与者 P_1 和 P_2 的理性假设满足 3.1 节中的 5 条假设，使用有限状态自动机模型对 FDEP-BR 交易阶段进行建模。用二元组 $\pi_{Agent}=\langle\Sigma_{Agent},E\rangle$ 来表示 FDEP-BR 模型，其中，E 表示通信环境，Σ_{Agent} 表示有限理性的协议参与者。以参与者 P_1 为例，形式化描述如下：

(1)$\Sigma_{Agent}=\langle Q,X,Y,\delta_{int},\delta_{exp},N,S,W,u,f,F\rangle$。其中，$Q=\{init,sent,receive,verify,recover,end\}$，表示主体内部状态构成的集合。其中，状态 *init* 表示初始化，*sent* 表示发送，*receive* 表示接收，*verify* 表示验证，*recover* 表示恢复，*end* 表

示交协议执行结束。$X=\{In\_P_1\_0, In\_P_1\_1, Out\_P_1\_1\}$,表示参与者 P_1 的外部输入/内部输出集合。$Y=\{init(), sent(), receive(), verify\_s(), verify\_k(), recover(), end()\}$,表示参与者产生的内部事件结合。其中,$verify\_s()$ 事件表示验证对手发送的份额是否正确,$verify\_k()$ 表示验证恢复成功的密钥是否正确。δ_{int} 表示参与者内部状态转移规则,具体如下:$\delta_{int}(init, \wedge, timeout())=(init, init())$;$\delta_{int}(init, \wedge, send())=(send, send())$;$\delta_{int}(send, \wedge, receive())=(receive, receive())$;$\delta_{int}(receive, \wedge, verify\_s())=(verify, verify())$;$\delta_{int}(verify, \wedge, recover())=(recover, recover())$;$\delta_{int}(verify, \wedge, end())=(end, end())$;$\delta_{int}(verify, \wedge, send())=(send, send())$;$\delta_{int}(verify, \wedge, receive())=(receive, receive())$;$\delta_{int}(recover, \wedge, verify\_k())=(verify, verify())$。$\delta_{exp}$ 表示参与者外部状态转移规则,具体如下:$\delta_{exp}(send, In\_A\_1)=(Out\_A\_1)$。$N=\{P_1, P_2\}$,表示参与者集合。$S=[s_1, s_2]$,表示参与者可选策略集,其中 s_1 表示发送份额,s_2 表示不发送份额或发送错误份额;W 表示有限理性博弈主体的知识集;$u: W \rightarrow R$ 表示有限理性参与者的效用函数,即有限理性的参与者只有在一轮博弈结束后才能获知所选策略的收益。$P=[p_1, p_2]$,表示倾向因子集合,其中 p_1 表示参与者选择 s_1 的概率,p_2 表示参与者选择 s_2 的概率。f 为参与者的学习流程,该流程以策略组合为输入,以 3 个动作为输出,输出动作分别为:更新知识集 W、更新倾向因子 P、做出决策。$F=\{init, end\}$,表示终止态。

(2)$E=\langle Timer, R(\pi)\rangle$。其中,$Timer$ 表示一个全局时钟;$R(\pi)$ 表示对博弈 π 的轮计时器。

为了便于给出状态转移规则图,用 q_0 表示观望状态 $init$,q_1 表示发送状态 $sent$,q_2 表示接收状态 $receive$,q_3 表示检验状态 $verify$,q_4 表示恢复状态 $recover$,q_5 表示协议结束状态 end。

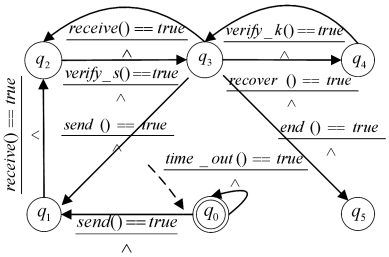

图 1　P_1 的内部状态转移规则

Fig. 1　Internal state transition rule for P_1

5.2　仿真算法

仿真算法是有限理性协议仿真中最为重要的模块,根据 5.1 节对 FDEP-BR 建立的模型,要求仿真算法能真实地描述参与者有限理性学习调整特征(即能真实描述主体内部的状态转移),更强调个体的主体性分析,因此群体层面的学习模型不再适用。针对个体层面,较为经典的学习模型有强化学习模型、信念学习模型和经验加权吸引(EWA)学习模型[23]等,这类学习模型描述的参与者具有一定的认知能力,能够有意识地做出决策。其中,EWA 学习模型是强化学习模型和信念学习模型的结合,同时具备两种学习模型的优势,相比单纯的强化和信念学习模型,其能够更好地描述个体行为。因此,采用 EWA 学习模型来描述 FDEP-BR 中参与者的学习调整过程。

传统的 EWA 学习模型中,参与者在决策时总是选择吸引值最大的策略。为了加强对有限理性特征的刻画,一方面考虑到参与者能根据策略的不同偏好(吸引)做出决策;另一方面考虑参与者决策时可能做出完全随机的选择。因此,引入"突变概率"和"轮盘赌法"对 EWA 学习模型中的决策进行适当改进。假设参与者 i 的策略集为 $s_i=\{s_i^1, \cdots, s_i^n\}$,已知第 t 轮经历权重 $N_i(t)$、吸引 $A_i(t)$、自己选择的策略 $s_i(t)$、对手选择的策略 $s_{-i}(t)$,则参与者 i 可以通过 EWA 学习决策算法得到第 $t+1$ 轮的经历权重 $N_i(t+1)$、吸引 $A_i(t+1)$ 和选择策略 $s_i(t+1)$。EWA 学习决策算法如算法 1 所示。

算法 1　EWA 学习决策算法

输入:$N_i(t)$, $A_i(t)$, $s_i(t)$, $s_{-i}(t)$

输出:$N_i(t+1)$, $A_i(t+1)$, $s_i(t+1)$

Step1　参与者 i 根据第 t 轮的经历加权 $N_i(t)$,计算 t+1 轮的经历加权 $N(t+1)$:

$$N(t+1)=\rho N(t)+1$$

Step2　i 根据第 t 轮的吸引 $A_i(t)$,计算 t+1 轮的吸引 $A_i(t+1)$(其中,$a_i^j(t)\in A_i(t)$ 为策略 s_i^j 的吸引):

$$a_i^j(t+1)=\frac{\varphi N(t) * a_i^j(t)+[\sigma+(1-\sigma)I] * \pi}{N(t+1)}, j\in[1,n]$$

Step3　i 根据策略 s_i^j 的吸引 $a_i^j(t+1)$ 计算选择概率:

$$p_i^j=a_i^j(t+1)/\sum_{k=1}^{n} a_i^k(t+1)$$

Step4　生成介于 0 和 1 之间的随机数:x=Random(0,1),如果 x<MR,则令 $p_i^j=1/n, j\in[1,n]$;

Step5　参与者 i 根据策略的选择概率 p_i^j,按"轮盘赌法"做出决策:

$s_i(t+1)$=Swich(r=Random(0,1)){

$s_i^1: 0\leqslant r<p(s_i^1)$;

$s_i^2: p(s_i^2)\leqslant r<p(s_i^1)+p(s_i^2)$;

⋮

$s_i^n: p(s_i^n)+\cdots+p(s_i^{n-1})\leqslant r<p(s_i^1)+\cdots+p(s_i^n)$;}

算法 1 中,$N_i(t)$ 为参与者 i 的第 t 轮经历加权,表示对过去经历的"等价观测",包括自己选中和未选中的策略;$A_i^j(t)$ 表示 t 轮参与者 i 对策略 s_i^j 的吸引,也可理解为支付;参数 ρ 为经历权重的贴现率;参数 φ 为吸引的贴现率;σ 为未被选中策略支付的权重;$\pi=\pi(s_i^j, s_{-i}(t))$ 为第 t 轮其他参与者选择 $s_{-i}(t)$ 时,参与者 i 选择 s_i^j 的实际支付;$I=I(s_i^j, s_i(t))$ 为示性函数:

$$I(s_i^j, s_i(t))=\begin{cases}1, & s_i^j=s_i(t)\\ 0, & s_i^j\neq s_i(t)\end{cases}$$

参数 $MR\in(0,1)$ 为突变概率,表示参与者随机选择的概率,用于描述参与者决策时犯错或短暂的散失理性。

5.3　FDEP-BR 仿真与结果分析

5.3.1　实验环境介绍

仿真实验是基于 Jade-Repast 集成平台(Jade Repast Integration Platform,JRIP)进行的。在仿真之前,首先在计算机上配置 jdk1.7,并安装开发环境 Eclipse;然后在 Eclipse 上对两种平台进行"选取加"的集成[24],即选取两种平台的优势功能进行集成(Jade 平台具有方便快捷的主体开发优势;Repast J 平台具有宏观仿真进程控制和可视化强的优势)。计算机的 CPU 型号为 Intel(R) Core(TM) i5-3210M,内存为 8 GB,操作系统为 Win7。

5.3.2 仿真参数介绍

在 FDEP-BR 仿真中，可以通过交换双方对于选择发送策略(s_1)的选择概率和吸引的变化来观察参与者的理性进化过程，以此来验证 FDEP-BR 的均衡状态与预期是否具有一致性。首先对 FDEP-BR 的一些必要参数进行设置，如表 3 所列。

表 3 协议参数设置

Table 3 Setting of protocol parameter

参数	N	δ	r_0	l	h	v	(U^+,U,U^-,U^{--})
取值	2	3	3	20	20	23	(7,4,2,0)

表 3 中，N 表示参与协议的人数；δ 表示参与者的惩罚值，即当参与者在某一轮偏离了协议，则将受到 δ 轮首先发送份额的惩罚；l 表示协议执行一次的总交互轮数；h 表示协议的有效执行次数，即若超过 h 还未交换成功则交换失败，满足 $h<v$；v 表示协议的最大执行次数；r_0 为协议的测试轮数，满足 $r_0<l$，即在前 r_0 轮交换双方都选择偏离协议均不会让任意一方遭受损失；U^+ 表示自己选择策略 s_1 而对手选择策略 s_2 时所获得的收益，U 表示双方均选择策略 s_1 时所获得的收益，U^- 表示双方均选择策略 s_2 时所获得的收益，U^{--} 表示自己选择策略 s_2 而对手选择策略 s_1 时所获得的收益。特别注意的是，参数 r_0 和 h 的具体取值对交换参与者均是未知的，且在 3.1 节中的 BRH 下，参与者在交换之前并不知道每个策略的具体收益，只有在每一轮交换结束后才知道自己所选策略的具体收益并完善收益矩阵的信息。

表 3 列出了协议的基本参数取值，惩罚机制 M^{δ}_{RE} 中参数 $e_1=e_2=1$，在进行协议仿真时，采用算法 1 来描述参与者的学习调整行动，则对算法 1 的必要参数进行设置，如表 4 所列，其中参数 ρ，φ 和 σ 的选取满足[23]：$\sigma\approx 0.5$，$\varphi\in(0.8,1)$，$\rho\in(0,\varphi)$。

表 4 算法 1 的参数设置

Table 4 Parameter setting of algorithm 1

参数	$N_1(0)$	$N_2(0)$	ρ	φ	σ	MR
取值	1	1	0.9	0.95	0.5	0.05

综上，根据表 3 和表 4 对 FDEP-BR 模型和算法 1 进行参数设置，并基于 Jade-Repast 集成平台进行程序实现。

5.3.3 实验结果与分析

当交换双方对于策略 s_1 和 s_2 的初始吸引为 $a_i^1(0)=a_i^2(0)=0.5$ 时，启动 FDEP-BR 的仿真模型，通过算法 1 进行学习调整。策略 s_1 的选择概率调整如图 2 所示。

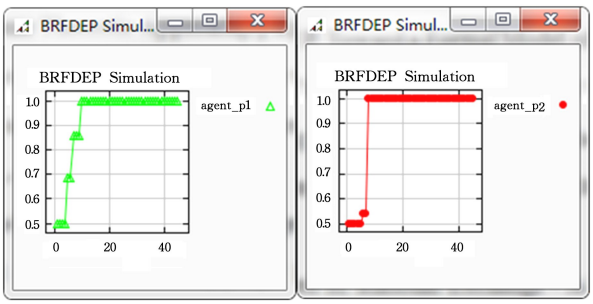

图 2 策略s_1的选择概率调整情况(1)

Fig. 2 Selection probability adjustment(1) for strategy s_1

图 2 中，横轴表示协议执行轮数，纵轴表示选择策略 s_1 的概率。由图 2 可知，参与者 P_1 和 P_2 选择 s_1 的概率均从 0.5 不断变化调整到 1，即交换双方能在交换过程中不断学习进化，最终达到均衡状态选择发送策略 s_1，并在 47 轮达成交换。

当交换双方对于策略 s_1 和 s_2 的初始吸引 $a_i^1(0)=0.1$，$a_i^2(0)=0.9$ 时(即选择 s_1 和 s_2 的概率分别为 $p_1=0.1$，$p_2=0.9$，参与者更倾向于偏离协议)，启动 FDEP-BR，通过算法 1 进行学习调整。策略 s_1 的选择概率调整如图 3 所示。

图 3 策略 s_1 的选择概率调整情况(2)

Fig. 3 Selection probability adjustment(2) for strategy s_1

由图 3 可知，参与者 P_1 和 P_2 选择 s_1 的概率均从 0.1 不断变化调整到 1，并最终在 35 轮达成了交换。

综上，通过仿真表明 FDEP-BR 的均衡结果与预期具有一致性，即参与者 P_1 和 P_2 即使在交换初期更倾向于选择策略 s_2(偏离协议的概率达到 0.9)，但仍然能在交换过程中不断调整自己选择两种策略的概率，使得最终选择策略 s_1 的概率达到 1，并最终达成交换(最终达成交换的具体轮数与关键密钥所在位置有关)。

结束语 针对理性交换协议因使用了理性假设从而在 BRH 下可能失效的问题，文中首次基于 BRH 设计了 FDEP-BR。与理性交换协议相比，FDEP-BR 虽然为了让有限理性的参与者具有学习进化的机会，牺牲了一定的效率(REP 和 FDEP-BR 轮复杂度分别为 O(1)和 O($l*v$))，但是具有更广泛的适用场景，具有有限理性公平性，能抵抗非合作攻击。通过仿真表明，FDEP-BR 的均衡结果与预期具有一致性。本文工作的价值在于首次将公平交换协议的主体假设推进到了有限理性，使基于此假设设计的协议更具有现实性；同时给出一种验证有限理性公平交换协议是否具有“一致性”的验证方法。在 FDEP-BR 中，虽然交换公平性不依赖可信第三方的参与来保证，但在参数生成阶段仍需可信第三方参与生成必要参数，下一步将设计不需要第三方参与的有限理性公平数据交换协议。

参 考 文 献

[1] ASOKAN N. Fairness in electroniccommerce[D]. Waterloo: University of Waterloo, 1998.

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

[3] BUTTYÁN L, HUBAUX J P. Toward a Formal Model of Fair Exchange—a Game Theoretic Approach Technical Report SSC/1999/039[R]. Epfl, 1999: 1-16.

[4] BUTTYÁN L. Removing the financial incentive to cheat inmicro

payment schemes[J]. Electronics Letters，2000，36(2)：132-133.

[5] BUTTYÁN L，JEAN-PIERRE H. Rational Exchange－A Formal Model Based on Game Theory[M]// Electronic Commerce. Berlin：Springer，2001：114-126.

[6] BUTTYÁN L，HUBAUX J P，ČAPKUN S. A Formal Model of Rational Exchange and Its Application to the Analysis of Syverson's Protocol[J]. Journal on Computer Security，2004，12(3-4)：551-587.

[7] BUTTYÁN L，HUBAUX J P，CAPKUN S. A Formal Analysis of Syverson's Rational Exchange Protocol[C]// Computer Security Foundations Workshop(CSFW). IEEE，2002：193.

[8] 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.

[9] 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.

[10] ALCAIDE A，ESTEVEZ-TAPIADOR J M，HERNANDEZ-CASTRO J C，et al. A multi-party rational exchange protocol[C]// Proceedings of Workshops on the Move to Meaningful Internet Systems. Berlin：Springer，2007：42-43.

[11] CAMPOS F A，PHAM V. Rational information exchange model：A new optimization approach for equilibrium computing[C]// Proceedings of the 6th International Conference on Modeling，Simulation，and Applied Optimization. IEEE，2015：1-6.

[12] TAO X，LI G，SUN D，et al. A game-theoretic model and analysis of data exchange protocols for Internet of Things in clouds[J]. Future Generation Computer Systems，2016，76：582-589.

[13] LV Z，PENG C G，LIU H，et al. Rational fairness exchange protocols based on maximum entropy principle[J]. Application Research of Computers，2014，31(2)：563-567. (in Chinese)
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.

[14] LIU H，PENG C G，ZHANG H，et al. Game Logic Formal Model of Rational Secure Protocol[J]. Computer Science，2015，42(9)：118-126. (in Chinese)
刘海，彭长根，张弘，等. 一种理性安全协议的博弈逻辑描述模型[J]. 计算机科学，2015，42(9)：118-126.

[15] NIU C C，PENG C G，LI X. Rational Model of Exchange Protocol and Its Mechanism Design on Fairness[J]. Application Research of Computer，2017，34(5)：1504-1508. (in Chinese)
牛翠翠，彭长根，李新. 一种交换协议的理性模型及其公平机制设计[J]. 计算机应用研究，2017，34(5)：1504-1508.

[16] ZHAO J，WU X H，TAO J. A Rational Exchange Protocol Model Based on Dynamic Game[J]. Computer Applications and Software，2011，28(7)：121-124. (in Chinese)
赵君，吴小红，陶杰. 一种基于动态博弈的理性交换协议模型[J]. 计算机应用与软件，2011，28(7)：121-124.

[17] ZHOU X，JIN J H，LI Y B，et al. Multi-Party Fair Exchange Protocol Based on Rational Secure Sharing[J]. Journal of Information Engineering University，2016，17(6)：705-708. (in Chinese)
周燮，金江浩，李延斌，等. 基于理性秘密共享的多方公平交换协议[J]. 信息工程大学学报，2016，17(6)：705-708.

[18] SIMON H A. A Behavioral Model of Rational Choice[J]. Quarterly Journal of Economics，1955，69(1)：99-118.

[19] ELLSBERG D. Risk，Ambiguity，and the Savage Axioms[J]. Quarterly Journal of Economics，1961，75(4)：643-669.

[20] ALLAIS M，HAGEN O. Expected Utility Hypotheses and the Allais Paradox[J]. Journal of the American Statistical Association，1979，79(385)：224.

[21] HALPERN J，TEAGUE V. Rational secret sharing and multiparty computation：extendedabstract[C]// Thirty-Sixth ACM Symposium on Theory of Computing. ACM，2004：623-632.

[22] TIAN Y，MA J，PENG C，et al. Secret Sharing Scheme with Fairness[C]// IEEE International Conference on Trust，Security and Privacy in Computing and Communications. IEEE，2011：494-500.

[23] CAMERER C，HO T H. Experience-weighted Attraction Learning in Normal Form Games-Camerer-2003-Econometrica - Wiley Online Library[J]. Econometrica，2010，67(4)：827-874.

[24] NI S B. Design and Implementation of Two Kinds of Multi-agent Platform Integration Schemes[D]. Kunming：Yunnan University，2015. (in Chinese)
倪盛斌. 两种多主体平台集成方案的设计与实现[D]. 昆明：云南大学，2015.

(上接第 107 页)

[15] VAN D W，ENGELBRECHT A P. Data clustering using particle swarm optimization[C]// The 2003 Congress on Evolutionary Computation，2003. IEEE，2003(1)：215-220.

[16] KAO Y C，LEE S Y. Combining K-means and particle swarm optimization for dynamic data clustering problems[C]// Proceedings of IEEE International Conference on Intelligent Computing and Intelligent Systems，2009：757-761.

[17] ANIL K J. Data clustering：50 years beyond K-Means[J]. Pattern Recognition Letters，2010，31(8)：651-666.

[18] WENDI B H，ANANTHA P C，HARI B. An application-specific protocol architecture for wireless micro sensor networks[J]. IEEE Trans on Wireless Communications，2002，1(4)：660-670.

[19] MARGI C B，PETKOV V，OBRACZKA K，et al. Characterizing energy consumption in a visual sensor network testbed[C]// International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities(Tridents Com). Barcelona，Spain，2006：335-339.