doi:10.11959/j.issn.1000-436x.2015249

基于马尔可夫决策的理性秘密共享方案

田有亮[1]，王雪梅[2]，刘琳芳[1]
(1. 贵州大学 理学院，贵州 贵阳 550025；2. 贵阳职业技术学院，贵州 贵阳 550023)

摘 要：基于马尔可夫决策理论研究理性密码共享系统模型和秘密重构方法。首先利用马尔可夫决策方法，提出适合于理性秘密共享的系统模型，该模型包括参与者集合、状态集合、风险偏好函数、状态转移函数、回报函数等。在模型中，引入秘密重构中的参与者的风险偏好函数刻画秘密共享模型的状态集合和状态转移函数。其次，基于所提出的系统模型构造相应的理性秘密共享方案，基于马尔可夫策略解决各理性参与者在秘密共享方案中的秘密重构问题。最后对方案进行理论分析证明，给出理性秘密重构方案中折扣因子、回报函数、参与者风险偏好函数间的函数关系，其结果表明所提系统模型方法的合理性和有效性。

关键词：理性秘密共享；马尔可夫决策；博弈论；折扣因子；风险偏好函数
中图分类号：TP309 **文献标识码**：A

Rational secret sharing scheme based on Markov decision

TIAN You-liang[1], WANG Xue-mei[2], LIU Lin-fang[1]
(1. College of Science, Guizhou University, Guiyang 550025, China; 2.Guiyang Vocational and Technical College, Guiyang 550023, China)

Abstract: The reconstruction methods of a rational secret sharing based on the Markov decision was studied. Firstly, a rational secret sharing system model was proposed using the Markov decision process, which included the players set, the states set, the risk preference function, the state transfer function, the return function, etc. The risk preference function was introduced in order to depict the state set and the state transfer function in this model. Secondly, a rational secret sharing scheme was constructed based on the proposed system model, which was able to solve the secret reconstruction problems according to the Markov strategy. Finally, the functional relations of among the discount factor, the return function and the risk preference function was proposed in this scheme. The analysis results show that the proposed model and scheme are rationality and validity.

Key words: rational secret sharing; Markov decision; game theory; discount factor; risk preference function

1 引言

秘密共享是面向多方密码协议的基础和重要工具之一。理性秘密共享是传统密码学和算法博弈论相结合的产物，它有效扩展了传统密码协议的研究领域和应用空间。2004 年，Halpern 和 Teague[1] 首次提出理性秘密共享和安全多方计算协议。

目前，该交叉领域的研究主要包括 2 个方面：一方面是应用秘密协议到博弈论模型中，如应用安全多方计算协议代替博弈均衡模型中的可信仲裁者（trusted mediator），利用安全多方计算协议安全计算各参与者的类型参数[2,3]；另一方面是应用博弈论方法到密码学中，利用博弈模型中的理性假设代替密码学中参与者要么是诚实的要么是恶意的假设[4~11]。Zhang 等[10]用非完美信息的扩展式博弈建模理性秘密共享方案。田有亮等[11]在博弈论框架下

收稿日期：2015-05-18；**修回日期**：2015-08-11
基金项目：国家自然科学基金资助项目（61170280, 61363068,61472310）；中国博士后基金资助项目（2013M530705）；贵州省自然科学基金资助项目（20132112）；贵州大学博士基金资助项目（2012-024），贵州大学青年基金资助项目（201305）
Foundation Items: The National Natural Science Foundation of China (61170280, 61363068,61472310); China Postdoctoral Science Foundation (2013M530705); The Natural Science Foundation of Guizhou Province (20132112); The Doctors Science Foundation of Guizhou University (2012024); The Youth Foundation of Guizhou University (201305)

分析秘密共享体制的分发机制和重构机制，并给出相应的解决方案；田有亮等[11]也基于贝叶斯博弈研究一次秘密共享问题，解决该类理性秘密共享体制的合作问题[12]；2013 年，Tian 等[13]基于博弈论框架，研究安全通信协议问题；最近，Tian 等[13]从贝叶斯理性的角度提出贝叶斯理性秘密共享[14]。此外，国内学者也越来越重视这方面的研究[15~18]。

可见，理性秘密共享的研究已经引起密码学领域的重视，并且已经取得一些研究成果，但是，相关研究还有待进一步深入。从所引文献来看，应用博弈论方法来研究秘密共享问题，未能很好解决在秘密重构中理性参与者的自利行为所导致各参与者最终退出重构协议，无论是基于惩罚策略的还是其他方法，均一定程度上存在该问题。

本文针对该问题，利用马尔可夫决策方法，构建理性秘密共享模型。在模型中，引入理性参与者的风险偏好函数，探究各参与者的个人风险偏好对秘密重构结果的影响。在理性秘密共享方案的构造过程中，根据参与者个人风险偏好函数，结合马尔可夫决策状态转移函数决定自己每轮行动；尤为重要的是，在整个协议重构阶段，一旦参与者参加执行协议，那么随着执行轮数的增加，参与者的最佳选择是继续合作，直到协议成功结束；否则他将损失更大。基于这些方法，本文有效地解决在理性秘密共享方案中因个人自利行为而导致各参与者合作失败的问题。

2　准备知识

本节介绍理性秘密共享和马尔可夫决策。

2.1　理性秘密共享

理性秘密共享是为了在 n 位理性参与者(记为 P)间实现秘密共享任务。准确地说，每位参与者 $P_i \in P$ 有一个效用函数 $u_i : \{0,1\}^n \to R$ ，R 代表秘密重构的所有可能结果。向量 $O:(o_1,\cdots, o_n)\in\{0,1\}^n$ 记为秘密重构的一个结果，这里 $o_i=1$ 当且仅当 P_i 最终得到共享秘密。为了简单，这里选取大家广泛采用的效用函数假设。即对 $1\leqslant i\leqslant n$，P_i 的效用函数 u_i 满足：

1) 对任意的 $O,O'\in\{0,1\}^n$，若 $o_i>o_i'$ 则 $u_i(O)>u_i(O')$；

2) 如果 $o_i=o_i'$ 和 $\sum_{i=1}^n o_i=\sum_{i=1}^n o_i'$，则 $u_i(O)>u_i(O')$。

上述 2 个条件表明：首先，P_i 总是希望只有自己知道共享秘密；其次，知道共享秘密的参与者越少越好。为了便于描述，用结果向量 O 来表示这 4 种情况下的收益：①$u_i=U^+$，表示 P_i 得到共享秘密而 $P_j(j\neq i)$ 没有得到；②$u_i=U$ 表示 P_i 和 P_j 都得到共享秘密；③$u_i=U^-$ 表示 P_i 和 P_j 都未得到共享秘密；④$u_i=U^{--}$ 表示只有 P_i 未得到共享秘密。根据效用函数的定义有 $U^+>U>U^->U^{--}$。用策略 C 表示参与者合作(广播秘密份额)，策略 D 表示参与者不合作(什么都不广播)。这里存在一个类似于囚徒困境问题：对于每位参与者来说，策略 C 弱优于策略 D，从而导致理性秘密共享博弈个参与者都选择不合作，导致秘密分享失败。

2.2　马尔可夫决策

马尔可夫决策过程最基本的模型是一个四元组（S, A, T, R）。

1) 状态集合 S：问题所有可能状态的集合。

2) 行动集合 A：问题所有可能行动的集合。

3) 状态转移函数 $T: S\times A\times S'\to[0,1]$, 用 $T(s, a, s')$ 来表示在状态 s，执行动作 a，而转移到状态 s'的概率 $P(s'|s,a)$。

4) 报酬函数 $R:S\times A\to R$：用 $R(s, a)$来表示在状态 s 执行动作 a 所能得到的立即报酬。

为了便于在后面建立、分析理性秘密共享的马尔可夫决策系统模型，对马尔可夫决策模型的几点说明。

1) 本文所述的马尔可夫模型讨论离散参数的情况，包括时间、状态及行动的参数等。

2) 模型中的状态是对于在某一时间点对该系统的描述，以 S_1, S_2, S_3, …这样的方式表示，标号状态的数目代表状态空间的大小。在所建立的系统模型中，用概率方法来处理各参与者对自己所处状态的推断。

3) 在建立的秘密共享系统模型中，各参与者的行动将参与改变当前所处的状态。当某一行动被某参与者执行，各参与者当前所处的状态将根据一定概率发生改变，转换为另一状态，其概率分布与所执行的行动有关。这里讨论的是时齐马尔可夫过程，即所有行动的执行时间是相同的，状态转移的时间间隔一致。

4) 从状态集合到动作集合的一个映射 $\pi: S\to A$，它代表决策问题的解，称之为策略。求解策

略问题的过程是参与者根据当前所处状态 s，然后执行策略对应的行动 $\pi(s)$，并根据状态转移函数进入下一状态，重复此过程直到问题结束。在每步决策中用该策略所能获得的长期期望回报来评价其优劣。

3 系统模型

在本系统中不考虑秘密分发阶段秘密分发者与各参与者间的交互、决策问题。在模型中假设密秘共享方案中秘密共享分发阶段已结束，各参与者 $P_i \in P$（P 为参与者集合）拥有子秘密 sk_i，其中，满足一定存储结构的参与者集合一起能够重构出其共享的秘密 sk。本节结合秘密共享体制和马尔可夫决策理论，建立理性秘密共享的马尔可夫系统模型，为后面的方案构造和分析提供理论模型依据。

图 1 描述的是在马尔可夫决策模型下，各协议参与者互相交互的过程。参与者 P_i 根据当前的状态，执行行动（合作 C 或不合作 D），依据协议的状态获得此次行动的收益，以及所处新的当前状态。

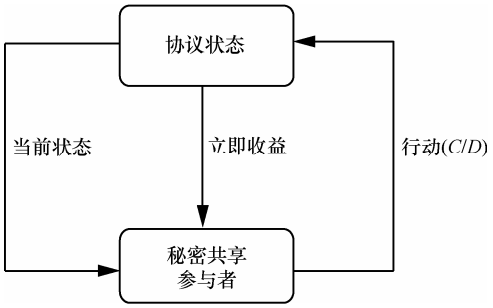


图 1　理性秘密共享马尔可夫决策模型

理性秘密共享的马尔可夫决策模型是一个六元组（P, RP, S, A, T, R）。

1) 参与者集合 P：参与执行秘密重构的参与者集合，记作 $P=\{P_1,\cdots,P_n\}$。

2) 参与者风险偏好 RP：指参与者在理性秘密共享重构的不同状态下所能承担的风险程度。

3) 状态集合 S：秘密共享决策过程中所有可能状态的集合。

4) 行动集合 A：秘密共享决策过程中各参与者可能采取的所有行动集合。

5) 状态转移函数 $T: S\times A\times S'\to[0,1]$，用 $T(s, a, s')$ 来表示在状态 s，执行动作 a，而转移到状态 s'的概率 $P(s' \mid s, a)$。

6) 报酬函数 $R: S\times A\to\{r \mid r \in \alpha U^{++}+\beta U+\gamma U^{-}+\eta U^{--}: \alpha\geqslant 0, \beta\geqslant 0, \gamma\geqslant 0, \eta\geqslant 0, \alpha+\beta+\gamma+\eta=1\}$ 用 $R(s, a)$ 来表示在状态 s 执行动作 a 所能得到的立即报酬。

下面进一步详细说明理性秘密共享的马尔可夫决策模型参数。

3.1 参与者

参与者集合是由参加秘密重构时的各位参与者组成，这些参与者集合满足某种存取结构时才能正确重构共享秘密。

设 $P=\{P_1,\cdots,P_n\}$ 满足 $\varnothing\neq AS\subseteq 2^P$，称 AS 是 P 上的存取结构，如果集合 AS 满足单调性：若 $B\in AS$，则对 $\forall B'\in 2^P$ 和 $B\subseteq B'$，有 $B'\in AS$。若 AS 是 P 上的存取结构，则 AS 中的任何集合称为 P 上的授权集，简称授权集；对于 $2^P\setminus AS$ 中的任何集合，称为 P 上的非授权集，简称非授权集。

令 $AS_m=\{B\in AS \mid \forall B'\subseteq B\Rightarrow B'\notin AS\}$，称 AS_m 为 AS 的极小存取结构，AS_m 中的元素称为极小授权集。在 (t,n) 门限秘密方案中，极小存取结构 $AS_m=\{B\in P \| B|=t\}$。

经如上分析，理性秘密共享的马尔可夫决策模型中一个有效的参与者集合 B 应该满足

$$AS_m\subseteq B\subseteq AS \tag{1}$$

否则，对于参与者集合 $B\subset AS_m$ 是无效的，因无论各参与者采取何种策略，都不可能重构出正确的共享秘密。

3.2 风险偏好

在理性秘密共享中，因个体间的差异性和特殊性，各位参与者对协议结果的认同度不同，对风险的承担程度也会存在较大差异，同时对同一协议的同一个结果也存在差异。在理性秘密共享的马尔可夫决策模型中引入参与者偏好就是考虑到个体间的差异性而引入的。

另一方面，在理性秘密共享协议的不同状态下各参与者所面临的“风险”（这里的风险可考虑为出现在自己没有得到秘密的情况下对手获得共享秘密的概率）是不一样的，而且随着协议交互轮数的增加（在每轮的获得正确子秘密的情况下），参与者得到正确共享秘密的“风险”在逐渐降低。此时他们采取冒险行动将得不偿失，即当协议顺利运行到一定阶段后，各参与者此时只有坚持继续合作下去才是最佳选择，否则必将有损失。

基于以上分析，设参与者 $P_i\in P$ 的风险偏好为 $\delta_i\in[0,1]$，如图 2 所示。在协议执行到某 l 轮时，

其风险偏好可表示为参与者初始偏好 δ_i 和当前所处状态 S_l 的函数

$$RP: f_i(\delta_i, S_l) \to (0,1) \tag{2}$$

其中，$f_i(\delta_i, S_0) = \delta_i$。

从另外一个角度来看，参与者 $P_i \in P$ 在状态 S_j 下的风险偏好就是在该轮 P_i 采取不合作的概率。在图 2 中，显示参与者 P_i 越到接近协议执行结束阶段，选择去背叛冒险的风险偏好越低。

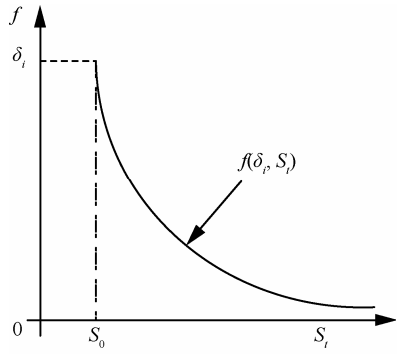


图 2　参与者 P_i 风险偏好函数

3.3　状态集合

在理性秘密共享马尔可夫决策模型中，其状态集合可分为 3 类，如图 3 所示。一类是初始状态，记为 $S_{\text{start}} = \{S_0\}$；一类是中间状态，记为 S_{middle}；最后一类是结束状态，记为 S_{over}。状态集合 $S = S_{\text{start}} \cup S_{\text{middle}} \cup S_{\text{over}}$，并且 S 是有限集合，集合元素的个数由协议交互的轮数所决定。协议从开始状态执行，然后经历中间状态，最后在某个结束状态。

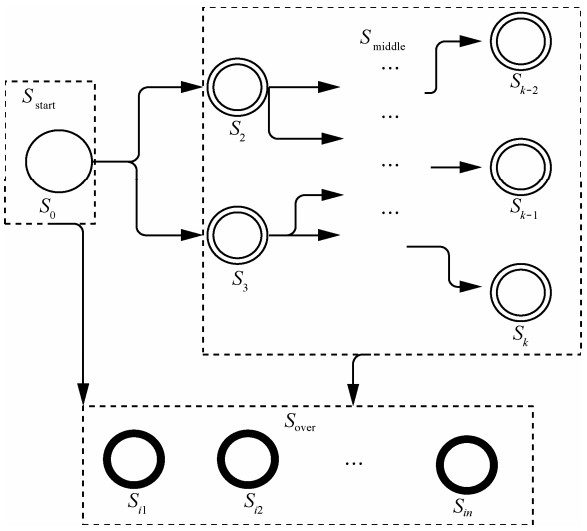


图 3　理性秘密共享模型状态

在密码协议执行过程中，各协议参与方主要采取合作或者欺诈方式交替执行协议的行动，秘密共享协议也不例外。但是，在理性秘密共享协议中，各参与者对当前所处的状态具有不确定性。在理性秘密共享系统模型中引入随机变量 $S_X \in S$，变量 S_X 不是由系统模型中未来的状态决定，而是受到过去的状态所影响，如图 4 所示。

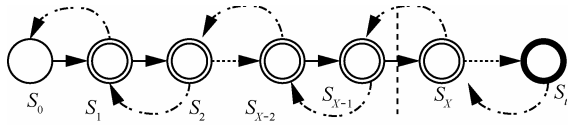


图 4　理性秘密共享状态马尔可夫链

图 4 表示随机动态的理性秘密共享系统，图中每个节点表示理性秘密共享协议运行在某一时刻所处的状态，即秘密共享协议执行到某一轮的情况。假设在系统所处的每一个状态均只与过去的有限个状态有关系，即这些状态间体现马尔可夫性质，形成马尔可夫链。也就是说对于随机变量 S_X，有

$$\Pr(S_X \mid S_0, \cdots, S_{X-1}) = \Pr(S_X \mid S_{X-1}) \tag{3}$$

3.4　行动

各参与者的行动会改变当前秘密共享系统当前的状态。在每一个状态 $S_j \notin S_{\text{over}}$ 下，参与者的行动集会有(*C*,*D*)，当有参与者执行 *D* 行动，则系统状态将转移到某个结束状态，如图 5 所示。在理性秘密共享协议中假定所有行动执行时间是相同的，状态转移的时间间隔是一致的，即该理性秘密共享模型所讨论的是时齐次马尔可夫过程。

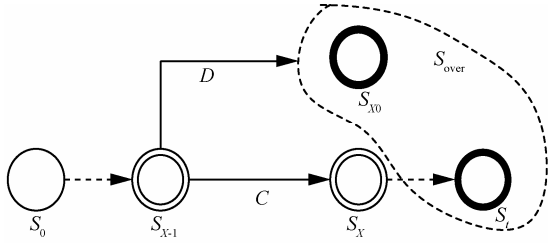


图 5　理性秘密共享模型行动

用 C_l=(C_1,⋯,C_n)表示在状态 S_l 各参与者均采取行动 *C* 的向量；C_l'=(C_1,⋯,D_i,⋯,C_n)表示在状态 S_l 至少存在一位参与者采取行动 *D* 的向量。

3.5　状态转移函数

状态转移函数描述的是理性秘密共享各参与者间在每个状态上所选择各种行动的可能性，它体现的是秘密共享系统的动态特性。这里考虑随机情形下的状态转移函数：$T: S \times A \to \Pr(S)$。用

$\Pr(S_j \mid S_i, a)$ 表示在秘密共享系统某个状态 S_i 下执行某一行动 a 的概率分布，记为 $T^a(S_i, S_j)$。

图 6 显示在理性秘密共享的马尔可夫决策模型中，对某一给定行动下系统各状态间的概率转移情况，比如在开始状态 S_0，参与者 $P_i \in P$ 的风险偏好是 δ_i，则各参与者都选择合作行动 C 的概率为 $\prod_{i=1}^{|P|}(1-\delta_i)$，存在某位参与者背叛的概率是 $\prod_{j=1,j\neq i}^{|P|}(1-\delta_j)f_i(\delta_i, S_0)$。因此有

$$T^{C_1}(S_0, S_1) = \prod_{i=1}^{|P|}(1-\delta_i) \tag{4}$$

$$T^{C_2'}(S_0, S_{10})\prod_{j=1,\mathrm{j}\neq \mathrm{i}}^{|P|}(1-\delta_j)f_i(\delta_i, S_0) \tag{5}$$

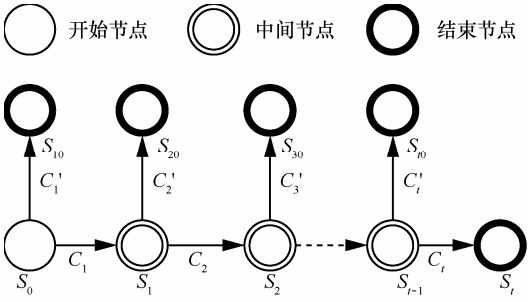


图 6 理性秘密共享模型的状态转移

在理性秘密共享系统模型中，因各状态间的依赖关系满足马尔可夫链，而且每个状态仅与其前面的一个状态存在依赖关系，初始状态仅与各参与者的初始风险偏好 δ_i 有关。因此，对于任意状态 $S_i \in S \setminus S_{\text{start}}$，其状态转移关系如下

$$T^{C_1}(S_i, S_{i+1}) = \prod_{j=1}^{|P|}(1-f_j(\delta_j, S_i)) \tag{6}$$

$$T^{C_1'}(S_i, S_{i0}) = \prod_{j=1,k\neq j}^{|P|}(1-f_j(\delta_j, S_i))f_k(\delta_k, S_i) \tag{7}$$

3.6 策略和值函数

和其他马尔可夫决策问题一样，在该系统模型中也用策略来代表理性秘密共享决策问题的解。定义策略是状态集合到行动集合的一个映射

$$\pi : S \to A \tag{8}$$

理性秘密共享系统模型求解的过程是各参与者根据自己当前的状态执行相应的行动 π，并加入下一状态，重复此过程直到状态转移到某个结束节点。

虽然模型的状态是有限的，但为了很好地刻画参与者的风险偏好随着系统的运行，他们的风险偏好越来越小的性质，类似于无限阶段决策问题中希望总报酬最优的处理方式，在系统中引入一个折扣因子 λ (0 < λ <1)，则参与者在某状态下选择行动所得到的报酬可表示为其数学期望的形式

$$\max \mathrm{E}\left[\lambda^t \sum R_t\right]$$

下面定义系统模型的值函数。

值函数 $V^\pi : S \to \mathbb{R}$，表示参与者在状态 S_t 选择策略 π 的期望回报，有

$$V^\pi(S_t) = \mathrm{E}\left[\sum_{t=0}^{\infty}\lambda^t R(S_t, \pi(S_t))\right] \tag{9}$$

以递归的形式表示有

$$V^\pi(S_t) = R(S_0, \pi(S_{t0})) + \lambda \sum_{S_l \in S} T^{\pi(S_t)}(S_t, S_l)V^\pi(S_l) \tag{10}$$

4 方案构造

本节基于上述理性秘密共享模型，构造理性秘密共享方案。在构造过程中，重点考虑方案满足 2 个条件：一是在方案中，每位参与者根据自己的风险偏好决定自己的初始行动；二是一旦参与者参加执行协议，那么随着执行轮数的增加，参与者的最佳选择是继续合作，直到协议成功结束；否则他将损失更大。所构造的方案分为准备阶段、分发阶段和重构阶段。

4.1 准备阶段

首先假设协议中有一位诚实可靠的秘密分发者（记为 P_0）想在参与者 $P=\{P_1,\cdots,P_n\}$ 间分享秘密 $sk \in Z_q^*$，其中，Z_q^* 是一素数阶为 q 的乘法群。

本阶段秘密分发者先公布报酬函数中参数 U^+、U、U^-、U^{--}的值，与参与者一起协商并公布相应的折旧系数 λ。每位参与者 P_i 的初始风险偏好 δ_i 是保密的，只有 P_i 自己知道，但各位参与者的风险偏好函数 RP：$f_i(\delta_i, S_l) \to (0,1)$ 是大家的共同知识，其性质如图 2 所示。

对于他人来说，参与者 P_i 的初始风险偏好 δ_i 是秘密信息，所以其折旧系数 λ 和轮数 l 协商均可采用求解相应问题的安全多方计算协议实现。

4.2 分发阶段

为在参与者间共享秘密 $sk \in Z_q^*$，秘密分发者 P_0 执行如下操作。

Step1 P_0 随机选取 $v = \mathrm{poly}(k) \in Z_q^*$，$k$ 是安全参数。

Step2 P_0 随机选取 sk_i，使 $sk=sk_1+sk_2+\cdots+sk_n$，$sk_i=sk_{i1}sk_{i2}\cdots sk_{iv}$，其中，$i$=1,2,$\cdots$,$n$。

Step3 P_0 计算系列秘密消息的认证码(mac(·)是消息认证函数)。

M_1=mac(sk)，M_1=mac(sk_1)，M_2=mac(sk_2)，…，M_n=mac(sk_n)；

M_{11}=mac(sk_{11})，M_{12}=mac(sk_{12})，…，M_{1v}=mac(sk_{1v})；M_{21}=mac(sk_{21})，M_{22}=mac(sk_{22})，…，M_{2v}=mac(sk_{2v})，…，M_{n1}=mac(sk_{n1})，M_{n2}=mac(sk_{n2})，…，M_{nv}=mac(sk_{nv})。

Step4　P_0 公布 $M_0,M_1,\cdots,M_n,M_{12},\cdots,M_{1v},\cdots,M_{n1}$，…，$M_{nv}$。

Step5　P_0 秘密发送 $sk_i=sk_{i1}sk_{i2}\cdots sk_{iv}$ 给 P_i(其中，i=1,2,…,n)。

4.3　重构阶段

Step1　当参与者 P_i 收到 $sk_i=sk_{i1}sk_{i2}\cdots sk_{iv}$，通过计算其 mac(·)函数，验证其消息认证码 M_i, M_{i1},…, M_{iv}(i=1,2,…,n)

$$M_i=\text{mac}(sk_i),\quad M_{ij}=\text{mac}(sk_{ij})$$

其中，j=1,2,…,v。

若通过验证，则继续；否则，选择行动 D。

Step2　（第 1 轮）参与者 P_i 计算 $\dfrac{U}{U^+}>\dfrac{\delta_i}{1-\delta_i}$ 和 $\dfrac{U^-}{U}>\dfrac{1-\delta_i}{\delta_i}$，则参与者 P_i 选择执行行动 C，即选择合作，给其他参与者 $P_{-i}\left(\dfrac{P}{P_i}\right)$ 秘密发送 sk_{i1}，转到 Step3；否则选择行动 D，退出协议。

Step3　（第 2 至 v 轮，记为第 j 轮）参与者 P_i 执行如下操作。

1) 如果 $M_{k(j-1)}$=mac($sk_{k(j-1)}$)成立(其中 $P_k\in P_{-i}$)，则转至 2)；否则选择行动 D。

2) 如果 $\dfrac{U}{U^+}>\dfrac{f_i(\delta_i,S_j)}{1-f_i(\delta_i,S_j)}$ 和 $\dfrac{U^-}{U}>\dfrac{1-f_i(\delta_i,S_j)}{f_i(\delta_i,S_j)}$，则给参与者 P_i 选择行动 C，秘密发送 sk_{ij} 给 P_{-i}；否则否则选择行动 D。

3) 继续重复第 2)、3）步至第 v 轮。

Step4　协议结束，退出。

5　方案分析

命题 1　在上述协议重构阶段第一轮，理性参与者 P_i 将选择相互合作（即选择行动 C），如果 $\dfrac{U}{U^+}>\dfrac{\delta_i}{1-\delta_i}$ 和 $\dfrac{U^-}{U}>\dfrac{1-\delta_i}{\delta_i}$。

证明　在协议重构阶段，协议第一轮（Step2）理性参与者 P_i 选择合作行动 C 的条件是：任何背叛行动，均不可能使其获得更大的回报。根据状态转移函数 $T^{C_1}(S_0,S_1)$ 和 $T^{C_1'}(S_0,S_{10})$，这就要求如下 2 种情况发生。

1) 对于任何理性参与者 P_i 来说，选择背叛的风险回报小于合作的回报，即式(11)成立。

在这种情况下仅假设存在 P_i 可能选择背叛行动，不考虑有多个参与者选择背叛的情形，因为对于 P_i 来说，只有他一人选择背叛时的收益 U^- 要高于还有其他参与者背叛的回报 U^{--}，因 $U^->U^{--}$

$$T^{C_1}(S_0,S_1)U>T^{C_1'}(S_0,S_{10})U^+ \tag{11}$$

根据式(4)和式(5)有

$$\prod_{i=1}^{|P|}(1-\delta_i)U>\prod_{j=1,j\neq i}^{|P|}(1-\delta_j)f_i(\delta_i,S_0)U^+$$

于是可得

$$\frac{U}{U^+}>\frac{\delta_i}{1-f_i(\delta_i,S_0)}=\frac{\delta_i}{1-\delta_i}$$

2) 对于任何理性参与者来说，大家选择背叛的回报小于合作的回报，即式(12)成立。同情况 1）的分析，这里也只考虑参与者背叛的情形。

$$\prod_{i=1}^{|P|}(1-\delta_i)U>\prod_{j=1}^{|P|}\delta_jU^- \tag{12}$$

由此可得

$$\frac{U^-}{U}>\frac{1-\delta_i}{\delta_i}$$

综合 1）和 2），命题得证！

命题 2　在上述协议重构阶段第二轮至协议结束前，各理性参与者将选择继续相互合作（即选择行动 C），如果 $\dfrac{U}{U^+}>\dfrac{f_i(\delta_i,S_j)}{1-f_i(\delta_i,S_j)}$ 和 $\dfrac{U^-}{U}>\dfrac{1-f_i(\delta_i,S_j)}{f_i(\delta_i,S_j)}$。

证明　根据重构协议第二轮（Step3）后的某 l 轮，理性参与者选择行动 C 的条件是情况 1）和情况 2）成立。

1) 对于任何理性参与者 P_i 来说，选择背叛的风险回报小于合作的回报，即式（13）成立。

$$T^{C_1}(S_i,S_{i+1})U>T^{C_1'}(S_i,S_{i0})U^+ \tag{13}$$

根据式(6)和式(7)有

$$\prod_{i=1}^{|P|}(1-f_i(\delta_i,S_l))U>\prod_{j=1,j\neq i}^{|P|}(1-f_i(\delta_j,S_l))f_i(\delta_i,S_1)U^+$$

由此可得

$$\frac{U}{U^+}>\frac{f_i(\delta_i,S_j)}{1-f_i(\delta_i,S_j)}$$

2) 对于任何理性参与者来说，大家选择背叛的回报小于合作的回报，即式(14)成立。

$$\prod_{i=1}^{|P|}(1-f_i(\delta_i,S_l))U>\prod_{i=1}^{|P|}f_i(\delta_i,S_j)U^- \quad (14)$$

于是可得

$$\frac{U^-}{U}>\frac{1-f_i(\delta_i,S_j)}{f_i(\delta_i,S_j)}$$

综合 1)和 2)，命题得证！

定理 1 在上述协议的重构协议过程中，如果 $v>\log\lambda\frac{f_i(\delta_i,S_j)U^+}{(1-f_i(\delta_i,S_j))U}$，则每位理性参与者在最后一轮（第 v 轮）将继续选择合作，此时其报酬为 λ^vU，其中，λ 是折扣因子，v 是协议执行轮数。

证明 根据命题 1 和命题 2 可有 $\frac{U}{U^+}>\frac{f_i(\delta_i,S_j)}{1-f_i(\delta_i,S_j)}$ 成立。下面关键证明在协议重构阶段的最后一轮，即第 v 轮各理性的参与者还继续选择合作，根据命题 1 和命题 2 可知，在非最后一轮，从回报函数的设置来说，只要满足命题 1 和命题 2 的条件，各理性的参与者将选择合作。

在最后一轮，在个人风险函数对其回报的影响下，来分析参与者回报与折扣因子的影响。对于理性参与者 P_i，其最后一轮选择继续合作要要求式(15)成立。

$$\sum_l^v\lambda^lf_l(\delta_i,S_l)U>\sum_l^{v-1}\lambda^lf_l(\delta_i,S_l)U+U^+ \quad (15)$$

由此可得

$$v>\log\lambda\frac{f_i(\delta_i,S_j)U^+}{(1-f_i(\delta_i,S_j))U}$$

此时，各理性参与者将在整个重构过程中选择合作到底，根据式(9)可知，其各参与者的回报为 λ^vU 。证毕！

由定理 1 可以看出，在基于马尔可夫决策方法的理性秘密共享方案中，各参与者在当前选择是否合作，与协议执行的前面有限步有关，见 3.5 节的状态转移函数。其协议的最后一步是否合作，与参与者的风险偏好函数、折扣因子和协议执行的轮数有关。其详细数量关系为定理 1 的结论，即

$$v>\log\lambda\frac{f_i(\delta_i,S_j)U^+}{(1-f_i(\delta_i,S_j))U}$$

另外，在协议效率方面，分别选取文献[10,11,13,14]中的方案进行对比分析，如表 1 所示，其中，k 表示方案中的安全参数，n 表示协议中参与者人数，L 表示协议中执行惩罚策略的次数。

表 1 方案效率对比分析

方案	安全基础	通信轮数	规则	均衡结果
文献[10]	消息认证码	L 足够大	惩罚策略	序贯均衡
文献[11]	单向函数	n+1	惩罚策略	纳什均衡
文献[13]	签密算法	常数轮	效用最大	纳什均衡
文献[14]	签密算法	Poly(k)	贝叶斯规则	贝叶斯均衡
本文	消息认证码	Poly(k)	状态转移函数	马尔可夫均衡

从表 1 可以看出，本文的方案在安全性上依赖于消息认证码的安全性，其通信轮数为 Poly(k)，与文献[14]中方案通信复杂度相当，在应用中略高于文献[11]和文献[13]的通信轮数。在各参与者策略选择和执行规则上，该方案依据马尔可夫模型中的状态转移函数进行转移和决策，其规则依赖于马尔可夫规则。与文献[10]和文献[11]不同，其需要执行处罚策略。特别在文献[10]中，其方案因其惩罚策略的执行而增加通信复杂度，结果是仅当其惩罚函数被执行足够大轮数时，才能保证其序贯均衡。在协议结果上，与文献[10,11,13,14]相比较，本文方案能达到更强的马尔可夫均衡，该方案对理性秘密共享的均衡进一步精炼，使协议更能满足一些特殊应用（网上拍卖、竞标、电子选举等）需求，特别是在当前云计算、大数据背景下将有更好的应用需求。

6 结束语

本文基于马尔可夫决策建模理性秘密共享。首先介绍理性秘密共享和马尔可夫决策；其次，基于马尔可夫决策方法，建立理性秘密共享系统模型；再次，基于马尔可夫决策和消息认证码，构造理性秘密共享方案；最后，对给出的所构造的理性秘密共享进行分析，给出了在所构建秘密共享方案中各理性参与者选择互相合作的条件。此外，本文提出的方法也能推广运用到理性安全多方计算等多方应用场景，这也是下一步将研究的问题。

参考文献：

[1] HALPEN J, TEAGUE V. Rational secret sharing and multiparty computation: extended abstract[A]. Proc of the 36th annual ACM Symposium on Theory of Computing[C]. New York, 2004. 623-632.

[2] FISCHERR M, WRIGHT R. An application of game-theoretic techniques to cryptography[EB/OL]. http://www.cs.rutgers. edu/~rwright1/Publications/dim93.ps, 2011.

[3] DODIS Y, HALEVI S, RABIN T. A cryptographic solution to a game theoretic problem[A]. Proc of CRYPTO2000[C]. Heidelberg, Springer, 2000. 112-131.

[4] GORDON S D, KATZ J. Rational secret sharing, revisited[A]. Proc of SCN 2006[C]. Heidelberg: Springer, 2006. 229-241.

[5] ABRAHAM I, DOLEV D, GONEN R, *et al*. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation[A]. Proc of the 25th Annual ACM Symp on Principles of Distributed Computing[C]. New York, 2006. 53-62.

[6] LYSYANSKAYA A, TRIANDOPOULOS N. Rationality and adversarial behaviour in multi-party computation(extended abstract)[A]. Proc of CRYPTO2006[C]. Heidelberg, Springer, 2006.180-197.

[7] MALEKA S, AMJED S，PANDU R C. The deterministic protocol for rational secret sharing[A]. Proc of IEEE Int Parallel and Distributed Processing Symp[C]. Piscataway, NJ,2008. 1-7.

[8] MALEKA S, AMJED S, PANDU R C. Rational secret sharing with repeated games[A]. Proc of Information Security Practice and Experience[C]. Berlin, Springer, 2008. 334-346.

[9] ASHAROY G, LINDELL Y. Utility dependence in correct and fair rational secret sharing[A]. Proc of CRYPTO2009[C]. Heidelberg, Springer, 2009. 559-576.

[10] ZHANG Z F, LIU M L. Rational secret sharing as extensive games[J]. Science China Information Sciences, 2013, 56(3): 1-13.

[11] 田有亮, 马建峰, 彭长根, 等. 秘密共享体制的博弈论分析[J]. 电子学报, 2011, 39 (12): 2790-2795.
TIAN Y L, MA J F, PENG C G, *et al*. Game-theoretic analysis for the secret sharing scheme[J]. Acta Electronica Sinica, 2011,39(12): 2790-2795.

[12] TIAN Y L, MA J F, PENG C G, *et al*. One-time rational secret sharing scheme based on Bayesian game [J]. Wuhan University Journal of Nature Science, 2011, 16(5): 430-434.

[13] TIAN Y L, MA J F, PENG C G, *et al*. A rational framework for secure communication[J]. Information Sciences, 2013, 250: 215-226.

[14] TIAN Y L, PENG C G, LIN D D, *et al*. Bayesian mechanism for rational secret sharing scheme[J]. Science China Information Sciences, 2015, 58(5):1-13.

[15] 田有亮, 彭长根,马建峰, 等. 通用可组合公平安全多方计算协议[J].通信学报, 2014, 35(2):54-62.
TIAN Y L, PENG C G, MA J F, *et al*. Universally composable secure multiparty computation protocol with fairness[J]. Journal on Communications, 2014, 35(2):54-62.

[16] 张恩, 蔡永泉. 理性的安全两方计算协议[J]．计算机研究与发展, 2013,50(7):1409-1417.
ZHANG E, CAI Y Q. Rational secure two-party computation protocol[J]. Journal of Computer Research and Development, 2013,50 (7): 1409-1417.

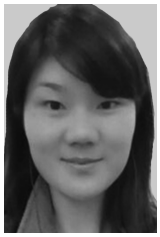
[17] 彭长根, 刘海, 田有亮, 等. 混合偏好模型下的分布式理性秘密共享方案[J]. 计算机研究与发展, 2014, 51(7):1476-1485.
PENG C G, LIU H, TIAN Y L, *et al*. A distributed rational secret sharing scheme with hybrid preference model[J]. Journal of Computer Research and Development, 2014, 51(7):1476-1485.

[18] 王伊蕾, 郑志华, 王皓, 等. 满足可计算序贯均衡的理性公平计算[J]. 计算机研究与发展, 2014, 51(7):1527-1537.
WANG Y L, ZHENG Z H, WANG H, *et al*. Rational fair computation with computational sequential equilibrium[J]. Journal of Computer Research and Development, 2014, 51(7):1527-1537.

作者简介：

田有亮（1982-），男，贵州盘县人，博士，贵州大学副教授，硕士生导师，主要研究方向为算法博弈论、密码学与安全协议等。

王雪梅[通信作者]（1982-），女，贵州贵阳人，贵阳职业技术学院讲师，主要研究方向为应用概率统计、大数据分析应用等。E-mail:wxmgyzyjsxy@163.com。



刘琳芳（1980-），女，河南焦作人，贵州大学讲师，主要研究方向为计算机应用技术等。