中国科学 : 信息科学　2012 年　第 42 卷　第 1 期 : 32–46
www.scichina.com　info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS
论　文

理性密钥共享的扩展博弈模型

张志芳*, 刘木兰

中国科学院数学与系统科学研究院数学机械化重点实验室, 北京 100190
* 通信作者. E-mail: zfz@amss.ac.cn

收稿日期: 2010–05–11; 接受日期: 2011–01–05
国家自然科学基金 (批准号: 60821002/F02, 11001254) 资助项目

摘要　理性密钥共享体制通过引入惩罚策略使得参与者不会偏离协议, 常采用的惩罚是一旦发现有人偏离就立即终止协议. 这种惩罚策略有时导致惩罚人自身利益严格受损, 从而降低了对被惩罚人的威慑. 为了克服这一弱点, 本文以扩展博弈为模型分析了理性密钥共享体制. 首先给出 (2,2) 门限的理性密钥共享体制, 证明了所给的协议是该博弈的一个序贯均衡, 即经过任何历史之后坚持原协议仍然是每一个参与者的最优选择. 特别地, 在发现有人偏离后, 协议所给出的惩罚策略既可以有效惩罚偏离者又能够完全维护惩罚人的利益. 这是本文对前人设计的理性密钥共享体制的一个重要改进. 然后针对将协议扩展到 (t,n) 门限情形, 实现密钥分发人离线, 达到计算的均衡等相关问题给出了一般的解决方案.

关键词　理性密钥共享　扩展博弈　序贯均衡　博弈论　密码学

1　引言

(t,n) 门限密钥共享最早由 Blakley[1] 和 Shamir[2] 在 1979 年分别独立提出, 它要解决的问题是密钥分发人 (dealer) 要在 n 个参与者之间共享一个密钥, 使得只有至少 t 参与者才能够联合恢复该密钥, 任何少于 t 个参与者都不能得到该密钥. 在密码学中关于这个问题的研究都是基于这样一个基本假设：每一个参与者或者是诚实的 (即一定会忠实地执行协议) 或者是恶意的 (即可能任意地背叛协议). 2004 年 Halpern 和 Teague[3] 在博弈论的框架下研究了该问题, 进而提出理性密钥共享 (rational secret sharing) 的概念. 他们假设所有的参与者都是理性的, 每个人的行为都是为了最大化自身利益, 不再存在绝对的诚实或任意的背叛. 显然, 理性参与者的假设更贴近实际生活, 目前已有很多工作涉及到将博弈论和密码学相结合 [4,5], 这其中的一个重要问题就是理性的密钥共享.

赋予每个参与者一个收益函数, 则密钥共享的过程可以看成是 n 个参与者之间的一个博弈. 正如文献 [3] 所指出的, 如果密钥重构只是一个一次性过程, 即要求所有参与者公开各自持有的份额, 然后每个人都可以计算重构函数, 那么没有参与者愿意公开自己的份额 (因为躲在一旁偷听将有可能获得更大的收益), 这会导致密钥重构无法实现. 为了解决这一问题, 和 “重复囚徒困境”[6] 中采取的办法一样, 可以将重构过程重复多次, 并且引入对背叛者的惩罚来制约偏离行为. 但是, 在现有的理性密钥共享体制 [3,7~11] 中几乎都采用这样的惩罚策略: 一旦发现有人偏离就立即终止协议. 这一惩罚策略有时

引用格式: 张志芳, 刘木兰. 理性密钥共享的扩展博弈模型. 中国科学: 信息科学, 2012, 42: 32–46

导致惩罚人自身利益严格受损. 例如, 在 (2,2) 门限体制中, 如果因为在协议的某一轮没有按时收到对方正确的消息, 而从此拒绝再与对方合作, 那么他自己也将永远失去得到密钥的机会. 因此, 这种惩罚策略对于惩罚人本身来说也是相当苛刻的, 在一定程度上降低了该惩罚策略对被惩罚人的威慑. 另一方面, 消息在信道中传输有时会出现滞后或发生错误, 如果因此导致合作终止, 显然对于双方来说都是不合理的.

博弈论中把一些不合理的惩罚策略称为 “空威胁” 或 “不可置信的威胁”, 它的产生主要是由于将一个动态的博弈过程用简单的一次性博弈 (即策略博弈, strategic game) 来分析, 因而忽略了行为的序列结构和动态变化. 扩展博弈 (extensive game) 是消除空威胁的一个很好的模型. 简单来说, 策略博弈中所有的参与者一次性地选择好他所有的行为组合, 而扩展博弈允许参与者在博弈进行的过程中适时地根据情况选择下一步的行为. 因此, 扩展博弈中行为的合理性是要求在经过任何一段历史后都必须满足的. 特别地, 针对偏离行为 (出现偏离行为可以看成一段历史) 采取的惩罚策略也必须是最优选择. 在扩展博弈中采用子博弈完美均衡 (subgame perfect equilibrium) 和序贯均衡 (sequential equilibrium) 来刻画满足这种合理性要求的策略.

本文以扩展博弈为模型研究理性密钥共享, 设计了满足序贯均衡的理性密钥共享体制, 从而消除了之前协议中惩罚策略的不合理性, 即我们给出的惩罚策略既能有效地惩罚背叛者又能完全维护惩罚人自身的利益.

相关工作及主要结果. 理性密钥共享的一个核心问题就是如何刻画 “合理性” (rationality), 即最终的协议应该是一个满足什么条件的均衡 (equilibrium). Halpern 和 Teague[3] 最初提出用反复剔除被弱占优策略的 Nash 均衡 (Nash equilibrium surviving iterated deletion of weakly dominated strategies) 作为理性密钥共享的解, 这一概念被文献 [7] 沿用. 但是, Kol 和 Naor[9,10] 后来指出这个概念并不能排除有些明显不好的策略, 进而他们提出严格的 Nash 均衡 (strict Nash equilibrium)、持久均衡 (everlasting equilibrium)、计算的 $\mathcal{C}$- 弹性均衡 (computational $\mathcal{C}$-resilient equilibrium) 等概念. 但是这些均衡的概念或者要求过于严格以至难以实现, 或者需要基于计算困难性假设. 考虑到参与者在执行行为时可能出现的微小偏差, Fuchsbauer 等 [8] 提出计算意义下相对于颤抖稳定的 Nash 均衡 (computational Nash equilibrium stable with respect to trembles). 这些均衡的概念都是在策略博弈的模型下提出的, 没有对行为的序列结构进行考虑. Maleka 等 [11] 研究了密钥共享的重复博弈模型, 但是他们只考虑了 Nash 均衡, 而没有讨论在重复博弈下更有意义的均衡, 如子博弈完美均衡等. Ong 等 [12] 运用了子博弈完美均衡的概念, 但是在他们的模型中需要假设有一小部分完全诚实的参与者. 实际上, 在文献 [3] 的结论部分以及综述文献 [4,13] 中已经提到, 怎样实现理性密钥共享的子博弈完美均衡等其他更为复杂的均衡是一个值得今后进一步研究的重要问题.

基于理性密钥共享体制的一般框架, 我们以带不完全信息和同时行动的扩展博弈 (extensive game with imperfect information and simultaneous moves) 为模型展开研究. 该模型更加准确全面地刻画了密钥共享的过程, 在该模型下合理性的要求由序贯均衡的概念给出, 它是子博弈完美均衡在不完全信息博弈中的扩展. 我们的主要贡献就是严格地在扩展博弈模型下分析了理性密钥共享, 并设计了满足序贯均衡的具体协议. 与基于策略博弈的理性密钥共享体制相比, 我们的主要优势在于使得惩罚策略更加合理, 既有效惩罚背叛又完全维护惩罚人自身利益. 此外, 我们还初步讨论了序贯均衡的 k 弹性以及如何实现计算意义下的序贯均衡等问题.

文章的第 2 节预备知识部分将介绍理性密钥共享、扩展博弈、序贯均衡等相关概念. 第 3 节首先给出一个 (2,2) 门限密钥共享的扩展博弈模型, 并设计了满足序贯均衡的具体协议, 由此给出一个 (2,2)

门限的理性密钥共享体制. 第 4 节继续讨论如何改进该体制, 包括如何去掉密钥分发人在线的假设, 如何扩展到一般的 (t,n) 门限, 还讨论了关于同时广播和计算意义下的均衡等问题. 第 5 节是全文的结论部分.

2 预备知识

2.1 理性密钥共享

理性密钥共享就是在 n 个理性的参与者之间实现共享密钥. 具体来说, 每个参与者, 例如 P_i, 有一个定义在博弈的所有可能结果上的收益函数 (utility function) $u_i : \{0,1\}^n \to \mathbb{R}$, 这里用一个向量 $\boldsymbol{O} = (o_1, \ldots, o_n) \in \{0,1\}^n$ 表示博弈的一个结果, 其中 $o_j = 1$ 当且仅当 P_j 最后恢复出密钥, $1 \leqslant j \leqslant n$. 我们采用如下被广泛使用的关于收益函数的假设: 对于 $1 \leqslant i \leqslant n$, P_i 的收益函数 u_i 满足

1) 对于任意的 $\boldsymbol{O}, \boldsymbol{O'} \in \{0,1\}^n$, 如果 $o_i > o'_i$, 那么 $u_i(\boldsymbol{O}) > u_i(\boldsymbol{O'})$;

2) 如果 $o_i = o'_i$ 并且 $\sum_{i=1}^n o_i < \sum_{i=1}^n o'_i$, 那么 $u_i(\boldsymbol{O}) > u_i(\boldsymbol{O'})$.

这两个条件说明 P_i 总是更希望最后恢复出密钥, 其次, 越少的人恢复出密钥越好. 理性密钥共享就是要设计一个协议, 使得在密钥重构阶段每个参与者都愿意 (即以最大化自身收益为目标) 出示自己的秘密份额, 从而实现密钥的重构. 在实际设计协议时, 只要满足任何偏离协议的行为都会使偏离者收益严格减少就可以了.

考虑一个简单的 (2,2) 门限密钥共享的例子. 在密钥重构阶段, 如果轮到 P_i $(i = 1, 2)$ 出示秘密份额, 那么他有两种行为可供选择: 出示秘密 (记为 B) 或保持沉默 (记为 S). 假设所有的秘密份额都可以被公开验证 (例如, 通过消息认证码 [14~16] 或签名来实现), 那么出示虚假消息将会以很大概率被检测到, 因此我们将这种行为等同于 "保持沉默" 进行处理. 可以将 (2,2) 门限密钥共享的一次性密钥重构过程看成一个两人的策略博弈, 其中每个人有两种行为 "B" 或 "S" 供选择. 用图 1 来表示这个博弈. 其中行代表 P_1 的行为, 列代表 P_2 的行为. 收益值 $a, b, c, d \in \mathbb{R}$, 表中每个数对的第一个分量表示 P_1 在对应的行为组合下获得的收益, 第二个分量为 P_2 的收益. 根据我们关于收益函数的假设, 显然有 $a > b > c > d$.

在上述策略博弈中出现的一个主要问题就是, 对于每个参与者来说, 选择策略 S 永远不会比策略 B 差, 有时甚至可获得更大的收益, 用博弈论的术语即策略 S 是弱占优的 (weakly dominant). 显然, 一个理性的参与者一定会选择弱占优的策略. 因此在这个一次性的密钥重构博弈中, 没有人会愿意公开自己的秘密份额. 同样的问题也出现在一般的 (t,n) 门限密钥共享中, 并且可以看到即使重构过程被重复多次, 只要次数确定 (即参与者预先知道何时结束), 那么仍然没有人愿意公开秘密 [3]. 理性密钥共享体制通过建立随机机制将重构过程重复多次, 并且对偏离行为采取惩罚, 最终实现密钥的恢复. 为了更准确地分析这种多阶段的过程, 我们选择以扩展博弈作为基本模型.

2.2 扩展博弈

和策略博弈中所有参与者一次性地确定所有行为组合不同, 扩展博弈对于参与者依次采取行为的这种序列结构作了详细描述. 基于本文所研究的问题模型, 这里我们主要介绍带不完全信息和同时行动的扩展博弈 (以后简称为 "扩展博弈").

定义 1 一个扩展博弈由以下成分构成:

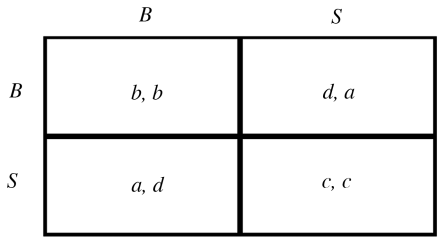

图 1 (2,2) 门限密钥共享的策略博弈

Figure 1 A strategic game of 2-out-of-2 secret sharing

• 参与者集合 N: 是一个有限集合 $N=\{1,2,\ldots,|N|\}$.

• 历史集合 H: 是一个序列的集合, 满足条件:

– 对于任意的 $h=(a^k)_{k=1}^{L}\in H$, h 称为一段长度为 L 的历史 (L 可以是 ∞). 序列的每一项 a^k 是第 k 步所有采取行动的参与者的一个行为组合.

– 对于任意的 $(a^k)_{k=1}^{L}\in H$ 和 $K<L$, 有 $(a^k)_{k=1}^{K}\in H$. 特别地, 空历史 $\emptyset\in H$.

对于任意的 $h\in H$, 在 h 之后可能出现的所有行为组合记为 $A(h)=\{a\mid(h,a)\in H\}$. 如果历史 h 满足 $A(h)=\emptyset$ 或者 h 的长度为 ∞, 则称 h 是终止的. 将所有终止的历史构成的集合记为 Z.

• 参与者函数 $P: H\backslash Z\to 2^N\cup\{\mathfrak{c}\}$: 为每一个没有终止的历史指定下一步行动的参与者集合或映射为外部机会 $\mathfrak{c}$. 如果 $P(h)=A\subseteq N$, 表示 h 之后由子集 N 中的所有参与者同时采取行动; 如果 $P(h)=\mathfrak{c}$, 表示由机会 $\mathfrak{c}$ 确定下一步的行动.

• 函数 $f_{\mathfrak{c}}$: 为每一个满足 $P(h)=\mathfrak{c}$ 的历史 h 指定集合 $A(h)$ 上的一个概率分布.

• 对于每个参与者 $i\in N$, 有信息分割 $\mathcal{I}_i$: 它是集合 $\{h\in H\mid i\in P(h)\}$ 的一个划分, 满足只要 h 和 h' 处在分割的同一元素中, 就有 $A(h)=A(h')$. 其中 $\mathcal{I}_i$ 的每一个元素 $I_i\in\mathcal{I}_i$ 称为一个信息集.

• 收益函数 U_i: 定义在每一个终止的历史下参与者 i 获得的收益.

将一个扩展博弈记为 $\langle N,H,P,f_{\mathfrak{c}},(\mathcal{I}_i),(U_i)\rangle$. 为了进一步解释扩展博弈的各个成分, 下面以一个 (2,2) 门限的密钥共享进行说明, 它也可以看成我们后面在第 3 节将要用到的一个子协议.

例 2 首先, 密钥分发人以概率 p 在参与者之间共享真实的密钥 s, 以概率 $1-p$ 共享空记号 $\perp$. 收到秘密份额以后, 任何单个参与者不知道到底共享的是 s 还是 $\perp$. 在重构阶段, 规定参与者 1 首先出示其秘密份额, 然后 2 再出示自己的份额. 这里只是为了理解定义而人为给出的一个简单例子, 不涉及它在实际生活中的合理性.

参与者可以选择的行为仍然是 B 和 S, 可能的收益为 a,b,c,d (定义同前). 为了后面讨论问题方便, 此处考虑有时候可能存在附加收益 $\varepsilon>0$, 即尽管参与者最后不能恢复秘密, 但是他诚实地出示了自己的秘密份额, 则认为他为自己赢得了好的声誉, 获得附加收益 $\varepsilon>0$.

将密钥分发人看成外部机会 $\mathfrak{c}$, 则可以把上述过程看成一个扩展博弈, 用图 2 中的树来表示. 树的每个节点表示在那一时刻行动的主体, 可以是 $\mathfrak{c}$ 或参与者集合. 每条边代表发生的一个行动组合. 为简单起见, 这里以 p 和 $1-p$ 分别表示密钥分发人共享 s 和共享 $\perp$ 的行为. 每条从根到叶子的路代表一个终止的历史, 叶子下端标注的数对为在该历史下两人获得的收益.

例如, 路 (p,B,S) 表示这样一个历史, 密钥分发人 $\mathfrak{c}$ 首先共享 s, 然后参与者 1 出示了自己的份额, 之后, 参与者 2 保持沉默. 在这段历史下, 1 获得收益 $d+\varepsilon$, 2 获得收益 a.

在树中连接两个节点、并且以 1 标注的虚线表示历史 (p) 和 $(1-p)$ 同属于参与者 1 的一个信息集. 实际上, 当到达该信息集 $I_1=\{(p),(1-p)\}$ 后, 参与者 1 无法区分到底该信息集中的哪个历史真

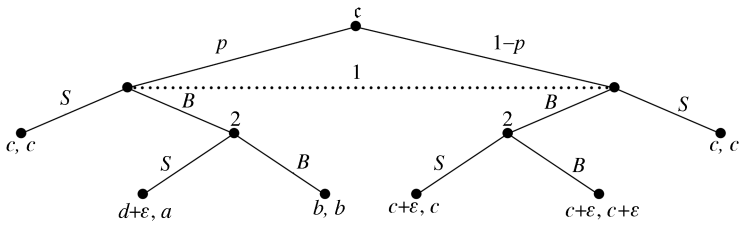

图 2　(2,2) 门限密钥共享的一个扩展博弈

Figure 2　An extensive game of 2-out-of-2 secret sharing

实地发生了. 正是因为这个原因, 我们称该扩展博弈是不完全信息的. 进一步, 我们给出两个参与者信息分割的详细描述:

$$\mathcal{I}_1 = \{\{(p), (1-p)\}\},\ \ I_2 = \{\{(p, B)\}, \{(1-p, B)\}\}\ . \tag{1}$$

即参与者 1 有一个信息集 (含两个历史), 参与者 2 有两个信息集, 每个都只含一个历史, 因此参与者 2 总能清楚地知道到底哪段历史真实地发生了.

2.3　扩展博弈的序贯均衡

为了描述扩展博弈中参与者的策略, 需要用到下面关于状态的概念.

定义 3　扩展博弈的一个状态是一个二元组 (β, μ), 其中

• $\beta = (\beta_i)_{i\in N}$ 是行为策略组合. 具体地, $\beta_i = (\beta_i(I_i))_{I_i\in\mathcal{I}_i}$ 而 $\beta_i(I_i)$ 表示到达信息集 I_i 后参与者 i 可能采取的策略.

• $\mu = (\mu_i)_{i\in N}$ 称为信念系统, 具体地, $\mu_i = (\mu_i(I_i))_{I_i\in\mathcal{I}_i}$ 而 $\mu(I_i)$ 是 I_i 中历史的一个概率分布, 表示参与者 i 对可能发生的历史的一个判断 (或信念).

在例 2 中, 对应于式 (1) 中的表示, 记 $\mathcal{I}_1 = \{I_1\}$ 和 $\mathcal{I}_2 = \{I_{21}, I_{22}\}$. 如下给出一个状态:

– $\beta_1(I_1) = (B:1; S:0)$, 简记为 $\beta_1(I_1) = B$, 即参与者 1 到达信息集 I_1 后采取行为 B.

– $\beta_2(I_{21}) = S$, 即参与者 2 到达信息集 $I_{21} = \{(p, B)\}$ 后采取行为 S.

– $\beta_2(I_{22}) = B$, 即参与者 2 到达信息集 $I_{22} = \{(1-p, B)\}$ 后采取行为 B.

– $\mu_1(I_1) = (p, 1-p)$, 表示参与者 1 相信密钥分发人以概率 p 共享 s, 以概率 $1-p$ 共享 $\perp$.

– μ_2 平凡定义, 因为每个信息集只含有一个历史.

博弈论的一个主要研究内容就是分析在各种博弈中可能出现的结果, 或者等价地, 为每个参与者提供最合理的策略. 在策略博弈中, 通常用 Nash 均衡, 相关均衡等概念定义合理策略. 在扩展博弈中, 常用的概念是序贯均衡, 它是子博弈完美均衡在不完全信息博弈中的扩展概念.

定义 4　状态 (β, μ) 称为扩展博弈 $\langle N, H, P, f_c, (\mathcal{I}_i),\ (U_i)\rangle$ 的一个序贯均衡, 如果它满足下面两个条件:

1) (β, μ) 是序贯理性的: 对于任意的参与者 $i \in N$ 和任意的信息集 $I_i \in \mathcal{I}_i$, 不等式 $U_i(\beta, \mu \mid I_i) \geqslant U_i((\beta_{-i}, \beta_i'), \mu \mid I_i)$ 对于参与者 i 的每个策略 β_i' 都成立, 其中策略组合 (β_{-i}, β_i') 表示 i 选择策略 β_i' 而其他参与者都坚持 β 中对应的策略, $U_i((\beta_{-i}, \beta_i'), \mu \mid I_i)$ 表示在信息集 I_i 到达的条件下, 采取策略组合 (β_{-i}, β_i') 时参与者 i 获得的收益.

2) (β, μ) 是一致的: 存在收敛到 (β, μ) 的状态序列 $((\beta^n, \mu^n))_{n=1}^{\infty}$, 其中 β^n 是完全混合策略, 并且 μ^n 可由 β^n 按照 Bayes 法则导出.

由于本文中考虑的扩展博弈平凡地满足第二个条件 (详见命题 6 证明), 这里对一致性条件就不再解释了 (可参考文献 [17] 的第 12 章). 第一个条件可以看成子博弈完美均衡要求策略的最优性在经过任何一段历史后都满足的一个扩展. 作为说明, 我们看例 2 以及在定义 3 后给出的状态 (β,μ), 即 $\beta_1(I_1)=B,\ \beta_2(I_{21})=S,\ \beta_2(I_{22})=B,\ \mu_1(I_1)=(p,1-p)$. 对于参与者 1 来说,

$$U_1(\beta,\mu\mid I_1)=U_1((B,\beta_2),\mu\mid I_1)=(d+\varepsilon)p+(c+\varepsilon)(1-p)\ ,$$
$$U_1((S,\beta_2),\mu\mid I_1)=cp+c(1-p)=c\ .$$

可以看到, 只要 $(d+\varepsilon)p+(c+\varepsilon)(1-p)\geqslant c$, 即 $\varepsilon\geqslant p(c-d)$, 那么状态 (β,μ) 对于参与者 1 而言就是序贯理性的. 对于参与者 2 的序贯理性是显然的. 又因为一致性条件平凡满足, 因此 (β,μ) 是一个序贯均衡.

3 (2,2) 门限密钥共享的扩展博弈

这一节我们先建立 (2,2) 门限密钥共享的一个扩展博弈模型, 再设计出满足序贯均衡的具体协议.

3.1 博弈模型

假设密钥分发人是诚实的, 记参与者集合为 $N=\{1,2\}$. 我们关于 (2,2) 门限密钥共享的博弈模型由 3 类子博弈构成: Norm(k), Puni$(1,t)$ 和 Puni$(2,t)$, 其中参数 k,t 是正整数. 下面给出具体描述.

子博弈 Norm(k) 即在第 k 次重构时要求两人同时公开秘密份额, 它由以下步骤构成:

N.1 密钥分发人以概率 p 共享 s, 以概率 $1-p$ 共享 $\perp$.

例如, 密钥分发人随机选取 $s_1,s_2\in\{0,1\}^{|s|}$, 使得以概率 p 满足关系 $s_1\oplus s_2=s$, 以概率 $1-p$ 满足关系 $s_1\oplus s_2=\perp$. 这里空记号 $\perp$ 可以认为是具有特殊形式的字符串, 例如假设密钥空间的字符串都是以 1 开头, 则以 0 开头的字符串就被认为是 $\perp$. 然后, 将 $(s_i,\mathrm{Mac}(s_i))$ 发送给参与者 i, 其中 $\mathrm{Mac}(s_i)$ 是 s_i 的认证消息.

N.2 到密钥重构时刻, 参与者 1 和 2 同时公开自己的秘密份额.

• 如果两人公开的消息都没有通过认证, 则到下一密钥重构时刻 (约定每经过一个固定的时间步长开始新一次的密钥重构) 重新执行 N.2 步.

• 如果只有参与者 i 公开的份额通过认证, 参与者 j $(j=N-\{i\})$ 没有通过认证, 则 i 广播消息 "j 在欺骗".

• 如果两人公开的份额都通过认证, 则计算这两个份额的异或值.

– 如果该异或值是空记号 $\perp$, 则广播消息 "重构失败".

– 否则, 将所得的异或值作为被恢复的密钥, 广播消息 "重构成功".

子博弈 Puni$(1,t)$, 即连续第 t 次惩罚参与者 1, 它包含以下步骤:

P.1 和 N.1 步相同.

P.2 到密钥重构时刻, 参与者 1 先公开自己的秘密份额.

• 如果 1 公开的份额没有通过认证, 则到下一密钥重构时刻重新执行 P.2 步.

P.3 如果 1 公开的份额通过认证, 则参与者 2 接着公开自己的秘密份额.

• 如果 2 公开的份额没有通过认证, 则参与者 1 广播消息 "2 在欺骗".

• 否则, 两个参与者都计算所公开份额的异或值.

– 如果该异或值是空记号 $\perp$, 则广播消息 “重构失败”.

– 否则, 将所得的异或值作为被恢复的密钥, 广播消息 “重构成功”.

子博弈 Puni$(2,t)$ 即连续第 t 次惩罚参与者 2. 和 Puni$(1,t)$ 类似, 只是将参与者 1 和 2 位置互换.

注意到在上述每个子博弈中, 密钥分发人只在第一步被调用. 每个子博弈将伴随广播消息 “1 在欺骗”, “2 在欺骗”, “重构失败”, 或 “重构成功” 结束. 也就是说, 我们要求对于密钥分发人的每一次密钥共享 (对应了一次子博弈), 只有当至少一人公开的秘密份额通过认证, 这一次的共享才会结束; 否则将重复要求对应的参与者公开正确的秘密份额.

我们给出的关于 (2,2) 门限密钥共享的扩展博弈模型, 记为 EG-(2,2)RSS, 实际上是将上述 3 类子博弈按照一定顺序组合. 简单来说, 最开始重复执行子博弈 Norm$(\cdot)$, 直到发现有某一个参与者 i 在欺骗, 于是转为连续 L 次执行子博弈 Puni$(i,\cdot)$, 我们将在后面确定 L 的值. 如果在这 L 次子博弈中没有发现欺骗, 则 L 次结束后返回执行 Norm$(\cdot)$. 否则, 一旦发现欺骗, 例如参与者 j 在欺骗, 则立即转入连续 L 次执行 Puni$(j,\cdot)$. 具体描述如下:

博弈模型 EG-(2,2)RSS

E.1 置 $k \leftarrow 1$.

E.2 执行子博弈 Norm(k).

• 如果最后收到广播消息 “1 在欺骗”, 则置 $k \leftarrow k+1$, $t \leftarrow 1$, 转到 E.3 步.

• 如果最后收到广播消息 “2 在欺骗”, 则置 $k \leftarrow k+1$, $t \leftarrow 1$, 转到 E.4 步.

• 如果最后收到广播消息 “重构失败”, 则置 $k \leftarrow k+1$, 转到 E.2 步.

• 否则, 博弈结束.

E.3 执行子博弈 Puni$(1,t)$.

• 如果最后收到广播消息 “2 在欺骗”, 则置 $k \leftarrow k+1$, $t \leftarrow 1$, 转到 E.4 步.

• 如果最后收到广播消息 “重构失败”,

– 当 $t < L$ 时, 置 $k \leftarrow k+1$, $t \leftarrow t+1$, 重新开始执行 E.3 步.

– 当 $t = L$ 时, 置 $k \leftarrow k+1$, 转到 E.2 步.

• 否则, 博弈结束.

E.4 执行子博弈 Puni$(2,t)$.

• 如果最后收到广播消息 “1 在欺骗”, 则置 $k \leftarrow k+1$, $t \leftarrow 1$, 转到 E.3 步.

• 如果最后收到广播消息 “重构失败”,

– 当 $t < L$ 时, 置 $k \leftarrow k+1$, $t \leftarrow t+1$, 重新开始执行 E.4 步.

– 当 $t = L$ 时, 置 $k \leftarrow k+1$, 转到 E.2 步.

• 否则, 博弈结束.

图 3 说明了博弈 EG-(2,2)RSS 的结构. 其中节点 $\mathfrak{c}, \mathfrak{c}_1$ 和 $\mathfrak{c}_2$ 分别代表了子博弈 Norm$(\cdot)$, Puni$(1,\cdot)$ 和 Puni$(2,\cdot)$ 中的密钥分发人. 注意, 它们是同一个密钥分发人, 这里只是为了区别不同类型的子博弈, 才用了不同的记号. 由于该博弈可能出现经过很多次重构过程才会结束的情况, 为简单起见, 我们以叶子处的空心节点表示博弈继续. 如果空心节点有标注 ($\mathfrak{c}, \mathfrak{c}_1$ 或 $\mathfrak{c}_2$), 则表示下一节点转到树上有同样标注的节点; 如果空心节点以一段弧线与前一节点相连, 则表示下一节点转到与之相连的节点. 特别地, 当空心节点标注为 “$\mathfrak{c}$ 或 $\mathfrak{c}_i$”, 表示下一步是转到 Norm$(\cdot)$ 还是 Puni$(i,\cdot)$ 将由是否已经连续执行 L 次

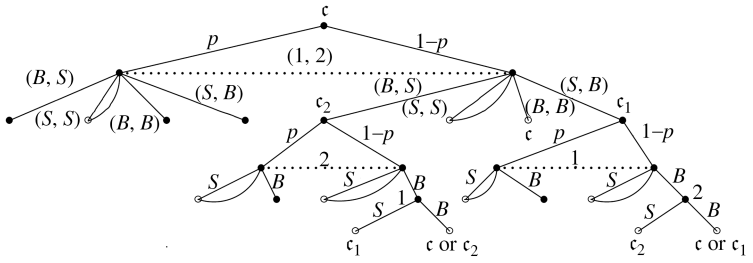

图 3 扩展博弈 EG-(2,2)RSS

Figure 3 Extensive game of 2-out-of-2 secret sharing

决定, $i = 1, 2$. 为简单起见, 我们假设理性参与者无逗留行为, 即一旦恢复出密钥后立即退出协议. 叶子处的实心节点表示博弈结束.

根据扩展博弈 $\langle N, H, P, f_{\mathfrak{c}}, (\mathcal{I}_i), (U_i)\rangle$ 的定义 1, 在上面已经给出了 EG-(2,2)RSS 的 $N, H, P, f_{\mathfrak{c}}, (\mathcal{I}_i)$, 接下来定义收益函数 (U_i). 给定所有终止历史集合 Z 上的一个概率分布 Prob(·), 定义

$$U_i = \sum_{z \in Z} u_i(z)\mathrm{Prob}(z), \tag{2}$$

其中 $u_i(z)$ 表示参与者 i 在历史 z 下获得的收益. 为了进一步定义 $u_i(z)$, 我们采用在重复博弈中经常用到的取平均收益的办法. 细节如下:

对于 EG-(2,2)RSS 的任意一个终止的历史 $z \in Z$, 令 $k(z)$ 表示在历史 z 中发生的子博弈 (即 Norm(·), Puni(1, ·) 或 Puni(2, ·)) 的次数. 对于 $1 \leqslant l \leqslant k(z)$, 令 $u_i^{\,l}(z)$ 表示参与者 i 在第 l 次子博弈中获得的收益. 参考第 2.1 小节给出的收益值, 我们有

- $u_i^{\,l}(z) = a$, 如果只有参与者 i 在第 l 次子博弈中恢复出密钥.
- $u_i^{\,l}(z) = b$, 如果两个参与者都在第 l 次子博弈中恢复出密钥.
- $u_i^{\,l}(z) = c$, 如果两个参与者都没有在第 l 次子博弈中恢复出密钥.
- $u_i^{\,l}(z) = d$, 如果只有参与者 i 没在第 l 次子博弈中恢复出密钥.

根据平均收益原则, 定义

$$u_i(z) = \frac{\sum_{l=1}^{k(z)} u_i^{\,l}(z)}{k(z)}, \text{ 对于任意的 } z \in Z\ . \tag{3}$$

结合式 (2) 和 (3), 我们给出了 EG-(2,2)RSS 中收益函数的完整定义. 在重复博弈中还有一些用于定义收益函数的其他原则, 如平均折扣原则, 最大原则等, 参见文献 [17].

3.2 EG-(2,2)RSS 博弈的序贯均衡

这一小节将给出博弈 EG-(2,2)RSS 的一个序贯均衡. 根据定义 4, 需要对任意的状态 (β, μ) 和信息集 I_i 计算收益值 $U_i(\beta, \mu \mid I_i)$. 从图 3 可以看到, 每个信息集至多含有两个历史, 并且处在同一信息集的两个历史所经历的子博弈序列是相同的. 因此, 对于任一信息集 I_i, 令 $k(I_i)$ 表示到达该信息集时已经完成的子博弈的个数. 此外, 由于我们的博弈模型中采用的信念系统 μ 与参与者所用的策略无关, 即到达含有两个历史的信息集 I_i 时, 参与者 i 总认为密钥分发人以概率 p 共享 s, 以概率 $1-p$ 共享 $\perp$. 所以, 在后面我们将不再特别说明信念系统 μ, 特别地, 记 $U_i(\beta \mid I_i) = U_i(\beta, \mu \mid I_i)$.

引理 5 在平均收益原则下, 对于博弈 EG-(2,2)RSS 的任意策略 β 和信息集 I_i, 有

$$U_i(\beta \mid I_i) \in \left[\sum_{l=1}^{\infty} \frac{(l+k(I_i)-1)c+d}{l+k(I_i)}(1-p)^{l-1}, \sum_{l=1}^{\infty} \frac{(l+k(I_i)-1)c+a}{l+k(I_i)}(1-p)^{l-1}\right].$$

证明 因为以到达信息集 I_i 为条件, 所以只需考虑以 I_i 中的历史为前缀的终止历史, 简单记为 $z : z \ni I_i$. 根据式 (2) 和 (3), 有

$$U_i(\beta \mid I_i) = \sum_{z:z\ni I_i} u_i(z)\mathrm{Prob}_\beta(z|I_i) = \sum_{z:z\ni I_i} \frac{\sum_{l=1}^{k(z)} u_i{}^l(z)}{k(z)}\mathrm{Prob}_\beta(z|I_i)\ ,$$

其中 $\mathrm{Prob}_\beta(z|I_i)$ 是采取策略 β 时发生历史 z 的概率.

对于任意的终止历史 $z : z \ni I_i$, 有 $k(z) > k(I_i)$. 首先考虑 $k(z) < \infty$ 的情形. 因为每一个子博弈结束时, 至少有一个参与者能够恢复出密钥分发人在这次子博弈中共享的秘密（s 或 $\perp$）, 并且理性参与者一旦恢复出密钥就会退出协议, 可以推出沿历史 z 在前 $k(z)-1$ 次子博弈中密钥分发人共享的都是 $\perp$, 两人都没有恢复出密钥, 即 $u_i{}^l(z) = c$, $1 \leqslant l < k(z)$. 在最后一次子博弈中, 共享 s 和共享 $\perp$ 的情形都可能发生. 例如, 共享 $\perp$ 时如果某个参与者总是出示虚假的份额, 那么博弈将会重复要求他出示真实信息. 但是不管哪种情形发生, 一定有 $u_i^{k(z)}(z) \in [d, a]$.

对于 $1 + k(I_i) \leqslant l < \infty$, 记 $z_l = \{z \in Z \mid I_i \in z,\ k(z) = l\}$. 从上一段的分析可以看到, 对于任意的 $z \in z_l$, $u_i(z) \in [\frac{(l-1)c+d}{l}, \frac{(l-1)c+a}{l}]$, 并且 $\mathrm{Prob}_\beta(z_l|I_i) = (1-p)^{l-k(I_i)-1}$. 对于 $k(z) = \infty$, 仍然有 $u_i(z) \in [d, a]$, 但是 $\mathrm{Prob}_\beta(z|I_i) = (1-p)^\infty = 0$. 因此, 由

$$U_i(\beta \mid I_i) = \sum_{z:z\ni I_i} u_i(z)\mathrm{Prob}_\beta(z|I_i) = \sum_{l=1+k(I_i)}^{\infty} u_i(z_l)\mathrm{Prob}_\beta(z_l|I_i)\ ,$$

立即推出引理结论.

下面证明一个重要性质：一次偏离性质 (one deviation property), 它对于证明序贯均衡非常关键. 已有结论, 对于有限的扩展博弈一次偏离性质成立 [17]. 由于我们的博弈 EG-(2,2)RSS 可能出现无限长度的历史, 因此需要对该性质进行重新证明.

命题 6 在扩展博弈 EG-(2,2)RSS 中一个状态 (β, μ) 是序贯均衡, 当且仅当它满足一次偏离性质, 即对于任意的参与者 $i \in N$ 和任意的信息集 $I_i \in \mathcal{I}_i$, $U_i(\beta_i', \beta_{-i} \mid I_i) \leqslant U_i(\beta_i, \beta_{-i} \mid I_i)$ 对于 β_i 在 I_i 处任意的一次偏离策略 β_i' 都成立, 其中 β_i 在 I_i 处的一次偏离策略 β_i' 是指 $\beta_i'(I_i) \neq \beta_i(I_i)$, 而 对于所有的 $I_i' \neq I_i$ 都有 $\beta_i'(I_i') = \beta_i(I_i')$.

证明 必要性由定义 4 立即得到, 只证明充分性. 设 (β, μ) 满足一次偏离性质. 用反证法, 假设 (β, μ) 不是序贯均衡. 由于在博弈 EG-(2,2)RSS 中关于不确定历史的信念主要来自于密钥分发人是共享 s 还是 $\perp$ 的行为, 而这两种行为的概率分布是完全确定和公开的, 即前者概率为 p 后者为 $1-p$, 所以 (β, μ) 平凡满足一致性条件, 只可能不满足序贯理性的条件, 即存在参与者 i 和信息集 I_i, 使得对于某个 $\beta_i' \neq \beta_i$, 有

$$U_i(\beta_i', \beta_{-i} \mid I_i) > U_i(\beta_i, \beta_{-i} \mid I_i)\ .$$

根据引理 5, $U_i(\beta_i', \beta_{-i} \mid I_i) \in [\sum_{l=1}^{\infty} \frac{(l+k(I_i)-1)c+d}{l+k(I_i)}(1-p)^{l-1}, \sum_{l=1}^{\infty} \frac{(l+k(I_i)-1)c+a}{l+k(I_i)}(1-p)^{l-1}]$. 因为 $\frac{(l+k(I_i)-1)c+d}{l+k(I_i)}(1-p)^{l-1}$ 和 $\frac{(l+k(I_i)-1)c+a}{l+k(I_i)}(1-p)^{l-1}$ 在 l 趋向于 ∞ 时都趋于 0, 所以当 $k(z)$ 足够大

时, 在历史 z 下获得的收益 $u_i(z)$ 对于 $U_i(\beta_i', \beta_{-i} \mid I_i)$ 的值不会有太大的影响. 具体地, 对于任意的 $\epsilon > 0$, 存在正整数 T, 如下定义策略 β_i'':

$$\begin{cases} \beta_i''(I_i') = \beta_i'(I_i'), & \text{对于任意满足 } k(I_i') \leqslant T \text{ 的信息集 } I_i', \\ \beta_i''(I_i') = \beta_i(I_i'), & \text{对于任意满足 } k(I_i') > T \text{ 的信息集 } I_i' \text{ .} \end{cases}$$

即将 β_i' 在第 $T+1$ 次子博弈之后的策略修改为和 β_i 一样. 取 T 足够大, 则第 $T+1$ 次子博弈之后获得的收益对于整个收益的影响很小, 有 $|U_i(\beta_i'', \beta_{-i} \mid I_i) - U_i(\beta_i', \beta_{-i} \mid I_i)| < \epsilon$. 适当地选择 $\epsilon > 0$, 可以做到

$$U_i(\beta_i'', \beta_{-i} \mid I_i) > U_i(\beta_i, \beta_{-i} \mid I_i), \tag{4}$$

即 β_i'' 也是一个可以使得参与者 i 收益增加的偏离策略, 但是 β_i'' 在第 $T+1$ 次子博弈之后和 β_i 相同, 它们的差别只出现在前 $T+1$ 次子博弈中. 不妨设 β_i'' 在前 $T+1$ 次子博弈中偏离 β_i 的子博弈次数最少. 记 I_i'' 为信息集满足 $\beta_i''(I_i'') \neq \beta_i(I_i'')$, 而对于任意 $k(I_i') > k(I_i'')$ 的 I_i' 都有 $\beta_i''(I_i') = \beta_i(I_i')$. 我们说

$$U_i(\beta_i'', \beta_{-i} \mid I_i'') > U_i(\beta_i, \beta_{-i} \mid I_i'') \text{ .}$$

否则, 修改 β_i'' 在 I_i'' 处的行为, 使得不等式 (4) 仍然成立, 但是偏离 β_i 的子博弈次数减少, 这与 β_i'' 的选取矛盾.

已经有 $\beta_i''(I_i'') \neq \beta_i(I_i'')$ 和对于任意的 $k(I_i') > k(I_i'')$ 满足 $\beta_i''(I_i') = \beta_i(I_i')$. 构造策略 $\tilde{\beta}_i$ 使得 $\tilde{\beta}_i(I_i'') = \beta_i''(I_i'')$ 而对于任意的 $I_i' \neq I_i''$ 都有 $\tilde{\beta}_i(I_i') = \beta_i(I_i')$. 则有

$$U_i(\beta_i'', \beta_{-i} \mid I_i'') = U_i(\tilde{\beta}_i, \beta_{-i} \mid I_i'') \text{ ,}$$

这是因为在到达 I_i'' 条件下的收益值与满足 $k(I_i') \leqslant k(I_i'')$ 的其他信息集 I_i' 处的行为无关, 而对于 $k(I_i') > k(I_i'')$ 的信息集 I_i', 有 $\tilde{\beta}_i(I_i') = \beta_i(I_i') = \beta_i''(I_i')$.

显然, $\tilde{\beta}_i$ 是 β_i 在 I_i'' 处的一次偏离策略, 而使得参与者 i 的收益增加, 这与 (β, μ) 满足一次偏离性质的条件矛盾, 因此假设不成立, (β, μ) 是序贯均衡.

命题 6 提供了一个较为简单的方法来判断博弈 EG-(2, 2)RSS 中策略的序贯理性. 下面我们给出 EG-(2,2)RSS 的一个策略 (记为策略 A), 并证明它满足序贯均衡.

策略 A 参与者 $i \in N = \{i, j\}$ 的策略如下:

- 在子博弈 Norm$(\cdot)$ 中轮到 i 出示份额时, i 总选择行为 B;
- 在子博弈 Puni$(i, \cdot)$ 中轮到 i 出示份额时, i 总选择行为 B;
- 在子博弈 Puni$(j, \cdot)$ 中轮到 i 出示份额时, i 首先计算 j 通过认证的份额与自己份额的异或值,
  - 如果该异或值为 $\perp$, 则 i 选择行为 B;
  - 否则, i 将异或值作为恢复的密钥, 选择行为 S.

命题 7 在平均收益原则下, 当 L 足够大和 p 足够小时, 策略 A 满足博弈 EG-(2,2)RSS 的序贯均衡.

证明 根据命题 6, 只需要证明策略 A 满足一次偏离性质. 为方便起见, 记策略 A 为 β. 对于任意的参与者 $i \in N$ 和任意的信息集 $I_i \in \mathcal{I}_i$, 到达信息集 I_i 时, 已经经过了 $k(I_i)$ 次子博弈. 下面按照第 $k(I_i)+1$ 次子博弈的类型分情况进行证明.

1) 第 $k(I_i)+1$ 次子博弈是 Norm$(k(I_i)+1)$.

如果两个参与者都坚持策略 β, 那么整个博弈将按照子博弈 $\mathrm{Norm}(k(I_i)+1)$, $\mathrm{Norm}(k(I_i)+2)$, …, 继续下去直到密钥分发人在某一次子博弈中共享了密钥 s. 因此, 参与者将在这些子博弈中每次获得收益 c 一直到最后一次子博弈获得收益 b. 根据引理 5, 有

$$U_i(\beta_i,\beta_{-i}\mid I_i)=\sum_{l=1}^{\infty}\frac{(k(I_i)+l-1)c+b}{k(I_i)+l}(1-p)^{l-1}p\,.$$

如果参与者 i 在到达信息集 I_i 时采取了一次偏离策略 β_i', 而另一参与者坚持策略 β_{-i}, 不失一般性, 设 $\beta_i'(I_i)=S$ 而对于任意的 $I_i'\neq I_i$ 都有 $\beta_i'(I_i')=\beta_i(I_i')$. 参与者采取随机行为 (即混合策略) 时, 获得的收益是这里分析的收益的一个凸组合, 不影响证明结果. 在策略组合 (β_i',β_{-i}) 下, 整个博弈将按照 $\mathrm{Norm}(k(I_i)+1)$, $\mathrm{Puni}(i,1),\ldots,\mathrm{Puni}(i,L)$, $\mathrm{Norm}(k(I_i)+L+2)$, $\mathrm{Norm}(k(I_i)+L+3),\ldots$, 进行下去, 其中一旦真实密钥 s 在某一次子博弈中被共享, 则整个博弈就会结束. 如果在子博弈 $\mathrm{Norm}(k(I_i)+1)$ 结束, 参与者 i 在该次子博弈中获得收益 a; 如果在 $\mathrm{Puni}(i,\cdot)$ 时结束, 参与者 i 将在这最后一次子博弈中获得收益 d. 因此, 有

$$\begin{aligned}U_i(\beta_i',\beta_{-i}\mid I_i)=&\frac{k(I_i)c+a}{k(I_i)+1}p+\sum_{l=2}^{L+1}\frac{(k(I_i)+l-1)c+d}{k(I_i)+l}(1-p)^{l-1}p\\&+\sum_{l=L+2}^{\infty}\frac{(k(I_i)+l-1)c+b}{k(I_i)+l}(1-p)^{l-1}p.\end{aligned}\tag{5}$$

为了统一形式, 有

$$\begin{aligned}U_i(\beta_i,\beta_{-i}\mid I_i)=&\frac{k(I_i)c+b}{k(I_i)+1}p+\sum_{l=2}^{L+1}\frac{(k(I_i)+l-1)c+b}{k(I_i)+l}(1-p)^{l-1}p\\&+\sum_{l=L+2}^{\infty}\frac{(k(I_i)+l-1)c+b}{k(I_i)+l}(1-p)^{l-1}p\,.\end{aligned}\tag{6}$$

要使 β 在 I_i 处满足一次偏离性质, 即要求

$$U_i(\beta_i',\beta_{-i}\mid I_i)\leqslant U_i(\beta_i,\beta_{-i}\mid I_i).\tag{7}$$

由式 (5) 和 (6), 这等价地要求

$$\frac{a-b}{b-d}\leqslant\sum_{k=1}^{L}\frac{(1-p)^k}{\frac{k}{1+k(I_i)}+1}\,.$$

由于不等式 (7) 要求对于任意的信息集 I_i 都满足, 这只要上式特别地在 $k(I_i)=0$ 时满足就可以达到, 即要求满足 $\frac{a-b}{b-d}\leqslant\sum_{k=1}^{L}\frac{(1-p)^k}{k+1}$. 取 L 足够大, 使得对于某个 $\epsilon>0$, 有 $\sum_{k=1}^{L}\frac{(1-p)^k}{k+1}\geqslant\sum_{k=1}^{\infty}\frac{(1-p)^k}{k+1}-\epsilon$. 因为

$$\sum_{k=1}^{\infty}\frac{(1-p)^k}{k+1}=\frac{1}{1-p}\left(\sum_{k=1}^{\infty}\frac{(1-p)^k}{k}-1+p\right)=\frac{1}{1-p}(-\ln p-1+p)>-\ln p-1.$$

因此, 当 $-\ln p-1>\frac{a-b}{b-d}$, 即 $p<e^{-1-\frac{a-b}{b-d}}$ 时, 有 $\sum_{k=1}^{\infty}\frac{(1-p)^k}{k+1}>\frac{a-b}{b-d}$. 取 $\epsilon=\sum_{k=1}^{\infty}\frac{(1-p)^k}{k+1}-\frac{a-b}{b-d}$ 和 L 充分大使得 $\sum_{k=1}^{L}\frac{(1-p)^k}{k+1}\geqslant\sum_{k=1}^{\infty}\frac{(1-p)^k}{k+1}-\epsilon$, 则不等式 (7) 满足.

2) 第 $k(I_i)+1$ 次子博弈是 $\mathrm{Puni}(i,t)$, $1\leqslant t\leqslant L$.

如果参与者 i 偏离 β_i 而采取行为 S, 这样只会延迟密钥被最后恢复的耗时, 不会增加 i 的收益.

3) 第 $k(I_i)+1$ 次子博弈是 Puni(j,t), $1\leqslant t\leqslant L$.

显然, 在这种情形下, 参与者 i 的一次偏离不会带来收益的增加.

综上, 取 $p<e^{-1-\frac{a-b}{b-d}}$, 同时取 L 足够大使得 $\sum_{k=1}^{L}\frac{(1-p)^k}{k+1}\geqslant\sum_{k=1}^{\infty}\frac{(1-p)^k}{k+1}-(\sum_{k=1}^{\infty}\frac{(1-p)^k}{k+1}-\frac{a-b}{b-d})$, 那么策略 A(即策略 β) 满足博弈 EG-(2,2)RSS 的序贯均衡.

显然如果采取策略 A, 最后两个参与者都能够恢复出密钥, 并且上面已经证明策略 A 是一个序贯均衡. 因此, 在扩展博弈 EG-(2,2)RSS 中采用策略 A 实际上给出了一个 (2,2) 门限的理性密钥共享体制. 特别地, 可以看到子博弈 Puni$(1,\cdot)$ 和 Puni$(2,\cdot)$ 实际上分别对应了对参与者 1 和 2 的惩罚, 由于满足序贯均衡, 这些惩罚策略在惩罚偏离者的同时也维护了惩罚人自身的利益.

4 进一步讨论

在这一节我们将对上节给出的理性密钥共享体制 EG-(2,2)RSS 中的相关方面做出改进和进一步讨论.

4.1 密钥分发人离线

在 EG-(2,2)RSS 的每一次子博弈中, 都需要密钥分发人重新给每位参与者分发一个秘密份额. 由于整个 EG-(2,2)RSS 博弈由多次子博弈构成, 因此它需要密钥分发人一直保持在线的状态. 但是在现实生活中, 在线的密钥分发人是一个很不实际的假设, 我们希望密钥分发人只在协议的最开始用到, 此后就退出协议, 即保持离线状态. 为了实现这一目的, 可以通过参与者之间的安全多方计算来模拟每一次子博弈中秘密份额的重新分发 [7]. 下面简单介绍如何利用单向陷门置换 (one-way trapdoor permutation) 来实现密钥分发人离线 [8].

对于 $i\in N=\{1,2\}$, 设 f_i,g_i 是单向陷门置换, 它们的陷门由密钥分发人和参与者 i 掌握, 即他们都可以在多项式时间里求出 f_i 和 g_i 的逆. 令 h_{f_i},h_{g_i} 分别表示 f_i,g_i 的核心断言 (hard-core predicate[18]). 设密钥 $s\in\{0,1\}^l$, 令 $y\in\{0,1\}^l$ 是一个公开的字符串. 在博弈 EG-$(2,2)$RSS 之前增加一个初始阶段: 密钥分发人秘密地按照参数为 p 的几何分布 1)选取 $i^*\in\{1,2,\ldots\}$. 然后, 发送给参与者 i 秘密份额 $s\oplus(h_{f_j}(f_j^{-(i^*-1)l-1}(y)),\ldots,h_{f_j}(f_j^{-(i^*-1)l-l}(y)))$ 及标记 $(h_{g_j}(g_j^{-(i^*-1)l-1}(y)),\ldots,h_{g_j}(g_j^{-(i^*-1)l-l}(y)))$. 之后, 密钥分发人退出协议.

在初始阶段之后, 博弈还是按照前面规定的子博弈 Norm$(\cdot)$, Puni$(1,\cdot)$ 和 Puni$(2,\cdot)$ 的序列结构进行. 不同的是在每次子博弈中, 例如第 k 次子博弈中, 参与者 i 需要公开 $(f_i^{-(k-1)l-1}(y),\ldots,f_i^{-(k-1)l-l}(y))$ 和 $(g_i^{-(k-1)l-1}(y),\ldots,g_i^{-(k-1)l-l}(y))$. 参与者 j 可以验证 i 所公开信息的正确性, 因为 f_i,g_i 是容易计算的. 如果验证通过, 则将第二条信息在核心断言 h_{g_i} 下与自己在初始阶段从密钥分发人处得到的标记对比, 如果一致则说明 $i^*=k$, 从而可以根据第一条公开信息和自己掌握的秘密份额恢复出密钥; 如果不一致, 则转入下一次的子博弈.

4.2 同时广播

与过去的许多理性密钥共享体制 [3,7,19,20] 一样, 这里需要用到同时广播信道假设, 也就是说, 在

1) 设每次抛币以概率 p 出现正面, 以概率 $1-p$ 出现反面. 独立重复多次抛币, 则 i^* 为首次出现正面所需的抛币次数

子博弈 Norm(·) 中, 要求两个参与者同时公开自己的秘密份额, 这意味着每个参与者在决定自己公开的消息 (或决定是否公开消息) 时无法看到对方将要公开的消息. 同时广播信道有时也被认为是不标准的信道假设, 已有很多工作开始研究如何去掉这一假设 [8~10]. 由于我们的惩罚策略的启动主要依赖于参与者在 Norm(·) 中是否同时广播消息, 因此目前还不能在本文协议中去掉这一假设. 如何在标准通信模型下给出维护惩罚人自身利益的理性密钥共享体制是个值得进一步研究的问题.

4.3 扩展到 (t,n) 门限

在 (t,n) 门限的理性密钥共享体制中, 一个关键问题是需要考虑可能出现多个参与者合谋而产生的偏离, 因此需要满足 k 弹性均衡 [19], 即任何至多 k 个人合谋偏离, 只要其他参与者仍然坚持原策略, 那么这 k 个合谋者中的任何一个人都不会获得更多的收益. 以 EG-(2,2)RSS 为基础实现 k 弹性均衡, 一个直观的解决办法是在子博弈 Norm(·) 中如果发现有至多 k ($k < t$) 个人没有按要求公开正确的消息, 那么其余的 $n-k$ 个参与者共同决定一个关于这 k 个偏离者的置换. 在下一次子博弈中, 首先按照这个置换顺序由这 k 个偏离者依次公开自己的秘密份额, 然后其余的 $n-k$ 个参与者再同时公开信息. 这可以看作对 k 个偏离者的一次惩罚. 和命题 7 一样, 可以通过具体的计算来决定每一次惩罚需要持续的次数 L 以及概率 p 的选择.

4.4 计算的均衡

在我们的博弈模型中, 为了去掉密钥分发人在线的假设, 用到安全多方计算或单向陷门置换, 因此我们在这里需要对每个参与者的计算能力做出限制; 对应地, 在讨论博弈的均衡时也可以考虑到计算能力的限制, 即计算的均衡, 要求任何计算能力有限的理性参与者至多能从偏离协议中获得收益增加一个可忽略值. 但是, 如何定义计算的序贯均衡是一个有待解决的问题. Katz 在 [13] 中对这一问题进行过简单讨论. 在这里, 我们按照一般定义计算均衡的办法 [8,10], 要求计算的序贯均衡满足在任何历史下, 任何计算能力有限的理性参与者至多能从偏离协议中获得收益增加一个可忽略值. 可以证明, 在 3.2 小节给出的策略 A 满足这一意义下的计算的序贯均衡.

5 结论

本文以扩展博弈为模型研究了理性密钥共享体制, 设计了满足序贯均衡的密钥共享协议, 使得相应的惩罚策略很好地维护了惩罚人自身的利益, 较之前的协议更加合理化. 然而, 严格地在扩展博弈的框架下讨论理性是一个很复杂的问题, 我们的协议依赖于同时广播信道的假设, 同时对于 k 弹性的均衡以及计算的均衡等问题只是进行了初步的探讨, 还有很多问题需要进一步深入研究.

参考文献

1 Blakley G R. Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference, New York, 1979. 313–317

2 Shamir A. How to share a secret. Commun ACM, 1979, 22: 612–613

3 Halpern J, Teague V. Rational secret sharing and multiparty computation. In: Proceedings of the 36th STOC. New York: ACM Press, 2004. 623–632

4 Dodis Y, Rabin T. Cryptography and game theory. In: Nisan N, Roughgarden T, Tardos E, et al, eds. Algorithmic Game Theory. Cambridge: Cambridge University Press, 2007. 181–207
5 Katz J. Bridging game theory and cryptography: Recent results and future directions. In: Proceedings of TCC 2008, LNCS 4948. Heidelberg: Springer, 2008. 251–272
6 Fudenberg D, Tirole J. Game Theory. Cambridge: MIT Press, 1992
7 Gordon S D, Katz J. Rational secret sharing, revisited. In: Proceedings of SCN 2006, LNCS 4116. Heidelberg: Springer, 2006. 229–241
8 Fuchsbauer G, Katz J, Naccache D. Efficient rational secret sharing in standard communication networks. In: Proceedings of TCC 2010, LNCS 5978. Heidelberg: Springer, 2010. 419–436
9 Kol G, Naor M. Games for exchanging information. In: Proceedings of STOC 2008. New York: ACM Press, 2008. 423–432
10 Kol G, Naor M. Cryptography and game theory: Designing protocols for exchanging information. In: Proceedings of TCC 2008, LNCS 4948. Heidelberg: Springer, 2008. 320–339
11 Maleka S, Shareef A, Pandu Rangan C. Rational secret sharing with repeated games. In: Proceedings of ISPEC 2008, LNCS 4991. Heidelberg: Springer, 2008. 334–346
12 Ong S J, Parkes D V, Rosen A, et al. Fairness with an honest minority and a rational majority. In: Proceedings of TCC 2009, LNCS 5444. Heidelberg: Springer, 2009. 36–53
13 Katz J. Ruminations on defining rational MPC. Talk given at SSoRC, Bertinoro, Italy, 2008. http://www.daimi.au.dk/jbn/SSoRC2008/program
14 Gordon S D, Hazay C, Katz J, et al. Complete fairness in secure two-party computation. In: Proceedings of STOC 2008. New York: ACM Press, 2008. 413–422
15 Rabin T, Ben-Or M. Verifiable secret sharing and multiparty protocols with honest majority. In: Proceedings of the 21th Annual ACM Symposium on Theory of Computing (STOC). New York: ACM, 1989. 73–85
16 Wegman M, Carter L. New hash functions and their use in authentication and set equality. J Comput Syst Sci, 1981, 22: 265–279
17 Osborne M, Rubinstein A. A Course in Game Theory. Cambridge: MIT Press, 2004
18 Goldreich O. Foundations of Cryptography I: Basic Tools. Cambridge: Cambridge University Press, 2001
19 Abraham I, Dolev D, Gonen R, et al. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In: Proceedings of the 25th ACM Symposium Annual on Principles of Distributed Computing. New York: ACM Press, 2006. 53–62
20 Lysyanskaya A, Triandopoulos N. Rationality and adversarial behavior in multi-party computation. In: Proceedings of CRYPTO 2006, LNCS 4117. Heidelberg: Springer, 2006. 180–197

Rational secret sharing as extensive games

ZHANG ZhiFang* & LIU MuLan

Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China*
*E-mail: zfz@amss.ac.cn

Abstract The threat that comes from previously used punishment strategies in rational secret sharing is weakened because the punishment somtimes also causes loss to the punisher himself. In this paper, we first model 2-out-of-2 rational secret sharing in an extensive game with imperfect information, and then provide a strategy for achieving secret recovery in this game. Moreover, we prove that the strategy is a sequential equilibrium which means after any history of the game no player can benefit from deviations so long as the other players stick to the strategy. In particular, when a deviation is detected, the punishment executed by the punisher is still his optimal

option. Therefor, by considering rational secret sharing as an extensive game, we design punishment strategies that effectively punish the deviants and meanwhile guarantee punishers' benefit. Hence, these punishments are more credible than previous ones. Except assuming the existence of simultaneous channels, our scheme can have dealer off-line and extend to the t-out-of-n setting, and also satisfies computational equilibria in some sense.

Keywords rational secret sharing, extensive game, sequential equilibrium, game theory, cryptography

ZHANG ZhiFang was born in 1980. She received the Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science (AMSS), Beijing in 2007. Currently, she is an assistant researcher at AMSS. Her research interests include information security and cryptography.

LIU MuLan was born in 1941. She graduated from University of Science and Technology of China in 1964. She is a professor at Academy of Mathematics and Systems Science (AMSS). Her research interests include information security, cryptography, and computer algebra.