(2,2)贝叶斯理性秘密共享方案

刘 海[1,2],彭长根[1,2],田有亮[1,2,3],吕 桢[1,2],刘荣飞[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;
3.中国科学院信息工程研究所信息安全国家重点实验室,北京 100093)

摘 要: 在理性秘密共享协议中,自利性目标可能会驱使理性参与者偏离协议,从而影响协议的公平性.在(t,n)门限理性秘密共享方案中,其特殊情形(2,2)理性秘密共享方案的公平性较难实现.在同时考虑理性参与者的眼前利益和长远利益的基础上,基于不完全信息动态博弈模型,通过分析理性参与者在(2,2)秘密重构阶段可能采取的策略和信念系统,引入理性参与者的期望收益,研究了(2,2)理性秘密共享重构阶段的完美贝叶斯均衡问题.进一步结合机制设计理论中的 VCG(Vickrey-Clarke-Groves)机制,设计激励相容的交互记录机制来约束理性参与者的行为,在不需要秘密分发者保持在线的情形下,提出一个适用于异步通信的公平的(2,2)理性秘密共享方案.

关键词: 理性秘密共享; 不完全信息; 信念系统; 完美贝叶斯均衡; 机制设计
中图分类号: TP309, TN918 **文献标识码:** A **文章编号:** 0372-2112 (2014)12-2481-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.12.021

The (2,2) Bayesian Rational Secret Sharing Scheme

LIU Hai[1,2], PENG Chang-gen[1,2], TIAN You-liang[1,2,3], LÜ Zhen[1,2], LIU Rong-fei[1,2]
(1. *College of Science, Guizhou University, Guiyang, Guizhou* 550025, *China*; 2. *The Institute of Cryptography and Data Security, Guizhou University, Guiyang, Guizhou* 550025, *China*; 3. *The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: The rational secret sharing is an intersection direction between the traditional secret sharing and game theory. In the rational secret sharing scheme, the selfishness maybe impels rational players to deviate from the protocols so as to influence the fairness of scheme. In the existing threshold rational secret sharing schemes, the fairness of (2,2) rational secret sharing scheme, which is a special case, is hard to be realized, especially implementing on the asynchronous communication channel. To achieve fairness of (2,2) rational secret sharing over the asynchronous communication channel, this paper firstly analyzes rational players' utility by simultaneously discussing their short-term interest and long-term interest. Then through illustrating rational players' available actions and belief systems, and computing their expected utilities with the dynamic games of incomplete information, the perfect Bayesian equilibrium for reconstruction phase of (2,2) rational secret sharing is studied. Furthermore, combining with the VCG (Vickrey-Clarke-Groves) mechanism of design theory, the incentive compatibility mechanism, which is named recording interaction, is designed to restrict the behavior of rational players. Consequently, the fair (2,2) rational secret sharing scheme is presented, which does not need the dealer to keep on-line over the asynchronous communication channel.

Key words: rational secret sharing; incomplete information; belief system; perfect Bayesian equilibrium; mechanism design

1 引言

(t,n)门限秘密共享是针对密钥管理中密钥的泄露问题和遗失问题提出的一种分发、保存和恢复密钥的方法.它最早是于 1979 年由 Shamir[1] 和 Blakey[2] 分别基于拉格朗日插值法和几何空间中点的性质提出的.

在传统的秘密共享方案中,参与者都被假设为诚实的或恶意的.2004 年,Halpern 和 Teague[3] 将博弈论与秘密共享相结合,首次提出理性秘密共享的概念.在理性秘密共享方案中,参与者都是"理性"的.他们提出了基于随机交互次数的(t,n)理性秘密共享方案.但是,该方案不适用于(2,2)门限情况.2006 年,Gordon 和 Kazt[4] 改进了 Halpern 和 Teague 的方案,引入活跃参与者,通过适当选取秘密分发者分发正确共享主秘密的概率,首次基于同步信道实现(2,2)理性秘密共享.随后,关于理性秘密共享的研究也取得了一定的成果[5~9].然而,这些研究都是基于完全信息博弈模型展开的.2011 年,Tian 等[10] 用贝叶斯博弈研究理性秘密共享方案中理性参与

收稿日期:2013-06-18;修回日期:2014-04-02;责任编辑:覃怀银
基金项目:国家自然科学基金项目(No.60963023,No.61262073,No.61363068);贵州省自然科学基金项目(No.20092113,No.20132112);贵州大学引进人才科研项目(No.2012024);贵州大学研究生创新基金资助项目(No.2013017,No.2013018)

者不合作的问题,提出一个基于同步信道的一次理性秘密共享方案.2013 年,Zhang 等[11]首次将不完全信息博弈模型与理性秘密共享相结合,引入序贯均衡的概念用于设计理性秘密共享方案.然而,在他们的方案中,依然采用了同步信道,并要求秘密分发者保持在线.

机制设计是考虑构造怎样的博弈,使得该博弈的均衡解是社会目标,主要涉及信息效率和激励相容两个方面的问题.激励相容是指在给定机制下,真实报告自己的个人信息是参与者的占优策略均衡.机制设计已被广泛的运用到计算机领域[12~14].然而,在现有的理性秘密共享方案[15,16]的研究中,虽已多次使用"机制"一词,但都还未将机制设计的相关理论运用到理性秘密共享的研究中.

本文首先结合文献[3]和文献[17]中两种不同的理性参与者偏好模型,同时考虑理性参与者的眼前利益和长远利益,分析理性参与者在既希望获得眼前利益又希望获得长远利益时的偏好收益.结合不完全信息动态博弈模型中的完美贝叶斯均衡,研究异步信道中,(2,2)不完全信息理性秘密共享重构阶段中参与者的信念系统,计算期望收益,分析完美贝叶斯均衡策略.引入 VCG(Vickrey-Clarke-Groves)机制,设计一个有效约束理性参与者"自利性"行为的激励相容的交互记录机制,并基于该机制提出一个公平的(2,2)贝叶斯理性秘密共享方案.在该方案中利用拉格朗日插值法将子秘密拆分为影子秘密进行交互的方法,解决现有方案中要求理性秘密分发者保持在线的问题.

2 准备知识

2.1 完美贝叶斯均衡

一个策略—信念系统组合($\text{pure}\_s;\rho$)是一个完美贝叶斯均衡[18],如果它满足:

(1)在每一个信息集中,行动的参与者必须对博弈进行到该信息集中的哪个节点有一个"推断";

(2)给定参与者的推断,参与者的策略必须满足序贯理性的要求;

(3)在处于均衡路径之上的信息集中,由贝叶斯法则及参与者的均衡策略给出"推断";

(4)对处于均衡路径之外的信息集,由贝叶斯法则以及可能情况下的参与者的均衡战略决定"推断".

2.2 VCG 机制

VCG 机制[19]是一类在拟线性效用环境下满足个人理性的策略一致机制.

3 (2,2)理性秘密共享重构阶段的贝叶斯分析

令 $P=\{P_1,P_2\}$ 为理性参与者集合,$R=\{r_1,r_2\}$ 是参与者信誉值集合,其中 r_i 是参与者 P_i 的信誉值.在本文中,假设理性参与者 P_i 拥有足够的耐性追求自己利益的最大化.

假设理性参与者使用拉格朗日插值法将子秘密拆分成影子秘密后进行交互.当参与者 P_i 收到子秘密 S_i 后,利用拉格朗日插值法将子秘密 S_i 拆分成影子秘密 s_{i1} 和 s_{i2}.若 $r_i \leqslant r_{\_i}$,此时在秘密重构阶段参与者 P_i 率先将自己拥有的影子秘密传递给参与者 $P_{\_i}$.当秘密重构完成后由 $P_{\_i}$ 率先对 r_i 进行修改(把 $P_{\_i}$ 不改变 r_i 认为是降低 r_i 的一种特殊情况).

3.1 参与者偏好收益

本文同时考虑理性参与者的眼前利益(是否获得共享主秘密)和长远利益(信誉值是否得到提高).假设理性参与者 P_i 的收益如表 1 所示:

表 1 理性参与者的偏好收益

P_i 的收益	P_i 是否获得秘密	$P_{_i}$是否获得秘密	r_i 是否获提高	$r_{_i}$是否获提高	P_i 的收益	P_i 是否获得秘密	$P_{_i}$是否获得秘密	r_i 是否获提高	$r_{_i}$是否获提高
$u_i^{(1)}$	是	否	提高	降低	$u_i^{(9)}$	否	否	提高	降低
$u_i^{(2)}$	是	否	提高	提高	$u_i^{(10)}$	否	否	提高	提高
$u_i^{(3)}$	是	是	提高	降低	$u_i^{(11)}$	否	是	提高	降低
$u_i^{(4)}$	是	是	提高	提高	$u_i^{(12)}$	否	是	提高	提高
$u_i^{(5)}$	是	否	降低	降低	$u_i^{(13)}$	否	否	降低	降低
$u_i^{(6)}$	是	否	降低	提高	$u_i^{(14)}$	否	否	降低	提高
$u_i^{(7)}$	是	是	降低	降低	$u_i^{(15)}$	否	是	降低	降低
$u_i^{(8)}$	是	是	降低	提高	$u_i^{(16)}$	否	是	降低	提高

则对于参与者 P_i 来说,其偏好收益为:

$$u_i^{(1)}>u_i^{(2)}>u_i^{(3)}>u_i^{(4)}>u_i^{(5)}>u_i^{(6)}>u_i^{(7)}>u_i^{(8)}>u_i^{(9)}>u_i^{(10)}>u_i^{(11)}>u_i^{(12)}>u_i^{(13)}>u_i^{(14)}>u_i^{(15)}>u_i^{(16)}.$$

3.2 参与者类型

令 $\Theta=\Theta_1\times\Theta_2$ 是理性参与者类型组合,其中 $\Theta_i=\{\theta_i^h,\theta_i^d\}$,表示参与者 $P_i(1\leqslant i\leqslant 2)$ 的类型空间.θ_i^h 表示

参与者 P_i 的类型是诚实的,θ_i^d 表示参与者 P_i 的类型是不诚实的.

假设 μ_i 是理性参与者 $P_i(1\leqslant i\leqslant 2)$类型空间 Θ_i 的概率分布,则有:

$\mu_1^h=\text{Prob}(\theta_1^h\mid r_1,r_2)$,$\mu_1^d=\text{Prob}(\theta_1^d\mid r_1,r_2)$,使得 $\mu_1^h+\mu_1^d=1$;

$\mu_2^h=\text{Prob}(\theta_2^h\mid r_1,r_2)$,$\mu_2^d=\text{Prob}(\theta_2^d\mid r_1,r_2)$,使得 $\mu_2^h+\mu_2^d=1$.

3.3　参与者策略和信念系统

令 $A=\{A_1,A_2\}$表示理性参与者的行为集合,其中 $A_i=\{a_{i1},a_{i2},a_{i3},a_{i4},a_{i5},a_{i6}\}$表示参与者 P_i 的行为集合.$a_{ij}(1\leqslant i,j\leqslant 2)$表示参与者 P_i 传递正确的影子秘密 s_{ij}给 P_j;$a_{i3}(1\leqslant i\leqslant 2)$表示参与者 P_i 传递完整的子秘密 S_i 给 P_j;$a_{i4}(1\leqslant i\leqslant 2)$表示参与者 P_i 退出协议;$a_{i5}(1\leqslant i\leqslant 2)$表示参与者 P_i 提高理性参与者 P_j 的信誉值;$a_{i6}(1\leqslant i\leqslant 2)$表示参与者 P_i 传递错误的影子秘密 s_{i1}给 P_j.用 $\langle a_{ik},a_{il}\rangle$表示参与者 P_i 在选择行为 a_{ik}后,又立即选择行为 a_{il}.在(2,2)理性秘密共享重构博弈阶段中,不妨设 $r_1\leqslant r_2$,则(2,2)理性秘密共享重构阶段博弈如图 1 所示,其中"●"表示博弈终止.

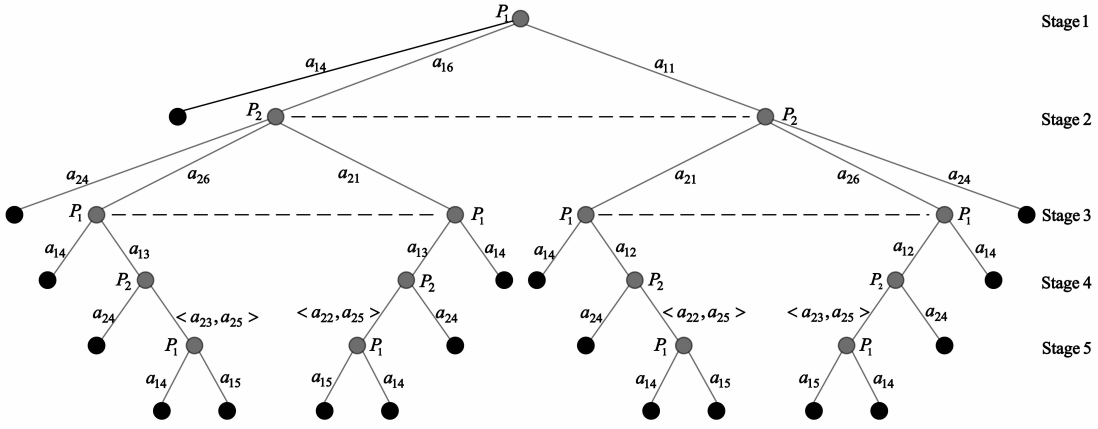


图1　(2,2)贝叶斯理性秘密共享重构阶段博弈

理性参与者 P_1 的纯策略为:

$\text{pure}\_s_1\in\text{pure}\_S_1=\{(\text{pure}\_s_1^{(1)},\text{pure}\_s_1^{(2)},\text{pure}\_s_1^{(3)})_h,(\text{pure}\_s_1^{(1)},\text{pure}\_s_1^{(2)},\text{pure}\_s_1^{(3)})_d\}$

其中,$(\text{pure}\_s_1^{(1)},\text{pure}\_s_1^{(2)},\text{pure}\_s_1^{(3)})_h$ 表示 P_1 是诚实时采取的纯策略;

$(\text{pure}\_s_1^{(1)},\text{pure}\_s_1^{(2)},\text{pure}\_s_1^{(3)})_d$ 表示 P_1 是不诚实时采取的纯策略.

并且,$\text{pure}_s_1^{(1)}\in\{a_{11},a_{16}\}$表示 P_1 在秘密共享重构阶段 Stage 1 采取的行为;

$\text{pure}_s_1^{(3)}\in\{a_{12},a_{13},a_{14}\}$表示 P_1 在秘密共享重构阶段 Stage 3 采取的行为;

$\text{pure}_s_1^{(5)}\in\{a_{14},a_{15}\}$表示 P_1 在秘密共享重构阶段 Stage 5 采取的行为.

理性参与者 P_2 的纯策略为:

$\text{pure}\_s_2\in\text{pure}\_S_2=\{(\text{pure}\_s_2^{(1)},\text{pure}\_s_2^{(2)})_h,(\text{pure}\_s_2^{(1)},\text{pure}\_s_2^{(2)})_d\}$

其中,$(\text{pure}\_s_2^{(1)},\text{pure}\_s_2^{(2)})_h$ 表示 P_2 是诚实时的采取的纯策略;

$(\text{pure}\_s_2^{(1)},\text{pure}\_s_2^{(2)})_d$ 表示 P_2 是不诚实时的采取的纯策略.

并且,$\text{pure}_s_2^{(2)}\in\{a_{21},a_{26}\}$表示 P_2 在秘密共享重构阶段 Stage 2 采取的行为;

$\text{pure}_s_2^{(4)}\in\{\langle a_{22},a_{25}\rangle,a_{24}\}$表示 P_2 在秘密共享重构阶段 Stage 4 采取的行为.

利用"海萨尼转换"分析上述博弈.令"自然"N(用"○"表示)首先确定理性参与者 P_1 的类型(如图 2 所示).

在上述贝叶斯博弈中,P_2 的信念是关于 P_1 的行为的概率分布:

(1)在 Stage 1 时,$\alpha_1^h,\alpha_1^d:\Theta_1\to\Delta(A_1)$,满足:

$\alpha_1^h(a_{11})+\alpha_1^h(a_{16})=1$,$\alpha_1^d(a_{11})+\alpha_1^d(a_{16})=1$;

(2)在 Stage 3 时,$\beta_1^h,\beta_1^d:\Theta_1\to\Delta(A_1)$,满足:

$\beta_1^h(a_{12}\mid a_{11})+\beta_1^h(a_{14}\mid a_{11})=1$,$\beta_1^d(s_{12}\mid s_{11})+\beta_1^d(\text{quit}_1\mid s_{11})=1$

并且 P_2 相信:$\text{Prob}_2(a_{13}\mid a_{16},\theta_1^h)=0$,$\text{Prob}_2(a_{14}\mid a_{16},\theta_1^h)=1$;$\text{Prob}_2(a_{13}\mid a_{16},\theta_1^d)=0$,$\text{Prob}_2(a_{14}\mid a_{16},\theta_1^d)=1$.

(3)在 Stage 5 时,$\gamma_1^h,\gamma_1^d:\Theta_1\to\Delta(A_1)$,满足:

$\gamma_1^h(a_{15}\mid a_{12})+\gamma_1^h(a_{14}\mid a_{12})=1$,$\gamma_1^d(a_{15}\mid a_{12})+\gamma_1^d(a_{15}\mid a_{12})=1$

并且 P_2 相信:$\text{Prob}_2(a_{15}\mid a_{12},a_{11},\theta_1^h)=1$,$\text{Prob}_2(a_{14}\mid a_{12},a_{11},\theta_1^h)=0$.

同样地,P_1 的信念是关于 P_2 的行为的概率分布:

(1)在 Stage 2 时,$\alpha_2^h,\alpha_2^d:\Theta_2\to\Delta(A_2)$,满足:

$\alpha_2^h(a_{21})+\alpha_2^h(a_{26})=1$,$\alpha_2^d(a_{21})+\alpha_2^d(a_{26})=1$;

(2)在 Stage 4 时,$\beta_2^h,\beta_2^d:\Theta_2\to\Delta(A_2)$,满足:

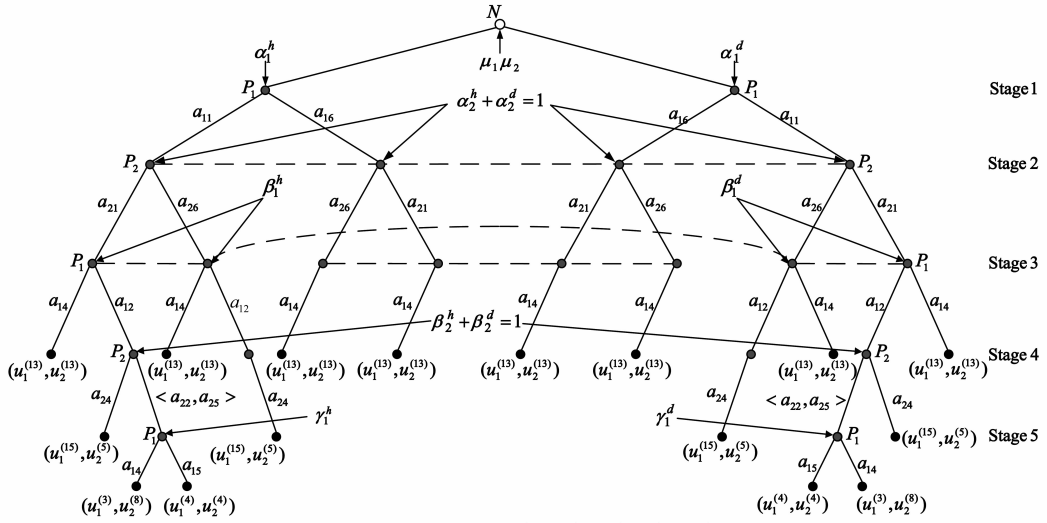


图2 (2,2)贝叶斯理性秘密共享重构博弈

$\beta_2^h(\langle a_{22}, a_{25}\rangle \mid a_{21}) + \beta_2^h(a_{24} \mid a_{21}) = 1$, $\beta_2^d((a_{22}, a_{25}) \mid a_{21}) + \beta_2^d(a_{24} \mid a_{21}) = 1$

并且 P_1 相信: $\mathrm{Prob}_1(\langle a_{23}, a_{25}\rangle \mid a_{26}, \theta_2^h) = 0$, $\mathrm{Prob}_1(a_{24} \mid a_{26}, \theta_2^h) = 1$;

$\mathrm{Prob}_1(\langle a_{23}, a_{25}\rangle \mid a_{26}, \theta_2^d) = 0$, $\mathrm{Prob}_1(a_{24} \mid a_{26}, \theta_2^d) = 1$;

$\mathrm{Prob}_1(\langle a_{23}, a_{25}\rangle \mid a_{21}, \theta_2^d) = 0$, $\mathrm{Prob}_1(a_{24} \mid a_{21}, \theta_2^d) = 1$;

$\mathrm{Prob}_1(a_{24} \mid a_{21}, \theta_2^h) = 0$, $\mathrm{Prob}_1(\langle a_{23}, a_{25}\rangle \mid a_{21}, \theta_2^h) = 1$.

3.4 理性参与者的期望收益

令 $\mathrm{EU}(\theta_i, \mathrm{pure}\_s_i)$ 表示理性参与者 P_i 在其采用纯策略 pure_s_i 时的期望收益. 则参与者 P_1 在 Stage 1 时选择行为 a_{11} 和 a_{16} 的期望收益为:

$$\begin{aligned}\mathrm{EU}(\theta_1^h, a_{11}) &= \mu_2^h \times [\alpha_2^h(a_{21})(u_1^{(13)} + u_1^{(4)}) + \alpha_2^h(a_{26})(u_1^{(13)} + u_1^{(15)})] \\ &\quad + \mu_2^d \times [\alpha_2^d(a_{21})(u_1^{(13)} + u_1^{(15)}) + \alpha_2^d(a_{26})(u_1^{(13)} + u_1^{(15)})] \\ &= u_1^{(13)} + u_1^{(15)} + (u_1^{(4)} - u_1^{(15)})\mu_2^h\alpha_2^h(a_{21});\end{aligned}$$

$$\begin{aligned}\mathrm{EU}(\theta_1^h, a_{16}) &= \mu_2^h \times [\alpha_2^h(a_{21})u_1^{(13)} + \alpha_2^h(a_{26})u_1^{(13)}] + \mu_2^d \\ &\quad \times [\alpha_2^d(a_{21})u_1^{(13)} + \alpha_2^d(a_{26})u_1^{(13)}] \\ &= u_1^{(13)};\end{aligned}$$

$$\begin{aligned}\mathrm{EU}(\theta_1^d, a_{11}) &= \mu_2^h \times [\alpha_2^h(a_{21})(u_1^{(13)} + u_1^{(4)} + u_1^{(3)}) + \alpha_2^h(a_{26})(u_1^{(13)} + u_1^{(15)})] + \mu_2^d \times [\alpha_2^d(a_{21})(u_1^{(13)} + u_1^{(15)}) + \alpha_2^d(a_{26})(u_1^{(13)} + u_1^{(15)})] \\ &= u_1^{(13)} + u_1^{(15)} + (u_1^{(3)} + u_1^{(4)} - u_1^{(15)})\mu_2^h\alpha_2^h(a_{21});\end{aligned}$$

$$\begin{aligned}\mathrm{EU}(\theta_1^d, a_{16}) &= \mu_2^h \times [\alpha_2^h(a_{21})u_1^{(13)} + \alpha_2^h(a_{26})u_1^{(13)}] + \mu_2^d \times [\alpha_2^d(a_{21})u_1^{(13)} + \alpha_2^d(a_{26})u_1^{(13)}] \\ &= u_1^{(13)}.\end{aligned}$$

显然, $\mathrm{EU}(\theta_1^h, a_{11}) > \mathrm{EU}(\theta_1^h, a_{16})$; $\mathrm{EU}(\theta_1^d, a_{11}) > \mathrm{EU}(\theta_1^d, a_{16})$. 所以理性参与者 P_1 在 Stage 1 时将不会选择行为 a_{16}.

同理, 理性参与者 P_2 在 Stage 2 时将不会选择行为 a_{26}.

在(2,2)贝叶斯理性秘密共享重构博弈 Stage 3 时理性参与者 P_1 的期望收益为:

$$\begin{aligned}\mathrm{EU}(\theta_1^h, \{(a_{11}), (a_{12})\}) &= \mu_2^h\alpha_2^h(a_{21})u_1^{(4)} + \mu_2^d\alpha_2^d(a_{21})u_1^{(15)} + \mu_2^h\alpha_2^h(a_{26})u_1^{(15)} + \mu_2^d\alpha_2^d(a_{26})u_1^{(15)} \\ &= u_1^{(15)} + \tilde{L}\mu_2^h \qquad (1)\end{aligned}$$

其中, $\tilde{L} = \alpha_2^h(a_{21})u_1^{(4)} - \alpha_2^d(a_{21})u_1^{(15)}$ (2)

$$\mathrm{EU}(\theta_1^h, \approx) = 2u_1^{(13)} \qquad (3)$$

"$\approx$"表示理性参与者的纯策略 $(\mathrm{pure}\_s_1^{(1)} \setminus a_{11}, \mathrm{pure}\_s_1^{(2)} \setminus a_{12}, \mathrm{pure}\_s_1^{(3)})_h$.

推论 1 在上述(2,2)贝叶斯理性秘密共享博弈 Stage 3 中, 如果 $\mu_2^h > \dfrac{2u_1^{(13)} - u_1^{(15)}}{\tilde{L}}$, 则理性参与者 P_1 在上述博弈中, 将会选择行为 a_{12}; 否则, 就会选择行为 a_{14}.

证明 由上述式(1)和式(3)知, 当 $\mathrm{EU}(\theta_1^h, \{a_{11}, a_{12}\}) > \mathrm{EU}(\theta_1^h, \approx)$ 时, 即: $\mu_2^h > \dfrac{2u_1^{(13)} - u_1^{(15)}}{\tilde{L}}$ 时, 理性参

与者 P_1 由于其“自利性”,将会选择行为 a_{12}.

在(2,2)贝叶斯理性秘密共享重构博弈 Stage 4 时理性参与者 P_2 的期望收益为:

$$\begin{aligned}\mathrm{EU}(\theta_2^h,\mathrm{pure}\_s_2)=&\mu_1^h\times[\alpha_1^h(a_{16})(u_2^{(13)}+u_2^{(13)})\\&+\alpha_1^h(a_{11})(\beta_1^h(a_{14}\mid a_{11})u_2^{(13)}\\&+\beta_1^h(a_{12}\mid a_{11})u_2^{(4)}\\&+\beta_1^h(a_{14}\mid a_{11})u_2^{(13)}\\&+\beta_1^h(a_{12}\mid a_{11})u_2^{(5)})]\\&+\mu_1^d\times[\alpha_1^d(a_{16})(u_2^{(13)}+u_2^{(13)})\\&+\alpha_1^d(a_{11})(\beta_1^d(a_{14}\mid a_{11})u_2^{(13)}\\&+\beta_1^d(a_{12}\mid a_{11})(\gamma_1^d(a_{15}\mid a_{12})u_2^{(4)}\\&+\gamma_1^d(a_{14}\mid a_{12})u_2^{(8)})\\&+\beta_1^d(a_{14}\mid a_{11})u_2^{(13)}\\&+\beta_1^d(a_{12}\mid a_{11})u_2^{(5)})]\\=&2u_2^{(13)}+\mu_1^hL_1+L_2\end{aligned}\tag{4}$$

其中,$L_1=L_3-L_2$; (5)

$$\begin{aligned}L_2=&[u_2^{(5)}+u_2^{(8)}-2u_2^{(13)}\\&+(u_2^{(4)}-u_2^{(8)})\gamma_1^d(a_{15}\mid a_{12})]\alpha_1^d(a_{11})\beta_1^d(a_{12}\mid a_{11})\end{aligned}\tag{6}$$

$$L_3=(u_2^{(4)}+u_2^{(5)}-2u_2^{(13)})\alpha_1^h(a_{11})\beta_1^h(a_{12}\mid a_{11})\tag{7}$$

$$\begin{aligned}\mathrm{EU}(\theta_2^d,\mathrm{pure}\_s_2)=&\mu_1^h\times[\alpha_1^h(a_{16})(u_2^{(13)}+u_2^{(13)})\\&+\alpha_1^h(a_{11})(\beta_1^h(a_{14}\mid a_{11})u_2^{(13)}\\&+\beta_1^h(a_{12}\mid a_{11})u_2^{(5)}\\&+\beta_1^h(a_{14}\mid a_{11})u_2^{(13)}\\&+\beta_1^h(a_{12}\mid a_{11})u_2^{(5)})]\\&+\mu_1^d\times[\alpha_1^d(a_{16})(u_2^{(13)}+u_2^{(13)})\\&+\beta_1^d(a_{12}\mid a_{11})u_2^{(5)}\\&+\alpha_1^d(a_{11})(\beta_1^d(a_{14}\mid a_{11})u_2^{(13)}\\&+\beta_1^d(a_{14}\mid a_{11})u_2^{(13)}\\&+\beta_1^d(a_{12}\mid a_{11})u_2^{(5)})]\\=&2u_2^{(13)}+\mu_1^hL_1'+L_2'\end{aligned}\tag{8}$$

其中,$L_1'=L_3'-L_2'$; (9)

$$L_2'=(2u_2^{(5)}-2u_2^{(13)})\alpha_1^d(a_{11})\beta_1^d(a_{12}\mid a_{11})\tag{10}$$

$$L_3'=(2u_2^{(5)}-2u_2^{(13)})\alpha_1^h(a_{11})\beta_1^h(a_{12}\mid a_{11})\tag{11}$$

推论 2　在上述(2,2)贝叶斯理性秘密共享重构博弈中,如果 $\mu_1^h>\dfrac{L_2'-L_2}{L_1-L_1'}$,则理性参与者 P_2 在上述博弈 Stage 4 时,将会选择行为$\langle a_{22},a_{25}\rangle$;否则,就会选择行为 a_{24}.

证明　由上述式(4)和式(8)知,当 $\mathrm{EU}(\theta_2^h,\mathrm{pure}_s_2)>\mathrm{EU}(\theta_2^d,\mathrm{pure}_s_2)$时,即:$\mu_1^h>\dfrac{L_2'-L_2}{L_1-L_1'}$时,理性参与者由于其“自利性”,将会选择行为$\langle a_{22},a_{25}\rangle$;否则,就会选择行为 a_{24}.

3.5　(2,2)贝叶斯理性秘密共享重构博弈完美贝叶斯均衡

(2,2)理性秘密共享重构博弈的完美贝叶斯均衡是使得对于理性参与者 P_1 在信息集 I_1^1,I_1^2,理性参与者 P_2 在信息集 I_2^1 处的行为是对于其余参与者的任意行为都是最优反应.因此,当 $\mu_1^{h^*}>\dfrac{L_2'^*-L_2^*}{L_1^*-L_1'^*}$,$\mu_2^{h^*}>\dfrac{2u_1^{(13)}-u_1^{(15)}}{\tilde{L}^*}$,其中 L_1^*,$L_1'^*$,L_2^*,$L_2'^*$,$\tilde{L}^*$ 满足式(2)、(5)、(6)、(7)、(9)、(10)、(11),$\rho^*=(\mu_1^*,\mu_2^*,\alpha_1^{h^*},\alpha_1^{d^*},\alpha_2^{h^*},\alpha_2^{d^*},\beta_1^{h^*},\beta_1^{d^*},\beta_2^{h^*},\beta_2^{d^*},\gamma_1^{h^*},\gamma_1^{d^*})$时:

$(\mathrm{pure}_s^*;\rho^*)=(\{(a_{11},a_{12},a_{15})_h,(a_{11},a_{12},a_{14})_d\},\{(a_{21},\langle a_{22},a_{25}\rangle)_h,(a_{21},\langle a_{22},a_{25}\rangle)_d\};\rho^*)$是一个候选的完美贝叶斯均衡;

当 $\mu_1^{h^\circ}<\dfrac{L_2'^\circ-L_2^\circ}{L_1^\circ-L_1'^\circ}$,$\mu_2^{h^\circ}<\dfrac{2u_1^{(13)}-u_1^{(15)}}{\tilde{L}^\circ}$,其中 L_1°,$L_1'^\circ$,L_2°,$L_2'^\circ$,$\tilde{L}^\circ$满足式(2)、(5)、(6)、(7)、(9)、(10)、(11),$\rho^*=(\mu_1^\circ,\mu_2^\circ,\alpha_1^{h^\circ},\alpha_1^{d^\circ},\alpha_2^{h^\circ},\alpha_2^{d^\circ},\beta_1^{h^\circ},\beta_1^{d^\circ},\beta_2^{h^\circ},\beta_2^{d^\circ},\gamma_1^{h^\circ},\gamma_1^{d^\circ})$时:

$(\mathrm{pure}\_s^\circ;\rho^\circ)=(\{(a_{14})_h,(a_{14})_d\},\{(a_{14})_h,(a_{14})_d\};\rho^\circ)$

也是一个候选的完美贝叶斯均衡.

定理 1　策略和信念系统组合$(\mathrm{pure}_s^*;\rho^*)$是(2,2)贝叶斯理性秘密共享重构博弈完美贝叶斯均衡.

证明　先证参与者在每个信息集合中都有一个“推断”.

在(2,2)理性秘密共享重构博弈 Stage 2 时,理性参与者 P_2 选择 $\alpha_1^{h^*}$ 和 $\alpha_1^{d^*}$,使得:

$\alpha_1^{h^*}(a_{11})+\alpha_1^{h^*}(a_{16})=1$,$\alpha_1^{d^*}(a_{11})+\alpha_1^{d^*}(a_{16})=1$

又因为 $\mu_1^{h^*}+\mu_1^{d^*}=1$

所以 $\mu_1^{h^*}\alpha_1^{h^*}(a_{11})+\mu_1^{h^*}\alpha_1^{h^*}(a_{16})+\mu_1^{d^*}\alpha_1^{d^*}(a_{11})+\mu_1^{d^*}\alpha_1^{d^*}(a_{16})=1$

在 Stage 3 时,理性参与者 P_1 选择 $\alpha_2^{h^*}$ 和 $\alpha_2^{d^*}$,对于信息集合 I_1^1、I_1^2 使得:

$\alpha_2^{h^*}(a_{21})+\alpha_2^{h^*}(a_{26})=1$,$\alpha_2^{d^*}(a_{21})+\alpha_2^{d^*}(a_{26})=1$

又因为 $\mu_2^{h^*}+\mu_2^{d^*}=1$

所以 $\mu_2^{h^*}\alpha_2^{h^*}(a_{21})+\mu_2^{h^*}\alpha_2^{h^*}(a_{26})+\mu_2^{d^*}\alpha_2^{d^*}(a_{21})+\mu_2^{d^*}\alpha_2^{d^*}(a_{26})=1$

所以理性参与者在每一个信息集合都有一个“推断”.

再证给定参与者的“推断”,其策略满足序贯理性.

令 $\mathrm{BG}^{(2)}$表示理性参与者 P_2 到达信息集 I_2 后的博弈,当 $\mu_1^{h^*}>\dfrac{L_2'^*-L_2^*}{L_1^*-L_1'^*}$时,由式(4)、(8)知:$\mathrm{EU}(\theta_2,a_{21},$

$BG^{(2)}) > EU(\theta_2, a_{26}, BG^{(2)})$;

令 $BG^{(1)}$表示理性参与者 P_1 到达信息集 $I_1^{(1)}$ 后的博弈,当 $\mu_2^{h*} > \frac{2u_1^{(13)} - u_1^{(15)}}{\tilde{L}^*}$时,由式(1)、(3)知:$EU(\theta_1, a_{12}, BG^{(1)}) > EU(\theta_2, a_{14}, BG^{(2)})$

在(2,2)理性秘密共享重构博弈 Stage 2 时,P_2 相信 P_1 其类型是 θ_1^h 时,在 Stage 1 选择行为 a_{11}的概率是 σ^h,选择行为 a_{16}的概率是 ζ^h,则其选择行为 a_{14}的概率是 $1 - \sigma^h - \zeta^h$.

所以 $\alpha_1^{h*}(a_{11})$和 $\alpha_1^{h*}(a_{16})$应满足:$\alpha_1^{h*}(a_{11}) = \frac{\sigma^h}{\sigma^h + \zeta^h}, \alpha_1^{h*}(a_{16}) = \frac{\zeta^h}{\sigma^h + \zeta^h}$

同理,$\alpha_1^{d*}(a_{11})$和 $\alpha_1^{d*}(a_{16})$应满足:

$$\alpha_1^{d*}(a_{11}) = \frac{\sigma^d}{\sigma^d + \zeta^d}, \alpha_1^{d*}(a_{16}) = \frac{\zeta^d}{\sigma^d + \zeta^d}$$

P_1 在信息集 $I_1^{(1)}$ 时也具有:

$$\alpha_2^{h*}(a_{21}) = \frac{\xi^h}{\xi^h + \psi^h}, \alpha_1^{h*}(a_{26}) = \frac{\psi^h}{\xi^h + \psi^h}; \alpha_1^{d*}(a_{21}) = \frac{\xi^d}{\xi^d + \psi^d}, \alpha_1^{d*}(a_{26}) = \frac{\xi^d}{\xi^d + \psi^d}$$

其中,当 P_2 类型是 θ_2^h 时,选择行为 a_{21}的概率为 ξ^h,选择行为 a_{26}的概率为 ψ^h;

当 P_2 类型是 θ_2^d 时,选择行为 a_{21}的概率为 ξ^d,选择行为 a_{26}的概率为 ψ^d;

对于不处于均衡路径上的信息集 $I_1^{(2)}$,当 P_1 在信息集 $I_1^{(2)}$ 时也具有:

$$\alpha_2^{h*}(a_{21}) = \frac{\xi^h}{\xi^h + \psi^h}, \alpha_1^{h*}(a_{26}) = \frac{\psi^h}{\xi^h + \psi^h}; \alpha_1^{d*}(a_{21}) = \frac{\xi^d}{\xi^d + \psi^d}, \alpha_1^{d*}(a_{26}) = \frac{\xi^d}{\xi^d + \psi^d}$$

所以,策略和信念系统组合$(pure_s^*; \rho^*)$是(2,2)贝叶斯理性秘密共享重构博弈完美贝叶斯均衡.

4 交互记录机制

定义 1(交互记录机制) 交互记录机制 $M = (\tilde{A}_{j,i}, e_{j,i})$,其中:

(1)$\tilde{A}_{j,i} = \{\tilde{A}_{j,i}^{b(1)}, \cdots, \tilde{A}_{j,i}^{b(k)}\}$表示参与者 P_j 所记录的 P_i 在此次交互活动中所采取的行为,其中 $\tilde{A}_{j,i}^{b(l)}$是参与者 P_j 记录 P_i 在第 $l(1 \leqslant l \leqslant k)$轮中所采取是策略;

(2)$e_{j,i}$表示在每次交互活动完成后,参与者 $P_j(i \neq j)$根据本次交互活动对 P_i 的交互记录评价.该评价对于所有参与者是公开可见的,参与者 P_i 无权对其进行修改.

当交互完成后,理性参与者 $P_j(i \neq j)$根据本次交互活动记录 P_i 的行为,并对其进行评价 $e_{j,i}$.令 $\lambda > 0$ 为一正整数,则:$e_{j,i} = \begin{cases} \lambda, & P_i \text{ 是诚实的} \\ -\lambda, & P_i \text{ 是不诚实的} \end{cases}$.

定理 2 交互记录机制 $M = (\tilde{A}_{j,i}, e_{j,i})$是激励相容机制.

证明 理性参与者 P_i 在该机制下的收益为 $v_i(a, \theta_i) = u_i(a, \theta_i) + w_i e_{j,i}$,其中 w_i 表示理性参与者 P_i 对参与者 P_j 的评价 $e_{j,i}$的看重程度.

社会选择函数:$Soc(a_i, e_{j,i}) = u_i(a, \boldsymbol{\theta})$.其中,

参与者的目标函数为:

$$g(a_i, e_{j,i}) = \arg\max_{a_i \in \tilde{A}_{j,i}} [Soc_i(a_i, e_{j,i})] \quad (12)$$

使得:$u_i(a, \boldsymbol{\theta}) \geq u_j(a, \boldsymbol{\theta})$.

因此,

$$u_i = v_i(a, \theta_i) - [Soc(a, e_{j,i}) - Soc(a, e_{j,-i})] \quad (13)$$

由式(12)、(13)可知机制 $M = (\tilde{A}_{j,i}, e_{j,i})$满足 VCG 机制的分配规则和支付规则.

所以,交互记录机制 $M = (\tilde{A}_{j,i}, e_{j,i})$是激励相容机制

5 (2,2)贝叶斯理性秘密共享方案

本文利用承诺函数来构造公平的(2,2)贝叶斯理性秘密共享方案.承诺函数 $C(\cdot)$是一个单向函数,可在确保秘密信息不被泄露的情况下,为秘密信息的正确性提供验证.为了简单,假设共享秘密 $S = S_1 \oplus S_2$ 时,承诺函数 $C(S) = C(S_1) \oplus C(S_2)$.

(1)秘密分发协议 π_{Dis}

Step1 Dealer 选择拉格朗日多项式,将 S 拆分成 S_1 和 S_2,并计算 $C(S), C(S_1)$和 $C(S_2)$;

Step2 Dealer 将 S_i 秘密地发送给参与者 P_i,并广播 $C(S), C(S_1)$和 $C(S_2)$;

(2)秘密重构协议 π_{Rec}

Step1 参与者 P_i 将收到的子秘密 S_i 用拉格朗日插值法将子秘密 S_i 拆分成影子秘密 s_{i1}和 s_{i2};

Step2 若 $r_i = \min\{r_1, r_2\}$,则参与者 P_i 将影子秘密 s_{i1}传递 P_{-i},否则,参与者 P_{-i}将影子秘密 s_{-i1}传递给 P_i;

Step3 参与者 P_{-i}收到 P_i 传递的影子秘密 s_{i1}后,传递影子秘密 s_{-i1}给 P_i,否则,使用交互记录机制 M,并返回 Step1;

Step4 参与者 P_i 收到 P_{-i}传递的影子秘密 s_{-i1}后,传递影子秘密 s_{i2}给 P_{-i},否则,使用交互记录机制 M,并返回 Step1;

Step5 参与者 P_{-i}收到影子秘密 s_{i2}后,重构子秘密 S_i',验证 $C(S_i')$:如果 $C(S_i) = C(S_i')$,则传递影子秘密 s_{-i2}给 P_i,提升 r_i,否则,就执行交互记录机制 M,并返回 Step1;

Step6　参与者 P_i 收到 s_{-i2} 后,重构子秘密 S'_{-i},验证 $C(S'_{-i})$:如果 $C(S_{-i})=C(S'_{-i})$,则提升 r_{-i},使用交互记录机制 M,否则,使用交互记录机制 M;

Step7　参与者 P_{-i} 使用交互记录机制 M.

下面给出方案的公平性分析:

(1)若 P_i 不发送影子秘密 s_{i1},则 P_{-i} 将执行交互记录机制 M,且 P_i 和 P_{-i} 都无法得到共享秘密 S.此时,P_i 和 P_{-i} 的收益为 $u_{-i}^{(13)}$ 和 $u_{-i}^{(13)}$;

(2)若 P_i 发送错误的影子秘密 s_{i1} 时,则 P_{-i} 将执行交互记录机制 M,且 P_i 和 P_{-i} 都无法得到共享秘密 S.此时,P_i 和 P_{-i} 的收益为 $u_{-i}^{(13)}$ 和 $u_{-i}^{(13)}$;

(3)若 P_i 发送错误的影子秘密 s_{i2} 或不发送影子秘密 s_{i2} 时,P_i 和 P_{-i} 的收益为 $u_{-i}^{(13)}$ 和 $u_{-i}^{(13)}$;

(4)若 P_i 发送正确的影子秘密 s_{i2} 后,P_{-i} 不发送影子秘密 s_{-i2}、发送错误的影子秘密 s_{-i2},或发送正确的影子秘密但降低 r_i 时,P_i 将执行交互记录机制 M.此时,P_i 的收益为 $u_i^{(15)}$ 或 $u_i^{(7)}$;P_{-i} 对应的收益为 $u_{-i}^{(5)}$ 或 $u_{-i}^{(7)}$;

(5)若 P_{-i} 发送正确的影子秘密 s_{-i2} 并提高 r_i 后,P_i 降低 r_{-i},则 P_{-i} 执行交互记录机制 M.此时,P_i 和 P_{-i} 的收益为 $u_i^{(7)}$ 和 $u_{-i}^{(7)}$;

(6)若 P_i 和 P_{-i} 都正确的执行协议,则 P_i 和 P_{-i} 的收益为 $u_i^{(4)}$ 和 $u_{-i}^{(4)}$.

通过上述分析,可以发现对于理性参与者 P_i 和 P_{-i} 来说,只有正确执行协议时,得到的收益最大,符合理性参与者的自利性.此时,理性参与者 P_i 和 P_{-i} 均可既获得共享秘密又可提升自己的信誉值.

综上所述,可得:

定理 3　基于交互记录机制 $M=(\tilde{A}_{j,i},e_{j,i})$ 的(2,2)贝叶斯理性秘密共享方案是公平的.

6　结论

公平的(2,2)理性秘密共享方案是构建适用于理性环境的各类安全协议的基础模块,如利用(2,2)理性秘密共享方案设计理性多方计算协议[20],理性交换协议[21].

本文通过理性参与者利用拉格朗日插值法将子秘密拆分成影子秘密进行交互的方法,有效地解决理性秘密分发者保持在线的问题.并利用海萨尼转换,分析理性参与者类型不确定的情况下在异步信道进行交互的信念,计算其期望均衡,给出(2,2)贝叶斯理性秘密共享重构阶段的完美贝叶斯均衡.并初步探讨结合机制设计理论中 VCG 机制,设计激励相容的交互记录机制,提出一个公平的(2,2)贝叶斯理性秘密共享方案.

参考文献

[1] SHAMIR A. How to share asecret[J]. Communications of the ACM, 1979, 22(11): 612 – 613.

[2] BLAKLEY GR. Safeguarding cryptographic keys[A]. Smith M. Proceedings of the 1979 AFIPS National Computer Conference[C]. New York: AFIPS Press, 1979. 313 – 317.

[3] HALPERN J, TEAGUE V. Rational secret sharing and multiparty computation: extended abstract[A]. Calinescu G. Proceedings of the 36th Annual ACM Symposium on Theory of Computing[C]. New York: ACM Press, 2004. 623 – 632.

[4] GORDON S D, KATZ J. Rational secret sharing revisited[A]. Yung M. LNCS4116: Proceedings of the 5th International Conference on Security and Cryptography for Networks [C]. Berlin: Springer Press, 2006. 229 – 241.

[5] ABRAHAM I, DOLEV D, GONENEN R, et al. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation[A]. Ruppert E. Proceedings of the 25th Annual ACM Symposium on Principles of Distributed Computing[C]. New York: ACM Press, 2006. 53 – 62.

[6] KATZ J. Bridging game theory and cryptography: recent results and future directions[A]. Canetti R. LNCS4948: Proceedings of the 5th Conference on Theory of Cryptography[C]. Berlin: Springer Press, 2008. 251 – 272.

[7] MALEKA S, SHAREEF A, RANGAN C. P. Rational secret sharing with repeated games[A]. Susilo W. LNCS4991: Proceedings of the 4th International Conference on Information Security Practice and Experience [C]. Berlin: Springer Press, 2008. 334 – 346.

[8] ASHAROV G, LINDELL Y. Utility dependence in correct and fair rational secret sharing[A]. Halevi S. LNCS5677: Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology[C]. Berlin: Springer Press, 2009. 559 – 576.

[9] 田有亮,马建峰,彭长根. 秘密共享体制的博弈论分析[J]. 电子学报,2011,39(12):32 – 46.
TIAN You-liang, MA Jian-feng, PENG Chang-gen. Game-theoretic analysis for the secret sharing scheme[J]. Acta Electronica Sinica, 2011, 39(12): 32 – 46. (in Chinese)

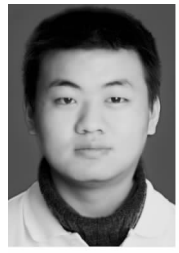
[10] TIAN You-liang, MA Jian-feng, PENG Chang-gen, et al. One-time rational secret sharing scheme based on Bayesian game [J]. Wuhan University Journal of Natural Sciences, 2011, 16(5): 430 – 434.

[11] ZHANG Zhi-fang, LIU Mu-lan. Rational secret sharing as extensive game [J]. Science China Information Sciences, 2013, 56(3): 1-13.

[12] FEIGENBAUM J, PAPADIMITRIOU C, SAMI R, et al. A bgp-based mechanism for lowest-cost routing[J]. Journal of

Distributed Computing,2005,18(1):61 – 72.
[13] FEIGENBAUM J, SHENKER S. Distributed algorithmic mechanism design: recent results and future directions[A]. Marathe M. Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobil Computing and Communication[C]. New York: ACM Press, 2002. 1 – 13.
[14] PARKES D, SHEIDMAN J. Distributed implementations ofvickrey-clarke-groves mechanisms[A]. Scerri P. Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multi-Agent Systems[C]. Washington: IEEE Computer Society Press, 2004. 261 – 268.
[15] DANIV, MOVAHEDI M, SAIA J. Scalable mechanisms for rational secret sharing[A]. Fraigniaud P. Proceedings of the 30th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing[C]. New York: ACM Press, 2012. 187 – 196.
[16] JOYEE D S, ASIM K P. Achieving correctness in fair rational secret sharing[A]. Kanade T. LNCS8257: Proceedings of the 12th International Conference on Cryptology and Network Security[C]. Berlin: Springer Press, 2013. 139 – 161.
[17] NOJOUMIAN M, STINSON D, GRAINGER M. Unconditionally secure social secret sharing scheme[J]. IET Information Security, 2010, 4(4): 202 – 211.
[18] OSBORNE M, RUBINSTEIN A. A Course in Game Theory [M]. Cambridge: MIT Press, 2004.
[19] NISAN N, RONEN A. Algorithmic mechanism design [J]. Games and Economic Behavior, 2001, 35(1/2): 166 – 196.
[20] GROCE A, KATZ J. Fair computation with rational players [A]. Johansson T. LNCS7237: Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin: Springer Press, 2012. 81 – 98.
[21] 张恩. 理性信息交换密码协议若干模型及应用研究[D]. 北京: 北京工业大学计算机学院, 2013.

作者简介



刘 海 男, 1984 年 4 月出生于贵州省贵阳市. 硕士研究生, 主要研究方向为密码学与安全协议.
E-mail: liuhai4757@163.com

彭长根(通讯作者) 男, 1963 年 8 月出生于贵州锦屏县. 现为贵州大学教授、博士生导师. 主要研究方向为密码学与信息安全.
E-mail: gzu_cgpeng@163.com