秘密共享体制的博弈论分析

田有亮[1,2],马建峰[1],彭长根[2],姬文江[1]
(1.西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071;
2.贵州大学理学院,贵州贵阳 550025)

摘 要: 本文提出理性第三方的概念,在秘密共享中任何理性的局中人都可以充当"可信中心"来分发秘密信息,这样使秘密共享体制更具有普适性.基于博弈论分析秘密分发协议,它被形式化为 n 个二人博弈.证明在这些博弈中,理性秘密分发者总是选择欺骗各局中人以获得更大的收益,同时提出解决该问题的理性秘密分发机制.最后,基于健忘传输协议提出秘密重构机制,有效解决秘密重构中各局中人的不合作问题.

关键词: 博弈论;纳什均衡;秘密共享;理性第三方
中图分类号: TP309, TN918 **文献标识码:** A **文章编号:** 0372-2112 (2011) 12-2790-06

Game-Theoretic Analysis for the Secret Sharing Scheme

TIAN You-liang[1,2], MA Jian-feng [1], PENG Chang-gen[2], JI Wen-jiang[1]
(1. *Key Laboratory of Computer Networks and Information Security* (*Ministry of Education*), *Xidian University*, *Xi'an*, *Shaanxi* 710071, *China*;
2. *College of Science Guizhou University*, *Guiyang*, *Guizhou* 550025, *China*)

Abstract: This paper proposes the concept of rational trusted party. Any rational party can be the TTP to distribute the shares in the secret sharing such that it is to be more suitable for use. As far as we know, that is firstly to analyze distribution of shares with game theory in secret sharing scheme. It is formalized as n tow-person games. It is proven that rational dealer always selects cheating all players to get more payoffs in these games. Simultaneously a rational secret distribution mechanism is proposed to solve this problem. Moreover, we construct a mechanism of reconstruction of secret based on oblivious transfer protocol, which solve the problem of players' non-cooperation in reconstruction phase.

Key words: game theory; Nash equilibrium; secret sharing; rational third party

1 引言

我们知道,秘密共享体制是针对密钥管理中密钥的泄露和遗失问题提出的.它是一种分发、保存以及恢复秘密密钥(或其它秘密信息)的方法.博弈论是应用数学的一个重要分支,它所要考虑的是各位局中人在针对其他局中人的所选策略下,怎样做决策对自己最有利.博弈环境下的局中人都假定是理性的,各位局中人掌握的信息都是对称的,而在密码协议(如秘密共享、安全多方计算等)中考虑其局中人要么是诚实的,要么是邪恶的.2004 年,Halpern 和 Teague[1] 介绍了理性秘密共享(Rational Secret Sharing)和多方计算(Multiparty Computation)问题.

在理性秘密共享方案中,每位局中人的行为都是自私的(selfish),他们有自己的偏好及效用函数,每位局中人总是尽最大可能让自己的收益最大化.在秘密共享方案中,局中人的效用是通过他们能否知道其共享的秘密来刻画的.Abraham[2] 等学者在局中人可以结盟的情况下,分析了理性秘密共享和安全多方计算问题;Lysyanskaya 和 Triandoulos[3] 在混合模型下分析了多方计算问题,其局中人要么是理性的,要么是邪恶的,邪恶的敌手至多能控制 $\lceil n/2 \rceil - 2$ 位局中人.Maleka 等学者[4] 基于重复博弈研究了理性秘密共享问题.Gilad Asharov 和 Yehuda Lindell[5] 研究了秘密共享的在博弈论环境下的效用等问题.陈晶等[6] 研究在网络环境下研究基于概率密度的信任博弈模型.可见,基于博弈论的密码协议及信息安全技术已被越来越多的学者所关注.

然而,在理性秘密共享体制中,研究者们主要关注门限结构的理性秘密共享体制,重点研究秘密重构问题,未涉及一般的秘密共享体制及秘密共享体制中的秘密分发协议.针对这些问题,本文研究假定秘密分发者(庄家)也是理性的,提出理性第三方(Rational Third Party, RTP)的概念.在理性假定下,设计理性秘密分发机制,有效防止秘密分发者的欺诈行为及秘密分发博弈达到更优的纳什均衡.分别在门限结构和一般访问结构下

收稿日期:2010-09-07;修回日期:2011-04-30
基金项目:国家科技部重大专项(No.2011ZX03005-002);国家自然科学基金(No.60872041, No.61072066, No.60963023, No.60970143);中央高校基本科研业务费项目(No.JY10000903001, No.JY10000901034)

分析秘密重构协议,当各理性局中人在更愿意得到共享秘密的偏好下,各局中人选择广播自己正确的子秘密是最佳策略.但是,在秘密重构协议中各局中人易产生不合作行为,大家都不发送自己的子密钥,这样就让大家陷入一种"僵局".博弈论中称之为空威胁(Empty threat).最后设计一个秘密重构机制解决各理性局中人的合作问题.

2 准备知识

本节介绍相关背景知识和基本概念.本节内容主要参考文献[7]和文献[8].

2.1 秘密共享

设 $P=\{P_1,\cdots,P_n\}$ 是 n 个局中人的集合,$\varnothing\neq AS\subseteq 2^P$,我们称 AS 是 P 上的存取结构(access structure),如果集合 AS 满足单调性:若 $A\in AS$,则对 $\forall A'\in 2^P$ 和 $A\subseteq A'$,有 $A'\in AS$.若 AS 是 P 上的存取结构,则 AS 中的任何集合称为 P 上的授权子集,简称授权集;对于 $2^P\setminus AS$中的任何集合,称为 P 上的非授权子集,简称非授权集.令 $AS_m=\{A\in AS\mid \forall B\in 2^P, B\cap A=\varnothing\Rightarrow B\notin AS\}$,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 $AS_m=\{A\subseteq P\mid |A|=t\}$.

定义 1(秘密共享体制) 秘密共享体制 Γ 是一个三元组 $\{P,\Pi,RE\}$,简记为 $\Gamma=\{P,\Pi,RE\}$.其中 $P=\{P_1,\cdots,P_n\}$ 是 n 个局中人的集合,AS 是 P 上的存取结构.设 $S,S_1,\cdots,S_n,R$ 是 $n+2$ 个有限集,称 S 为主秘密空间,$S_1,\cdots,S_n$ 分别为 $P_1,\cdots,P_n$ 的子密钥空间,R 是随机输入集合.Π 是秘密分发算法,由影射 $\Pi: S\times R\to S_1\times\cdots\times S_n$ 实现;重构算法 $RE=\{RE: S_1\times\cdots S_{|A|}\to S\mid A\in AS\}$,且 Π 和 RE 满足如下的条件:

(1)重构要求:对任何 $A\in AS$,$H(S\mid S_A)=0$,这里 $H(\cdot)$是熵函数,S_A 表示集合 A 中局中人的子密钥.

(2)安全性要求:对任何 $B\in 2^P\setminus AS$,$0<H(S\mid S_B)<H(S)$.

如果在条件(2)中要求 $H(S\mid S_B)=H(S)$,则称 Γ 是一个完美的秘密共享体制.

2.2 博弈论概念

下面简单介绍博弈和博弈的纳什均衡:

定义 2(博弈) 博弈表达的基本式由局中人集合 P、策略空间 S 和效用函数 u 三个要素组成,即 $G=\{P,S,u\}$,其中 $P=\{P_1,\cdots,P_n\}$,$S=\{S_1,\cdots,S_n\}$,$u=\{u_1,\cdots,u_n\}$.效用函数 $u_i: S\to R$(R 代表实数空间),它表示第 i 位局中人在不同策略组合下所得到的收益.

定义 3(纳什均衡) 一个策略组合 $\boldsymbol{s}^*=(s_1^*,\cdots,s_n^*)$是博弈 $G=\{P,S,u\}$的一个纳什均衡,如果对于每一个局中人 $P_i(i=1,\cdots,n)$,对于所有的 $s_j\in S_i$,不等式 $u_i(s_i^*,s_{-i}^*)\geqslant u_i(s_j,s_{-i}^*)$都成立.

直观的讲,如果每一个参与者 $i\neq j$ 遵从策略 s_i^*,则参与者 j 应该都不会背离 s_j^*,因为它背离该策略不会得到任何好处.一般情况下,一个博弈可能存在多个纳什均衡.

2.3 安全多方计算

多方安全计算就是:拥有秘密输入的多方,希望用各自的输入共同计算一个函数.计算要求每方都能接收到正确的输出(正确性),并且每方只能了解他们自己的输出(保密性).

一个多方安全计算协议是一个为了解决安全多方计算问题的协议.它涉及多方(k 方),每方的计算能力都限制在多项式时间上.

2.4 健忘传输协议

健忘传输协议是诸多密码算法的一个基础协议.

健忘传输 OT_1^k 协议(Oblivious Transfer: 1-out-of-k):发送者 Alice 有 k 个秘密数据($S_1,\cdots,S_k$),选择者 Bob 要选择的 k 个数据之一 $S_i(1\leqslant i\leqslant k)$.在协议结束后,Alice 不知道哪个数是 Bob 需要的,Bob 不知道 Alice 的另外任意一个数的信息.

3 秘密共享体制分析

3.1 效用函数分析

3.1.1 庄家的效用分析

在秘密分发阶段,需要一位庄家 P_0 来分发秘密信息,它是绝对诚实可信的.但在现实中很难找到这样一个可信中心.在此假设 P_0 与其他局中人一样,其行为是理性的,称之为理性第三方(Rational Third Party, RTP).一位 RTP 是否能保证每个局中人都能得到一个由 P_0 分发的正确子密钥呢?这是个非常值得关注的问题.假定 RTPP_0 对分发协议 Π,总希望能在局中人 $P_1,\cdots,P_n$ 中分发成功(不存在被拒绝接受的情况).然而,在分发过程中,P_0 的最大期望是他给局中人 $P_i(i=1,2,\cdots,n)$分发一个错误的子密钥 s_i,且 P_i 没有拒绝接受;其次是 P_i 接受,若 s_i 是正确的;第三种情况是当 s_i 是错误的时候,P_i 拒绝;第四,P_0 分发一个正确的 s_i,但 P_i 拒绝接受.

对于分发者 P_0,设 v_1、v_2、v_3 和 v_4 代表上述四种不同的收益,即:v_1: P_0 分发错误的子密钥且 P_i 接受(欺骗成功);v_2: P_0 分发正确的子密钥且 P_i 接受(没有欺骗);v_3: P_0 分发错误的子密钥且 P_i 拒绝(欺骗失败);v_4: P_0 分发正确的子密钥且 P_i 拒绝(P_0 不可信,分发失败).

通过上述假定和分析,显然有 $v_1>v_2>v_3>v_4$.

3.1.2 秘密分发阶段局中人的效用分析

对于每一个局中人 $P_i(i=1,2,\cdots,n)$来说,不是任随 P_0 分发来的子密钥就接受,他有一个验证协议来验证其子密钥的正确性,或者通过 P_0 的历史来判断是否应该接受其子密钥.可见,秘密共享的分发协议可以看成是由 n 个二人博弈组成的,这 n 个二人博弈之间又有一定的关系,这种关系主要是由分发协议所决定的.对于局中人 $P_i(i=1,2,\cdots,n)$,在分发协议中的局中人只有 P_0 和 P_i,P_i 总是不希望被欺骗,但 P_i 希望收到正确的子密钥 s_i,而不希望收到错误的子密钥.

用 μ_1、μ_2、μ_3 和 μ_4 来表示相应的收益,即:μ_1:表示 P_i 接受了正确的子密钥(没有被欺骗);μ_2:表示 P_i 拒绝了正确的子密钥(没有被欺骗);μ_3:表示 P_i 拒绝了错误的子密钥(没有被欺骗);μ_4:表示 P_i 接受了错误的子密钥(被欺骗成功).

对于每位局中人来说,当然都希望在没有被欺骗的情况下,自己收到的子密钥是正确无误的,因此有 $\mu_1>\mu_2>\mu_3>\mu_4$.

3.1.3 秘密重构阶段局中人的效用分析

在秘密重构阶段,文献[1,4]中简要分析过该问题.每位理性的局中人首先都希望自己得到这个秘密而其他局中人不能得到该秘密;其次,若其他局中人得到共享秘密,希望自己也知道该秘密;第三种情况是,若自己不知道该秘密,也希望其他任何一位局中人都不知道该共享秘密;第四,当然最糟糕的情况,其他局中人都知道共享秘密而自己不知道.对于局中人 P_i,设 w_1、w_2、w_3 和 w_4 代表上述四种不同的收益,即:w_1:局中人 P_i 得到这个秘密而其他局中人不能得到该秘密;w_2:局中人 P_i 知道共享秘密,其他局中人也知道该秘密;w_3:局中人 P_i 不知道共享秘密,其他任何一位局中人都不知道该共享秘密;w_4:局中人 P_i 不知道共享秘密,而其他局中人都知该秘密.经分析,显然有 $w_1>w_2>w_3>w_4$.

3.2 秘密分发协议的博弈论分析

3.2.1 秘密分发博弈

在秘密分发阶段,这 n 个局中人与秘密分发者 P_0 之间的游戏不是一个 $n+1$ 人博弈,而是 n 对二人博弈,但是它们间又有一定的内在关系,这种关系主要是由分发协议 Π 所决定的.记该博弈为 $\Pi=\{\Pi_1,\cdots,\Pi_n\}$.首先分析下它们之间的博弈,对于 $\Pi_i(i=1,\cdots,n)$来说:

(1)局中人是 P_0 和 P_i;

(2)P_0 的策略 S_{01}和 S_{02},其中 S_{01}是发送正确的子秘密 s_i 给 P_i,S_{02}是发送错误的子秘密 s_i 给 P_i(这里不考虑秘密分发者不给局中人 P_i 分发子秘密的情况,因为对于一位 RTPP_0 来说,显然发送正确或者错误的子秘密给 P_i 都严格优于不给局中人 P_i 分发子秘密);P_i 的策略 S_{i1}和 S_{i2},其中 S_{i1}:P_i 接收 s_i,S_{i2}:P_i 拒接 s_i;

(3)结果和收益如表 1 所示:

表 1

$P_0 \setminus P_i$	S_{i1}	S_{i2}
S_{01}	(v_2,μ_1)	(v_4,μ_2)
S_{02}	(v_1,μ_4)	(v_3,μ_3)

下面分析纳什均衡:对于 P_0 来说,若他选择策略 S_{01},则其收益为 v_2 或 v_4;若选择策略 S_{02},则其收益至少是 v_3,甚至可能是 v_1,因此对于 P_0 来说,其最佳策略是 S_{02}.同样分析可知 P_i 的最佳策略亦为 S_{i2}.所以(S_{02},S_{i2})是唯一的纳什均衡点.也就是说,在秘密分发博弈 $\Pi_i(i=1,\cdots,n)$中,秘密分发者 P_0 总是分发错误的子秘密,而局中人 P_i 总是拒绝.

这里存在一个非常严重的问题:秘密分发者 P_0 是理性的,如在分发协议 $\Pi=\{\Pi_1,\cdots,\Pi_n\}$中都达到了纳什均衡,则该秘密分发协议总是失败的.从而我们有如下结论:

定理 1 在秘密共享体制 $\Gamma=\{P,\Pi,RE\}$中,若秘密分发者 P_0 及各局中人均是理性的当且仅当秘密分发者 P_0 选择欺骗各局中人.

充分性证明 在理性假设下,若 P_0 不选择欺骗局中人 P_i,即他选择了策略 S_{01},在上述效用函数假定下,则他可能的收益为 v_1 或 v_4,而当他选择策略 S_{02}时,其收益至少是 v_3.由于 $v_3>v_4$,因此理性的秘密分发者将会选择策略 S_{02},即总是选择欺骗各局中人.

必要性证明(反证法) 设秘密分发者 P_0 总是选择欺骗各局中人,则他是非理性的.若秘密分发者 P_0 是非理性的,则他将会考虑选择策略 S_{01}以获得可能比 v_3 更高的收益 v_2,这与假定相矛盾.因此,若秘密分发者 P_0 总是选择欺骗各局中人,则他是理性的.

显然,对于秘密分发者和各局中人来说,纳什均衡所产生的并不是他们最大收益,其最大收益为(v_2,μ_1).我们自然要问:在什么机制下,使得 RTPP_0 不存在欺诈行为并得到更佳的收益呢?这里我们可以考虑引入博弈论中自然(Nature).Nature 知道秘密分发者 P_0 及各局中人 P_i 的策略分布.各局中人根据 Nature 提供的知识来做出决策.博弈 $\Pi_i(i=1,\cdots,n)$的描述见图 1.在该博弈中,Nature 先开始行动.使得秘密分发者 P_0 知道局中人 P_i的策略(S_{i1},S_{i2})分布为(β,$1-\beta$);局中人 P_i 知道 P_0 的策略(S_{01},S_{02})分布为(α,$1-\alpha$).此时的收益情况见表 2.

表 2

$P_0 \setminus P_i$	$S_{i1}:\beta$	$S_{i2}:1-\beta$
$S_{01}:\alpha$	(v_2,μ_1)	(v_4,μ_2)
$S_{02}:1-\alpha$	(v_1,μ_4)	(v_3,μ_3)

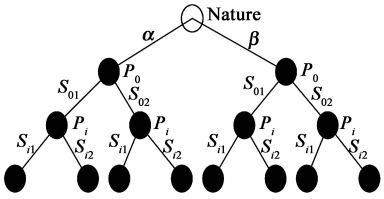

图1　秘密分发博弈

秘密分发者 P_0 的期望收益由从纯策略下的$(v_1+v_2+v_3+v_4)/4$变为$((1-\alpha)\beta v_1+\alpha\beta v_2+(1-\alpha)(1-\beta)v_3+\alpha(1-\beta)v_4)$;局中人 P_i 的期望收益由$(v_1+v_2+v_3+v_4)/4$变为$((\alpha\beta\mu_1+\alpha(1-\beta)\mu_2+(1-\alpha)(1-\beta)\mu_3+(1-\alpha)\beta\mu_4)$.当 $\alpha>1/2$ 和 $\beta>1/2$,则策略(S_{01},S_{i1})为该博弈的纳什均衡,其收益为(v_2,μ_1),明显优于(v_3,μ_3).

对于 P_0 和 P_i 来说,其策略的概率分布都是秘密信息.而在现实中很难找到这样的 Nature 都知道这些分布.下节给出解决该问题的具体机制.

3.2.2　理性秘密分发机制

秘密分发者 P_0 想在 n 位局中人间分发秘密 S.为了简单,我们记分发机制 $\Pi=\{\Pi_1,\cdots,\Pi_n\}$为:$P_0$ 将秘密 $S=(S_1=\oplus\cdots\oplus S_n)$中的 S_i 秘密分发给 P_i.具体方法描述如下.

分发机制 Π_i 分为三个子协议:Commit,SComputed 和 Distributed.

(1)Commit

协议 Commit 分为两步,如图 2 所示.

Step 1　P_0 计算 $C(S)$, $C(S_1)$, $\cdots$, $C(S_n)$,且满足 $C(S)=C(S_1)\oplus\cdots\oplus,C(S_n)$.其中函数 $C(\cdot)$为承诺单向函数,是公共信息.

Step 2　P_0 向局中人广播 $C(S)$和 $C(S_i)$, $i=1,2\cdots,n$.

图 2　Commit 协议

(2)SComputed

说明:利用 2.3 节的安全多方计算技术计算函数 $SC(x,y)=(SC_0(x,y),SC_i(x,y))$,$x$ 是 P_0 的秘密信息(x 代表策略 S_{01}的概率分布),y 是 P_i 的秘密信息(y 表示策略 S_{i1} 的概率分布).其协议分为四步,如图 3 所示.

Step 1　P_0 秘密输入 x,P_i 秘密输入 y.

Step 2　如果 $x\geqslant 1/2$ 和 $y\geqslant 1/2$,则:

$SC_0(x,y)=0, SC_i(x,y)=0$;

否则,如果 $x<1/2$ 则:

$SC_0(x,y)=1, SC_i(x,y)=1$;

Step 3　Step 3　如果 $y<1/2$,则:

$SC_0(x,y)=1, SC_i(x,y)=1$;

Step 4　输出$(SC_0(x,y),SC_i(x,y))$.

图 3　SComputed 协议

(3)Distributed

该子协议分为三步,如图 4 所示.

Step 1　如果 $SC_0(x,y)=0$,则 P_0 选择策略 S_{01};否则,P_0 选择策略 S_{02}.

P_i 执行如下两步:

Step 2　P_i 计算收到的 $C(S_i^*)$,验证是否 $C(S_i^*)=C(S_i)$,若成立,则转 Step3;否则,P_i 选择策略 S_{i2}.

Step 3　如果 $SC_i(x,y)=0$,则 P_i 选择策略 S_{i1};否则,P_i 选择策略 S_{i2}.

图 4　Distributed 协议

我们有如下结论:

定理 2　假定庄家和局中人都是理性的,在上述机制下秘密分发博弈 $\Pi=\{\Pi_1,\cdots,\Pi_n\}$达到均衡结果$(v_2,\mu_1)$.

证明　根据博弈机制描述,在该博弈 Commit 阶段,保证了秘密分发者 P_0 不可能存在欺诈行为而获得更好的收益;否则,P_0 将有能力攻破单向函数 $C(\cdot)$.也就是说,一方面,对 P_0 来说,它若分发一个错误的子密钥 S_i 给 P_i,S_i 能通过验证的概率是可以忽略的,所以它总是分发一个正确的子密钥给 P_i,否则,将不能保证通过验证机制.另一方面,对 P_i 来说,若收到的子密钥能通过 P_i 的验证,则接收;否则就拒绝接收.可见,对于理性的秘密分发者 P_0 来说,它分发给 P_i 一个错误的子密钥的概率是可以忽略的.这样就可以保证 P_i 总能收到一个正确的子密钥.博弈的 Distributed 阶段依据 SComputed 阶段的结果进行决策.根据函数 $SC(x,y)=(SC_0(x,y),SC_i(x,y))$的功能描述,则 P_0 和 P_i 根据共同的偏好进行决策:当 P_0 的偏好是发送正确的子秘密给 P_i,无论 P_i 的偏好如何,选择接收都是上策;当 P_0 的偏好是发送错误的子秘密给 P_i,则在博弈的 Distributed 阶段不能通过 P_i 的验证,则 P_i 将采取拒绝策略,从而导致 P_0 的收益为 $v_3(<v_2)$.因此在该机制下,对于理性的庄家和局中人来说,(S_{01},S_{i1})是他们的最佳选择,从而产生均衡结果(v_2,μ_1).

3.3　秘密重构协议的博弈论分析

3.3.1　秘密重构博弈

在秘密共享体制 $\Gamma=\{P,\Pi,RE\}$中,秘密重构协议 RE 是 n 位局中人恢复共享秘密 S 的特定方法.在(t,n)门限方案中,任何 t 位局中人合作能重构共享秘密,而任何 $t-1$ 位局中人共谋都得不到共享秘密的任何信息;在一般的秘密共享体制中,任何一个授权子集中的局中人合作能恢复共享秘密,而属于非授权子集中的成员合谋却得不到关于共享秘密的任何信息.

在所有局中人都是理性的假设下,秘密重构协议 RE 就是一个 n 人博弈,仍记为 RE,$RE=\{P,A_i,U_i\}$.其中 P 是局中人集合,A_i 是 P_i 的策略集合,U_i 是 P_i 的收

益集合.详细说明如下:

(1)局中人 $P=\{P_1,\cdots,P_n\}$;

(2)局中人 P_i 的策略集合 $A_i=\{A_{i1},A_{i2},A_{i3}\}(i=1,2,\cdots,n)$,$A_{i1}$:$P_i$ 广播正确的子密钥 S_i,A_{i2}:P_i 广播错误的子密钥 S_i',A_{i3}:P_i 保持沉默,什么都不广播;

(3)局中人 P_i 的收益 $U_i=\{w_1,w_2,w_3,w_4\}$,其中 w_1:局中人 P_i 得到这个秘密而其他局中人不能得到该秘密;w_2:局中人 P_i 知道共享秘密,其他局中人也知道该秘密;w_3:局中人 P_i 不知道共享秘密,其他任何一位局中人都不知该共享秘密;w_4:局中人 P_i 不知道共享秘密,而其他局中人都知道该秘密;且 $w_1>w_2>w_3>w_4$.

下面分析纳什均衡:首先分析(t,n)门限秘密共享体制下的情况.因为对于每个局中人 P_i 来说,它都有三个可选的策略 A_{i1},A_{i2}和 A_{i3}.当 P_i 选择 A_{i1}时,分两种情形讨论:

(1) 当有大于等于 $t-1$ 位局中人也选择策略 $A_{j1}(j=1,2,\cdots,l,t-1\leqslant l\leqslant n)$时,无论余下局中人选择 A_{i2}还是 A_{i3},其局中人都能获得共享秘密 s,此时 P_i 的收益是 w_2,其他局中人的收益也是 w_2;

(2) 当有小于 $t-1$ 位局中人也选择策略 $A_{j1}(j=1,2,\cdots,l,l<t-1)$时,此时 P_i 的收益可能是 w_3 或 w_4,当 $l=t-2$ 时,无论余下局中人选择 A_{i2}还是 A_{i3},此时就有 $n-t+1=n-l-1$ 位局中人的收益是 w_1,而此情况下 P_i 及余下局中人的收益是 w_4;当 $l<t-2$ 时,所有局中人的收益均为 w_3(这里不考虑部分局中人结盟的情形).

当 P_i 选择 A_{i2}时,分两种情形:

(1)当有大于等于 t 位局中人选择策略 $A_{j1}(j=1,2,\cdots,l,t\leqslant l\leqslant n)$时,无论余下局中人选择 A_{i2}还是 A_{i3},其局中人都能获得共享秘密 s,此时 P_i 的收益是 w_1,其他局中人的收益是 w_2;

(2)当有小于 t 位局中人也选择策略 $A_{j1}(j=1,2,\cdots,l,l<t)$时,此时 P_i 的收益可能是 w_1 或 w_3,当 $l=t-1$ 时,无论余下局中人选择 A_{i2}还是 A_{i3},此时就有 $n-t+1=n-l-1$ 位局中人的收益是 w_1(包括 P_i 在内),余下局中人的收益为 w_4;当 $l<t-2$ 时,所以局中人的收益均为 w_3(这里不考虑部分局中人结盟的情形).

当 P_i 选择策略 A_{i3}时,此情况类似于 P_i 选择策略 A_{i2}时的情形.

可见,对于任何一位局中人 P_i 来说,如果他更愿意得到共享秘密,则选择 A_{i1}的收益是最大的,此时纳什均衡是$(A_{11},A_{21},\cdots,A_{n1})$.

在一般秘密共享体制下,对任意一个授权子集 B,任意 $P_i\in B$,若 P_i 选择策略 A_{i1}时,除非 B 中余下的局中人都选择策略 $A_{j1}(P_j\in B)$,大家都得到共享秘密.否则,无论余下的局中人都选择策略 A_{j2}还是 $A_{j3}(P_j\in B)$,他们都不可能获得共享秘密.

因此,在一般的秘密共享体制下,对于任何一位局中人 P_i 来说,如果他更愿意得到共享秘密,则选择 A_{i1}的收益是最大的,此时$(A_{11},A_{21},\cdots,A_{|B|})$是纳什均衡.

通过上面的分析很容易看出,在后广播他们子秘密的局中人能够获得更大的收益.2004 年,Halpern 和 Teague[1]针对门限方案分析了类似结论.由此可见,由于大家都是理性的,没有哪位局中人有动力来给他人发送自己的子密钥.因此大家的最优策略就是都不发送自己的子密钥,这样就让大家陷入一种"僵局".博弈论中称之为空威胁(Empty threat).下面给出解决该问题的机制.

3.3.2 理性秘密重构机制

为了简单记共享秘密 $S=(S_1\oplus\cdots\oplus S_n)$,$P_i$ 拥有子秘密 S_i,且知道秘密及子秘密的承诺信息 $C(S)$和 $C(S_i)(i=1,\cdots,n)$.重构秘密 S 的具体机制描述如下:

重构机制分为如下两步:Cycle Distribution 和 OTPooling.

(1)Cycle Distribution

协议 Cycle Distribution 如图 5 所示.

Cycle Distribution$(P_1,\cdots,P_n)$

Begin

Step 1 $P_1,\cdots,P_n$ 共同随机产生一个数 $k(1\leqslant k\leqslant n)$,每位 P_i 置 $flag_i=S_i$.(说明:当 $k=n$ 时,$k+1=1$.下同此规定)

Step 2 For $j=1$ to $n-2$

For $i=0$ to $n-1$

(a) P_{k+i}将其子秘密$flag_{k+i}(=S_{k+i})$传送给 P_{k+i+1}.

(b) P_{k+i+1}收到 $flag_{k+i}$后,验证其正确性及是否已有该子秘密.如果通过验证,则 P_{k+i+1}置 $flag_{k+i+1}=flag_{k+i}$,并发送 $flag_{k+i+1}$给 P_{k+i+2};否则,广播 P_{k+i}为"CHEAT",转执行协议 PuniCD$(k+i,j)$.

End For

End For

Step3 重置各局中人的身份为 $P_{i1},\cdots,P_{in}((i_1,\cdots,i_n)$是$(1,\cdots,n)$的一个置换).

End

图 5 Cycle Distribution 协议

惩罚协议 PuniCD(k,j)如图 6 所示.该协议表示 Cycle Distribution 协议执行至第 j 轮因 P_k 的背叛行为而执行的协议.

(2)OTPooling

当成功执行完 Cycle Distribution 协议执行 OTPooling 协议,该协议分为两步,如图 7 所示.

对该机制的分析,我们有如下结论:

定理 3 假定各局中人都是理性的,在上述机制下秘密重构博弈 RE 达到均衡结果$(w_2,\cdots,w_2)$.

PuniCD(k,j)
Begin
Step 1　如果 $j=1$,则重置时钟,重执 Cycle Distribution($P_1,\cdots,P_n$)协议.
Step 2　如果 $j>1$,则剔除局中人 P_k,转执 Cycle Distribution($P_1,\cdots,P_{n-1}$)协议.
End

图 6　PuniCD 协议

Step 1　$P_1,\cdots,P_n$ 一起随机产生序列($j_1,\cdots,j_n$)(说明:($j_1,\cdots,j_n$)是(1,…,n)的一个置换).
Step 2　For $l=1$ to n
　如果 P_l 已得到秘密,则:
　　P_l 退出协议.
　否则,就执行如下两步:
　(a) P_l 与 P_{jl}同时执行两个健忘传输协议 OT_1^{n-1},取回所需结果.
　(b) P_l 根据(a)的结果计算恢复 S,并可验证 S 的正确性.

图 7　OTPooling 协议

证明　Cycle Distribution($P_1,\cdots,P_n$)顺利执行结束后,则理性的局中人将都有 $n-1$ 份子秘密(若某位局中人在某轮有欺诈行为,根据其惩罚协议,他将获得更少的子密钥),且互不相同.每位局中人都仅需要一份子密钥就能恢复出共享秘密,而且各自所需的子秘密也互不相同.协议 Cycle Distribution($P_1,\cdots,P_n$)中的 Step3 步打乱了各局中人的身份信息,使得在后面的协议中各参与者互不知道对方需要何份子秘密,能够猜中的概率为 $1/n$.这样保证 OTPooling 协议执行前,发送者不知道哪个子密钥是接收者所需要的.最后各局中人通过 OTPooling 协议取回自己所需的那份子密钥.

通过该机制,各参与者的最佳策略都是采取合作.否则他将得到更差的收益(当然,这里没有考虑各局中人结盟的情况).从而每位局中人都得到共享密码,根据其效用函数知他们的收益均为 w_2.从而达到 Nash 均衡($w_2,\cdots,w_2$).

4　结论

本文基于博弈论研究了秘密共享问题,详细分析在博弈论环境下秘密共享体制并提出理性秘密分发机制和密码重构机制.在理性秘密共享中,局中人仅关心自己的收益,无论在秘密分发协议还是在秘密重构协议中,做决策的依据都依赖于其效用.但是在秘密学中,如何刻画各局中人的效用函数亦非常困难,甚至其效用无法刻画.文中也仅给出各局中人的效用界定.虽然近年来在理性秘密共享方面已取得很多研究成果,但还有很多问题值得我们进一步深入研究.

参考文献

[1] Halpern J, Teague V. Rational secret sharing and multiparty computation: extended abstract[A]. Proceedings of the 36th Annual ACM Symposium on Theory of Computing[C]. New York, USA: ACM, 2004. 623 – 632.

[2] Abraham I, Dolev D, Gonen R, Halpern J. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation[A]. Proceedings of the 25th Annual ACM Symposium on Principles of Distributed Computing[C]. New York, USA: ACM, 2006. 53 – 62.

[3] Lysyanskaya A, Triandopoulos N. Rationality and adversarial behaviour in multi-party computation (extended abstract)[A]. CRYPTO2006[C]. Heidelberg: Springer, 2006. 180 – 197.

[4] Maleka S, Amjed S, Pandu Rangan C. Rational secret sharing with repeated games[A]. ISPEC2008[C]. Heidelberg: Springer, 2008. 334 – 346.

[5] Asharov G, Lindell Y. Utility dependence in correct and fair rational secret sharing[A]. CRYPTO2009[C]. Heidelberg: Springer, 2009. 559 – 576.

[6] 陈晶,杜瑞颖,王丽娜,田在荣.网络环境下一种基于概率密度的信任博弈模型[J].电子学报,2010,38(2):427 – 433.
Chen Jing, Du Ruiying, Wang Lina, Tian Zairong. Atrust game method basing on probability model in networks[J]. Acat Electronica Sinica, 2010, 38(2): 427 – 433. (in Chinese)

[7] Osborne M. An Introduction to Game Theory[M]. Oxfor: Oxford University Press, 2004.

[8] 刘木兰,张志芳.密钥共享体制与安全多方计算[M].北京:电子工业出版社,2008.

作者简介

田有亮　男,1982 出生,贵州盘县人,西安电子科技大学博士生,主要研究方向为博弈论、安全协议分析及分布式密码体制等.
E-mail: youli-angtian@163.com

马建峰　男,1963 出生,陕西西安人,博士,西安电子科技大学教授,博士生导师,主要研究方向为网络与信息安全、密码学等等.
E-mail: jfma@mail.xidian.edu.cn

彭长根　男,1963 出生,贵州锦屏人,博士,贵州大学教授、硕士生导师,主要研究方向为密码学、信息安全等.
E-mail: sci.cgpeng@gzu.edu.cn

姬文江　男,1984 出生,陕西西安人,西安电子科技大学博士生,主要研究方向为网络仿真、无线局域网以及移动网络安全等.
E-mail: wenj_ji@163.com