密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2017, 4(3): 209–217

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

基于分组的理性秘密共享方案*

李梦慧[1,3], 田有亮[2,3,4]

1. 贵州大学数学与统计学院, 贵阳 550025
2. 贵州大学计算机科学与技术学院, 贵阳 550025
3. 贵州大学密码学与数据安全研究所, 贵阳 550025
4. 贵州省公共大数据重点实验室, 贵阳 550025

通讯作者: 田有亮, E-mail: youliangtian@163.com

摘 要: 理性秘密共享是博弈论与秘密共享相结合的新兴研究方向, 它拓展了博弈理论和传统秘密共享的应用领域, 已成为密码学的研究热点. 但是多数研究者在构造出理性秘密共享方案的同时忽略了方案的效率问题. 理性秘密共享方案的通信轮数是影响方案效率的主要因素. 现有的多数方案为了实现均衡等需求都采用未知轮数, 即不让理性参与者知道当前重构轮是测试轮还是真秘密所在的轮, 此方法造成通信复杂度较高, 导致方案效率低下, 这在一定的程度上会增加额外的通信开销. 针对上述问题, 基于不完全信息动态博弈模型, 研究门限理性秘密共享方案的完美贝叶斯均衡问题. 利用椭圆曲线上双线性对的随机函数设计一个知识承诺方案, 该方案为可验证的, 以此来检验分发者和参与者的欺骗问题. 结合“均匀分组”思想使理性参与者以组为单位进行通信, 可降低方案的通信复杂度, 进而构造出两轮理性秘密共享方案. 分析证明本方案具有可验证性, 能够实现秘密重构博弈的完美贝叶斯均衡. 并从轮复杂度、通信类型和前提假设三个方面与现有的典型方案进行对比, 表明本方案不仅满足安全性需求且执行效率更高.

关键词: 理性秘密共享; 双线性对; 博弈论; 完美贝叶斯均衡

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000175

中文引用格式: 李梦慧, 田有亮. 基于分组的理性秘密共享方案[J]. 密码学报, 2017, 4(3): 209–217.

英文引用格式: LI M H, TIAN Y L. Rational secret sharing scheme based on group[J]. Journal of Cryptologic Research, 2017, 4(3): 209–217.

Rational Secret Sharing Scheme Based on Group

LI Meng-Hui[1,3], TIAN You-Liang[2,3,4]

1. College of Mathematics and Statistics , Guizhou University, Guiyang 550025, China
2. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
3. Institute of Cryptography and Data Security, Guizhou University, Guiyang 550025, China
4. Guizhou Provincial Key Laboratory of Public Big Data, Guiyang 550025, China

Corresponding author: TIAN You-Liang, E-mail: youliangtian@163.com

Abstract: Rational secret sharing is an emerging research direction of the combination of game theory and secret sharing, which extends the application field of game theory and traditional secret sharing, and has become a research hot research of cryptography However, most researchers in the

* 基金项目: 国家自然科学基金项目 (61363068, 61262073); 贵州省教育厅科技拔尖人才支持项目 (黔教合 KY 字 [2016] 060); 贵州省科技基金计划项目 (黔科合基础 [2016]1023); 贵州大学研究生创新基金 (研理工 2016016)
收稿日期: 2016-03-31 定稿日期: 2017-04-06

construction of a rational secret sharing scheme while ignoring the scheme efficiency issues. The number of communication round of a rational secret sharing scheme is the main factor that influence the efficiency of the scheme. In order to achieve the equilibrium, most of the existing schemes have unknown number of communication rounds, i.e., rational participants do not know whether the current round is test round or the true secret round. This method has high communication complexity and low efficiency, and to a certain extent can add additional communication expense. According to the above problem, based on the incomplete information dynamic game model, and study on the perfect Bayesian equilibrium problem of threshold rational secret sharing scheme, by using bilinear pairings on elliptic curve random function, this paper designs a knowledge commitment scheme. The scheme is verifiable, it can test the distributor and the participants' cheating. "Homogeneous grouping" makes rational participants as a group for the unit to communicate, which can reduce the communication complexity of the scheme, and enables the construction of two-round rational secret sharing scheme. Analysis shows that this scheme has the verifiability, can achieve the perfect bayesian equilibrium of reconstructing secret game. The scheme is compared with existing typical schemes with respect to complexity, types of communication and premise assumption, it is shown that the scheme satisfies the security requirements and is more efficient.

Key words: rational secret sharing; bilinear pairings; game theory; perfect bayesian equilibrium

1 引言

秘密共享作为近代密码学的重要研究分支, 是构造安全多方计算协议的基础. 最早的秘密共享方案于 1979 年由 Shamir [1] 基于拉格朗日插值多项式提出的 (t,n) 门限秘密共享方案, 该方案简单、实用, 但是忽略了成员的欺骗问题. 对此, Chor 等人 [2] 针对防止参与者的欺骗问题提出可验证秘密共享 (Verifiable Secret Sharing, VSS);Feldman [3] 和 Pedersen [4] 分别提出可以检验秘密分发者和参与者欺骗的可公开验证秘密共享方案. 对于可验证、可公开验证秘密共享方案, 大都没有考虑协议的通信复杂度.

2004 年 Halpern 和 Teague [5] 最先给出理性模型下的秘密共享问题的一般方法并应用于安全多方计算中, 但他们的协议不能在 $(2,2)$ 情况下执行, 协议的通用性和执行效率受到一定的影响. 2008 年, Kol 和 Naor [6] 基于同时广播信道, 设计了一个信息论安全的秘密共享方案, 但不能防止拥有长秘密份额的人与短秘密份额的人合谋, 该方案的通信复杂度为 $O(1/\beta^2)$. 考虑密码协议中合谋的存在, Abrham 等 [7] 定义了可以抵抗最多 k 人合谋的 k-弹性均衡. 彭长根等 [8] 针对既希望得到正确的秘密又希望提高自身信誉值的理性参与者, 设计了讨价还价机制, 提出一个无秘密分发者参与的 $(2,2)$ 理性秘密共享方案, 协议的通信轮数与参与人数有关. 2011 年, 田有亮等 [9] 提出一个理性第三方的概念, 并设计了一个理性秘密重构机制, 使得理性参与者经过 $(n-1)(n-2)$ 次点对点通信之后, 再经过 n 次健忘传输可获得秘密. 此外, 提出基于马尔科夫决策的理性秘密共享方案 [10], 重构阶段需要执行 v 轮.

由此可见, 理性秘密共享方案为了实现纳什均衡, 抵抗合谋攻击、公平性等问题, 大都将方案设计成未知轮数的, 这样会造成协议的通信复杂度较高, 导致协议的效率较低. 随后, 研究者们对常数轮方案展开研究. 2005 年, Damgård 和 Ishai [11] 针对 $t < N/5$ 贿赂的情况, 设计了一个三轮协议, 并保证了公平性, 协议针对 $t < N/2$ 贿赂情况没有精确的轮复杂度. Asharov 等 [12] 提出著名的五轮协议, 并且保证了公平性. 对于 $t = 1$ 的情况, 在 2010 年 Ishai 等 [13] 证明了 $N \geqslant 5$ 时足以安全的计算一般函数并且保证公平性, 他们也证明了在服务器—客户机模型下的一个两轮协议, 拥有更受限制的贿赂模式. 2014 年刘海等 [14] 根据理性参与者同时考虑眼前利益和长远利益的情况, 基于不完全信息动态博弈模型, 提出适用于异步通信的公平的 $(2,2)$ 理性秘密共享方案. 2015 年 Tian 等 [15] 考虑不同参与者类型, 基于贝叶斯博弈模型, 协议参与者根据信念和贝叶斯偏好采取行动, 提出贝叶斯理性秘密共享方案, 但该方案的通信复杂度较高, 造成协议效率低下. 同年, Gordon 和 Liu 等 [16] 证明在错误假设下, 证明保证输出传递的三轮协议要比实现公平性困难, 提出了门限全同态加密方案, 允许参与者将弹性密文改变为非中止方的公钥, 不用增加额外的轮就可以处理参与者中止的情况.

本文针对上述问题提出两轮理性秘密共享方案. 首先利用双线性对性质设计一个知识承诺方案, 该方案满足知识承诺的绑定性和隐藏性要求, 理性参与者可利用承诺值验证秘密份额的有效性. 其次, 根据参与者类型, 基于贝叶斯博弈, 分析理性参与者采取的行动策略和信念系统, 考虑理性参与者的效用, 研究理性秘密共享方案的贝叶斯均衡问题. 利用 “均匀分组” 思想, 在重构阶段将理性参与者分三组, 并将得到的秘密份额分为两个影子秘密, 执行正、反向各分发一轮的分组转发影子秘密阶段和公开阶段, 构造出两轮 (t,n) 理性秘密共享方案. 最后, 与现有的典型理性秘密共享方案进行对比, 进一步表明本文所提方案在满足安全性的同时, 仅两轮就可重构出秘密, 因此效率更高.

2 预备知识

本节介绍双线性映射和博弈论的相关知识.

2.1 双线性映射

定义 1 设 G_1 和 G_2 分别为加法循环群和乘法循环群, 且 $|G_1|=|G_2|=p$, g 为群 G_1 的生成元. 如果满足下列性质:

1) 双线性性: 对任意的 $P_1,P_2\in G_1$ 和 $a,b\in Z_q^*$, 有 $e(P_1^a,P_2^b)=e(P_1,P_2)^{ab}$.

2) 非退化性: 存在 $P_1,P_2\in G_1$, 使得 $e(P_1,P_2)\neq 1$.

3) 可计算性: 对任意的 $P_1,P_2\in G_1$, 存在有效的算法可计算 $e(P_1,P_2)$.

则称映射 $e: G_1\times G_1\to G_2$ 为双线性映射.

定义 2 双线性 Diffie-Hellman 问题 (BDHP): 在 (G_1,G_2,e) 中, 给定 (P,aP,bP,cP), 对于任意的 $a,b,c\in Z_q^*$, 计算 $e(p,p)^{abc}\in G_2$.

BDH 假设: 在求解 BDH 问题上, 不存在 PPT 算法有不可忽略的优势.

2.2 博弈论相关知识

博弈论中认为参与者是理性的, 理性参与者总是以最大化自身利益为行动目标. 对于理性秘密共享协议而言, 在秘密重构阶段, 首先, 他们都想要得到秘密, 其次, 想要更少的人得到秘密, 参与者的收益仅依赖于博弈的输出值即效用函数值. 理性参与者的集合记为 $N=\{P_1,P_2,\cdots,P_n\}$, σ_i 表示参与者 P_i 采取的策略, $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 表示 n 个参与者的策略组合, $\sigma_{-i}=(\sigma_1,\cdots,\sigma_{i-1},\sigma_{i+1},\cdots,\sigma_n)$ 表示除了参与者 P_i 外其余玩家的策略, 对于策略组合 $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 和 $\sigma'=(\sigma_1',\sigma_2',\cdots,\sigma_n')$, $(\sigma_i',\sigma_{-i})=(\sigma_1,\cdots,\sigma_{i-1},\sigma',\sigma_{i+1},\cdots,\sigma_n)$ 表示参与者 P_i 的策略为 σ_i', 其他参与者按照策略组合 $\sigma_{-i}=(\sigma_1,\cdots,\sigma_{i-1},\sigma_{i+1},\cdots,\sigma_n)$ 执行协议. $o=(o_1,o_2,\cdots,o_n)$ 表示协议的输出结果, 则有以下两种情况:

1) 若参与者 P_i 正确的输出秘密 s, 则 $o_i=1$;

2) 若参与者 P_i 没有输出正确的秘密 s, 则 $o_i=0$.

定义 3 (效用函数) $u_i(\sigma)$ 表示当参与者按照策略组合 σ 执行协议时参与者 P_i 的效用函数. $u_i(o)$ 表示输出为 o 时参与者 P_i 的效用, 记参与者 P_i 了解到真正的秘密, 则 $u_i(o)=1$, 否则 $u_i(o)=0$. 对于输出结果 o 和 o' 而言, 参与者的效用函数有如下假设:

1) $o_i>o_i'\Rightarrow u_i(o)>u_i(o')$;

2) $o_i=o_i'$ 且 $\sum_{j\in N}o_j<\sum_{j\in N}o_j'\Rightarrow u_i(o)>u_i'(o)$.

下面定义参与者 P_i 的效用函数值:

1) $u_i(o)=U^+$ 表示参与者 P_i 得到秘密, 其余参与者没有得到秘密;

2) $u_i(o)=U$ 表示所有参与者 P_i 都得到秘密;

3) $u_i(o)=U^-$ 表示所有参与者均没有得到秘密;

4) $u_i(o)=U^{--}$ 表示参与者 P_i 没有得到秘密, 其余参与者得到秘密.

定义 4 (博弈) $\Gamma=\{N,S,u\}$ 表示博弈的三元组, 其中 $N=\{P_1,P_2,\cdots,P_n\}$ 表示参与者的集合, $S=\{S_1,S_2,\cdots,S_n\}$ 表示策略空间, $u=\{u_1,u_2,\cdots,u_n\}$ 表示效用集合.

定义 5 (完全信息扩展式博弈) 在扩展式博弈 G 中, 若参与者 $P_i \in \mathcal{P}$ 的类型 $T_i \in \mathcal{T}_i$ 为其私人信息, 其中 $\mathcal{T}_i$ 为参与者 P_i 的类型空间, 则称 G 为完全信息扩展式博弈, 协议参与者在每次采取行动之后都会更新对其他参与者类型分布的判断.

定义 6 (完美贝叶斯均衡) 给出 S 和 ρ,$(S;\rho)$ 称作完美贝叶斯均衡当且仅当策略信念系统 $(S;\rho)$ 满足 1)-4):

1) 给定策略组合 S, 对于任意的 $P_i \in \mathrm{P}$ 和 $I_i \in \mathrm{I}_i$,P_i 在其所处的节点上的信念 $\rho(I_i) \in \Delta(I_i)$.

2) 假设连续博弈由参与者 P_i 的信息集 $I_i \in \mathrm{I}_i$ 和信念 $\rho(I_i)$ 定义, 策略信念系统 $(S;\rho)$ 是从 I_i 开始的纳什均衡.

3) 贝叶斯规则和策略组合 S 决定了在任何均衡路径信息集上的信念. 即如果 $I_i \in \mathrm{I}_i$ 是参与者 P_i 按照策略组合 S 实现正概率的信息集, 那么根据贝叶斯规则可计算得出 $\rho(I_i) \in \Delta(I_i)$.

4) 贝叶斯规则和可能情况下的参与者的策略组合 S 决定了任何非平衡路径信息集上的信念。

3 基于双线性对的两轮分组理性秘密共享方案

本文描述的方案引入惩罚机制: 在方案执行过程中, 若有参与者有偏离行为, 则对欺骗者有一个公开的惩罚值, 并将其剔除方案. 基于 BDH 假设, 利用双线性对知识承诺方案和离散对数难题设计可验证的理性秘密共享方案, 本方案分为秘密共享阶段和秘密重构阶段, 其中秘密重构阶段包括分组转发阶段和公开阶段.

3.1 可选策略集合和信念系统

将 n 位理性参与者分为 3 个组, 分别记为 $A = \{A_1, A_2, \cdots, A_a\}$, $B = \{B_1, B_2, \cdots, B_b\}$, $C = \{C_1, C_2, \cdots, C_c\}$, 其中, $a+b+c = n$, 参与者以组为单位进行通信, 自然规定了每个参与者的类型, 每组内的各个参与者类型相同. 类型空间 $T = T_A \times T_B \times T_C$, 其中, A 组内参与者的类型空间为 $T_A = \{A^h, A^d\}$, B 组内的参与者类型空间为 $T_B = \{B^h\}$, C 组内的参与者类型空间为 $T_C = \{C^h\}$, h 表示参与者的类型是 “好” 的, d 表示参与者的类型是 “坏” 的, 那么, 在类型空间 T_A, T_B 和 T_C 上的概率分布 θ_A、θ_B 和 θ_C 分别为:

$$\theta_A^h = \Pr(A^h|B), \theta_A^d = \Pr(A^d|B), s.t. \theta_A^h + \theta_A^d = 1$$

$$\theta_B^h = \Pr(B^h|C) = 1, \theta_B^d = \Pr(B^d|C) = 0$$

$$\theta_C^h = \Pr(C^h|A) = 1, \theta_C^d = \Pr(C^d|A) = 0$$

A, B, C 三组内的参与者的行动集合分别为 $M_A = \{C, D, \mathrm{quit}_A\}$, $M_B = \{C, \mathrm{quit}_B\}$, $M_C = \{C, \mathrm{quit}_C\}$, A 组中参与者的一个纯策略组合 $S_A \in S_A = \{(s_1, s_3)_h, (s_2, s_3)_d\}$, B 组参与者的一个纯策略 $s_B \in S_B = \{(s_1, s_3)\}$, C 组参与者的一个纯策略 $s_C \in S_C = \{(s_1, s_3)\}$, 其中 $s_1 \in \{C\}, s_2 \in \{D\}, s_3 \in \{\mathrm{quit}_A, \mathrm{quit}_B\}$.

在理性秘密共享方案的最后公开阶段利用贝叶斯规则, A 组参与者的信念是关于 B 组参与者行动集合上的概率分布:

$$\beta : T_B \to \Delta(M_B), s.t. \beta(C) + \beta(\mathrm{quit}_B) = 1$$

B 组参与者的信念是关于 C 组参与者行动集合上的概率分布:

$$\gamma : T_C \to \Delta(M_C), s.t. \gamma(C) + \beta(\mathrm{quit}_C) = 1$$

C 组参与者的信念是关于 A 组参与者行动集合上的概率分布:

$$\alpha_h, \alpha_d : T_A \to \Delta(M_A), s.t. \alpha_h(C) + \alpha_h(D) + \alpha_h(\mathrm{quit})_A = 1$$
$$\alpha_d(C) + \alpha_d(D) + \alpha_d(\mathrm{quit}_B) = 1$$

3.2 系统参数

本文构造的 (t,n) 理性秘密共享方案中, 门限值 $1<t\leqslant 1+n/3$(每个参与者自身有一个份额, 在重构过程中至多可以再得到另外一组参与者的 $n/3$ 个份额), 记秘密分发者为 D, n 个理性参与者的集合为 $N=\{P_1,P_2,\cdots,P_n\}$, 分发者要在 n 个参与者间共享的秘密为 $s\in Z_q^*$.

3.3 方案描述

1) 秘密分享阶段

Step1 分发者 D 对秘密 s 实施承诺:$C_0=C(s)=e(sP,P+Q),s\in Z_q^*$.

Step2 分发者 D 随机选择 $t-1$ 次多项式 $f(x)=\sum_{j=0}^{t-1}a_jx^j$, 其中 $s_0=s$,$a_j\in Z_q^*(j=1,2,\cdots,t-1)$, 计算并公开广播 $C_j=C(a_j)(j=1,2,\cdots,t-1)$.

Step3 分发者 D 计算 $s_i=f(i)$ 并发送给参与者 P_i, P_i 收到秘密份额 s_i 后可以根据

$$C(s_i)=\prod_{j=0}^{t-1}C_j^{i^j} \tag{1}$$

验证秘密份额的正确性.

若 (1) 式成立, 则 P_i 收到的秘密份额是正确的, 否则是错误的. 得到 t 个份额后, 可利用 Lagrange 插值多项式重构秘密

$$s=\prod_{i\in B}(s_i\cdot\prod_{j\in B\setminus\{i\}}\frac{0-x_j}{x_i-x_j})\mod q \tag{2}$$

并利用 C_0 来验证重构出的秘密 s 的正确性:

$$C_0=e(sP,P+Q)=e(P,P)^se(P,Q)^s \tag{3}$$

将 n 位理性参与者分为 3 个组, 分别记为 $A=\{A_1,A_2,\cdots,A_a\}$, $B=\{B_1,B_2,\cdots,B_b\}$, $C=\{C_1,C_2,\cdots,C_c\}$, 其中 $a+b+c=n$, A_i 随机选择一次多项式将自己的秘密份额拆分为一组影子秘密 $(s_{i1}^A,S_{i2}^A)(i=1,2,\cdots,a)$, 并公开对秘密份额和影子秘密的承诺, 同理将自己的秘密份额分别拆分为 $(s_{i1}^B,S_{i2}^B)(i=1,2,\cdots,b)$,$(s_{i1}^C,S_{i2}^C)(i=1,2,\cdots,c)$, 并公开对秘密份额和影子秘密的承诺.

2) 秘密重构阶段

a. 分组转发阶段

Round 1

Step1 A 组所有成员向 B 组成员公开广播其影子秘密 s_{i1}^A.

Step2 B 组成员利用 A 组成员公开的承诺验证得到 s_{i1}^A 的正确性, 如果验证通过, 协议进入下一步, 否则, 向其余参与者广播 A_i 是欺骗者, 建议将 A_i 剔除出局, 重新运行剩余 $n-1$ 人分组转发阶段.

Step3 B 组所有成员向 C 组成员公开广播其影子秘密 s_{i1}^B.

Step4 C 组成员利用 B 组成员公开的承诺验证得到 s_{i1}^B 的正确性, 如果验证通过, 协议进入下一步, 否则, 向其余参与者广播 B_i 是欺骗者, 建议将 B_i 剔除出局, 重新运行剩余人 $n-1$ 分组转发阶段.

Step5 C 组所有成员向 A 组成员公开广播其影子秘密 s_{i1}^C.

Step6 A 组成员利用 C 组成员公开的承诺验证得到的 s_{i1}^C 的正确性, 如果验证通过, 协议进入第二轮, 否则, 向其余参与者广播 C_i 是欺骗者, 建议将 C_i 剔除出局, 重新运行剩余 $n-1$ 人分组转发阶段.

Round 2

第二轮的分组转发阶段与第一轮类似, 不过影子秘密的广播变为第二个影子秘密. 由 A 组成员先向 C 组成员广播第二个影子秘密 s_{i2}^A, 然后, C 组成员向 B 组成员广播第二个影子秘密 s_{i2}^C, B 组成员向 A 组成员广播其第二个影子秘密 s_{i2}^B. 同样, 欺骗者将被剔除出局, 重新运行 $n-1$ 人分组转发阶段.

b. 公开阶段

Step1 A 组成员计算 $\alpha_h(C)=\mathrm{Pr}_B(C|\theta_B^h),\alpha_h(D)=\mathrm{Pr}_B(C|\theta_B^h),\alpha_h(\mathrm{quit}_B)=\mathrm{Pr}_B(\mathrm{quit}_B|\theta_B^h)$ 和 $\alpha_d(C)=\mathrm{Pr}_B(C|\theta_B^h),\alpha_d(D)=\mathrm{Pr}_B(C|\theta_B^h),\alpha_d(\mathrm{quit}_B)=\mathrm{Pr}_B(\mathrm{quit}_B|\theta_B^h)$, 且计算其预期效用, 得出最优策

略. 若 $s_A^* = C$ 则公开其第二轮得到的份额 s_{i2}^B, 如果 $s_A^* = D$, 则公开假的影子份额, 否则, 退出协议.

Step2 C 组成员得到 A 组成员公开的影子秘密 s_{i2}^B 后, 验证其正确性, 如果正确, 则更新其信誉值 $\theta_B = \Pr_B(\theta_B^0|C)$, 如果验证未通过即发送假的影子秘密, 则 $\theta_B = \Pr(\theta_B^0|D)$, 如果 A 组成员未发送影子秘密, 则更新其信誉值为 $\theta_B = \Pr(\theta_B^0|D)$, 其中 $\theta_B^0 > 1/2$.

Step3 同理, 接下来分别由 B、C 两组成员分别根据贝叶斯规则公开其在第二轮得到的影子秘密。

最终, 当秘密重构者得到 t 个份额后可以根据拉格朗日差值多项式重构出秘密 s.

下面描述本方案重构过程 (如图 1). 经分组广播和公开阶段后, 理性参与者 A_1 得到 (s_{11}^C, s_{12}^C), 可根据拉格朗日插值多项式得到 C_1 的秘密份额 s_C, 再结合本身已有的秘密份额 s_A, 可得到秘密 s. 同样的理性参与者 B_1,C_1 也可得到秘密 s.

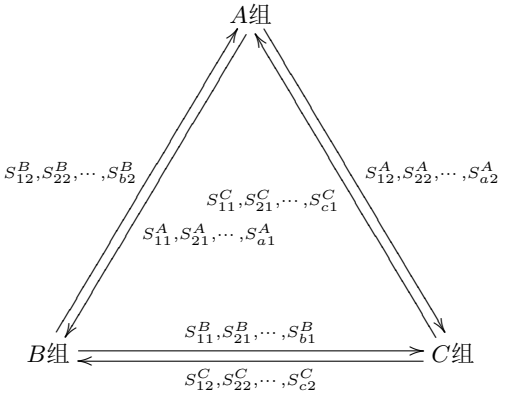

图 1 三组秘密重构

Figure 1 Three-group secret refactoring

4 方案分析

本节对提出的理性秘密共享方案的正确性、安全性、贝叶斯均衡进行分析.

4.1 正确性分析

下证 (1) 式的正确性.

证明: 因为:$s_i = f(i)$, 所以

$$\begin{aligned} C(s_i) &= e(s_i P, P+Q) \\ &= e(f(i)P, P+Q) \\ &= e(\sum_{j=0}^{t-1} a_j i^j P, P+Q) \\ &= e(a_0 P, P+Q) \cdot e(a_1 P, P+Q)^i \cdot e(a_2 P, P+Q)^{i^2} \cdots e(a_{t-1} P, P+Q)^{i^{t-1}} \\ &= e(P,P)^{a_0} \cdot e(P,Q)^{a_0} \cdot e(P,P)^{a_1 i} \cdot e(P,Q)^{a_1 i} \cdots e(P,P)^{a_{t-1} i^{t-1}} \cdot e(P,Q)^{a_{t-1} i^{t-1}} \\ &= \prod_{j=0}^{t-1} C_j^{i^j} \end{aligned} \tag{4}$$

则 $C(s_i) = \prod_{j=0}^{t-1} C_j^{i^j}$. □

本方案的验证算法是基于双线性对的, 因此, 存在有效的算法计算它.

理性参与者在得到同一个成员的两个影子秘密后, 同样可以利用类似 (1) 式的方法验证得到的影子秘密的正确性, 然后可基于 Lagrange 插值多项式, 恢复出该成员的秘密份额, 当共得到 t 个不同成员的秘密份额后, 再次利用 (2) 式重构出主秘密 s. 因此, 本文提出的两轮 (t,n) 理性秘密共享方案是正确的.

4.2 安全性分析

定理 1 对于任意的 $s \in Z_q^*$, 分发者和拥有秘密份额的人无法用两种方式分别打开承诺 $C(s)$ 和 $C(s_i)$.

证明: 假设分发者 D 能够用两种方式打开 $C(s)$, 即存在 $s' \in Z_q^*$ 且 $s' \neq s$, 使得等式 $C(s') = C(s)$ 成立, 即 $e(s'P, P+Q) = e(sP, P+Q)$.

由本方案的参数设置可知: 群 G_1 是一个阶为素数 q 的加法循环群, 则 $P, Q \in G_1$ 都是其生成元, 且阶均为 q. 因此 $qP = qQ = o$, 其中 o 为群 G_1 的零元. $e(s'P, P+Q) = e(P, P+Q)^{s'} = e(P, P+Q)^s = e(sP, P+Q)$, 所以, $s'P = sP$. 又因为 $s \neq s$, 不妨设 $s' = s+t, 0 < t < q$, 则 $s'P - sP = tP = o$, 与 P 的阶为 q 矛盾, 因此 $s' = s$, 证得秘密分发者 D 只能以一种方式打开承诺 $C(s)$.

同理, 理性参与者也只能用一种方式打开承诺 $C(s_i)$.

因为没有人知道 P, Q 的离散对数和 e 的双线性性质, 因此 $e(P,P) \neq e(P,Q)$; 又因在群 G_2 上离散对数问题是难解的, 即使验证者得到承诺 $C(s)$, 且通过计算得知 $e(P,P)$,$e(P,Q) \in G_2$, 但是离散对数是难解的, 所以, 验证者无法得到 s. 并且, 验证者想要通过 $C(s) = e(sP, P+Q) = e(P, sP+sQ)$ 得到承诺的内容也是不可能的. 因此本方案满足知识承诺的绑定性要求和隐藏性要求. □

引理 1 该方案是可验证的, 能有效的防止理性参与者间的欺诈行为. 保证了至少 t 个秘密份额才能重构秘密, 任何少于 t 个秘密份额都无法重构秘密, 即防止秘密分发者和一些理性参与者合谋得到一个 $(t' < t, n)$ 秘密共享方案.

证明: 一方面, 该方案可以防止秘密的分发者对理性参与者分发假的份额. 理性参与者可以通过 (1) 式验证得到的秘密份额 $C(s_i)$ 的正确性. 分发者要想伪造假的秘密份额通过 (1) 式的验证, 由定理 1 可知是不可能的, 所以, 分发者不能欺骗成功. 另一方面, 可以有效防止理性参与者 P_i 之间的欺骗行为. 如果, 理性参与者提供假的影子秘密, 同理可得, 理性参与者之间也不可能欺骗成功.

因为秘密分发者选择的是 $t-1$ 次多项式, 所以要想恢复出多项式 $f(x)$, 一定得到 t 个数对 (i, s_i), 否则得不到 s 的任何信息, 当拥有至少 t 个数对就可以根据 (2) 式计算得到 $s = f(0)$. 所以, 本文所提出的方案是安全的. □

4.3 贝叶斯均衡分析

定理 2 在本方案中, 策略信念系统 $(s^*, \beta^*) = (\{(s_1)_h, (s_1)_d\}, \{s_1\}; (\theta_A^*, \theta_B^*, \theta_C^*, \alpha_h^*, \alpha_d^*, \beta^*, \gamma^*))$ 满足完美贝叶斯均衡, 当且仅当 $\theta_C^{h^*} \geqslant U^-/L_1^*, \theta_B^{h^*} \geqslant U^-/L_2^*, \theta_A^{h^*} \geqslant U^-/(U^- - L_3^*)/L_4^*$.

证明: B 组理性参与者选择纯策略 s_1 和 s_3 时的期望收益为:

$$\mathrm{EU}(B^h, s_1) = \theta_C^h \left[\gamma_h(s_1)U + \gamma_h(s_3)U^-\right] = \theta_C^h \cdot L_1$$

$$\mathrm{EU}(B^h, s_3) = U^-$$

因此, 当 $\mathrm{EU}(B^h, s_1) \geqslant \mathrm{EU}(B^h, s_3)$, 即 $\theta_C^h \geqslant U^-/L_1$ 时,B 组理性参与者会选择纯策略 s_1.

自然规定了 C 组参与者的类型和概率, 则 $\theta_C^h = 1$. 参与者 B 定义了概率 γ_h^* 分布满足 $\gamma_h^*(s_1) + \gamma_h^*(s_3) = 1, \theta_C^{h^*} \cdot \gamma_h^*(s_1) + \theta_C^{h^*} \cdot \alpha_h^*(s_3) = 1$, 因此理性参与者在每个信息集上都有信念, 满足贝叶斯要求 1.

一旦博弈停止,B 组的所有参与者达到信息集 I_B, 假设 G 是同一个信息集上博弈的开始, 那么根据 $\theta_C^h \geqslant U^-/L_1$,$B$ 组参与者的预期效用 $\mathrm{EU}(B, s_3, G) \leqslant \mathrm{EU}(B, s_1, G)$, 因此, B 组参与者将不会偏离协议, 满足贝叶斯要求 2.

在均衡路径的信息集 I_B 上, B 组中的参与者能够根据 C 组中的参与者在博弈中采取的行动策略, 得到概率分布 γ_h^*, 根据 B 组中参与者的信念, 如果 B 组中的参与者认为一个 "好" 的参与者集合 C 采取行动 s_1 的概率为 μ_h, 采取行动 s_2 的概率为 φ_h, 则其采取行动 s_3 的概率为 $1-\mu_h-\varphi_h$, 则有

$$\alpha_h^*(s_1)=\frac{\mu_h}{\mu_h+\varphi_h}, \alpha_h^*(s_3)=\frac{\varphi_h}{\mu_h+\varphi_h}$$

在任何非均衡路径上的信息集中, 要求 4 也被满足.

同理可得 $\theta_B^h \geqslant U^-/L_2^*$, $\theta_A^h \geqslant U^-/(U^- - L_3)/L_4^*$, 其中,$L_3^* = \alpha_h(s_1)U - \alpha_d(s_2)U^{--} + [\alpha_h(s_3) - \alpha_d(s_3)]U^-$, $L_4^* = \alpha_d(s_2)U^{--} + \alpha_d(s_3)U^-$.

因此, 策略信念系统是理性秘密共享重构博弈的完美贝叶斯均衡. □

5 方案性能对比

本节对所提出的方案与现有的几个典型的理性秘密共享方案进行性能对比. 主要从影响方案实用性的三个方面即轮复杂度、通信类型、前提假设方面进行对比 (如表 1).

表 1 性能对比

Table 1 Performance comparison

方案	轮复杂度	通信类型	前提假设
Halpern and Teague [5]	$o(5\times\alpha^{-3})$	同时广播信道	重构阶段需要分发者在线
Kol and Naor [5]	$o(1/\beta^2)$	同时广播信道	重构阶段不需分发者在线
彭长根 [8]	n	非同时广播信道	重构阶段不需分发者在线
田有亮 [9]	$(n-1)(n-2)$	点对点广播信道	重构阶段不需分发者在线
本方案	2	同时、非同时广播信道	重构阶段不需分发者在线

根据表 1, 在轮复杂度方面, Halpern 和 Teague [5]、Kol 和 Naor [6] 方案的轮复杂度都与选择的参数有关, 文献 [8] 的轮复杂度与参与者的数量有关. 田有亮 [9] 提出的方案通信复杂度为 $(n-1)(n-2)$, 并且还需要经过健忘传输协议重构秘密. 本方案的轮复杂度仅为 2, 大大降低了通信开销. 在通信类型方面, 与文献 [5,6,8,9] 相比, 本方案需要两个通信信道, 因此维护信道的开销比其他方案稍高. 在前提假设方面, 文献 [5] 要求秘密分发者始终在线, 本方案在秘密重构阶段不需要分发者在线使方案更能满足实用性需求.

6 总结

降低通信复杂度是提高方案效率的有效途径, 双线性对是构造密码算法的重要工具. 本文在 Shamir 秘密共享方案的基础上, 首先基于双线性对构造了知识承诺方案, 解决了分发者和参与者的诚实问题, 其次基于贝叶斯博弈构造了两轮 (t,n) 理性秘密共享方案. 最后, 对所构造的方案进行分析, 在保证安全性需求的同时, 更有效的的提高了理性秘密共享方案的执行效率. 本方案未考虑参与者合谋的情况, 抗合谋攻击的理性秘密共享方案将是下一步要研究的问题.

References

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

[2] CHOR B, GOLDWASSER S, MICALI S, et al. Verifiable secret sharing and achieving simultaneity in the Presence of faults[C]. In: Proceedings of the 26th Annual Symposium on Foundations of Computer Science. IEEE Computer Society, 1985: 383–395.

[3] FELDMAN P. A Practical scheme for non-interactive verifiable secret sharing[C]. In: 28th Annual Symposium on Foundations of Computer Science, 1987. IEEE, 1987: 427–438.

[4] PEDERSEN T P. Distributed Provers with applications to undeniable signatures[C]. In: Advances in Cryptology—EUROCRYPT 1991. SPringer Berlin Heidelberg, 1991: 221–242.
[5] HALPERN J, TEAGUE V. Rational secret sharing and multiparty computation[J]. Proceedings of Annual ACM Symposium on Theory of Computing, 2004: 623–632.
[6] KOL G, NAOR M. Games for exchanging information[C]. In: ACM Symposium on Theory of Computing. 2007: 423–432.
[7] ABRAHAM I, DOLEV D, GONEN R, et al. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation[C]. In: Proceedings of the 25th Annual ACM Symposium on Principles of Distributed Computing. ACM, 2006: 53–62.
[8] PENG C, LIU H, TIAN Y, et al. A distributed rational secret sharing scheme with hybrid Preference model[J]. Journal of Computer Research & Development, 2014, 51(7): 1476–1485.
[9] TIAN Y L, MA J F, PENG C G, et al. Game-theoretic analysis for the secret sharing scheme[J]. Chinese Journal of Electronics, 2011, 39(12): 2790–2795.
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.
[10] TIAN Y L, WANG X M, LIU L F. Rational secret sharing scheme based on Markov decision[J]. Journal on Communications, 2015, 36(9): 222–229.
田有亮, 王雪梅, 刘琳芳. 基于马尔可夫决策的理性秘密共享方案 [J]. 通信学报, 2015, 36(9): 222–229.
[11] DAMGÅRD I, ISHAI Y. Constant-round multiparty computation using a black-box pseudorandom generator[C]. In: Advances in Cryptology—CRYPTO 2005. SPringer Berlin Heidelberg, 2005: 378–394.
[12] ASHAROV G, JAIN A, LÓPEZ-ALT A, et al. Multiparty computation with low communication, computation and interaction via threshold FHE[C]. In: Advances in Cryptology—EUROCRYPT 2012. SPringer Berlin Heidelberg, 2012: 483–501.
[13] ISHAI Y, KUSHILEVITZ E, PASKIN A. Secure multiparty computation with minimal interaction[C]. In: Advances in Cryptology—CRYPTO 2010. SPringer Berlin Heidelberg, 2010: 577–594.
[14] LIU H, PENG C G, TIAN Y L, et al. The (2,2) Bayesian rational secret sharing scheme[J]. Chinese Journal of Electronics, 2014, 42(12): 2481-2488.
刘海, 彭长根, 田有亮, 等. (2,2) 贝叶斯理性秘密共享方案 [J]. 电子学报, 2014(12): 2481–2488.
[15] 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.
[16] GORDON S D, LIU F H, SHI E. Constant-round MPC with fairness and guarantee of output delivery[C]. In: Annual Cryptology Conference. SPringer Berlin Heidelberg, 2015: 63–82.

作者信息

李梦慧 (1991–), 河南焦作人, 硕士. 主要研究领域为理性秘密共享方案效率优化.
Email: menghuili361@163.com

田有亮 (1982–), 贵州盘县人, 博士, 教授. 主要研究领域为博弈论、安全协议及分布式密码等.
Email: youliangtian@163.com