

常数轮公平理性秘密共享方案

李梦慧^{1,2}, 田有亮^{2,3,4}, 冯金明^{1,2}

- (1. 贵州大学数学与统计学院, 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. 贵州省公共大数据重点实验室, 贵州 贵阳 550025;
4. 贵州大学计算机科学与技术学院, 贵州 贵阳 550025)

摘要: 在理性秘密共享方案中, 公平性是所有参与者期望的目标。基于均匀分组原理研究了常数轮理性秘密共享方案, 结合双线性对有关知识和双变量单向函数构造知识承诺方案, 该方案是可验证的, 以此来检验分发者和参与者的欺骗问题。分发者分给各组参与者的子秘密份额数量最多相差 1, 有效约束参与者的偏离行为。参与者按照协议执行 4 轮即可实现公平重构秘密, 一定程度上降低了公平理性秘密共享方案的通信复杂度, 具有一定应用价值。

关键词: 秘密共享; 通信复杂度; 博弈论; 双线性对

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00136

Constant-round fair rational secret sharing scheme

LI Meng-hui^{1,2}, TIAN You-liang^{2,3,4}, FENG Jin-ming^{1,2}

- (1. College of Mathematics and Statistics, Guizhou University, Guiyang 550025, China;
2. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China;
3. Key Laboratory of Public Data of Guizhou Province, Guiyang 550025, China;
4. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

Abstract: In the rational secret sharing scheme, fairness is the goal that all participants expect. Based on the principle of uniform grouping, the scheme was verified by combining bilinear pair knowledge and bivariate one-way function to verify the deception problem of the distributor and the participant. The number of sub-secret shares distributed by the distributor to each group of participants is at most one, effectively restricting the deviation behavior of the participant. In the end, participants can implement fair reconstruction secret in four rounds according to the protocol, which reduces the communication complexity of fair and rational secret sharing scheme to a certain extent, and has certain application value.

Key words: secret sharing, communication complexity, game theory, bilinear pairing

1 引言

秘密共享方案是分布式密码协议的基础。秘

密共享方案的公平性指要么所有参与者都能获得共享秘密, 要么都得不到秘密。公平性最早的研究可以追溯到 Even 等^[1]的工作, 他们非正式地证

收稿日期: 2016-10-21; 修回日期: 2016-12-17。通信作者: 田有亮, youliangtian@163.com

基金项目: 国家自然科学基金资助项目 (No.61363068); 贵州省教育厅科技拔尖人才支持基金资助项目 (No.黔教合 KY 字[2016]060)

Foundation Items: The National Natural Science Foundation of China (No.61363068), The of the Science and Technology Top-notch Talent Support Project of the (No.Guizhou-Education-Contact-KY-Word [2016]060)

明了电子签名交换是不可行的。Ong 等^[2]提出一个适用于任何门限秘密共享方案的秘密重构协议，并且证明了当存在少数诚实参与者和绝大多数理性参与者的情况下，该协议是公平的，参与者两轮就可重构秘密。Lee^[3]提出了公平的理性秘密共享方案，其中恶意参与者的数量 $v < \frac{t}{2}$ ，该方案采用异步广播信道，最终参与者有相同的概率重构出秘密。Tian 等^[4]研究秘密共享协议的公平性问题，提出公平的秘密分发和重构方案，分别在 3 种攻击模型下证明了方案的公平性和安全性。Cai 等^[5]提出理性秘密共享协议，解决了协议的公平性问题。Damgard 等^[6]针对 $t < \frac{n}{5}$ 贿赂的情况，设计了一个三轮协议，并保证了公平性，协议要求私密的点对点通道，但是建立这些需要额外增加轮数。2012 年，Asharov 等^[7]提出著名的五轮协议，并且保证了公平性。在拥有少数恶意者的多方情况下，Garg 等^[8]提出一个两轮协议，但是该协议没有保证公平性。2014 年，De 等^[9]通过引入包括获得秘密的效用和计算产生的花费的混合效用模型，提出了针对偏好尽可能少的通信和计算量的“silent”成员及偏好最大化自身利益的“non-silent”成员的分发者公平理性秘密共享方案，该方案的通信复杂度与秘密分发者选取的参数 β 有关。随后，Gordon 等^[10]指出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的中止行为。2015 年，刘海等^[11]基于重构顺序调整机制提出公平理性秘密共享方案，该方案基于秘密分发者随机选取重构轮数，设计具有未知重构轮数的理性秘密共享方案，有效约束了参与者的自利行为，并且该方案实现了子博弈完美均衡。

明了电子签名交换是不可行的。Ong 等^[2]提出一个适用于任何门限秘密共享方案的秘密重构协议，并且证明了当存在少数诚实参与者和绝大多数理性参与者的情况下，该协议是公平的，参与者两轮就可重构秘密。Lee^[3]提出了公平的理性秘密共享方案，其中恶意参与者的数量 $v < \frac{t}{2}$ ，该方案采用异步广播信道，最终参与者有相同的概率重构出秘密。Tian 等^[4]研究秘密共享协议的公平性问题，提出公平的秘密分发和重构方案，分别在 3 种攻击模型下证明了方案的公平性和安全性。Cai 等^[5]提出理性秘密共享协议，解决了协议的公平性问题。Damgard 等^[6]针对 $t < \frac{n}{5}$ 贿赂的情况，设计了一个三轮协议，并保证了公平性，协议要求私密的点对点通道，但是建立这些需要额外增加轮数。2012 年，Asharov 等^[7]提出著名的五轮协议，并且保证了公平性。在拥有少数恶意者的多方情况下，Garg 等^[8]提出一个两轮协议，但是该协议没有保证公平性。2014 年，De 等^[9]通过引入包括获得秘密的效用和计算产生的花费的混合效用模型，提出了针对偏好尽可能少的通信和计算量的“silent”成员及偏好最大化自身利益的“non-silent”成员的分发者公平理性秘密共享方案，该方案的通信复杂度与秘密分发者选取的参数 β 有关。随后，Gordon 等^[10]指出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的中止行为。2015 年，刘海等^[11]基于重构顺序调整机制提出公平理性秘密共享方案，该方案基于秘密分发者随机选取重构轮数，设计具有未知重构轮数的理性秘密共享方案，有效约束了参与者的自利行为，并且该方案实现了子博弈完美均衡。

明了电子签名交换是不可行的。Ong 等^[2]提出一个适用于任何门限秘密共享方案的秘密重构协议，并且证明了当存在少数诚实参与者和绝大多数理性参与者的情况下，该协议是公平的，参与者两轮就可重构秘密。Lee^[3]提出了公平的理性秘密共享方案，其中恶意参与者的数量 $v < \frac{t}{2}$ ，该方案采用异步广播信道，最终参与者有相同的概率重构出秘密。Tian 等^[4]研究秘密共享协议的公平性问题，提出公平的秘密分发和重构方案，分别在 3 种攻击模型下证明了方案的公平性和安全性。Cai 等^[5]提出理性秘密共享协议，解决了协议的公平性问题。Damgard 等^[6]针对 $t < \frac{n}{5}$ 贿赂的情况，设计了一个三轮协议，并保证了公平性，协议要求私密的点对点通道，但是建立这些需要额外增加轮数。2012 年，Asharov 等^[7]提出著名的五轮协议，并且保证了公平性。在拥有少数恶意者的多方情况下，Garg 等^[8]提出一个两轮协议，但是该协议没有保证公平性。2014 年，De 等^[9]通过引入包括获得秘密的效用和计算产生的花费的混合效用模型，提出了针对偏好尽可能少的通信和计算量的“silent”成员及偏好最大化自身利益的“non-silent”成员的分发者公平理性秘密共享方案，该方案的通信复杂度与秘密分发者选取的参数 β 有关。随后，Gordon 等^[10]指出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的中止行为。2015 年，刘海等^[11]基于重构顺序调整机制提出公平理性秘密共享方案，该方案基于秘密分发者随机选取重构轮数，设计具有未知重构轮数的理性秘密共享方案，有效约束了参与者的自利行为，并且该方案实现了子博弈完美均衡。

明了电子签名交换是不可行的。Ong 等^[2]提出一个适用于任何门限秘密共享方案的秘密重构协议，并且证明了当存在少数诚实参与者和绝大多数理性参与者的情况下，该协议是公平的，参与者两轮就可重构秘密。Lee^[3]提出了公平的理性秘密共享方案，其中恶意参与者的数量 $v < \frac{t}{2}$ ，该方案采用异步广播信道，最终参与者有相同的概率重构出秘密。Tian 等^[4]研究秘密共享协议的公平性问题，提出公平的秘密分发和重构方案，分别在 3 种攻击模型下证明了方案的公平性和安全性。Cai 等^[5]提出理性秘密共享协议，解决了协议的公平性问题。Damgard 等^[6]针对 $t < \frac{n}{5}$ 贿赂的情况，设计了一个三轮协议，并保证了公平性，协议要求私密的点对点通道，但是建立这些需要额外增加轮数。2012 年，Asharov 等^[7]提出著名的五轮协议，并且保证了公平性。在拥有少数恶意者的多方情况下，Garg 等^[8]提出一个两轮协议，但是该协议没有保证公平性。2014 年，De 等^[9]通过引入包括获得秘密的效用和计算产生的花费的混合效用模型，提出了针对偏好尽可能少的通信和计算量的“silent”成员及偏好最大化自身利益的“non-silent”成员的分发者公平理性秘密共享方案，该方案的通信复杂度与秘密分发者选取的参数 β 有关。随后，Gordon 等^[10]指出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的中止行为。2015 年，刘海等^[11]基于重构顺序调整机制提出公平理性秘密共享方案，该方案基于秘密分发者随机选取重构轮数，设计具有未知重构轮数的理性秘密共享方案，有效约束了参与者的自利行为，并且该方案实现了子博弈完美均衡。

明了电子签名交换是不可行的。Ong 等^[2]提出一个适用于任何门限秘密共享方案的秘密重构协议，并且证明了当存在少数诚实参与者和绝大多数理性参与者的情况下，该协议是公平的，参与者两轮就可重构秘密。Lee^[3]提出了公平的理性秘密共享方案，其中恶意参与者的数量 $v < \frac{t}{2}$ ，该方案采用异步广播信道，最终参与者有相同的概率重构出秘密。Tian 等^[4]研究秘密共享协议的公平性问题，提出公平的秘密分发和重构方案，分别在 3 种攻击模型下证明了方案的公平性和安全性。Cai 等^[5]提出理性秘密共享协议，解决了协议的公平性问题。Damgard 等^[6]针对 $t < \frac{n}{5}$ 贿赂的情况，设计了一个三轮协议，并保证了公平性，协议要求私密的点对点通道，但是建立这些需要额外增加轮数。2012 年，Asharov 等^[7]提出著名的五轮协议，并且保证了公平性。在拥有少数恶意者的多方情况下，Garg 等^[8]提出一个两轮协议，但是该协议没有保证公平性。2014 年，De 等^[9]通过引入包括获得秘密的效用和计算产生的花费的混合效用模型，提出了针对偏好尽可能少的通信和计算量的“silent”成员及偏好最大化自身利益的“non-silent”成员的分发者公平理性秘密共享方案，该方案的通信复杂度与秘密分发者选取的参数 β 有关。随后，Gordon 等^[10]指出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的中止行为。2015 年，刘海等^[11]基于重构顺序调整机制提出公平理性秘密共享方案，该方案基于秘密分发者随机选取重构轮数，设计具有未知重构轮数的理性秘密共享方案，有效约束了参与者的自利行为，并且该方案实现了子博弈完美均衡。

明了电子签名交换是不可行的。Ong 等^[2]提出一个适用于任何门限秘密共享方案的秘密重构协议，并且证明了当存在少数诚实参与者和绝大多数理性参与者的情况下，该协议是公平的，参与者两轮就可重构秘密。Lee^[3]提出了公平的理性秘密共享方案，其中恶意参与者的数量 $v < \frac{t}{2}$ ，该方案采用异步广播信道，最终参与者有相同的概率重构出秘密。Tian 等^[4]研究秘密共享协议的公平性问题，提出公平的秘密分发和重构方案，分别在 3 种攻击模型下证明了方案的公平性和安全性。Cai 等^[5]提出理性秘密共享协议，解决了协议的公平性问题。Damgard 等^[6]针对 $t < \frac{n}{5}$ 贿赂的情况，设计了一个三轮协议，并保证了公平性，协议要求私密的点对点通道，但是建立这些需要额外增加轮数。2012 年，Asharov 等^[7]提出著名的五轮协议，并且保证了公平性。在拥有少数恶意者的多方情况下，Garg 等^[8]提出一个两轮协议，但是该协议没有保证公平性。2014 年，De 等^[9]通过引入包括获得秘密的效用和计算产生的花费的混合效用模型，提出了针对偏好尽可能少的通信和计算量的“silent”成员及偏好最大化自身利益的“non-silent”成员的分发者公平理性秘密共享方案，该方案的通信复杂度与秘密分发者选取的参数 β 有关。随后，Gordon 等^[10]指出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的中止行为。2015 年，刘海等^[11]基于重构顺序调整机制提出公平理性秘密共享方案，该方案基于秘密分发者随机选取重构轮数，设计具有未知重构轮数的理性秘密共享方案，有效约束了参与者的自利行为，并且该方案实现了子博弈完美均衡。

2 基本知识

本节主要介绍双变量单向函数、双线性映射、效用函数和扩展式博弈相关知识。

定义 1 双变量单向函数。

若 $E = f(x, y)$ 满足以下 6 个性质，则称其为双变量单向函数。

- 1) 给定 x 、 y 容易计算出 $E = f(x, y)$ 。
- 2) 给定 x 和 E ，很难计算出 y 的值。
- 3) 不知道 y 时，对任意的 x ，很难计算出 E 的值。
- 4) 给定 y ，很难找到 2 个不同的 x_1, x_2 使 $f(x_1, y) = f(x_2, y)$ 。
- 5) 给出 x 和 E ，很难计算出 y 。
- 6) 给出 x_1 和 $f(x_1, y)$ ，很难计算出 $f(x_2, y)$ 的值。

定义 2 双线性映射。

设 G_1 和 G_2 分别是阶为素数 q 的加法群和乘法群， P 是 G_1 的一个生成元。若映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足以下 3 个条件则称映射 e 为双线性映射。

- 1) 双线性。对 $\forall P, Q \in G_1, a, b \in \mathbb{Z}_q^*$ 有 $e(aP, bQ) = e(P, Q)^{ab}$ 。
- 2) 非退化性。若 P 是 G_1 的生成元，则 $e(P, P)$ 是 G_2 的生成元，即 $e(P, P) \neq 1$ 。
- 3) 可计算性。对 $\forall P, Q \in G_1$ ，总存在有效的算法计算 $e(P, Q)$ 。

定义 3 双线性 Diffie-Hellman 问题 (BDHP)。

在 (G_1, G_2, e) 中，给定 (P, aP, bP, cP) ，对任意的 $a, b, c \in \mathbb{Z}_q^*$ ，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。

定义 4 效用函数。

在理性秘密共享协议中，理性参与者根据利益最大化采取行动，即基于每一步收到的所有信息决定其行动策略。本文定义理性参与者 P_i 的效用函数 $u_i: \{0, 1\}^n \rightarrow S_R, S_R$ 表示秘密重构后所有可能的结果。向量 $\mathbf{O}: (o_1, o_2, \dots, o_n) \in \{0, 1\}^n$ 表示所有理性参与者秘密重构的一个结果。当且仅当 $o_i = 1$ 时，理性参与者 P_i 得到了共享秘密，否则 $o_i = 0$ 。理性参与者 P_i 效用函数 u_i 满足：

1) 对 $\forall \mathbf{O}, \mathbf{O}' \in \{0,1\}^n$, 如果 $o_i > o'_i$, 则 $u_i(\mathbf{O}) > u_i(\mathbf{O}')$;

2) 如果 $o_i = o'_i$ 且 $\sum_{i=1}^n o_i < \sum_{i=1}^n o'_i$, 则 $u_i(\mathbf{O}) > u_i(\mathbf{O}')$ 。

因此, 对理性参与者 P_i 来说, 首先, 他想要独得秘密; 其次, 想要更少的其他参与者得到秘密。本文用以下 4 种情况表示 P_i 收益。

1) $u_i = U^+$ 表示理性参与者 P_i 独得共享秘密获得的收益。

2) $u_i = U$ 表示所有人都得到秘密时 P_i 的收益。

3) $u_i = U^-$ 表示所有人均没有得到秘密时 P_i 的收益。

4) $u_i = U^-$ 表示 P_i 没有得到秘密, 其余人均得到秘密时的收益。

定义 5 扩展式博弈。

扩展式博弈是一个六元组 $G = \{P, A, H, F, I, U\}$, 具体描述如下。

1) $P = \{P_1, P_2, \dots, P_n\}$ 表示理性参与者集合, 其中, P_i 表示第 $i (i=1, 2, \dots, n)$ 个理性参与者, P_{-i} 表示除了理性参与者 P_i 外其余所有理性参与者的集合。

2) $A = \{A_1, A_2, \dots, A_n\}$ 表示 n 个理性参与者的策略集。其中, $A_i = \{a_i^1, a_i^2, \dots, a_i^k\}$ 是理性参与者 P_i 的策略集, $a_i^j \in A_i (i=1, 2, \dots, k)$ 是理性参与者 P_i 的第 j 种策略, $a = (a_1, a_2, \dots, a_n)$ 表示每一个理性参与者选择一个策略 $a_i \in A_i (1 \leq i \leq n)$ 组成的策略组合。除理性参与者 P_i 外, 其余理性参与者的策略组合表示为 $a_{-i} = (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$ 。策略组合 $a = (a_1, a_2, \dots, a_n)$ 和 $a' = (a'_1, a'_2, \dots, a'_n)$, $(a'_i, a_{-i}) = (a_1, \dots, a_{i-1}, a'_i, a_{i+1}, \dots, a_n)$ 表示理性参与者 P_i 的行动策略为 a'_i , 其余理性参与者策略组合为 $a_{-i} = (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$ 。

3) H 表示历史序列集合。 $h = \{a_k\}_{k=1,2,\dots,K} \in H$ 表示长度为 K 的历史。对 $\forall h \in H$, h 随后可能出现的所有策略组合用 $A(h) = \{a | (h, a) \in H\}$ 表示, 若 $A(h) = \emptyset$, 那么历史序列 h 是终止的, Z 表示所有终止节点组成的集合。

4) $F: H/Z \rightarrow P$ 表示为非终止历史 $h \in H/Z$ 指定下一步采取行动的理性参与者。

5) $I = \{I_1, I_2, \dots, I_n\}$ 表示信息分割的集合, 其中, $I_i = \{I_i^1, I_i^2, \dots, I_i^K\}$ 表示理性参与者 P_i 对历史 $\{h \in H | F(h) = P_i\}$ 的信息集。如果 $h, h' \in I_i^j (1 \leq$

$j \leq K)$, 当理性参与者处在同一信息集中时, 有 $A(h) = A(h')$ 。

6) $U = \{u_1, u_2, \dots, u_n\}$ 表示 n 个理性参与者的效用函数的集合。 u_i 表示理性参与者 P_i 的效用函数。 $u_i(a)$ 表示当参与者采取策略组合 a 时, P_i 的效用。

定义 6 纳什均衡。

在博弈三元组 $\Gamma = \{N, S, U\}$ 中, 策略组合 $a = (a_1, a_2, \dots, a_n) \in A$ 是 Γ 的一个纳什均衡, 如果对理性参与者 $P_i (i=1, 2, \dots, n)$, 所有的 $a'_i \in A$, 都有 $u_i(a) \geq u_i(a'_i, a_{-i})$ 成立。

3 公平理性秘密共享方案

3.1 参数假设

本方案假设秘密分发者 D 要在 n 个理性参与者 $P_i (i=1, 2, \dots, n)$ 间共享秘密 $S \in Z_q^*$, 一个公开可见的公告板 B 用于记录公开信息, U_i 表示重构结束后, 除惩罚值外, 理性参与者 P_i 获得的收益。

3.2 惩罚机制

在理性参与者重构秘密过程中, 若发生偏离协议的行为, 则该参与者将会得到一个公开的惩罚值 $U_p < 0$, 被记录在公告板上, 并且协议终止。

定义 7 惩罚机制。

如果 P_i 公开的是假份额, 则 $P_j (j \neq i)$ 向其余所有理性参与者广播 P_i 是欺骗者, 并在公告板上记录下对 P_i 的惩罚值 U_p^i ($U_p^i < 0$ 且 $U_i^+ + U_p^i < U$)。

注: 协议开始前每个参与者均没有获得惩罚值。

定理 1 定义 7 所述惩罚机制为激励相容机制。

证明 若理性参与者 P_i 偏离协议, 根据惩罚机制, $P_j (j \neq i)$ 会在公告板 B 上记录对 P_i 的惩罚值且协议终止, 即使 P_i 能获得秘密, 但其得到一个公开的惩罚值, 使其最终收益小于 U , 这与理性参与者追求自身利益最大化相矛盾。因此, 理性参与者按照协议执行是最佳策略。所以, 本文利用的惩罚机制是激励相容机制。

3.3 秘密分发协议

Step1 秘密分发者 D , 将理性参与者 n 每 3 个人分为一组, 共 k 组 (这里只考虑 n 为 3 的整

数倍的情况), 即计算 $\frac{n}{3} = k$, 随机选取 $r^* \in (1, k)$, 记 $S_{r^*} = S$, 在集合 Z_q^* 中随机选取 $k-1$ 个整数, 分别记为 $S_1, S_2, \dots, S_{r^*-1}, S_{r^*+1}, \dots, S_k$, 满足 $S_1 < S_2 < \dots < S_{r^*-1} < S_{r^*} > S_{r^*+1} > \dots > S_k$ 和 $S_1 + S_2 + \dots + S_{r^*-1} + S_{r^*+1} + \dots + S_k = S_{r^*}$ 。

Step2 秘密分发者 D 计算并公开对所有 S_i 的承诺 $C_{i0} = C(S_i) = e(S_i P, P + Q)$, 其中 $i = 1, 2, \dots, k$ 。

Step3 秘密分发者 D 利用双变量单向函数 $E = F(x, y)$, 计算 $E_i = F(S_i, y)$, 并公开 E_i 和 y , 其中 $i = 1, 2, \dots, k$ 。

Step4 秘密分发者 D 随机选取 $a_{i0}, a_{i1}, a_{i2} \in Z_q^*, i = 1, 2, \dots, k$, 构造多项式 $f_i(x) = a_{i0} + a_{i1}x + a_{i2}x^2$, 其中 $a_{i0} = S_i$ 。计算并公开对系数的承诺 $C_{ij} = C(a_{ij})$, 其中 $j = 1, 2$ 。

Step5 秘密分发者 D 随机选取 $g_{il}(x) = b_{i0} + b_{i1}x + b_{i2}x^2, l = 1, 2, 3$, 计算 $C_{i0} = C(r_{i0}) = e(r_{i0}P, P + Q)$, 其中 $r_{i0} = b_{i0}$, 计算并公开对系数的承诺 $C_{ilj} = C(b_{ilj})$, 其中 $j = 1, 2$ 。

Step6 秘密分发者 D 计算每个多项式的值, 分别标记为 $(r_{i11}, r_{i12}, r_{i13}) = (g_{i1}(1), g_{i1}(2), g_{i1}(3))$, $(r_{i21}, r_{i22}, r_{i23}) = (g_{i2}(1), g_{i2}(2), g_{i2}(3))$, $(s_{i1}, s_{i2}, s_{i3}) = (f_i(1), f_i(2), f_i(3))$, $(r_{i31}, r_{i32}, r_{i33}) = (g_{i3}(1), g_{i3}(2), g_{i3}(3))$ 。

Step7 秘密分发者 D 将子秘密份额 $(r_{i11}, r_{i21}, s_{i1})$ 、 $(r_{i12}, r_{i22}, s_{i2})$ 、 $(r_{i13}, r_{i23}, s_{i3}, r_{i33})$ 分别分发给第 i 组中的 3 个理性参与者, 且每个理性参与者只知道自己和其他参与者的份额数只相差 1, 理性参与者得到份额后可利用

$$C(r_{ilm}) = \prod_{j=0}^2 C_{ilj}^{m^j} \quad (1)$$

$$C(s_{im}) = \prod_{j=0}^2 C_{ij}^{m^j} \quad (2)$$

验证份额的正确性 ($m = 1, 2, 3$)。

3.4 秘密重构协议

在得到分发者分发的秘密份额后, 参与者只知道自己的份额与其他成员相比至多相差 1, 并不知道在第几轮能重构出真正有用的份额。

1) 组内重构协议 (第 i 组 $i = 1, 2, \dots, k$)

Round1 3 个理性参与者分别公开第一个份

额 $(r_{i11}, r_{i12}, r_{i13})$, 利用式(1)验证子秘密份额的正确性, 若理性参与者 P_i 公开的子秘密份额不正确, 则在公告板 B 上记录 P_i 是欺骗者, 且给其一个惩罚值 U_p , 将其剔除出局, 协议停止。若正确, 则利用拉格朗日差值多项式计算 b_{i10} 。

$$b_{i10} = \sum_{m \in B} \left(r_{i1m} \prod_{\alpha \in B \setminus \{m\}} \frac{x - x_\alpha}{x_m - x_\alpha} \right) \bmod q \quad (3)$$

验证 $E_i \neq F(b_{i10}, y)$, 则转入下一轮。

Round2 3 个理性参与者分别公开第二个份额 $(r_{i21}, r_{i22}, r_{i23})$, 利用式(1)验证子秘密份额的正确性, 若理性参与者 P_i 公开的子秘密份额不正确, 则在公告板 B 上记录 P_i 是欺骗者, 且给其一个惩罚值 U_p , 将其剔除出局, 协议停止。若正确, 则利用拉格朗日差值多项式计算子秘密 b_{i20} 。

$$b_{i20} = \sum_{m \in B} \left(r_{i2m} \prod_{\alpha \in B \setminus \{m\}} \frac{x - x_\alpha}{x_m - x_\alpha} \right) \bmod q \quad (4)$$

验证 $E_i \neq F(b_{i20}, y)$, 则转入下一轮。

Round3 3 个理性参与者分别公开第一个份额 (s_{i1}, s_{i2}, s_{i3}) , 利用式(2)验证子秘密份额的正确性, 若理性参与者 P_i 公开子秘密份额不正确, 则在公告板 B 上记录 P_i 是欺骗者, 且给予其一个惩罚值 U_p , 将其剔除出局, 协议停止。若正确, 则利用拉格朗日差值多项式计算子秘密 a_{i0} 。

$$a_{i0} = \sum_{m \in B} \left(s_{im} \prod_{\alpha \in B \setminus \{m\}} \frac{x - x_\alpha}{x_m - x_\alpha} \right) \bmod q \quad (5)$$

若验证 $E_i = F(a_{i0}, y)$ 成立, 则记 $a_{i0} = S_i$, 进入组间重构协议。

2) 组间重构协议

k 个组各选出一名代表依次在公告板上写下本组在组间重构得到的 $S_i (i = 1, 2, \dots, k)$, 并利用公开的双变量单向函数值及其公开参数, 验证该 S_i 是否正确, 若第 i 组公开的是正确的 S_i , 则第 $i+1$ 组将本组得到的 S_{i+1} 公开, 当某个 S_i 满足 $S_1 < S_2 < \dots < S_{i-1} < S_i > S_{i+1} > \dots > S_k$ 时, 理性参与者将得到共享秘密 $S_i = S_{r^*} = S$ 。

4 方案分析

下面对本文所提理性秘密共享方案的正确性、安全性和公平性进行分析。

4.1 正确性分析

下面证明式(1)的正确性。

证明 因为 $r_{ilm} = g_{il}(m)$ ，所以

$$\begin{aligned} C(r_{ilm}) &= e(g_{il}(m)P, P+Q) \\ &= e((b_{il0} + b_{il1}m + b_{il2}m^2)P, P+Q) \\ &= e(P, P)^{b_{il0}} e(P, Q)^{b_{il1}m} e(P, P)^{b_{il2}m^2} \\ &= C_{il0} C_{il1}^m C_{il2}^{m^2} = \prod_{j=0}^2 C_{ilj}^{m^j} \end{aligned}$$

同理可得式(2)的正确性。

在秘密份额分发阶段，当理性参与者 P_i 收到秘密分发者 D 发送来的子秘密份额，利用式(1)和式(2)验证子份额的正确性，从而防止分发者的欺骗行为。在秘密重构阶段，当 P_i 得到其他 2 个参与者的子秘密份额，首先，利用式(1)和式(2)验证其份额的正确性，可以防止理性参与者的欺骗行为，当 3 个成员都公开正确份额时，可利用拉格朗日差值多项式(3)~式(5)计算出秘密 S_i ；然后，进行最后一轮组间比较，最大的即为分发者要共享的真正子秘密 S ，并且可以利用公告板 B 上公开的双变量单向函数的公开值，验证秘密 S 的正确性。

4.2 安全性分析

引理 1 在上述方案中，对多项式 $f_i(x)$ 系数 a_{i0}, a_{i1}, a_{i2} 的承诺 C_{i0}, C_{i1}, C_{i2} 是安全的，当且仅当 BDH 假设成立。

证明 必要性（反证法）。假设本文方案中的承诺函数是安全的，但 BDH 假设不成立。因为 BDH 假设不成立，所以存在一个有效算法 A ：对群 G_1 中给定的 $P, aP, bP, cP (a, b, c \in Z_q^*)$ 算法 A 成功计算出 $e(P, P)^{abc}$ 的概率为 ε 。接下来，证明算法 A 可以攻破上述承诺函数。随机选取 $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in Z_q^*$ ，分别将 $(P, \alpha P, \beta P, \gamma P)$ 和 $(P, \alpha' P, \beta' P, \gamma' P)$ 作为算法 A 的输入，由 BDH 假设不成立可知，算法 A 成功输出 $e(P, P)^{\alpha\beta\gamma}$ 和 $e(P, P)^{\alpha'\beta'\gamma'}$ 的概率为 ε ，又因 $C_{im} = e(P, P)^{\alpha\beta\gamma}$ ， $e(P, P)^{\alpha'\beta'\gamma'}$ ，即 $e((\alpha\beta\gamma)P, P) = \frac{C(f_{im})}{e(P, P)^{\alpha'\beta'\gamma'}}$ ，因此得出 f_{im} ，这与承诺函数是安全的相矛盾。所以，如果上述承诺函数是安全的，则 BDH 假设成立。

充分性（反证法）。假设 BDH 假设成立，但

上述方案中的承诺函数是不安全的。因此，存在有效算法 B ：将群 G_1 中的任意元素 Q_1, Q_2, Q_3 作为算法 B 的输入，算法 B 可以成功计算出 f_{im} 的概率为 ε ，满足 $C_{im} = e(f_{im}P, P+P) = e(Q_1, Q_2+Q_3)$ 。设 $f_{im} = \alpha P$ ， $\alpha \in Z_q^*$ 和 $Q_1 = \alpha_1 P, Q_2 = \alpha_2 P, Q_3 = \alpha_3 P (\alpha_1, \alpha_2, \alpha_3 \in Z_q^*)$ 算法 B 能成功计算出 f_{im} 的概率为 ε 且满足 $e(\alpha_1 P, \alpha_2 P + \alpha_3 P) = e(\alpha P, P+P)$ ，即为 $e(P, P)^{\alpha_1(\alpha_2+\alpha_3)} = e(P, P)^{2\alpha} \Rightarrow e(P, P)^{2^{-1}\alpha^{-1}\alpha_1(\alpha_2+\alpha_3)}$ ，令 $a = 2^{-1}\alpha^{-1}$ ， $b = \alpha_1$ ， $c = \alpha_2 + \alpha_3$ 则算法 B 可以成功计算出 $e(P, P)^{abc}$ ，这与 BDH 假设成立相矛盾。因此，如果 BDH 假设成立，则本文方案中的承诺函数是安全的。

同理可得，对多项式系数 $g_{il}(x)$ 系数的承诺也是安全的，当且仅当 BDH 假设成立。

引理 2 任何理性参与者都不可能伪造一个秘密 S^* ，满足双变量单向函数 $E = F(S^*, y)$ 。

证明 根据双变量单向函数的 6 个性质知，任何理性参与者都不可能伪造一个 S'_i 使 $F(S'_i, y) = F(S_i, y) = E_i$ 。

4.3 公平性分析

对所有理性参与者 P_i ，分别考虑以下几种情况。

1) 若参与者 P_i 均按照协议执行，则所有参与者都能得到共享秘密 S 。

2) 在组内重构阶段，每个参与者不知道自己的份额比其他 2 个成员的份额数量是多 1 个还是少 1，最好的策略就是按照协议执行，可得本组的共享子秘密，才会有进入组间重构的机会。若有一个参与者 P_j 在此阶段最终重构轮前偏离协议，公开假的子秘密份额，则该参与者不能通过承诺值验证，被剔除出局，并在公告板 B 上记录 P_j 是欺骗者，且给 P_j 一个惩罚值 U_p ，协议结束，所有参与者均没有得到共享秘密。若 P_j 在最终重构轮偏离协议，将被检测出来， P_j 猜中该轮是子秘密重构轮的概率最大为 $\frac{1}{3}$ ，而其得到的子秘密

正好是真正子秘密 S_r 的概率为 $\frac{1}{Z_q^*}$ ，其余组可以经过组内重构得出子秘密，通过求和可以得到真正共享秘密 S 。此时，所有参与者均得到共享秘密。

3) 在组间重构阶段，若有一个参与者 P_j 偏离协议，则不能通过承诺值验证，会被剔除出局，并在公告板 B 上记录 P_j 是欺骗者，且给 P_j 一个惩

罚值 U_p ，其猜中自己重构出的秘密是真正秘密的概率为 $\frac{1}{Z_q^*}$ ，其他参与者通过求和可得到真正共享

秘密 S 。此时，所有参与者均得到真正共享秘密。

4.4 纳什均衡分析

定理 2 如果协议的参与者均是理性的，则在 BDH 假设下，本文方案可以实现纳什均衡 $U, U, \dots, U$ 。

证明 在方案中的组内重构阶段，每组内的任意 2 个理性参与者子秘密份额的数量都不超过 1。在本方案中第 3 轮之前，第 i 组内的理性参与者 P_{i1} 没有得到组内其他成员的所有子秘密份额，因此，所有成员均会按照协议执行。在最后一轮时，可能会出现以下 2 种情况。

1) 若组内所有成员的子秘密份额数都相等，在最后一轮，第 i 组内的理性参与者 P_{i1} 不确定另 2 个成员 P_{i2} 、 P_{i3} 是否拥有多 1 个的子秘密份额，为了重构出完整的秘密，理性参与者均会在最后一轮广播真实的子秘密份额。

2) 若组内成员的子秘密份额数量相差 1，记第 i 组内的 3 个成员分别为 P_{i1} 、 P_{i2} 、 P_{i3} 其分别拥有的子秘密份额数量分别为 d_{i1} 、 d_{i2} 、 d_{i3} ，设 $d_{i1}=d_{i2}=d_{i3}-1$ ，在最后一轮，各参与者广播自己的子秘密份额，且期待在下一轮得到组内其他成员的子秘密份额，在下一轮， P_{i1} 、 P_{i2} 已经广播完自己所有的子秘密份额，但此时 P_{i3} 并不知道其他 2 个成员的子秘密份额已经广播完毕，并且希望得到下一轮 P_{i1} 、 P_{i2} 的子秘密份额。因此，理性参与者要想得到秘密，所有参与者都需按照协议执行。

在组间重构阶段，理性参与者依次在公告板 B 上公开自己重构的秘密，若第 i 组理性参与者在此阶段偏离协议，即使其得到真正的秘密份额 S ，其他参与者可以通过求和得到真正的共享秘

密 S ，并且在公告板上记录第 i 组欺骗，给予欺骗者一个惩罚值 U_p 。此时，欺骗组中的每个成员获得的最终收益为 $U_i = U + U_p < U$ 。因此，对理性参与者来说，最好的策略就是按照协议执行，并得到最终收益为 U 。

5 方案对比

在通信复杂度、通信类型、前提假设这 3 个方面，将本文方案与文献[5,7,9,11]方案进行对比分析，如表 1 所示，其中， b 为分发者随机选取的整数， β 表示概率参数， K 表示分发者从 $(2, Round)$ 中随机选取的整数。

由表 1 可知，在通信复杂度方面，文献[5,9,11]方案的通信轮数都与所选参数有关，文献[7]方案至少为 4 轮，本文方案仅需 4 轮即可重构秘密。在维护信道所需开销方面，文献[5,9,11]方案需要单一信道，本文方案需要 2 个信道，因此开销要比文献[5,9,11]方案稍高，但比文献[7]方案中要维护点对点信道安全所需开销要低的多，且本文方案不需要秘密分发者在线。因此，本文方案更能满足实用性需求。

6 结束语

本文基于重复博弈构造理性秘密共享方案，理性参与者按照协议执行会比偏离协议获得更多的收益。本文方案引入了惩罚机制，能够更好地维护诚实理性参与者的利益，结合承诺方案和双变量单向函数，可以有效地防止秘密分发者和理性参与者的欺骗行为，利用分组思想，可有效降低方案的计算量和通信复杂度，并且该方案实现了公平性。本文方案是在假设没有参与者合谋的情况下构造的，下一步将主要研究抗合谋攻击的理性秘密共享方案。

表 1 本文方案与其他公平理性秘密共享方案对比

方案	通信复杂度	信道类型	重构阶段前提假设
文献[5]	与 b 、 β 的选取有关	同时通信信道	不需要分发者在线
文献[7]	5	点对点通信信道	不需要分发者在线
文献[9]	与 β 的选取有关	同时通信信道	需要分发者在线
文献[11]	与 K 的选取有关	非同时通信信道	不需要分发者在线
本文方案	4	同时、非同时通信信道	不需要分发者在线

参考文献:

- [1] EVEN S, YACOBI Y. Relations among public key signature schemes[R]. Technion Computer Science Department Technical Report CS0175. 1980.
- [2] ONG S J, PARKES D C, ROSEN A, et al. Fairness with an honest minority and a rational majority[C]//The Conference on Theory of Cryptography. 2009:36-53.
- [3] LEE Y C. A simple (v, t, n) -fairness secret sharing scheme with one shadow for each participant[C]//The International Conference on Web Information Systems and Mining. 2011:384-389.
- [4] TIAN Y L, MA J F, PENG C G, et al. Secret sharing scheme with fairness[C]//2011 International Joint Conference on IEEE Trust-Com-11/IEEE ICESS-11/FCST-11. 2011:494-500.
- [5] CAI Y Q, PENG X Y. Rational secret sharing protocol with fairness[J]. Chinese Journal of Electronics, 2012, 21(1): 149-152.
- [6] DAMGÅRD I, ISHAI Y. Constant-round multiparty computation using a black-box pseudorandom generator[C]//Advances in Cryptology-CRYPTO. 2005: 378-394.
- [7] ASHAROV G, JAIN A, LÓPEZ-ALT A, et al. Multiparty computation with low communication, computation and interaction via threshold FHE[C]//Advances in Cryptology-EUROCRYPT. 2012: 483-501.
- [8] GARG S, GENTRY C, HALEVI S, et al. Two-round secure MPC from Indistinguishability obfuscation[M]//Theory of Cryptography. Berlin Heidelberg: Springer, 2014: 74-94.
- [9] DE S J, RUJ S, PAL A K. Should silence be heard? fair rational secret sharing with silent and non-silent players[M]//Cryptology and Network Security. Beilin: Springer, 2014:240-255.
- [10] GORDON S, LIU F H, SHI E. Constant-round MPC with fairness and guarantee of output delivery[C]//Advances in Cryptology-CTYPTO. 2015:63-82.
- [11] 刘海, 李兴华, 马建峰. 基于重构顺序调整机制的理性秘密共享

方案[J]. 计算机研究与发展, 2015, 52(10):2332-2340.

LIU H, LI X H, MA J F. Rational secret sharing scheme based on reconstructed sequential adjustment mechanism [J]. Journal of Computer Research and Development, 2015, 52 (10): 2332-2340.

作者简介:



李梦慧 (1991-), 女, 河南焦作人, 贵州大学硕士生, 主要研究方向为理性秘密共享协议效率优化。



田有亮 (1982-), 男, 贵州盘县人, 博士, 贵州大学教授, 主要研究方向为密码与安全协议及算法博弈论。



冯金明 (1993-), 男, 甘肃崆峒人, 贵州大学硕士生, 主要研究方向为可搜索加密。