理性公平的秘密共享方案

刘 海[1),2),3)] 李兴华[4),5)] 田有亮[3),6)] 雒 彬[4),5)] 马建峰[3),4),5)] 彭长根[3),6)]

[1)](贵州财经大学信息学院 贵阳 550025)

[2)](贵州财经大学数据与高性能计算国际联合研究中心 贵阳 550025)

[3)](贵州大学公共大数据国家重点实验室 贵阳 550025)

[4)](西安电子科技大学网络与信息安全学院 西安 710071)

[5)](西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)

[6)](贵州大学计算机科学与技术学院 贵阳 550025)

摘 要 理性秘密共享是将自利的理性用户引入到传统秘密共享中,力图在现实环境中实现公平的秘密重构,使得所有用户均能获得共享秘密.然而,由于忽略了理性用户的自利性行为,现有理性秘密共享的公平性定义允许出现用户不发送子秘密也能获得共享秘密的不公平情形.这导致在使用以该定义为指导所设计的理性秘密共享方案时,并不能确保所有用户均能获得共享秘密;甚至还会出现发送错误子秘密欺骗其他用户,导致其他用户将重构出的虚假的共享秘密视为真实秘密的极端情形.为解决该问题,本文结合秘密共享的存取结构,形式化定义了秘密共享的理性公平性.并以此为指导,通过在秘密分发阶段为每个理性用户发送大量虚假子秘密,使得理性用户难以准确猜测出真实共享子秘密的方法,设计一个混淆激励机制,并提出一个理性公平的秘密共享方案.理论分析和大量实验表明,该方案能有效地约束理性用户在秘密重构阶段的自利性行为,确保所有用户能获得真实的共享秘密,高效地实现公平的秘密共享.

关键词 理性秘密共享;理性公平;混淆;存取结构;激励机制

中图法分类号 TP391 **DOI 号** 10.11897/SP.J.1016.2020.01517

Rational Fair Secret Sharing Scheme

LIU Hai[1),2),3)] LI Xing-Hua[4),5)] TIAN You-Liang[3),6)] LUO Bin[4),5)]

MA Jian-Feng[3),4),5)] PENG Chang-Gen[3),6)]

[1)](*School of Information, Guizhou University of Finance and Economics, Guiyang* 550025)

[2)](*International Joint Research Center for Data Science and High-Performance Computing, Guizhou University of Finance and Economics, Guiyang* 550025)

[3)](*State Key Laboratory of Public Big Data, Guizhou University, Guiyang* 550025)

[4)](*School of Cyber Engineering, Xidian University, Xi'an* 710071)

[5)](*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071)

[6)](*College of Computer Science and Technology, Guizhou University, Guiyang* 550025)

Abstract With the development of communication technologies, the advanced technologies like cloud computing and IoT (Internet of Things) are emerging, which bring convenience and become part of our daily life. Unfortunately, when enjoying the convenient life, the users' privacy may disclose because they need to provide some individual sensitive data. To protect the users' privacy effectively, the cryptography participating in multi-user has attracted more attention, especially

收稿日期:2019-08-28;在线发布日期:2020-02-13.本课题得到国家自然科学基金(U1708262,U1736203,U1836205,61772008)、国家重点研发计划(2017YFB0801805)、贵州省科技计划项目(黔科合基础[2020]1Y265)、贵州财经大学校级科研基金项目(2019XYB17)资助.
刘 海,博士,主要研究方向为隐私保护和安全协议设计.E-mail:liuhai4757@163.com.**李兴华**(通信作者),博士,教授,主要研究领域为网络与信息安全、隐私保护和密码学.E-mail:xhli1@mail.xidian.edu.cn.**田有亮**,博士,教授,主要研究领域为博弈论、密码学与安全协议.**雒 彬**,博士研究生,主要研究方向为信任评估和隐私保护.**马建峰**,博士,长江学者特聘教授,主要研究领域为网络与信息安全、编码理论、密码学.**彭长根**,博士,教授,主要研究领域为数据隐私保护.

secret sharing. Secret sharing is one of the most common and classical distributed cryptographic schemes, which allows the certain number of users can obtain the secret together, but any subset of users of size less than the prescribed number cannot obtain the secret even they collude with others. In traditional secret sharing, the users are regarded as either honest or malicious. Honest users follow the prescribed scheme faithfully, whereas malicious users behave in arbitrary manners. However, in real applications, the users are selfish and always try to maximize their profits, which coincides with the selfish characteristic of rational users in game theory. Under this circumstance, rational secret sharing is proposed by introducing selfish users into traditional secret sharing, which assumes that the users prefer to obtain the secret above all else, otherwise prefer the fewest number of other users to obtain the secret. The purpose is to realize the fair secret reconstruction in real applications. Unfortunately, when directly adopting the existing rational secret sharing schemes, some unfair solutions arise, which lead that some of the users reconstruct the secret but not send the shares, whereas the others cannot obtain the secret after sending the shares. More seriously, some of the users can cheat the other users into viewing a fake secret as the real. The crucial reason is that, the users' selfish behaviors are not considered completely in the existing fairness definition of rational secret sharing, and the existing schemes are devised under the guidance of this fairness definition. To address this problem, this paper formalizes rational fairness of secret sharing by combining it with the minimum access structure, and demonstrates that the proposed definition allows the users to reconstruct the real secret only when both of them send the shares honestly. Furthermore, to show that the proposed fairness definition is meaningful, an incentive obfuscation mechanism is devised and an advanced rational secret sharing scheme is presented. In the proposal, a great quantity of fake shares are generated for rational users to make them not able to identify the real one, and the users are punished by not receiving any shares in the future when they do not send the shares honestly. In this way, none of users deviates from the scheme prescribed, thereby realizing the fair secret reconstruction. Through the comparisons of the existing schemes in applicable scenarios, reconstruction rounds, requirements on trust users, computation of rational users' payments, and other complicated cryptographic tools, the advantages of our scheme are analyzed to illustrate the usability. Additionally, the extensive experiments illustrate that the computation overhead and communication cost of the presented scheme are limited, indicating that our scheme can realize the fair secret reconstruction efficiently.

Keywords rational secret sharing; rational fairness; obfuscation; access structure; incentive mechanism

1 引 言

随着移动通信技术的不断发展,云计算、物联网、车联网、船联网等新兴技术不断普及.这在给人们带来便捷生活的同时,对用户的隐私保护也提出了新的挑战.为了有效保护万物互联时代下用户的个人隐私,多方参与的分布式密码方案受到了国内外学者的广泛关注[1].(t,n)秘密共享是多方参与的分布式密码方案的重要组成.其基本思想是:将共享秘密 K 拆分成 n 份子秘密分发给不同的用户,使得任意不少于 t 个的用户在一起就可恢复出共享秘密 K,而任意少于 t 个的用户即使合谋也得不到关于共享秘密 K 的任何信息.它已被广泛地用于保护移动通信[2]、数据查询[3]、云存储[4]、广告推送[5]等应用中的用户隐私.

在传统秘密共享的研究中,均假设用户是诚实或恶意的[6].然而,在现实中,用户既不是诚实的,也不是恶意的,而是自利的.自利的用户总是追求自身利益最大化.因此,若在现实应用中使用传统秘密共

享方案，当 $t-1$ 个用户发送自己的子秘密后，由于剩余的 $n-t+1$ 个用户已能重构出共享秘密，因此他们将不再发送自己的子秘密.此时，对已发送子秘密的用户来说，他们将无法重构出共享秘密.这显然是不公平的，从而极大地影响了传统秘密共享的实用性.

为了设计更贴近现实的秘密共享方案，Halpern 和 Teague[7]将博弈论的理性用户引入到传统秘密共享的研究中，通过分析自利的理性用户参与秘密共享时的偏好，首次提出理性秘密共享的概念.随后，理性秘密共享得到了国内外学者的广泛研究[8-11].然而，在使用现有的理性秘密共享方案时，仍不能确保所有用户都能重构出共享秘密；甚至还会出现发送子秘密的用户重构出一个虚假的秘密并将其视为真实共享秘密的极端情形.例如，某公司财务总监使用现有理性秘密共享方案将公司的财务账目作为共享秘密拆分后分发给公司的会计和出纳，当需要重构财务账单时，就可能会出现先发送自己拥有的子秘密的会计不能恢复出财务账单，而不发送自己拥有的子秘密的出纳却能恢复出财务账单的情形，使得出纳能通过修改财务账单来掩盖自己的腐败行为；又如某公司将未来的发展计划作为共享秘密拆分给产品研发和产品销售经理进行保存，当要恢复研发计划时，销售经理就可能通过发送错误的子秘密欺骗研发经理，使其将重构出的错误的发展计划视为真实的计划，影响公司发展，使得销售经理能通过上述欺骗行为非法获取来自其他竞争公司的额外收益.造成上述问题的根本原因是：由于忽略了理性用户的自利性行为，导致现有理性秘密共享的公平性定义允许出现“用户不正确地发送自己拥有的子秘密也能重构出共享秘密”的不公平情形.

为解决上述问题，本文通过分析理性用户的自利性行为，结合秘密共享的存取结构，给出了适用于理性用户参与的秘密共享的理性公平性定义，并从理论上证明了该公平性定义只允许出现“用户正确地发送自己拥有的子秘密给其余用户”的情形.此外，为表明所提出的理性公平性定义具有实用性，本文通过在秘密分发阶段为每个理性用户发送大量虚假子秘密，使得理性用户难以准确猜测出正确共享子秘密，一旦理性用户不发送自己拥有的子秘密，其在未来的秘密重构轮中将不会收到任何子秘密的方法，设计了一个理性公平的理性秘密共享方案.本文的主要贡献如下：

(1) 证明现有的公平性定义允许出现“用户不正确地发送自己拥有的子秘密也能重构出共享秘密”的不公平情形.并结合秘密共享的存取结构，给出了理性公平性的形式化定义.

(2) 以提出的理性公平性定义为指导，设计了一个混淆激励机制，并构造了一个理性公平的秘密共享方案.理论证明所提方案能有效约束理性用户的自利性行为，实现公平的秘密共享.

(3) 大量实验表明使用本方案时，秘密分发者和理性用户所需的计算代价和通信开销较小，具有较好的实用性.

2　相关工作

根据理性用户在秘密重构阶段交互时使用的通信类型，现有理性秘密共享方案可分为两类：基于同步通信的理性秘密共享方案和基于异步通信的理性秘密共享方案.

2.1　基于同步通信的理性秘密共享方案

Halpern 和 Teague[7]将博弈论中的理性用户引入到传统秘密共享中，提出了理性秘密共享的概念.他们通过分析理性用户参与秘密重构时的偏好，利用随机交互真实子秘密和虚假子秘密的方法设计了一个 (t,n) 理性秘密共享方案.然而，他们的方案并不适用于 $t=n=2$ 的情形.为解决上述问题，Gordon 和 Katz[12]在理性秘密重构中引入“观察员”来监视每轮通信中各理性用户的策略选择，并在后通信轮中对理性用户的选择策略进行指引，从而设计了首个 $(2,2)$ 理性秘密共享方案.Abraham 等人[13]指出理性用户在参与秘密重构时可能会合谋.为防止该情形的发生，他们在秘密分发阶段为每个理性用户分发多个秘密，并通过引入可信第三方来指定每轮交互的子秘密，提出防合谋的理性秘密共享方案.为不依赖可信第三方实现公平的理性秘密共享，Maleka 等人[14]将理性秘密重构阶段的交互过程视为多轮重复博弈，设计了一个随机交互轮数的理性秘密共享方案.随后，Maleka 等人[15]又指出在实际应用中，往往需要共享多个秘密，而重复使用上述方案将消耗理性用户大量的计算和通信资源.因此，他们在理性用户参与重复博弈时的收益函数中引入折扣因子，使得理性用户的收益随着交互轮数的增多而逐步减少，从而提出适用于多秘密共享的理性秘密共享方案.

当使用上述方案时，理性用户在秘密重构阶段中需进行多轮交互.为减少交互轮数，Micali 和 Shelat[16]基于密封拍卖模型，设计了一个只需 6 轮交互的理性秘密共享方案.Tian 等人[17]考虑理性用

户拥有的背景知识会影响其参与理性秘密重构时的策略选择,结合不完全信息博弈模型,提出了一个仅需 1 轮交互的理性秘密共享方案.然而,若直接使用该方案,即使所有的理性用户均诚实地参与秘密重构,也可能会出现没有任何用户能重构出共享秘密的特殊情形.为解决上述问题,Zhang 和 Liu[18] 采用多轮重复博弈的思想,通过不断调整理性用户参与秘密重构时选择不同策略的概率,实现公平的理性秘密重构.Asharov 和 Lindell[19] 指出原有方案为了确保公平性,均假设秘密分发者 Dealer 能准确地获知每个理性用户的收益函数,从而降低了方案的实用性.因此,他们利用安全多方计算,提出了一个不依赖理性用户收益的理性秘密共享方案.但是该方案仅适用于 $n\geq 3$ 的情形.

此外,Nojoumian 等人[20] 将理性秘密共享视为一类特殊的社会活动,提出社会理性秘密共享的概念.随后,Nojoumian 和 Stinson[21] 将信誉值作为一种特殊的货币,设计了仅需 1 轮交互的社会理性秘密共享方案.并且,为提高社会理性秘密共享方案的可用性,Nojoumian[22] 通过数据拟合的方法,给出了社会理性秘密共享中理性用户的收益函数.

然而,在现实应用中,如云存储数据访问控制、基于群组的位置服务查询等,同步通信难以实现,从而导致该类理性秘密共享方案的实用性较低.

2.2 基于异步通信的理性秘密共享方案

Kol 和 Naor[23] 利用健忘传输、安全多方计算等密码技术构造了首个适用于异步通信的理性秘密共享方案.在他们的方案中,每次交互只有一个理性用户发送子秘密,且不依赖可信第三方.但是,理性秘密分发者 Dealer 和理性用户的计算代价较大.为降低理性用户的资源消耗,Kol 和 Naor[24] 采用逆向归纳方法分析了理性用户在多轮子秘密交互过程中的策略选择,设计了信息论安全的理性秘密共享方案.为降低秘密分发者 Dealer 的资源消耗,Fuchsbauer 等人[25] 通过引入可验证的随机函数(verifiable random function)让理性用户在秘密重构阶段中不能确定其他理性用户发送的子秘密的正确性,使得理性用户不会偏离预定方案的执行.Zhang 和 Liu[26] 通过让理性用户只有遵从预定方案的执行,才能正确地获知子秘密交互轮数的方法来实现公平的理性秘密共享.Cai 和 Shi[27] 通过让秘密分发者 Dealer 在秘密分发阶段对分发的子秘密进行概率加密(probability encryption),避免后发送子秘密的理性用户能先验证重构出的共享秘密的真实性,从而确保理性秘密共享公平性.但是上述方案均要求秘密分发者 Dealer 准确地获知理性用户参与秘密重构的收益函数.

除上述采用密码技术来实现公平的理性秘密共享外,Wang 和 Cai[28] 通过让理性用户重复交互相同子秘密的方法,不断调整理性用户的策略选择,从而确保所有理性用户均能重构出共享秘密.Yu 和 Zhou[29] 指出需防止多个理性用户在子秘密交互中合谋.因此,他们通过分析理性用户在重复交互相同子秘密过程中的偏好变化,提出概率安全和公平的理性秘密共享方案.Wang 和 Xu[30] 考虑理性用户在理性秘密共享中的长远收益,通过减少理性用户长远收益的方法来约束理性用户的自利性行为.Jin 等人[31] 指出当理性用户考虑自己的长期收益时,理性用户参与秘密共享的收益函数将发生改变.因此,他们综合考虑理性用户短期收益(即是否重构出共享)和长远收益,给出理性用户的混合收益函数.为降低秘密分发者 Dealer 和理性用户的资源开销,Ong 等人[32] 通过引入诚实的参与用户,通过将参与用户划分为不同的群组,使得每个群组中均存在诚实用户,从而提出了需 2 轮交互的理性秘密共享方案.Dani 等人[33] 通过让理性用户延迟重构共享秘密的方法,设计了仅需 1 个子秘密交互轮的理性秘密共享方案.Tian 等人[34] 分析理性用户拥有的背景知识对其策略选择的影响,将理性用户信誉的增减作为一种奖惩,构造了仅需 1 轮交互的理性秘密共享方案.Kawachi 等人[35] 通过在秘密分发阶段分发不同的共享秘密,并指定理性用户在秘密重构阶段中发送子秘密的先后顺序,提出了仅需 3 轮子秘密交互就能实现公平的理性秘密共享.但是上述方案均要求存在可信第三方/用户.

此外,Sourya 等人[36] 对理性用户在秘密重构阶段选择“不发送任何子秘密”的策略进行分析,探讨了理性用户选择该策略时的收益.Zhang 等人[37]、Sourya 和 Ruj[38] 分别针对理性用户通信受限特殊情形下的理性秘密共享方案进行研究.Liu 等人[39] 将机制设计模型引入到理性秘密共享方案的设计,给出了设计理性秘密共享方案的参考模型.

然而,上述所有理性秘密共享方案在设计时均使用现有理性秘密共享的公平性定义为指导.由于现有理性秘密共享的公平性定义允许“理性用户不发送子秘密也能重构出共享秘密”,因此以该公平性定义为指导而设计出的理性秘密共享方案在实际使用时,会出现“发送子密钥的理性用户无法恢复出共享密钥,而不发送子密钥的用户却能重构出共享密钥”的不公平情形;甚至还会出现“发送错误的子秘

密欺骗其余理性用户，使其将重构出的错误秘密视为真实共享秘密”的极端情形.

3　预备知识

3.1　系统模型

理性秘密共享由两个阶段组成，分别是秘密分发阶段和秘密重构阶段. 在这两个阶段中，本文均采用无需可信第三方的分布式结构，如图 1 所示.

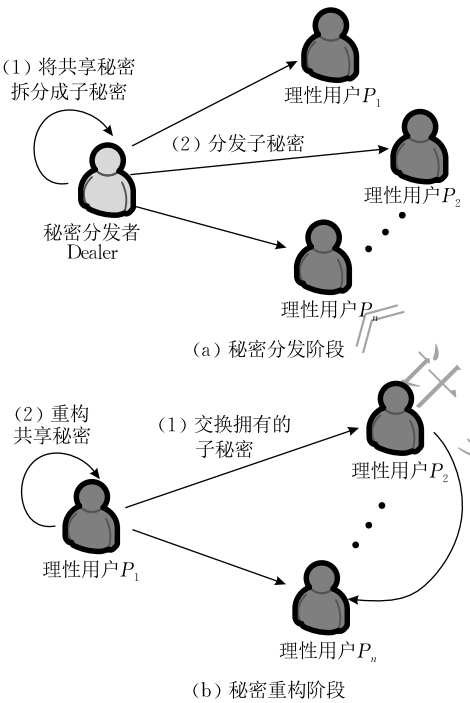


图 1　系统结构

(1) 秘密分发阶段

当要在理性用户 $P_1,P_2,\cdots,P_n$ 间共享秘密 K 时，秘密分发者 Dealer 在有限域 F_q 上随机选择 $t-1$ 个元素 $a_1,a_2,\cdots,a_{t-1}$ 构造多项式 $f(x)=K+\sum_{i=1}^{t-1}a_ix^i$，并计算 $f(i)$；然后将子秘密 $k_i=(i,f(i)\bmod q)$ 秘密地分发给理性用户 P_i. 当所有理性用户 P_i 收到子秘密 k_i 后，秘密分发者 Dealer 销毁共享 K，秘密分发结束. 其中，$K\in F_q$；$q>n$ 是大素数；$1\leq i\leq n$.

(2) 秘密重构阶段

当要恢复共享秘密 K 时，理性用户 P_i 将自己获得的子秘密 k_i 发送给理性用户 P_j，而理性用户 P_j 在收到子秘密 k_i 后就发送自己拥有的子秘密 k_j. 所有的理性用户交互完各自拥有的子秘密后，就可利用拉格朗日插值法计算 $K=f(0)=\sum_{i=1}^{t}l_i(0)f(i)$ 重构出共享秘密 K. 其中，$l_i(x)=\prod_{j=1,j\neq i}^{t}\frac{x-i}{i-j}$ 是拉格朗日插值基函数；$i\neq j$ 且 $1\leq i,j\leq n$.

3.2　理性秘密重构博弈

在理性秘密共享中，影响其公平性的主要原因是理性用户为了追求自身利益最大化，在秘密重构阶段中可能会发送错误的子秘密或者不发送任何子秘密给其余理性用户. 为更好地分析理性用户在理性秘密重构阶段中的策略选择，本文结合扩展型博弈模型，给出理性秘密重构博弈的形式化模型.

定义 1(理性秘密重构博弈模型). 理性秘密重构博弈 $G_S=\{P,A,F,H,U,\Theta\}$ 是一个六元组，具体解释如下：

(1) $P=\{P_1,P_2,\cdots,P_n\}$ 是参与秘密重构的理性用户集合. 其中，P_i 表示第 i 个理性用户；$P_{-i}=\{P_1,\cdots,P_{i-1},P_{i+1},\cdots,P_n\}$ 称为理性用户 P_i 的对手集合，是由理性用户 P_i 外的其余用户组成的集合；$1\leq i\leq n$.

(2) $A=\{A_1,A_2,\cdots,A_n\}$ 是理性用户的策略集合. $A_i=\{a_i^{\text{honest}},a_i^{\text{fake}},a_i^{\text{slient}}\}$ 是理性用户 P_i 的策略集合，其中 a_i^{honest} 表示理性用户 P_i 将自己拥有的子秘密正确地发送给其余用户；a_i^{fake} 表示理性用户 P_i 未将自己拥有的子秘密正确地发送给其余用户；a_i^{silent} 表示理性用户 P_i 不发送任何子秘密给其余用户. 策略组合 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$ 是由每个理性用户 P_i 选择一个策略 $a_i\in A_i$ 所组成的向量.

(3) H 是历史序列集合. $\forall\boldsymbol{h}\in H$，其表示在某时刻时已行动的理性用户所选择的策略组成的策略组合. 在 $\boldsymbol{h}$ 之后的可能出现的所有策略组合记为 $A(\boldsymbol{h})=\{\boldsymbol{a}|(\boldsymbol{h},\boldsymbol{a})\in H\}$. 空字符 $\hbar\in H$，表示理性秘密重构博弈 G_S 开始. 如果某历史 $\boldsymbol{h}'\in H$ 使得 $A(\boldsymbol{h}')=\varnothing$，则该历史 $\boldsymbol{h}'$ 称为终止的(即表示理性秘密重构博弈 G_S 结束)，其中 $\varnothing$ 是空集合. Z 表示由所有终止的历史组成的集合.

(4) $F:(H/Z)\rightarrow P$ 是理性用户分配函数. 它为未终止的历史 $\boldsymbol{h}\in H/Z$ 指定下一个选择策略的理性用户 $P_i\in P$. 当所有用户同时进行策略选择，即采用同步信道通信时，$F(\hbar)=P$.

(5) $U=\{u_1,u_2,\cdots,u_n\}$ 是理性用户的收益集合. $u_i:A_1\times A_2\times\cdots\times A_n\rightarrow\{W_i^+,W_i,W_i^-,W_i^{--}\}$ 是理性用户 P_i 参与理性秘密重构博弈 G_S 所得到的收益. 其中，W_i^+ 表示理性用户 P_i 重构出共享秘密，而其余理性用户未能重构出共享秘密时的收益；W_i 表示理性用户 P_i 重构出共享秘密，而其余理性用户也能重构共享秘密时的收益；W_i^- 表示理性用户 P_i 未能重构出共享秘密，而其余理性用户也未能重构出共享秘密时的收益；W_i^{--} 表示理性用户 P_i 未能重构

出共享秘密，而其余理性用户却重构出共享秘密时的收益.

(6) $\Theta=\{\theta_1,\theta_2,\cdots,\theta_n\}$ 是理性用户的偏好集合. 其中，$\theta_i=W_i^+\geq W_i\geq W_i^-\geq W_i^{--}$ 表示理性用户 P_i 参与理性秘密重构博弈 G_S 时的自利性偏好，即：理性用户 P_i 首先希望只有自己能重构出共享秘密；其次，在自己获得共享秘密的同时，尽可能地让其余用户不能重构出共享秘密.

3.3 存取结构

为更一般化地分析参与理性秘密重构的理性用户集合中的哪些子集可重构出共享秘密，下面给出存取结构的相关概念.

定义 2(存取结构). 设 $P=\{P_1,P_2,\cdots,P_n\}$ 是 n 个用户组成的用户集合. 对于任意给定的非空集合 $AS\subseteq 2^P$，如果其满足单调性，即：

当 $\exists A\in AS$ 时，$\forall A'\in 2^P$ 且 $A\subseteq A'$，有 $A'\in AS$ 则称集合 AS 为 P 上的存取结构. 其中，2^P 表示集合 P 的全部子集构成的集合.

定义 3(最小存取结构). 令集合 AS 为用户集合 P 上的存取结构，则称集合

$$AS_m=\{A\in AS\mid \forall A'\in 2^P, A'\subset A\Rightarrow A'\notin AS\}$$

为存取结构 AS 上的最小存取结构.

基于上述定义，可给出任意用户 $P_i\in P$ 关于用户集合 P 的最小存取结构，简称用户 P_i 的最小存取结构.

定义 4(用户 P_i 的最小存取结构). 令集合 AS_m 是用户集合 P 上的最小存取结构，如果集合 $AS_m^{P_i}\subseteq AS_m$ 满足：$\forall A\in AS_m^{P_i}$，有 $P_i\in A$，则称该集合 $AS_m^{P_i}$ 是用户 P_i 的最小存取结构.

在 (t,n) 理性秘密共享中，它的存取结构是由参与秘密重构的用户数量不少于 t 的用户集合所构成的，即 $AS=\{P'\subseteq P\mid\mid |P'|\geq t\}$；最小存取结构 $AS_m=\{P''\in P\mid\mid |P''|=t\}$ 是由 t 个参与秘密重构的用户所组成的集合构成的；而参与者 P_i 的最小存取结构为 $AS_m^{P_i}=\{P'''\in AS\mid P'''\in AS_m \text{且} P_i\in P'''\}$.

3.4 机制设计

机制设计[40]是微观经济学中的重要组成，其主要研究的是如何设计合理的机制，使得参与社会经济活动的用户在追求个人收益最大化的同时，实现机制设计者的期望目标. 其形式化定义如下所示.

定义 5(机制). 机制 $M=\{o,p\}$ 是一个二元组，具体解释如下：

(1) o 是机制 M 的分配规则. 即机制根据参与社会经济活动的每个用户 P_i 所选择的策略 a_i，计算得到相应的输出结果 $o(\boldsymbol{a})$. 其中，$1\leq i\leq n$；n 表示参与社会经济活动的用户数量；$\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$.

(2) $p=\{p_1,p_2,\cdots,p_n\}$ 是机制 M 的支付规则. 即机制 M 根据用户 P_i 选择的策略 a_i，提供给用户 P_i 的一个转移支付 p_i.

4 理性公平性

4.1 现有理性秘密共享公平性的缺陷

在现有理性秘密共享的研究中，其公平性可表述为：当理性秘密重构博弈结束时，所有的理性用户均获得共享秘密，或没有任何理性用户能获得共享秘密. 为便于论述现有理性秘密共享公平性定义的缺陷，本文先给出现有理性秘密共享公平性的定义，详细内容可参考文献[19].

定义 6(现有理性秘密共享的公平性). 假设执行某理性秘密共享方案在 n 个理性用户 $P_1,P_2,\cdots,P_n$ 间共享秘密. 如果对任意的理性用户 P_i 来说，当理性秘密重构结束时，其获得的收益 u_i 满足：

$$u_i(a_i,\boldsymbol{a}_{P_{-i}})=W_i \text{或} u_i(a_i,\boldsymbol{a}_{P_{-i}})=W_i^-.$$

那么就称该理性秘密共享方案是公平的. 其中，$a_i\in A_i$ 表示理性用户 P_i 在执行理性秘密重构时选择的策略；$\boldsymbol{a}_{P_{-i}}=(a_1,\cdots,a_{i-1},a_{i+1},\cdots,a_n)$ 是由理性用户 P_i 的对手 $P_j\in P_{-i}$ 参与理性秘密重构时选择的策略 $a_j\in A_j$ 所构成的策略组合；$i\neq j$ 且 $1\leq i,j\leq n$.

下面利用反证法证明上述公平性定义存在缺陷.

命题 1. 当理性用户均是自利时，现有理性秘密共享的公平性定义允许“理性用户不发送自己的子秘密也能获得共享秘密”或“发送错误的子秘密欺骗其余理性用户，将重构出错误的共享秘密当作真实共享秘密”.

证明. 令 $P=\{P_1,P_2,\cdots,P_n\}$ 表示参与理性秘密重构的用户集合；$P'=\{P_{j_1},P_{j_2},\cdots,P_{j_k}\}$ 表示参与理性秘密重构博弈 G_S 中正确地发送子秘密的用户集合，即理性用户 $P_{j_l}\in P'$ 参与理性秘密重构博弈 G_S 时选择策略 $a_{j_l}^{\text{honest}}$；$\overline{P}'=\{P_{m_1},P_{m_2},\cdots,P_{m_{n-k-1}}\}$ 表示在参与理性秘密重构博弈 G_S 时未正确地发送子秘密的理性用户集合，即理性用户 $P_{j_l}\in\overline{P}'$ 参与理性秘密重构博弈 G_S 时选择策略 $a_{m_q}^{\text{other}}\neq a_{m_q}^{\text{honest}}\in A_{m_q}$. 其中，$1\leq l\leq k$；$1\leq k\leq n-1$；$1\leq q\leq n-k-1$；$P'\cup\overline{P}'\cup\{P_i\}=P$.

(1) 当 $t\leq k\leq n-1$，即至少已有 t 个理性用户将自己拥有的子秘密正确地发送给其余理性用户时：

若理性用户 P_i 选择策略 a_i^{fake}，即未将自己拥有的子秘密正确地发送给其余用户，那么理性用户

P_i、P_{j_l}和P_{m_q}的收益u_i、u_{j_l}和u_{m_q}分别为

$$u_i(a_i^{\text{fake}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_i;$$

$$u_{j_l}(a_i^{\text{fake}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_{j_l};$$

$$u_{m_q}(a_i^{\text{fake}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_{m_q}.$$

故策略组合$(a_i^{\text{fake}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})$满足现有理性秘密共享的公平性.

同理，若理性用户P_i选择策略a_i^{silent}，即不发送任何子秘密给其余理性用户，那么理性用户P_i、P_{j_l}和P_{m_q}的收益u_i、u_{j_l}和u_{m_q}分别为

$$u_i(a_i^{\text{silent}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_i;$$

$$u_{j_l}(a_i^{\text{silent}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_{j_l};$$

$$u_{m_q}(a_i^{\text{silent}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_{m_q}.$$

故策略组合$(a_i^{\text{silent}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})$也满足现有理性秘密共享的公平性.

显然，当有$k\geq t$个理性用户$P_{j_1},P_{j_2},\cdots,P_{j_k}$已将自己的拥有的子秘密正确地发送给其余理性用户时，对于理性用户P_i来说，有

$$u_i(a_i^{\text{fake}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})\geq u_i(a_i^{\text{honest}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})$$

和 $u_i(a_i^{\text{silent}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})\geq u_i(a_i^{\text{honest}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})$.

其中，当发送错误的子秘密能欺骗其余理性用户将重构出错误的秘密视为真实的共享秘密或考虑发送子秘密需要消耗理性用户的通信成本时，上式不等号成立.

因此，理性用户P_i在参与理性秘密重构博弈G_S时，不会选择策略a_i^{honest}.

(2) 当$t=n$时，即理性用户必须要拥有n个子秘密才能重构出共享秘密. 此时，对于理性用户P_i来说，若$k<n-1$，即少于$n-1$个理性用户将自己的拥有子秘密正确地发送给其余理性用户，则理性用户P_i、P_{j_l}和P_{m_q}的收益u_i、u_{j_l}和u_{m_q}分别满足：

$$u_i(a_i,a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_i^-;$$

$$u_{j_l}(a_i,a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_{j_l}^-;$$

$$u_{m_q}(a_i,a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})=W_{m_q}^-.$$

故策略组合$(a_i,a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{honest}},a_{m_1}^{\text{other}},\cdots,a_{m_{n-k-1}}^{\text{other}})$满足现有理性秘密共享的公平性. 其中，$a_i\in A_i$.

若$k=n-1$，即已有$n-1$个理性用户将自己的拥有子秘密正确地发送给其余理性用户，则理性用户P_i和P_{j_l}的收益u_i和u_{j_l}分别满足：

$$\begin{cases}u_i(a_i^{\text{honest}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}})=W_i\\ u_{j_l}(a_i^{\text{honest}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}})=W_{j_l}\end{cases};$$

$$\begin{cases}u_i(a_i^{\text{fake}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}})=W_i^+\\ u_{j_l}(a_i^{\text{fake}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}})=W_{j_l}^-\end{cases};$$

$$\begin{cases}u_i(a_i^{\text{silent}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}})=W_i^+\\ u_{j_l}(a_i^{\text{silent}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}})=W_{j_l}^-\end{cases}.$$

此时，只有策略组合$(a_i^{\text{honest}},a_{j_1}^{\text{honest}},\cdots,a_{j_k}^{\text{hontest}})$满足现有理性秘密共享的公平性.

综上所述，现有理性秘密共享的公平性定义允许“理性用户不发送自己的子秘密也能获得共享秘密”或“发送错误的子秘密欺骗其余理性用户，将重构出错误的共享秘密当作真实共享秘密”.　　证毕.

4.2　理性公平性

通过上述分析发现，当$t=n$时，由于理性秘密共享具有特殊的最小存取结构$AS_m=\{P\}$，即所有的理性用户均要将自己的拥有的子秘密正确地发送给其余用户时，可实现公平的理性秘密共享. 因此，本文通过引入用户的最小存取结构，给出秘密共享的理性公平性定义，其形式化描述如下所示.

定义 7(理性公平性).　一个(t,n)理性秘密共享方案被称为是理性公平的，当且仅当对于任意理性用户$P_i(1\leq i\leq n)$来说，当理性秘密重构结束时，$\forall P'=\{P_{e_1},P_{e_2},\cdots,P_{e_{t-1}},P_i\}\in AS_m^{P_i}$，其选择策略$a_i$的收益$u_i$满足：

(1) $u_i(a_i,\boldsymbol{a}_{P'_{-i}})\geq u_i(a_i',\boldsymbol{a}_{P'_{-i}})$；

(2) $u_i(a_i,\boldsymbol{a}_{P'_{-i}})=W_i$或$u_i(a_i,\boldsymbol{a}_{P'_{-i}})=W_i^-$.

其中，$a_i,a_i'\in A_i$是理性用户P_i参加理性秘密重构时所选择的策略且$a_i\neq a_i'$；$P'=\{P_{e_1},P_{e_2},\cdots,P_{e_{t-1}},P_i\}$是理性用户$P_i$的关于理性秘密共享的最小存取结构；$P_{-i}=\{P_{e_1},P_{e_2},\cdots,P_{e_{t-1}}\}$；$\boldsymbol{a}_{P'_{-i}}=(a_{e_1},a_{e_2},\cdots,a_{e_{t-1}})$表示用户集合$P'$中其余理性用户$P_{e_j}$参加博弈$G_S$选择的策略$a_{e_j}$组成的策略组合；$1\leq j\leq t-1$且$e_j\neq i$.

在上述理性公平性的形式化定义中，条件(1)是为了说明当理性用户P_i在秘密重构阶段中可选择策略a_i和a_i'时，会根据自利性原则，选择策略a_i来追求自身收益最大化；条件(2)是为了确保理性秘密重构的公平性，对执行过程进行约束，即当任意t个理性用户进行理性秘密重构时，他们均能重构出真实的共享秘密或均未重构出真实的共享秘密.

下面证明本文给出的理性公平性定义不允许出现任何不公平的情形.

命题 2.　当理性用户均是自利时，本文提出的理性公平性定义仅允许“理性用户将自己拥有的子秘密正确地发送给其余用户”.

证明.　与命题 1 证明相似，令集合$P'=\{P_{e_1},$

$P_{e_2},\cdots,P_{e_{t-1}},P_i\}$是任意一个包含理性用户 P_i的用户集合,且$|\hat{P}|=t$. 假设理性用户在秘密重构阶段未正确地将自己拥有的子秘密发送给其余理性用户,即选择策略 $a_i'\neq a_i^{\text{honest}}$.

此时,若其余 $t-1$ 个用户 $P_{e_1},P_{e_2},\cdots,P_{e_{t-1}}$ 将自己拥有的子秘密正确地发送给其余用户时,理性用户选择策略 a_i'的收益为

$$u_i(a_i',\boldsymbol{a}_{\hat{P}_{-i}}^{\text{honest}})=W_i^{+}.$$

而对于理性用户 P_{e_j}来说,其收益为

$$u_{e_j}(a_{e_1}^{\text{honest}},\cdots,a_{e_{j-1}}^{\text{honest}},a_{e_j}^{\text{honest}},a_{e_{j+1}}^{\text{honest}},\cdots,a_{e_{t-1}}^{\text{honest}},a_i')=W_{e_j}^{--}.$$

其中,$1\leq j\leq t-1$.

显然,$u_i(a_i',\boldsymbol{a}_{\hat{P}_{-i}}^{\text{honest}})\neq u_{e_j}(a_i',\boldsymbol{a}_{\hat{P}_{-i}}^{\text{honest}})$. 故当理性用户选择策略 $a_i'\neq a_i^{\text{honest}}$时,并不满足理性公平性.

因此,当理性用户均是自利的时,本文提出的理性公平性定义中仅允许"理性用户将自己拥有的子秘密正确地发送给其余用户". 证毕.

5 理性公平的秘密共享方案

为进一步表明本文所提的理性公平性定义具有实用性,本节基于混淆思想,设计一个理性公平的秘密共享方案.

5.1 混淆激励机制

本文基于机制设计模型,设计一个混淆激励机制来约束理性用户在理性秘密重构阶段的自利性行为. 基本思想如下:通过让秘密分发者 Dealer 为每个理性用户分发包含多个虚假子秘密的子秘密集合,使得理性用户在秘密重构阶段的交互完成前难以确认重构出的哪个秘密是真实的共享秘密;一旦理性用户在秘密重构阶段中未将自己拥有的子秘密正确地发送给其余用户或不发送任何子秘密,则该用户在随后的子秘密交互过程中将受到惩罚,不会收到其余理性用户发送的任何子秘密.

令策略 $a_i^{(k)}$表示理性用户 P_i发送其拥有的第 k $(1\leq k\leq N)$个子秘密所选择的策略,其中 N 是正整数. 本文设计的混淆激励机制如下所示.

定义 8(混淆激励机制). 针对基于异步通信的理性秘密共享,混淆激励机制 $M_{obf}=\{\boldsymbol{o}^{(k)},p_i^{(k)}\}$是个二元组,其中:

(1) $\boldsymbol{o}^{(k)}=(a_1^{(k)},a_2^{(k)},\cdots,a_n^{(k)})$是在理性秘密重构阶段的第 k 轮交互中,每个理性用户 P_i在混淆激励机制 M_{obf}下选择策略 $a_i^{(k)}$所构成的策略组合.

(2) $p_i^{(k)}$是理性用户 P_i在混淆激励机制下选择策略 $a_i^{(k)}$后所获得的转移支付,其满足:

$$p_i^{(k)}(a_i^{(k)})=\begin{cases}a_{j\to i}^{(k)\text{-honest}}, & a_i^{(k)}=a_i^{(k)\text{-honest}}\\ a_{j\to i}^{(k)\text{-silent}}, & a_i^{(k)}\in\{a_i^{(k)\text{-fake}},a_i^{(k)\text{-silent}}\}\end{cases},$$

其中,$j\neq i$ 且理性用户 P_j在秘密重构阶段的第 k 轮交互中比理性用户 P_i后进行策略的选择;$a_i^{(k)\text{-honest}}$表示理性用户 P_i在第 k 轮交互中将自己拥有的子秘密正确地发送给其余用户;$a_i^{(k)\text{-fake}}$表示理性用户 P_i在第 k 轮交互中未将自己拥有的子秘密正确地发送给其余用户;$a_i^{(k)\text{-silent}}$表示理性用户 P_i在第 k 轮交互中不发送任何子秘密给其余用户;$a_{j\to i}^{(k)\text{-honest}}$表示理性用户 P_j在第 k 轮交互中将自己拥有的子秘密正确地发送给用户 P_i;$a_{j\to i}^{(k)\text{-silent}}$表示理性用户 P_j在第 k 轮交互中不发送任何子秘密给用户 P_i.

当理性用户在秘密重构阶段中同步发送自己拥有的子秘密时(即所有用户同时选择自己的策略),我们只需将上述混淆激励机制中的 $p_i^{(k)}$修改为

$$p_i^{(k)}(a_i^{(k)})=\begin{cases}a_{j\to i}^{(k+1)\text{-honest}}, & a_i^{(k)}=a_i^{(k)\text{-honest}}\\ a_{j\to i}^{(k+1)\text{-silent}}, & a_i^{(k)}\in\{a_i^{(k)\text{-fake}},a_i^{(k)\text{-silent}}\}\end{cases},$$

也就是说,混淆机制将根据理性用户 P_i在第 k 轮交互中选择的策略 $a_i^{(k)}$,在第 $k+1$ 轮交互中给予转移支付.

5.2 我们的方案

下面基于上述混淆激励机制,构造一个理性公平的秘密共享方案. 该方案由理性秘密分发协议和理性秘密重构协议组成.

5.2.1 理性秘密分发协议

为防止理性用户在秘密重构阶段中猜测出真实的共享秘密 K^{real},在秘密分发阶段,秘密分发者 Dealer 首先生成虚假秘密 $K^{1\text{-fake}},K^{2\text{-fake}},\cdots,K^{N'\text{-fake}}$,并利用这 N'个虚假秘密和真实的共享秘密 K^{real}为每个理性用户 P_i生成子秘密集合 k_set_i. 确保理性用户在秘密重构阶段中至少能重构出一个虚假秘密 $K^{\text{fake}}\in\{K^{1\text{-fake}},K^{2\text{-fake}},\cdots,K^{N'\text{-fake}}\}$,使得重构出该虚假秘密 K^{fake}的次数仅比重构出的真实秘密 K^{real}的次数少 1 次. 其中,具体协议如下所示.

Step 1. 秘密分发者 Dealer 根据真实共享秘密 K^{real}生成 N'个虚假秘密 $K^{1\text{-fake}},K^{2\text{-fake}},\cdots,K^{N'\text{-fake}}$,并利用 $K^{1\text{-fake}},K^{2\text{-fake}},\cdots,K^{N'\text{-fake}},K^{\text{real}}$生成分发秘密集合 $K=\{K_1,K_2,\cdots,K_N\}$. 其中,$N'\geq 2$ 且是正整数;$K_1,K_2,\cdots,K_N$是重复使用 $N'+1$个共享秘密 $K^{1\text{-fake}},K^{2\text{-fake}},\cdots,K^{N'\text{-fake}},K^{\text{real}}$而构成的一个共享秘密排列,其满足:

(1) $\exists K_1^{i'\text{-fake}},K_2^{i'\text{-fake}},\cdots,K_{N^{n'}}^{i'\text{-fake}}\in K$,有

$$|K_1^{i'\text{-fake}}|=|K_2^{i'\text{-fake}}|=\cdots=|K_{N^{n'}}^{i'\text{-fake}}|=|K^{\text{real}}|-1;$$

(2) $\forall K_{N-k},K_{N-k+1},\cdots,K_N\in K$,有

$$|K_{N-k}|=|K_{N-k+1}|=\cdots=|K_N|<|K^{\text{real}}|-1;$$

(3) N'和 k 是两个随机正整数且 $1\leq k\leq N$.

Step 2. 秘密分发者 Dealer 构造 N 个 $t-1$ 阶多项式 $f_1(x),f_2(x),\cdots,f_N(x)$,使得

$$\begin{cases} f_m(x)\neq f_{m'}(x), & m\neq m', \\ f_i(x)=K_m+\sum_{r=1}^{t-1}a_r x^r, & 1\leq m\leq N \end{cases}$$

并利用这些多项式将分发秘密 $K_m\in K$ 拆分成 n 份子秘密 $k_1^m,k_2^m,\cdots,k_n^m$. 其中,$k_i^m=f_m(i)$;$1\leq i\leq n$.

Step 3. 秘密分发者 Dealer 选择安全的签名函数 $sign(\cdot)$,并利用自己的私钥 Dealer_{SK} 为子秘密 k_i^m 计算承诺信息 $c_i^m=sign_{\text{Dealer}_{SK}}(k_i^m\|ID_i\|m)$. 其中,$ID_i$ 是理性用户 P_i 的身份;"‖"是连接符.

Step 4. 秘密分发者 Dealer 为理性用户生成子秘密集合 $k\_set_i=\{k_i^1,k_i^2,\cdots,k_i^N\}$ 和承诺信息集合 $c\_set_i=\{c_i^1,c_i^2,\cdots,c_i^N\}$. 然后将子秘密集合 k_set_i 发送给理性用户 P_i;将承诺信息集合 c_set_i 和签名验证函数 $verf(\cdot)$ 发送给所有的理性用户.

5.2.2　理性秘密重构协议

当要重构共享秘密时,所有的理性用户根据收到的子秘密集合进行交互,即在第 m 轮交互中,每个理性用户 P_i 发送其子秘密集合 k_set_i 中的第 m 个子秘密 k_i^m. 其余理性用户收到 P_i 发送的子秘密后,利用验证函数 $verf(\cdot)$ 和秘密分发者的公钥 Dealer_{PK} 验证子秘密的正确性. 若发现理性用户 P_i 未正确地发送子秘密 k_i^m,则在之后的第 $m+1$ 轮至第 n 轮交互中,其余理性用户均不再发送任何子秘密给理性用户 P_i. 若确认理性用户 P_i 正确地发送子秘密 k_i^m,则继续进行交互,直至将所有的子秘密都交互完毕后,从重构出的诸多秘密中挑选重复数量最多的作为真实的共享秘密. 具体协议如下所示.

Step 1. 在任意第 m 轮子秘密交互中,当轮到理性用户 P_i 发送子秘密时,

(1) 对于已行动过的理性用户 $P_{i'}$,

① 若收到理性用户 $P_{i'}$ 发送的子秘密 $k_{i'}^m$,且确认该子秘密的正确性,则将 $k_{i'}^m$ 发送给理性用户 $P_{i'}$.

② 若收到理性用户 $P_{i'}$ 发送的子秘密 $k_{i'}^m$,但确认该子秘密不是秘密分发者 Dealer 指定发送的子秘密,则不发送任何子秘密给理性用户 $P_{i'}$.

③ 若未收到理性用户 $P_{i'}$ 发送的子秘密 $k_{i'}^m$,则不发送任何子秘密给理性用户 $P_{i'}$.

(2) 对于还未行动过的理性用户 P_j,则发送自己拥有的子秘密 k_i^m.

Step 2. 理性用户 $P_j\in P_{-i}$ 收到子秘密 k_i^m 后,利用秘密分发者 Dealer 的公钥 Dealer_{PK}、验证函数 $verf(\cdot)$ 以及承诺信息 c_i^m 验证该子秘密的正确性,即 P_i 发送的子秘密 k_i^m 是否就是秘密分发者 Dealer 指定的在第 m 轮中发送的子秘密:

(1) 若 $verf_{\text{Dealer}_{PK}}(c_i^m,ID_i,m)=k_i^m$,则表示理性用户 P_i 在第 m 轮交互中,正确地发送了自己拥有的子秘密,则广播消息"Honest";

(2) 若 $verf_{\text{Dealer}_{PK}}(c_i^m,ID_i,m)\neq k_i^m$,则表示理性用户 P_i 在第 m 轮交互中,未正确地发送自己拥有的子秘密,则广播消息"Fake".

若理性用户 P_j 未收到任何子秘密,则广播消息"silent".

Step 3. 理性用户发送完自己拥有的子秘密 k_i^m 后,则轮到下一位未行动的理性用户 P_{i+1} 发送自己拥有的子秘密.

Step 4. 当在第 m 轮交互中收到子其余理性用户发送的子秘密 $k_{i_1}^m,k_{i_2}^m,\cdots,k_{i_{n'}}^m$ 后:

(1) 若 $t-1\leq n'\leq n-1$,即至少有 $t-1$ 个其余理性用户正确地发送自己拥有的子秘密,则利用朗格朗日插值法恢复共享秘密 K_m.

(2) 若 $n'<t-1$,即仅有不多于 $t-2$ 个其余理性用户正确地发送自己拥有的子秘密,此时无法恢复出共享秘密 K_m,交互终止.

Step 5. 若在交互过程中所有理性用户均已能正确地识别出真实的共享秘密,则协议终止. 否则,重构出所有的秘密 $K_1,K_2,\cdots,K_N$ 后,若 $\forall K',K''\in\{K_1,K_2,\cdots,K_N\}$,有 $|K'|>|K''|$,则将 K' 视为真实的共享秘密 K^{real}.

值得注意的是,通过修改理性用户发送子秘密的先后顺序,本方案也可适用于同步通信情形.

6　方案分析

本方案采用 $t-1$ 阶多项式对分发的秘密 K_m $(1\leq i\leq N)$ 进行拆分. 此时,根据方程组解的性质,当且仅当理性用户 P_i 拥有 t 个子秘密,才能重构出 K_m,否则不能得到关于秘密 K_m 的任何信息.

此外,当理性用户 P_i 分发子秘密 k_i^m 时,如果其不交互秘密分发者指定交互的子秘密 k_i^m(无论是自己伪造的子秘密,或者分发应在其余轮交互的子秘密 $k_i^{m'}$,或者分发其余理性用户发送的子秘密 k_j^m),由于存在承诺信息 $c_i^m=sign_{\text{Dealer}_{SK}}(k_i^m\|ID_i\|m)$,其余理性用户均可正确地识别出 P_i 的欺骗行为. 而当收到不少于 $t-1$ 个其余理性用户发送的关于 K_m 的子秘密后,就可利用拉格朗日插值法重构出秘密 K_m. 因此,本方案是安全的和正确的. 下面,详细给

出本方案的公平性证明.

6.1 公平性

定理 1. 当理性用户的自利性偏好满足:$W_i^+ \geq W_i \geq W_i^- \geq W_i^{--}$时,若 N 足够大,那么本方案是理性公平的.

证明. 不妨设任意 t 个用户 $P_{i_1}, P_{i_2}, \cdots, P_{i_t}$ 参与理性秘密重构.其中,理性用户 P_{i_g} 在秘密分发阶段获得的子秘密集合为 $k\_set_{i_g}\{k_{i_g}^1, k_{i_g}^2, \cdots, k_{i_g}^N\}$, $1 \leq g \leq t$.下面证明在任意第 m 轮中,理性用户 P_{i_g} 均会选择策略 $a_{i_g}^{(m)\text{-honest}}$,即将子秘密 $k_{i_g}^m$ 发送给其余理性用户.

由于在秘密分发者构造的分发秘密集合 K 中,生成的虚假秘密 $K^{i'_1\text{-fake}}, K^{i'_2\text{-fake}}, \cdots, K^{i'_{N''}\text{-fake}}$ 和真实的秘密 K^{real} 间满足:

$|K^{i'_1\text{-fake}}| = |K^{i'_2\text{-fake}}| = \cdots = |K^{i'_{N''}\text{-fake}}| = |K^{\text{real}}| - 1$,

即虚假秘密 $K^{i'_1\text{-fake}}, K^{i'_2\text{-fake}}, \cdots, K^{i'_{N''}\text{-fake}}$ 和真实秘密 K^{real} 的数量只相差 1 个.此外,在分发秘密集合 K 中,$K_{N-k}, K_{N-k+1}, \cdots, K_N \neq K^{\text{real}}$.其中,$k$ 是一个随机数.

因此,不失一般性地,在任意第 $m(m \neq N)$ 轮交互中,每个理性用户 P_{i_g} 都不能正确地识别出真实的共享秘密 K^{real},即

$$\Pr_{i_g}[K_{m'} = K_{\text{real}} \mid K_{m'} \in \{K_1, K_2, \cdots, K_m\}] = \varepsilon,$$

其中,ε 是可忽略的.而一旦理性用户 P_i 在第 m 轮中不发送子秘密 k_i^m 给其余理性用户,在之后的交互中将不会有任何理性用户给其发送子秘密.

那么,对理性用户 P_{i_g} 来说,在第 m 轮中,分别选择策略 $a_{i_g}^{(m)\text{-honest}}$、$a_{i_g}^{(m)\text{-fake}}$ 和 $a_{i_g}^{(m)\text{-silent}}$ 的收益满足:$u_{i_g}(a_{i_g}^{(m)\text{-honest}}) \geq W_{i_g} \geq u_{i_g}(a_{i_g}^{(m)\text{-fake}}) = u_{i_g}(a_{i_g}^{(m)\text{-silent}})$.因此,在第 m 轮中,理性用户 P_{i_g} 只会选择策略 $a_{i_g}^{(m)\text{-honest}}$.在进行第 N 轮交互时,由于

$$\begin{cases} |K^{i'_1\text{-fake}}| = |K^{i'_2\text{-fake}}| = \cdots = |K^{i'_{N''}\text{-fake}}| = |K^{\text{real}}| - 1 \\ K_{N-k}, K_{N-k+1}, \cdots, K_N \neq K^{\text{real}} \end{cases},$$

则在之前重构出的秘密 $K_1, K_2, \cdots, K_{N-1}$ 中,一定存在一个 $K_{m''}$ 使得其重复的数量最多,即

$\exists K_{m''} \in \{K_1, K_2, \cdots, K_{N-1}\}$,有 $|K_{m''}| = \max\limits_{1 \leq \tilde{m} \leq N-1} |K_{\tilde{m}}|$.

此时,理性用户 P_{i_g} 已识别出真实的共享秘密 K^{real}.因此,理性用户 P_{i_g} 分别选择策略 $a_{i_g}^{(N)\text{-honest}}$、$a_{i_g}^{(N)\text{-fake}}$ 和 $a_{i_g}^{(N)\text{-silent}}$ 的收益满足:

$u_{i_g}(a_{i_g}^{(N)\text{-honest}}) = u_{i_g}(a_{i_g}^{(N)\text{-fake}}) = u_{i_g}(a_{i_g}^{(N)\text{-silent}}) = W_{i_g}$.

所以,在第 N 轮交互中,理性用户没有动机偏离预定的理性秘密重构协议,故会选择策略 $a_{i_g}^{(N)\text{-honest}}$.

综上所述,当理性用户的自利性偏好满足:$W_i^+ \geq W_i \geq W_i^- \geq W_i^{--}$时,若 N 足够大,那么本方案是理性公平的. 证毕.

6.2 时间复杂性

本文将承诺信息的验证视为计算承诺信息的一个逆计算,故它们具有相同的时间复杂性,用 $O^{\text{Time}}(sign)$ 表示.

在分发阶段中,秘密分发者 Dealer 首先需要生成分发秘密集合 $K = \{K_1, K_2, \cdots, K_N\}$,并利用 $t-1$ 阶多项式将秘密 K_m 拆分成 $k_1^m, k_2^m, \cdots, k_n^m$.因此,每拆分一个秘密 K_m 需要 $O^{\text{Time}}(n)$ 次计算.那么,拆分秘密分发秘密集合 K 中的 N 个秘密所需的计算复杂性为 $O^{\text{Time}}(n \cdot N)$.随后,为防止理性用户在秘密重构阶段中进行欺骗,秘密分发者 Dealer 还需要为每个子秘密 $k_i^m (1 \leq i \leq n, 1 \leq m \leq N)$ 计算承诺信息 $c_i^m = sign_{\text{Dealer}_{SK}}(k_i^m \parallel ID_i \parallel m)$.因此计算承诺信息所需的计算复杂性为 $O^{\text{Time}}(n \cdot N \cdot sign)$.

在重构阶段中,当理性用户 P_i 收到其余理性用户 $P_j \in P_{-i}$ 发送的子秘密 k_j^m 后,需利用验证函数 $verf(\cdot)$ 和秘密分发者的公钥 Dealer_{PK} 验证子秘密的正确性,即计算 $verfy_{\text{Dealer}_{PK}}(c_j^m, ID_j, m) = k_j^m$,故每验证一个子秘密就需 $O^{\text{Time}}(sign)$ 计算复杂性.而每个理性用户 P_j 需发送 N 个子秘密 $k_j^1, k_j^2, \cdots, k_j^N$.因此,为验证其余理性用户发送的子秘密的正确性,理性用户 P_i 共需 $O^{\text{Time}}((n-1) \cdot N \cdot sign) = O^{\text{Time}}(n \cdot N \cdot sign)$ 次计算.当在任意第 m 轮交互完成后,理性用户 P_i 需利用收到的子秘密 $k_1^m, k_2^m, \cdots, k_n^m$ 重构出分发秘密 K_m,至多需要 $O^{\text{Time}}(n)$ 次计算.因此,重构出所有分发秘密 $K_1, K_2, \cdots, K_N$ 所需的计算复杂性为 $O^{\text{Time}}(n \cdot N)$.此外,从重构出的分发秘密 $K_1, K_2, \cdots, K_N$ 中统计每个秘密重复出现的次数,并通过查找出现次数最多的秘密得到真实的共享秘密 K^{real},故从重构出的分发秘密 $K_1, K_2, \cdots, K_N$ 中识别出共享秘密 K^{real} 所需的计算复杂性为 $O^{\text{Time}}(N)$.

综上所述,当使用本方案在 n 个理性用户间共享秘密时,

(1) 对于秘密分发者来说,其所需的计算复杂性为

$$\begin{aligned} O_{\text{Dealer}}^{\text{Time}} &= O^{\text{Time}}(n \cdot N) + O^{\text{Time}}(n \cdot N \cdot sign) \\ &= O^{\text{Time}}(n \cdot N \cdot sign). \end{aligned}$$

(2) 对于理性用户来说,其所需的计算复杂性为

$$\begin{aligned} O_{\text{User}}^{\text{Time}} &= O^{\text{Time}}(n \cdot N \cdot sign) + O^{\text{Time}}(n \cdot N) + O^{\text{Time}}(N) \\ &= O^{\text{Time}}(n \cdot N \cdot sign). \end{aligned}$$

6.3 通信复杂性

令 $|k_i^m|$ 和 $|c_i^m|$ 分别表示发送的子秘密 k_i^m 和承诺信息 c_i^m 的长度,其中 $1 \leq i \leq n$ 且 $1 \leq m \leq N$.不妨设,$\forall i \neq j$ 和 $m \neq m'$,下式

$$\begin{cases}|k_i^m|=|k_j^m|=|k_i^{m'}|=|k| \\ |c_i^m|=|c_j^m|=|c_i^{m'}|=|sign|\end{cases}$$

成立，即秘密分发者 Dealer 为每个用户分发在子秘密的长度以及承诺信息长度均相等. 下面简要分析本方案的通信复杂性.

在分发阶段中，秘密分发者 Dealer 在将子秘密集合 $k\_set_i=\{k_i^1,k_i^2,\cdots,k_i^N\}$ 分发给每个理性用户 P_i 后，还需将承诺信息集合 $c\_set_i=\{c_i^1,c_i^2,\cdots,c_i^N\}$ 和签名验证函数 $verf(\cdot)$ 发送给所有的理性用户. 因此，秘密分发者 Dealer 的通信复杂性为

$$\begin{aligned}O_{\text{Dealer}}^{\text{Comm}}&=O^{\text{Comm}}(n\cdot N\cdot|k|)+O^{\text{Comm}}(n\cdot N\cdot|sign|)+\\&\quad O^{\text{Comm}}(|verfy|)\\&=O^{\text{Comm}}(n\cdot N\cdot|\max|)+O^{\text{Comm}}(|verfy|),\end{aligned}$$

其中，$|\max|=\max\{|k|,|sign|\}$；$O^{\text{Comm}}(n\cdot N\cdot|k|)$ 表示分发子秘密时的通信复杂性；$O^{\text{Comm}}(n\cdot N\cdot|sign|)$ 表示发送承诺信息所需要的通信复杂性；$O^{\text{Comm}}(|verfy|)$ 表示发送验证函数 $verfy(\cdot)$ 所需的复杂性；$|verfy|$ 表示发送的验证函数 $verfy(\cdot)$ 长度.

在重构阶段中，每个理性用户 P_i 仅需将自己拥有的子秘密 $k_i^1,k_i^2,\cdots,k_i^m$ 发送给其余理性用户，因此理性用户 P_i 的通信复杂性为

$$O_{\text{User}}^{\text{Comm}}=O^{\text{Comm}}(N\cdot|k|).$$

6.4　方案对比

下面通过与现有适用于异步通信的理性秘密共享方案进行对比，进一步说明本方案在实现理性公平性的同时还具有较好的可用性. 具体对比如表 1 所示.

表 1　方案对比

	理性公平性	可信用户	重构阶段中的交互轮数	重构交互轮数依赖关于理性用户收益的计算	使用其它密码技术	实用情形
方案[23]	×	×	N	√	安全多方计算、健忘传输、零知识证明	$t,n\geq 2$
方案[25]	×	×	N	√	可验证随机函数	$t,n\geq 2$
方案[26]	×	×	N	√	—	$t,n\geq 2$
方案[32]	×	×	2	√	—	$t,n\geq 2$
方案[35]	×	×	3	√	—	$t=n\geq 3$
本方案	×	×	N	√	—	$t,n\geq 2$

方案[23]是首个适用于异步通信的理性秘密共享方案，但是该方案由于使用安全多方计算协议、健忘传输协议和零知识证明来约束理性用户在秘密重构阶段的自利性行为，导致其计算复杂性较高. 为降低理性用户的计算代价，方案[25]通过构造可验证随机函数(Verifiable Random Function，VRF)使得理性用户直至交互完成才能确定其他理性用户发送的子秘密的正确性，从而确保每个理性用户均不会偏离预定方案的执行. 随后，方案[26]为了避免使用可验证随机函数，进一步降低秘密分发者 Dealer 的计算代价，通过让秘密分发者 Dealer 将为每个理性用户分发的子秘密再次进行拆分，使得理性用户只有在交互结束后才能获知如何正确地重构出子秘密，从而确保每个用户均能重构出共享秘密. 然而，当使用上述三个方案时，在秘密分发阶段中，Dealer 需要根据每个理性用户的收益函数来确定他们在秘密重构阶段中的交互轮数，即交互轮数 N 满足：$N=\max\{N_1,N_2,\cdots,N_n\}$. 其中，$1\leq i\leq n$ 且 $N_i=\dfrac{W_i^+-W_i^-}{W_i-W_i^-}$. 但是，在现实应用中，准确地掌握每个理性用户 P_i 的收益(即 W_i^+、W_i 和 W_i^-)是较为困难的. 一旦不能准确地设定交互轮数 N，那么在秘密重构阶段中就可能会出现“正确发送子秘密的理性用户未能重构出真实的共享秘密，而未正确发送子秘密的用户却能重构出真实共享秘密”的不公平情形.

为降低理性用户在秘密重构阶段中的交互轮数，方案[32]通过将参与秘密重构的理性用户划分成不同群组的方式来进行交互，提出了一个仅需两轮交互的理性秘密共享方案. 但是，在实际应用中，完全可信的用户较难找到. 此外，在使用该方案时，还可能会出现“正确发送子秘密和不正确发送子秘密的用户均不能重构出共享秘密”的极端情形，从而导致“空威胁(empty threat)”情形的出现，即没有理性用户发送自己拥有的子秘密给其余理性用户. 方案[35]通过让秘密分发者 Dealer 在秘密分发阶段指定理性用户在秘密重构阶段中发送子秘密先后顺序的方法，提出了一个无需可信用户参与且仅需 3 轮交互的理性秘密共享方案. 然而，该方案在使用时，依然可能会出现“不发送子密钥的用户仍能重构出共享密钥”的不公平情形. 此外，该方案仅适用于 $t=n>2$ 的特殊情形.

本方案通过在秘密分发阶段为每个理性用户发送大量虚假子秘密，使得理性用户难以准确猜测出真实共享子秘密的方法，在无需可信用户参与且不依赖其他密码技术(如安全多方计算、可验证随机函数等)的情形下实现了理性公平的秘密重构. 此外，

在使用本方案时，秘密分发者 Dealer 也无需准确地知道每个理性用户的收益函数，即可通过生成随机数的方式确定秘密重构阶段的交互轮数.

综上所述，本方案具有较好的可用性.

7 实 验

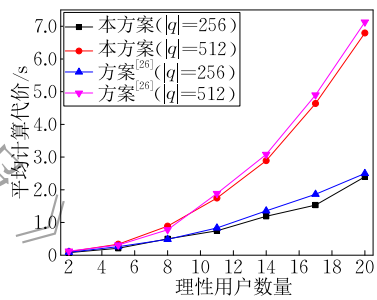
为说明上述提出的理性公平的秘密共享方案具有较好的实用性，本文利用 Miracl 密码学软件开发包对该方案进行模拟实验. 该密码学软件开发包是目前最常采用的一种密码学开发包，其定义了大量与密码学相关的基础函数，如大整数的生成、素数的判断等.

本实验首先在有限域 F_q 上随机构造 $t-1$ 阶多项式 $f_m(x)=\sum_{j=0}^{t-1}a_{j\_m}x^j$，使得 $f_m(0)=K_m$；并利用该多项式通过计算 $k_i^m=(i,f_m(i)\bmod q)$，将分发秘密 K_m 拆分成 n 份子秘密 $k_1^m,k_2^m,\cdots,k_n^m$. 其中，q 是大素数；多项式系数 $a_0,a_1,\cdots,a_{t-1}\in F_q$；$1\le i\le n$. 此外，还选用国家密码管理局公布的 SM2 椭圆曲线公钥密码算法为每个子秘密 k_i^m 进行签名生成承诺信息 $c_i^m=sign_{\mathrm{Dealer}_{SK}}(k_i^m\|ID_i\|m)$，并通过计算 $verf_{\mathrm{Dealer}_{PK}}(c_{i'}^m,ID_{i'},m)$ 来验证理性用户发送的子秘密的正确性. 本实验设定秘密分发者的密钥长度为 256 bit；理性用户 P_i 的身份信息 ID_i 长度为 8 bit；当前重构轮数 m 的表示长度为 8 bit. 针对不同长度的 q 值，即 $|q|=256$ 和 $|q|=512$，通过变化门限值 t、理性用户数量 n 和重构交互轮数 N，分别进行 100 次实验. 实验所用算法均采用 C++ 编程语言实现，实验环境为 Intel Core i5-4590 3.30 GHz CPU，8 GB DDR4-2400 RAM，操作系统为 Windows 7-64 bit.

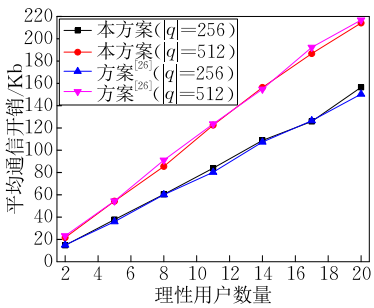
7.1 本方案所需的计算代价和通信开销

我们通过与方案[26]进行对比，表明本方案在无需准确地知道理性用户的收益函数且能实现理性公平的秘密重构的同时，并未增加秘密分发者 Dealer 和理性用户 P_i 的计算代价和通信开销，从而进一步说明本方案具有较好的实用性. 如表 1 所示，方案[26]是现有最好的理性秘密共享方案之一. 该方案无需可信用户参与，也无需使用其他复杂的秘密技术（如安全多方计算、可验证随机函数），且适用于异步通信情形. 在该部分实验中，设置 $2\le t=n\le 20$；秘密重构交互轮数 $N=20$.

在本方案中，秘密分发者 Dealer 生成 N 个共享秘密 $K_1,K_2,\cdots,K_N$，然后将每个秘密 K_m 拆分成 n 份 $k_1^m,k_2^m,\cdots,k_n^m$ 并计算每个子秘密 k_i^m 对应的承诺信息 c_i^m，共拆分 $n\cdot N$ 次；随后，秘密分发者 Dealer 通过点对点通信方式将子秘密 k_i^m 发送给理性用户 P_i，然后广播所有的承诺信息. 而在方案[26]中，秘密分发者首先将共享秘密 K^{real} 拆分成 n 份 $k_1^{\mathrm{real}},k_2^{\mathrm{real}},\cdots,k_n^{\mathrm{real}}$，然后再将每个子秘密 k_i^{real} 拆分成 N 份子秘密 $k_i^{1\text{-real}},k_i^{2\text{-real}},\cdots,k_i^{N\text{-real}}$ 并计算其相应的承诺信息，共拆分 $n\cdot N+1$ 次；随后，秘密分发者 Dealer 将子秘密 k_i^m 以及相应的承诺信息 c_i^m 通过点对点通信的方式发送给理性用户 P_i. 其中，$1\le i\le n$；$1\le m\le N$. 因此，秘密分发者 Dealer 使用本方案时，由于拆分共享秘密的次数比使用方案[26]时少 1 次，其所需的平均计算代价较低；而由于需要发送的子秘密和承诺信息数量与使用方案[26]时相同，故其所需的通信开销也相同. 如图 2(a)所示. 例如，当 $n=20$ 且 $|q|=512$ 时，若使用本方案，秘密分发者 Dealer 所需的平均计算代价和通信开销分别为 6.795 s 和 214.156 Kb；若使用方案[26]，其所需的平均计算代价和通信开销分别为 7.128 s 和 216.763 Kb. 如图 2(b)所示. 由此可见，对于秘密分发者 Dealer 来说，不仅无需准确地知道每个理性用户的收益函数，其所需的计算代价和通信开销也未增加.



(a) 平均计算代价

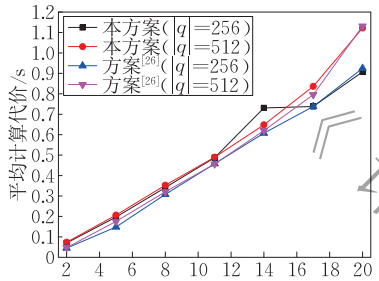


(b) 平均通信开销

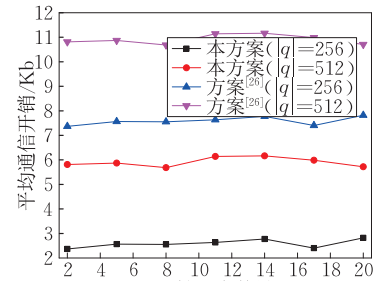
图 2 秘密分发者的平均计算代价和通信开销

此外，如图 3 所示，使用本方案和方案[26]时，理性用户所需的平均计算代价基本相同；而使用本方案时理性用户所需的平均通信开销低于使用方案[26]时所需的通信开销. 造成上述现象的原因是：当使用本方案时，由于秘密分发者将所有子秘密的承诺信息进行广播，因此在秘密重构阶段中，理性用

户 P_i 仅需发送自己拥有的子秘密 k_i^m 给其余用户；而使用方案[26]时，由于秘密分发者仅将子秘密 k_i^m 对应的承诺信息 c_i^m 发送给理性用户 P_i，故理性用户 P_i 需在秘密重构阶段中将自己拥有的子秘密 k_i^m 和 c_i^m 发送给其余用户来表明自己的诚实行为. 此外，无论使用本方案还是方案[26]，在验证其余理性用户发送的子秘密 $k_1^m,\cdots,k_{i-1}^m,k_i^m,\cdots,k_n^m$ 的正确性后，理性用户 P_i 均采用插值法恢复出共享秘密 K_m. 例如，当 $n=20$ 且 $|q|=512$ 时，若使用本方案，理性用户所需的平均计算代价和通信开销分别为 1.122 s 和 5.719 Kb；若使用方案[26]，其所需的平均计算代价和通信开销分别为 1.131 s 和 10.708 Kb. 因此，本方案也未增加理性用户的平均计算代价和通信开销.



(a) 平均计算代价



(b) 平均通信开销

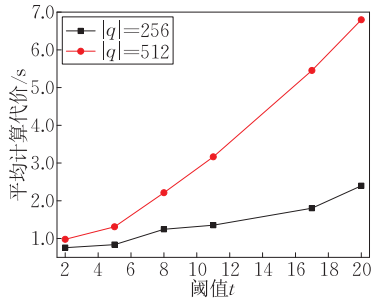
图 3　理性用户的平均计算代价和通信开销

综上所述，与方案[26]相比，本方案在实现理性公平性且不要求秘密分发者 Dealer 准确获知理性用户的收益函数的同时，还未增加秘密分发者 Dealer 和理性用户的平均计算代价和通信开销. 这表明本方案具有较好的实用性.

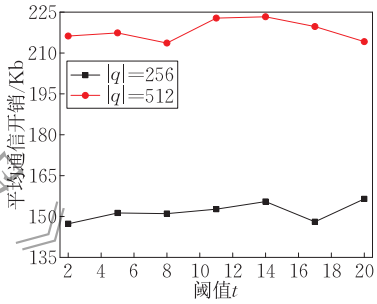
7.2　门限值 t 对本方案的影响

下面分析门限值 t 对本方案所需平均计算代价和通信开销的影响. 在该部分实验中，设定 $n=N=20$.

对于秘密分发者 Dealer 来说，当要将秘密 K_m 拆分成子秘密 $k_1^m,k_2^m,\cdots,k_i^m$ 进行分发时，首先需要从有限域 F_q 中挑选 $t-1$ 个系数 $a_{1\_m},a_{2\_m},\cdots,a_{t-1\_m}$ 构造 $t-1$ 阶多项式 $f_m(x)=K_m+\sum_{j=1}^{t-1}a_{j\_m}x^j$，并计算子秘密 $k_i^m=(i,f_m(i)\bmod q)$. 其中 $K_m\in F_q$；$1\le i\le n$；$1\le m\le N$. 因此，随着门限值 t 的增加，秘密分发者 Dealer 构造 $t-1$ 阶多项式以及计算 k_i^m 所需的计算代价也随之增加. 但是，无论门限值 t 如何变化，秘密分发者 Dealer 需要发送的子秘密数量以及承诺信息数量均不会发生变化，故秘密分发者 Dealer 所需的平均通信开销并不随着门限值 t 的变化而变化. 例如，当阈值 t 从 2 变化到 20 且 $|q|$ 分别为 256 和 512 时，其平均计算代价分别从 0.759 s 和 0.977 s 提升至 2.397 s 和 6.795 s，如图 4(a) 所示；而所需平均通信开销则保持不变，分别为 150.045 Kb 和 220.136 Kb，如图 4(b) 所示.



(a) 平均计算代价

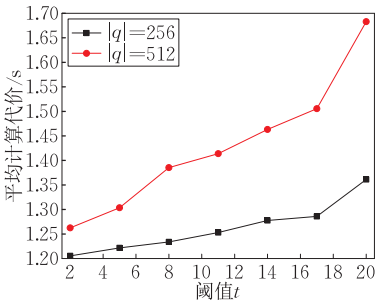


(b) 平均通信开销

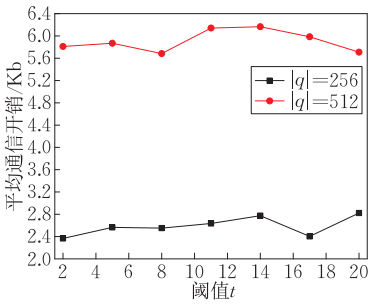
图 4　阈值 t 对秘密分发者的影响

对于理性用户 P_i 来说，随着阈值 t 的变化，其在收到其余理性用户发送的子秘密后，利用拉格朗日插值法计算 $f(x)=\sum_{i=1}^{t}l_i(x)f_m(i)$ 恢复出秘密 K_m 所需要的加法运算、乘法运算以及乘法运算的逆运算次数也在增多，从而导致理性用户 P_i 所需的计算代价也随之增大. 其中，$l_i(x)=\prod_{j=1,j\ne i}^{t}\frac{x-i}{i-j}$；$1\le m\le N$. 但是，理性用户需要发送的子秘密数量并不随着阈值 t 的变化而改变. 综上所述，理性用户的平均计算代价随着阈值 t 的增大而增加，而其平均通信开销随着阈值 t 的增大而保持不变. 如图 5 所示.

值得强调的是，在本实验中，秘密分发者 Dealer 和理性用户的平均通信开销出现波动的原因是：针对不同的阈值 t，随机生成的多项式系统不同，使得

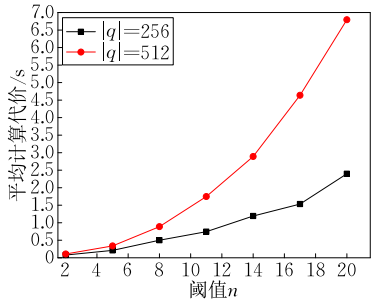


(a) 平均计算代价

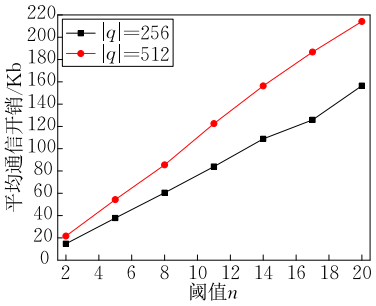


(b) 平均通信开销

图 5 阈值 t 对理性用户的影响



(a) 平均计算代价



(b) 平均通信开销

图 6 阈值 n 对秘密分发者的影响

计算出的子秘密的长度发生改变,从而导致秘密分发者 Dealer 和理性用户发送子秘密所需的平均通信开销也随之波动.

7.3 理性用户数量 n 对本方案的影响

本部分实验用于分析当使用本方案实现公平的秘密共享时,理性用户数量 n 对秘密分发者 Dealer 和理性用户所需计算代价的影响. 其中,设定 $t=2$ 和 $N=20$.

如图 6 所示,当参与秘密共享的理性用户数量增多,即阈值 n 变大时,秘密分发者 Dealer 在秘密分发阶段中需将共享秘密 $K_m(1\leq m\leq N)$ 拆分并发送的子秘密 $k_i^m(1\leq i\leq m)$ 的数量也随之增多. 同时,为了防止理性用户在秘密分发阶段发送错误的子秘密给其余用户,秘密分发者 Dealer 还要为每个子秘密 k_i^m 计算相应的承诺信息 $c_i^m=sign_{\mathrm{Dealer}_{SK}}(k_i^m\|ID_i\|m)$. 因此,随着拆分的子秘密数量的不断增多,秘密分发者 Dealer 需要计算和发送的承诺信息的数量也在不断增加. 这就造成了秘密分发者 Dealer 所需的计算代价和通信开销随着 n 的变大而增加.

在秘密重构阶段的任意第 m 轮交互中,随着理性用户数量 n 的增加,理性用户 P_i 需要接收到其余理性用户发送的子秘密数量也随之增多. 每当理性用户 P_i 收到一个其余理性用户 P_j 发送来的子秘密 k_j^m,其都要计算 $verf_{\mathrm{Dealer}_{PK}}(c_j^m,ID_j,m)$ 来验证该子秘密的正确性. 因此,理性用户所需的平均计算代价随着理性用户数量 n 的增加而不断提高. 如图 7 所示. 但是,在本方案中,理性用户 P_i 是通过广播通信将自己拥有的子秘密发送给其余用户,其需要发送的子秘密数量仅受分发秘密数量 N 的影响. 因此,当理性用户数量 n 增多时,理性用户的平均通信开销的变化趋势与图 5(b)所示相同,保持不变.

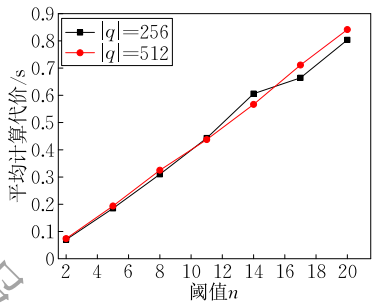


图 7 阈值 n 对理性用户平均计算代价的影响

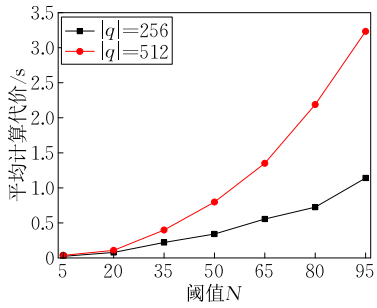
7.4 分发秘密数量 N 对本方案的影响

最后简要分析分发的秘密数量 N 对本方案所需平均计算代价和通信开销的影响. 设定 $t=n=2$.

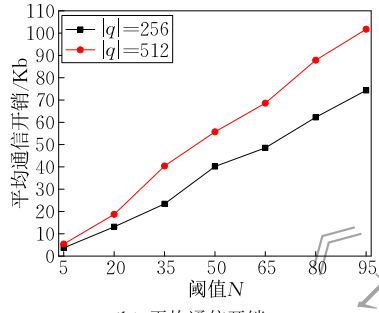
对于秘密分发者 Dealer 来说,随着分发秘密数量 N 的增多,其需要拆分和发送的子秘密数量以及关于这些子秘密的承诺信息数量也随之增加. 因此,随之阈值 N 的增大,秘密分发者 Dealer 的平均计算代价和通信开销也在不断提高. 如图 8 所示.

而对于理性用户来说,随着分发秘密数量 N 的增多,其在秘密重构阶段中需要交互的子秘密数量也不断增加. 这就使得理性用户在秘密重构阶段收到其余理性用户发送的子秘密数量也随之增多,从而提高了理性用户验证其余用户发送子秘密的正确性所需

的计算代价.综上所述,理性用户的平均计算代价和通信开销随着阈值 N 的增大而提高.如图 9 所示.

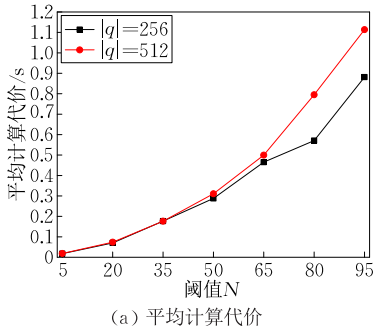


(a) 平均计算代价

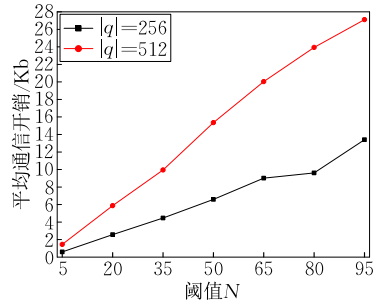


(b) 平均通信开销

图 8　阈值 N 对秘密分发者的影响



(a) 平均计算代价



(b) 平均通信开销

图 9　阈值 N 对理性用户的影响

8　总　结

现有理性秘密共享的公平性定义未能充分考虑理性用户的自利性行为,从而导致该公平性定义允许出现"发送子密钥的理性用户无法恢复出共享密钥,而不发送子密钥的用户却能重构出共享密钥"的不公平情形;甚至还会出现"发送错误的子秘密欺骗其余理性用户,使其将重构出的错误秘密视为真实共享秘密"的极端情形.因此,以该公平性定义为指导所设计出的方案在实际使用时,并不能实现公平的秘密共享.为了解决该问题,本文通过分析理性用户的自利性行为,将最小存取结构引入到理性秘密重构中,形式化地定义了秘密共享的理性公平性.为表明所提出的理性公平性的实用性,本文以理性公平性定义为指导,通过在秘密分发阶段为每个理性用户发送大量虚假子秘密,使得理性用户难以准确猜测出真实共享子秘密的方法,设计一个混淆激励机制,并构造了理性公平的秘密共享方案.理论分析和大量实验表明,本方案能有效地约束理性用户在秘密重构阶段中的自利性行为,确保所有用户均能重构出真实的共享密钥,高效地实现公平的秘密共享.

参　考　文　献

[1] Cao Z F. New Directions of Modern Cryptography. Florida: CRC Press, 2012

[2] Fu A, Qin N, Wang Y, et al. Nframe: A privacy-preserving with non-frameability handover authentication protocol based on (t,n) secret sharing for LTE/LTE—A networks. Wireless Networks, 2017, 23(7): 2165-2176

[3] Maitraye D, Nusrat J M, Sharmin A, et al. A novel secret sharing approach for privacy-preserving authenticated disease risk queries in genomic databases//Proceedings of the 42nd Annual International Conference on Computer Software and Applications (COMPSAC 2018). Tokyo, Japan, 2018: 645-654

[4] Liu H, Li X H, Xu M F, et al. A fair data access control towards rational users in cloud storage. Information Sciences, 2017, 418: 258-271

[5] Leon J H, Gamze T, Zekeriya E. BAdASS: Preserving privacy in behavioural advertising with applied secret sharing//Proceedings of the 12th International Conference on Provable Security (ProvSec 2018). Jeju, South Korea, 2018: 397-405

[6] Mahdi C. Nearly optimal robust secret sharing. Designs, Codes and Cryptography, 2019, 87(8): 1777-1796

[7] Halpern J, Teague V. Rational secret sharing and multiparty computation: Extended abstract//Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC 2004). Chicago, USA, 2004: 623-632

[8] Dodis Y, Rabin T. Cryptography and Game Theory. Cambridge: Cambridge University Press, 2007

[9] Katz J. Bridging game theory and cryptography: Recent results and future directions//Proceedings of the 5th International Conference on Theory of Cryptography (TCC 2008). New York, USA, 2008: 251-272

[10] Nanavati N R, Jinwala D C. A game theory based repeated rational secret sharing scheme for privacy preserving distributed data mining//Proceedings of the 10th International Conference on Security and Cryptography (SECRYPT 2013). Reykjavík, Iceland, 2013: 512-517

[11] Nanavati N R, Lalwani P, Jinwala D C. Game-theoretic privacy preserving constructions for rational and malicious secret sharing models for collaborative frequent itemset mining. International Journal of Knowledge Engineering and Data Mining, 2017, 4(3/4): 320-346

[12] Gordon S D, Katz J. Rational secret sharing, revisited//Proceedings of the 5th International Conference on Security and Cryptography for Networks (SCN 2006). Maiori, Italy, 2006: 229-241

[13] Abraham I, Dolev D, Gonen R, et al. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation//Proceedings of the 25th Annual ACM Symposium on Principles of Distributed Computing (PODC 2006). Denver, USA, 2006: 53-62

[14] Maleka S, Amjed S, Rangan C P. The deterministic protocol for rational secret sharing//Proceedings of the 22nd IEEE International Symposium on the Parallel and Distributed Processing (IPDPS 2008). Miami, USA, 2008: 1-7

[15] Maleka S, Shareef A, Rangan C P. Rational secret sharing with repeated games//Proceedings of the 4th International Conference on Information Security Practice and Experience (ISPEC 2008). Sydney, Australia, 2008: 334-346

[16] Micali S, Shelat A. Purely rational secret sharing (extended abstract)//Proceedings of the 6th International Conference on Theory of Cryptography (TCC 2009). San Francisco, USA, 2009: 54-71

[17] Tian Y L, Ma J F, Peng C G, et al. One-time rational secret sharing scheme based on Bayesian game. Wuhan University Journal of Natural Sciences, 2011, 16(5): 430-434

[18] Zhang Z F, Liu M L. Rational secret sharing as extensive games. Science China Information Sciences, 2013, 56(3): 1-13

[19] Asharov G, Lindell Y. Utility dependence in correct and fair rational secret sharing. Journal of Cryptology, 2011, 24(1): 157-202

[20] Nojoumian M, Stinson D R, Grainger M. Unconditionally secure social secret sharing scheme. IET Information Security, 2010, 4(4): 202-211

[21] Nojoumian M, Stinson D R. Socio-rational secret sharing as a new direction in rational cryptography//Proceedings of the 3rd International Conference on Decision and Game Theory for Security (GameSec 2012). Budapest, Hungary, 2012: 18-37

[22] Nojoumian M. Generalization of socio-rational secret sharing with a new utility function//Proceedings of the 20th International Conference on Privacy, Security and Trust (PST 2014). Toronto, Canada, 2014: 338-341

[23] Kol G, Naor M. Cryptography and game theory: Design protocols for exchanging information//Proceedings of the 5th International Conference on Theory of Cryptography (TCC'08). New York, USA, 2008: 320-339

[24] Kol G, Naor M. Games for exchanging information//Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC'08). New York, USA, 2008: 423-432

[25] Fuchsbauer G, Katz J, Naccache D. Efficient rational secret sharing in standard communication networks//Proceedings of the 7th International Conference on Theory of Cryptography (TCC 2010). Zurich, Switzerland, 2010: 419-436

[26] Zhang Z F, Liu M L. Unconditionally secure rational secret sharing in standard communication networks//Proceedings of the 13th Annual International Conference on Information Security and Cryptology (ICISC 2010). Seoul, Korea, 2010: 355-369

[27] Cai Y Q, Shi H L. Rational secret sharing scheme based on probability encryption without trusted center. Journal of Networks, 2011, 6(6): 899-903

[28] Wang J, Cai Y Q. A rational secret sharing scheme based on repeated game//Proceedings of the 7th International Conference on Computational Intelligence and Security (CIS 2011). Sanya, China, 2011: 615-619

[29] Yu Y, Zhou Z F. An efficient rational secret sharing protocol resisting against malicious adversaries over synchronous channels//Proceedings of the 8th International Conference on Information Security and Cryptology (Inscrypt 2012). Beijing, China, 2012: 69-89

[30] Wang Y L, Xu Q L. 2-out-of-2 rational secret sharing in extensive form//Proceedings of the 7th International Conference on Computational Intelligence and Security (CIS 2011). Sanya, China, 2011: 847-851

[31] Jin J H, Zhou X, Ma C G, et al. A rational secret sharing relying on reputation//Proceedings of the 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS 2016). Ostrawva, Czech Republic, 2016: 384-387

[32] Ong S J, Parkes D C, Rosen A, et al. Fairness with an honest minority and a rational majority//Proceedings of the 6th International Conference on Theory of Cryptography (TCC 2009). San Francisco, USA, 2009: 36-53

[33] Dani V, Movahedi M, Rodriguez Y, et al. Scalable mechanism for rational secret sharing. Distributed Computing, 2015, 28(3): 171-187

[34] Tian Y L, Peng C G, Lin D D, et al. Bayesian mechanism for rational secret sharing scheme. Science China Information Sciences, 2015, 58(5): 1-13

[35] Kawachi A, Okamoto Y, Tanaka K, et al. General constructions of rational secret sharing with expected constant-round reconstruction. The Computer Journal, 2017, 60(5): 711-728

[36] Sourya J D, Ruj S, Pal A K. Should silence be heard? Fair rational secret sharing with silent and non-silent players//Proceedings of the 13th International Conference on Cryptology and Network Security (CANS 2014). Heraklion, Greece, 2014: 240-255

[37] Zhang En, Yuan P Y, Du J. Verifiable rational secret sharing scheme in mobile networks. Mobile Information Systems, 2015, 462345: 1-7

[38] Sourya J D, Ruj S. Failure tolerant rational secret sharing// Proceedings of the 30th International Conference on Advanced Information Networking and Applications (AINA 2016). Montana, Switzerland, 2016: 925-932

[39] Liu H, Li X H, Ma J F, et al. Reconstruction methodology for rational secret sharing based on mechanism design. Science China Information Sciences, 2017, 60(8): 1-3

[40] Nisan N. Algorithmic mechanism design. Games and Economic Behavior, 2001, 35: 166-196

LIU Hai, Ph. D. His research interests include privacy protection and security protocol design.

LI Xing-Hua, Ph. D., professor. His research interests include network and information security, privacy protection and cryptography.

TIAN You-Liang, Ph. D., professor. His research interests include game theory, cryptography and security protocols.

LUO Bin, Ph. D. candidate. Her research interests include privacy protection and trust evaluation.

MA Jian-Feng, Ph. D., Yangtze river scholar professor. His research interests include network and information security, coding theory and cryptography.

PENG Chang-Gen, Ph. D., professor. His research interest is data privacy protection.

Background

With the development of communication technologies, emerging technologies like cloud computing and IoT(Internet of Things) arise, which bring convenience and become part of our daily life. However, when enjoying the convenient life, the users' privacy may disclose because they need to provide some individual data. To protect the users' privacy effectively, the cryptography participating in multi-player has attracted more attention, especially secret sharing.

In traditional secret sharing, the users are regarded as either honest or malicious. Honest users follow the prescribed protocol faithfully, whereas malicious users behave in arbitrary manners. However, in real applications, the users are selfish and always try to maximize their profits, which coincides with the selfish characteristic of rational users in game theory. Under this circumstance, rational secret sharing is proposed at the intersection of game theory and traditional secret sharing, which has been used widely, such as in the field of location privacy protection and data access control of cloud storage.

Unfortunately, due to the lack of adequate consideration about the users' selfish behaviors, the existing fairness definition of rational secret sharing implies some unfair solutions, which allows some of the users to reconstruct the secret but not send the shares, whereas the others cannot obtain the secret after sending the shares. More seriously, some of the users can cheat, making the other users view a fake secret as the real. Therefore, the existing rational secret sharing schemes cannot realize the fair secret sharing. To address this problem, this paper formalizes rational fairness of secret sharing by introducing into the access structure. Based on the proposed definition of rational fairness as guidance, through the generation of a great quantity of fake shares for rational users to make them not able to identify the real one, an incentive obfuscation mechanism is devised and a novel rational secret sharing scheme is presented. Theoretical analysis demonstrates that our scheme can motivate the users to send their shares honestly and make both of them reconstruct the real secret, thereby guarantee the fairness of rational secret sharing. Additionally, the extensive experiments illustrate that the computation overhead and communication cost of the proposal are limited, which shows that the presented scheme is applicable.

This work was sponsored in party by the National Natural Science Foundation of China under Grant (Nos. U1708262, U1736203, U1836205, 61772008), the National Key Research and Development Program of China under Grant (No. 2017YFB0801805), the Science and Technology Program of Guizhou Province under Grant (No. [2020]1Y265), the Research Foundation of Guizhou University of Finance and Economics under Grant (No. 2019XYB17).