密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2017,4(1):1–15

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

密码学与博弈论的交叉研究综述*

彭长根[1,2,3], 田有亮[1,2,3], 刘 海[4], 丁红发[5,6]

1. 贵州大学 计算机科学与技术学院, 贵阳 550025
2. 贵州省公共大数据重点实验室(贵州大学), 贵阳 550025
3. 贵州大学 密码学与数据安全研究所, 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. 贵州大学 理学院, 贵阳 550025
6. 贵州财经大学 信息学院, 贵阳 550025

通讯作者: 彭长根, E-mail: peng_stud@163.com

摘 要: 博弈论与密码学的学科相似性催生了博弈密码学这个新兴的交叉研究方向, 博弈论为解决密码协议中的一些安全目标提供了一种契机. 传统的密码系统只考虑诚实参与者或恶意参与者, 本文从博弈论和密码学的共性出发, 通过自利参与者的引入, 介绍了博弈密码学研究的出发点和思路, 形式化描述了密码系统博弈模型及相关概念; 进一步介绍了理性密码协议安全性定义, 初步从博弈均衡的角度探讨了密码协议的公平性, 并基于均衡理论对密码协议的安全性和公平性模型及定义进行分析; 对理性公平交换、理性秘密共享和理性安全多方计算的研究现状进行了综述和分析, 指出了存在的相关问题; 阐述了经济学中的机制设计及其在博弈密码协议设计中的应用及前景; 最后简单叙述了我们的一些工作, 介绍了基于特殊博弈模型、混合偏好模型和均衡理论的理性密码协议设计思路, 重点探讨了理性密码协议的公平机制设计问题. 针对博弈密码学作为极具挑战性的研究领域, 本文同时给出了一些需要深入探讨的相关问题.

关键词: 博弈论; 密码学; 均衡; 公平性; 机制设计
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000158

中文引用格式: 彭长根, 田有亮, 刘海, 丁红发. 密码学与博弈论的交叉研究综述[J]. 密码学报, 2017, 4(1): 1–15.
英文引用格式: PENG C G, TIAN Y L, LIU H, DING H F. A survey on the intersection of cryptography and game theory[J]. Journal of Cryptologic Research, 2017, 4(1): 1–15.

A Survey on the Intersection of Cryptography and Game Theory

PENG Chang-Gen[1,2,3], TIAN You-Liang[1,2,3], LIU Hai[4], DING Hong-Fa[5,6]

1. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
2. Guizhou Provincial Key Laboratory of Public Big Data (Guizhou University), Guiyang 550025, China
3. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China
4. School of Network and Information Security, Xidian Universality, Xi'an 710071, China
5. College of Science, Guizhou University, Guiyang 550025, China
6. School of Information, Guizhou University of Finance and Economics, Guiyang 550025, China

Corresponding author: PENG Chang-Gen, E-mail: peng_stud@163.com

* 基金项目: 国家自然科学基金(61662009, 61262073, 61363068); 贵州省公共大数据重点实验室项目([2016]4001); 贵州省教育厅创新团队项目(2013-09)

收稿日期: 2016-08-23 定稿日期: 2016-11-17

Abstract: Rational cryptography is an emerging direction of the cross-discipline of cryptography and game theory. Game theory provides an opportunity to reach some secure goals in cryptography. In view of the fact that traditional cryptography only considers honest participants or malicious participants, starting with the similarity of game theory and cryptography, this paper first discusses basic research ideas of rational cryptography, and formalizes its game models and concepts based on introduction of selfish participants. This paper further introduces the security of rational cryptographic protocols, gives fairness of cryptographic protocols from the views of game equilibrium, and analyzes the security and fairness models in cryptography based on equilibrium theory. Furthermore, some known results about the rational fair exchange, rational secret sharing and rational multi-party computation are overviewed extensively. Then the definition of mechanism design in microeconomic is stated and its application prospect in rational cryptography is discussed. Finally, the designs of rational cryptographic protocols based on special game model, hybrid preference model and equilibrium theory in this field are introduced. In particular, the fair mechanism designs of rational cryptographic protocols are recommended. The challenges and opportunities of this promising topic are summarized at the end of this paper.
Key words: game theory; cryptography; equilibrium; fairness; mechanism design

1 引言

密码学和博弈论的共性都是研究两个或多个互不信任实体的交互活动, 都是通过设计相应的算法机制, 解决实体之间的合作与竞争冲突问题. 然而, 它们的研究目标和内容体系有所不同. 密码学侧重于协议的设计与实现, 主要目标是在对手有恶意行为时, 设计协议算法以解决保密性、认证性、正确性和公平性; 而博弈论更侧重于博弈策略及规则设计, 其面对的环境更加开放, 参与者从自利的理性出发设计交互策略以达到获取最大利益的目标.

传统的密码协议模型一般只考虑诚实参与者和恶意参与者, 但随着应用需求的提升, 密码协议的参与者可能会从利益最大化的角度来选择自己的行为, 如电子商务、网上拍卖、分布式智能计算、复杂接入结构、云安全等方面的应用. 从这个意义上来说, 密码协议的这种理性参与者正好与博弈论中的理性局中人相符. 密码学和博弈论两个研究领域的惊人相似性引起了国内外相关学者的广泛关注, 近年来两个分支的交叉研究取得了一些非常丰富的成果[1,2], 其交叉问题的研究主要体现在两条线路: 一条线路是利用密码技术解决博弈论中的一些问题, 其中最主要的研究是探讨采用密码协议取代博弈模型中的可信仲裁者(Trusted Mediator)[3–7], 如采用安全多方计算协议充当可信仲裁者; 另一条路线是通过考虑密码学的特点以及计算能力和计算代价的限制, 扩展传统的博弈论的内容以适应密码学的目标需求[4,5,8]. 在这种背景下, 一个以具有理性参与者的秘密共享研究为核心的、博弈论与密码学相结合的研究方向—理性密码学(Rational Cryptography)[9]应运而生, 并逐渐成为研究热点[10].

早在1993年, Fischer和Wright[11]就分析了密码协议和博弈论之间的关系, 应用博弈论技术来分析多方密码交换协议. Buttyan和Hubaux[12]根据纳什均衡定义了理性交换的概念, 证明公平交换能推出理性交换, 反之则不成立. 后来 Gossner[13]将密码学方法应用到博弈论中, 证明通过公开通信, 原来的无限博弈的相关均衡能够被实现. Dodis 等[4]解决当存在可信第三方时, 其效用是可比较的二人博弈存在性判定问题. Brandt和Sandholm[14]用密码学本原来提供分布式机制的正确性和隐私保护. Asharov[15]在博弈意义下研究了密码协议的安全性和公平性的形式化问题, 通过考虑两方协议 Fail—Stop 攻击模型, 重点探索了当有恶意攻击时, 如何实现协议的保密性、正确性和公平性.

目前, 基于博弈论的密码学的研究方向主要表现在三个方面: 理性交换协议(Rational Exchange Protocol)、理性秘密共享(Rational Secret Sharing)和理性安全多方计算(Rational Secure Multiparty Computation). 尤其是, Halpern 和 Teague[9]首次提出的理性秘密共享和理性安全多方计算的概念, 对博弈论和密码学的交叉研究产生了极大的影响. 这些研究领域的核心是借助博弈论的概念和方法修改传统密

码学的目标, 如安全性和公平性. 基于博弈论的密码协议的关键点是在诚实参与者和恶意参与者基础上, 再引入具有自利性的理性参与者, 这样其攻击行为和合谋行为相较于传统方式发生了很大的变化. 因此, 安全性和公平性的合理定义、以收益函数为核心的机制设计就成为了博弈密码学的研究关键, 也就是通过合理的收益目标和机制设计, 使理性参与者都遵守协议的执行. 例如, 在理性秘密共享体制中, 通常以参与者都希望"自己能获取其他参与者的秘密, 但又不希望他人得到自己的秘密"为目标. 事实上这是一种假设参与者有特定的偏好及对偏好先验知识的量化方法, 这种先验知识的了解会直接影响到结果[16,17].

本文以博弈论和密码学的学科相似性为出发点, 力图综述和提炼这个交叉方向的研究结果和相关问题, 介绍博弈论在密码学领域中应用的基本概念和基本方法, 重点综述博弈密码学近年来的主要研究方向、研究成果, 分析相关概念、定义、结果及存在的问题; 总结我们近年来在理性分布式密码协议及其公平性、理性交换协议和机制设计等方面的相关研究工作; 最后, 给出博弈密码学发展方向的思考及展望.

2 博弈论与密码学的相关概念及问题

2.1 密码学的不可区分安全

密码学的根本目标是解决保密性和认证性, 一个密码系统是一个五元组:

$$\mathrm{CS}=(P,C,K,\mathrm{Enc},\mathrm{Dec})$$

其中: P 表示明文空间, C 表示密文空间, K 表示密钥空间, Enc 表示加密算法, Dec 表示解密算法.

对于计算安全的密码协议, 其安全性的定义[18]是根据敌手能力(攻击模型)来划分的. 安全性论断就是要在特定的计算模型下, 证明在某种敌手模型下能够达到预期的安全目标. 对于一个加密系统, 其安全性通常以计算不可区分性来衡量, 即对于敌手 A, 其在多项式时间内成功区分密文 $\mathrm{Enc}_k(m_0)$ 和 $\mathrm{Enc}_k(m_1)$ 的概率是可忽略的. 即:

$$\left|\Pr\left[A\left(\mathrm{Enc}_k(m_0)\right)=1\right]-\Pr\left[A\left(\mathrm{Enc}_k(m_1)\right)=1\right]\right|<\varepsilon(n)$$

其中 $m_0,m_1\in P$, $\varepsilon(\cdot)$ 是可忽略函数.

在密码模型中, 我们一般假设协议的参与者 P_1 和 P_2 总是诚实的, 他们需要共同抵御敌手的攻击. 这样的系统可以被简单地看成一个两方通信博弈, 即协议参与者 P_1 和 P_2 应该采用何种策略抵御攻击者, 而敌手又应采取何种策略使协议的参与者相信此次通信是安全的.

2.2 典型博弈模型

(1) 标准型博弈

标准型博弈 $G=\{P,A,U\}$ 是一个三元组, 其中:

- $P=\{P_1,\cdots,P_n\}$ 是参与者集合, $|P|=n$. P_i 表示第 i ($1\leqslant i\leqslant n$) 个参与者, P_{-i} 表示除了参与者 P_i 外的其余所有参与者的集合.
- $A=\{A_1,\cdots,A_n\}$ 是策略集合. 记参与者 P_i 的策略为 a_i, $a_i\in A_i$. 其中 A_i 为参与者 P_i 可选择的策略组成的策略集合. n 个参与者各选择一个策略形成的向量 $a=(a_1,\cdots,a_n)$ 称为策略组合. 记参与者 P_i 的对手 P_{-i} 所采取策略的组合为 a_{-i}.
- U 是参与者在不同策略组合下的效用函数. $U=\{u_1,\cdots,u_n\}$, $u_i:A\to R$ (R 代表实数空间), 表示参与者 P_i 在不同策略组合下所得到的收益.

(2) 扩展型博弈

扩展型博弈是一个多元组 $G=(P,A,H,F,U)$, 其中:

- $P=\{P_1,\cdots,P_n\}$ 是参与者集合，$|P|=n$. P_i 表示第 i ($1\leqslant i\leqslant n$) 个参与者，P_{-i} 表示除了参与者 P_i 外的其余所有参与者的集合.
- $A=\{A_1,\cdots,A_n\}$ 是参与者的行为集合，其中 $A_i=\{a_{i1},\cdots,a_{im}\}$ 为参与者 P_i 可选择的行为组成的行为集合，a_{ik} 表示参与者 P_i 的第 k ($1\leqslant k\leqslant m$) 种行为；n 个参与者各选择一个行为 $a_i\in A_i$ ($1\leqslant i\leqslant n$) 形成的向量 $a=(a_1,\cdots,a_n)$ 称为行为组合. 记参与者 P_i 的对手 P_{-i} 所采取策略的组合为 $a_{-i}=(a_1,\cdots,a_{i-1},a_{i+1},\cdots,a_n)$.
- H 是历史序列集合，其中空字符 $\varepsilon\in H$. 对于任意的 $h=\{a^l\}_{l=1}^{L}\in H$, 称 h 为一段长度为 L 的历史，其中 a^l 是第 l 步所有采取行动的参与者的一个行为组合. 对于任意的 $h\in H$，在 h 之后可能出现的所有行为的组合记为 $A(h)=\{a|(h,a)\in H\}$. 如果 $A(h)=\varphi$, 则称 h 是终止的. Z 表示所有的终止历史组成的集合.
- 函数 $F:(H\setminus Z)\to P$, 为没有终止的历史 $h\in H\setminus Z$ 指定下一步行动的参与者集合.
- $U=\{u_1,\cdots,u_n\}$ 是参与者在不同策略组合下的效用函数集合，其中 $u_i:Z\to R$ (R 代表实数空间)，表示参与者 P_i 在不同策略组合下所得到的收益.

2.3 基于博弈的密码模型

博弈论考虑的参与者都是理性的，理性参与者具有“自利性”，他们只追求自身利益最大化. 即:

(1) 如果 $\text{infor}_i(a)=1$, $\text{infor}_i(a')=0$, 则: $u_i(a)>u_i(a')$;

(2) 如果 $\text{infor}_i(a)=\text{infor}_i(a')$, 且 $\text{infor}_j(a')\leqslant\text{infor}_i(a)$, 则: $u_i(a)>u_i(a')$;

其中，$\text{infor}_i(a)\in\{0,1\}$ 表示理性参与者 P_i 是否获得所需要的.

在通信协议执行过程中，如果协议参与者是“自利”的，只在乎自己是否得到需要的信息，而不关心对方是否获得信息. 他们在协议执行过程中，可能发送错误的信息骗取对方的信息，这将导致传统密码协议的安全性并不适用于具有理性参与者参与的情形.

文献[19]提出具有理性参与者参与的密码协议，不再只是协议执行方与攻击方的两方博弈过程，而应该考虑为协议参与者 P_i 与其敌手 P_{-i} (包括攻击者，协议的其余参与者)的多方博弈.

令理性通讯协议 $\phi(M)=(\phi_1(M_1),\phi_2(M_2),\cdots,\phi_n(M_n))$, 其中 $\phi_i(M_i)$ 表示理性通讯方 P_i 的程序，令该通讯博弈为 $G^{P_1,\cdots,P_n,A,\text{CE}}_{\{\alpha_1,\cdots,\alpha_n,\varepsilon\}}$, 其中 A 表示攻击者；CE 表示通讯环境；α_i 表示理性参与者获得信息的概率；ε 表示攻击者 A 获得信息的概率. 则通讯协议 $\phi(M)$ 被称为一个理性安全通讯协议当且仅当:

(1) $(a_1^*,\cdots,a_n^*,a_A^*)$ 是博弈 $G^{P_1,\cdots,P_n,A,CE}_{\{\alpha_1,\cdots,\alpha_n,\varepsilon\}}$ 的纳什均衡，其中，$o=(\alpha_1,\cdots,\alpha_n,\varepsilon)$ 表示在策略组合 $(a_1^*,\cdots,a_n^*,a_A^*)$ 下博弈的均衡结果;

(2) 对于其他纳什均衡 $(a_1,\cdots,a_n,a_A)$, 有 $u_i(a_1,\cdots,a_n,a_A)\leqslant u_i(a_1^*,\cdots,a_n^*,a_A^*)$.

称通讯协议 $\phi(M)$ 是一个公平的理性通讯协议当且仅当 $\alpha_1\approx\cdots\approx\alpha_n$ 且 ε 是可忽略函数时.

具有理性参与者的博弈密码协议的理性攻击模型、理性安全模型及理性公平性与传统密码协议有很大的区别，如何构建合理的博弈模型形式化表示密码协议还有待更深入的研究.

3 博弈密码学的相关研究领域

3.1 均衡

传统博弈中一般都将纳什均衡作为博弈的解, 它是 Nash 在 20 世纪 50 年代提出来的, 是目前都比较认可的博弈解, 它是博弈论中研究的一个核心内容, 也是探讨博弈密码协议的重要工具.

策略组合 $a^*=\left(a_1^*,\cdots,a_n^*\right)$ 称为标准型博弈 $G=\{P,A,U\}$ 的一个纳什均衡, 如果对于任意参与者 P_i, 任意的策略 $a_i\in A_i$, 满足: $u_i\left(a_i^*,a_{-i}^*\right)\geqslant u_i\left(a_i,a_{-i}^*\right)$.

博弈密码协议中, 参与者可能同时采取行动, 也可能先后采取行动, 也就是密码学中的通过同步信道或者异步信道进行信息传递. 当采用异步信道时, 使用标准型博弈下的纳什均衡将受到极大的限制.

扩展型博弈中的参与者轮流采取行动, 其在观察到其他参与者的行动后可能会偏离自己的策略, 从而产生“空威胁”, 子博弈完美均衡可以作为解决“空威胁”的一个途径.

行为组合 $a^*=\left(a_1^*,\cdots,a_n^*\right)$ 称为扩展型博弈 $G=\{P,H,A,F,U\}$ 的一个子博弈完美均衡, 如果对于任意参与者 P_i, 任意的策略 $a_i\in G|_h$, 满足: $F(h)=i$, 且 $u_i\left(a_i^*|_h,a_{-i}^*|_h\right)\geqslant u_i\left(a_i,a_{-i}^*|_h\right)$, 其中 $a^*|_h$ 是每个博弈 $G|_h$ 中的纳什均衡.

在不完全信息扩展型博弈中, 参与者不知道其他参与者在自己行动之前所采取的行动, 贝叶斯均衡、完美贝叶斯均衡可以解决密码协议中不完全信息下的相关博弈问题.

行为组合 $a^*(\theta)=\left(a_1^*(\theta_1),\cdots,a_n^*(\theta_n)\right)$ 称为扩展型博弈 G 的一个贝叶斯均衡, 如果对于任意参与者 P_i, 满足:

$$a_i^*(\theta)\in\arg\max_{a_i\in A_i(t_i)}\sum_{\theta_{-i}\in\Theta_{-i}}p_i\left(\theta_{-i}\mid\theta_i\right)u_i\left(a_i,a_{-i}^*\left(\theta_{-i}\right);\theta_i\right)$$

策略—信念系统组合 $(\text{pure}\_s;\rho)$ 称为一个精炼贝叶斯均衡, 如果它满足:

条件 1: 在每一个信息集中, 应该行动的参与者必须对博弈进行到哪个节点有一个“推断”.

条件 2: 给定参与者的推断, 参与者的策略必须满足序贯理性要求.

条件 3: 在处于均衡路径之上的信息集中, “推断”由贝叶斯法则及参与者的均衡策略给出.

条件 4: 对处于均衡路径之外的信息集, “推断”由贝叶斯法则及可能情况下的参与者的均衡战略决定.

通过将有理性参与者的密码协议的交互行为转化为一个博弈模型, 利用恰当的衡策略组合及求解, 不失为研究博弈密码协议相关性质的有效途径, 如安全性和公平性等. 另外, 将博弈论中的均衡概念应用到密码学时, 可以在满足自私性和排他性的同时, 实现协议的正确性和隐私性[20]. 在博弈论中, 博弈活动的参与者可能具有不同的偏好. 这些偏好可用参与者的类型, 如排他性、利己性进行抽象的表示. 因此, 在博弈活动中, 理性的参与者总会根据自己的类型选择最大化自身利益的博弈策略. 均衡理论能帮助参与者分析其余参与者的策略选择, 从而制定自己的应对策略. 它能保证各参与者在具有不同类型的情形下, 使得每个理性参与者的收益实现最大化.

3.2 密码协议中的博弈公平性

公平性(Fairness)是安全协议的一个重要的属性, 一直是密码学研究的热点. 它是指如果协议能够保证协议执行者在协议执行完成后, 要么都得到各自需要的信息, 要么都得不到. 也就是说, 公平性可使正确执行协议的一方相对于其他参与方来说, 不能处于劣势. 任何一方主动终止协议, 都不会对其他方造成损失.

在现有的公平性研究中, 针对不同的需求目标, 陆续出现了公平性的一些定义. Asokan[21,22]提出强公平与弱公平的概念, 但它仅考虑协议的结束时刻, 不适用于协议的整个执行过程, Pagnia[23]提出在协议结束后通过补偿措施来保证其公平性. 公平交换协议最早是由 Blum 等[24]提出. 在他们的方案中, 无需可信

第三方(TTP)的存在, 通过让参与者采用逐步交换信息的部分内容的方式实现公平交换, 因此也称为逐步交换协议. 然而, 他们的方案要求交换双方有相似计算能力, 并且存在“一个比特的不公平”以及交换轮数多而导致效率低下也是一个问题. 随后, 针对文献[24]方案中存在的“一个比特不公平”的问题, 学者们又提出通过削弱 TTP 的功能, 采用整体交换的方式实现公平交换. 1996 年, Coffey 和 Saidha[25]在协议中提出内联 TTP(inline TTP), inline TTP 参与协议主体的每一次信息交换, 这使得对 TTP 依赖程度和通信代价都较高. 同年, Zhou 等[26]将在线 TTP(online TTP)引入到公平交换协议中. 在线 TTP 主要实现转发密钥等关键信息, 从而降低了协议对 TTP 的依赖程度. 1997 年, Asokan 等[27]提出极具影响力的乐观公平交换协议. 在他们的方案中, 首次提出了离线 TTP(offline TTP)的概念. 离线 TTP 只有当协议执行产生异常时, 才介入进行争端仲裁. 这大大降低了对 TTP 的依赖和通信的开销. 随后, 针对公平交换协议的研究基本上都是基于 offline TTP 进行的. Bao 等[28]在带有离线第三方的情况下将待交换的完整信息作为一个计算输出, 提出了一个整体公平交换协议, 实现了真公平与高效率的统一. 但这个协议仅能应用于交换签名, 不具普适性.

交换协议的执行效率和对 TTP 的过多依赖依然是现有公平交换协议进入应用领域的主要障碍, 这在一定程度上制约了公平交换协议的发展. 因此, 通过引入理性参与者后, 在博弈的角度下研究公平性是一个很有意义的工作. 在博弈环境下的理性密码协议主要集中在理性公平交换协议研究, 对其他理性密码协议的公平性关注还较少. 1998 年, Syverson[29]首次提出了理性交换的概念, 基于弱比特秘密承诺函数设计了理性交换协议—Syverson 协议; Buttyan 和 Hubaux[30]在博弈意义下初步探讨了交换协议的不同公平性定义; 2001 年, Buttyan 等[12]进一步研究了公平交换与理性交换的关系, 指出公平性能推导出理性, 反之则不成立. 随后又基于扩展型博弈提出理性交换的形式化定义[31], 并基于该定义分析 Syverson 协议. Alcaide 等[32,33]通过计算理性参与者的期望收益, 分析两方理性交换协议的方法, 并首次提出面向多方的理性公平交换协议. 除此之外, 基于理性公平交换协议的电子合同签署协议的设计与分析, 也相继有文献进行研究和关注[34–36]. 在目前已有的理性交换研究中, 其公平性的含义基本上只考虑结果的瞬时公平, 很少考虑长远公平或过程公平等.

无可信第三方的交换协议的完全公平性几乎难以实现, 博弈意义下的公平性有望从另一种角度提供一种研究公平性的思路. 博弈意义下的逐步释放不但是理性交换协议公平性实现的主要方式, 同时也成为理性安全多方计算公平性研究的重点. 2011 年, Asharov 等[15]证明在安全计算中公平性和逐步释放是相互蕴含的, 他们还证明在理想环境下对于某些特殊的函数和效用集合的理性公平计算问题是不可能的. 下面简单介绍 Asharov 等给出的一个公平性的形式化定义:

f 是一个非平凡的二元函数, π 是一个两方协议. 理性参与者 P_0,P_1, 协议 π 满足逐步释放的性质, 即对于任意大的输入 $x_0^0,x_0^1,x_1^0,x_1^1,n$, 随机选择 $b_0,b_1\in\{0,1\}$, 理性参与者 $P_i(1\leqslant i\leqslant 2)$ 在协议完成后得到的效用函数为:

$$u_i^{\pi,A}\left(x_0^0,x_0^1,x_1^0,x_1^1,n\right)=\begin{cases}1, & \text{if output}_{\pi_i}=f_i\left(x_0^{b_0},x_1^{b_1},n\right)\text{ and output}_{\pi_{-i}}\neq f_{-i}\left(x_0^{b_0},x_1^{b_1},n\right)\\ -1, & \text{if output}_{\pi_i}\neq f_i\left(x_0^{b_0},x_1^{b_1},n\right)\text{ and output}_{\pi_{-i}}=f_{-i}\left(x_0^{b_0},x_1^{b_1},n\right)\\ 0, & \text{otherwise}\end{cases}$$

其中, $f_i\left(x_0^{b_0},x_1^{b_1},n\right)$ 是理性参与者 P_i 期望得到的正确输出, output_{π_i} 是理性参与者 P_i 实际得到的输出.

称协议 π 是公平的, 若对任意大的输入 $x_0^0,x_0^1,x_1^0,x_1^1,n$, 存在一个可忽略函数 $\varepsilon(n)$, 使得理性参与者在协议完成后的期望收益满足:

$$E\left(u_i^{\pi,A}\left(x_0^0,x_0^1,x_1^0,x_1^1,n\right)\right)\leqslant\varepsilon(n)$$

其中, $E\left(u_i^{\pi,A}\left(x_0^0,x_0^1,x_1^0,x_1^1,n\right)\right)=\left|\Pr\left(u_i^{\pi,A}\left(x_0^0,x_0^1,x_1^0,x_1^1,n\right)=1\right)-\Pr\left(u_i^{\pi,A}\left(x_0^0,x_0^1,x_1^0,x_1^1,n\right)=-1\right)\right|$.

该公平性的形式化定义表明, 在特定博弈模型下, 协议若满足最后的结果公平性及逐步释放的性质, 则蕴含协议满足过程公平性. 这样, 为过程公平或长远公平的复杂研究提供了一种新思路, 通过瞬时公平性研究过程公平或长远公平, 简化公平协议的分析与设计.

3.3 理性秘密共享

(t,n)门限秘密共享[37,38]是一种对关键信息进行分散管理的有效方法, 通过关键信息的分存和恢复算法实现控制权的分享. 在(t,n)门限秘密共享中, 秘密分发者将信息拆分成 n 份传递给 n 个参与者, 使得其存储结构[39] AS 满足:

$$\mathrm{AS}=\left\{A\subseteq P\middle|t\leqslant|A|\leqslant n\right\}$$

在传统的秘密共享方案中, 参与者要么是诚实的, 要么是恶意的.

2004 年, Halpen 和 Teague[9]提出的理性秘密共享, 是将博弈论应用到密码学的标志性研究. 在他们的方案中, 提出了“理性”参与者概念, 并给出理性参与者 P_i 效用函数的假设: $U^+>U>U^->U^{--}$. 其中,

(1) U^+: 只有理性参与者 P_i 获得共享秘密;

(2) U: 理性参与者 P_i 和 P_{-i} 都获得共享秘密;

(3) U^-: 理性参与者 P_i 和 P_{-i} 都未获得共享秘密;

(4) U^{--}: 只有理性参与者 P_{-i} 获得共享秘密.

他们证明了在(t,n)门限理性秘密共享方案中理性参与者存在不合作行为, 还证明了传统的固定交互次数通过重复剔出弱策略无法保证在有限的时间内实现理性秘密共享协议, 提出了使用随机交互次数的方案可以在期望的时间内实现公平的 (3,3) 理性秘密共享协议. 其公平性定义为: 协议结束后, 各理性参与者的最终收益为: $u_i=u_{-i}=U$. 然而, 该方案并不能处理 (2,2) 的情况.

2006 年, Gordon 和 Kazt[40]改进了 Halpern 和 Teague 的方案. 他们的方案中引入了活跃参与者的概念. 在交互过程中, 系统中存在 t^* (其中 $t^*\geqslant t$)个活跃参与者监视交互过程, 基于共享秘密的随机性, 通过适当选取秘密分发者分发正确秘密的概率 β, 首次实现 (2,2) 理性秘密共享, 并且还解决了秘密分发者一直在线的问题. 同年, Abraham 等[3]引入 k-resilient 纳什均衡理论, 研究了理性秘密共享协议中理性参与者的合谋行为, 他们的方案通过对插值多项式进行预处理, 使共享秘密以概率 α 进行分发, 恰当选择 α 就可以使博弈达到 k-resilient 纳什均衡, 防止 k 个理性参与者合谋. 2007 年, Dodis 和 Rabin[1]研究了密码学和博弈论的一些交叉问题, 特别是用密码学中的安全多方计算协议来解决博弈环境下的可信第三方问题. 2008 年, Maleka 等[41]将理性参与者秘密重构阶段的交互过程看作重复博弈, 通过惩罚策略(Grim Trigger Strategy)证明在参与者无法确定交互次数的情况下, 可以实现理性秘密共享. 随后, Maleka 等[42]又将重复博弈与秘密共享相结合, 引入折扣因子 $\delta\in(0,1)$, 使得理性参与者的收益为 $u_i+\delta u_i+\delta^2u_i+\cdots$, 提出确定性的理性秘密共享方案. 该方案在同步信道下, 通过设计惩罚策略, 使得即使存在 t 个恶意参与者也能实现理性秘密共享. 同年, Katz[43]给出密码学和博弈论交叉领域的研究综述. 2009 年, Asharov 和 Lindell[16]研究了秘密共享在博弈论环境下的效用等问题. Micali 和 Shelat[44]、Ong 等[45]通过引入诚实参与者设计公平的具有固定轮数的理性秘密共享方案. Nojoumian 等[46]提出了一个有特殊功能的信任函数, 基于该信任函数于 2010 年提出了一个无条件安全的社会秘密共享方案[47]. 同年, 李大伟等[48]给出关于理性秘密共享协议的一个研究综述, 对相关方案从采用的信道、期望执行时间和随机数取值等方面进行比较, 提出一些开放性问题和解决思路. Tian 等[49]针对理性秘密共享方案的一些不可能结果, 用贝叶斯博弈研究一次理性秘密共享问题, 引入完美贝叶斯均衡, 解决理性秘密共享方案中参与者不合作问题. Wang 等[50]将参与者的半诚实模型引入到理性秘密共享方案的研究中, 给出了适用于点对点通信的理性秘密共享方案. Zhang 等[51]利用不完全

信息扩展式博弈研究理性秘密共享问题, 他们在理性秘密共享方案中引入完美序列均衡. 随后, Sourya 和 Asim[52]、Varsha 等[53]分别对理性秘密共享方案的正确性以及交互信息量再次进行研究, 并提出相应的理性秘密共享方案. Sourya 等[54]利用广播加密算法, 设计了适用于通信资源受限情形下的理性秘密共享方案. 彭长根等[55]通过对参与者的眼前利益和长远利益进行统一考虑, 提出了理性参与者的混合收益模型. 刘海等[56]利益贝叶斯博弈模型对理性秘密重构博弈进行分析, 并结合 VCG 机制设计激励相容的交互记录机制来约束理性参与者的自理性行为, 确保(2,2)理性秘密共享博弈的公平性. Tian 等[57]通过提高理性参与者的信誉值作为额外激励, 考虑不完全信息情形下理性秘密重构博弈, 构造出仅需 1 个秘密重构轮的(2,2)理性秘密共享方案. 2015 年, Maitra 等[58]首次在量子通信模式下, 提出了能够达到严格 Nash 均衡的理性秘密共享方案. Zhang 等[59]通过定义一种能够实现非交互式验证证明的可验证随机函数, 在移动网络中构造了公平的理性秘密共享方案. Harn 等[60]提出了一种异步理性秘密共享, 摒除了秘密重构阶段的内部和外部敌手, 且无需对交互性和诚实参与者数量的要求. 2016 年, 祁冠杰和周展飞[61]通过多轮交互和真实轮数未知的机制保证理性秘密共享协议执行, 并用可验证随机函数和拜占庭一致广播协议检测和屏除恶意参与者.

3.4 理性安全多方计算

Halpern 和 Teague 首次[9]提出理性秘密共享的同时, 也提出理性安全多方计算. 他们将其认为是理性秘密共享方案的一种直接应用.

保密性、正确性和公平性是安全多方计算的重要性质, 文献[15]利用效用函数从博弈论的角度分别给出了隐私性、正确性和公平性的定义. 具体如下:

保密性: 设 π 为一个计算 f 的两方计算协议, 对于每个 a_0,a_1 和 b, 和每个猜测算法 B, 参与者 P_0 关于 $x\in\{a_0,a_1\}$ 的效用函数为:

$$u_0^p\left(h_{\pi_B^p,P_1}(x,b,n),a_0,a_1,b\right)=\begin{cases}-1, & \text{if guess}_{\pi_B^p,P_1}=1 \text{ and } x=a_1\\ 0, & \text{otherwise}\end{cases}$$

其中 b 为猜测算法 B 的行动, n 为安全参数, $h_{\pi_B^p,P_1}(x,b,n)$ 是参与者 P_1 使用猜测算法 B 对参与者 P_0 的行动进行猜测的历史, $\text{guess}_{\pi_B^p,P_1}=1$ and $x=a_1$ 表示参与者 P_1 使用猜测算法 B 猜中参与者 P_0 的行动.

设 f 和 π 如上所示, 协议 π 对参与者 P_0 是博弈论保密的, 如果协议 π_B^p 是关于 u_0^p、u_1^p、保密性分布集合 $D_{f,n}^p=\{a_0,a_1,b\}$ 和概率多项式时间的算法 B 是一个纳什协议.

正确性: 设 π 为一个失败—停止博弈, 对于每个如上的 a,b, 协议 π 的正确性定义为:

$$u_i^c\left(h_{\pi,P_i}^{\varphi}\right)=1$$

$$u_i^c\left(\text{output}_{\pi,P_i},a,b\right)=\begin{cases}1, & \text{if output}_{\pi,P_i}=f_i(a,b)\\ 0, & \text{otherwise}\end{cases}$$

其中 $u_i^c\left(h_{\pi,P_i}^{\varphi}\right)=1$ 表示参与者 P_i 没有参与计算时的效用为 1, 参与者 P_i 使用协议 π 正确计算出 $f_i(a,b)$ 时的效用为 1, 其他为 0.

公平性: 设 f 为一个非平凡的两方计算函数, π 是一个两方计算协议, 对于参与者的输入 $x_0^0,x_0^1,x_1^0,x_1^1,n$、策略组合 (σ_1,σ_2) 和概率多项式时间 B_0, 参与者 P_0 的效用函数为:

$$u_0^f(\sigma_0,\sigma_1)=\begin{cases}1, & \text{if output}_{\pi_{B'},P_0}^f=f_0(x_0,x_1) \text{ and output}_{\pi_{B'},P_1}^f\neq f_1(x_0,x_1)\\ -1, & \text{if output}_{\pi_{B'},P_0}^f\neq f_0(x_0,x_1) \text{ and output}_{\pi_{B'},P_1}^f=f_1(x_0,x_1)\\ 0, & \text{otherwise}\end{cases}$$

其中 $B'=(B_0,B_1)$, B_i 表示参与者 P_{-i} 过早中止时参与者 P_i 用来猜测自己输出的算法.

因此, 其公平性定义为: 设 f 为非平凡两方计算函数, π 是计算 f 的两方计算协议, 对于任意的如上输入和具有概率多项式时间计算能力的敌手 A, 称协议 π 公平地计算 f, 如果在上述效用函数下存在可忽略函数 $\varepsilon(n)$, 使得:

$$E\left(u_0^f\left(\sigma_0,\sigma_1\right)\right)\leqslant\varepsilon(n)$$

其中, $E\left(u_0^f\left(\sigma_0,\sigma_1\right)\right)=\left|\Pr\left(u_0^f\left(\sigma_0,\sigma_1\right)=1\right)-\Pr\left(u_0^f\left(\sigma_0,\sigma_1\right)=-1\right)\right|$ 为期望收益函数.

2005 年, Izmalkov 等[6]首次提出理性安全计算问题. 他们提出当所有参与者都是理性的时候, 安全计算的安全性也必须要保证. 理性安全计算中各参与者的效用是用协议执行结束后各参与者得到协议输出结果来刻画, 他们用 Real/Ideal 模型中的两种不同类型博弈间的不可区分性来保证理性安全计算的安全性. 在理想环境中的博弈存在一个仲裁者(Mediator), 而现实环境中的理性安全计算协议不存在这样的仲裁者; 他们还指出任何理想环境中的有仲裁者的非完全信息博弈都能被一个投票箱博弈(Ballot-box Game)安全的仿真. 2006 年, Lysyanskaya 和 Triandopoulos[62]提出混合行为模型, 即参与者要么是理性的, 要么是邪恶的(Adversarial), 在此模型中分析了多方计算问题. 他们通过在同步广播信道上实施一个可验证的安全多方计算协议防止理性参与者偏离协议, 并通过非交互式零知识证明来确保理性参与者输入的正确性. 他们还证明了邪恶的敌手至多能控制 $\lceil n/2\rceil-2$ 位局中人. 2012 年, Groce 和 Katz[63]再次对两方理性公平计算进行研究, 他们提出的方案[64]存在“空威胁”问题. 他们分别在 Fail-Stop 环境和 Byzantine 环境下, 利用不确定轮数的方法, 设计 SharGen 功能函数, 使得理性参与者在猜测正确轮数的概率 $\alpha<\left(a_0-u_0^*\right)\big/\left(b_0-u_0^*\right)$ 时, 该协议是公平的. 但是, 在他们的方案中, 要求理性参与者同时进行策略选择. 为了解决上述问题, Wallrabenstein 和 Clifton[65]利用完美贝叶斯博弈模型来刻画在不完全信息博弈下, 理性参与者的博弈信念与策略选择顺序间的关系, 利用完美贝叶斯均衡消除理性多方计算中不可置信的均衡解, 提出了一个公平的理性多方安全计算方案. 随后, Wang 等[66]将理性参与者的信誉引入到理性计算博弈过程中, 利用理性参与者信誉值的动态变化来约束其自理性行为, 提出了社会理性多方安全计算方案. Wang 等[67]通过定义基于秘密份额获取量的效用函数提出了一种激励驱动博弈模型, 用模块化的思想扩展了理性多方计算的公平性模型. 王伊蕾等[68,69]考虑私有类型理性参与者的理性安全计算, 在非完美信息博弈下设计了可计算序贯博弈使其达到更高要求的公平, 并进一步利用模糊理论设计了非完美信息的模糊博弈计算.

3.5 密码协议中的机制设计

机制设计是博弈论和社会选择理论的综合运用, 是考虑构造怎样的博弈, 使得该博弈的均衡解是社会目标. 其面对的经济活动往往是信息不完全及决策分散化的环境, 密码体制也会面临此类问题. Naor[70]提出了机制设计运用于密码学的想法, 但之后在密码协议的机制设计方面很少有深入的研究. 2004 年 Halpern 和 Teague[9]具有开创性的工作中就已使用“机制”(Mechanism)一词. 随后在理性秘密共享[45,71]和理性多方安全计算[72]中, 也多次使用“机制”. 但是都还未将机制设计的相关理论运用到博弈密码协议的研究中.

机制 $M=(o,p)$, 其中: 每个参与者 $P_i(1\leqslant i\leqslant n)$ 都选择一个策略, 构成一个行为组合 $a=\left(a_1,a_2,\cdots,a_n\right)$. 机制将策略组合作为输入, 计算得到一个输出结果 $o=O(a)$, 称之为机制的分配规则; 机制还根据输入的策略组合, 给所有参与者 P_i 以转移支付 $p_i=p_i(a)(1\leqslant i\leqslant n)$, 称之为机制的支付规则. 机制设计者所期望达到的目标用社会选择函数 $g:\Theta_1\times\Theta_2\times\cdots\times\Theta_n\to O$, 其中 Θ_i 是理性参与者的类型空间. 当该机制执行后的均衡结果总是社会选择函数 g 的配置相一致时, 则称该机制下的均衡执行了 g. 所谓的真实上报直接显示机制是指参与者的策略就根据自己的真实类型 $\theta_i\in\Theta_i$ 向机制报告一个类型 θ_i', 如果参与者上报的是关于自己类型的真实信息, 即 $a_i\left(\theta_i\right)=a_i\left(\theta_i'\right)$, 那么该机制就是真实上报直接显示机制. 当一个直接机制下的博弈

均衡能够保证真实上报时, 则称该机制激励相容(Incentive Compatible).

机制在形式上与执行博弈密码协议的理性参与者的策略选择和最终获得的收益高度一致. 并且协议执行的期望结果可以通过设计合理的社会选择函数来表示. 因此, 设计公平的博弈密码协议即可转化通过设计合理的激励相容机制, 使得理性参与者在该机制下均衡的执行表现公平性的社会选择函数 f. 然而, 机制设计在博弈论中主要被运用到不完全信息静态博弈模型当中. 然而在博弈密码协议中, 尤其是在分布式博弈密码协议中, 使用同步信道几乎很难实现, 适用于异步通信的激励相容机制还有待深入研究.

机制设计的规范探讨起源于赫尔维茨于 1960 和 1973 年的开创性工作, 他规范地讨论了机制设计理论, 从而奠定了机制设计理论的基本框架. Nisan 和 Ronen[73]于 1999 年证明了机制设计理论在计算机领域的可计算性, 并给出了一个任务分配的实例. 2005 年, Feigenbaum 和 Shenker[74]总结了当时分布式环境下机制设计理论 DAMD(Distributed Algorithm Mechanism Design)的研究成果, 并指出了 DAMD 未来的研究方向. 随后, Feigenbaum[75]等首次将 DAMD 应用于计算机网络领域来解决具体的实际问题. 机制设计理论已被广泛的应用到了计算机的各个领域, 如: 域间计算[76,77]、Ad hoc 网络[78]、P2P 文件共享[79,80]、拥塞控制[81]和资源分配[82]等.

目前关于机制设计理论被引以注意的成果之一是 VCG 机制. VCG 机制最早是由 Vickrey[83]提出的第二价格拍卖机制构成的, 然后由 Clarkes[84]和 Groves[85]分别对其进行了扩展. VCG 机制是一类在拟线性效用环境下满足个人理性、策略一致的机制. 还是在所有满足个人理性、策略一致的机制中使得机制设计者期望收益最高的机制. VCG 机制的分配规则和支付规则应满足:

(1) 分配规则

$$o\left(\theta_1,\theta_2,\cdots,\theta_n\right)=\arg\max_{o\in O}\sum_{i=1}^{n}u_i\left(\theta_i,o\right)$$

(2) 支付规则

$$p_i\left(\theta_1,\theta_2,\cdots,\theta_n\right)=\sum_{j\neq i}u_j\left(\theta_j,o^*_{-i}\right)-\sum_{j\neq i}u_j\left(\theta_j,o^*\right)$$

其中, $o^*\left(\theta_1,\theta_2,\cdots,\theta_n\right)=\arg\max_{o\in O}\sum_i u_i\left(\theta_i,o\right)$, $o^*_{-i}\left(\theta_1,\theta_2,\cdots,\theta_n\right)=\arg\max_{o\in O}\sum_{j\neq i}u_j\left(\theta_j,o\right)$.

理性密码协议的参与者是理性的, 这种参与者和经济活动中的参与者一样具有自利性, 从这个角度上来说, 借助经济学中已有的机制设计理论, 解决理性密码协议中诸如“空威胁”、“搭便车”等问题, 并激励协议的正常完成, 不失为是一种有前景的方法. 通过随机化机制、惩罚机制及非精确均衡机制[86]等方法防范参与者的背叛行为, 能够保证协议运行达到其相应的预期结果.

4 我们的部分工作

近年来, 团队针对一些典型博弈密码协议中的有关问题进行了探索和研究, 包括密码协议的博弈模型及形式化、公平性、“空威胁”及“搭便车”等偏离协议的行为等; 利用博弈论相关均衡理论和机制设计方法、通用可组合框架对博弈论和密码学相交叉的基础协议及其公平性展开了研究. 主要工作有:

(1) 研究理性秘密共享体制中一般秘密共享体制及秘密共享体制中的秘密分发阶段, 假定秘密分发者(庄家)也是理性的, 提出理性第三方(Rational Third Party, RTP)的概念. 在理性假定下, 设计理性秘密分发机制, 有效防止秘密分发者的欺诈行为及秘密分发博弈达到更优的纳什均衡. 分别在门限结构和一般访问结构下分析秘密重构协议, 当各理性参与者在更愿意得到共享秘密的偏好下, 各参与者选择广播自己正确的子秘密是最佳策略. 但是, 在秘密重构协议中各参与者易产生不合作行为, 大家都不发送自己的子密钥, 出现“空威胁”情形. 最后设计一个秘密重构机制解决各理性参与者的合作问题.

(2) 研究仅执行一次理性秘密共享情况下的合作问题. Maleka 等[41]的工作表明在这种情况下实现秘密共享是不可能的. 而且在一次秘密共享方案中采用惩罚策略会转变成“空威胁”. 首先基于贝叶斯博弈构造

(2,2) 理性秘密共享模型, 该模型能考虑不同类型的协议参与者. 然后, 我们基于该模型提出一个 (2,2) 理性秘密共享方案, 解决了一次理性秘密共享方案的未解问题. 最后, 我们证明若协议参与者依照他们的信念系统和贝叶斯规则作决策, 其策略组合是一个完美贝叶斯均衡, 并且不要求同步信道.

(3) 研究理性秘密共享协议的合作问题. 基于贝叶斯博弈, 两方和多方场景下理性秘密共享的一种新的方法学被提出. 我们应用贝叶斯博弈分析秘密共享模型, 该模型从贝叶斯理性的观点更为合理的解释和说明了理性秘密共享协议. 与纯理性秘密共享模型相比, 贝叶斯模型在许多场景下都较为合理, 更符合社会实际的要求. 我们还提出了相应的理性秘密共享协议的贝叶斯机制, 解决参与者间能长期合作的秘密共享问题.

(4) 研究分布式理性秘密共享博弈的合作问题. 结合扩展性博弈模型, 形式化描述分布式理性秘密共享方案. 并同时考虑理性参与者的眼前利益和长远利益, 提出一种新的理性参与者混合偏好模型:

$$\overline{u}_i(a)=\left[w_i^{(s)}S\_\text{infor}_i(a)+w_i^{(L)}S\_\text{infor}_i(a)\right]\cdot u_i(a)$$

其中, $w_i^{(s)},w_i^{(L)}\in[0,1]$.

此外, 通过结合机制设计理论的策略一致机制设计了一个激励相容的信誉讨价还价机制以此有效约束理性参与者的行为从而实现了公平的 (t,n) 分布式理性秘密共享方案的构造.

(5) 2008 年, Maleka 等在重复博弈(repeated games)和惩罚策略的基础上提出了 Maleka 方案[42], 分析表明“格雷欣法则”在 Maleka 方案中会起作用, 诚实的参与者反而会被逐出协议, 这是不公平的. 为了解决这一问题, 我们构造了一个基于激励机制的秘密共享方案. 按照得到秘密的期望高低对参与者进行分类, 并引入激励机制, 对遵守协议的参与者做出鼓励, 对破坏协议的参与者做出处罚. 该方法保证了协议的正确性和公平性.

(6) 在文献[3]中第一次研究秘密共享方案的公平性问题, 后面研究其公平性问题的论文较少. 其实现公平性的方法主要有两种: 一种是要求在秘密重构过程中逐步释放信息以期获得共享秘密的方法; 另一种是要求在参与重构的成员中诚实的参与者占大多数, 否则不能实现秘密的公平重构.

针对该问题, 团队研究秘密共享体制中秘密重构的新方法. 我们从概率的角度定义秘密共享体制的公平性. 同时, 基于该定义提出公平的秘密共享方案, 并且在三种不同的攻击模型下证明该方案的安全性和公平性.

(7) 信誉机制是在电子市场中用于产生和传播信誉信息的一种工具, 可以对交易双方的行为产生约束, 降低交易风险. 理性的交易者在合理的信誉机制引导下, 会采取诚信的交易行为, 最大化自己的长期利益, 这为理性秘密共享的研究提供了新的思路.

参考社会网络的信誉机制, 探究了门限秘密共享中参与者的信任度量及信誉计算方法, 针对现有二次拟合信任函数的运算效率低的问题, 结合理性参与者的行为策略和交互信息的价值, 并考虑信任值增加单位, 提出了一个新的一次信任函数

$$T_{t+1}=\begin{cases}T_{t+1}^{C}=T_t+\lambda\cdot\Delta T^{C}, & \text{合作}\\ T_{t+1}^{D}=T_t+\lambda\cdot\Delta T^{D}, & \text{背叛}\end{cases}$$

并基于该信任函数构建了高效运行、信誉存储和通信成本较低的信誉机制, 设计了更为适用的信誉模型, 构建出一个面向理性秘密共享的信誉激励驱动机制. 基于博弈论首先分析了完全理性参与者在信誉机制下的行为偏好, 采用激励相容原理, 设计了合理的信誉惩罚机制, 有效地约束了完全理性参与者在理性秘密共享活动中的行为.

5 结语与展望

博弈论和密码学都是致力于解决多方协同系统中的复杂性与利益欺诈问题, 参与者的合作与竞争的

解决方案成了两个方向的共同目标. 博弈论为解决密码学中的安全性和公平性提供了一种契机, 同时为信息安全的应用提供了更广阔的前景和拓展空间. 本文重点从博弈的角度对密码协议的安全性和公平性进行了分析, 对理性秘密共享、理性多方安全计算和理性公平交换协议的研究现状进行了综述, 阐述并分析了经济学中的机制设计及其在博弈密码协议设计中的应用前景, 最后简单叙述了我们的一些工作. 博弈密码学的研究工作基本还处于起步和探索阶段, 在密码系统中引入理性参与者后, 其理性攻击模型、理性合谋模型、收益函数有待更进一步的研究, 理性密码协议中效率、算法机制设计和安全模型及安全证明更是有待探索的问题. 博弈论作为应用数学和经济学的交叉学科, 目前又进一步走向密码学领域, 既使得多学科交叉展现出新的魅力, 又为密码学开辟了极具挑战性的方向.

References

[1] DODIS Y, RABIN T. Cryptography and Game Theory[M]. Cambridge University Press, 2007.
[2] JUN S, VARAIYA P. Mechanism design for networking reseach[J]. Information Systems Frontiers, 2003, 5(1): 29–37.
[3] 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.
[4] DODIS Y, HALEVI S, RABIN T. A cryptographic solution to a game theoretic problem[C]. In: Annual International Cryptology Conference. Springer Berlin Heidelberg, 2000: 112–130.
[5] HALPERN J, PASS R. Game theory with costly computation[C]. In: Proceedings of the Behavioral and Quantitative Game Theory: Conference on Future Directions. ACM, 2010: 120–142.
[6] IZMALKOV S, MICALI S, LEPINSKI M. Rational secure computation and ideal mechanism design[C]. In: 46th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2005. IEEE, 2005: 585–594.
[7] IZMALKOV S, LEPINSKI M, MICALI S. Verifiably secure devices[C]. In: Theory of Cryptography Conference. Springer Berlin Heidelberg, 2008: 273–301.
[8] GRADWOHL R, LIVNE N, ROSEN A. Sequential rationality in cryptographic protocols[C]. In: Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science. IEEE, 2010: 623–632.
[9] HALPEN J, TEAGUE V. Rational secret sharing and multiparty computation: extended abstract[C]. In: Proceedings of the 36th Annual ACM Symposium on Theory of Computing. ACM, 2004: 623–632.
[10] NIELSEN J B. Summary report on rational cryptographic protocols[R]. Deliverable D.PROVI.7, University of Aarhus, ECRYPT IST-2002-507932, 2007.
[11] FISCHER M J, WRIGHT R N. An application of game theoretic techniques to cryptography[J]. Discrete Mathematics and Theoretical Computer Science, 1993, 13.
[12] BUTTYAN L, HUBAUX J P. Rational exchange-a formal model based on game theory[C]. In: Proceedings of the 2nd International Workshop on Electronic Commerce. Springer Berlin Heidelberg, 2001: 16–17.
[13] GOSSNER O. Repeated games played by cryptographically sophisticated players[R]. Technical Report Paper 9836, Catholique de Louvain-Center for Operations Research and Economics, 1999.
[14] BRANDT F, SANDHOLM T. On correctness and privacy in distributed mechanisms[C]. In: Agent-Mediated Electronic Commerce. Designing Trading Agents and Mechanisms. Springer Berlin Heidelberg, 2006: 212–225.
[15] ASHAROV G, CANETTI R, HAZAY C. Towards a game theoretic view of secure computation[C]. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2011: 426–445.
[16] ASHAROV G, LINDELL Y. Utility dependence in correct and fair rational secret sharing[C]. In: Annual International Cryptology Conference. Springer Berlin Heidelberg, 2009: 559–576.
[17] CLEVE R. Limits on the security of coin flips when half the processors are faulty[C]. In: Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing. ACM, 1986: 364–369.
[18] GOLDWASSER S, MICALI S. Probabilistic encryption[J]. Journal of Computer and System Science, 1984, 28(2): 270–299.
[19] TIAN Y L. Distributed Cryptographic Protocol and Fairness[D]. Xidian University, 2012.
田有亮. 分布式密码协议及公平性研究[D]. 西安电子科技大学, 2012.
[20] CABALLERO P, HERNANDEZ C, BRUNO C. A rational approach to cryptographic protocols[J]. Mathematical and Computer Modelling, 2007, 46(1–2): 80–87.
[21] ASOKAN N. Fairness in electronic commerce[D]. University of Waterloo, 1998.
[22] ASOKAN N, SHOUP V, WAIDNER M. Optimistic fair exchange of digital signatures[J]. IEEE Journal on Selected in Communication, 2000, 18(4): 593–610.
[23] PAGNIA H, VOGT H, GÄRTNER F C. Fair exchange[J]. The Computer Journal, 2003, 46(1): 55–75.

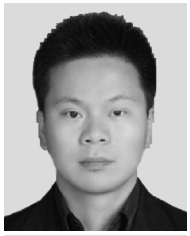
[24] BLUM M. Coin flipping by telephone: a protocol for solving impossible problems[J]. A Special Issue on Cryptography, 1983, 15(1): 23–27.
[25] COFFEY T, SAIDHA P. Non-repudiation with mandatory proof of receipt[J]. Computer Communication Review, 1996, 26(1): 6–17.
[26] ZHOU J, GOLLMAN D. A fair non-repudiation protocol[C]. In: IEEE Symposium on Security and Privacy, 1996. IEEE, 1996: 55–61.
[27] ASOKAN N, SCHUNTER M, WAIDNER M. Optimistic protocols for fair exchange[C]. In: Proceedings of the 4th ACM conference on Computer and Communications Security. ACM, 1997: 7–17.
[28] BAO F, DENG R H, MAO W. Efficient and practical fair exchange protocols with off-line TTP[C]. In: IEEE Symposium on Security and Privacy, 1998. IEEE, 1998: 77–85.
[29] SYVERSON P. Weakly secret bit commitment: Applications to lotteries and fair exchange[C]. In: 11th IEEE Computer Security Foundations Workshop, 1998. IEEE, 1998: 2–13.
[30] BUTTYAN L, HUBAUX J. Toward a formal model of fair exchange–a game theoretic approach[R]. Technical Report EPFL SSC/1999/039, Laboratory of Computer Communications and Applications, 1999.
[31] BUTTYAN L, HUBAUX J P, CAPKUN S. A formal model of rational exchange and its application to the analysis of syverson's protocol[J]. Journal of Computer Security, 2004, 12(3–4): 551–587.
[32] ALCAID A, ESTEVEZ-TAPIADOR J M, HERNANDEZ-CASTRO J C, et al. An extended model of rational exchange based on dynamic games of imperfect information[C]. In: Proceedings of Emerging Trends in Information and Communication Security, Springer Berlin Heidelberg, 2006: 396–408.
[33] ALCAIDE A, ESTEVEZ-TAPIADOR J M, HERNANDEZ-CASTRO J C, et al. A multi-party rational exchange protocol[C]. In: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". Springer Berlin Heidelberg, 2007: 42–43.
[34] CHADHA R, MITCHELL J C, SCEDROV A, et al. Contract signing, optimism, and advantage[C]. In: International Conference on Concurrency Theory. Springer Berlin Heidelberg, 2003: 366–382.
[35] KREMER S, RASKIN J F. Game analysis of abuse-free contract signing[C]. In: 15th IEEE Computer Security Foundations Workshop, 2002. IEEE, 2002: 206–220.
[36] SANDHOLM T, WANG X F. (Im)possibility of safe exchange mechanism design[C]. In: American Association for Artificial Intelligence Eighteenth National Conference on Artificial Intelligence. 2002: 338–344.
[37] BLAKLEY G R. Safeguarding cryptographic keys[C]. In: Proceeding of the National Computer Conference 1979. 1979: 313–317.
[38] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612–613.
[39] BRICKELL E. F, STINSON D. R. Some improved bounds on the information rate of perfect secret sharing schemes[J]. Journal of Cryptology, 1992, 5(3): 153–166.
[40] GORDON S D, KATZ J. Rational secret sharing, revisited[C]. In: International Conference on Security and Cryptography for Networks. Springer Berlin Heidelberg, 2006: 229–241.
[41] MALEKA S, SHAREEF A, RANGAN C P. The deterministic protocol for rational secret sharing[C]. In: IEEE International Symposium on Parallel and Distributed Processing—IPDPS 2008. IEEE, 2008: 1–7.
[42] MALEKA S, SHAREEF A, RANGAN C P. Rational secret sharing with repeated games[C]. In: International Conference on Information Security Practice and Experience. Springer Berlin Heidelberg, 2008: 334–346.
[43] KATZ J. Bridging game theory and cryptography: Recent results and future directions[C]. In: Theory of Cryptography Conference. Springer Berlin Heidelberg, 2008: 251–272.
[44] MICALI S. Purely rational secret sharing[C]. In: Theory of Cryptography Conference. Springer Berlin Heidelberg, 2009: 54–71.
[45] ONG S J, PARKES D C, ROSEN A, et al. Fairness with an honest minority and a rational majority[C]. In: Theory of Cryptography Conference. Springer Berlin Heidelberg, 2009: 36–53.
[46] NOJOUMIAN M, LETHBRIDGE T C. A new approach for the trust calculation in social networks[C]. In: International Conference on E-Business and Telecommunication Networks. Springer Berlin Heidelberg, 2006: 64–77.
[47] NOJOUMIAN M, STINSON D R, GRAINGER M. Unconditionally secure social secret sharing scheme[J]. IET Information Security, 2010, 4(4): 202–211.
[48] LI D W, YANG G, YU C G. A survey of rational secret sharing schemes[J]. Journal of Nanjing University of Posts and Telecommunications, 2010, 30(2): 89–94.
李大伟, 杨庚, 俞昌国. 理性参与者秘密共享方案研究综述[J]. 南京邮电大学学报, 2010, 30(2): 89–94.
[49] TIAN Y L, MA J F, PENG C G, et al. One-time rational secret sharing scheme based on Bayesian game[J]. Wuhan University Journal of Natural Sciences, 2011, 16(5): 430–434.
[50] WANG Y L, WANG H, XU Q L. Rational secret sharing with semi-rational players[J]. International Journal of Grid and Utility Computing, 2012, 3(1): 59–87.

[51] ZHANG Z F, LIU M L. Rational secret sharing as extensive game[J]. Science China Information Sciences, 2013, 56(3): 1–13.
[52] DE S J, PAL A K. Achieving correctness in fair rational secret sharing[C]. In: International Conference on Cryptology and Network Security. Springer International Publishing, 2013: 139–161.
[53] VARSHA D, MAHNUSH M, JARED S. Scalable mechanisms for rational secret sharing[J]. Distributed Computing. 2015, 28(3): 171–187.
[54] DE S J, RUJ S, PAL A K. Should silence be heard? Fair rational secret sharing with silent and non-silent players[C]. In: International Conference on Cryptology and Network Security. Springer International Publishing, 2014: 240–255.
[55] PENG C G, LIU H, TIAN Y L, et al. A distributed rational secret sharing scheme with hybrid preference model[J]. Journal of Computer Research and Development, 2014, 51(7): 1476–1485.
彭长根, 刘海, 田有亮, 等. 混合偏好模型下的分布式理性秘密共享方案[J]. 计算机研究与发展, 2014, 51(7): 1476–1485.
[56] LIU H, PENG C G, TIANG Y L, et al. The (2,2) Bayesian rational secret sharing scheme[J]. Acta Electronica Sinica, 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, 42(12): 2481–2488.
[57] 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.
[58] MAITRA A, DE S J, PAUL G, et al. Proposal for quantum rational secret sharing[J]. Physical Review A, 2015, 92(2): 022305.
[59] ZHANG E, YUAN P, DU J. Verifiable rational secret sharing scheme in mobile networks[J]. Mobile Information Systems, 2015, 2015.
[60] HARN L, LIN C, LI Y. Fair secret reconstruction in (*t*, *n*) secret sharing[J]. Journal of Information Security and Applications, 2015, 23: 1–7.
[61] QI G J, ZHOU Z F. Rational secret sharing scheme resisting against malicious adversaries in standard communication networks[J]. Journal of Cryptologic Research, 2016, 3(4): 408–418.
祁冠杰, 周展飞. 标准信道下的抗敌手的理性秘密共享方案[J]. 密码学报, 2016, (04): 408–418.
[62] LYSYANSKAYA A, TRIANDOPOULOS N. Rationality and adversarial behavior in multi-party computation[C]. In: Annual International Cryptology Conference. Springer Berlin Heidelberg, 2006: 180–197.
[63] GROCE A, KATZ J. Fair computation with rational players[C]. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2012: 81–98.
[64] BEIMEL A, LINDELL Y, OMRI E, et al. 1/p-secure multiparty computation without honest majority and the best of both worlds[C]. In: Annual Cryptology Conference. Springer Berlin Heidelberg, 2011: 277–296.
[65] WALLRABENSTEIN J R, CLIFTON C. Equilibrium concepts for rational multiparty computation[C]. In: International Conference on Decision and Game Theory for Security. Springer International Publishing, 2013: 226–245.
[66] WANG Y L, LIU Z, WANG H, et al. Social rational secure multi-party computation[J]. Concurrency and Computation Practice and Experience, 2014, 26(5): 1067–1083.
[67] WANG Y, CHEN L, LEUNG H, et al. Fairness in secure computing protocols based on incentives[J]. Soft Computing, 2015: 1–9.
[68] WANG Y L, ZHENG Z H, WANG H, et al. Rational fair computation with computational sequential equilibrium[J]. Journal of Computer Research and Development, 2014, 51(07): 1527–1537.
王伊蕾, 郑志华, 王皓, 等. 满足可计算序贯均衡的理性公平计算[J]. 计算机研究与发展, 2014, 51(07): 1527–1537.
[69] WANG Y, LI T, CHEN L, et al. Rational computing protocol based on fuzzy theory[J]. Soft Computing, 2016, 20(2): 429–438.
[70] NAOR M. Cryptography and mechanism design[C]. In: Proceedings of the 8th Conference on Theoretical Aspects of Rationality and Knowledge. Morgan Kaufmann Publishers Inc., 2001: 163–167.
[71] DANI V, MOVAHEDI M, RODRIGUEZ Y, et al. Scalable rational secret sharing[C]. In: Proceedings of the 30th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing. ACM, 2011: 187–196.
[72] IZMALKOV S, MICALI S, LEPINSKI M. Rational secure computation and ideal mechanism design[C]. In: 46th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2005. IEEE, 2005: 585–594.
[73] NISAN N, RONEN A. Algorithmic mechanism design[J]. Games and Economic Behavior, 2001, 35(1-2): 166–196.
[74] FEIGENBAUM J, SHENKER J. Distributed algorithmic mechanism design: recent results and future directions[C]. In: Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications. IEEE, 2002: 1–13.
[75] FEIGENBAUM J, PAPADIMITRIOU C, SAMI R, et al. A bgp-based mechanism for lowest-cost routing[C]. In: Proceedings of the 21st Symposium on Principles of Distributed Computing. IEEE, 2002: 173–182.
[76] ARCHER A, TARDOS E. Frugal path mechanism[C]. In: Proceedings of 13th ACM-SIAM Symposium on Discrete Algorithms. ACM, 2002: 991–999.

[77] HERSHBERGER J, SURI S. Vickrey prices and shortest paths: What is an edge worth?[C]. In: 42nd IEEE Symposium on Foundations of Computer Science, 2001. IEEE, 2001: 252–259.
[78] ANDEREGG L, EIDENBENZ S. Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents[C]. In: Proceedings of the 9th Annual International Conference on Mobile Computing and Networking. ACM, 2003: 245–259.
[79] FELDMAN M, LAI K, STOICA I, et al. Robust incentive techniques for peer-to-peer networks[C]. In: Proceedings of the 5th ACM Conference on Electronic Commerce. ACM, 2004: 102–111.
[80] MA R T, LEE C M, LIU J C, et al. Incentive p2p network: a protocol to encourage information sharing and contribution[J]. SIGMETRICS Performance Evaluation Review, 2003, 31(2): 23–25.
[81] JUN S, VARAIYA P. Mechanism design for networking reseach[J]. Information Systems Frontiers, 2003, 5(1): 29–37.
[82] NG C, PARKES D C, SELTZER M. Virtual worlds: Fast and strategyproof auctions for dynamic resource allocation[C]. In: Proceedings of the 4th ACM Conference on Electronic Commerce. ACM, 2003: 238–239.
[83] VICKREY W. Counter speculation, auctions and competitive sealed tenders[J]. Journal of Finance, 1961, 16(1): 8–37.
[84] CLARKE E. H. Multipart pricing of public goods[J]. Public Choice, 1971, 11(1): 17–33.
[85] GROCE A, KATZ J. Fair computation with rational players[C]. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2012: 81–98.
[86] DANI V, MOVAHEDI M, SAIA J. Scalable mechanisms for rational secret sharing[J]. Distributed Computing, 2015, 28(3): 171–187.

作者信息

彭长根(1963–), 贵州锦屏人, 博士, 教授, 博士生导师, 中国密码学会理事. 主要研究领域为密码学与信息安全、大数据隐私保护.
E-mail: peng_stud@163.com



田有亮(1983–), 贵州盘县人, 博士, 教授. 主要研究领域为博弈论、安全协议分析及分布式密码体制等.
E-mail: youliangtian@163.com

刘海(1984–), 贵州贵阳人, 博士研究生. 主要研究领域为隐私保护和理性密码协议.
E-mail: liuhai4757@163.com

丁红发(1988–), 博士研究生, 讲师. 主要研究领域为密码协议、数据安全.
E-mail: 605574103@qq.com