理性协议公平性进展研究

王伊蕾　李绍静　著

清华大学出版社

理性协议公平性进展研究

王伊蕾　李绍静　著

清华大学出版社
北京

内 容 简 介

本书全面介绍理性安全计算协议的研究背景、效用函数、纳什均衡、阶段博弈和扩展博弈等基本概念，并在此基础上分别介绍不同情况下理性安全协议中公平性的实现问题。本书主要借鉴重复博弈中促进参与者合作的 TFT(Tit-for-Tat)策略；另外考虑理性参与者在社会网络中的特性，还研究了声誉对理性协议公平性的影响；除此之外，还针对理性参与者依次采取行动的情况，探讨了满足可计算序贯均衡对公平性的影响。

全书共分 7 章：第 1 章介绍理性协议的研究背景和意义，国内外研究现状。第 2 章介绍一些关于博弈论的基本概念，这些基本概念是后续章节的基础。第 3 章介绍在理性安全两方计算中，如何通过引入 Tit-for-Tat 策略和声誉，使得参与者可以有效地遵守协议，最终实现公平性。第 4 章介绍理性安全两方计算中如何将声誉作为效用函数的一部分，继而重新定义效用函数，并在此基础上，重新对理性参与者分类。第 5 章介绍一种复杂的理性协议计算模型，提出一种更强的均衡概念，可以实现公平性。第 6 章和第 7 章对理性协议计算进行了总结和展望。

本书适合作为高等院校计算机、信息安全专业高年级本科生、研究生的教材，同时也可供对理性协议比较熟悉并且对多方安全计算协议有所了解的广大科技工作者和研究人员参考。

图书在版编目(CIP)数据

理性协议公平性进展研究/王伊蕾，李绍静著. —北京：清华大学出版社，2015
ISBN 978-7-302-40056-1

Ⅰ. ①理…　Ⅱ. ①王…　②李…　Ⅲ. ①密码术－研究　Ⅳ. ①TN918.3

中国版本图书馆 CIP 数据核字(2015)第 092699 号

责任编辑：白立军
封面设计：傅瑞学
责任校对：焦丽丽
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：7.5　　**字　　数**：122 千字
版　　次：2015 年 5 月第 1 版　　**印　　次**：2015 年 5 月第 1 次印刷
印　　数：1～400
定　　价：39.00 元

产品编号：064182-01

前 言

安全多方计算(Secure Multi-Party Computation,SMPC)是现代密码学的重要研究方向之一,它不但作为密码学基础的一部分,研究分布式情况下进行安全计算的基本原理和方法,还是很多应用型密码学协议的直接基础,例如合同签订、电子投票、电子拍卖和电子签名等。SMPC 可以描述为这样一个问题:多个相互独立的参与者拥有各自的私有输入,他们希望能够使用这些输入计算一个约定的函数。基本目标是,能够得到正确输出结果的同时不泄露自己私有输入的任何额外信息。假设存在一个可信第三方(Third Trusted Party,TTP)且每个参与者与 TTP 之间有一条完全保密的信道,各参与方通过保密信道将输入交给 TTP 计算这个约定的函数,TTP 结束计算后,将计算结果通过保密信道发送给每个参与者。至此多方计算完成并且可以实现基本目标,这就是安全多方计算的理想模型。

多方安全计算的目的是使现实环境下的协议实现理想模型的基本目标,这些目标可以用几个特性概括,即隐私性、正确性、输入独立性和输出公平性。输出公平性是指被腐败的参与者(Corrupted Parties)和诚实的参与者要么同时得到计算结果,要么同时得不到计算结果。Cleve(STOC 1986)证明了公平性在少数诚实参与者的情况下是不可能实现的,因此在传统 SMPC 中,尤其是在安全两方计算(Secure Two-Party Computation,STPC)中,公平性经常会被忽略。然而,公平性无论在 SMPC 还是在 STPC 中,都是非常重要的特性,尤其是在类似于合同签订和电子拍卖这样的现实协议中。最近很多文献给出了实现公平性的 SMPC 协议,例如,有的协议实现了非合作计算(Non-Cooperation Computation,NCC)函数的公平性,有的协议利用物理信封和投票箱实现公平性。另外很多较弱的公平性定义也相继提出来,例如部分公平性(Partial Fairness)。

理性安全多方计算(Rational Secure Multi-Party Computation,RSMPC)作为一种新方法,为实现 SMPC 协议的公平性提供一种新的思路。理性安全多方计算是指带有理性

参与者的安全多方计算。理性参与者与传统安全多方计算中参与者最大的不同之处在于他们是否遵守协议是根据他们的效用来决定的。这与传统 SMPC 中的诚实参与者、半诚实参与者和恶意敌手有很大的区别，因为这些参与者和敌手都不依效用来行动。理性参与者与 Aumann 和 Lindell(JOC 2010)中提到的隐蔽敌手有类似之处，他们都具有偏离协议的动机，而且都希望通过偏离协议获得各自的利益。RSMPC 的思想来源于博弈论(Game Theory)，因此在分析和证明 RSMPC 协议时，也采取博弈论中的证明思路。首先为每个参与者设定效用函数，这里效用函数的设定不是随意的，而是根据一些经典博弈进行改造的。例如绝大多数参与者的效用函数来源于囚徒困境(Prisoner's Dilemma)这一经典博弈。其次，设计协议，使协议的最终结果能够保证隐私性、正确性、输入独立性和输出公平性。最后，证明遵守协议是一个均衡，每个参与者都没有偏离协议的动机。也就是说，每个参与者只有遵守协议才能够最大化他们的效用，否则就会得到一个较低的效用。从博弈论的角度来看，RSMPC 协议的主要任务是如何设计好协议，使得每个参与者都与其他参与者合作而不是背叛其他参与者。如果合作(即遵守协议)对每一个参与者来说都是一个占优策略，那么公平性自然可以得到保证。

本书主要研究理性安全两方计算中公平性的实现问题，即如何促进参与者合作。

(1) 首先将重复囚徒困境博弈中为了促进合作而使用的 TFT(Tit-for-Tat)策略引入到 RSMPC 协议中来，因为在 RSMPC 中，为了实现公平性，必须保证参与者有合作的动机。利用 TFT 策略，理性参与者可以至少在协议的前几轮合作，获得足够的份额恢复出函数值。虽然在引入 TFT 策略时，声誉作为震慑理性参与者的一个因素被考虑到效用函数中，但是在效用函数的定义中并没有体现出来。

(2) 本书的另一个工作是将声誉作为效用函数定义的一部分，扩展了根据囚徒困境博弈定义的效用。根据新的效用函数，重新定义了理性参与者类型。给定合适的参数，本书证明了双方合作本身就是纳什均衡。因此 RSMPC 协议只需要一轮就可以完成份额的交换和函数值的恢复，这极大地提高了 RSMPC 协议的效率。

(3) 本书最后讨论了一个复杂但是更符合实际情况的 RSMPC 协议，即在不完全信息下，参与者有私有类型的情况。在这种情况下，理性参与者的效用函数不是以囚徒困境为基础，而是以连锁店博弈为基础，并且均衡类型也不是纳什均衡而是更强的序贯均衡。

给定合适参数，公平性在理性安全两方计算中也可以实现。

以上3个问题主要研究了如何有效地在两个参与者之间实现公平性，可以证明，通过不同的策略和效用函数定义，公平性能够在理性两方计算协议中实现。这与传统两方安全计算中关于公平性的结论不同，这种不同源于对理性参与者的界定不同，正是因为有了效用这一特性，使得一些传统两方安全计算中不可能的结论变为可能。

除了公平性，RSMPC中还有很多公开问题，例如，如何设计更合理的策略促使每个参与者合作，如何设定更加符合实际的效用函数，是否存在除囚徒困境以外的经典博弈适合作为RSMPC的基础，参与者除了效用以外是否还具有其他属性。理性安全协议中的公平性是多方安全计算致力解决的问题。本书是作者在密切跟踪该领域技术研究成果的基础上总结而成的，是一本全面论述理性协议公平性实现的著作，全书图文并茂，深入浅出，可读性强，并将理论与实践有机结合，以期为读者进一步学习、研究和应用打下基础。但是理性协议的公平性实现是一个复杂的问题，在本书撰写过程中参考了大量国内外有关理性协议的文献，直接引用的有数百篇。在此，向相关作者表示衷心的感谢。

本书的出版得到山东省优秀中青年科学家科研奖励基金(No. BS2014DX016)、国家青年科学基金(No. 61202475)、鲁东大学博士基金(No. LY2015033)和福建省网络安全与密码技术重点实验室(福建师范大学)开放课题(No. 15004)的资助。另外，本书的编写还得到鲁东大学邹海林教授、山东大学计算机科学与技术学院徐秋亮教授的大力支持，青岛农业大学的李绍静老师参与了本书的编写工作。在此对这些教授的鼓励和帮助表示衷心的感谢。

特别感谢清华大学出版社，感谢责任编辑及其他参与此书编辑工作的各位老师为本书顺利出版而付出的辛勤劳动。

由于作者水平有限，书中不足之处在所难免，恳请广大读者和同行批评指正。

王伊蕾

2015年3月于烟台

目 录

第1章 绪论

1.1 研究背景

博弈论和密码学协议都关注于相互不信任的参与者间如何通过“交互”来实现某个目标的研究。这两个研究领域，在很长一段时间里没有交集，不同的学者进行着独立的研究。然而最近，为了设计出更加实际的、互不信任的参与者间的协议，博弈论和密码学开始慢慢结合在一起。它们的结合主要体现在两个方面。

(1) 密码学协议应用到博弈论中。如果存在一个外部的可信方，称之为中介(mediator)，就有可能存在特定的均衡。这一方面的主要工作是：是否可以通过参与者间“交互”的协议替代这个外部的可信方，同时还保证这个特定的均衡成立。

(2) 博弈论应用到密码学协议中。通常情况下，密码学协议中的参与者假设为诚实的或者恶意的。诚实的参与者总是正确地执行协议，而恶意的参与者可能会采取任何恶意的行为偏离协议的执行。从博弈论的角度看，参与者既不是诚实的也不是恶意的，而是理性的(rational)。也就是说，理性的参与者仅关心如何最大化他的效用。可以从博弈论的角度解释参与者的类型，参与者没有义务必须诚实地参与协议(除非参与协议可以给他带来效用)，也没必要一定任意的偏离协议(有可能偏离协议会带来较低的效用)。因此这一方面的主要工作是：什么样的模型和协议适合这种理性的参与者，或者说理性参与者的加入可以解决传统密码学协议的什么问题。

安全多方计算是指若干互不信任的参与者，在不泄露自己输入的情况下，如何安全地计算一个给定的函数，使得每个参与者都可以得到计算结果。1982 年，姚期智先生在 FOCS'82 中提出“百万富翁”问题[1]，开创了安全两方计算领域研究的先河。1987 年 Goldriech、Micali 和 Wigderson 将安全计算由两方推广到多方，即安全多方计算[2]

(Secure Multi-Party Computation,SMPC)。两方计算需要满足的性质[3-9]总结如下。

① 隐私性(privacy):没有参与者可以获得他预期输出以外的任何信息。

② 正确性(correctness):每一个参与者都能够保证得到正确的输出。

③ 独立性(independence):被腐败的参与者(corrupted parties)的输入必须独立于诚实参与者的输入。

④ 公平性(fairness):被腐败的参与者必须接收到与诚实参与者相同的输出,即当诚实参与者得到正确输出时,被腐败的参与者也得到正确输出;当诚实参与者得到错误输出时,被腐败的参与者也得到错误的输出。

以上性质可以通过理想/现实(Ideal/Real)模型来刻画[2],如果一个协议能够满足以上几个性质,就说这个协议是安全的。

一个协议是安全的,如果它能够"模拟"一个"理想情景(ideal setting)",其中参与者将他们的输入发送给"可信第三方(trusted party)"。可信第三方可以在本地计算输出,并且把这些值发送给参与者。

这种方法的证明过程如下。考虑一个理想世界,存在一个可信第三方负责计算。参与者把他们的输入发送给可信第三方。当收到双方的输入后,可信第三方计算相应的函数值,最终把计算结果发送给参与者。在理想世界下,因为第三方被参与者们信任,因此满足上面的几个性质。现实世界下协议的安全性质,通过模拟理想世界下的计算得以保证。也就是说,假设存在一个恶意敌手,如果这个恶意敌手在现实世界下所做的破坏和在理想世界下所做的破坏相当,那么就说这个协议是安全的。

经过近 30 年的发展,安全多方计算至今已形成一个广受关注的学科方向。在讨论传统的安全多方计算时,需要涉及所有参与者和一个攻击者,攻击者具有一定的能力,例如他可以腐败几个参与者,获取他们本次执行的所有信息。在理想世界下,安全计算的正确性、保密性都能得到保证。如果一个协议在现实世界中得到的输入输出分布和在理想世界下得到的输入输出分布是计算不可区分的,就认为协议能够安全计算该函数。传统多方计算的敌手包括两种类型,一种是半诚实参与者(Semi-honest),另一种是恶意参与者(Malicious adversary)。非正式地说,半诚实参与者总是遵循协议,但是试图通过他们的中间结果,推导出其他参与者的输入信息。恶意参与者可以腐败其他的参与者,获得他们

的所有信息，被腐败的参与者可以按照任意的形式执行协议，例如，中途退出协议、替换自己真实的输入以及拒绝执行协议等。Aumann 和 Lindell[10] 提出了一种介于半诚实和恶意参与者之间的类型，称之为隐蔽攻击者(covert)。隐蔽参与者的提出具有很广泛的经济、政治和外交等应用背景。这种参与者的特点是：在一定的概率下，腐败其他参与者进行恶意的行为，否则不腐败其他参与者。理性参与者首先由 Halpern 和 Teague[11] 提出，他们发现参与者在动机不充分时并不总是分享他们的份额，这与传统的诚实参与者不同，这种参与者是否分享他们的份额取决于他们的效用(Utility)，因此称之为理性参与者。也就是说，参与者既不是完全诚实也不是任意恶意，而是理性地根据其效用决定是否分享份额。

1.2　本书的贡献

本书的贡献在于给予两方计算中理性参与者合作的动机，从而促进理性参与者正确按照协议执行，没有偏离协议的动机，最终保证公平性的实现。

(1) 为每个参与者设计合适的策略，使他们有合作的动机。

(2) 在保持其他因素不变的情况下，重新定义每个参与者的效用函数，理性参与者在新的效用函数定义下，只需要交互一轮就可以实现相互合作的结果。

(3) 在更加复杂的协议背景下，考虑参与者具有私有类型的情况，序贯均衡对理性多方计算的影响。

本书的两方计算协议包括两个阶段，第一个阶段是份额生成和分发，它的主要功能是分别接受参与者 p_1 和 p_2 的输入 x 和 y，计算函数 $f(x,y)$，生成两个随机数 s 和 t 满足 $s \oplus t = f(x,y)$[1]。生成 s 和 t 的 n 个 Shamir[12] 份额 $s_1, s_2, \cdots, s_n$ 和 $t_1, t_2, \cdots, t_n$，把这些份额分别发送给 p_1 和 p_2。第二轮是一个包括 n 轮的现实协议，其中 p_1 和 p_2 相继将自己的份额发送给对方，希望获得另一个随机数，最终获得输出值 $f(x,y)$。

本书的贡献包括以下 3 个方面。

(1) 从协议的描述可以看出，如果参与者双方都是诚实的，那么双方很容易得到输出，公平性得以实现。如果双方都是理性的，那么每个参与者在发送他自己份额的同时，

会计算自己的效用。如果发送份额可以增加自己的效用,那么就发送,否则就不发送。如果把发送看作是与对方合作,不发送是与对方不合作。这一情况与囚徒困境类似[13],因此可以使用囚徒困境中参与者的效用函数定义。从博弈论的角度看,公平性问题就转换为如何使相互合作成为均衡的问题,即如何找到一个相互合作的均衡。TFT(Tit-for-Tat)策略在囚徒困境博弈中,可以促进双方参与者的合作,因此本书将这一策略引入到理性两方计算协议中。如果理性参与者在执行协议时,均遵守 TFT 策略,那么可以实现协议的公平性。

(2) 然而 TFT 策略并不能从根本上解决理性两方协议需要常数轮交互的情况,为了降低参与者之间的交互,本书考虑了声誉(reputation)对效用函数的影响,并将其作为效用函数的一部分。此时理性参与者的效用函数与囚徒困境中定义的效用函数不同。在新效用函数的基础上,本书又重新定义了理性参与者的类型,证明了在不同条件下,不同类型参与者相互合作是 Nash 均衡。在新效用函数的定义下,满足给定条件,参与者在协议的第二阶段,只需要一轮就可以完成协议,并且双方参与者均采取合作的策略,这大大提高了协议的效率。

(3) 对于更加复杂的实际情况,例如,参与者有私有类型的情况,囚徒困境原有的效用函数和本书改进的效用函数都不能有效地描述参与者的效用。因此,本书根据连锁店博弈[13]中效用函数的定义,重新给出参与者的效用函数。同时,描述了理性两方计算的序贯结构,重新定义了参与者的行动空间、私有类型、协议执行历史等相关的概念。最后,为了在这种复杂情况下,依然保证协议的公平性,提出了可计算序贯均衡的概念,并且证明了,在满足给定条件下,可以通过可计算序贯均衡保证理性两方计算协议的公平性。

1.3 相关工作

1.3.1 传统多方计算下的公平性研究

公平性的研究最早可以追溯到 Even 和 Yacobi[14]的工作,他们非正式地证明了电子签名交换是不可能。随后 S. Even[15]等人又提出了基于 1-out-of-2 茫然传输子协议的随机协议,这些协议适用于合同签订[16,17]、挂号信、抛掷硬币[18-20]等领域。Cleve[21]给出这

种不可能性的严格证明，结果表明公平地投掷一枚硬币是不可能。Cleve 后续的工作[22]讨论了更强的攻击，这些攻击还依赖于可计算攻击能力的敌手。Boneh 和 Naor[23]给出了关于公平合同签订的下界，接近于 Cleve 等人提出[21]的下界。Garay 等人给出了一个通用的 SFE 协议[24]，这个协议在满足两个非常强的假设条件下，可以证明是公平的。这两个条件是：

① 恶意参与者的运行时间上限是事先已知的；

② 诚实参与者的计算允许偶尔超过这个上限。Luby 等人提出了一个相对较弱的公平性概念[25]。根据这个概念，公平协议具备以下两个特征：

① 每一个参与者正确地猜对自己输出的概率缓慢上升且接近于 1；

② 所有参与者猜对输出的概率确保与其他人相同。Gordon 等人[26]证明了某些函数性可以实现完全公平(complete fairness)。Moran 等人[27]解决了一个关于公平性的公开问题，他们证明 Cleve[21]基于掷币协议的下界是可以达到的。Beimel 等人[28]将 Moran 等人的工作[27]扩展到多方模型下，其中被腐败的参与者的个数不超过 2/3 诚实参与者的个数。即便如此，在使用标准密码假设的朴素模型下(plain model)，公平性仍难以实现。一些文献使用信息逐渐释放的方法在朴素模型下实现公平性[15,23,29-34]。同样地，参与者的输出也被随着时间增长而增长的噪音掩饰，并且参与者对输出值的确定性随着协议的执行不断增长[25,35,36]。Asokan 等人[37]提出了一个比较乐观的模型，这个模型允许使用一个可信第三方(Trusted Third Party, TTP)，但是只有当一个参与者是恶意的时，这个可信第三方才能够参与到协议中来。另外一种模型是由 Chen、Kudla 和 Paterson[38]提出的，Lindell[39]对此进行了扩展。在这个模型下，公平性是合法的(legally)而不是技术上可行的(technically enforceable)。合法性通过以下方法获得：诚实参与者将要么接收到他的输出，要么接收到一个其他参与者发来的核对信息，为了使这个核对信息失效，支付的一方将不得不泄露一些信息，而这些泄露的信息恰好让诚实参与者计算他们的输出。

Katz[40]提出了一个比完全公平弱的概念——部分公平(partial fairness)，如果存在一个理想世界的模拟器，他的输出不能以 ε 的优势与现实世界敌手的输出区分开来，就称一个协议可以实现函数性的 ε 部分公平。Gordon 等人[41,42]研究了朴素模型下的两方计算的部分公平，证明了在朴素模型下，部分公平也不能实现。Beimel 等人[28]研究了多方计

算的情形。Asharov 等人[43]提供了暗含公平掷币函数的完整描述，根据 Cleve[21]的工作，这些函数不能够实现公平性，除此之外，Asharov 等人给出了两种能够实现公平性的 Fail-stop 模型。Gordon 等人讨论了公平性函数性之间的规约问题[44]，他们证明没有一个短原语(short primitive)对于公平性是完全的(complete)，他们基于参与者输入规模建立了一个公平性层次(hierarchy)。但是这种层次划分方法对于其他安全计算收效甚微，还有其他的划分层次的方法，例如，根据调用原语的个数划分层次[45,46]，根据私有性标准划分层次[47]以及根据可否规约到其他原语[48]来划分层次[49]。

Agrawal 和 Prabhakaran[50]研究了很多经典安全计算中公平性的实现问题以及它们之间的联系，系统地研究了公平抽样问题(例如，无输入的函数性)。主要结论包括以下几方面。

(1) 公平交换不能通过 r 轮协议规约到公平掷币问题，除非允许出错的概率为 $\Omega\left(\frac{1}{r}\right)$。

(2) 带有有理数概率(rational probability)的有限公平抽样问题都可以规约到公平掷币问题和不公平的两方计算问题。因此针对这类问题，公平掷币是完全的。

(3) 只有那些建立在没有任何公平预设过程的公平协议基础上的公平抽样问题是平凡问题，也就是说，两个参与者可以独立地抽取他们的输出。其他的都有 $\Omega\left(\frac{1}{r}\right)$的错误概率，接近于 Moran 等人[27]中公平抽样的上限。

(4) 使用光谱图理论(spectral graph theory)证明无法将带有公共信息[51-54](common information)的抽样问题规约到没有公共信息的抽样问题(例如，“噪声”掷币会以很小的概率产生不一致)。

最近，Asharov、Lidell 和 Zarosim[55]在声誉系统下研究了多方计算的公平性和有效性。在声誉系统中，一个实体集合中每个实体都有一个相应的值，这些值是对每个实体可靠性的一个评估[56]。声誉系统应用在很多领域，例如，电子商务系统和对等网络系统[57]。在多方计算协议中，这些评估可以看作是每个实体诚实地执行协议的概率。Asharov、Lidell 和 Zarosim 讨论了能够利用声誉系统构造公平有效的多方计算协议。他们的结论包括以下几方面。

① 提出一个基于声誉系统的多方计算模型，并且给出在这种模型下正式的安全定义。

② 从技术角度讨论了基于声誉系统的多方计算问题，研究了在什么条件下可以实现公平性。

③ 证明了当声誉大于 1/2 的参与者个数是关于安全参数 n 的超对数级函数时，就存在完全安全的多方计算协议。

1.3.2　理性多方计算下的公平性研究

Halpern 和 Teague[11] 理性多方计算协议（简称 HT 协议）建立在理性秘密分享基础之上，他们首先证明了没有确定性的策略能够通过重复弱劣策略删除[58]，因此不存在一个确定性的理性多方计算协议。随后他们给出了一个随机策略，证明了该策略可以通过重复弱劣策略删除，在此基础上构造了一个理性多方安全计算协议。但是该协议只适合于多于两个参与者的情况，并且协议的执行依赖于同步通信信道，同时该协议对多于 3 个参与者合谋的情况，不具备健壮性。因此他们提出许多开放性问题。

（1）HT 协议的结论在同步通信信道下成立，在异步通信信道中是否成立。

（2）在不存在安全第三方的情况下，安全多方计算是否可以进行。

（3）HT 协议的结论集中在纳什均衡和重复弱劣策略删除，没有涉及其他更强的均衡概念。

（4）HT 协议结论依赖于参与者都知道共同的效用函数，如果去掉这一条件，结果如何。

针对 HT 协议提出的开放问题，许多工作给出了很多在不同效用函数定义和不同通信模型下的解决方案[59-70]。理性秘密分享机制可以看成是一个理性安全计算协议。Katz[62] 讨论了博弈论和密码学协议之间的联系，Katz 指出博弈论和密码学协议均研究相互不信任的参与者之间交互的问题，这两个看似不相关的领域可以相互渗透。他指出了两个研究方向。

（1）在博弈论中应用密码学协议。博弈论中的一些均衡可以通过设置可信中介（trusted mediator）来获得，这一研究方向的主要问题是：这个可信中介可否通过由参与

者自行执行的分布式密码学协议来代替。

(2) 在密码学协议中应用博弈论,这也是理性多方安全计算主要研究的一个方向。传统密码学模型假设一些参与者诚实地执行协议,一些参与者恶意地破坏协议。而博弈论模型将这些参与者看作是利己主义者(self-interest),即理性(rational)。这一研究方向的主要问题是:如何在博弈论的情境下设计和研究有实际意义的密码学协议。

目前大部分理性秘密分享机制和理性多方计算协议讨论的是在理性参与者的情况下,如何实现公平性问题[11,26,1,71-73]。另外还有一些文献[74-80]为了实现公平性,使用了一些比较强的通信工具,如物理信封和投票箱等。

最近一些关于理性秘密分享和理性多方计算的混合模型也相继提出。S. J. Ong等[81]提出一个少数诚实参与者和多数理性参与者的理性秘密分享机制,可以有效地实现公平性。Lysyanskaya 和 Triandopoulos[82]首次在 UC(Universal Composable)模型[83]下讨论了同时具有理性参与者和恶意参与者的混合模型下的理性多方计算协议。Lysyanskaya 等人研究的理性参与者的行为类似于诚实参与者[82],而且他们讨论的函数是非合作计算(Non-Cooperation Computation,NCC)函数。他们给出了一个协议允许理性参与者模拟可信第三方,联合计算一个函数,满足以下条件。

(1) 假设每一个理性参与者倾向于他自己得到计算结果,而其他参与者得不到计算结果。

(2) 理性参与者能够通过以下方式得到保护,即如果敌手能够控制超过$\left[\frac{n}{2}\right]-2$个参与者,敌手要么只能使得所有理性参与者退出协议,要么只能得到和他们输入输出同分布的信息。Lysyanskaya 和 Triandopoulos 讨论了可计算 t-安全的函数优先协议(Computationally t-secure preferred protocol for function)。

Abraham 等人[63]讨论了存在参与者合谋情况下的理性安全多方计算协议。与 HT 协议相比,他们的方案优点有 3 个。

(1) HT 协议只讨论了存在一个参与者合谋的情况,而 Abraham 讨论了不超过 $t-1$ 个参与者合谋的情况,并在此基础上提出了抗 $t-1$ 合谋的纳什均衡。

(2) HT 协议的方案不适用于只有两个参与者的情况,而 Abraham 的方案对于两个