机制设计理论及其在计算机网络协议设计中的应用研究*)

游文霞[1,2] 王先甲[1] 冯 霞[2] 文俊浩[3]

(武汉大学系统工程研究所 武汉 430072)[1] (武汉大学工程及计算机图学中心 武汉 430072)[2]

(重庆大学软件学院 重庆 400030)[3]

摘 要 计算机网络协议的设计一般假设参与者是完全服从的。对于域间路由、IP 多播、P2P 文件共享等问题,这个假设并不成立。这些问题中各参与者都是自治的主体,其行为是自利的,以追求自身的利益最大化为目标。这给网络协议的设计带来挑战。机制设计理论用于设计多主体之间的博弈规则,以获得期望的结果。该理论为计算机网络中出现的这类问题的协议设计提供了方向。本文首先介绍了机制设计的基本概念,并以路由为例说明了其在计算机网络中的具体应用。传统的机制设计理论是微观经济学和博弈论的分支,在具体应用到计算机网络中需要处理很多新的问题,例如计算复杂性、隐私、分布式计算等。文章对近年来该领域的研究成果做了总结,并指出了未来的研究方向。

关键词 机制设计,计算机网络,VCG 机制,激励相容,隐私保护

Theory of Mechanism Design and its Application in the Field of Protocol Design of Computer Networks

YOU Wen-Xia[1,2] WANG Xian-Jia[1] FENG Xia[2] WEN Jun-Hao[3]

(System Engineering Institute, Wuhan University, Wuhan 430072)[1]

(Center of Engineering and Graphics, Wuhan University, Wuhan 430072)[2]

(Faculty of Software Engineering, Chongqing University, Chongqing 400030)[3]

Abstract Agents are generally supposed to be obedient in designing the protocols of computer networks. However this supposition does not come into existence in such problems as domain routing, IP Multicast, P2P file sharing etc. The agents in these scenes are autonomous; their actions are selfish and their expected objects are to maximize their own benefits. New challenges appear in designing the protocols of computer networks. The theory of mechanism design aims at designing game rules of multi-agents, and obtaining desired outcomes. This theory gives new direction for these problems. The paper firstly introduces basic concepts in the theory of mechanism design, and illustrates the application of this theory, for example network routing. Traditional theory of mechanism design is the branches of microeconomics and game theory. Many questions come forth when applying the protocol design of computer networks, such as computation complex, privacy, distributed computation and so on. The paper summarizes the research results recently, and points out the future research directions.

Keywords Mechanism design, Computer network, VCG mechanism, Incentive compatible, Privacy reversing

1 引言

计算机网络是用通信网络连接起来的计算机集合体,在网络协议的作用下完成资源共享和信息交流。网络协议定义了通信双方传递信息的语法、语义和时序,来完成诸如流量控制、差错控制、路由、寻址等功能[1]。网络协议设计一般假设协议参与者是完全服从的。网络参与各方协调一致,按照协议的规定完成特定的任务。但计算机网络中的有些问题,这个假设就不成立。例如域间路由,不同的域属于不同的所有者,各个域可以自主地决定来自其他域的 IP 包通过与否[13]。网格计算中的任务分配[22]也是一个例子。由于资源是属于不同的所有者的,他们可以自主地决定是否使用资源来执行任务。这类问题的共同特点是:网络协议参与者是理性的(Rational)。每个参与者均是独立的主体,有自身的利益,并根据自身利益出发决定其行为。而传统的网络协议设计中将网络参与者假设为服从的(Obedient)。因此,不能期望理性主体忠实地服从已经设计好的协议,最合理的是希望每个理性主体试图利用设计好的协议采取行动来满足自身利益,同时又能达到设计者的目标。这样一种协议必须针对这种行为提前进行设计[7]。计算机网络中出现的这类问题给网络协议设计带来挑战。

站在系统的角度,计算机网络理性主体自主决策,采取行动可以看作是一个博弈的过程。对应的计算机网络协议则是博弈的规则。这类问题的协议设计就变成了博弈规则的制定问题。这正是机制设计理论所要解决的。国外学者已经将机制设计理论应用到了域间路由[13~16]、IP 多播[17~19]、Ad hoc 网络[20,21]、网格计算[22,23]、P2P 文件共享[24~28]、拥塞控制[29]、电子拍卖[30]、网络负载平衡[31]、资源分配[32,33]等领域,并对机制实施过程中的计算复杂性[7,34~36],隐私保护[37~44],分布式计算[45~48]以及其他问题[49~55]进行了研究,并取得了相当多的成果。这方面的工作还在继续。国内却鲜见该方面的研究报告。本文介绍了机制设计理论的基本框架,并以路由为

*)国家自然科学基金资助(项目编号:60574071)。**游文霞** 博士研究生,主要研究方向:决策论、博弈论,及其在计算机领域中的应用研究。

例，说明了机制设计的基本应用；总结了国外在该领域的研究热点及成果；并指出了未来研究方向。

2 机制设计理论

机制设计理论又叫执行理论(Implementation Theory)，是博弈论和微观经济学的一个分支，用来设计博弈规则(机制)，以获得期望的结果。机制使得参与者有激励按照设计者希望的行为动作，从而实现这个结果[2,3]。机制设计理论的问题最初是来源于微观经济学的，但是采用的工具是博弈论[7]。和传统的博弈论分析方法不同。机制设计是设计规则，传统的博弈论是在规则存在的前提下分析博弈的均衡解。机制设计理论已成为现代经济学的核心理论，被广泛应用于拍卖、垄断性商品定价、最优税收等多个领域。多位经济学家，如 Mirrless 和 Vickrey(1996)，Akerlof，Spence 和 Stigliz (2001)等，由于其在机制设计理论的杰出贡献而获得诺贝尔经济学奖。本节先介绍机制设计理论的框架；接着定义常用术语并描述机制设计理论中重要的显示原理；最后描述机制设计理论最重要的成果：VCG 机制。有关机制设计理论更详细的介绍，请参阅文[7～9]。

2.1 机制设计理论框架

图 1 是机制设计理论的框架图。

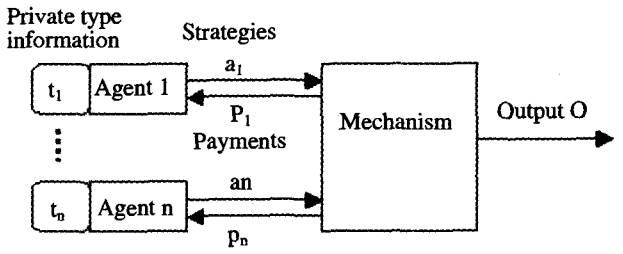

图 1 机制设计理论框架

设机制有 n 个参与人(agent)，每个参与人都有自己的私有信息 $t_i \in T_i (i=1,2,\cdots,n)$，称为参与人的类型。$T_i$ 是参与人 i 的类型空间。T_i 是公共知识，即所有参与人都知道 T_i，所有参与人都知道所有参与人知道 T_i，但是 t_i 只有参与人 i 知晓。参与人参与机制，会采取策略(Strategy)。对于每个参与人，策略是其类型的函数，即：$a_i=a_i(t_i)(a_i \in A_i, t_i \in T_i)$。

机制中每个参与人都选择一个策略，这样就构成了一个策略组合 $a=(a_1,a_2,\cdots,a_n)$。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，给所有参与人以转移支付(payment) $p_i=p_i(a)$，$(i=1,2,\cdots,n)$。记 $p=(p_1(a),p_2(a),\cdots,p_n(a))(p \subseteq R^n)$，称为机制的支付规则。分配规则描述了机制选择的分配结果，而支付规则用于激励自利的参与人在最大化自己效用的同时，采取系统认为的正确行为。分配规则和支付规则是一个机制的两个组成方面。

每个参与人对不同的输出结果具有不同的偏好，记为 $v_i(O,t_i)$。它是类型为 t_i 的参与人对可行结果 o 满意程度的数值化度量，称之为参与人 i 对结果 o 的估值(value)。在机制确定的分配规则和支付规则下，参与人获得的效用(Utility)通常都假设是拟线性的，即 $u_i(o,t_i)=v_i(t_i,\tilde{o})-p_i$。由于效用依赖于参与人的私有类型信息 t_i，因此每个参与人的效用机制并不知晓。如果参与人的目的就是最大化其效用 u_i，则称这样的参与人是理性的。

2.2 形式化描述

定义 1(社会选择函数) 社会选择函数定义为 $F: T_1 \times T_2 \times \cdots \times T_n \to O$。即根据给定参与人的类型 $t=(t_1,t_2,\cdots,t_n)$，选择一个机制的结果 $F(t)=o$。

社会选择函数 $F: T_1 \times T_2 \times \cdots \times T_n \to O$ 定义了机制设计者所希望达到的系统的全局目标，它是机制进行决策的依据。

定义 2(机制) 给定 n 个参与人的集合 N，各参与人类型空间为 $T_i(i=1,2,\cdots,n)$，策略空间为 $A_i(i=1,2,\cdots,n)$，可行的结果集合 O，机制被定义为一个二元组(o,p)。其中，$o: A_1 \times A_2 \times \cdots \times A_n \to O$ 为机制的分配规则，说明了机制需要执行的社会选择函数。

$(p=(p_1,p_2,\cdots,p_n)$

$(p_i: A_1 \times A_2 \times \cdots \times A_n \to R)$是机制的支付向量，定义了机制的支付规则。

机制设计问题就是在参与者拥有私有类型信息时，通过确定合理的支付，来激励参与者采取理性的行动，达到机制所要求由社会选择函数所制定的目标。

定义 3(机制的解) 给定机制，参与者进行博弈满足均衡的策略组合称为机制的解。均衡可以是占优策略均衡(Dominant strategy Equilibrium)或是贝叶斯纳希均衡(Bayesian Nash Equilibrium)。

由于参与人的策略是其私有类型的函数，给机制设计问题带来难度，但是，著名的显示原理将参与人的策略空间变换为参与人的类型空间，从而简化了机制的设计。

定理 1(显示原理) 给定任何一个机制和该机制下的任何一个均衡策略，都存在一个直接机制，使得在这个机制下：

- 参与者真实地报告自己的估值是一个弱占优均衡策略；
- 配置结果(分配和支付)和给定的原始机制的均衡所得的结果是相同的。

定义 4(直接显示机制) 在一个直接显示机制中，参与人的策略就是根据自己的真实类型 t_i 向机制报告一个类型 t_i'，$t_i'=a_i(t_i)$。如果参与人报告的是关于自己类型的真实信息，即 $t_i=a_i(t_i)$，则该显示机制是真实的(truth revealing)。

梅耶森的显示原理指出，任何一个机制所能达到的配置结果都可以通过一个(说实话的)直接显示机制实现，因此，机制的设计者只需考虑直接机制的设计。

定义 5(策略一致的机制) 在一个直接显示机制中，如果说真话是一个占优的策略均衡(dominant-strategy equilibrium)，那么该机制是策略一致的(strategy-proof)。

策略一致的机制也是占优策略的激励相容(Incentive Compatible)机制。激励相容的机制是指在均衡时，所有的参与者都真实地报告自己类型信息的机制。换言之，一个直接显示机制是真实的，则参与人在宣布自己类型的时候是激励相容的。策略一致是机制的一个非常重要的属性，它暗示在任何情况下，任何代理人都不能从谎报其类型中获益。因此，满足策略一致属性的机制得到了广泛的关注。

2.3 VCG 机制

VCG 机制首先是由 Vickrey 提出的第二价格拍卖机制构成的[4]，后来由 Clarkes 和 Groves 进一步进行了扩展[5,6]，因而，VCG 机制又简称为 Groves 机制。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。不仅如此，它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。因此，它是目前研究最多应用最广的一种机制。

定义 6(VCG 机制) VCG 机制是一类拟线性效用环境下的策略一致的机制：

(1)分配规则

$o(t_1,t_2,\cdots,t_n)=\arg\max_{o\in O}\sum_i v_i(t_i,o)$；

(2)支付规则

$p_i(t_1,t_2,\cdots,t_n)=\sum_{j\neq i}v_j(t_j,o^*-i)-\sum_{j\neq i}v_j(t_j,o^*)$。

$o^*(t)=\arg\max_{o\in O}\sum_i v_i(t_i,o),o-i^*(t)$

$=\arg\max_{o\in O}\sum_{j\neq i}v_j(t_j,o),(t_1,t_2,\cdots,t_n)=t$。

分配规则的定义表明 VCG 机制实现的社会选择函数是社会福利函数，该函数使得各参与人的估值之和最大。

支付规则右式第一项表示在参与者 i 不参与机制的情况下，机制获得期望结果 o^*-i 时，所有参与者的估值之和；第二项表示在期望结果 o^* 下，除了参与者 i 外的估值之和。可以看出，VCG 机制下的每个参与者的支付和其估值是无关的。代理没有激励撒谎，因为撒谎不会使得他的支付增加。

在 VCG 机制下，每个参与人最终获得的效用是：

$u_i(t)=\sum_j v_j(t_j,o^*)-\sum_{j\neq i}v_j(t_j,o^*-i)$该式表示参与者 i 的效用等于其作为一个整体带给机制的增加值。

3 路由应用

机制设计理论已经在计算机网络的多个领域得到了广泛的应用[13~33]，这些应用可以分为三类[8]：路由、资源分配和网上电子贸易。路由包括了域间路由，Ad Hoc 网络路由和 IP 多播等。资源分配含网格资源分配，P2P 文件共享，网络拥塞控制(实际上是带宽分配)，网络负载平衡等。而网上电子贸易最主要的形式是电子拍卖。这些问题的参与者都是理性的，希望个人的效用最大。为完成路由等应用，需要设计合理的协议(机制)，激励参与者采取合理的行动，从而实现协议(机制)所要求达到的目标。

网络路由是近年来机制设计理论在计算机网络应用研究的一个热点[13~21]。本节以单播路由为例，说明如何设计一个机制，使得在各个理性的参与者之间，能够保证路由可以有效地进行。

网络定义为一个带权图$\langle V,E,w\rangle$，V 是图顶点的集合，E 是图的边，w 是各边的权，代表传输的代价。同时给定一个源顶点 s 和目标顶点 t。希望找到一个机制，机制实施的结果是使得从 s 到 t 的路径是最短路径(即传输代价最小)。

定义不同的边属于不同的参与者，每个参与者只有一条边。每个参与者传输一个包需要付出代价，该代价为正值。而这个代价只有参与者自己知道，属于私有信息，即参与者的类型。机制的输出结果集 $O=\{$所有从 s 到 t 的可能路径$\}$。若一条包含边 e 的路径被选中，则参与者的估值为 $-w_e$，否则为 0。如果路由结果是从 s 到 t 的最小路径，则机制使得社会福利函数得到最大值(总的传输的代价最小)[7]。

由于网络路由的目标是代价最小，即机制的社会选择函数是社会福利函数，因此，利用 VCG 机制，可以解决该问题。VCG 机制是策略一致的机制，这样每个参与者(边)向机制汇报的权值都是真实的，并且在汇报真实权值会使得该参与者的效用最大。依据 VCG 机制的定义，对于图$\langle V,E,w\rangle$的每条边(参与者)，定义的支付如下：

(1)如该边不包含在最短路径内，则 $p(e)=0$。

(2)如该边包含在最短路径内，则 $p(e)=\bar{W}_e-W_{-e}$。

W_{-e}是不包含 e 的最小路径的各条边的权的和；$\bar{W}_e$ 而是包含 e 的最小路径的各条边的权的和，但除去边 e 的权。

在该支付之下，最短路径上的每条边的效用 $u(e)=-w_e-(\bar{W}_e-W_{-e})=W_{-e}-W_e$。即在边 e 不参与路由下的最短路径权重之和，减去边 e 参与路由下的最短路径权重之和。

下面以一个具体的图为例来说明。

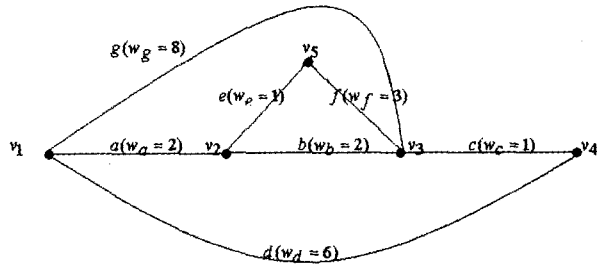

图 2 路由示意图

源顶点是 v_1，目标顶点是 v_4。最短路径是 abc，该路径的传输代价是 $w_a+w_b+w_c=5$。根据以上定义，边 d、e、f、g 的支付均为 0，因为它们都不在最短路径上。如果边 a 不在图中，则 s 从到 t 的最短路径是 d，相应的传输代价是 $w_d=6$。对于边 a 而言，其支付 $p_a=(w_b+w_c)-w_d=(2+1)-6=-3$，效用为 $u_a=v_a-p_a=-2-(-3)=1$。注意，这儿给参与者 a(边)的支付为 -3，表示的是机制需要给参与者值为 3 的支付，这样代理 a(边)在付出代价 2 时，参与这个机制最后获得的效用是 1。依次类推，

$p_b=(2+1)-6=-3,u_b=-2-(-3)=1$；

$p_c=(2+2)-6=-2,u_b=-1-(-2)=1$。

在以上机制定义的支付规则下，每个参与者就有激励汇报其真实的传输代价，这样参与者会获得最大效用，同时，机制的最终目标也得以实现。

4 问题与对策

机制设计理论在计算机网络的应用，实际上是将微观经济学理论和博弈论应用到计算机科学中。传统的机制设计，假设参与者是完全理性的；参与者和机制的计算能力是无限的；参与者需要向机制这个"中心"汇报其私有信息；机制实施中的通信是无代价的，可靠的；机制中参与者的数量是固定的。但在网络这个计算平台上，这些假设并不是都成立[10,12]。应用机制设计还需要处理众多的问题。

(1)计算复杂性

机制设计应用在网络计算平台上时，机制设计者和参与者都只有有限的计算能力。众多学者对机制设计中的计算复杂性开展了研究。J. Hershberger 在文[14]中针对最短路由中采用 VCG 机制确定支付的计算复杂性问题，提出了一种新的解决方法。当路由图有 n 个节点，m 条边，使用 Dijkstra 算法计算每条最短路径的计算复杂性是 $O(n\log n+m)$。从源节点到目标节点最多有 $n-1$ 条边，因此对所有边计算支付原始的计算代价是 $O(n^2\log n+nm)$。采用新的算法后，计算复杂性变为 $O(m+n\log n)$。A. Archerr 在文[15]中指出采用 VCG 机制给最小代价路径上的每条边的转移支付是很高的。在两大类图里，没有机制能够在说真话的基础上不付出高昂的代价。J. Feigenbaum 在文[16]中研究了基于策略的

路由，这更加符合域间路由的实际情况。文章提出了一个策略一致的，多项式时间的机制。

V. Conitzer 在文[34]中指出，对于确定性的机制设计，对于占优策略实施和贝叶斯纳希实施，机制设计是 NP 难的。如果采用随机算法，则机制设计计算可行。N. Nisan 在文[7]中指出任务分配问题的机制设计是一个 NP 难问题。文章提出采用近似算法来实现多项式时间的计算。Noam. Nisan 又在文[35]中说明了 VCG 机制在处理诸如组合拍卖的时候时，计算上不可行。如果采用近似算法，则机制在说真话的属性上不满足。为了解决这个问题，提出可行的说真话(feasible truthful)的概念，利用主体有限的计算能力，来实现可行的说真话。文[11]和文[36]还给出了单参数和多参数参与者机制设计问题的近似算法。

(2)代理的隐私

机制采取激励鼓励参与者向机制这个中心汇报私有信息，会引起个人隐私的泄漏。J. Feigenbaum 和 N. Nisan 最早在文[37]中提出了机制设计中的隐私问题。F. Brandt 和 T. Sandholm. 在文[38～41]对于无条件的隐私(也称信息论意义上的隐私)进行了研究。但是隐私研究最主要的工具是密码学上的安全多方计算协议。该协议要解决的问题是：多人进行一个函数的计算，每人有一个输入；协议的结果是每人除了知道函数的结果和自己的输入外，不再知晓其他的信息。安全多方计算在隐私保护的查询、隐私保护的数据挖掘方面已经得到应用，现在已经应用到机制设计的隐私保护问题中。文[42～44]提供了安全多方计算的原理及其在机制设计中的应用。

(3)分布式计算

机制设计理论应用到计算机网络，实际上就是应用到一个分布式的计算环境中。为了尽量减少机制这个默认“中心”的计算负荷，以及保护参与者的隐私，J. Feigenbaum、C. H. Papadimitriou 和 S. Shenker 在文[17]中首先提出了分布式算法机制设计的概念，并将其应用到 IP 多播问题中。文[13]给出了域间路由问题基于 BGP 协议的最短路径算法，提出并实现了分布式的算法。文[45]是分布式算法机制设计的经典文章，文章介绍了分布式算法机制设计基础以及取得的研究成果，并提出了未来有待研究的 22 个问题。文[46]是分布式算法机制设计的一篇博士论文，对于分布式算法的近似算法、分布式算法和已经存在协议的兼容以及 NP 难问题进行了研究。

D. Parkes 在文[47]研究了 VCG 机制的实现，提出了分布式计算的几个原则：基于分区；基于信息揭示和基于冗余。文[48]研究了分布式激励兼容的机制，指出机制实现过程中各参与者会相互分发信息，共同实现机制要求的目标。

(4)其他问题

机制在执行过程中存在不确定性。文[49]针对任务分配，指出参与者的私有信息不仅仅是完成任务的代价，还有失败的概率。文章提出了容错的机制设计，并给出了该机制正反两方面的结论。文[50]对容错机制设计做了进一步说明。

机制设计问题中，各参与者之间的信任是需要重点考虑的问题。文[51～53]研究了机制设计中的信任。

包含理性参与者的分布式系统中，证明参与者算法的诚实或是不诚实是一个令人期待的目标。文[54]形式化了理性参与者算法的诚实性，文[55]阐述 P2P 文件共享系统中的 BT 软件的诚实性，指出了验证不诚实的方法。

文[56]将机制设计看作多目标优化问题，并利用遗传算法来解决双边拍卖问题。文[57]和[58]研究了自动产生的机制，能够针对不同的参与人数，参与人不同的类型信息以及社会选择函数，自动产生符合要求的机制。文[59]研究了机制设计中的通信复杂性。文[60]对于参与者对于各种不同的社会选择结果的偏好不完全知晓的情况进行了分析，指出参与者需要合作才能揭示各自的偏好，从而知道估值。

展望 机制设计理论在计算机网络中的应用研究已经取得了大量的成果。但是仍然存在一些问题，需要综合计算机科学、博弈论和系统科学来解决。

- 设计出既有较低的计算复杂性，又有激励兼容性质的机制仍是一个有待继续研究的问题；
- 机制的解一般考虑的是静态博弈，对于动态博弈意义下的解需要开展研究；
- 机制的解一般考虑的是非合作博弈，对于合作博弈意义下的解需要开展研究；
- 机制中参与人可能会合谋，防范合谋是一个研究方向；
- 参与人的私有类型信息为向量或是更复杂的情况，如何设计机制；
- 当计算机网络中各参与者既包括理性参与者，又含服从参与者和攻击者时，如何设计机制；
- 针对具体的问题开展机制设计的研究，使得机制符合应用的实际。

正如伯克利大学 C. H. Papadimitriou 教授所预言，传统的计算平台，正从冯·诺依曼体系结构的单机，转换到 Internet 平台。在这个大平台之上，机制设计理论将大有用武之地。冯·诺依曼既是一位计算机科学家，同时又是一位博弈论的开创者。多年来，计算机科学和博弈论沿着两条不同的方向前进，伴随 Internet 的在全球的普及，两者终于开始结合了。本文愿抛转引玉，促进国内在该领域的研究。

参 考 文 献

1 谢希仁. 计算机网络教程. 北京：人民邮电出版社，2002
2 张维迎. 博弈论与信息经济学. 上海：上海三联书店，1996
3 张守一. 现代经济对策论. 北京：高等教育出版社，1998
4 Vickrey W. Counter speculation, auctions and competitive sealed tenders. Journal of Finance, 1961. 8～37
5 Clarke E H. Multipart pricing of public goods. Public Choice, 1971. 17～33
6 Groves T. Incentives in teams. Econometrica, 1973. 617～631
7 Nisan N, Rosen A. Algorithmic mechanism design. Games and Economic Behavior, 2001, 35: 166～196
8 Nisan N. Algorithms for Selfish Agents. In: Proceedings of the Symposium on Theoretical Aspects of Computer Science, LNCS 1563, Springer, Berlin, 1～17
9 Parkes D C. Iterative Combinatorial Auctions: Achieving Economic and Computational Efficiency (Chapter 2): [PhD thesis]. University of Pennsylvania, May 2001. http://www.eecs.harvard.edu/~parkes/pubs/ch2.ps
10 Dash R K, Parkes D C, Jennings N R. Computational mechanism design: A call to arms. IEEE Intelligent Systems, 2003, 18(6): 40～47
11 Archer A, Tardos E. Truthful mechanism for one-parameter agents. In: Proc. of the 42nd IEEE Symp. on Foundations of Computer Science, October 2001. 482～491
12 Sandholm T. Making markets and democracy work: A story of incentives and computing. In: Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI), 2003. 1649～1671
13 Feigenbaum J, Papadimitriou C, Sami R, Shenker S. A BGP-

based Mechanism for Lowest-Cost Routing. In: Proceedings of the 21st Symposium on Principles of Distributed Computing, ACM Press, New York, 2002. 173～182
14 Hershberger J, Suri S. Vickrey prices and shortest paths: What is an edge worth? In: Proceedings of the 42nd Symposium on the Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, 2002. 129～140
15 Archer A, Tardos E. Frugal path mechanisms. In: Proceedings of 13th ACM-SIAM Symposium on Discrete Algorithms (SODA'02), ACM Press/SIAM, New York, 2002. 991～999
16 Feigenbaum J, Sami R, Shenker S. Mechanism design for policy routing. In: Proceedings. of the 23rd ACM Symposium on Principles of Distributed Computing (PODC'04), 2004. 11～20
17 Feigenbaum J, Papadimitriou C, Sami R, Shenker S. Sharing the cost of multicast transmissions. In: Proc. 32nd Annu. ACM Symp. Theory Comput., May 2000. 218～227
18 WeiZhao, Wang Xiang-Yang, Li Zheng Suny, Yu Wang. Design Multicast Protocols for Non-Cooperative Networks. In: Proceedings of the 24th Annual Joint Conference of the IEEE Communication Society (INFOCOM 2005)
19 Yuen S, Li Baochun. Strategyproof Mechanisms for Dynamic Multicast Tree Formation in Overlay Networks. In: Proceedings of IEEE INFOCOM 2005, Miami, Florida, March 2005
20 Anderegg L, Eidenbenz S. Ad hoc-vcg: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In ACM MobiCom, 2003. 245～259
21 Wang W, Li X Y. Truthful low-cost unicast in selfish wireless networks. In: Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks, IPDPS 2004
22 He Linli. Designing Computational Economic-Based Distributed Resource and Task Allocation Mechanisms for Self-Interested Agents in Computational Grids: [PhD thesis]. Deborah Lord Department of Computer Science, Texas A&M University, Texas, USA, May 2005
23 Grosu D. AGORA: Architecture for Strategy proof Computing in Grids. In: Proceedings of the Third International Symposium on Parallel and Distributed Computing/Third International Workshop on Algorithms, Models and Tools for Parallel Computing on Heterogeneous Networks (ISPDC/HeteroPar'04) Jul. 2004
24 Feldman M, Lai K, Stoica I, Chuang J. Robust incentive techniques for peer-to-peer networks. In: Proc. of the 5th ACM Conference of Electronic commerce New York, NY, USA, May 2004
25 Ma R T, Lee C M, Lui J C, Yau D K. Incentive p2p networks: a protocol to encourage information sharing and contribution. SIGMETRICS Performance Evaluation Review, 2003, 31(2): 23～25
26 Ma R T B, Lee S C M, Lui J C S, Yau D K Y. A game theoretic approach to provide incentive and service differentiation in p2p networks. In: Proc. of the joint international conference on Measurement and modeling of computer systems, New York, NY, 2004. 189～198
27 Shneidman J, Parkes D. Rationality and self-interest in peer to peer networks. In: Int. Workshop on Peer-to-Peer Systems (IPTPS), 2003
28 Ma R, Lee S, Lui J, Yau D. Incentive P2P Networks: Theory and implementation: [Technical report of Dept. of CSE]. Chinese University of Hong Kong
29 Shu Jun, Varaiya P. Mechanism Design for Networking Research. Information Systems Frontiers, 2003, 5(1): 29～37
30 Shoham Y, Tennenholtz M. Behavioral mechanism design as an online marketing tool. In: Proceedings of the 5th ACM Conference of Electronic Commerce New York, NY, USA, May 2004
31 Grosu D, Chronopoulos A T. Algorithmic mechanism design for load balancing in distributed systems. In: Proc. of the 4th IEEE Intl. Conf. on Cluster Computing, September 2002. 445～450
32 Porter R. Mechanism design for online real-time scheduling. In: Proceedings of the 5th ACM conference on Electronic commerce. May 2004
33 Ng C, Parkes D, Seltzer M. Virtual worlds: Fast and strategy-proof auctions for dynamic resource allocation. In: Proc. of the ACM Conference on Electronic Commerce, June 2003. 238～239
34 Conitzer V, Sandholm T. Complexity of mechanism design. In: Proc. of 18th Conference on Uncertainty in Artificial Intelligence (UAI), 2002. 103～110
35 Nisan N, Ronen A. Computationally feasible VCG mechanisms. In: Proceedings of the ACM Conference on Electronic Commerce (ACM-EC), Minneapolis, MN, 2000. 242～252
36 Briest P, Krysta P, Vocking B. Approximation techniques for utilitarian mechanism design. In STOC'05, 2005
37 Feigenbaum J, Nisan N, Ramachandran V, Sami R, Shenker S. Agents' privacy in distributed algorithmic mechanisms. Position Paper, 2002
38 Brandt F, Sandholm T. (Im)possibility of unconditionally privacy-preserving auctions. In: C. Sierra and L. Sonenberg, eds. Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS), ACM Press, 2004. 810～817
39 Brandt F, Sandholm T. Decentralized voting with unconditional privacy. In: S. Koenig and M. Wooldridge, eds. Proceedings of the 4th International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS), ACM Press, 2005. 357～364
40 Brandt F, Sandholm T. On correctness and privacy in distributed mechanisms. In: P. Faratin and J. A. Rodriguez-Aguilar, eds. Selected and revised papers from the 6th AAMAS Workshop on Agent-Mediated Electronic Commerce (AMEC), LNAI, 2004. 1～14
41 Brandt F, Sandholm T. Unconditional privacy in social choice. In: Proceedings of the 10th Conference on Theoretical Aspects of Rationality and Knowledge (TARK), Singapore, June 2005. 207～218
42 Suzuki K, Yokoo M. Secure generalized Vickrey auction using homomorphic encryption. In: Proc. of 7th FC Conference, LNCS, Springer, 2003, 2742: 239～249
43 Goldwasser S. Multi party computations: Past and present [A]. In: Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing [C]. New York: ACMPress, 1997. 21～24
44 Naor M, Pinkas B, Sumner R. Privacy preserving auctions and mechanism design. In: 1st ACM Conf. on Electronic Commerce, 1999. 129～139
45 Feigenbaum J, Shenker S. Distributed Algorithmic Mechanism Design: Recent Results and Future Directions. In: Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, New York, ACM Press, 2002. 1～13
46 Sami R. Distributed Algorithmic Mechanism Design: [PhD thesis]. New Haven, Connecticut: Yale University, 2003
47 Parkes D, Shneidman J. Distributed implementations of Vickrey-Clarke-Groves mechanisms. In: Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS), IEEE Press, 2004. 261～268
48 Mu'alem A. On decentralized incentive compatible mechanisms. In: Proceedings of the 6th ACM Conference on Electronic Commerce Jun. 2005
49 Porter R, Ronen A, Shoham Y, Tennenholtz M. Mechanism design with execution uncertainty. In: Proc. of the Int. Conf. on Uncertainty in AI, 2002. 414～421
50 Porter R, Ronen A, Shoham Y, Tennenholtz M. Fault tolerant mechanism design. In: Proceedings of the 18th Annual Conference on Uncertainty in Artificial Intelligence (UAI-02), Edmonton, Canada, 2002
51 Dash R K, Ramchurn S D, Jennings N R. Trust-based mechanism design. In: Proceedings of the Third International Conference on Autonomous Agents and Multi-Agent Systems, New York, 2004, 2: 726～753
52 Ramchurn S D. Multi-Agent Negotiation Using Trust and Persuasion: [PhD Thesis]. School of Electronics and Computer Science, University of Southampton, UK, December, 2004. http://eprints.ecs.soton.ac.uk/10200/01/thesis.pdf

53 Lipmaa H, Asokan N, Niemi V. Secure Vickrey auctions without threshold trust. In: M. Blaze, ed. Proc. of 6th FC Conference, volume 2357 of LNCS. Springer, 2002
54 Shneidman J, Parkes D C. Specification Faithfulness in Networks with Rational Nodes. In: Twenty-Third Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2004), July 2004
55 Shneidman J, Parkes D C, Massoulie L. Faithfulness in Internet algorithms. In: Proceedings of the ACM SIGCOMM workshop on Practice and theory of incentives in networked systems Sep. 2004
56 Phelps S, McBurney P, Parsons S, Sklar E. Applying genetic programming to economic mechanism design: evolving a pricing rule for a continuous double auction. In: Proceedings of the second international joint conference on Autonomous agents and multi agent systems. Jul. 2003
57 Conitzer V, Sandholm T. Automated mechanism design for a self-interested designer. In: Proceedings of the 4th ACM Conference on Electronic Commerce. Jun. 2003
58 Conitzer V, Sandholm T. Applications of automated mechanism design. In: Proceedings of the UAI Bayesian Modeling Applications Workshop, Acapulco, Mexico, 2003
59 Nisan N, Segal I. The communication requirements of efficient allocations and supporting prices. Journal of Economic Theory, 2006. Forthcoming. http:// www. stanford. edu/~ isegal/prices. pdf
60 Larson K, Sandholm T. Mechanism design and deliberative agents. In: Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems Jul. 2005

(上接第 19 页)

再根据引理 1～3，我们有

$$NC_{s_i^1,s_i^a}(0)$$
$$=q+\sum_{i\notin P_0}\left(\frac{i+1}{q}\right)\left(\frac{i+a}{q}\right)+\sum_{\substack{i+1\in Q_0\\ i\notin P}}\left(\frac{i}{p}\right)\left(\frac{i+a}{q}\right)$$
$$+\sum_{\substack{i+a\in Q_0\\ i\notin P}}\left(\frac{i}{p}\right)\left(\frac{i+a}{q}\right)$$
$$=q+\left(\frac{-1+a}{q}\right)-\sum_{i+1\in Q_0}\left(\frac{i}{p}\right)+\left(\frac{-a+1}{q}\right)\sum_{i+a\in Q_0}\left(\frac{i}{p}\right)$$
$$-p-\sum_{i\in P_0}\left(\frac{i+1}{q}\right)\left(\frac{i+a}{q}\right)$$
$$=q-p+1。$$

所以，当素数 p 和 q 恒定时，序列$\{s_i^1\}$和其它任意一个NMJS具有同样的无转移互相关值，这个值在 p 和 q 为孪生素数时取得最小。

对于任意非零的 ω，如果 $A_s(\omega)=C_{a,b}(\omega)=\frac{-1}{n}$，则称$\{s(i)\}$具有理想的相关值分布。实际上，满足这样的条件是非常困难的。对于密钥流序列，只要它们的相关值的分布相对比较平坦就可以了。为满足密钥流序列大周期的需要，本文中的 p 和 q 的取值都比较大(大于 48 比特)。由定理 1 和 2 可知，这时的相关值分布是非常平坦的。具有平坦的低相关值分布的序列也具有平坦的二元段(run)分布，其对应的密码函数也具有平坦的差分分布和高的非线性度[1]。从而，这种序列若作为密钥流，则具有很强的抗差分攻击的能力[1]。

结束语 笔者新设计了大量的二元序列，并给出了其中一类序列的自相关值以及它与其它类的序列在无转移情况下的互相关值。结果表明，这类序列在一定条件具有非常平坦的低相关值分布，并且这种分布是可控的。这类序列的实现方法和修改的 Jacobi 序列[2]非常类似。如果考虑这些序列在流密码中的应用，线性复杂度及游程分布等性质有待进一步研究。

参 考 文 献

1 Green D H, Green P R, Modified Jacobi sequences [J]. In: IEE Proc. Comput Dig Tech, July 2000, 147 (4): 241～251
2 Cusick T, Ding Cunsheng, Renvall A. Stream Ciphers and Number Theory [M]. North-Holland Mathematical Library 66. Elsevier Science Pub Co, April 1, 1998
3 Damgard I B. On the Randomness of Legendre and Jacobi Sequences [A]. In: Advances in Cryptograpy-CRYPTO' 88, LNCS403 [C]. Berlin: Springer-Verlag, 1990. 163～172
4 Brandstatter N, Winterhof A. Some Notes on the Two-prime Generator of Order 2 [J]. IEEE Trans Inf Theory, October 2005, 151(10): 3654～3657

(上接第 43 页)

6 Lee S C, Shields C. Tracing the Source of Network Attack: A Technical, Legal and Societal Problem[A]. In: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security [C], 2001. 239～246
7 Stone R. CenterTrack: An IP Overlay Network for Tracking DoS Floods[A]. In: Proceedings of USENIX Security Symposium[C], 2000
8 Ferguson P, Senie D. Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing (RFC 2827). The Internet Society, 2000
9 Global Incident Analysis Center. Special Notice - Egress filtering. http://www. sans. org/y2k/egress. htm.
10 Dean D, Franklin M, Stubblefield A. An Algebraic Approach to IP Traceback[A]. In: Proceedings of the Network and Distributed System Security Symposium(NDSS)[C], 2001, 2: 119～137
11 Song Xiaodong, Perrig A. Advanced and Authenticated Marking Schemes for IP Traceback[A]. In: Proceedings of IEEE INFOCOMM[C], 2001. 878～886
12 Snoeren A C, Partridge C, Sanchez L A, et al. Hash-based IP Traceback[A]. In: Proceeding of SIGCOMM[C], 2001, 8: 3～14
13 Cheswick B, Burch H, Branigan S. Mapping and Visualizing the Internet[A]. In: Proceedings of USENIX Annual Technical Conference[C], 2000
14 Floyd S, Paxson V. Difficulties in Simulating the Internet. IEEE/ACM Transactions on Networking, 2001, 9(4): 392～403
15 Snoeren A C, Partridge C, Sanchez L A, et al. Hash-based IP Traceback[A]. In: Proceeding of SIGCOMM[C], 2001, 8: 3～14
16 Hastings J R. Incremental Bayesian Segmentation for Intrusion Detection: [Maseter's Thesis]. Massachusetts Institue of Technology, 2003
17 Park K, Lee Heejo. On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack[A]. In: Proceedings of IEEE INFOCOM[C], 2001. 338～347
18 徐永红. Internet 拥塞控制/信息可用性技术研究: [学位论文]. 南京理工大学, 2002
19 Sanchez L A, Milliken W C, Snoeren A C, et al. Hardware Support for a Hash-based IP Traceback[A]. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEXII)[C], 2001. 146～152
20 Bellovin S. The ICMP Traceback Message. Internet Draft, IETF, March 2000