成果名称：奥尔(Ore)多项式的计算和分解

完成人：李子明

[简介] 李子明研究员把交换多项式的子结式理论推广到非交换的Ore多项式上，建立了Ore环上的子结式定理和算法， 给出了计算最大右公因子和最小左公倍式的模方法，上述的算法被国际最著名的符号计算软件Maple采用，实现在Maple商用软件包OreTools中，被6个处理微分、差分算子，积分和求和的商用软件包反复调用，大大提高了相关函数的效率。在多元Ore多项式环方面，他们给出了计算有限维偏微分模所有子模的第一个算法，给出了计算有限维偏线性方程组超指数函数解的第一个算法。这两个算法已经推广到Laurent-Ore代数上，从而得到了分解有限维微分、差分和微分-差分混合系统的完全算法。

代表性论著：

1. S. Abramov, H.Q. Le, and Z. Li. Univariate Ore polynomial rings in computer algebra. *Journal of Mathematical . Sciences*. Vol. 131, Springer, pp. 5885-5902, 2005.
2. Z. Li, F. Schwarz, and S. Tsarev. Factoring systems of linear PDE's with finite-dimensional solution spaces. *Journal of Symbolic Computation,* Vol 36, Acdemic Press, pp. 443-471, 2003.
3. Z. Li. A subresultant theory for Ore polynomials with applications. *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, O. Gloor (ed.), ACM Press, pp. 132--139, 1998.

成果名称：大型复杂无线通信网络的信道容量研究

完成人：谢亮亮

[简介] 谢亮亮等首次对大型复杂无线通信网络的信道容量研究提供了理论框架。他们将距离的概念显性地引入到信道模型中来，发现最终结果严重依赖于信号关于传播距离的衰减速度；他们发展了多重最大流最小截理论，给出了迄今已知的最准确的信息流上界刻画；他们发展了多层中继信道编码方法，实现的信息传输率为已知最高的。

以上成果发表一年多来，被同行引用次数97次；美国普林斯顿大学学者评价：“开始了无线网络尺度律的系统研究”；瑞士联邦理工学院学者评价：“第一次从信息论观点对大型无线网络的可实现性做了肯定性研究”。

代表性论著：

1. L.-L. Xie and P.R. Kumar, A network information theory for wireless communications: Scaling laws and optimal operation, *IEEE Transactions on Information Theory*, vol.50, pp.748-767, May 2004.
2. L.-L. Xie and P.R. Kumar, On the path-loss attenuation regime for positive cost and linear scaling of transport capacity in wireless networks, Submitted to *IEEE Transactions on Information Theory*, 2005.
3. L.-L. Xie and P. R. Kumar, An achievable rate for the multiple-level relay channel, *IEEE Transactions on Information Theory*, vol.51, pp.1348-1358, April 2005.

成果名称：密钥共享体制和安全多方计算

完成人：刘木兰

[简介] 刘木兰研究员的研究成果主要包括以下两个方面：

安全多方计算和密钥共享体制：安全多方计算是信息安全基础理论的基石；密钥管理中的密钥共享体制是研究多方计算的重要工具。他们提出了并行安全多方计算的概念，建立了线性多密钥共享体制算法，使得并行安全多方计算协议的研究成为可能。利用建立的实现线性多密钥共享体制算法，设计并严格证明了并行安全多方计算协议。有关工作应邀在密码学研究国际联盟主管的国际上三大密码会之一亚密会2005上作报告。它是我国1999－2005七年间被亚密会邀请的唯一报告。（该部分合作者为肖亮亮，张志芳）

交换环上对称密码体制理论：在我国，最早将计算代数用于信息安全理论研究，并出版了专著“Grobner基理论及其应用”。他们成功地将计算代数Grobner基理论结合交换代数中的理想论及环论，用于对称密码体制研究；确切而系统地刻划了环上高维线性递归阵列的结构和高维循环码结构。著名奥地利数学家和系统理论专家Ulrich Oberst和印度学者Shiva Shank等表示希望合作，有关文章在网上（Eluwer Academic Publishers）被访问次数曾排

前三名.（该部分合作者为陆佩忠）。

代表性论著：

1. Peizhong Lu，Mulan Liu，and Ulrich Oberst， Linear Recurring Arrays, Linear Systems and Multidimensional Cyclic Codes over Quasi-Frobenius Rings. Acta Applicandae Mathematicae, 80:175-198,2004. (2004 Eluwer Academic Publishers）
2. Liangliang Xiao and Mulan Liu, Linear multi-secret sharing schemes, Science in China Ser. F 48(2005), 125-136
3. Zhifang Zhang, Mulan Liu, and Liangliang Xiao, Parallel Multi-party Computation from Linear Multi-secret Sharing Schemes, ASIACRYPT 2005, Lecture Notes in Computer Science 3788, 2005, 156-173.

成果名称：综合集成方法理论及应用

完成人：顾基发、唐锡晋、舒光复

[简介] （1） 在NSFC重大项目“支持宏观经济决策的人机结合综合集成体系研究”（顾基发为第三主持人）中，对综合集成方法论从意见综合与模型集成两个角度进行了深入探索，研究了面向OCGS的建模问题，提出了模型体系和综合集成系统建模的各种策略，归纳为6类建模方法，并应用于宏观经济问题和构建综合运输体系的研究。发展并建立了多类信息、多类知识混合变量系统重构分析方法和模型，并应用于GDP增长预测。2005年1月重大项目通过专家验收，被评为“特优”。

（2） 所提出的物理事理人理系统方法论在近10年里不断发展，开展了多领域的应用，如区域水资源管理、商业自动化综合评价、劳动力市场发展、商业标准体系制订、大学评价等，不断得到国内外的反响和新的应用，如在国家高新技术开发区评价、塔里木流域可持续发展、企业管理和一澳中水资源合作项目等。EOLSS大百科全书中有专门介绍WSR的条目。并促进了综合集成系方法论研究。

（3）率先从事我国载人飞船的安全性评估，提出CPRA(中国概率风险评估)，已用于我国载人航天工程921-4全箭和故检分系统安全性定性、定量分析与评估示例，实现了从定性到定量综合集成的应用。

（4） 在01-03年所承担的中国科学院军工项目中，对模型集成的研究基础上，实现了武器系统论证中三个最主要指标（效能、风险、费用）的分析和综合评价等系列基于Web的支持工具，并应用于海军与陆军武器系统论证与综合评价项目，专家评价为“所取得的研究成果在整体上具有先进性、创新性和实用性”。

（5） 提出了在解决复杂问题过程的普遍存在的“沟通-协作-共识”的群体活动C^3过程模型；论述了各种意义下的共识，总结出三种主要的会议模式，提出了基于研讨厅思想的MDTMC(Meeting- Data– Tool– Method (Model)-Consensus)系统。

（6） 从综合集成研讨厅中综合数据、信息、模型和专家经验的设想出发，根据已完成的诸多成果，特别是实现的计算机支持工具和环境，设计实施了一系列的试验，并在国际应用系统分析研究所（IIASA）举办的综合集成特别专题会上的演示以“SARS对2003年我国宏观经济影响”为议题的试验，得到了国际评价。

（7） 研究群体知识涌现及其支持机制，开发了相应的支持工具的雏型（群体研讨环境－GAE）。并应用于香山科学会议等会议成果分析；开展了一系列的试验和研究生课程教学实验。其中2005年春季针对时事问题所进行的试验模式得到了国家信息化专家委员会副主任、何德全院士的关注，并对其下属有关人员进行了应用培训。

（8） 探索研究社会网络，将所参与的NSFC重大项目组织结构所构成的一个一般的“关系网络”，延伸为学术交流、论文引用、致谢与交流研讨活动而导致的“协作网络”以及反映如何阐释综合集成研究的“关键词网络”，定量研究了科学合作与协作中的一些现象和规律，探索了“人理”因素在科学发现中的影响作用。

（9） 2004年9月被邀请参加“社情统计预报系统模型”（即中国社会稳定预警系统，机密项目），负责总体组。

代表性相关论文

1. Gu J.F. and Tang X.J. Meta-synthesis approach to complex system model- ing, *European Journal of Operational Research*, 166(3), 597–614, 2005.
2. Gu J.F. and Tang X.J. *Wu-li Shi-li Ren-li* System Approach to a Major Project on the Research of Meta- synthesis System Approach. *Inte- rnational Journal of Knowledge and Systems Sciences*, 1(1):70-77, 2004
3. 顾基发，唐锡晋，综合集成与知识科学，*系统工程理论与实践*，22(10), 2-7, 2002.
4. 顾基发，王浣尘，唐锡晋．综合集成与复杂系统专辑，*系统工程学报*，16(5), 2001.其中包括：
   a) 唐锡晋．模型集成, *系统工程学报*, 2001, 16(5):322-329.
   b) 顾基发．意见综合 — 怎样达成共识？*系统工程学报*，2001, 16(5):340-348.
   c) 舒光复．综合集成系统重构分析在宏观经济决策中的应用, *系统工程学报*，2001, 16(5):349-353.
5. Gu J.F. and Tang X.J. Designing a water resources management de- cision support system: an application of the WSR Approach, *System Practice and Action Research*, 13(1): 59-70, 2000.