

学科发展

量子信息技术^{*}

郭光灿

(中国科学技术大学量子信息重点实验室 合肥 230026)

摘要 量子信息技术是量子物理与信息科学交叉的新兴学科。它为信息科学的持续发展提供新的原理和方法。阐明了量子信息技术发展的背景及其奇特的信息功能,介绍国际发展的状况和趋势。中国科学院将量子信息作为优先发展领域之一给予有力支持。简要介绍了近几年来我院在这个领域中取得的主要研究成果。对我院如何发展量子信息技术提出几点看法。

关键词 量子信息技术, 研究现状, 发展趋势



我们的时代是信息时代,信息科学在改善人类生活质量和推进社会文明发展中发挥着无可比拟和令人惊叹的作用。人类对信息需求的日益增加,促进人们不断地致力于信息技术的发展,然而现有的信息系统,如

电子计算机、通信网络、信号检测等,其信息功能已开拓到接近极限值的程度。例如,电子计算机在过去 30 年中每个芯片的晶体管数目随着时间指数增长,这个所谓的 Moore 定律预示着,十多年之后计算机存储单元将会是单个原子,于是就出现诸如量子效应究竟对计算机运算速度会产生什么样的影响这一类问题。图灵理论作为计算机科学的基石,无法回答这类问题。此外,现在计算机不可避免的能耗也会限制芯片集成度的提高,最终会导致单个 CPU 仅能达到某个极限速度。因此,信息科学的进一步发展必须借助于新的原理和新的方法,于是人

们面临着新的挑战:21 世纪的信息科学将向何处发展?

量子特性在信息领域中有着独特的功能,在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面可能突破现有的经典信息系统的极限。于是便诞生了一门新的学科分支——量子信息科学,它是量子力学与信息科学相结合的产物,包括量子密码术、量子通信、量子计算和量子测量等,近年来在理论和实验上已经取得了重要突破,引起各国政府、科技界和信息产业界的高度重视。人们越来越坚信,量子信息科学为信息科学的发展开创了新的原理和方法,注入了新的活力,将在 21 世纪发挥出巨大潜力。因此,世纪之交也正是信息科学从经典跨越到量子的关键性时刻!

1 国际研究现状和发展趋势

1.1 量子通信

量子通信是以量子态作为信息单元来实现信息的有效传送。根据传送信息类型的不同可分为两类:一是传送经典信息,如量子密码、量子身份认证、量子比特承诺等;二是传送量子信息,如量子隐

* 收稿日期:2002 年 6 月 20 日

形传态(quantum teleportation), 量子通信网络等。

由于现广泛使用的密码体系本质上是不安全的,一旦量子计算机研制成功,所有保密体系将被攻破,能确保通信安全的是量子密码体系。量子密码的工作原理是用量子态表示经典随机数(密钥),基于量子不可克隆定理,任何窃听的企图都会被合法用户所发现,因此,原则上量子密码是绝对安全的,其安全性由量子力学的基本原理所保证。目前美、英、瑞士等国正致力于这方面的研究并在实验上取得重要进展,已经在光纤上实现 67 公里的密钥传送,在自由空间中实现 10 公里的密钥传送。西方国家的目标是在近 5 年之内实现量子密码实用化。目前在技术上遇到的主要困难是:如何增加量子密钥传输距离。有待突破的重要关键技术:一是红外(1.3 微米、1.5 微米)单光子探测器。这是因为光纤量子密钥传输是采用单个光子来实现的,光纤损耗阻碍着传输距离的提高,1.3 微米和 1.5 微米是现在所使用光纤损耗最小的波长。现有成熟的单光子探测器工作波长在可见光,理论上光子在光纤中传输的极限距离约为 20 公里。因此,实用的红外单光子计数器成为关键性问题。二是单光子光源。现在量子密码研究中所使用的单光子光源是将相干光脉冲衰减到平均每个脉冲只有 0.2 个光子,这是一种近似的单光子源,其效率低,既影响量子密钥的传输距离,又影响其安全性,因为这种光源有可能在一个脉冲中同时出现两个光子。因此,研制真实的单光子源成为量子密码研究的另一个关键性问题。美国、日本、西欧正在大力开展这些关键技术的研究,最近在 *Nature*、*Science* 上报道了他们得到的重要进展,但仍未获得根本上的突破。

量子通信网络的工作原理是采用量子通道来传送量子信息,与现有通信网络相比,量子通信有三大优点:一是保密性强,原则上可以做到通信的绝对安全保密;二是具有同时进行信息处理和信息传输的功能,可实现多端的分布计算;三是能有效地降低通信复杂度,即多端计算某个函数所需的经典通信次数可以减少。因此量子通信网络可能创建新的通信原理和方法。美国由军方主持已制定了在十年内实现全球量子因特网的目标,并组织许

多大学和研究所着手实施此项计划。

最简单的量子通信是量子隐形传态,它可以实现将量子信息传送到远处,但不传送该量子信息的物理载体本身。量子隐形传态原理是以量子信息开创者之一、美国 IBM 的 Bennett C. H. 教授为首的多国联合研究小组在 1993 年提出的,1997 年底,奥地利研究组在实验上首次演示成功,论文发表在 *Nature* 上(论文第二作者为中国科学技术大学潘建伟),引起国际学术界和媒体的极大兴趣。

目前,国际学术界所设想的量子通信网络是采用光子(飞行的量子比特)来传送量子信息,而采用原子(静止的量子比特)来存储和处理量子信息。当前,这个领域仍处在单元技术的基础研究阶段,有许多关键性问题亟待解决,其中重要的有:实现有效的量子隐形传态,尽管有若干实验室已演示成功这种新型的量子信息传送原理,但由于“Bell 态测量”这个关键技术未获突破,人们只能在实验上测量四个 Bell 态中的两个,最大成功概率只有 50%。因此,如何有效测量 Bell 态成为重要的研究课题。④目前设想的量子处理器是置于光腔中的原子,但光腔的损耗会破坏存储在“光腔原子”中的量子信息,为此,要求光腔 Q 值要非常高,目前技术上达不到。因此,研究实际可行的量子处理器便成为关键性的问题之一。④远程的纠缠量子通道是实现全球量子通信网络最重要的条件,但纠缠态在环境的影响下会遭到破坏,从而导致所传送的量子信息泄漏到环境中去,到达终端的量子信息便不同于输入的量子信息,即保真度小于 1。目前已提出许多办法来克服这个困难,如纠缠纯化,纠缠浓缩等,但这些方法仍未从根本上解决远程纠缠量子通道这个关键性的问题,因为保真度随传送距离按指数衰减。

1.2 量子计算

量子计算的前景十分诱人,而且在理论和实验的研究上都不断地取得重要进展。但量子计算的实现在技术上遇到严重的挑战。实现量子计算必须解决三个方面的问题:一是量子算法,它是提高运算速度的关键,目前研究成功 Shor 量子并行算法, Grover 量子搜寻算法等;二是量子编码,它是克服消相干的有效办法,目前已有量子纠缠、量子避

错和量子防错三种不同原理;三是实现量子计算的物理体系(即多个量子比特的量子逻辑网络),目前在腔 QED、离子阱、核磁共振、量子点等已实现少数量子比特,但距实现有效量子计算的需求相差甚远,各国科学家正从不同途径来探索实现可扩展的量子逻辑网络的方法,虽然不断取得进展,在 *Nature*、*Science* 上每年都有许多文章发表,但仍未从根本上突破。这个领域仍处于基础性的探索阶段。

尽管量子信息技术的发展遇到许多困难和挑战,但它关系到国家安全以及未来高新技术的激烈竞争,因此,各国政府、军界、商界均极其重视,并不断加大投入。

2 我院的研究进展

中国科学院非常重视量子信息这一新兴学科,采取了一系列有力措施来推动其在我国的发展。1998 年由中国科学技术大学主办了第一次量子信息领域的香山科学会议,王大珩院士亲临主持,这次会议促进了国内学术界对量子信息的关注并吸引越来越多的学者加入到该领域的研究行列。为了适应量子信息科学的发展,我院在中国科学技术大学建立了量子信息重点实验室,并进入中国科学院知识创新工程试点序列。1999 年在武汉召开院内量子信息研讨会,2000 年江绵恒副院长亲自参加院内量子信息发展战略研讨会,并做了重要指示。中国科学院先后支持两项知识创新工程方向性项目:“量子物理与信息”和“量子通信技术的研究”,并积极组织申报科技部“973”项目,使“量子通信与量子信息技术”于 2001 年立项。2001 年 9 月中国科学技术大学主办“2001 年量子信息国际学术会议”,有 150 多位学者和研究生参加,其中包括 Bennett C. H., Zoller P., Grover L. K. 等 10 多位国际知名学者。目前我院将“量子信息”列入知识创新工程重点支持的领域之一。在我院各级领导强有力的支持下,我院科研人员在量子信息技术领域已取得一系列重要的进展。

2.1 量子密码

我院物理研究所和中国科学技术大学分别成功地演示了光纤量子密钥的传送。中国科学技术大学还提出了“信道加密”的新型量子密码方案,如图 1 所示。现有的量子密码方案都采用“信源加

密”,如图 1(a) 所示,信源(0, 1)用非正交态表示,在传输过程中,任何窃听都会被合法用户所发现,量子不可克隆定理确保密钥的安全性。图 1(b) 为“信道加密”方案,信源为经典信息,在传输时,加密器将 0 和 1 两个态变换成完全相同的混合态,在终端再用解密器恢复为密钥,只要加密器和解密器处于纠缠态,此方案是绝对安全的,比较现有其它方案,该方案具有很多优点。

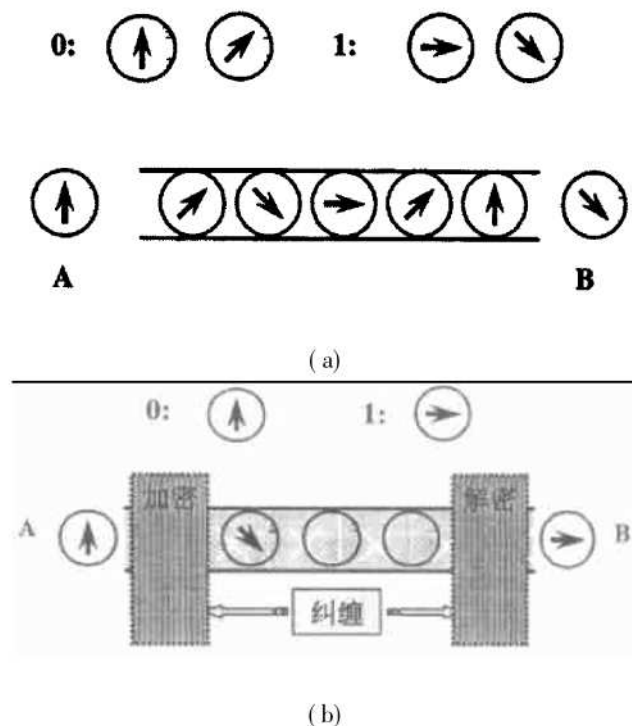


图 1 (a) 信源加密, (b) 信道加密

2.2 量子通信网络

在量子通信的研究中,通常认为光腔中原子作为信息存贮-处理器较为合适。但由于光腔中光场的消相干会严重影响其正常运行,因此,对光腔 Q 值的要求很高,现有技术水平难以实现。

我们提出一种能有效克服光腔消相干影响的新型量子处理器,它应用两个原子与腔模的非共振相互作用,在大失谐条件下,并设光腔模初始为真空态,此时原子与腔膜不会交换能量,因此,光腔始终处于真空态,系统对腔的耗散和热辐射就不敏感,这样就大大降低了对光腔 Q 值的要求。我们同时证明这个装置可实现许多量子信息功能,如制备原子纠缠态、实现量子受控非门、隐形传送原子态等(见图 2)。法兰西科学院院士、法国巴黎高等师范学校的著名教授 Haroche S. 采用这个模型在实验

上成功制备了原子纠缠态。他在论文摘要中写道,“遵循郑和郭最近提出的模型,我们报道实验结果

……”,并指出这种方法“为复杂纠缠操作开创了很有希望的前景。”

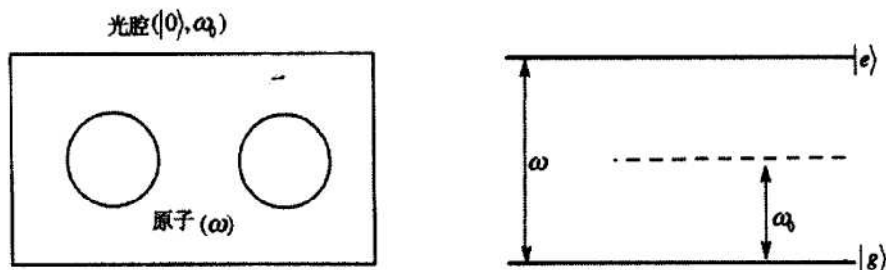


图2 非共振两原子量子信息处理器原理图

中国科学技术大学年轻教授段路明在国际合作研究中提出一种远程量子通信的可行方案,解决保真度随距离指数衰减的重大难题,该结果发表在 *Nature* 上。目前中国科学技术大学正在开展该方案的实验研究。

中国科学技术大学首次在实验中研究量子通信复杂度。量子通信网络的优点之一是可以有效降低通信复杂度,即在完全多端分布计算时所需的通信次数减少,但迄今尚无实验研究成果的报道。我们提出的两体通信模型可以演示量子通信的优点。

我们在实验中研制成功由 Ar^+ 激光泵浦 BBO 晶体产生的偏振纠缠光子源,输出为两个孪生光子,其纠缠度可调,可从非纠缠到最大纠缠($>98\%$)。在输出两臂上采用对光子偏振态的局域操作,结果用 4 个光子探测器(效率 70%)的符合计数给出(见图 3, 4)。实验结果表明,通道的纠缠度越大,通信复杂度越低。该实验首次演示了量子通信的特性。

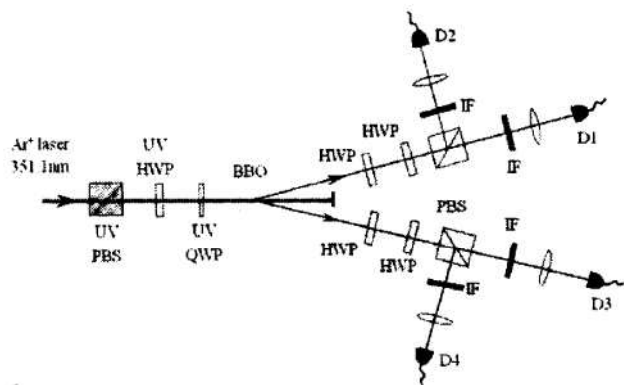


图3 量子通信复杂度实验装置

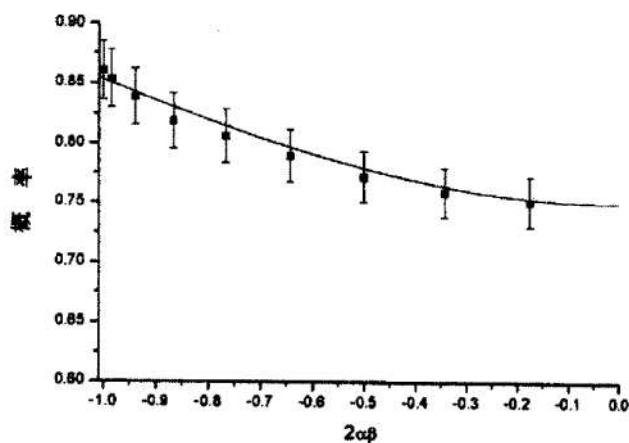


图4 量子通信复杂度实验数据曲线

2.3 量子计算的基础研究

武汉物理与数学研究所研制成功了 2 个量子比特核磁共振体系,并演示出量子密集编码等(发表在 *PRA*)。

中国科学技术大学研制成功 4 个量子比特的核磁共振体系(发表在 *PRA*),并采用 NRM 体系在实验上演示量子游戏(发表在 *PRL*),获国际好评, *Nature* 网页上发表专文给予介绍。

中国科学技术大学在国际首创量子避错编码原理并已被美国学者在实验上证实。量子计算机实际应用的最主要障碍是环境会不可避免地破坏量子相干性,使其丧失运算速度快的优越性。这个消相干问题曾严重地困惑着国际学术界。国际上广泛研究的量子纠错编码是基于独立消相干的假设,我们研究了“集体消相干”过程,发现有一类特殊量子态在环境作用下不会发生消相干,我们称之为

为相干保持态。英国学者也独立发现了这一类特殊量子态。

我们进一步将这类相干保持态用于量子编码,其原理是将消相干的量子信息编码到这类态上,使之在存储期间可保持其相干性,待使用时再用解码方法提取出来。这个编码原理具有效率高、易操作,且能推广到量子门操作上的优点。该论文入选在美国召开的第一届 NASA 量子计算机和量子通信国际会议的大会报告,并被 *Science*、*Nature*、*PRL*、*PRA* 等刊物引用 35 次。美国加州大学(伯克利)、MIT 和 Los Alamos 国家实验室的若干著名小组相继证明:应用这类相干保持态可构造无消相干的子空间来实现可靠的量子计算;最近,美国 Los Alamos 和 NIST 等实验室三个研究组分别采用光子、离子和原子核在实验上演示成功,三篇论文均发表在 *Science* 上。

中国科学技术大学段路明博士在国际合作研究中提出在原子体系中实现原子纠缠方法,把物理学中最热门的两个领域 BEC 和量子信息结合起来,有可能使原子钟的精度提高三个量级(*Nature* 发表了该成果)。段路明在 *Science* 上发表“几何量子计算”的可行方案,被评价为新的重要突破。

2.4 量子信息的基础研究

在国际上首创概率量子克隆原理,为有效提取量子信息提供了新的途径。量子不可克隆定理既是量子密码安全性的依靠,也给量子信息的提取设置了不可逾越的界限,于是国际学术界便着眼于不精确克隆的研究,以解决量子信息有效提取这一重要难题。我们应用“么正-塌缩”原理,提出了概率量子克隆原理,它以某种概率克隆出保真度为 1 的非正交态。

有关上述工作的论文已作为该领域的原创性工作被 *Nature*、*PRL*、*PRA* 等刊物引用 30 余次。国际学术界称之为“段-郭概率克隆机”,将最大克隆效率公式称为“段-郭界限”。我们在实验上研制成功“概率量子克隆机”和“普适量子克隆机”,这项实验成果得到学术界高度评价,英国学者 Chefles A. 在其综述论文中评价该实验为“该领域近年来最激动人心的进展之一”,“有可能揭示出信息处理和传输的最终物理极限”;美国著名学者 Hillery M. 在其综述

论文中指出,“在合肥的中国科学技术大学郭光灿所领导的小组已在实验上达到最大保真度,郭和他的合作者采用线性光学方法……”;牛津大学 Bouwmeester 小组在 *Nature* 发表的论文,也肯定我们的实验“将单个光子的自由度近似地复制到同一光子的额外自由度上。”

中国科学院理论物理研究所孙昌璞研究员在量子绝热纠缠、“薛定谔猫佯谬”可能解、新型量子通信载体、高维量子态远程制备和量子信息基本问题等方面做出了一系列国际一流的理论成果。

3 发展我院量子信息技术的思考

我院将“量子信息技术”作为优先发展领域给予大力扶植和支持,无疑是个卓有远见的战略决策。目前我院在这个领域的研究水平处于国内领先地位,成为我国发展量子信息技术最重要、最活跃的研究基地。当然,我们还应清醒地认识到,虽然我们在某些方面做出了国际领先或先进水平的成果,但从整体上看,与先进国家相比仍有不小差距。汪成为院士曾经说过,我们中国人常常醒得比较早,穿衣洗漱也不慢,但跑着跑着就落在别人后面。这非常形象地道出了我们在国际激烈竞争中存在的“后劲不足”的状况。科学创新是建立在长期积累基础之上的。“后劲不足”的一个重要因素就是积累不够,尤其是技术支持条件缺乏。例如,我们有能力提出新型量子处理器的理论模型,但只有法国 Haroche S. 院士研究组才能在两个月之内在实验上加以实现,因为他们从事腔量子电动力学的实验研究已有 10 多年历史,有着丰富的技术储备和经验积累,这是别人无法比拟的。我国近年来的科研经费投入有很大增长,实验条件有明显改善,但因长期拖欠造成了现在的技术支撑仍不是很强。面对这种现实,如何发展我国的量子信息这门有着重要应用前景的新技术,是我们应当认真思考的问题。

(1) 发挥优势,找准切入点。在量子信息领域,我们虽然在整体上落后,但局部上有自己的优势,因此,我们必须在现有优势的基础上去寻找当前若干重要的关键性科学问题,以此作为切入点,集中力量,坚持不懈地研究下去,一旦突破将会对量子信息技术的发展产生重要的影响。

(2) 立足长远, 加强技术积累。对于我们落后于别人的某些关键技术, 不可能依靠从国外输入, 而应立足于长远的需求, 尽早有计划地布署。如红外单光子探测器, 这是远程光纤量子密码的关键性器件, 日本、美国有长期技术积累, 我们落后很多, 应支持国内条件较好的单位, 如上海技术物理研究所、半导体研究所, 协力开展研究。

(3) 提倡学科交叉, 发挥团队作用。量子信息是涉及物理、数学、信息科学、计算机科学等多学科的交叉, 只有这些学科领域的研究人员相互协作, 发挥各自所长, 才可能有所突破, 才能参与国际竞争。

(4) 突出重点, 长远布局。量子通信是量子信息领域中有可能最早得到实际应用的技术, 而且事关国家的信息安全, 应作为近期重点给予支持; 对于量子计算研究应做长远布局, 例如, 固态量子计算是很有希望的方案之一, 近期应支持院内在量子点、超导、纳米材料方面基础较好的单位开展相关

的基础性研究, 以期未来有新的突破。

主要参考文献

- 1 Einstein A, Podolsky B, Rosen N. *Phys. Rev.*, 1935, 47: 777.
- 2 Milburn G J 著, 郭光灿等译. 费曼处理器. 南昌: 江西教育出版社, 1999, 49- 55.
- 3 郭光灿等. *物理*, 1999, 28(2): 120.
- 4 Bennett C H, Wiesner S J, *Phys. Rev. Lett.*, 1992, 69: 2 881- 2 884.
- 5 Bennett C H et al. *Phys. Rev. Lett.*, 1993, 70: 1 895- 1 898.
- 6 Bouwmeester D et al. *Nature*. 1997, 390: 575- 579.
- 7 Zheng S B, Guo G C, *Phys. Rev. Lett.* 2000, 85: 5 392.
- 8 Duan L-M, Guo G-C. *Phys. Rev. Lett.*, 1998, 80: 4 999.
- 9 Duan L-M, Guo G-C. *Phys. Rev. Lett. A*, 1997, 79: 1 953.
- 10 Kwiat P G et al. *Science*, 2000, 290: 498- 501.
- 11 Keilpinski P et al. *Science*, 2001, 291: 1 013- 1 015.

The Technique of Quantum Information

Guo Guangcan

(Key Laboratory of Quantum Information, USTC, CAS, 230026 Hefei)

The technique of quantum information is a new developing field that involves both the quantum physics and the information science. It equips the information science with new principles and methods and ensures its persistent development. This paper introduces the backgrounds of quantum information technique and illustrates the strange functions dealing with information. It also gives a brief view to the international developing situation and prospect. The Chinese Academy of Science has given strong support to the subject of quantum information as an area with priority. We here introduce the main research results in this area that we have obtained in the recent years. Finally, we propose some suggestions on the further development of technique of quantum information in our academy and thus to induce more valued ideas.

郭光灿 中国科学技术大学理学院常务副院长, 中国科学院量子信息重点实验室主任, 教授, 博士生导师。1942 年 12 月出生于福建惠安。1965 年毕业于中国科学技术大学后留校工作至今, 1981—1983 年在加拿大多伦多大学做访问学者。中国科学院知识创新工程方向性项目“量子通信技术的研究”首席专家, 国家自然科学基金委员会创新群体学术带头人, 科技部“973”项目“量子通信与量子信息技术”首席科学家。长期从事量子光学和量子信息等方面的教学和科研工作, 在 *PRL*、*PRA* 等国内外刊物上发表论文 200 余篇, *SCI* 收录 160 余篇, *SCI* 引用 540 多次, 出版著作 12 部, 已培养博士 13 名、硕士 29 名。