量子信息科技的理论基础、发展前景与我们的对策

梅昌超，万小龙

（华中科技大学，湖北 武汉 430074）

摘　要：系统回顾了量子信息科学与技术的理论基础，概括介绍了量子通信技术的发展现状与前景，并为武汉中国光谷相应科技发展战略提出初步建议。

关键词：量子信息；量子通信；量子计算

中图分类号：O413.1　　**文献标识码**：A　　**文章编号**：1001-7348(2004)04-0028-03

量子通信和量子计算（量子信息学）是最近几年迅猛发展起来的新兴学科，由于它潜在的巨大实际应用价值和重大科学理论意义，正引起社会各方面越来越多的关注。武汉中国光谷作为我国光电子信息产业基地，应该充分重视信息科技这一未来发展趋势的前瞻性、基础性和交叉性研究。

1　量子通信的理论基础

量子信息涉及到经典信息论、计算机科学、理论物理学的许多方面，其中还用到概率论、数论、群论等数学知识，属交叉性学科。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以突破现有的经典信息系统的极限。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，预计其巨大发展潜力将在5~15年内得到充分发挥，为信息科学应用开辟更广阔的新天地。

从基础理论上说，信息，归根结底是编码在物理系统态中的东西，从物理角度看，信息源于物理态在时空中的变化，信息传输是编码物理态的传输，信息处理是计算机的物理系统态的有控制演化，信息的提取则是对编码物理态的测量。因此，信息科学的深入发展需要基础物理理论的指导。

从应用技术上说，随着计算机在生产生活中的应用日益广泛，对计算机的运算速度的要求越来越高，单机运算速度主要是靠减小元件尺寸来提高的，照著名的摩尔定律，芯片将在10~20年内变成单原子器件。于是必须考虑到微观的量子效应带来的影响，而

---

(3)增强其下属机构——内部审计部门的职能。内部审计部门本身的独立性和专业胜任能力是相当必要的。一般地，要求内部审计部门隶属于审计委员会，审计部门的主管由审计委员会任命；同时，内部审计的重点要由以前的财务审计走向管理审计，从监督走向服务，以提升企业价值为目标。这就要求内部审计人员精通各方面的知识。可以说，内部审计人员的工作是审计委员会正常开展工作的基础。

(4)积极做好内部审计和外部审计的沟通和交流。如果内部审计的工作是值得信赖的，外部审计可以减少工作量，从而可以减少企业总的审计费用（实证表明，外部审计的费用是内部审计费用的两倍以上）。同时，外部审计人员的工作也可以作为内部审计人员的工作参考。把内外审计连接起来的桥梁就是审计委员会。

(5)减少与管理当局的冲突。审计委员会在工作过程中既要保持身份独立、经济利益独立、精神独立的同时，又要尽量和管理当局沟通，减少相互之间的摩擦与冲突。审计委员会还应指导内部审计部门和人员积极主动地做好内部审计工作，通过为管理当局提供服务，为企业直接或间接地创造价值，赢得管理当局对内部审计工作的认同、理解和支持，减少工作中的矛盾与冲突。否则，审计委员会的职能就无法有效发挥。

参考文献：

[1]刘力云.审计委员会制度述评[J].审计研究，2000,(3).

[2]武俊.上市公司审计委员会制度在美、英、加的发展及其启示[J].外国经济与管理，2000,(7).

[3]沃而特·J·萨蒙等.公司治理[M].北京：中国人民大学出版社，2000.

（责任编辑：高建平）

收稿日期：2004-02-10

基金项目：本文系武汉东湖高新技术开发区战略研究院课题"量子通信技术发展前景研究"，并受国家社会科学基金"量子力学哲学研究"(03C8X003)和教育部人文社会科学重点研究基地（山西大学-科学技术哲学）2002年招标课题"当代物理学前沿的哲学问题研究"资助。

作者简介：梅昌超，华中科技大学公共管理学院讲师，经济学博士生，主要研究方向为公共管理学和高新技术开发区管理。万小龙，华中科技大学人文学院副教授，科学技术哲学博士，主要研究方向为量子力学哲学与高新技术开发区管理。

对于微观量子效应，经典信息理论和图灵机理论对此无能为力。这样便激发了以量子物理学为基础理论的量子信息论的研究，以及以量子系统作为存储元件，以量子态作为信息单元的新型计算机原理和特性的量子计算机的开发。

量子力学的诞生深刻地改变了人类社会：在20世纪推动了社会发展的核能、激光、半导体等高科技，都是源于量子力学。量子信息论思想由来已久。量子力学从上世纪20年代创立以来，尽管其在实验上巨大成功，但对其物理意义与哲学意义的诠释一直存在着争论。量子客体的波粒两象性迫使人们不得不引入波函数（量子态）来描述量子客体的状态，著名物理学家与思想家Feynman曾指出：量子力学的精妙之处在于引入几率幅（即量子态）的概念。事实上，量子世界的千奇百怪的特性正是起源于这个量子态，而关于量子理论的长期激烈争论的焦点也在这个量子态。在近百年的学术争论中，影响最大的就是薛定谔（1935年）提出的所谓"薛定谔猫"佯谬和爱因斯坦等人（1935年）提出的质疑量子力学完备性的EPR佯谬。EPR问题经半个多世纪的广泛研究，终于在上世纪80年代的一系列精确实验中有了倾向性的结果：EPR粒子对（或更精确地说是EPRB对）呈现的远程关联不仅是量子力学理论的主要特征，而且是测量中确定存着的一种实验现象。

1981年，Feynman最先提出，EPR关联是一种像质量、能量那样的资源，我们在原则上可以利用量子力学系统态的纠缠实现比经典信息量传输大得多的量子信息的传输。Feynman的这一假说确定了量子信息论的开端。事实上，按照量子力学理论，EPR粒子对处在所谓的纠缠态上，这个量子态最大地违背Bell不等式，有着奇特的性质：我们无法单独地确定某个粒子处在什么量子态上，这个态给出的唯一信息是两个粒子之间的关联这类整体的特性，现在实验上已能成功地制备这类纠缠态。

1993年，Bennet根据EPR量子信息的解释和量子非克隆原理，提出了量子隐形传态即在技术上可行的第一个量子信息传输的方案。经典比特可以看成量子比特的特例。用量子态来表示信息是量子信息的出发点，有关信息的所有问题都必须采用量子力学理论来处理。信息的演变遵从薛定谔方程，信息传输就是量子态在量子通道中的传送，信息处理（计算）是量子态的幺正变换，信息提取便是对量子系统实行量子测量。量子比特可以制备在两个逻辑态0和1的相干叠加态，换句话讲，它可以同时存储0和1。考虑一个N个物理比特的存储器，若它是经典存储器，则它只能存储2N个可能数据当中的任一个，若它是量子存储器，则它可以同时存储2N个数，而且随着N的增加，其存储信息的能力将指数上升。例如，一个250量子比特的存储器（由250个原子构成）可能存储的信息数比现有已知的宇宙中全部原子数目还要多。

1997年，我国青年学者潘建伟参加的奥地利研究组首次在实验上成功实现了这种量子隐形传态，在国际上引起极其强烈的震动。

另一方面，Shor于1994年提出的绍化算法（shor's Algorithm）利用量子态的相干性，对大数因子分为平等复杂性计算，使得将经典计算需数亿年的时间减少到几分钟即可完成。Shor的开创性工作有力地刺激了量子计算机和量子密码术的发展，成为量子信息科学发展的重要里程碑之一。

而根据量子不可克隆原理，任何对量子信息的提取均会破坏原有量子态（原则上不可利用克隆技术来窃取信息），即量子力学的不确定性原理使任何窃取信息的过程都会留下痕迹而被发现。

总之，量子通信在提高运算速度、确定信息安全、大信息容量方面具有对经典通信不可比拟的优势，量子信息科学为信息科学的发展开创了新的原理和方法，将为信息科技带来新的革命。

2 量子通信技术的新进展

量子信息技术包括量子密码、量子通信、量子计算和量子测量等。尽管目前量子计算机实现上有巨大困难，近期内难以建成量子计算机，但量子信息科学技术的巨大发展潜力，目前已受到各国政府、科技专家和公众的广泛关注。在量子器件方面的最新进展是IBM公司在2001年底已成功开发用7个原子组成的"shor算法"的模型量子计算机，而实用量子计算机至少需要1万个原子位。量子计算适合高度并行问题，不能完全取代日常运用的电子计算机。实现量子因特网要解决若干关键技术：高亮度纠缠资源，量子隐形传态，Bell态测量，纠缠交换，纠缠纯化，信息存贮和处理，量子编码等。目前没有一种技术具有可扩展性，即没有找到制作大位数量子芯片的方法。因此，虽然实现量子计算原理上已无障碍，但尚未掌握良好制备与操纵量子态的技术。不过，学术界越来越认可量子通信技术20年后将成为信息社会的支柱。

国际上重要的西方国家（美、英、法、加拿大、以色列、日本、瑞典、奥地利、意大利、瑞士等），特别是美国和欧盟均投入大量人力物力于量子通信、量子计算的理论与实验研究，量子信息已成为学术界的热门课题，其发展十分迅猛，参与研究的国家、机构和人员日益增多，有关国际会议连接不断。以美国为例，加州理工大学、MIT和南加州大学联合成立了量子信息和计算研究所，其长远目标就是通过多学科交叉和多单位协作以实现量子计算机，近期规划为量子算法、量子网络设计、量子门设计、量子编程、量子模拟的理论和实验研究。在Los Alamos国家实验室，正在实验研究局域网的量子密码体系和自由空间中（地-空或低轨道卫星之间）的量子密钥传送，以及离子阱量子计算机原理实验；美国标准和技术研究所（NIST）正在研究量子逻辑门和制备薛定谔猫态等，Stanford大学研究基于核磁共振的量子计算机。至于欧洲，则成立了以英国、法国、德国、意大利、奥地利和西班牙等国在内的量子信息物理学研究网，基主要的研究内容是量子密码、量子通讯和量子计算。这是继欧洲核子中心和航天技术的国际合作之后，又一大规模的针对科技重大问题的国际合作。此外，加拿大在Montereal大学成立了量子信息实验室，澳大利亚在国立大学建立了量子通讯研究所，荷兰的国家数学和计算机科学研究所、芬兰的Helsinki大学理论物理部等，也积极开展了量子信息的研究。量子信息研究另一个十分显著的特点是信息产业界的投入，例如IBM、AT&RTR、Bell实验室、英国电话电报公司等，这从一个侧面有力地表明量子信息和量子计算将具有广阔的实际应用前景。

更值得注意的是政府和国防部门的重视。例如美国的量子信息和计算研究所为美国军队研究部门（Army Research Office）管

理,隶属于美国国防部高级研究计划司超大规模计算工程;英国国防部研究局直接卷入与英国电话电报公司合作的量子保密通讯的实验;北大西洋公约组织则出资支持牛津大学 A.Ekurt 教授的量子信息研究计划。这说明量子信息的研究与国家安全有着紧密的联系。

目前最成熟的是量子密码技术,已实现光纤上 20km、真空约 1km 的量子密钥传输,5~10 年内可能投入实际应用。量子通信速度比目前通信技术快 1 000 万倍,估计 10 年以上时间内可建立量子因特网。欧美国家利用量子加密进行通信的技术已进入实际运用阶段,但通信距离一般只有几十 km,日本总务省量子信息通信研究推进会日前举行会议,提出了以新一代量子信息通信技术为对象的长期研究战略,计划在 2020 年至 2030 年间,建成绝对安全保密的高速量子信息通信网,以实现通信技术质的飞跃。日本专家认为,今后信息技术的研究课题是利用量子技术进行加密,来建成能高速通信的通信网。日本计划 5 年内实现在 100km 左右的中距离通信中,使用量子加密技术,到 2007 年将构筑起量子信息技术高速通信实验系统,在 2020 年至 2030 年间建成利用量子加密技术的安全高速的量子信息通信网。负责起草长期研究战略报告的东京大学教授今井秀树在记者招待会上说,量子通信技术 20 年后将成为信息社会的支柱。

国内最早从事这个研究的是中国科技大学。他们率先在国际重要刊物上发表大量有关量子编码、量子通讯、量子密码术、量子态制备和操作等方面的论文,其中在国际上最有影响的成果是提出"量子防错码"这种新的量子编码方案,受到国际上高度重视。此外,中科院物理所、华东师范大学在量子密码方面已作了跟踪性实验工作,武汉物理所正开始筹备用 PAUUL 阱俘获离子的实验工作,还有其他单位对此有浓厚兴趣,正筹备开展工作。

北京大学与清华大学于 2002 年联合成立量子信息与测量实验室。中科院上海光机所于 2003 年 11 月在量子力学重点实验室首次实现了量子信息存储,对光通信和光量子信息处理领域具有潜在的科学价值和应用价值。留奥科学家、中科大教授潘建伟去年的工作又有重大突破,其"自由量子态隐形传输"被欧洲物理学会评为 2003 年国际物理学 10 大进展之一,这一研究成果表明,可在不破坏被传输态的条件下成功地传输量子态,实现高精度量子纯化。

3 对策

新经济革命是由信息科技革命引起的,至今中国在其中主要是引进国际先进水平的科技成果并本土化(以汉字处理技术为代表)。网络泡沫的破灭可以看作是信息科技革命浪潮的第一子浪的结束。目前正处于两次大的科技子浪之间的间隙期。第一子浪主要是信息技术本身的核心创新所主导。笔者预计信息技术的第二子浪将是信息科技与其他基础科技的联合创新。信息技术与物质基础科学理论的结合,也即与量子科学结合而成为的量子信息科技,最具可能爆发革命。我国部分学者在这方面的研究水平已走到了世界前列。

正在武汉建设的国家光电子产业基地集湖北省、武汉市的技术优势和产业优势,已取得了相当成绩。然而,纵观光谷"十五"规划指南,"十五"期间武汉国家光电子产业基地将优先发展的信息光电子、能量光电子、消费光电子、软件等 4 大领域,重点发展光纤光缆、光电器件、光通信系统及设备、IP 网络系统及设备、移动通信系统及设备、光电材料、工业激光设备与应用、激光生物医学仪器及成套设备、激光器与光学元器件、光电测量仪器、光机电一体化设备、光存储、光显示、光输入/输出、光源/电源、信息家电等 16 类光电产品以及集成电路设计、信息安全软件、通信类支撑软件、CAD/CAM/CAPP 等应用软件,GPS/GIS/RS、ITS 和智能建筑系统等 4 类软件产品,其中作为原始技术创新的仍然有进一步加强的必要。并且,从整体上说,这些项目仍然主要是以经典信息学为基础的。不容否认,这些应用技术的发展对提升我国光电子产业水平和满足我国日益增长的社会信息需求无疑是正确的,也是必要的。然而,根据摩尔定律,信息技术以十分惊人的速度发展,高技术产业的产品是不能保值的,能够保值的是持续处于技术上游的原始创新能力,而这种创新能力的维持必须有强大的科学理论和领先核心技术的基础研究作后盾。量子信息学最重要的基础是量子力学,而量子力学不同于经典力学的最迷人方面就是量子态的纠缠整体性。相比之下,前述武汉光谷规划指南的 20 类发展项目可能仍未全面涉及量子信息学的这一基本特征。如果武汉光谷能良好代表信息科技的这一中长期发展方向,那么她将成为名副其实为"中国光谷"。

武汉光谷在上世纪 90 年代末筹办时曾提出 5 年再造一个新武汉的口号,就是基于当时光电子产品的丰厚利润和巨大市场而考虑的。如今,随着加入 WTO,光纤产品由于国际上跨国技术公司的大幅度降价,某些光谷龙头光纤公司的利润率也已快速下滑,因此我们认为,武汉光谷在进一步努力实现已定规划的基础上,必须充分注意信息科技发展的新动向,具体说:

(1)鉴于量子信息科技的世界发展主流,武汉光电子的产业管理、投资方和科技研发人员必须上下来一次量子通信科技先进性与发展前景的知识普及,充分认识到未来 20 年内将是量子信息的时代,并作好这方面的前瞻性战略发展研究。

(2)鉴于我国科学家在量子信息领域某些方面的国际领先地位,开发区应与国内著名研发机构提前进行有效合作,学习 IBM 等国际著名企业的经验。加强投入专项基金,让一部分科研人员从纷杂的下游应用技术开发中解脱出来,潜心于中长期原始创新研究。

(3)鉴于量子信息技术近期较成熟的是量子密码技术,而量子态的非经典信息传送仍必须辅以经典光纤传输实现,开发区应积极争取国家支持,整合强大的光纤研产能力,争取在量子加密通信技术方面成为中国的首个产业发展基地,使武汉光谷真正成为非区域性的中国光谷,切实改变我国信息科学的落后面貌。

参考文献:

[1]郭光灿.神奇的量子信息技术. http://www.cpus.gov.cn/kjqy/file/gxjs.htm

[2]李承祖等.量子通信和量子计算[M].长沙:国防科技大学出版社,2000.

[3]Michael A. Nielsen AND Isaac L.Chuang: Quantum Computation and Quantum Information. Cambridge University Press; September 2000.

(责任编辑:曙 光)