科学通报 2012 年 第 57 卷 第 17 期：1498 ~ 1525
评 述 www.scichina.com csb.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

量子信息技术纵览

周正威, 陈巍, 孙方稳, 项国勇, 李传锋

中国科学技术大学中国科学院量子信息重点实验室, 合肥 230026
E-mail: zwzhou@ustc.edu.cn

2012-02-08 收稿, 2012-04-01 接受

摘要 量子信息技术经过近三十年突飞猛进的发展, 在理论和技术方面已经获得了举世瞩目的成就. 本文主要对量子信息技术各个热点研究分支的发展进行了概括性的介绍, 涉及到量子密码、量子通信、量子计算、量子模拟、量子度量学、量子信息物理基础等各个领域. 此外, 也讨论了原子、分子和光物理、固体物理的各个分支(超导约瑟夫森结系统、半导体量子点自旋系统、金刚石氮-空穴色心系统)、离子阱、核磁共振系统等各种物理体系在量子信息技术中的应用和发展. 通过对量子信息技术的研究和积累, 人们调控微观世界的能力获得了显著的提高. 量子密码技术已经接近实用化, 长程量子通信的原理性验证也不存在原则上的障碍. 量子模拟技术快速发展, 已经接近经典计算机可以模拟的极限. 同时, 量子度量学也获得了快速的发展. 本综述不仅反映了国际量子信息技术发展的状况, 而且也提炼了近年来中国量子信息科学技术在国际上取得的成就. 这些成就表明, 中国已经成为量子信息世界版图中一股不可或缺的力量.

关键词
量子信息技术
量子密码
量子通信
量子计算
量子模拟
量子度量学
量子信息物理基础

2011 年 9 月 26~27 日, 由中国科学院学部组织的“科学与技术前沿论坛——量子信息”在北京召开. 该次论坛由郭光灿院士召集, 报告人和正式代表共 62 名. 9 月 26 日全天, 分别由 14 位专家做了论坛报告, 报告者为从事量子信息研究的院士、国家重点基础研究发展计划的首席科学家和从事重要研究方向的杰出学者. 报告内容非常广泛, 涉及量子密码、量子通信、量子计算、量子模拟、量子度量学、量子信息物理基础. 9 月 27 日, 全体专家就中国量子信息科学技术发展的若干问题进行了研讨.

本文的主要目的是对量子信息技术做一个总体性的介绍, 在综述各个学科方向的历史以及国际发展动态的同时, 对 9 月 26 日的报告内容进行分类、汇总, 将它们放入整个国际量子信息技术发展的大框架中, 以期能反映出中国近年来量子信息科学技术发展的概貌.

本次论坛报告内容非常丰富广泛. 从研究方向上来划分, 报告内容基本涵盖了量子信息技术研究的各个分支; 从报告者的身份来划分, 有从事纯计算理论研究的数学家、理论物理学家, 以及从事各种物理体系研究的实验物理学家; 从实验物理学家所研究的物理体系来划分, 大的方向包括原子、分子和光物理、固体物理的各个分支(超导约瑟夫森结系统、半导体量子点自旋系统、金刚石 NV 色心系统)、离子阱系统、核磁共振技术等. 笔者能力有限, 虽然竭力为之, 难免有所疏漏. 另外, 一些杰出学者因故未能出席会议, 未能在本次论坛上汇报其成果, 他们的研究未能包含在这篇综述中, 实为憾事.

在下面的正文部分, 我们将列论坛报告所涉及的量子信息技术的各个研究方向, 分别对其背景和近期发展做简要的介绍.

1 量子密码技术

量子密码是一种可以通过公开信道完成安全密

英文引用格式: Zhou Z W, Chen W, Sun F W, et al. A survey on quantum information technology (in Chinese). Chin Sci Bull (Chin Ver), 2012, 57: 1498–1525, doi: 10.1360/972012-224

钥分发的技术, 是量子信息技术的一个重要分支. 通信双方在进行保密通信之前, 首先使用量子光源, 通过公开的量子信道, 依照量子密钥分配协议在通信双方之间建立对称密钥, 再使用建立起来的密钥对明文进行加密. 这种密钥建立方式的安全性由量子力学的测不准原理、不可克隆定律保证: 当有窃听者对信道中传输的光子进行窃听时, 会被合法的收发双方通过一定的校验步骤发现. 由于其物理安全保障机制不依赖于密钥分发算法的计算复杂度, 因此可以达到密码学意义上的无条件安全. 将量子密码技术安全分发的密钥用于一次一密加密, 可以实现无条件安全的保密通信. 图 1 给出了采用量子密码进行安全通信的基本过程.

量子密码的原始概念由美国人 Wiesner 于 20 世纪 70 年代提出[1]. 1984 年, IBM 公司的 Bennett 和加拿大 Brassard 共同提出了量子密钥分配的概念, 以及第一个量子密钥分配协议——BB84 协议, 奠定了量子密码学发展的基础[2]. 鉴于量子密码技术在下一代安全通信领域具有巨大的战略意义, 近年来, 美国、欧盟、日本等投入了巨大的人力物力进行这一技术的研究, 新一轮的技术竞赛正在激烈进行. 例如, 美国 DARPA 于 2002~2007 年在波士顿建设了一个 10 节点的量子密码网络[3], 欧洲于 2009 年在维也纳建立了一个 8 节点的量子密码网络[4], 2010 年日本 NICT 在东京建立了一个 4 节点的量子密码演示网络, 使用了 6 种量子密钥分配系统[5].

中国研究组在量子密码实用化研究领域走在了世界前列. 2004 年, 中国科学技术大学的韩正甫研究组分析了光纤量子系统工作不稳定的根本原因[6], 并发明了“法拉第-迈克尔逊”编解码器, 用于自适应补偿光纤量子信道受到的扰动, 大大提升了光纤量子密码系统的实际传输距离和稳定工作时间. 该小组利用这一方案, 在北京和天津之间的 125 km 商用光纤中演示了量子密钥分配, 创造了当时世界最长的

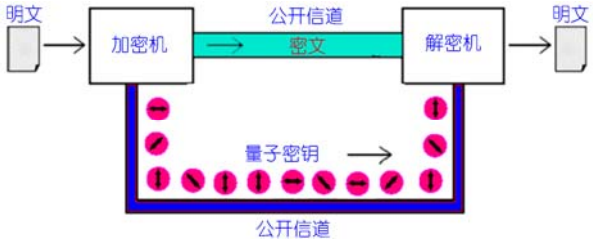

图 1　采用量子密码进行安全通信的示意图

商用光纤量子密码实验纪录[7]. 该小组随后发明了基于波分复用技术的“全时全通”型“量子路由器”, 实现了量子密码网络中光量子信号的自动寻址[8], 并使用这一方案分别在北京(2007 年)和芜湖(2009 年)的商用光纤通信网中组建了 4 节点和 7 节点的城域量子密码演示网络[9~11]. 中国科学技术大学潘建伟研究组也于 2008 年和 2009 年在合肥实现了 3 节点和 5 节点量子密码网络[12,13]. 目前, 国际上建成的几个重要的量子密码演示网络见图 2. 北京大学、华东师范大学、上海交通大学、华南师范大学、山西大学、国防科技大学等单位的研究组也在量子密码技术的研究上取得了出色的研究成果.

量子密码的安全性是其核心价值. 安全性分为协议安全性和实际系统安全性两个层面. 量子密码概念提出至今, 研究者已设计了多种量子密钥分配协议, 并围绕这些通信协议的无条件安全证明进行了大量的理论工作. 迄今为止, 一些主要协议的安全性证明已取得如下成果: BB84 协议的无条件安全性已经获得严格的证明[14,15]; 差分相位量子密码通信协议在无误码条件下的绝对安全性已获得证明[16], 但在有误码条件下的普遍安全性尚未获得完全的证明; 基于离散调制连续变量量子密钥分发协议的安全性已获得证明[17].

在协议安全性得到证明的基础上, 为了实现高可靠性的量子密码系统, 我们还需要跨越理想协议模型和实现技术之间的鸿沟. 这一问题的实质是: 物理原理所要求达到的完美条件在真实世界中是否能够被无限逼近? 如果理想的物理条件不能无限逼近, 那么有安全漏洞的实际量子密码系统的安全性如何保证? 这导致了对实际非理想条件下的量子密码系统进行攻防的问题. 实际的量子密码系统中, 光源、探测器和编解码器等部件都可能出现安全性漏洞.

我们以 BB84 量子密钥分配协议为例说明实际光源的安全性问题. BB84 协议要求使用单光子来编码量子比特, 然而受限于单光子源的研究状况, 实际实验中普遍采用弱相干光光源替代单光子光源. 但是, 由于此类光源存在一定概率的多光子脉冲, 如果采用分束攻击, 窃听者原则上可以从多光子携带的编码信息中获得两者建立的量子密钥, 并成功地欺骗通信双方. 韩国 Hwang[18], 加拿大 Lo 等人[19]和清华大学 Wang[20]提出并完善了诱骗态技术. 这一技术的核心思想是: 通过随机使用几种不同强度的弱相

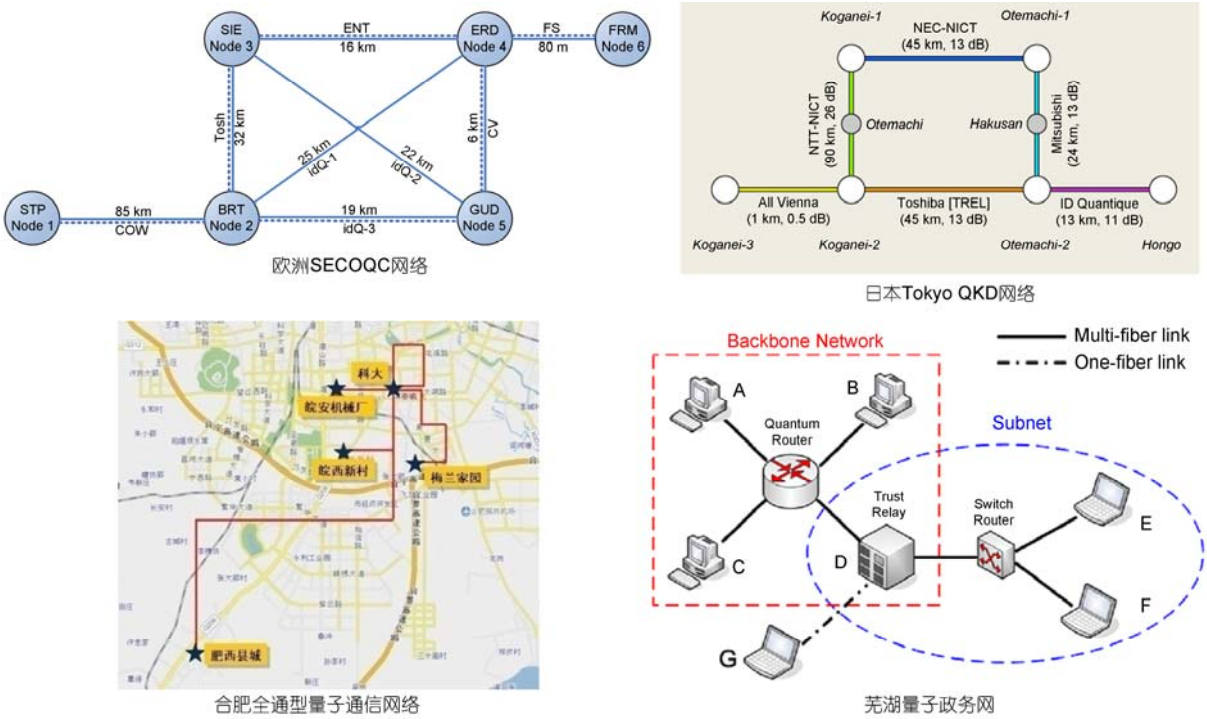

图 2 世界上几个重要的量子密码演示网络示意图

干光源, 可以检测出分束攻击窃听行为. 实现诱骗态方案的手段多种多样, 为了避免引入新的安全性漏洞, 必须对其实现方案进行严格的分析. 例如, Weinfurter 等人发现: 采用多激光器来产生诱骗态, 不同激光器的波长或其他物理特性可能存在差别, 从而泄露部分信息, 进而导致建立密钥的不安全[21].

Lo 等人从多探测器密钥分配系统入手, 最先对探测器的安全性进行了研究. 他们发现, 在多探头量子密钥分配系统中, 不同探测器的响应时间和探测效率一般会存在差异. 窃听者利用探测效率的不匹配可以控制接收端探测器的响应, 进而获取密钥信息[22]. Makarov 小组针对 InGaAs 的红外单光子探测器在“盖革”和线性工作模式下的区别, 利用强光使“盖革”模式的单光子探测器变成线性模式输出, 通过控制信号的光强, 可以使探测器输出的电信号高于或略低于甄别域值, 从而控制单光子探测器输出或不输出探测结果, 即彻底控制接收方的探测输出, 因此被称为强光致盲攻击. 利用这一攻击手段, 该小组完全攻破了 IDQuantique 公司的商用量子密码系统[23]. Weinfurter 小组提出了死时间攻击. 其基本原理是: 红外单光子探测器在“盖革”模式下, 需要在探测到光子后, 加入死时间以抑制雪崩效应. 窃听者可以制备强光偏振态, 当接收方在探测开门之前接收到窃听者制备的量子态后进入死时间状态, 使该探测器对在死时间内到达的合法量子信号不产生响应. 发送方发送的量子态只有在与窃听者的量子态相互正交的情况下才会引入计数, 而其他编码态在探测器的死时间内没有响应[24].

近年来, 人们意识到在实际密钥系统中的编解码环节上也存在安全漏洞. Lo 等人提出所谓的“相位重映射”攻击方法: 他们针对往返式系统, 利用调制器的有限响应时间, 精确控制量子态调制时间, 使量子态调制达不到既定的位置, 从而诱使发送方提前或推后调制相位[25]. 在实际调相系统中, 总是不可避免地存在调相器损耗和调制误差, 此时实际系统中发送的态与理想的态之间存在偏差. 韩正甫小组分析了这一问题, 发现调相器损耗和调制误差将导致实际的编码态和标准量子密钥分配协议编码态存在差异, 从而带来安全性漏洞, 他们提出了解决这些问题的方法, 给出了相应的密钥率公式[26,27]. 韩正甫小组利用光纤分束器件的波长相关特性提出了一种攻击方案, 可以有效地攻击使用波长相关光纤分束器件作为编解码器的量子密码系统[28].

表 1 部分地总结了当前实际量子密钥系统安全

表 1 量子密钥分配系统实际安全性研究

量子态制备方面	量子态测量方面	编解码器方面
分束攻击(Brassard 小组)	强光致盲攻击(Makarov 小组)	调制损耗(韩正甫小组)
多激光器安全性(Weinfurter 小组)	死时间攻击(Weinfurter 小组)	调制误差(韩正甫小组)
非可信光源(Lo, 郭弘小组)	时移攻击(Lo 小组)	波长攻击(韩正甫小组)
……	……	相位重映射(Lo 小组)

性研究的主要进展.

总体来讲, 量子密码协议的安全性是值得信赖的, 但是量子密钥分配系统的实现方案必须经过严格的评估. 对于现有的实际量子密码系统来说, 接收端安全性漏洞较之发射端大; 往返式系统安全性明显弱于单向系统; 单探测器系统安全性强于多探测器系统; 单激光器比多激光器安全; 主动器件比被动器件安全. 解决了上述的器件实现方案中的实际安全性问题, 量子密码才能做到真正的安全.

2 量子通信

说道量子通信, 一定会有人问: 量子密钥分配过程就是利用了量子状态, 达到了保密通信的目的, 这难道不是量子通信吗? 的确, 广义来讲, 量子密钥分配过程确是利用了量子状态行使保密通信的功能. 但是, 这里的量子态的功用在于建立通信双方之间经典信息的关联, 即量子态只是充当建立这个安全的经典信息关联的桥梁和保障, 人们最终还是利用这个经典信息关联来做经典意义上的密码通信. 而我们这里所说的量子通信, 则是完全利用量子信道来传送和处理真正意义上的量子信息.

那么量子网络有什么用? 这里, 我们可以对照一下经典的网络. 在几十年前, 电子计算机刚刚投入应用时, 它只是科研人员的专用物品, 是远离大众的稀有事物. 但是, 随着计算机网络的出现, 这一面貌被完全改变. 现在网络已经深入到人们的生活之中, 除了获取海量的信息、方便自由的通信, 还可以行使网上购物、网上银行等便捷的功能. 同样, 我们也可以展望量子网络. 量子网络的物理功能是联络量子处理终端(可以是量子计算机), 目前我们所知道的是: 它可以协调若干量子终端来处理更复杂的量子计算功能, 在目前量子计算机的可扩展性遇到阻碍的情况下, 这不啻为一个提升量子计算能力的可行途径; 利用量子网络, 可以行使全量子的通信协议, 用量子信息来完成特殊的信息处理功能; 利用量子网络在处理多节点计算时, 会大大降低通信的复杂度; 另外, 利用量子网络也可以行使经典信息的功能, 如直接利用量子网络中的量子纠缠来达到安全的密钥分发的目的. 相信, 随着这一事物逐渐地步入人类生活, 更多的功能将被开发出来.

量子通信最关键的一环是如何建立量子通道(也称为量子信道), 通过这个量子通道来安全无误地传送量子态的信息. 这一问题于 1993 年在理论上获得了解决[29]: 量子信息领域的开拓者 Bennett 及其合作者, 提出了著名的 quantum teleportation 方案, 中文翻译为“量子隐形传态”. 所谓量子隐形传态是指: 如果能够在量子通信的双方(Alice 和 Bob)之间建立最大的量子纠缠态(Bell 态), 那么 Alice 和 Bob 可以通过经典通信来协同两地的操作, 利用量子纠缠态, 可以将 Alice 处待发送的量子态准确无误地传送给 Bob. 作为代价, 成功传送量子态的同时, 量子纠缠态被损毁. 在这一量子通信的过程中, 承载 Alice 处量子态信息的物理的量子系统, 并没有被发送出去, 该系统仍然待在 Alice 处; 但是, 原先蕴藏在该系统中的量子态的信息, 已经借助量子纠缠态中奇妙的量子关联, 被传送到 Bob 处. 仿佛一个量子物体的灵魂被抽走, 重新装载在遥远异地的另外一个物体上, 所以被称为量子隐形传态. 有了量子隐形传态方案, 我们就可以利用量子纠缠来做量子信道, 充当联系各个节点的桥梁.

那么下面的一个问题就是, 如何在遥远的异地之间建立起高品质的量子纠缠态的联系? 这牵扯到一系列的问题. 因为量子纠缠态是一种由多个微观粒子构成的复合系统的量子态, 它如何产生? 如何跨越物理空间进行分发而不受破坏? 关于如何产生纠缠态, 目前已不是困难, 人们已经在各种不同的物理系统中产生量子纠缠态. 并且, 人们也找到了最适合做量子信道的物理系统, 那就是光子系统. 光子能够在媒介中快速传输而不易受到环境的扰动. 而世界上第一个量子隐形传态的实验验证, 也是奥地利

的 Zeilinger 小组于 1997 年在光子系统中完成的[30], 其实验的原理见图 3. 迄今为止, 基于纠缠光子的量子隐形传态的研究被广泛开展. 例如, 2003 年潘建伟和 Zeilinger 等人改进了先前的实验, 能够使得被传送的粒子能自由传播, 而不需要先前实验中必须通过破坏性的量子测量来证实实验成功与否[31]; 潘建伟等人于 2004 年在建立 5 光子纠缠的基础上, 完成了开放终端的量子隐形传态, 能够将待传送的量子态发送给非单一的用户[32]. 但是, 即便是光子系统, 传输距离仍有限制, 随着传输距离的增加, 光子纠缠的品质仍会下降, 以至于无法完成理想的量子信息的传输.

如何在大尺度空间范围内建立高品质的量子纠缠通道, 一些重要的理论方案被相继提出. 1993 年 Żukowski 等人提出了纠缠交换的方案: 对于两对纠缠光子, 每对拿出一个光子, 将它们做一个 Bell 态的测量之后, 剩余的两个光子由最初的没有纠缠的状态变成有纠缠的状态[33]. 这个 Bell 态测量的过程相当于将两段绳子接成一条长绳, 而这条长绳就成了新的、具有更长距离的纠缠通道. Bennett 等人在 1996 年提出了著名的纠缠纯化方案: 当身处异地的两者之间拥有很多对纠缠程度比较低的劣质纠缠态的时候, 他们可以通过一些局部的量子操作和经典通信过程, 能够从中提取出少量高品质的纠缠态[34]. 1998 年 Briegel 等人提出了量子中继的策略, 基本上就是结合了纠缠交换和纠缠纯化技术, 将遥远的两地分成很多中间节点, 分发纠缠态的过程仅仅在最短的节点间进行, 但是, 通过不断的纠缠纯化和纠缠交换过程, 原则上可以在这遥远的两地之间建立起高品质的纠缠态[35].

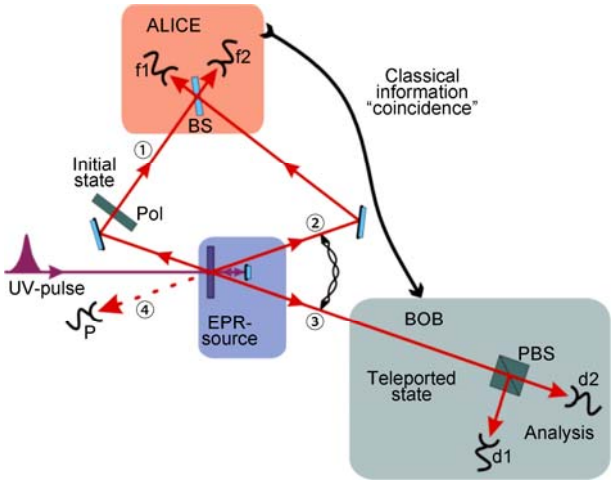

图 3 世界上第一个演示量子隐形传态的实验示意图

对于上述量子中继的方案, 在物理实现方面还需要一个重要条件, 就是在每个节点上都要有量子的存储器: 能够将光子的量子状态较长时间地存储下来, 并能够实施必要的量子操作步骤, 以实现纠缠纯化和纠缠连接. 在这方面, 一个重要的理论进展是 Duan 等人[36]提出了利用原子系综来做量子存储器的量子中继方案: 将光子信息存储在系综原子的激发模式中, 能够维持较长的时间; 同样, 再次利用光和原子的相互作用, 可以将存储于原子中的量子态的信息读取出来, 完成量子中继的步骤. 但 Duan 等人工作的一个不足之处在于, 为了存储光量子态的信息到原子系综, 需要单光子干涉过程: 这需要将干涉的两条路径长度的差值控制在亚波长量级的精度, 对于一个长路径的干涉, 这在实验上是很难完成的. 陈增兵和潘建伟等人改进了这一干涉过程, 用双光子干涉取代单光子干涉, 将干涉路径控制的精度提升至光子的相干长度范围, 大大提升了系综原子中继方案的可用性[37], 在实验上, 他们也做了成功的演示[38]. 目前, 潘建伟小组在基于冷原子系综的量子中继的研究方面已经取得了系列的进展, 除了完成单步量子中继的演示之外, 他们完成了光子与原子比特之间的量子隐形传态[39], 制备出适合于冷原子系综存储的窄带纠缠光源[40]. 在 2009 年, 他们将冷原子系综中量子态的存储时间提升至 1 ms[41], 接近当时的国际最好水平(当时的最高水平为 6 ms[42]), 2011 年, 他们完成了解除频率关联的窄带极化纠缠光子的存储, 将经光腔压窄的自发参量下转换过程产生的纠缠光子很好地存储于冷原子系综的量子态上, 便于进行进一步的操控[43].

除了量子中继技术之外, 还有一种可能增大量子通信距离的方法是: 在卫星和地面之间开展光量子态的传输(见图 4). 相对于在地表大气中的光子传输, 在星地之间的传输克服了地表曲率的影响, 同时也没有障碍物的阻碍; 另外, 地表于人造卫星之间只有 5~10 km 的水平大气等效厚度, 而大气对某些波长的光子吸收非常小, 同时也能保持光子极化纠缠品质; 在外太空无衰减和退相干. 一个可能的展望是: 由星地之间的量子通信来联系不同的城域量子网络, 完成量子密钥分配、量子隐形传态、类空间隔的量子非定域性的检验等任务. 在直接以大气为媒介传输

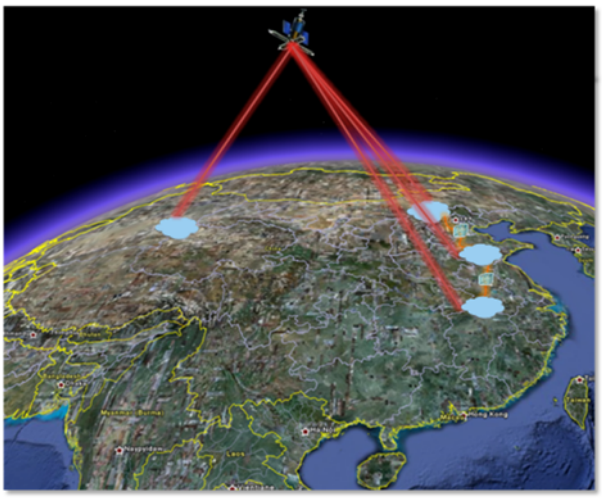

图 4　星地量子通信示意图

光子态的研究方面, 2007 年, 欧洲的实验组已经实现了 144 km 的自由空间量子密钥的分发[44]; 2010 年, 潘建伟小组实现了 16 km 自由空间量子隐形传态的验证, 该距离已经超过了星地之间的等效大气厚度, 佐证了星地量子通信的可行性[45].

综所上述, 构建一个全量子的通信网络, 需要有通信波段的纠缠光源、高品质的量子存储器、高效的量子中继技术、节点的量子信息处理技术等环节. 从目前的进展看, 将这些技术组合在一起, 构成一个全量子的通信网络, 不存在原则上的困难. 但是, 如何提高各个环节的品质, 优化整个系统, 达到高速率的量子信息的传输, 将是一个很大的技术挑战.

在量子通信中, 我们前面提到的用作量子信道的光子纠缠态, 都是用离散 Hilbert 空间中的量子态, 具有分离的自由度. 对于无限维 Hilbert 空间中的量子光场, 我们可以用所谓的连续变量的物理量(如光学模的正交分量)来刻画光场的量子性. 此时, 光场的纠缠特性体现在光场间的量子起伏. 采用连续变量的量子态依然可以行使量子通信量子计算的功能. 就量子通信而言, 在连续变量的纠缠态系统中, 人们也实验验证了量子隐形传态[46]和量子密集编码协议[47], 完成了以连续变量表征的光量子态在原子系统中的存储[48].

在以连续变量为基础的量子通信中, 高品质的纠缠态是人们追求的目标. 自 20 世纪 90 年代美国加州理工学院 Kimble 研究小组制备出连续变量的 EPR 纠缠态以来, 纠缠态的品质被不断提高. 2010 年, 山西大学彭堃墀院士研究组, 采用模清洁器以及改进的锁频技术, 将非简并光学腔中产生的 EPR 纠缠光场的纠缠度提高到 6 dB, 创造了当时世界上连续变量纠缠光的最高品质[49]. 另外, 山西大学张靖研究组在理论上提出了通过相敏简并光学参量放大器(DOPA)对于注入压缩真空态光场的操控和增强的方案[50], 彭堃墀院士组在实验上实现了这一理论预言, 当输入纠缠光场的纠缠度为 4 dB 时, 通过满足一定条件的参量放大器后纠缠度可达 5.5 dB[51].

同离散变量的纠缠态一样, 多组分的连续变量的纠缠态对多方的量子通信协议和利用纠缠态的单向量子计算至关重要. 2000 年, 英国的 Braunstein 等人提出: 将压缩态光场通过多个分束器的线性变换, 可以获得多组分纠缠的理论方案[52]. 2003 年, 彭堃墀院士组在世界上最早实现连续变量 3 组分纠缠态[53], 在此基础上完成了受控量子密集编码的实验演示; 2007 年, 他们又率先实现了连续变量的 4 组分纠缠态[54].

连续变量量子信息学已具备进一步发展的理论和实验基础, 形成去实现量子通信另一种有效的可能途径. 连续变量的纠缠光与现有的光通讯技术兼容, 能够无条件运转. 目前存在的主要问题是: 保真度还比较低. 一种可能的克服途径是建立分离变量与连续变量混合的杂化量子信息系统, 兼容二者的优势, 提高量子通信的品质.

3　量子计算

量子计算的概念最早由 Benoiff[55]和 Feynman[56]提出, 随后, 英国的 Deutsch 提出了量子图灵机模型, 完成了同经典图灵机模型的对应[57]. 自此, 量子计算机的研究开始步入正途. 量子图灵机(示意图见图 5)的计算同传统图灵机计算的最大差别在于, 表征基本信息单元的比特是个两能级的量子系统, 它的状态由 Hilbert 空间的基矢量叠加而成, 不同于经典比特只能处于 0, 1 两种可能; 对信息的操控满足闭系统的量子力学演化规律, 由薛定谔方程控制. 这样一来, 对 N 个量子比特的单次操纵, 等效于同时对 2^N 个基矢量同时做了变换. 量子图灵机的运转带有天然的并行性, 这是量子力学原理所赋予的. 但是, 对于最后信息的读出过程, 量子力学原理告诉我们只能读出这 2^N 种可能性中的一种, 每种可能性出现的几率由演化后状态的基矢量前面的几率幅决定. 所以, 原则上量子计算是一种概率计算, 人们通过对于

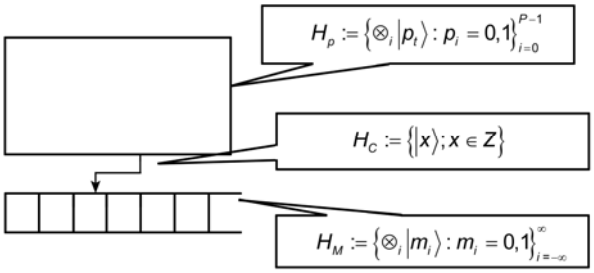

图 5 量子图灵机示意图

最后随机输出的结果的分析, 来求解问题的答案.

开始人们并不能确信这一计算模式能够带来怎样的后果, 但随着两个著名算法的发现, 使得人们对量子计算的前景给予厚望. 1994 年, 美国的 Shor 发明了量子 Shor 算法[58], 采用量子 Shor 算法, 可以用量子计算机求解大数的质因子分解, 进而可以攻破 RSA 密钥系统, 而到目前为止, 人们并没有找到有效的求解大数因子分解的经典算法. 1997 年, 美国的 Grover 发明了 Grover 算法[59], 利用 Grover 算法, 量子计算机可以以平方根加速所有的搜索问题, 这在实际中非常有用. 正是这两种重要算法的发现, 将量子计算机的研究带入了高潮.

关于量子计算的研究, 我们大致可以分为计算模式研究、硬件研究、软件和算法研究几个方向. 我们先来介绍计算模式.

关于计算模式, 大体可分为标准量子计算模式、基于测量的量子计算模式、拓扑量子计算模式和绝热量子计算模式 4 类.

(ⅰ) 标准量子计算模式. 标准量子计算模式的理论发展同经典计算机的理论发展非常类似. Deutsch 在建立量子图灵机的理论模型之后, 把建立一个普适量子计算机的任务转化为建立由量子逻辑门所构成的逻辑网络, 并指出构成这种逻辑的普适部件——Deutsch 门[60]. 对照于经典的逻辑电路, Deutsch 门的角色就像是异或门, 在经典电路模型中, 所有的逻辑电路都可以由异或门搭建; 同样, 对于量子逻辑电路, 级联量子 Deutsch 门, 可以搭建任意的量子逻辑电路. 1995 年, 美国的 Bennett 等人进一步简化了 Deutsch 门的设计, 获得了更为简单的普适逻辑门集合: 采用单量子比特的任意旋转和两量子比特的受控非门, 就可以搭建任意的量子逻辑电路[61].

同经典计算相类似, 量子计算也面临纠错问题, 只是量子错误所造成的危害比经典错误更甚. 因为量子错误本身可以看成一个不可控的量子操作, 它会对量子态造成并行的影响. 多次持续的量子错误影响之后, 其平均效果将使得量子的相干性尽失, 量子计算将退化为经典的概率计算从而丧失掉所有的优势. 我们将环境所造成的量子错误统称为量子退相干. 克服量子退相干的最主要手段是量子纠错码. 最早的量子纠错码方法也是 Shor 于 1995 年所提出[62], 随后量子纠错码的理论获得了很大的发展. 目前, 人们几乎将所有的传统的纠错编码手段都找到了量子情况下的对应.

对于成功的量子计算, 我们有一个总的图像: 我们首先要将所有要参与量子计算的比特, 在指数维度的 Hilbert 空间中制备出一个纯的量子态, 然后, 我们用量子逻辑电路对这个大空间中的量子状态进行幺正变换, 当运行完所有的逻辑变换之后, 对计算的末态进行量子测量, 输出计算结果. 进一步, 通过对结果的分析、处理, 获得待求解的数学问题的答案. 在这个过程中, 退相干过程将使量子态偏离原来的演化, 同时使得系统状态跟环境自由度相纠缠, 使得系统状态偏离原来的纯态特征而只能用混和态来描述. 如果退相干的程度不是十分大, 可以采用量子纠错码, 可以以很大的概率将系统纠错, 扭转到原来的轨道上来; 如果错误的概率超出了量子纠错码所能承受的阈值, 那么量子纠错失效. 当然, 对于一些由特殊错误类型占统治地位的环境, 我们可以发展主要纠正该错误类型的纠错码方法, 所以, 容错阈值并不是一个绝对的数值, 它依赖于错误的类型和使用的纠错码方法.

有了这样的一个物理图像, 量子计算的物理实现问题就变得清晰起来. 美国 IBM 的科学家 DiVincenzo 将量子计算的物理实现对物理系统的条件和人为的操控能力划分为如下 5 条, 我们称为 DiVincenzo 判据:

(1) 系统要有能力很好地表征量子信息的基本单元——qubit, 即一个两能级的 Hilbert 空间;

(2) 在计算开始时, 我们要能够对系统进行有效的初态制备, 将每一个 qubit 制备到 0 状态;

(3) 要有能力对系统的 qubits 实施普适量子逻辑门的操作. 具体而言, 要能够对单个量子比特实施任意的单 qubit 的幺正变换, 以及对任意两个量子比特实施受控非门操作;

(4) 要能够对量子计算机幺正演化的终态实施

有效的量子测量;

(5) 系统要有长的相干时间, 能够使得量子操作(包含纠错)和测量在相干时间内完成.

除了上述标准量子计算模型之外, 我们简单介绍一下另外几种量子计算模式. 它们或是为了简化操作过程(如基于测量的量子计算), 或是处于克服环境退相干的考虑(如拓扑量子计算和绝热量子计算), 但最终为实现量子计算机的目的, 都需要满足DiVincenzo 判据.

(ⅱ) 基于测量的量子计算模式. 该计算模式最早为奥地利 Innsbruck 大学的 Raussendorf 和 Briegel 于 2000 年提出, 当时被命名为单向量子计算[63]. 该计算模式的特点是: 在计算的初始阶段, 先制备出一个超大规模的纠缠态, 该纠缠态被命名为图态. 这种图态相对来说很容易制备, 只需要对初始化的 qubit 进行局域操作和紧邻的 Ising 相互租用即可. 图态制备完毕之后, 相当于完成了初始化过程, 接下来, 量子计算的所有逻辑门操作被证明只需要在图态上进行相应的局域测量和经典通信即可. 而局域操作和经典通信过程在很多物理体系中是最简单的操控手段, 而这种基于测量的量子计算模式将量子逻辑电路中两比特门的实现难度都退化到图态的制备上.

后来, 人们进一步证明了, 除了 Raussendorf 和 Briegel 所定义的图态, 很多多体纠缠态都能承担实现基于测量模式的量子计算的任务[64].

(ⅲ) 拓扑量子计算模式. 该方案最早由数学物理学家 Kitaev 于 1997 年提出[65], 他构造出一个具有特殊拓扑量子性质的强关联系统, 该系统低能激发的准粒子是一种非阿贝尔任意子, 这些任意子状态可以编码 qubit 信息; 同时, 任意子的交换满足群论中的辫群规则, 通过任意子之间的交换来完成逻辑门操作; 最后, 通过对任意子进行干涉测量来读出计算的结果. 拓扑量子计算的最大特点是: 在该系统中, 表征量子信息的量子态是一种拓扑态, 它基本上不受局域噪声的影响, 具有很强的天然容错功能.

(ⅳ) 绝热量子计算模式. 该方案最早为美国 MIT 的 Goldstone 等人所提出[66]. 该方案的核心思想是通过绝热演化特征来等效地实现量子幺正变换: 如果将系统冷却到零温, 则系统处于体系的基态(我们假定基态没有简并), 此时, 如果绝热地改变系统哈密顿量的参数, 则体系会绝热地跟随系统演化, 如果系统不会出现基态和激发态的能级交叉, 并且绝热演化的条件始终成立, 则系统量子态会一直处于系统的基态. 但是, 由于体系的哈密顿量已经改变, 所以此基态非彼基态, 演化后的基态同初始的基态之间相差一个幺正变换, 因此, 绝热过程有实现幺正演化的功效. 该方案的优点在于: 理想情况下, 系统始终处于基态, 不存在退相干的问题. 它的缺点是: 绝热条件依赖于基态和第一激发态之间的能隙. 能隙越窄, 所需要的绝热演化的时间久越长, 如果随问题的变大, 绝热演化时间指数地变长, 那么就失去了量子计算的意义. 但是, 这个问题在 2004 年被以色列数学物理学家 Aharonov 等人解决, 他们证明了绝热量子计算同标准量子计算模型的等价性[67].

国际上围绕量子计算机物理实现的研究已经进行了十几年, 学术上取得了显著的进展. 例如, 目前操控有效量子比特数目最多的系统——离子阱系统, 已经实现了 14 个量子比特的纠缠态的制备[68]. 从世界范围内的研究趋势来看, 人们对于实现量子计算物理系统的探索, 从开始时的百花齐放, 到现在的有所侧重. 虽然, 即使到现在人们还不能确定地回答, 未来的量子计算机究竟会在哪种物理系统中实现, 但研究的焦点渐渐移向容易实现器件化和产品化的固态物理系统, 如超导约瑟夫森结系统、半导体量子点自旋系统、金刚石 NV 色心系统、集成光子学系统等.

下面我们简单介绍一下当前国际上量子计算物理实现研究的几个热点体系.

(ⅰ) 超导约瑟夫森结系统. 超导量子计算的核心元件是超导约瑟夫森结, 这是一种“超导体-绝缘体-超导体”的三层结构, 其中的绝缘层很薄, 一般不超过 10 nm, 这样的厚度可以使得两块超导体内的库珀对产生相互的隧穿, 从而使得两块超导体的波函数的相位差根据器件的外界电磁偏置产生确定的联系. 这种约瑟夫森隧穿效应, 是构建和调控超导量子比特的物理基础.

自 1997 年第一个基于超导量子比特的理论方案被提出以来[69], 到目前为止, 按照所调控的物理自由度的不同, 超导量子比特被分为相位量子比特[70,71]、磁通量子比特[72~74]和电荷量子比特[75,76]三大类型. 它们的物理构建和能级结构的示意图见图 6. 同传统的原子光子之类的天然量子体系相比较, 超导量子比特系统具有以下特点: (1) 超导量子比特的能级结构依赖于超导量子电路的具体设计和外加电

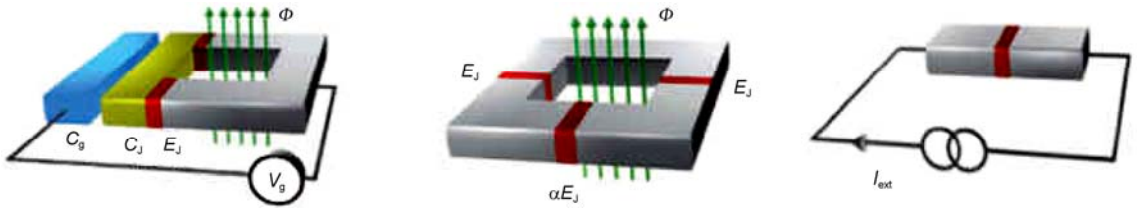

图 6 超导电荷、磁通、相位量子比特示意图

磁信号的控制，我们可以将其称为人工原子；(2) 基于现有的微电子制造工艺，约瑟夫森结量子电路具有良好的可扩展性，易于实现大规模量子比特的集成化，同时也易于实现同其他量子体系之间的耦合. 自 20 世纪 90 年代末以来，围绕上述 3 种类型的超导量子比特的实验研究被广泛开展，日本、美国和欧洲的研究组相继实现了单个量子比特的表征[70,74~76]、两量子比特的受控逻辑操作[77~79]和 3 个量子比特的简单逻辑电路的实现[80,81]. 值得一提的是，南京大学的孙国柱和于扬以及堪萨斯大学的韩思远等人在一个超导比特和两个两能级体系相耦合的系统中，实现了三量子比特系统的相干调控[81]. 而世界上最早的超导相位量子比特的表征和操控，是于扬和其导师韩思远教授在堪萨斯大学完成的[70].

目前，除了升级量子比特的数目之外，超导量子计算的另外一大趋势是：构建超导量子比特同超导微波腔中的微波光子比特之间相互耦合的杂化量子系统. 这个概念最早由耶鲁大学的 Schoekopf 等人提出[82]：超导电荷量子比特被放置在由三个平行的超导平板构成的传输线腔中，通过耦合电容来实现电荷量子比特同传输线腔中的电磁模式之间的耦合. 这里，传输线腔既可以作为操控器件来实现对单个量子比特的操作，又可以作为数据总线，实现远距离的两个量子比特之间的信息传递. 2004 年, Schoekopf 小组实现了传输线腔和电荷量子比特之间的共振强耦合，实验上观测到了强度为 12 MHz 的真空 Rabi 劈裂，远远大于传输线腔和量子比特的退相干强度[82]. 2007 年，美国 NIST 和耶鲁大学的实验组，在实验上实现了利用超导传输线腔耦合两个远程量子比特的实验. NIST 的小组实现了在共振强耦合区域内，两个超导相位量子比特通过传输线腔的耦合[83]；而耶鲁大学的小组实现了两个电荷量子比特在大失谐区域内的耦合[84]. *Nature* 杂志以“catch the quantum bus”为封面报道了这两个结果.

最近，加州大学河边分校和圣芭芭拉分校的研究者们更是提出了超导量子计算的 RezQu(振子-零态量子比特)构建[85](见图 7). 其基本想法是：将每个量子比特分别同两个超导传输线腔耦合起来，其中一个传输线腔作为存储器，另外一个传输线腔作为所有量子比特的数据总线. 量子比特的能级是可以调节的，通过调节量子比特的能级，与不同类型的传输线腔模共振，从而可以实现量子信息在存储器-量子比特，或是数据总线-量子比特之间交换. 如果一个量子位处于闲置状态，则该处的量子比特处于零态，量子信息被存储在存储器中，如果该处的量子比特需要进行单比特操作，则将存储器中的信息交换到量子比特上，再对量子比特进行操作，操作完成后再重新存储到存储器中. 如需实施两个量子位的操作，则将信息交换到量子比特上之后，调节量子比特的能级，将其同数据总线中的振子模式共振，通过量

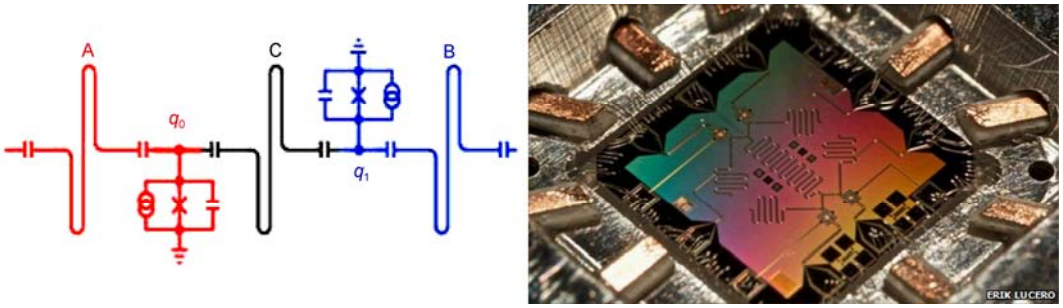

图 7 超导 RezQu 构建示意图及其超导芯片照片

子比特-数据总线-量子比特的交替作用, 实现两个量子位的逻辑门操作. 该构建方案的优点是, 除了能够保持超导电路良好的可扩展性之外, 由于用作存储器的量子振子的退相干时间要长于超导比特的退相干时间, 所以系统的相干性能够得到很好地保持. 2011 年, 2 个量子比特的 RezQu 处理器已经在实验上获得实现, 并且实施了 Noon 态的制备[86]. 进一步, 该小组实现了量子的 Von-Neumann 架构[87].

除了上述对于量子计算进行系统性地构建之外, 在超导量子比特系统中的单元技术的研究方面, 也取得了很大的进步. 例如, 在最初的超导量子计算的方案中, 比特之间的耦合是不可调节的, 虽然采用适当的方式可以加以克服[88,89], 但是会大大增加门操作的复杂程度. 在 2006 年, 人们在实验上实现了两个超导磁通量子比特之间的可控耦合[90], 其原理是使用第三个量子比特作为耦合器件, 通过对耦合器件能级的射频调制来有效开关两个量子比特之间的相互作用. 在实验中, 量子门的开关比达到了 19. 近年来, 随着材料加工和器件制备工艺的提高, 超导量子比特系统的退相干时间也被大大延长, 在电荷量子比特系统中, T1 达到了 60 μs, T2 达到了 14 μs.

超导量子比特系统, 除了用于标准的量子计算模型的探索之外, 还是绝热量子计算模式的可能候选者. 通过构建耦合的磁通量子比特阵列, 该系统可以模拟量子伊辛相互作用模型, 通过调节系统的控制参数, 可以对这个多体哈密顿系统进行绝热演化, 来寻找变参数情况下体系的基态. 这种所谓的量子退火算法, 可以用于解决特定的数学问题. 2011 年, 加拿大 D-wave 公司实现了 8 比特的量子退火算法[91].

由于超导系统具有高度可控性和易集成的优点, 它也有可能成为检验拓扑量子计算模式的候选体系. 验证拓扑量子计算的第一步是获得具有非阿贝尔统计的任意子激发. 复旦大学游建强等人近来提出在超导约瑟夫森结阵列中操纵和探测 Majorana 费米子的方案[92]. Majorana 费米子是一种已被人们预言但迄今尚未发现的具有非阿贝尔统计的准粒子, 如能在实验体系中探测和证实, 具有重要的学术价值.

(ⅱ) 半导体量子点自旋系统. 在量子计算中, 通常用作量子比特的半导体量子点有两种, 一种被称为“自组织生长的量子点”, 一种被称为“门控量子点”. 这里, 我们主要介绍基于门控量子点量子计算的研究进展.

1998 年, 瑞士巴塞尔大学的 Loss 和美国 IBM 研究院的 DiVincenzo 提出基于门控量子点上操纵单电子自旋的量子计算理论方案[93]. 所谓门控量子点是指, 使用分子束外延方法生长出高纯净和高迁移率的 GaAs-AlGaAs 半导体异质结晶片, 在其上刻蚀出金属门电极, 在门电极上加负压, 排空在门电极周围的二维电子气, 形成一个电子受限的空间, 使得只有少数电子, 甚至是单电子, 在百纳米大小的区域内运动. 当只有单个电子被放置在这个受限空间中时, 系统很像一个氢原子. 在外加磁场的作用下, 由于塞曼效应, 每个电子轨道会劈裂成自旋向上和自旋向下的两能级结构, 我们以此来表示量子比特中的 0 和 1. 量子比特之间的相互作用可以通过控制两个量子点区域之间的门电极的电压来实现, 这等效调控了两量子点区域的电子云之间的交叠(见图 8).

由于该系统继承了传统的半导体加工工艺, 具有很好的可集成性, 世界上多个著名的研究机构在基于半导体量子点的量子计算研究方面取得了一系列重要的进展, 如量子比特的制备、量子逻辑门的操作、量子测量和量子相干性都已经在实验中获得了成功的演示[94~106]. 2004 年, 荷兰 Delft 大学的 Kouwenhoven 研究组首先实现了量子点上自旋量子比特的表征[94].

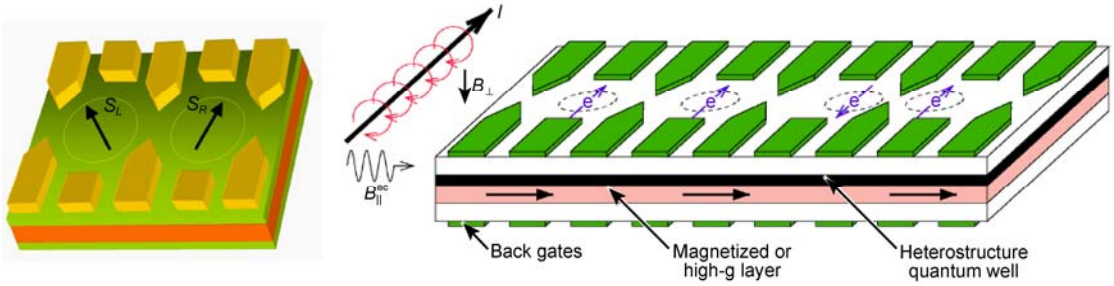

图 8　通过门控量子点实现量子计算的示意图

他们将单量子点放置在稀释制冷机中, 在 15 mK 环境中加一个 10 T 的强磁场, 使得塞曼能的劈裂达到 200 μeV, 这个能量比热能要大近一个数量级, 但是又小于轨道能级间隔和充电能. 从而, 在该系统中很好地孤立出一个两能级系统. 同样, 在 2004 年美国加州大学洛杉矶分校的姜宏文研究组和 Kouwenhoven 研究组, 用量子点接触的方法同时实现了对单量子点样品中自旋本征状态的读取[94,103]. 2005 年, 哈佛大学的 Marcus 研究组在一块双量子点样品中, 通过调控连接两个量子点区域的电极上的电压, 等效实现了两个受限空间中电子波函数之间的交叠程度的调控, 从而实现了平方根交换门的操作[95]. 2006 年, Kouwenhoven 研究组同样在一块双量子点样品中, 实现了用射频场对其中一个量子点中的自旋比特的单比特操作, 在 100 ns 的时间内观测到自旋比特的多个周期的 Rabi 震荡, 显示了自旋量子比特的量子相干性[96]. 2008 年, 日本的 Tarucha 研究组用一个倾斜的塞曼场, 实现了对样品中单个电子自旋的共振操作[106]. 这两类操作的实现, 就构成了量子计算的普适量子逻辑门集. 2007 年底, 荷兰 Delft 大学的 Vanderspyen 研究组在同一块半导体量子点器件上用全电学技术实验实现了量子计算的全部要素: 量子比特的制备、量子门的操作、量子测量和量子相干性的演示(见图 9)[100]. 该系统退相干的特征时间 T1 在 1 ms 左右[94], T2 在 10~25 ns 左右[96~98], 通过自旋回声和动力学极化核自旋的手段, T2 可以延长到 1 μs 左右[95,99], 从而能够在自旋退相干的时间之内完成多于 10^5 个平方根交换门操作, 这在所有固体系统中是相当高的.

目前, 该领域的研究趋势是设计和实现一些新的结构, 提高门操作的效率和精度, 同时进一步寻求新的高性能材料, 使自旋量子比特获得更长的相干时间. 在新结构的设计和探索方面, 哈佛大学的 Marcus 研究组最近通过电容耦合实现了两个双量子点之间的内部控制[107]. 中国科学技术大学郭国平研究组也曾经提出用超导传输线腔作为数据总线, 来耦合量子点自旋比特的方法[108,109], 引起了国际上实验组的关注. 近来, 在探索新的高性能材料方面迎来了契机, 人们开始关注一些具有零自旋背景的材料, 如 Si/SiO_2[110], Si/SiGe[111], Ge/Si 纳米线[112], 碳纳米管和石墨烯[113,114]等, 人们预言零自旋背景能使门控量子点中的自旋比特具有更长的相干时间.

我国在门控量子点自旋比特的研究上起步很晚, 从事这方面研究的主要是中国科学技术大学量子信息实验室的郭国平研究组, 但是近年来他们取得了长足的进步. 例如, 他们实现了在 Ge/Si 纳米线量子点上对自旋状态的超高速处理[115], 在世界上首次制备了处理石墨烯量子点附近的单电子晶体管结构, 并利用该单电子晶体管作为测量装置, 读出了量子点上的电子状态[116].

(iii) 金刚石 NV 色心系统. 在金刚石中, 氮原子可以取代其中一个碳原子, 并与邻近的碳空位形

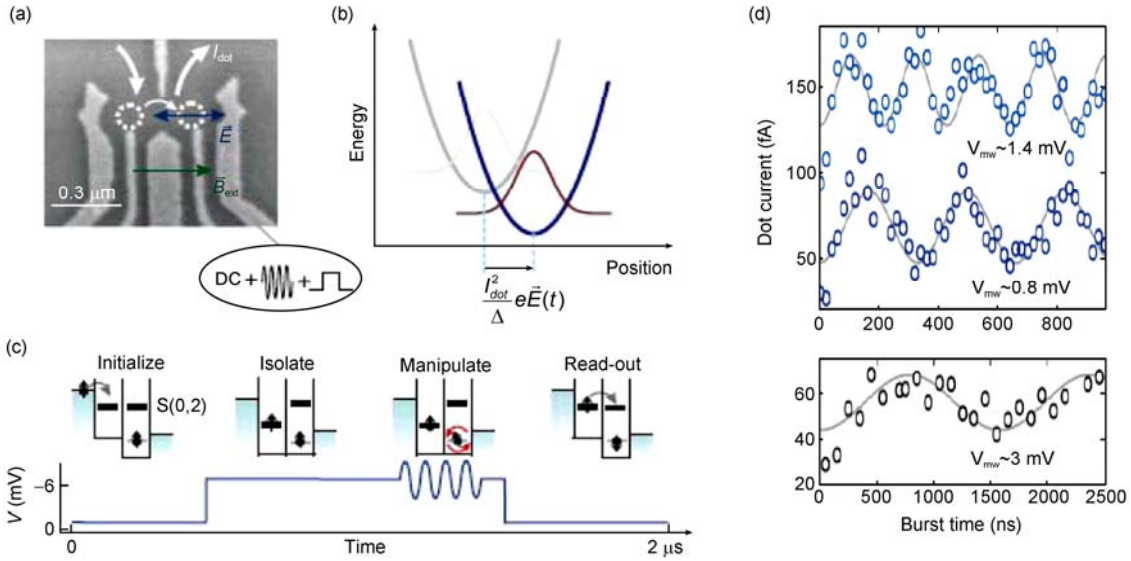

图 9 同一块半导体量子点器件上实现量子计算的全部要素所采用的实验装置、原理和结果

成一个 NV 色心. 带负电荷的 NV 色心光学跃迁远离金刚石材料自身的能级跃迁, 不会被金刚石吸收并具有良好的光学性质, 其激发态与基态间跃迁的零声子线在 637 nm 左右, 带宽几十兆赫兹, 自发辐射速率达百兆赫兹. 同时, 金刚石 NV 色心拥有良好的电子自旋能级, 其基态间磁共振跃迁对应 2.88 千兆赫兹, 室温下电子的相干时间就达毫秒量级. 实验上 NV 色心的跃迁频率可以通过电场和磁场方便地调节; 同时可以利用光学探测磁共振方法测量电子所处的状态, 并可以利用光学方法实现初态制备以及利用光学或者微波相干控制其能级跃迁. 此外, 金刚石中的单个 NV 色心可以电子束或离子束注入实现在几纳米内的定点制备, 辅以成熟的微纳光学加工工艺, 制备各种金刚石微腔和微纳结构, 可以实现基于金刚石材料的可集成化的量子信息操作. 国际上, 德国的斯图加特大学、美国哈佛大学以及美国加州大学圣芭芭拉分校在利用金刚石 NV 色心研究量子信息技术方面获得了众多成果.

金刚石中的 NV 色心可以通过共聚焦显微方式进行探测, 单个 NV 色心即是良好的单光子源[117], 脉冲宽度几个纳秒, 对应数百兆赫兹的发射效率. 实验上已经利用光学微纳结构, 如微环腔[118]、光子晶体腔、微柱和微透镜等提高光子发射速率以及收集效率. 此外, 利用光学泵浦, 可以把 NV 色心的制备在 m_s=0 的基态上; 与此同时, 利用电子能级的跃迁选择定责, 通过自发辐射荧光的探测, 可以识别电子处于 m_s=0 或 m_s=±1 态上. 实验上已经可以直接利用光学泵浦方式调节电子跃迁[119], 并已经观察到的两个 NV 色心发出荧光的双光子干涉现象. 产生了光子态与电子能级的纠缠态, 并通过对光子的塌缩测量, 实现两个远距离 NV 色心的纠缠[120], 为实现基于 NV 色心的可扩展量子信息操作提供了良好方式.

NV 色心电子能级在 m_s=0 与 m_s=±1 间的磁共振跃迁对应 2.88 千兆赫兹, 因为碳-12 的核自旋是零, 其相干时间较长, 普通的 NV 色心可达十微秒量级; 而在高纯度样品中, 可以利用动力学去耦方式, 把相干时间延长到毫秒(其能级及寿命示意图见图 10). 因此, 室温下就可以利用微波进行电子态的相干操纵, 实验上观察到单个 NV 色心的拉比振荡, 并可以实现电子态的单比特旋转操作, 操作频率可达千兆赫兹[121]. 中国科学技术大学杜江峰研究小组在研究 NV 色心的相干性方面做出了重要成果, 并实现了量

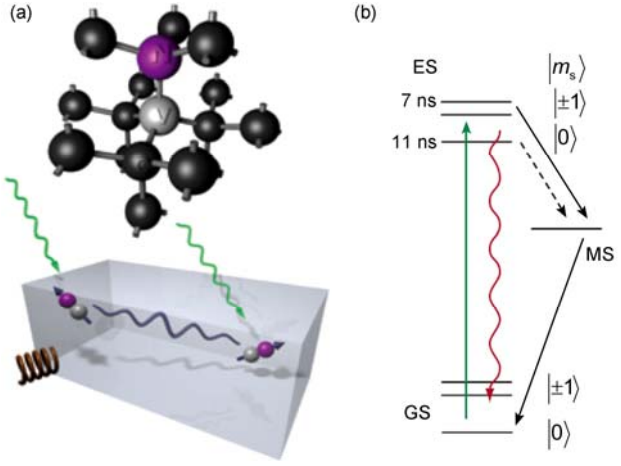

图 10　金刚石 NV 色心的能级及其寿命示意图

子算法的演示[122]. 通过与周围核自旋的耦合, 实验上已经实现了三个量子比特的纠缠[123]. 进一步, 可以把电子自旋态耦合到更长相干时间的核自旋中, 实现量子信息的存储.

利用基于能级寿命测量和其他光学探测技术, 可以实现间隔在数十纳米之内的相邻 NV 色心的识别和独立控制[124]. 而当两个 NV 色心间距在数十纳米之内, 它们之间偶极相互作用很强. 实验上已经观察到相邻 NV 色心之间的相互作用, 实现了两个 NV 色心的纠缠态[125]. 与此同时, 利用离子束注入, 可以控制 NV 色心在纳米尺度的精确制备, 并形成 NV 色心的晶格, 实现可扩展的 NV 色心系统.

此外, 实验已经实现了金刚石 NV 色心与光学微腔、微波超导腔[126]和纳米机械振子[127]的相干耦合. 室温下, 金刚石中的 NV 色心就可以实现从核自旋到光学的不同体系的相干耦合, 频率范围从微波频率到光学频率. 因此, NV 色心不仅仅自身可以用于量子信息操作, 还为未来实现可能的光学、机械振子、电子以及核自旋的杂化体系提供了良好的媒介. 因此, 不同 NV 色心间的耦合及可扩展性、NV 色心与其他体系的耦合, 以及可以利用现代微纳加工技术实现金刚石材料微纳结构[128]和高精度、高效率 NV 色心的产生, 是下一步研究的重点.

(ⅳ) 其他物理系统. 除了前面介绍的几种固态体系以外, 原子-分子-光物理系统也是研究量子计算的主流体系. 我们分别做简单的介绍.

离子阱系统, 是世界上最早尝试实现量子计算的物理体系. 该体系实现量子计算的理论方案最早

由 Cirac 和 Zoller 于 1994 年提出[129], 同年, 美国 NIST 的实验组就开始了该方向的研究. 目前, 无论从操控量子逻辑门的精度还是比特数目, 离子阱系统都达到了各个物理体系之冠. 2010 年, Innsbruck 大学的 Blatt 小组, 在线性离子阱系统中实现了 14 个离子的 GHZ 态的制备和 64 个离子的分辨, 结果发表在 2011 年的 *Physical Review Letters* 上[68]. 这是到目前为止人类相干操控量子比特的记录. 但是线性离子阱存在升级量子比特数目的困难. 首先, 当离子数目大时, 很难平衡掉离子间的库仑斥力而将其束缚在一维方向上; 其次, 寻址和逻辑门操作也会带来很大的困难. 为了能够升级量子比特数目, 同时解决系统集成性的困难, 美国 NIST 和马里兰大学的实验组在尝试采用芯片阱的技术, 将离子分段存储在不同的芯片阱区域里, 需要相互作用时, 再将拟进行相互作用的离子移动到相互作用区中来完成操作[130,131]. 另外一种更具潜力的做法是, 利用光子来连接不同芯片阱中的离子[132], 目前, 马里兰大学的 Monroe 研究组正在为此而努力. 就目前的趋势看, 基于离子阱的量子计算技术将在很多年之内领先其他物理体系. 我国在这个方向上起步较晚, 在 2011 年中国科学院武汉物理与数学研究所的冯芒、高克林研究组在线性离子阱中实现了 8 个 Ca 离子的囚禁.

中性原子系统. 在 1998 年[133]和 1999 年[134,135], 人们提出通过光学晶格束缚冷原子系统用于量子计算和量子模拟的方案. 由于中性原子整体不显电性, 不易受到外界电磁环境的干扰, 系统退相干的时间很长, 而由激光干涉所形成的周期势场可以将大量的冷原子束缚在光学晶格上. 这是目前所知最佳的量子模拟平台(关于量子模拟见下文). 但是在这个系统上实现真正意义的大规模的量子计算有很大难度. 一方面, 由于光晶格的周期为激光的二分之一波长量级, 所以很难再用激光寻址单个晶格格点, 来完成单比特的操作; 另一方面, 由于中性原子不显电性, 往往需要碰撞相互作用来诱导量子比特间的作用, 但是基于超交换作用所诱导的两体相互作用的强度太小, 很难在原子的退相干时间内完成大量的门操作(虽然原子的退相干时间很长). 现在, 人们在实验上已经克服了单格点寻址的困难[136]; 对于改善相互作用强度, 原则上可以利用里德堡原子高激发态的大的电偶极矩来诱导强的两体作用[137,138]. 但目前实验上还没能综合这些技术. 中国科学院武汉物理与数学研究所的詹明生研究组在从事基于中性原子的量子计算的实验研究, 目前他们在这个方向上已经取得了若干进展: 完成了用蓝失谐的偶极光阱囚禁了单个原子[139], 能够操控单阱-双阱的转移, 实现阱中装载双原子的效率达到 90%以上[140], 实现了在环形光晶格中 2~6 个原子的环形阵列.

线性光学系统. 2000 年, 由 Knill-Laflamme-Milburn 提出基于线性光学系统的量子计算方案(简称为 KLM 方案). 该方案提出, 仅需要优质的量子光源、高品质的单光子探测器, 再辅以线性光学器件的操作, 即可实现普适的量子计算[141]. 此外, 单向量子计算模式的实验验证也多在线性光学系统中实施. 中国的研究组在该方向的实验研究中走在世界前列. 2007 年, 潘建伟研究组在线性光学系统中实现了 Shor 算法的 15=3×5 分解[142]; 同年, 他们完成了 6 光子 cluster态的制备[143], 并先后在 cluster 态和非 cluster 态的情况下验证了单向量子计算模式[144,145]. 山西大学的张靖研究组, 将分离变量的 cluster 态的概念扩展至连续变量[146], 2007 年他们依据所提出的理论方案实验产生了连续变量的 4 组分链式 cluster 态[147].

由于篇幅所限, 关于量子计算的物理系统, 我们简单介绍到这里.

前面我们所介绍的 4 种量子计算的模式, 各有各的优势. 目前, 除了拓扑量子计算模式之外, 其他量子计算模式, 在少数几个量子逻辑比特的前提下, 都做了实验的验证, 实现了简单的逻辑门操作. 而对于拓扑量子计算而言, 虽然其特有的容错方式具有迷人的前景, 但是如何在实验上实现那些具有非阿贝尔任意子统计的量子多体系统, 是一个很大的挑战, 这不仅仅是对于量子计算, 对于基础理论也具有非凡的意义. 进一步, 如何有效升级量子计算的规模到多量子比特系统, 进而从计算速度上超越现有的经典计算机, 这是一个非常难的挑战, 对于任何一种计算模式都有很长的路要走.

在这一部分的最后, 我们来谈一下量子软件. 如果量子计算的硬件研究获得真正的突破, 大规模的量子信息处理能够获得实施, 那么量子软件的开发必将处于一个非常关键的地位. 由于量子系统与经典系统的本质差别, 现有的软件技术无法应用于量子计算机. 发展量子软件的一个基础是量子程序设计语言的理论和实现.

1996 年美国国家标准技术研究所 Knill 提出将量

子算法转化为伪代码的一系列基本原则, 这些原则对于后来量子程序设计语言的设计产生了很大的影响. 而第一个量子程序设计语言, 于 1998 年为奥地利维也纳工业大学的 Ömer 所提出, 它包含一个相当完整的经典子语言[148]. 随后, 很多经典程序语言的量子扩展被相继提出. 2003 年, 美国华盛顿大学计算机科学与工程系的 Oskin 与 Petersen 提出描述量子程序的量子代数, 试图为量子程序设计语言提供代数基础[149].

由于量子信息的特殊性, 很多在经典信息世界中能够完成的任务, 到了量子信息世界则变为不可能. 例如, 对比特信息的拷贝操作. 在经典世界中, 比特信息是可以被克隆的, 但是在量子世界中, 存在不可克隆原理, 即不存在一个普适的物理过程对任意的量子状态进行克隆操作[150]. 2004 年, 美国 Brown 大学的 van Tonder 利用线性逻辑的 type 系统建立量子 Lambda 演算, 希望克服量子不可克隆原理在量子程序中引起的困难[151].

对于计算机程序而言, 如何验证程序的正确性非常重要. 而量子世界与人类直觉有很大的不同, 这使得量子程序设计比经典程序设计更容易出错. 因此, 量子程序验证甚至比经典情况下的程序验证更为重要. 在经典情况下, Floyd-Hoare 逻辑是程序验证的基础[152,153], 在程序设计方法学中处于核心地位. 在量子计算领域, 国际上多个研究组试图建立量子程序的 Floyd-Hoare 逻辑, 但都没有成功. 在 2009 年, 清华大学的应明生教授彻底解决了这个问题, 建立了量子程序的完整的 Floyd-Hoare 逻辑, 并证明了其完备性[154].

鉴于目前物理系统中升级量子比特的困难, 分布式的量子计算是绕过这样障碍的一种可能途径, 即用中度规模的量子处理器作为量子信息处理终端, 不同终端之间用量子通信协议建立联系. 在经典计算领域, 进程代数是通讯协议验证的重要工具. 为了给量子通讯协议验证提供必要的形式化方法, 国际上多个研究组开展了进程代数的研究, 但是没有解决并行算子保持互模拟的问题. 2010 年, 应明生和冯元等人提出了一类新的量子进程代数解决了这个问题[155,156].

4 量子模拟

所谓量子模拟, 就是指在一个人工构建的量子多体系统的实验平台上去模拟在当前实验条件下难以操控和研究的物理系统, 获得对一些未知现象的定性或定量的信息, 促进被模拟的物理系统的研究. 量子模拟的概念最初由诺贝尔奖得主费曼于 1982 年提出[56]. 费曼最初意识到, 由于支配微观世界的基本规律是量子力学, 所以要想模拟一个微观多体系统的演化, 需要求解多体的薛定谔方程. 费曼发现, 这对于经典计算机来说, 是不可能完成的任务. 主要原因在于, 量子多体系统需要由量子波函数刻画, 而波函数所处的 Hilbert 空间的维数随量子客体的数目指数增长, 而经典计算机的存储空间根本不足以存储波函数的信息, 所以, 也就无法刻画系统演化的规律. 费曼当时的一个想法是: 如果我们所用于模拟的机器本身就是服从量子力学规律, 即机器的状态也由量子波函数来刻画, 我们用人工方法来控制机器, 使之具有与被模拟对象相同的等效哈密顿量. 于是, 我们就可以用这台“量子模拟机”来模拟量子多体系统的演化.

但是, 量子模拟作为一个研究热点则兴起于 1998 年, 这一年, Jaksch 等人提出用光学晶格中束缚的冷玻色原子来仿真 Bose-Hubbard 模型[133]. 通过对光学晶格的调控, Bose-Hubbard 模型哈密顿中的参数可以在很大范围内被随意调控, 于是可以观测体系从 Mott 绝缘态到超流态的量子相变. 这开创了采用人工量子平台来模拟强关联体系量子相变的先河, 近十年来, 产生了大量的理论工作. 迄今为止, 量子模拟的研究内容十分广泛, 除了模拟多体系统的演化、强关联系统的量子相变之外, 还可能被用于模拟物态方程、各种规范场、量子化学、中子星和黑洞、理论上预言但是尚未被观测到的准粒子, 以及新的物质的态等.

目前, 用于量子模拟可能的物理平台大致可以分为原子、离子和电子三类. 原子系统中除了被人们所熟知的光晶格束缚冷原子系统外, 还有微腔束缚原子的阵列系统等; 离子主要是指离子阱系统; 电子有超导约瑟夫森结阵列系统、量子点自旋的阵列系统以及液氦表面的电子系统等(见图 11)[157]. 在当前的这些可能候选者中, 冷原子系统以其独特的优势, 处于上述所有提及的系统中最优越的地位. 首先, 在现有的技术条件下, 它是目前所有提及的系统中唯一能够对大量粒子进行初始化的体系. 其次, 该系统具有很好的可调节性. 以光晶格束缚冷原子为例, 晶

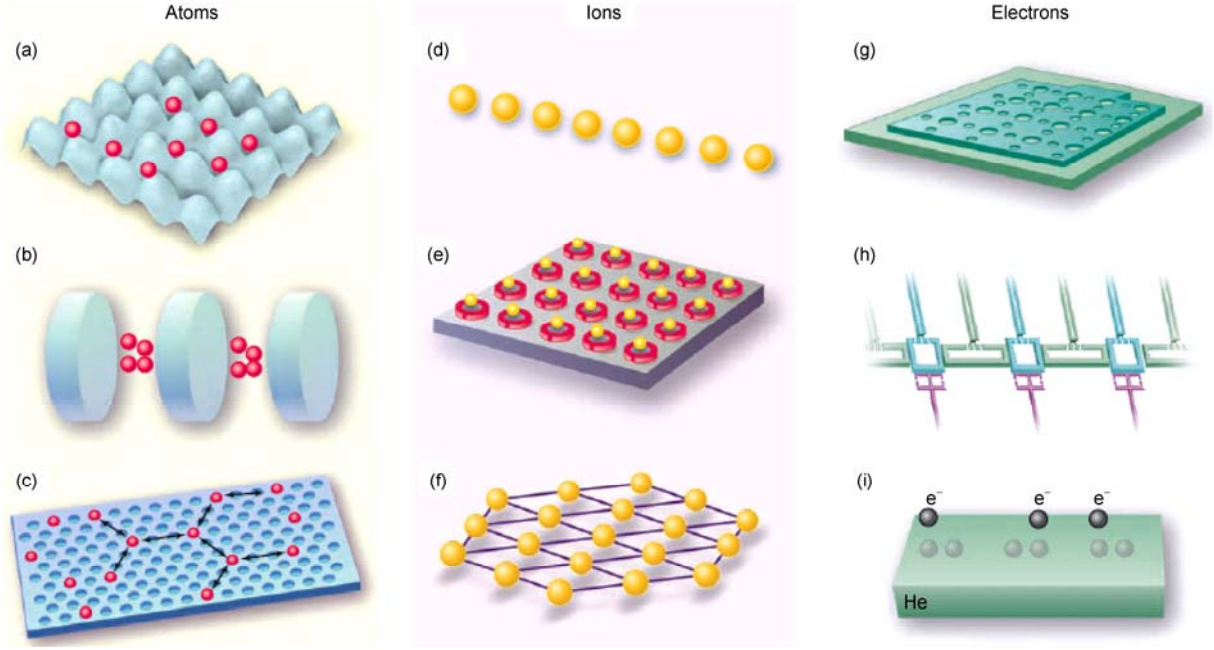

图 11 潜在的可以用于实现量子模拟的物理系统

格的维度、晶格参数和几何以及格点间的隧穿强度, 都可以通过调节光晶格势场来实现; 而粒子之间的散射强度, 则可通过 Feshbach 共振技术来调节; 此外, 人们还可以自由地控制原子的组分. 到目前为止, 人们操控冷原子晶格的能力也越来越强, 例如 2011 年, 德国的 Bloch 研究组已经实现了单原子的成像和寻址[136]; 美国的 Greiner 研究组利用单格点成像技术, 成功地模拟并探测了一维反铁磁自旋链[158], 这是继模拟 Bose-Hubbard 模型的量子相变以来, 量子模拟领域最重要的实验进展; 同样是2011年, 人们实现了二维经典阻挫模型的模拟[159].

采用冷原子系统进行量子模拟的先决条件是: 首先要对原子系综进行一系列的激光冷却和蒸发冷却, 使其达到几 nK 的温度. 这时, 对于玻色子而言, 将处于玻色-爱因斯坦凝聚(BEC)的状态; 对于费米子, 则处于量子简并的状态. 这时, 原子的相对热运动被高度抑制, 由于原子间相互作用所导致的量子特性则被显现出来. 我国的冷原子技术经历了几十年的发展, 目前已经逐渐追上了世界的步伐. 目前, 已经有中国科学院上海光学精密机械研究所、北京大学、中国科学院武汉物理与数学研究所、中国科学院物理研究所、中国科学技术大学等多家单位在实验上实现了 BEC, 山西大学的张靖研究组实现了费米子的量子简并. 目前, 张靖研究组和中国科学技术大学陈帅研究组已经在规范场的量子模拟方面取得了很好的实验进展. 另外, 中国科学院物理研究所的刘伍明研究员在早期冷原子相干性质的研究中取得了非常重要的理论进展, 他与合作者在理论上描述了玻色爱因斯坦能聚态的干涉现象[160], 在理论上预言可调幅和调频的原子激光[161], 发现分数量子涡旋晶格[162]等.

除了冷原子系统之外, 目前离子阱系统已经显示出实施中度规模的量子模拟的潜力. 如奥地利 Innsbruck 大学的 Blatt 研究组于 2011 年在线性离子阱中实现了开放系统的量子模拟器[163]和普适的数字式量子模拟[164]. 由于二维离子阱阵列原则上是可以实现的, 所以 10^2 量级的多体系统的量子模拟有可能在量子阱系统中获得实现. 在固态系统中, 超导约瑟夫森阵列系统目前最接近实现中度规模的量子模拟的目标.

另外, 量子模拟也有可能被用来研究少体系统. 例如, 对于相对论量子力学的很多预言难以在实验上真正观测到. 但是人们有可能以量子模拟的方式, 在低速系统中构建相对论的量子力学方程的演化, 进而观测量子模拟的结果. 这方面, 华南师范大学的朱诗亮等人, 提出了在冷原子系统中模拟相对论量子力学中的 Klein 隧穿效应[165]. 中国科学技术大学的杜江峰研究组, 在核磁共振系统中通过量子模拟

的方式获得了氢分子的基态能量[166], 模拟了化学中异构化反应的动力学[167]. 潘建伟研究组用 6 光子系统制备了图态去模拟阿贝尔任意子系统的编织效应[168]等.

从技术上讲, 量子模拟平台同量子计算机紧密相关, 量子比特数目可升级也是对两者共同的要求. 对于用作量子模拟的系统, 在操控难度和相干时间长度上的要求比量子计算低很多, 于是人们预期量子模拟机很有可能在实现大规模的量子计算之前而获得实际的应用, 有可能对物理学、化学、材料化学等学科产生重要的影响, 甚至有可能促成材料科学、能源等重要问题的解决.

5 量子度量学

人类的发展进程从某种意义上讲就是测量技术不断发展进步的过程. 从早期用手或者脚等的长度作为长度单位, 到目前人们通常使用的直尺、卷尺、游标卡尺等, 人类的测量精度得到了大大的提高. 在科学实验以及一些重要的应用中, 人们利用光的干涉以及激光等手段大大提高了测量的精度. 测量精度的提高不仅可以用来验证已有的物理学理论, 而且可以推动新的理论和技术的发展. 例如, 通过相位测量的方式可以以亚波长的精度测量任意一个相对位移, 这样的方法已经被运用到了宇宙学、纳米科技和医学等领域.

受经典物理学本身特性(如散粒噪声等)的限制, 经典度量学的发展目前已经接近经典物理所能达到的极限——标准量子极限(standard quantum limit, SQL). 人们希望能够找到另外一种方法或者系统来突破经典物理学的限制, 进一步提高测量的精度. 20 世纪初发展起来的量子力学, 尤其随着近二三十年来量子信息学的发展[169], 人们对量子纠缠态的性质、制备、控制以及测量方面做了大量的研究, 得到了丰富的研究成果. 近来, 人们利用量子态(特别是量子纠缠态), 结合经典度量学的方法与量子力学的特性, 使得测量精度在一些领域大大突破了经典物理极限(SQL). 例如, 对任意微小位移(在光学中表现为相位变化)的测量精度在某些情况下已经逼近量子力学极限——海森堡极限(Heisenberg limit)[170~172]. 这种利用量子力学方法, 尤其是利用到量子纠缠, 研究如何对物理系统中某个物理量进行更精确测量的研究方向叫量子度量学[173]. 量子度量学向人们承诺发展相比于经典度量学更为精确的测量技术. 目前量子度量学的研究主要集中在量子时钟、量子高精密相位测量、量子成像等领域.

(ⅰ) 原子钟. 为了提高时间(频率)的计量精度, 人们一直在寻求一个更准确的时间频率标准. 量子力学和微波波谱学的发展促成了原子钟的实现. 1936 年, Rabi 在哥伦比亚大学提出了原子和分子束谐振技术理论[174], 并实验得到原子跃迁只与其内部固有特征相关而与外界电磁场无关的结果, 提供了原子跃迁作为频率标准的可能性. 1948 年 Smith 和 Lyon 在美国国家标准局利用 Rabi 的理论做成了第一台氨分子钟, 但这个钟是吸收型的, 因为多普勒效应, 其长期稳定度也只有 10^{-7}, 没有实用价值. 但是, 随着技术的发展, 原子钟的精度有了极大的提高. 1996 年法国国家标准实验室(LPTF)的 Clairon 和法国高等师范大学的 Salomon 建成了基于冷原子喷泉概念的第一个铯原子时间频率基准[175]. 当前这种基准的不确定度已经进入 10^{-16} 量级[176].

随着飞秒激光的出现, 可以直接通过拍频法测量激光的绝对频率, 使光频与飞秒光梳结合为钟成为可能. 基于各种元素的光频标研究成为时间频率领域的新热点. 光钟与微波钟类似, 只是光钟的原子被激光冷却囚禁到很低的温度以消除跃迁的多普勒增宽, 然后用钟激光进行探测. 钟探测光频率锁定在原子的跃迁共振线上, 作为光钟的振荡器. 光钟又有离子光钟、原子光钟和光晶格光钟三种形式. 目前光钟的不确定度已经做到了 10^{-18} 量级[177].

近来, 人们开始考虑利用量子关联以及量子纠缠等特性进一步提高光谱测量的精度. 最近奥地利的 Roos 等人[178]利用无消相干子空间和特殊设计的纠缠态实现了对势井中的两个钙离子(Ca^+)光谱的精确测量. 研究发现, 通过利用纠缠态可以消除电四极移位的问题. 该研究为人们提供了一种光频标研究的新方法.

中国科学院上海光学精密机械研究所的王育竹院士研究组最近在小型星载原子钟的基础研究方面取得了若干进展. 他们将量子信息存储的技术应用到原子钟, 将探测光信息存储于原子介质中, 将光的信息转变为原子的自旋波. 当微波探测原子跃迁频率时, 由于已无光场存在, 消除了光场作用于原子产生的光频移效应. 当控制光诱发原子自旋波转化为信号光输出时, 信号光携带了微波探测原子跃迁的

信息(误差信息). 误差信号的探测是将粒子数差的探测转变为原子相干性的探测, 进而极大地提高了信号的对比度和信噪比, 从而改善原子钟的性能.

(ⅱ) 量子高精密相位测量. 量子高精密相位测量是利用非经典光场的特殊形式实现对任意光学相位的高精密测量, 其精度可以突破标准量子极限. 假设我们有 N 个光子, 如果这 N 个光子处于经典关联态, 那么由于输出的随机性(散粒噪声)导致了相位测量的精度将小于标准量子极限. 然而量子关联可以帮助我们克服这个限制. 20 世纪 80 年代, 人们利用压缩光场证明了这一性质[179~181]. 随后, 理论物理学家开始研究利用一般的量子态如何实现最佳的相位测量, 但是当时的实验条件无法实现利用相应的量子态进行相位测量. 最近, 随着三光子和四光子路径纠缠态 NOON 态的实验制备的成功实现, 人们又重新燃起了对量子精确测量的兴趣. 2007 年, Nagata 等人利用选择性投影测量的方式实现了利用 NOON 完成超高精度的相位测量工作[182]. 随后, 中国科学技术大学的孙方稳等人利用相似的方法得到了更高的测量精度[171].

以上工作都是对一个已知相位的起伏或者抖动的测量, 然而有时人们需要测量一个未知相位. 2007 年 Higgins 等人利用自适应测量和反馈控制的方式实现了对一个完全未知相位的精确测量, 该方法的理论精度可以达到海森堡极限[172]. 但是该工作在实验实现时, 由于多次通过相移装置而带来带宽的问题, 使得相位测量精度在更多光子的情况时大大受限. 2011 年澳大利亚 Griffith 大学和中国科学技术大学的项国勇等人利用多光子纠缠态, 改多次通过为单次通过, 利用贝叶斯分析和最优化的自适应反馈控制的方法成功解决了这一问题[183]. 该方法可以推广到利用任意的纠缠态输入.

目前, 人们开始考虑实际测量中如果有光子损耗等情况下如何实现更高精度的相位测量[184~186], 以及海森堡极限能否被突破等问题[187]. 同时量子高精密相位测量的方法已经开始被应用到物质浓度测量[188]和引力波测量中[189].

另外, 华东师范大学的张卫平研究组, 利用控制原子系综的内态相干性来实现光学相位共轭分束器, 并以此构建了非线性量子干涉仪. 他们证明该非线性量子干涉仪的条纹强度远高于同等条件下的线性干涉仪, 从而提高了相位测量的敏感度[190].

(ⅲ) 量子成像. 量子成像是近十年提出并发展起来的一个新的研究领域. 现在很多时候人们把鬼成像(ghost imaging)也叫做量子成像, 然而鬼成像完全可以用经典关联来实现, 例如现在逐步开始在军事方面用的基于鬼成像的量子雷达也可以用微波的经典关联来实现. 另外一种利用光与原子相互作用的受激发射损耗(STED)的方式进行超越衍射极限的成像方法也发展了十年有余, 已经逐步商用化. 本文所介绍的量子成像是利用量子光场实现的超高分辨率的成像.

早在 2001 年, Brambilla 等人就对自发参量下转换过程(SPDC)产生的双光子对的特性进行了详尽的理论分析. 相比于相干态, SPDC 产生两束光间的关联明显加强. 在实验上低噪声成像已经被实现. Brida 等人通过测量信号光(s 光)和休闲光(i 光)的光子数并相减, 得到了低于 shot-noise 的数据. 而 2010 年 2 月 *Nature Photonics* 刊登了 Brida 研究组关于对实际透过式图像进行低噪声成像的实验[191]. 在相同光子数的时候, 噪声达到了经典光所能到达的极限之下, 还是显示出了非经典光的巨大优势.

上面的方法只是提高了成像的对比度, 而分辨率并没有得到改进. 我们知道, 在传统的刻蚀(lithography)中, 要想减小条纹间距, 就必须减小光子的波长, 但是光子的能量(频率)必然随着增加, 当光子的能量足够高时, 就会对被刻蚀的基板和上面的物质造成损害, 而量子刻蚀束可以通过 N 个光子的纠缠特性, 得到 N 光子的整体波长为实际波长的 $1/N$. 这样, 在同样波长的条件下将条纹间距扩大 N 倍, 该方法将会在未来的芯片工业加工技术以及成像等方面有广泛的应用. 量子刻蚀(quantum lithography)的概念首先由 Scully 和 Rathe[192]于 1995 年提出, 但是该方向引起大家的兴趣是在 2000 年 Boto[193] 介绍了一种基于光子吸收的测量方案之后. 由于实验上的困难, 目前人们只能实现两光子的量子刻蚀实验[194~196]. 2010 年 Tsang[197]提出的基于质心测量的量子刻蚀方案大大提高了量子刻蚀的效率, 并且大大降低了实验难度. 紧接着, Shin 等人利用该方法实验实现了两光子的量子刻蚀, 得到了相比于标准量子刻蚀方法更高的探测效率. 当然由于 NOON 制备的困难, 更高精度(更多光子数)的实验实现还比较困难.

总之, 量子度量学利用量子力学特性, 尤其是量子纠缠, 为我们提供了更高精度的测量方法和技术.

但是要真正实用化, 如最近提出的量子雷达以及量子定时定位技术, 还有大量的基础工作以及实验技术需要解决.

6 量子信息物理基础

量子力学应用于信息科学诞生了量子信息科学, 量子信息领域的开拓者——美国 IBM 研究院的 Bennett 曾说: “量子信息对经典信息的扩展与完善, 就像复数对实数的扩展与完善一样”[198]. 近年来, 随着量子信息领域研究的不断深入, 反过来进一步推动了量子力学的发展, 丰富了量子物理的内涵, 加深了人们对量子世界的理解. 本部分主要论述量子信息的发展推动量子力学研究的若干事例, 如量子关联、基于熵的不确定关系、量子开放系统环境的控制等问题.

关联是自然界中普遍存在的现象. 在经典领域, 关联可以很好地在 Shannon 信息理论框架内进行刻画[199]. 但是在量子世界, 则不那么简单. 最初人们认识到量子纠缠是不同量子体系之间的一种特殊关联, 它不同于经典关联. 但是反过来, 量子世界中所有的非经典关联特性都是量子纠缠导致的吗? 最近, 人们认识到量子关联比量子纠缠更广泛和基础, 除了量子纠缠作为一种特殊的量子关联以外, 进一步人们发现即便是可分离的量子状态中也含有非经典关联, 即在没有量子纠缠的情况下, 量子关联依然可能存在. 人们理论上发现这种非纠缠的量子关联可以在非幺正的量子计算模型中实现计算的加速[200], 并已经在实验上获得了验证[201].

那么量子关联如何量化呢? 对于经典世界中的两个事件集, 它们之间的经典关联由两者的互信息量来定义. 对于两体量子系统, 我们可以直接推广这个概念, 用量子互信息量来刻画两体量子系统的总的关联, 这一点已经被 Groisman 等人所证实[202]. 于是, 从总的关联中剔除掉经典关联, 剩下来的就是量子关联. 但是具体如何剔除, 由于量子系统的复杂性, 人们很难给出一般性的解析形式. 目前存在几种形式化的定义, 其中非常著名的一个被称为量子失协[203]. 对于两体量子系统而言, 对其中一个子系统的测量, 将不可避免地导致对另一个子系统状态的扰动; 但对于经典系统则不然. 由于这点本质性的差别, 在经典情况下对经典互信息量存在两种等价的表达形式, 但在量子情况下, 这两种定义形式表现出不一致, 它们之间的差值被定义为量子失协.

量子失协包含量子体系中的量子纠缠和非纠缠的量子关联, 它度量了量子体系中总的非经典关联, 该概念一经提出立刻引起了广泛的关注. 目前已经证明几乎所有的量子态都含有量子失协[204]. 最近, 人们尤其关注量子失协(特别是非纠缠的量子关联)在量子信息处理过程中是如何被利用的, 包括 DQC1 的量子计算方案[200,201]以及 Grover 搜索算法[205]等, 这将有助于澄清量子方案能超越经典的真正原因. 量子失协这一概念除了在某些基本的量子信息理论方面有重要的应用之外, 在一些基本的物理问题中也起到重要的作用, 如解释麦克斯韦妖[206]和量子相变[207]等. 考虑到消相干环境, 量子失协在马尔科夫环境和非马尔科夫环境下的演化也被广泛研究. 在实验上, 中国科学技术大学中国科学院量子信息重点实验室的李传锋研究组, 利用光学系统分别研究了量子失协在马尔科夫环境和非马尔科夫环境下的演化规律[208,209], Soares-Pinto 等人也在 NMR 体系中研究了量子失协在马尔科夫环境下的演化情况[210]. 自量子失协的概念提出以后, 人们也开始从不同的角度考虑量子系统中各种关联的度量方法[211~215]. 最近, Modi 等人[216]利用距离相对熵的方法对量子体系中的各种关联进行定义. 这样, 所有的关联都能放在同一个框架内进行考虑, 并且可以直接推广到多体高维系统.

下面我们来谈一下海森堡不确定原理. 经典的海森堡不确定原理认为, 在一个量子力学系统中, 一个粒子的两个不对易的力学量(如位置和动量)不可被同时确定. 精确地确定其中一个力学量的同时, 必定不能精确地确定另外一个力学量. 最原始的不确定关系的表达式 $\Delta R\Delta S \geqslant \hbar/2$ 由海森堡提出[217], 由 Kennard 证明[218]. 此表达式只对特殊情况下成立. 一般情况下的不确定关系表达式 $\Delta R\Delta S \geqslant \frac{1}{2}\left|\langle [R,S] \rangle\right|$ 由 Robertson 给出[219]. 但是这个结果的右边的下限是态依赖的, 所以近 30 多年来 Deutsch 等人又发展了基于熵的不确定关系[220~223], 这类不确定关系的特点是下限不再依赖于具体的态. 爱因斯坦等人 1935 年提出的 EPR 佯谬认为: 如果 AB 两个粒子是孪生的, 可以同时准确测量 A 的位置和 B 的动量, 而从 B 的动量又可以推出 A 的动量, 等价于说可以同时确定 A 粒子的位置和动量. 爱因斯坦等人以此来质疑量子力学的完备性[224]. 对于 EPR 佯谬的持续研究催生了量

子纠缠的概念，人们认为利用量子纠缠，是有可能同时确定一个粒子的位置和动量的. 最近的理论研究进一步给出了这一问题的定量描述，在观测者拥有被测粒子“量子信息”的情况下，被测粒子测量结果的不确定度，依赖于被测粒子与观测者所拥有的另一个粒子(存储量子信息)的纠缠度的大小[225,226]. 当它们处于最大纠缠态时，两个不对易的力学量可以同时被准确测量，此时经典的海森堡不确定原理将不再成立. 此理论被称为新形式的海森堡不确定原理.

中国科学技术大学的李传锋研究组在最近的实验中首次验证了新形式的海森堡不确定原理(见图 12)[227]. 他们在光学系统中利用非线性过程产生的孪生光子对制备出一种特殊的纠缠态——贝尔对角态，把其中一个光子作为被测光子，另一个光子作为存储被测光子量子信息的辅助粒子. 他们通过将辅助光子存储在自行研制的自旋回声式的量子存储器中(存储时间可以达到 1.2 μs)，实现了对被测光子的两个不对易力学量的测量，并给出了两个力学量输出结果不确定度的下界. 与此同时，Prevedel 等人利用单模光纤作为存储器也实现了新形式的海森堡不确定关系的实验验证[228].

量子开放系统是量子力学的一个非常重要的研究方向. 因为薛定谔方程是描述封闭系统中量子态的演化的，而作为一个量子系统，不可避免地会同环境自由度发生相互作用，从而产生信息和能量的交换，这就是量子开放系统. 对于量子开放系统，其处理思路非常简单，我们只需要将所有的环境自由度包含进来，将这个大的系统看成一个闭系统，用薛定谔方程来处理. 对于某一时刻的系统状态的描述，我们可以通过约化掉环境的自由度，来获得系统的约化密度矩阵. 但是，由于这是一个量子多体系统，薛定谔方程的求解异常复杂，无法对一般情况进行求解.

在最初的研究中，人们考虑环境自由度非常大、系统和环境之间的耦合非常弱的情况，在这种情况下可以采用波恩-马尔科夫近似，进而可以求得系统约化密度矩阵演化的 Lindblad 方程，这种情况下，系统展现出马尔科夫特性，即系统的将来状态仅与系统的现在状态有关，与过去无关，也可以说系统流入环境的信息不会再反过头来影响系统. 但是，随着量子信息科学的发展，人们操控微观系统的能力越来越高，人们所处理的系统和环境越来越精细，波恩-马尔科夫近似下的结果越来越难以满足对系统精确描述的要求，所以对非马尔科夫行为的研究就显得越来越重要. 最近几年，科学家们提出了几种非马尔科夫性的定义[229~231]，使得非马尔科夫过程的定量研究成为可能.

如果量子开放系统是非马尔科夫性的，那么它流入环境的信息将在将来的某一时刻重新对系统造

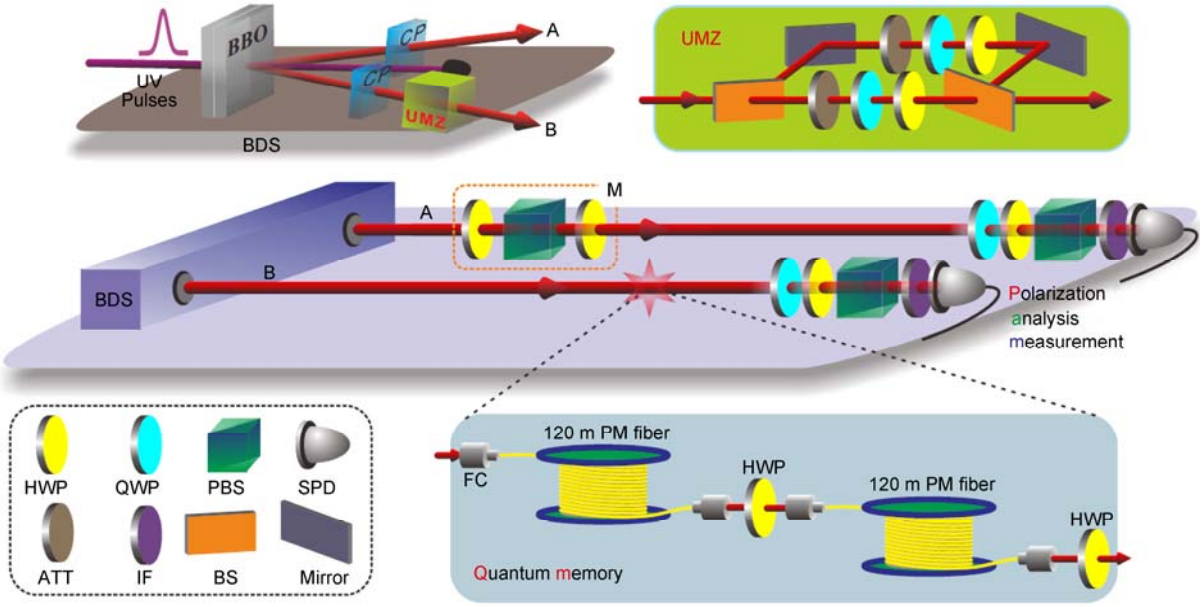

图 12　验证新形式海森堡不确定原理的实验示意图

成影响，这种情形下，环境就相当于量子信息的存储器. 通常情况下，由于环境具有复杂的自由度，人们很难实现对环境的调控，使之从马尔科夫环境变成为非马尔科夫环境. 但在 2011 年，李传锋研究组首次在实验上模拟了量子开系统中，环境从马尔科夫到非马尔科夫的转变[232]. 他们利用非线性晶体的自发参量下转换过程制备出高纯度纠缠光子对，并将其中一个光子的偏振比特作为量子系统，其频率(或者说波长)作为环境，然后通过石英片的双折射效应把量子系统与环境耦合起来，实现量子系统在环境中的演化. 他们通过在光路中加入特制的法布里-玻罗腔，通过改变法布里-玻罗腔的转动角度，利用另外一个光子辅助探测，从而实现了对环境(光子频率)的调控(见图 13)[233].

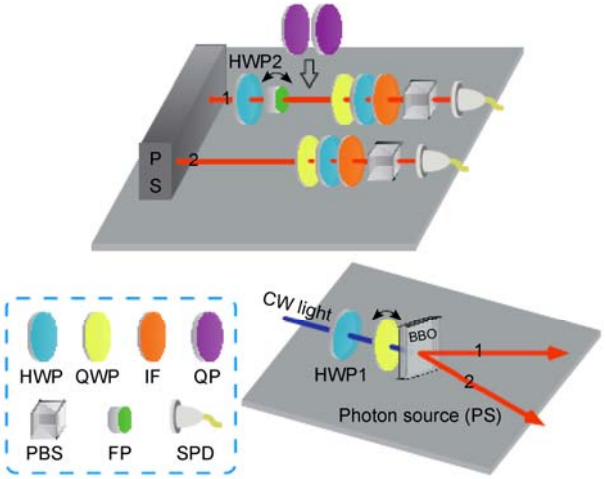

图 13　在光学系统中模拟从马尔科夫环境到非马尔科夫环境转变的实验示意图

环境自由度的存在，是造成量子系统退相干的主要原因，这给人们相干操控量子态带来很大困难. 为了克服这一困难，人们发展了若干方法，其中之一被称为动力学退耦合，即对系统施加若干控制脉冲，来斩断系统与环境自由度之间的联系(在脉冲控制的时间段中，将系统与环境的相互作用哈密顿量平均掉，使开放系统的行为类似于一个封闭系统). 在动

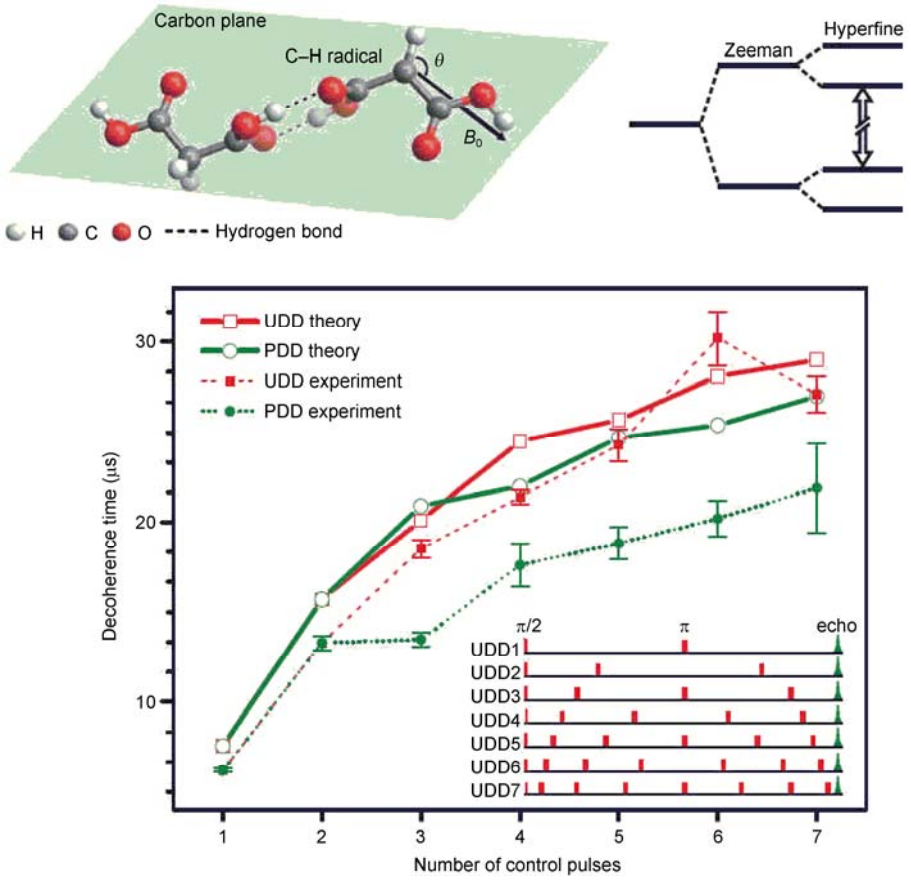

图 14　固态系统中通过 UDD 脉冲的控制，使系统相干性获得显著提升

力学退耦合的研究中, 一个重要的理论进展是, Uhrig 在 2007 年提出了 UDD 的动力学退耦合序列[234], 大大简化了动力学退耦合中所需要的翻转脉冲数目. 2009 年, 中国科学技术大学的杜江峰等人, 在实验上实现了 UDD 的脉冲控制[235]. 他们在真实的固态系统中, 使用 7 重 UDD 脉冲, 从而将系统相干性提升了 3 个量级(见图 14). 随后, 2010 年, Hanson 研究组也在金刚石 NV 色心中的单自旋系统中实现了对动力学退耦合过程的实验验证[236].

量子开系统中, 系统和环境相互作用复杂性有时会展现出很多有违直观的现象. 例如, 一般而言, 系统与环境的耦合作用越强, 系统的退相干会越显著. 但这一点并不总是正确. 香港中文大学的刘仁保等人发现, 在自旋 1 的系统中, 在动力学退耦合的控制之下, 多跃迁过程可以比单跃迁过程具有更长的相干时间, 虽然多跃迁过程会遭受更强的噪声影响, 他们将此命名为反常退相干[237]. 杜江峰等人在 NV 色心系统中验证了这一点[238].

通过上述的事例可以看出, 量子信息的深入发展也推动了量子力学本身的发展与完善, 使得人们对很多物理问题的认识比以前更深刻了.

7 结语

量子信息科学, 以量子计算研究为开篇, 以量子力学规律来改造经典信息的表征, 向人们展示出一幅奇妙的未来信息技术的图景. 经过近三十年的发展, 这一领域在理论和技术方面获得突飞猛进发展的同时, 依然展示着勃勃的生机. 虽然迄今为止, 人们距离制造出一台可实用化的、超越当前经典计算极限的量子计算机的目标依然遥远, 有若干瓶颈技术仍需克服. 但无庸置疑的是, 人们调控微观世界的能力获得了显著的提高: 量子密码技术已经接近实用化; 长程量子通信的原理性验证也不存在原则上的障碍; 量子模拟技术快速发展, 已经接近经典计算机可以模拟的极限; 量子计量学也获得了快速的发展. 这些都酝酿并孕育着崭新的量子信息时代. 而尤为可喜的是, 中国的研究人员在这一领域已经跟上了世界的步伐, 成为量子信息世界版图中一股不可或缺的力量.

参考文献

1 Wiesner S. Conjugate coding. SIGACT News, 1983, 15: 78–88
2 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984. 175–179
3 Elliott C, Colvin A, Pearson D, et al. Current status of the DARPA quantum network. In: Donkor E J, Pirich A R, Brandt H E, eds. Quantum Information and Computation III. Proc SPIE, 2005, 5815: 138–149
4 Peev M, Pacher C, Alléaume R, et al. The SECOQC quantum key distribution network in Vienna. New J Phys, 2009, 11: 075001
5 Sasaki M, Fujiwara M, Ishizuka H, et al. Field test of quantum key distribution in the Tokyo QKD network. Opt Express, 2011, 19: 10387–10409
6 Han Z F, Mo X F, Gui Y Z, et al. Stability of phase-modulated quantum key distribution systems. Appl Phys Lett, 2005, 86: 221103
7 Mo X F, Zhu B, Han Z F, et al. Faraday-Michelson system for quantum cryptography. Opt Lett, 2005, 30: 2632–2634
8 Zhang T, Mo X F, Han Z F, et al. Extensible router for a quantum key distribution network. Phys Lett A, 2008, 372: 3957–3962
9 Chen W, Han Z F, Zhang T, et al. Field experiment on a “Star Type” metropolitan quantum key distribution network. IEEE Photonics Technol Lett, 2009, 21: 575–577
10 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chin Sci Bull, 2009, 54: 2991–2997
11 Wang S, Chen W, Yin Z Q, et al. Field test of wavelength-saving quantum key distribution network. Opt Lett, 2010, 35: 2454–2456
12 Chen T Y, Liang H, Liu Y, et al. Field test of a practical secure communication network with decoy-state quantum cryptography. Opt Express, 2009, 17: 6540–6549
13 Chen T Y, Wang J, Liang H, et al. Metropolitan all-pass and inter-city quantum communication network. Opt Express, 2010, 18: 27217–27225
14 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050–2056
15 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444
16 Zhao Y B, Fung C H F, Han Z F, et al. Security proof of differential phase shift quantum key distribution in the noiseless case. Phys Rev A, 2008, 78: 042330

17 Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys Rev Lett, 2009, 102: 180504
18 Hwang W Y. Quantum key distribution with high loss: Toward global secure communication. Phys Rev Lett, 2003, 91: 057901
19 Lo H K, Ma X F, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504
20 Wang X B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. Phys Rev A, 2005, 72: 012322
21 Nauerth S, Fürst M, Schmitt-Manderbach T, et al. Information leakage via side channels in freespace BB84 quantum cryptography. New J Phys, 2009, 11: 065001
22 Qi B, Fung C H F, Lo H K, et al. Time-shift attack in practical quantum cryptosystems. Quant Inf Comput, 2007, 7: 73–82
23 Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nat Photonics, 2010, 4: 686–689
24 Weier H, Krauss H, Rau M, et al. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. New J Phys, 2011, 13: 073024
25 Fung C H F, Qi B, Tamaki K, et al. Phase-remapping attack in practical quantum-key-distribution systems. Phys Rev A, 2007, 75: 032314
26 Li H W, Yin Z Q, Han Z F, et al. Security of practical phase-coding quantum key distribution. Quant Inf Comput, 2010, 10: 771–779
27 Li H W, Yin Z Q, Han Z F, et al. Security of quantum key distribution with state-dependent imperfections. Quant Inf Comput, 2011, 11: 937–947
28 Li H W, Wang S, Huang J Z, et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. Phys Rev A, 2011, 84: 062308
29 Bennett C H, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1993, 70: 1895–1899
30 Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation. Nature, 1997, 390: 575–579
31 Pan J W, Gasparoni S, Aspelmeyer M, et al. Experimental realization of freely propagating teleported qubits. Nature, 2003, 421: 721–725
32 Zhao Z, Chen Y A, Zhang A N, et al. Experimental demonstration of five-photon entanglement and open-destination teleportation. Nature, 2004, 430: 54–58
33 Zukowski M, Zeilinger A, Horne M A, et al. “Event-ready-detectors” Bell experiment via entanglement swapping. Phys Rev Lett, 1993, 71: 4287–4290
34 Bennett C H, Brassard G, Popescu S, et al. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys Rev Lett, 1996, 76: 722–725
35 Briegel H, Dür W, Cirac J I, et al. Quantum repeaters: The role of imperfect local operations in quantum communication. Phys Rev Lett, 1998, 81: 5932–3935
36 Duan L M, Lukin M D, Cirac J I, et al. Long-distance quantum communication with atomic ensembles and linear optics. Nature, 2001, 414: 413–418
37 Zhao B, Chen Z B, Chen Y A, et al. Robust creation of entanglement between remote memory qubits. Phys Rhys Lett, 2007, 98: 240502
38 Yuan Z S, Chen Y A, Zhao B, et al. Experimental demonstration of a BDCZ quantum repeater node. Nature, 2008, 454: 1098–1101
39 Chen Y A, Chen S, Yuan Z S, et al. Memory-built-in quantum teleportation with photonic and atomic qubits. Nat Phys, 2008, 4: 103–107
40 Bao X H, Qian Y, Yang J, et al. Generation of narrow-band polarization-entangled photon pairs for atomic quantum memories. Phys Rev Lett, 2008, 101: 190501
41 Zhao B, Chen Y A, Bao X H, et al. A millisecond quantum memory for scalable quantum networks. Nat Phys, 2009, 5: 95–99
42 Zhao R, Dudin Y O, Jenkins S D, et al. Long-lived quantum memory. Nat Phys, 2009, 5: 100–104
43 Zhang H, Jin X M, Yang J, et al. Preparation and storage of frequency-uncorrelated entangled photons from cavity-enhanced spontaneous parametric downconversion. Nat Photonics, 2011, 5: 628–632
44 Schmitt-Manderbach T, Weier H, Fürst M, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Phys Rev Lett, 2007, 98: 010504
45 Jin X M, Ren J G, Yang B, et al. Experimental free-space quantum teleportation. Nat Photonics, 2010, 4: 376–381
46 Furusawa A, Sørensen J L, Braunstein S L, et al. Unconditional quantum teleportation. Science, 1998, 282: 706–709
47 Li X, Pan Q, Jing J, et al. Quantum dense coding exploiting a bright Einstein-Podolsky-Rosen beam. Phys Rev Lett, 2002, 88: 047904
48 Schori C, Julsgaard B, Sørensen J L, et al. Recording quantum properties of light in a long-lived atomic spin state: Towards quantum memory. Phys Rev Lett, 2002, 89: 057903
49 Wang Y, Shen H, Jin X, et al. Experimental generation of 6 dB continuous variable entanglement from a nondegenerate optical parametric amplifier. Opt Express, 2010, 18: 6149–6155
50 Chen H, Zhang J. Phase-sensitive manipulations of the two-mode entangled state by a type-II nondegenerate optical parametric amplifier inside an optical cavity. Phys Rev A, 2009, 79: 063826

51 Shang Y, Jia X, Shen Y, et al. Continuous variable entanglement enhancement and manipulation by a subthreshold type II optical parametric amplifier. Opt Lett, 2010, 35: 853–855
52 van Loock P, Braunstein S L. Multipartite entanglement for continuous variables: A quantum teleportation network. Phys Rev Lett, 2000, 84: 3482–3485
53 Jing J, Zhang J, Yan Y, et al. Experimental demonstration of tripartite entanglement and controlled dense coding for continuous variables. Phys Rev Lett, 2003, 90: 167903
54 Su X, Tan A, Jia X, et al. Experimental preparation of quadripartite cluster and Greenberger-Horne-Zeilinger entangled states for continuous variables. Phys Rev Lett, 2007, 98: 070502
55 Benioff P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. J Stat Phys, 1980, 22: 563–591
56 Feynman R P. Simulating physics with computers. Int J Theor Phys, 1982, 21: 467–488
57 Deutsch D. Quantum theory: The Church-Turing principle and the universal quantum computer. Proc Roy Soc Lond A, 1985, 400: 97–117
58 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science. New York: IEEE Computer Society Press, 1994. 124–134
59 Grover L K. Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett, 1997, 79: 325–328
60 Deutsch D. Quantum computational networks. Proc Roy Soc Lond A, 1989, 425:73–90
61 Barenco A, Bennett C H, Cleve R, et al. Elementary gates for quantum computation. Phys Rev A, 1995, 52: 3457–3467
62 Shor P W. Scheme for reducing decoherence in quantum computer memory. Phys Rev A, 1995, 52: R2493–R2496
63 Raussendorf R, Briegel H J. A one-way quantum computer. Phys Rev Lett, 2001, 86: 5188–5191
64 Gross D, Eisert J. Novel schemes for measurement-based quantum computation. Phys Rev Lett, 2007, 98: 220503
65 Kitaev A Y. Fault-tolerant quantum computation by anyons. Ann Phys, 2003, 303: 2–30
66 Farhi E, Goldstone J, Gutmann S, et al. Quantum computation by adiabatic evolution. arXiv: quant-ph/0001106
67 Aharonov D, van Dam W, Kempe J, et al. Adiabatic quantum computation is equivalent to standard quantum computation. SIAM J Comput, 2007, 37: 166–194
68 Monz T, Schindler P, Barreiro J T, et al. 14-qubit entanglement: Creation and coherence. Phys Rev Lett, 2011, 106: 130506
69 Shnirman A, Schön G, Hermon Z. Quantum manipulations of small Josephson junctions. Phys Rev Lett, 1997, 79: 2371–2374
70 Yu Y, Han S, Chu X, et al. Coherent temporal oscillations of macroscopic quantum states in a Josephson junction. Science, 2002, 296: 889–892
71 Martinis J, Nam S, Aumentado J, et al. Rabi oscillations in a large Josephson-junction qubit. Phys Rev Lett, 2002, 89: 117901
72 Friedman J R, Patel V, Chen W, et al. Quantum superposition of distinct macroscopic states. Nature, 2000, 406: 43–46
73 van der Wal C H, ter Haar A C J, Wilhelm F K, et al. Quantum superposition of macroscopic persistent-current states. Science, 2000, 290: 773–777
74 Chiorescu I, Nakamura Y, Harmans C J P M, et al. Coherent quantum dynamics of a superconducting flux qubit. Science, 2003, 299: 1869–1871
75 Nakamura Y, Pashkin Y A, Tsai J S. Coherent control of macroscopic quantum states in a single-Cooper-pair box. Nature, 1999, 398: 786–788
76 Vion D, Aassime A, Cottet A, et al. Manipulating the quantum state of an electrical circuit. Science, 2002, 296: 886–889
77 Yamamoto T, Pashkin Y A, Astafiev O, et al. Demonstration of conditional gate operation using superconducting charge qubits. Nature, 2003, 425: 941–944
78 Steffen M, Ansmann M, Bialczak R C, et al. Measurement of the entanglement of two superconducting qubits via state tomography. Science, 2006, 313: 1423–1425
79 Plantenberg J H, de Groot P C, Harmans C J P M, et al. Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits. Nature, 2007, 447: 836–839
80 Neeley M, Bialczak R C, Lenander M, et al. Generation of three-qubit entangled states using superconducting phase qubits. Nature, 2010, 467: 570–573
81 Sun G Z, We X D, Mao B, et al. Tunable quantum beam splitters for coherent manipulation of a solid-state tripartite qubit system. Nat Commun, 2010, 1: 51
82 Wallraff A, Schuster D I, Blais A, et al. Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics. Nature, 2004, 431: 162–167
83 Sillanpaa M A, Park J I, Simmonds R W. Coherent quantum state storage and transfer between two phase qubits via a resonant cavity. Nature, 2007, 449: 438–442

84 Majer J, Chow J M, Gambetta J M, et al. Coupling superconducting qubits via a cavity bus. Nature, 2007, 449: 443–447
85 Galiautdinov A, Korotkov A N, Martinis J M. Resonator/zero-qubit architecture for superconducting qubits. arXiv: 1105.3997
86 Wang H, Mariantoni M, Bialczak R C, et al. Deterministic entanglement of photons in two superconducting microwave resonators. Phys Rev Lett, 2011, 106: 060401
87 Mariantoni M, Wang H, Yamamoto T, et al. Implementing the quantum von Neumann architecture with superconducting circuits. Science, 2011, 334: 61–65
88 Zhou X, Zhou Z W, Guo G C, et al. Quantum computation with untunable couplings. Phys Rev Lett, 2002, 89: 197903
89 Zhou Z W, Yu B, Zhou X, et al. Scalable fault-tolerant quantum computation in decoherence-free subspaces. Phys Rev Lett, 2004, 93: 010501
90 Niskanen A, Harrabi K, Yoshihara F, et al. Quantum coherent tunable coupling of superconducting qubits. Science, 2006, 316: 723–726
91 Johnson M W, Amin M H S, Gildert S, et al. Quantum annealing with manufactured spins. Nature, 2011, 473: 194–198
92 You J Q, Wang Z D, Zhang W, et al. Manipulating and probing Majorana fermions using superconducting circuits. arXiv: 1108.3712
93 Loss D, DiVincenzo D P. Quantum computation with quantum dots. Phys Rev A, 1998, 57: 120–126
94 Elzerman J M, Hanson R, van Beveren L H W, et al. Single-shot read-out of an individual electron spin in a quantum dot. Nature, 2004, 430: 431–435
95 Petta J R, Johnson A C, Taylor J M, et al. Coherent manipulation of coupled electron spins in semiconductor quantum dots. Science, 2005, 309: 2180–2184
96 Koppens F H L, Buizert C, Tielrooij K J, et al. Driven coherent oscillations of a single electron spin in a quantum dot. Nature, 2006, 442: 766–771
97 Johnson A C, Petta J R, Taylor J M, et al. Triplet-singlet spin relaxation via nuclei in a double quantum dot. Nature, 2005, 435: 925–928
98 Koppens F H L, Folk J A, Elzerman J M, et al. Control and detection of singlet-triplet mixing in a random nuclear field. Science, 2005, 309: 1346–1350
99 Reilly D J, Taylor J M, Petta J R, et al. Suppressing spin qubit dephasing by nuclear state preparation. Science, 2008, 321: 817–821
100 Nowack K C, Koppens F H L, Nazarov Y V, et al. Coherent control of a single electron spin with electric fields. Science, 2007, 318: 1430–1433
101 Jeong H, Chang A M, Melloch M R. The Kondo effect in an artificial quantum dot molecule. Science, 2001, 293: 2221–2223
102 Fujisawa T, Austing D G, Tokura Y, et al. Allowed and forbidden transitions in artificial hydrogen and helium atoms. Nature, 2002, 419: 278–281
103 Xiao M, Martin I, Yablonovitch E, et al. Electrical detection of the spin resonance of a single electron in a silicon field-effect transistor. Nature, 2004, 430: 435–439
104 Craig N J, Taylor J M, Lester E A, et al. Tunable nonlocal spin control in a coupled-quantum dot system. Science, 2004, 304: 565–567
105 Fujisawa T, Hayashi T, Tomita R, et al. Bidirectional counting of single electrons. Science, 2006, 312: 1634–1636
106 Pioro-Ladriere M, Obata T, Tokura Y, et al. Electrically driven single-electron spin resonance in a slanting Zeeman field. Nat Phys, 2008, 4: 776–779
107 van Weperen I, Armstrong B D, Laird E A, et al. Charge-state conditional operation of a spin qubit. Phys Rev Lett, 2011, 107: 030506
108 Lin Z R, Guo G P, Tu T, et al. Generation of quantum-dot cluster states with a superconducting transmission line resonator. Phys Rev Lett, 2008, 101: 230501
109 Guo G P, Zhang H, Hu Y, et al. Dispersive coupling between the superconducting transmission line resonator and the double quantum dots. Phys Rev A, 2008, 78: 020302
110 Xiao M, House M G, Jiang H W. Measurement of the spin relaxation time of single electrons in a silicon metal-oxide-semiconductor-based quantum dot. Phys Rev Lett, 2010, 104: 096801
111 Shaji N, Simmons C B, Thalakulam M, et al. Spin blockade and lifetime-enhanced transport in a few-electron Si/SiGe double quantum dot. Nat Phys, 2008, 4: 540–544
112 Hu Y J, Churchill O H, Reilly D J, et al. A Ge/Si heterostructure nanowire-based double quantum dot with integrated charge sensor. Nat Nanotech, 2007, 2: 622–625
113 Ponomarenko L A, Schedin F, Katsnelson M I, et al. Chaotic Dirac billiard in graphene quantum dots. Science, 2008, 320: 356–358
114 Wang L J, Cao G, Tu T, et al. Ground states and excited states in a tunable graphene quantum dot. Chin Phys Lett, 2011, 28: 067301
115 Hao X J, Tu T, Cao G, et al. Strong and tunable spin-orbit coupling of one-dimensional holes in Ge/Si core/shell nanowires. Nano Lett, 2010, 10: 2956–2960
116 Wang L J, Cao G, Tu T, et al. A graphene quantum dot with a single electron transistor as an integrated charge sensor. Appl Phys Lett, 2010, 97: 262113

117 Kurtsiefer C, Mayer S, Zarda P, et al. Stable solid-state source of single photons. Phys Rev Lett, 2000, 85: 290–293
118 Faraon A, Barclay P E, Santori C, et al. Resonant enhancement of the zero-phonon emission from a colour centre in a diamond cavity. Nat Photonics, 2011, 5: 301–305
119 Buckley B B, Fuchs G D, Bassett L C, et al. Spin-light coherence for single-spin measurement and control in diamond. Science, 2010, 330: 1212–1215
120 Togan E, Chu Y, Trifonov A S, et al. Quantum entanglement between an optical photon and a solid-state spin qubit. Nature, 2010, 466: 730–734
121 Fuchs G D, Dobrovitski V V, Toyli D M, et al. Gigahertz dynamics of a strongly driven single quantum spin. Science, 2009, 326: 1520–1522
122 Shi F Z, Rong X, Xu N Y, et al. Room-temperature implementation of the Deutsch-Jozsa algorithm with a single electronic spin in diamond. Phys Rev Lett, 2010, 105: 040504
123 Neumann P, Mizuochi N, Rempp F, et al. Multipartite entanglement among single spins in diamond. Science, 2008, 320: 1326–1329
124 Maurer P C, Maze J R, Stanwix P L, et al. Far-field optical imaging and manipulation of individual spins with nanoscale resolution. Nat Phys, 2010, 6: 912–918
125 Neumann P, Kolesov R, Naydenov B, et al. Quantum register based on coupled electron spins in a room-temperature solid. Nat Phys, 2010, 6: 249–253
126 Zhu X B, Saito S, Kemp A, et al. Coherent coupling of a superconducting flux qubit to an electron spin ensemble in diamond. Nature, 2011, 478: 221–224
127 Arcizet A, Jacques V, Siria A, et al. A single nitrogen-vacancy defect coupled to a nanomechanical oscillator. Nat Phys, 2011, 7: 879–883
128 Aharonovich I, Greentree D A, Prawer S. Diamond photonics. Nat Photonics, 2011, 5: 397–405
129 Cirac J I, Zoller P. Quantum computations with cold trapped ions. Phys Rev Lett, 1995, 74: 4091–4094
130 Wineland D J, Monroe C, Itano W M, et al. Experimental issues in coherent quantum-state manipulation of trapped atomic ions. J Res Natl Inst Stand Tech, 1998, 103: 259–328
131 Kielpinski D, Monroe C, Wineland D J. Architecture for a large-scale ion-trap quantum computer. Nature, 2002, 417: 709–711
132 Duan L M, Blinov B B, Moehring D L, et al. Scalable trapped ion quantum computation with a probabilistic ion-photon mapping. Quant Inf Comput, 2004, 4: 165–173
133 Jaksch D, Bruder C, Cirac J I, et al. Cold Bosonic atoms in optical lattices. Phys Rev Lett, 1998, 81: 3108–3111
134 Brennen G K, Caves C M, Jessen P S, et al. Quantum logic gates in optical lattices. Phys Rev Lett, 1999, 82: 1060–1063
135 Jaksch D, Briegel H J, Cirac J I, et al. Entanglement of atoms via cold controlled collisions. Phys Rev Lett, 1999, 82: 1975–1978
136 Weitenberg C, Endres M, Sherson J F, et al. Single-spin addressing in an atomic Mott insulator. Nature, 2011, 471: 319–324
137 Jaksch D, Cirac J I, Zoller P. Fast quantum gates for neutral atoms. Phys Rev Lett, 2000, 85: 2208–2211
138 Lukin M D, Fleischhauer M, Cote R. Dipole blockade and quantum information processing in mesoscopic atomic ensembles. Phys Rev Lett, 2001, 87: 037901
139 Xu P, He X D, Wang J, et al. Trapping a single atom in a blue detuned optical bottle beam trap. Opt Lett, 2010, 35: 2164–2166
140 He X, Xu X D, Wang J, et al. High efficient loading of two atoms into a microscopic optical trap by dynamically reshaping the trap with a spatial light modulator. Opt Express, 2010, 18: 13586–13592
141 Knill E, Laflamme R, Milburn G J. A scheme for efficient quantum computation with linear optics. Nature, 2001, 409: 46–52
142 Lu C Y, Browne D E, Yang T, et al. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. Phys Rev Lett, 2007, 99: 250504
143 Lu C Y, Zhou X Q, Gühne O, et al. Experimental entanglement of six photons in graph states. Nat Phys, 2007, 3: 91–95
144 Chen K, Li C M, Zhang Q, et al. Experimental realization of one-way quantum computing with two-photon four-qubit cluster states. Phys Rev Lett, 2007, 99: 120503
145 Gao W B, Yao X C, Cai J M, et al. Experimental measurement-based quantum computing beyond the cluster-state model. Nat Photonics, 2011, 5: 117–123
146 Zhang J, Braunstein S L. Continuous-variable Gaussian analog of cluster states. Phys Rev A, 2006, 73: 032318
147 Su X L, Tan A H, Jia X J, et al. Experimental preparation of quadripartite cluster and Greenberger-Horne-Zeilinger entangled states for continuous variables. Phys Rev Lett, 2007, 98: 070502
148 Ömer B. Classical concepts in quantum programming. Int J Theor Phys, 2005, 44/7: 943–955
149 Petersen A, Oskin M. A new algebraic foundation for quantum programming languages. In: The 2nd Workshop on Non-Silicon Computing (NSC) held in conjunction with the 30th Annual International Symposium on Computer Architecture (ISCA), 2003
150 Wootters W K, Zurek W H. A single quantum cannot be cloned. Nature, 1982, 299: 802–803
151 van Tonder A. A lambda calculus for quantum computation. SIAM J Comput, 2004, 33: 1109–1135

152 Floyd R. Assigning meaning to programs. Proc Symp Appl Math, 1967, 19: 19–32
153 Hoare C A R. An axiomatic basis for computer programming. Commun ACM, 1969, 12: 576–580
154 Ying M S. Floyd-Hoare logic for quantum programs. ACM Trans Progr Lang Syst, 2011, 33: 19
155 Ying M S, Feng Y, Duan R Y, et al. An algebra of quantum processes. ACM Trans Comput Logic, 2009, 10: 19
156 Feng Y, Duan R, Ying M. Bisimulation for quantum processes. In: Proceedings of the 38th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. Austin, Texas, USA, 2011. 523–534
157 Buluta I, Nori F. Quantum simulators. Science, 2009, 326: 108–111
158 Simon J, Bakr W S, Ma R, et al. Quantum simulation of antiferromagnetic spin chains in an optical lattice. Nature, 2011, 472: 307–312
159 Struck J, Ölschläger C, Le Targat R, et al. Quantum simulation of frustrated classical magnetism in triangular optical lattices. Science, 2011, 333: 996–999
160 Liu W M, Wu B, Niu Q. Nonlinear effects in interference of Bose-Einstein condensates. Phys Rev Lett, 2000, 84: 2294–2297
161 Liang Z X, Zhang Z D, Liu W M. Dynamics of a bright soliton in Bose-Einstein condensates with time-dependent atomic scattering length in an expulsive parabolic potential. Phys Rev Lett, 2005, 94: 050402
162 Ji A C, Liu W M, Song J L, et al. Dynamical creation of fractionalized vortices and vortex lattices. Phys Rev Lett, 2008, 101: 010402
163 Barreiro J T, Müller M, Schindler P, et al. An open-system quantum simulator with trapped ions. Nature, 2011, 470: 486–491
164 Lanyon B, Hempel C, Nigg D, et al. Universal digital quantum simulation with trapped ions. Science, 2011, 334: 57–61
165 Zhang D W, Xue Z Y, Yan H, et al. Macroscopic Klein tunneling in spin-orbit-coupled Bose-Einstein condensates. Phys Rev A, 2012, 85: 013628
166 Du J, Xu N, Peng X, et al. NMR implementation of a molecular hydrogen quantum simulation with adiabatic state preparation. Phys Rev Lett, 2010, 104: 030502
167 Lu D, Xu N, Xu R, et al. Simulation of chemical isomerization reaction dynamics on a NMR quantum simulator. Phys Rev Lett, 2011, 107: 020501
168 Lu C Y, Gao W B, Gühne O, et al. Demonstrating anyonic fractional statistics with a six-qubit quantum simulator. Phys Rev Lett, 2009, 102: 030502
169 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000
170 Nagata T, Okamoto R, O'Brien J L, et al. Beating the standard quantum limit with four entangled photons. Science, 2007, 316: 726–729
171 Sun F W, Liu B H, Huang Y F, et al. Experimental demonstration of phase measurement precision beating standard quantum limit by projection measurement. Europhys Lett, 2008, 82: 24001
172 Higgins B L, Berry D W, Bartlett S D, et al. Entanglement-free Heisenberg-limited phase estimation. Nature, 2007, 450: 393–396
173 Giovannetti V, Lloyd S, Maccone L. Quantum metrology. Phys Rev Lett, 2006, 96: 010401
174 Rabi I I, Zaeharias J R, Millman S, et al. A new method of measuring nuclear magnetic moment. Phys Rev, 1938, 53: 318
175 Clairon A, Ghezali S, Santarelli G, et al. Preliminary accuracy evaluation of a cesium fountain frequency standard. In: Bergquist J, ed. Proceedings of the 5th Symposium on Frequency Standards and Metrology. Singapore: World Scientific, 1995. 49–59
176 Wynands R, Weyers S. Atomic fountain clocks. Metrologia, 2005, 42: 64–79
177 Chou C W, Hume D B, Koelemeij J C J, et al. Frequency comparison of two high-accuracy Al^+ optical clocks. Phys Rev Lett, 2010, 104: 070802
178 Roos C F, Chwalla M, Kim K, et al. 'Designer atoms' for quantum metrology. Nature, 2006, 443: 316–319
179 Chwalla M, Kim K, Monz T, et al. Precision spectroscopy with two correlated atoms. Appl Phys B, 2007, 89: 483–488
180 Caves C M. Quantum-mechanical noise in an interferometer. Phys Rev D, 1981, 23:1693–1708
181 Xiao M, Wu L A, Kimble H J. Precision measurement beyond the shot-noise limit. Phys Rev Lett, 1987, 59: 278–281
182 Grangier P, Slusher R E, Yurke B, et al. Squeezed-light-enhanced polarization interferometer. Phys Rev Lett, 1987, 59: 2153–2156
183 Xiang G Y, Higgins B L, Berry D W, et al. Entanglement-enhanced measurement of a completely unknown optical phase. Nat Photonics, 2011, 5: 43–47
184 Huver S D, Wildfeuer C F, Dowling J P. Entangled Fock states for robust quantum optical metrology, imaging, and sensing. Phys Rev A, 2008, 78: 063828
185 Kacprowicz M, Demkowicz-Dobrzanski R, Wasilewski W, et al. Experimental quantum-enhanced estimation of a lossy phase shift. Nat Photonics, 2010, 4: 357–360
186 Escher B M, de Matos Filho R L, Davidovich L. General framework for estimating the ultimate precision limit in noisy quantum-enhanced metrology. Nat Phys, 2010, 7: 406–411
187 Hall M J W, Berry D W, Zwierz M, et al. Universality of the Heisenberg limit for estimates of random phase shifts. arXiv: 1111.0788
188 Crespi A, Lobino M, Matthews J C F, et al. Measuring protein concentration with entangled photons. arXiv: 1109.3128

189 The LIGO Scientific Collaboration. A gravitational wave observatory operating beyond the quantum shot-noise limit. Nat Phys, 2011, 7: 962–965
190 Jing J, Liu C, Zhou Z, et al. Realization of a nonlinear interferometer with parametric amplifiers. Appl Phys Lett, 2011, 99: 011110
191 Brida G, Genovese M, Ruo Berchera I. Scanning-probe spectroscopy of semiconductor donor molecules. Nat Photonics, 2010, 4: 227–233
192 Rathe U V, Scully M O. Theoretical basis for a new subnatural spectroscopy via correlation interferometry. Lett Math Phys, 1995, 34: 297–307
193 Boto A N, Kok P, Abrams D S, et al. Quantum interferometric optical lithography: Exploiting entanglement to beat the diffraction limit. Phys Rev Lett, 2000, 85: 2733–2736
194 D'Angelo M, Chekhova M V, Shih Y. Two-photon diffraction and quantum lithography. Phys Rev Lett, 2001, 87: 013602
195 Shin H, Chan K W C, Chang H J, et al. Quantum spatial superresolution by optical centroid measurements. Phys Rev Lett, 2011, 107: 083603
196 Kawabe Y, Fujiwara H, Okamoto R, et al. Quantum interference fringes beating the diffraction limit. Opt Express, 2007, 15: 14244–14250
197 Tsang M. Quantum imaging beyond the diffraction limit by optical centroid measurements. Phys Rev Lett, 2009, 102: 253601
198 Bennett C H, DiVincenzo D P. Quantum information and computation. Nature, 2000, 404: 247–255
199 Shannon C E. A mathematical theory of communication. Bell Syst Tech J, 1948, 27: 379–423, 623–656
200 Datta A, Shaji A, Caves C M. Quantum discord and the power of one qubit. Phys Rev Lett, 2008, 100: 050502
201 Lanyon B P, Barbieri M, Almeida M P, et al. Experimentalquantum computing without entanglement. Phys Rev Lett, 2008, 101: 200501
202 GroismanB, Popescu S, Winter A. Quantum, classical, and total amount of correlations in a quantum state. Phys Rev A, 2005, 72: 032317
203 Ollivier H, Zurek W H. Quantum discord: A measure of the quantumness of correlations. Phys Rev Lett, 2001, 88: 017901
204 Ferraro A, Aolita L, Cavalcanti D, et al. Almost all quantum states have non-classical correlations. Phys Rev A, 2010, 81: 052318
205 Cui J, Fan H. Correlations in the Grover search. J Phys A: Math Theor, 2010, 43: 045305
206 Zurek W H. Quantum discord and Maxwell's demons. Phys Rev A, 2003, 67: 012320
207 Sarandy M S. Classical correlation and quantum discord in critical systems. Phys Rev A, 2009, 80: 022108
208 Xu J S, Xu X Y, Li C F, et al. Experimental investigation of classical and quantum correlations under decoherence. Nat Commun, 2010, 1: 7
209 Xu J S, Li C F, Zhang C J, et al. Experimental investigation of the non-Markovian dynamics of classical and quantum correlations. Phys Rev A, 2010, 82: 042328
210 Soares-Pinto D O, Celeri L C, Auccaise R, et al. Nonclassical correlation in NMR quadrupolar systems. Phys Rev A, 2010, 81: 062118
211 Terhal B M, Horodecki M, Leung D W, et al. The entanglement of purification. J Math Phys, 2002, 43: 4286–4298
212 DiVincenzo D P, Horodecki M, Leung D W, et al. Locking classical correlations in quantum states. Phys Rev Lett, 2004, 92: 067902
213 Oppenheim J, Horodecki M, Horodecki P, et al. Thermodynamical approach to quantifying quantum correlations. Phys Rev Lett, 2002, 89: 180402
214 Horodecki M, Horodecki P, Horodecki R, et al. Local versus nonlocal information in quantum-information theory: Formalism and phenomena. Phys Rev A, 2005, 71: 062307
215 Luo S. Using measurement-induced disturbance to characterize correlations as classical or quantum. Phys Rev A, 2008, 77: 022301
216 Modi K, Paterek T, Son W, et al. Unified view of quantum and classical correlations. Phys Rev Lett, 2010, 104: 080501
217 Heisenberg W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Z Phys, 1927, 43: 172–198
218 Kennard E H. Zur quantenmechanik einfacher bewegungstypen. Z Phys, 1927, 44: 326–352
219 Robertson H P. The uncertainty principle. Phys Rev, 1929, 34: 163–164
220 Bialynicki-Birula I, Mycielski J. Uncertainty relations for information entropy in wave mechanics. Commun Math Phys, 1975, 44: 129–132
221 Deutsch K. Uncertainty in quantum measurements. Phys Rev Lett, 1983, 50: 631–633
222 Kraus K. Complementary observables and uncertainty relations. Phys Rev D, 1987, 35: 3070–3075
223 Maassen H, Uffink J B. Generalized entropic uncertainty relations. Phys Rev Lett, 1988, 60: 1103–1106
224 Einstein A, Podolsky B, Rosen N. Can quantum mechanical description of physical reality be considered complete? Phys Rev, 1935, 47: 777–780
225 Berta M, Christandl M, Colbeck R, et al. The uncertainty principle in the presence of quantum memory. Nat Phys, 2010, 6: 659–662
226 Renes J M, Boileau J C. Conjectured strong complementary information tradeoff. Phys Rev Lett, 2005, 103: 020402
227 Li C F, Xu J S, Xu X Y, et al. Experimental investigation of the entanglement assisted entropic uncertainty principle. Nat Phys, 2011, 7: 752–756

228 Prevedel R, Hamel D R, Colbeck R, et al. Experimental investigation of the uncertainty principle in the presence of quantum memory. Nat Phys, 2011, 7: 757–761
229 Wolf M M, Eisert J, Cubitt T S, et al. Assessing non-Markovian quantum dynamics. Phys Rev Lett, 2008, 101: 150402
230 Rivas Á, Huelga S F, Plenio M B. Entanglement and non-Markovianity of quantum evolutions. Phys Rev Lett, 2010, 105: 050403
231 Breuer H P, Laine E M, Piilo J. Measure for the degree of non-Markovian behavior of quantum processes in open systems. Phys Rev Lett, 2009, 103: 210401
232 Liu B H, Li L, Huang Y F, et al. Experimental control of the transition from Markovian to non-Markovian dynamics of open quantum systems. Nat Phys, 2011, 7: 931–934
233 Barreiro J T. Environmental effects controlled. Nat Phys, 2011, 7: 927–928
234 Uhrig G S. Keeping a quantum bit alive by optimized π-pulse sequences. Phys Rev Lett, 2007, 98: 100504
235 Du J, Rong X, Zhao N, et al. Preserving electron spin coherence in solids by optimal dynamical decoupling. Nature, 2009, 461: 1265–1268
236 de Lange G, Wang Z H, Ristè D, et al. Universal dynamical decoupling of a single solid-state spin from a spin bath. Science, 2010, 330: 60–63
237 Zhao N, Wang Z Y, Liu R B. Anomalous decoherence effect in a quantum bath. Phys Rev Lett, 2011, 106: 217205
238 Huang P, Kong X, Zhao N, et al. Observation of an anomalous decoherence effect in a quantum bath at room temperature. Nat Commun, 2011, 2: 1579

A survey on quantum information technology

ZHOU ZhengWei, CHEN Wei, SUN FangWen, XIANG GuoYong & LI ChuanFeng

Key Laboratory of Quantum Information (CAS), University of Science and Technology of China, Hefei 230026, China

After nearly three decades of rapid development, the quantum information technology in the theoretical and technical studies has gained remarkable achievements. This review gives a brief introduction to the development of various hot research branches of quantum information technology, including quantum cryptography, quantum communication, quantum computing, quantum simulation, quantum metrology, and fundamental theory of quantum information. In addition, this review also discusses various physical systems which have been well applied in the quantum information technology, such as atomic, molecular and optical physics, different branches in solid state physics (superconducting Josephson Junction system, semiconductor quantum dots, Nitrogen-vacancy color centers in diamond), trapped ions, and nuclear magnetic resonance system. With the investigation and accumulation of quantum information technology, the ability to control microscopic world has been significantly improved. Quantum cryptography has been close to the practical application and the long-distance quantum communication has overcome the practical obstacles in principle. Quantum simulation is close to the limit of the classical computer. Also, quantum metrology has gained rapid development. This review not only shows the situation of the international development of quantum information technology, but also highlights the achievements of China in recent years. These achievements demonstrate that China is an indispensable force in the worldwide quantum information community.

quantum information technology, quantum cryptography, quantum communication, quantum computing, quantum simulation, quantum metrology, fundamental theory of quantum information

doi: 10.1360/972012-224