



# 量子信息技术研究现状与未来

郭光灿

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: gcguo@ustc.edu.cn

收稿日期: 2020-04-29; 接受日期: 2020-05-25; 网络出版日期: 2020-09-16

中国科学院前沿科学重点研究项目“第二次量子革命若干问题的实验研究”(批准号: QYZDY-SSW-SLH003) 资助

**摘要** 量子信息技术是量子力学与信息科学融合的新兴交叉学科, 它的诞生标志着人类社会将从经典技术迈进到量子技术的新时代, 本文将阐述量子信息技术的研究现状与未来. 文中描绘了量子技术发展远景, 即构建各种类型的量子网络, 包括量子云计算网络、分布式量子计算、量子传感网络和量子密钥分配网络等. 量子计算机已从实验室的研究迈进到企业的实用器件研制, 目前已发展到中等规模带噪声量子计算机 (noisy intermediate-scale quantum, NISQ) 的阶段. 在量子技术时代, 没有绝对安全的保密体系, 也没有无坚不摧的破译手段, 信息安全进入“量子对抗”的新阶段.

**关键词** 量子信息技术, 量子网络, 量子计算机, 量子密码

## 1 第二次量子革命

1900 年 Max Planck 提出“量子”概念, 宣告了“量子”时代的诞生. 科学家发现, 微观粒子有着与宏观世界的物理客体完全不同的特性. 宏观世界的物理客体, 要么是粒子, 要么是波动, 它们遵从经典物理学的运动规律, 而微观世界的所有粒子却同时具有粒子性和波动性, 它们显然不遵从经典物理学的运动规律. 20 世纪 20 年代, 一批天才的年轻物理学家建立了支配着微观粒子运动规律的新理论, 这便是量子力学. 近百年来, 凡是量子力学预言的都被实验所证实, 人们公认, 量子力学是人类迄今最成功的理论.

我们将物理世界分成两类: 凡是遵从经典物理学的物理客体所构成的物理世界, 称为经典世界; 而遵从量子力学的物理客体所构成的物理世界, 称为量子世界. 这两个物理世界有着绝然不同的特性, 经典世界中物理客体每个时刻的状态和物理量都是确定的, 而量子世界的物理客体的状态和物理量都是不确定的. 概率性是量子世界区别于经典世界的本质特征<sup>[1]</sup>.

量子力学的成功不仅体现在迄今量子世界中尚未观察到任何违背量子力学的现象, 事实上, 正是量子力学催生了现代的信息技术, 造就人类社会的繁荣昌盛. 信息领域的核心技术是电脑和互联网. 量

**引用格式:** 郭光灿. 量子信息技术研究现状与未来. 中国科学: 信息科学, 2020, 50: 1395–1406, doi: 10.1360/SSI-2020-0112

Guo G C. Research status and future of quantum information technology (in Chinese). Sci Sin Inform, 2020, 50: 1395–1406, doi: 10.1360/SSI-2020-0112

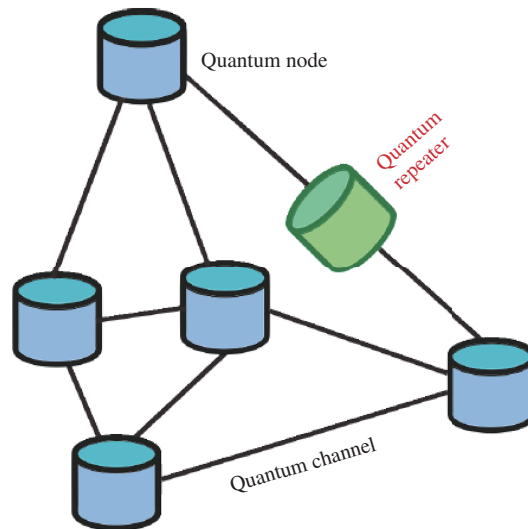


图 1 (网络版彩图) 量子网络  
Figure 1 (Color online) Quantum network

量子力学的能带理论是晶体管运行的物理基础, 晶体管是各种各样芯片的基本单元. 光的量子辐射理论 是激光诞生的基本原理, 而正是该技术的发展才产生当下无处不在的互联网. 然而, 晶体管和激光器 却是经典器件, 因为它们遵从经典物理的运行规律. 因此, 现在的信息技术本质上是源于量子力学的经 典技术.

20 世纪 80 年代, 科学家将量子力学应用到信息领域, 从而诞生了量子信息技术, 诸如量子计 算机、量子密码、量子传感等. 这些技术的运行规律遵从量子力学, 因此不仅其原理是量子力学, 器件本 身也遵从量子力学, 这些器件应用了量子世界的特性, 如叠加性、纠缠、非局域性、不可克隆性等, 因 而其信息功能远远优于相应的经典技术. 量子信息技术突破了经典技术的物理极限, 开辟了信息技术 发展的新方向. 一旦量子技术获得广泛的实际应用, 人类社会生产力将迈进到新阶段. 因此, 我们将量 子信息的诞生称为第二次量子革命, 而基于量子力学研制出的经典技术, 称之为第一次量子革命. 量 子信息技术就是未来人类社会的新一代技术.

## 2 量子网络

量子信息技术最终的发展目标就是研制成功量子网络 (如图 1 所示).

量子网络基本要素包括量子节点和量子信道. 所有节点通过量子纠缠相互连接, 远程信道需要量 子中继. 量子网络将信息传输和处理融合在一起, 量子节点用于存储和处理量子信息, 量子信道用于各 节点之间的量子信息传送.

与经典网络相比, 量子网络中信息的存储和传输过程更加安全, 信息的处理更加高效, 有着更加强 大的信息功能. 量子节点包括通用量子计算机、专用量子计算机、量子传感器和量子密钥装置等. 应 用不同量子节点将构成不同功能的量子网络. 典型的有 (表 1):

- (1) 由通用量子计算机作为量子节点, 将构成量子云计算平台, 其运算能力将强大无比;
- (2) 使用专用量子计算机作为量子节点可以构成分布式量子计算, 其信息功能等同于通用量子计 算机. 亦即应用这种方法可以从若干比特数较少的量子节点采用纠缠通道连接起来, 可以构成等效的

表 1 各类量子网络  
Table 1 Various quantum networks

Quantum nodes	Quantum networks
Universal quantum computers	Quantum cloud computing networks
Specialized quantum computers	Distributed quantum computing networks
Quantum sensors	Quantum sensor networks
Quantum key devices	Quantum key distribution networks

通用量子计算机;

(3) 量子节点是量子传感器, 所构成的量子网络便是高精度的量子传感网络, 也可以是量子同步时钟;

(4) 量子节点是量子密钥装置, 所构成的量子网络便是量子密钥分配 (QKD) 网络, 可以用于安全的量子保密通信.

当然, 单个量子节点本身就是量子器件, 也会有许多应用场景, 量子网络就是这些量子器件的集成, 其信息功能将得到巨大提升, 应用更广泛.

上述的量子网络是量子信息技术领域发展的远景, 当前距离这个远景的实现还相当遥远. 不仅尚无哪种类型量子网络已经演示成功, 即使是单个量子节点的量子器件也仍处于研制阶段, 距离实际的应用仍有着很长的路要走. 即便是单个量子节点研制成功, 要将若干量子节点通过纠缠信道构成网络也极其困难——通常采用光纤作为量子信息传输的通道, 量子节点的量子信息必须能强耦合到光纤通信波长的光子上, 该光子到达下个量子节点处再强耦合到该节点工作波长的量子比特上, 任何节点之间最终均可实现强耦合、高保真度的相干操控, 只有这样才能实现量子网络的信息功能. 目前, 连接多个节点的量子界面仍然处于基础研究阶段.

至于远程的量子通道, 必须有量子中继才能实现, 而量子中继的研制又依赖于高速确定性纠缠光源和可实用性量子存储器的研究, 所有这些核心器件仍然处于基础研究阶段, 离实际应用还很远.

因此整个量子信息技术领域仍然处于初期研究阶段, 实际应用还有待时日.

那么, 量子信息技术时代何时到来? 量子计算机是量子信息技术中最有标志性的颠覆性技术, 只有当通用量子计算机获得广泛实际应用之时, 我们才可断言人类社会已进入量子技术新时代.

3 量子计算机

电子计算机按照摩尔 (Moore) 定律迅速发展: 每 18 个月, 其运算速度翻一番.

20 世纪 80 年代, 物理学家却提出“摩尔定律是否会终结”这个不受人欢迎的命题, 并着手开展研究. 最后竟然得出结论: 摩尔定律必定会终结. 理由是, 摩尔定律的技术基础是不断提高电子芯片的集成度——即单位芯片面积的晶体管数目. 但这个技术基础受到两个主要物理限制: 一是由于非可逆门操作会丢失大量比特, 并转化为热量, 最终会烧穿电子芯片, 这也是当下大型超算中心遇到的巨大能耗困难所在; 二是终极的运算单元是单电子晶体管, 而单电子的量子效应将影响芯片的正常工作, 使计算机运算速度无法如预料地提高.

物理学家的研究结果并不影响当时摩尔定律的运行, 多数学者甚至认为物理学家是杞人忧天. 然而物理学家并未停止脚步, 着手研究第 2 个问题: 摩尔定律失效后, 如何进一步提高信息处理的速度——即后摩尔时代提高运算速度的途径是什么? 研究结果诞生了“量子计算”的概念. 1982 年美国物理

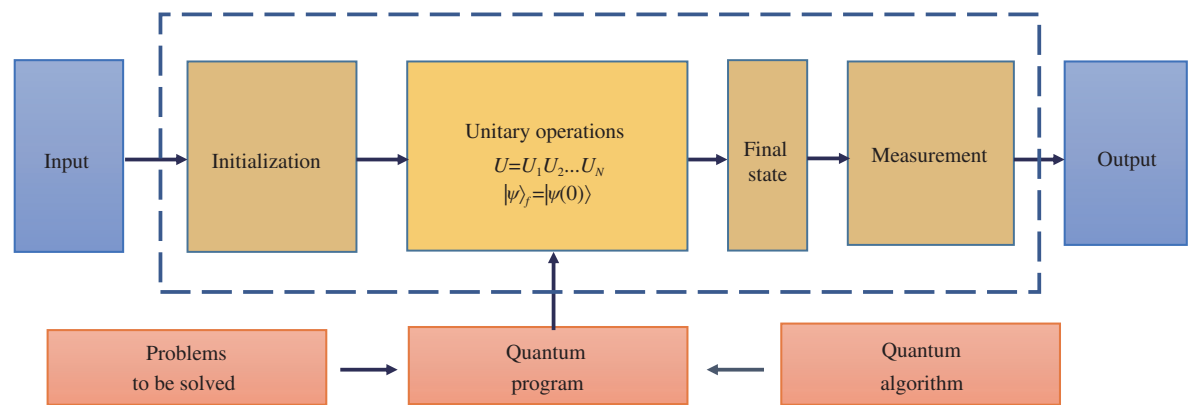


图 2 (网络版彩图) 量子计算机的工作原理  
Figure 2 (Color online) Operating principle of quantum computer

学家 Feynman 指出<sup>[2]</sup>, 在经典计算机上模拟量子力学系统运行存在着本质性困难, 但如果可以构造一种用量子体系为框架的装置来实现量子模拟就容易得多. 随后英国物理学家 Deutsch 提出“量子图灵机”<sup>[3]</sup>概念, “量子图灵机”可等效为量子电路模型. 从此, “量子计算机”的研究便在学术界逐渐引起人们的关注. 1994 年 Shor<sup>[4]</sup>提出了量子并行算法, 证明量子计算可以求解“大数因子分解”难题, 从而攻破广泛使用的 RSA 公钥体系, 量子计算机才引起广泛重视. Shor 并行算法是量子计算领域的里程碑工作. 进入 21 世纪, 学术界逐渐取得共识: 摩尔定律必定会终结<sup>[5]</sup>. 因此, 后摩尔时代的新技术便成为热门研究课题, 量子计算无疑是最有力的竞争者.

量子计算应用了量子世界的特性, 如叠加性、非局域性和不可克隆性等, 因此天然地具有并行计算的能力, 可以将某些在电子计算机上指数增长复杂度的问题变为多项式增长复杂度, 亦即电子计算机上某些难解的问题在量子计算机上变成易解问题. 量子计算机为人类社会提供运算能力强大无比的新的信息处理工具, 因此称之为未来的颠覆性技术. 量子计算机的运算能力同电子计算机相比, 等同于电子计算机的运算能力同算盘相比. 可见一旦量子计算得到广泛应用, 人类社会各个领域都将会发生翻天覆地的变化.

量子计算的运算单元称为量子比特, 它是 0 和 1 两个状态的叠加. 量子叠加态是量子世界独有的, 因此, 量子信息的制备、处理和探测等都必须遵从量子力学的运行规律. 量子计算机的工作原理如图 2 所示.

量子计算机与电子计算机一样, 用于解决某种数学问题, 因此它的输入数据和结果输出都是普通的数据. 区别在于处理数据的方法本质上不同. 量子计算机将经典数据制备在量子计算机整个系统的初始量子态上, 经由幺正操作变成量子计算系统的末态, 对末态实施量子测量, 便输出运算结果. 图 2 中虚框内都是按照量子力学规律运行的. 图中的幺正操作 ( $U$  操作) 是信息处理的核心, 如何确定  $U$  操作呢? 首先选择适合于待求解问题的量子算法, 然后将该算法按照量子编程的原则转换为控制量子芯片中量子比特的指令程序, 从而实现了  $U$  操作的功能. 量子计算机的实际操作过程如图 3 所示.

给定问题及相关数据, 科学家设计相应的量子算法, 进而开发量子软件实现量子算法, 然后进行量子编程将算法思想转化为量子计算机硬件能识别的一条条指令, 这些指令随后发送至量子计算机控制系统, 该系统实施对量子芯片系统的操控, 操控结束后, 量子测量的数据再反馈给量子控制系统, 最终传送到工作人员的电脑上.



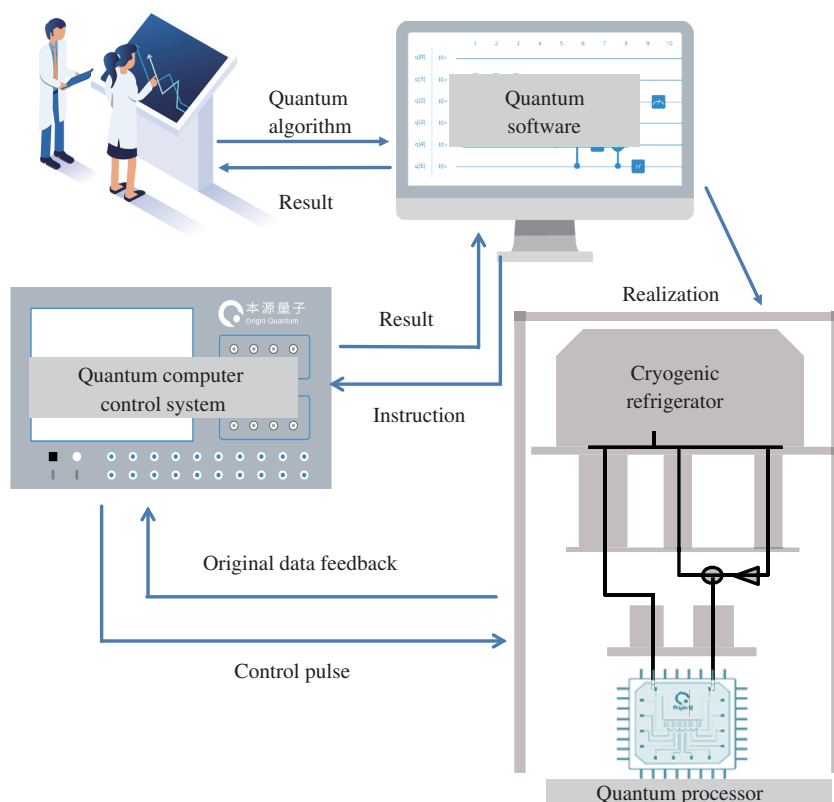


图 3 (网络版彩图) 量子计算机的实际操作过程

Figure 3 (Color online) Operating process of quantum computer

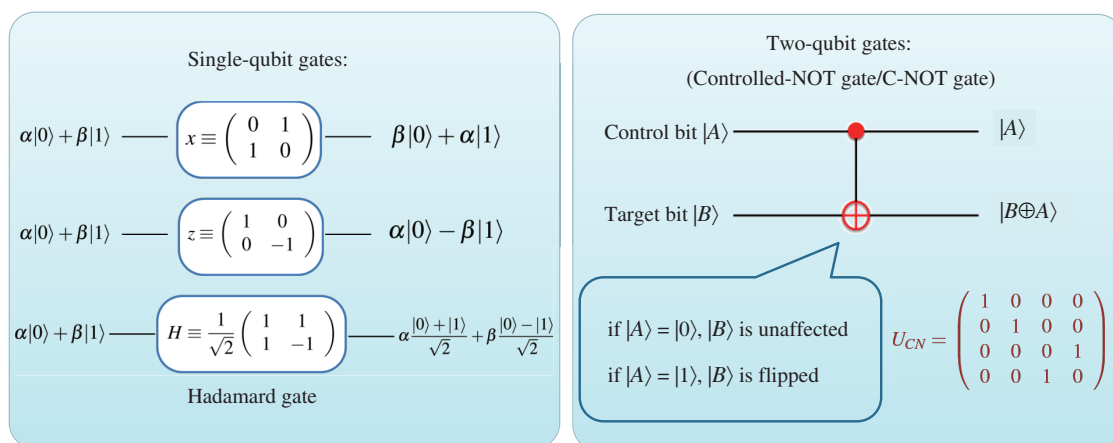


图 4 (网络版彩图) 单双量子比特门

Figure 4 (Color online) Single and double qubit gates

量子逻辑电路是用于实现  $U$  变换的操作, 任何复杂的  $U$  操作都可以拆解为单量子比特门  $U_i$  和双量子比特门  $U_{jk}$  的某种组合 (即可拆解定理),  $U_i$  和  $U_{jk}$  是最简单的普适逻辑门集. 典型的单双比特门如图 4 所示 [6~8].

基于量子图灵机 (量子逻辑电路) 的量子计算称为标准量子计算, 现在还在研究的其他量子计算模型还有: 单向量子计算、拓扑量子计算和绝热量子计算 (量子退火算法) 等。

量子计算机是宏观尺度的量子器件, 环境不可避免会导致量子相干性的消失 (即消相干), 这是量子计算机研究的主要障碍<sup>[9]</sup>。“量子编码”用于克服环境的消相干, 它增加信息的冗余度, 用若干物理量子比特来编码一个逻辑比特 (信息处理的单元)。业已证明, 采用起码 5 个量子比特编码、1 个逻辑比特, 可以纠正消相干引起的所有错误。量子计算机实际应用存在另一类严重的错误, 这种错误来源于非理想的量子操作, 包括门操作和编码的操作。科学家提出容错编码原理来纠正这类错误, 该原理指出, 在所有量子操作都可能出错的情况下, 仍然能够将整个系统纠正回理想的状态。这涉及到“容错阈值定理”, 即只有量子操作的出错率低于某个阈值, 才能实现量子容错。容错阈值与量子计算的实现构型有关, 在一维或准一维的模型中, 容错的阈值为  $10^{-5}$ <sup>[6]</sup>, 在二维情况 (采用表面码来编码比特), 阈值为  $10^{-2}$ 。经过科学家十多年的努力, 现在离子阱和超导系统的单双比特操作精度已经达到这个阈值。这个进展极大地刺激了人们对量子计算机研制的热情, 量子计算机的实现不再是遥不可及的。量子计算机的研制逐步走出实验室, 成为国际上各大企业追逐的目标。

量子计算机研制涉及以下关键技术部件: (1) 核心芯片, 包括量子芯片及其制备技术; (2) 量子控制, 包括量子功能器件、量子计算机控制系统和量子测控技术等; (3) 量子软件, 包括量子算法、量子开发环境和量子操作系统等; (4) 量子云服务, 即面向用户的量子计算机云服务平台。

量子计算机的研制从以科研院校为主体变为以企业为主体后发展极其迅速。2016 年 IBM 公布全球首个量子计算机在线平台, 搭载 5 位量子处理器。量子计算机的信息处理能力非常强大, 传统计算机到底能在多大程度上逼近量子计算机呢? 在不是非常大的逻辑深度下, 2018 年初创公司合肥本源量子计算科技有限公司推出当时国际最强的 64 位量子虚拟机, 打破了当时采用经典计算机模拟量子计算机的世界纪录。2019 年量子计算机研制取得重大进展: 年初 IBM 推出全球首套商用量子计算机, 命名为 IBM Q System One, 这是首台可商用的量子处理器 (图 5(a) 和 (b))。2019 年 10 月, Google 在 *Nature* 上发表了一篇里程碑论文, 报道他们用 53 个量子比特的超导量子芯片, 耗时 200 s 实现一个量子电路的采样实例, 而同样的实例在当今最快的经典超级计算机上可能需要运行大约 1 万年。他们宣称实现了“量子霸权”, 即信息处理能力超越了任何最快的经典处理器 (图 5(c) 和 (d))。

总之, 量子计算机研制已从高校、研究所为主发展为以公司为主力, 从实验室的研究迈进到企业的实用器件研制。量子计算机将经历 3 个发展阶段。

**(1) 量子计算机原型机。**原型机的比特数较少, 信息功能不强, 应用有限, 但“五脏俱全”, 是地地道道地按照量子力学规律运行的量子处理器。IBM Q System One 就是这类量子计算机原型机。

**(2) 量子霸权。**量子比特数在 50~100 左右, 其运算能力超过任何经典的电子计算机。但未采用“纠错容错”技术来确保其量子相干性, 因此只能处理在其相干时间内能完成的那类问题, 故又称为专用量子计算机。这种机器实质是中等规模带噪声量子计算机 (noisy intermediate-scale quantum, NISQ)。应当指出, “量子霸权”实际上是指在某些特定的问题上量子计算机的计算能力超越了任何经典计算机。这些特定问题的计算复杂度经过严格的数学论证, 在经典计算机上是指数增长或超指数增长, 而在量子计算机上是多项式增长, 因此体现了量子计算的优越性。目前采用的特定问题是量子随机线路的问题或玻色取样问题。这些问题仅是 Toy (玩具) 模型, 并未发现它们的实际应用。因此, 尽管量子计算机已迈进到“量子霸权”阶段, 但在中等规模带噪声量子计算 (NISQ) 时代面临的核心问题是探索这种专门机的实际用途, 并进一步体现量子计算的优越性。

**(3) 通用量子计算机。**这是量子计算机研制的终极目标, 用来解决任何可解的问题, 可在各个领域获得广泛应用。通用量子计算机的实现必须满足两个基本条件, 一是量子比特数要达到几万到几百万

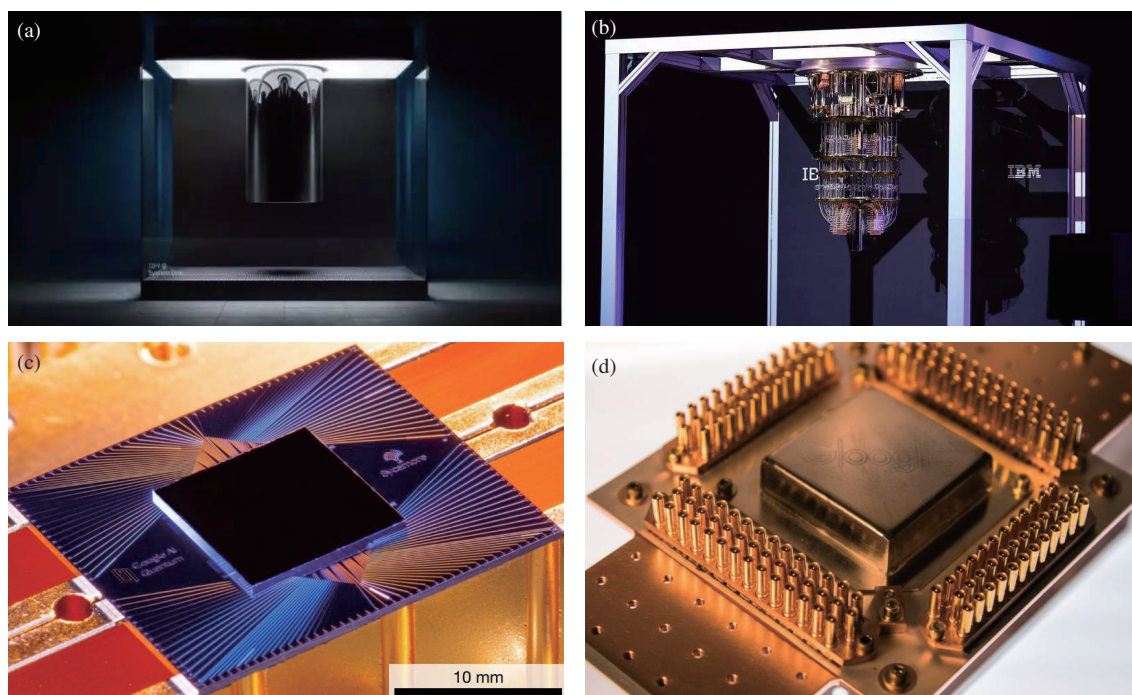


图 5 (网络版彩图) 2019 年量子计算机的研制取得重大进展. (a), (b) IBM 推出的全球首套商用量子计算机 IBM Q System One; (c), (d) Google 推出的 53 个量子比特的超导量子芯片

**Figure 5** (Color online) Great progress on development of quantum computer in 2019. (a), (b) The shielded and internal structure of the dilution refrigerator from IBM Q System One. (c), (d) Photographs of the sycamore chip. A 53-qubit quantum chip from Google.

量级, 二是应采用“纠错容错”技术. 鉴于人类对量子世界操控能力还相当不成熟, 因此最终研制成功通用量子计算机还有相当长的路要走.

#### 4 量子技术时代的信息安全

量子计算机具有强大的信息处理能力, 对现代密码技术构成了严重挑战, 量子技术时代的信息安全问题便成为人们关注的焦点之一. 现代保密通信的工作图如图 6 所示.

Alice 将欲发送的明文 (即数码信息) 输入进加密机, 经由某种密钥变换为密文, 密文在公开信道中传递给合法用户 Bob, 后者使用特定密钥经由解密机变换为明文. 任何窃听者都可从公开信道上获取密文, 窃听者 Eve 如果拥有与 Bob 相同的密钥, 便可轻而易举地破译密文. 如果窃听者虽不拥有破译的密钥, 但他具有很强的破译能力, 也可能获得明文. 只有当窃听者肯定无法从密文中获取明文, 这种保密通信才是安全的.

按照 Alice 与 Bob 拥有的密钥是否相同, 保密过程可分为私钥体系 (A 与 B 的密钥相同) 和公钥体系 (A 和 B 的密钥不同, 且 A 的密钥是公开的).

公钥体系是基于复杂算法运行的, 其安全性取决于计算复杂度的安全; 私钥体系一般也是基于复杂算法, 其安全性同样取决于计算复杂度的安全. 只有“一次一密”的加密方式 (即密钥长度等于明文长度, 且用过一次就不重复使用), 这种私钥体系的安全性仅取决于密钥的安全性, 与计算复杂度无关. 当前密钥分配的安全性取决于人为的可靠性.

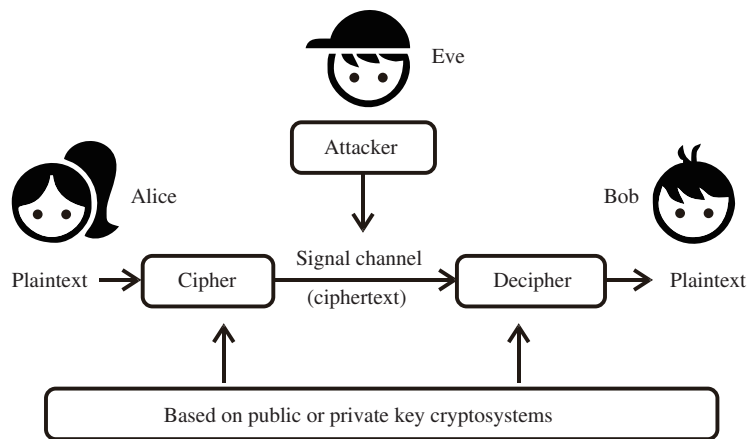


图 6 保密通信

Figure 6 Secure communication

量子计算机可以改变某些函数的计算复杂度, 将电子计算机上指数复杂度变成多项式复杂度, 从而挑战所有依赖于计算复杂度的密码体系的安全性. 唯有“一次一密”加密方法能经受住量子计算机的攻击, 这种方案的安全性仅依赖于密钥的安全性.

因此, 量子技术时代确保信息安全必须同时满足两个条件:

- (1) “一次一密”加密算法. 这要求密钥生成率要足够高;
- (2) 密钥“绝对”安全. 当前使用的密钥分配都无法确保绝对安全.

物理学家针对现有密钥分配方法无法确保“一次一密”方案中所使用的密钥的安全性, 提出了“量子密码”方案. 这种新的密码的安全性不再依赖于计算复杂度和人为可行性, 而仅仅取决于量子力学原理的正确性.

物理学家提出了若干量子密码协议 (如 BB84), 并从信息论证明, 这类协议是绝对安全的, 这就激励了越来越多科学家加入“量子密码”研究行列. 但人们很快就发现, 任何真实物理体系都无法达到量子密码协议所需求的理想条件, 存在着各种各样的物理漏洞, 使得研制出来的实际量子密码系统无法达到“绝对”安全, 只能是“相对”安全. 虽然可以经过努力堵住各种各样的物理漏洞, 甚至提出安全性更强的新的密码协议 (如设备无关量子密码协议等), 但终归无法确保真实的量子密码物理系统可以做到“绝对”安全<sup>[10]</sup>.

那么这种相对安全的“量子密码”是否可获得实际应用呢? 答案是肯定的. 如果能验证真实的量子密码体系可以抵抗现有所有手段的攻击, 就可以认定这类“量子密码”在当下是安全的, 可以用于实际.

中国科学院量子信息重点实验室长期从事量子密码研究, 2005 年发明了量子密码系统稳定性的方法, 首次在商用光纤实现从北京到天津 125 km 的量子保密通信演示 (图 7). 2007 年发明了量子路由器, 在商用光纤网络中实现 4 节点的量子保密通信 (图 8). 2009 年构造了芜湖量子政务网, 演示了量子密码的实际应用 (图 9).

当前量子密码的研究状况是:

- (1) 城域 (百公里量级) 网已接近实际应用, 密钥生成率可满足“一次一密”加密的需求, 现有各种攻击手段无法窃取密钥而不被发现. 当前必须建立密钥安全性分析系统以检查实际量子密码系统是否安全, 并制定相应的“标准”.



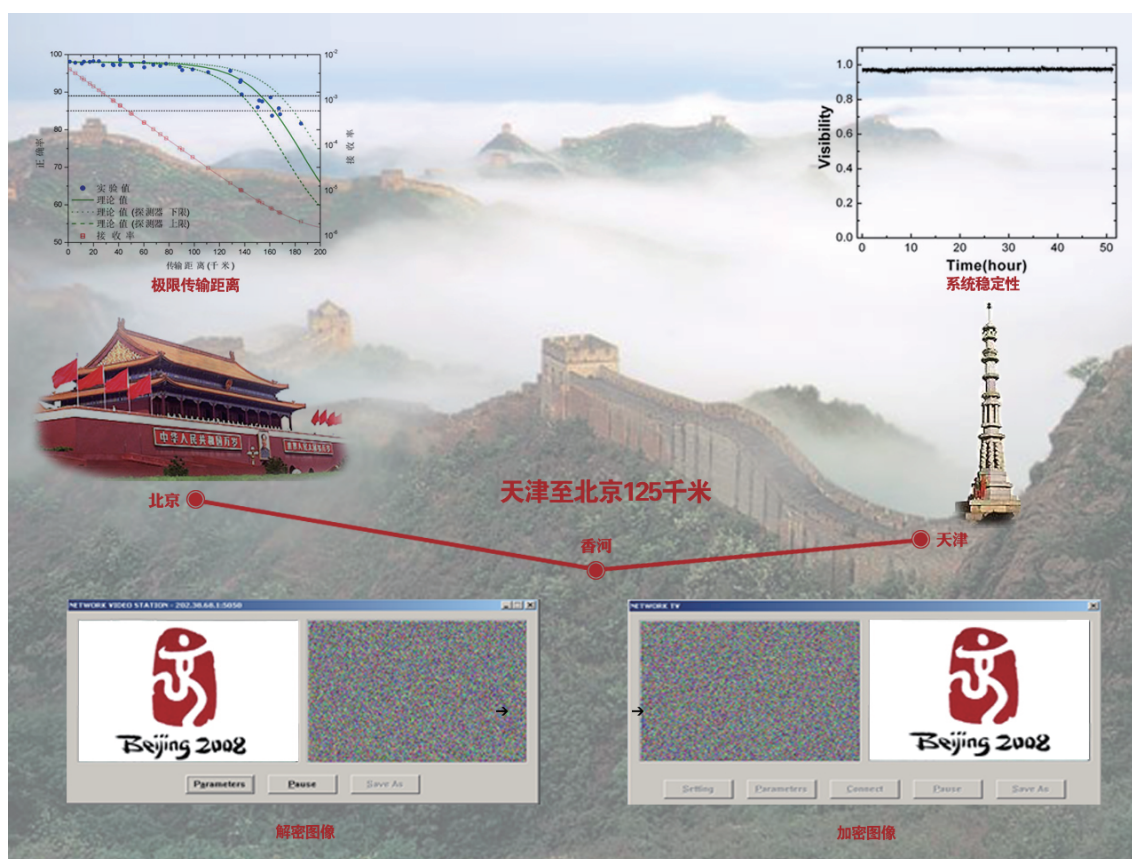


图 7 (网络版彩图) 2005 年北京 – 天津 125 km 量子保密通信演示网  
 Figure 7 (Color online) QKD demo network between Beijing and Tianjin in 2005

(2) 城际网的实用仍然相当遥远, 关键问题是可实用的量子中继器件尚未研制成功. 构建量子中继的核心技术是可实用的量子存储器和高速率的确定性纠缠光源, 这两种技术尚未取得突破性进展.

(3) 经由航空航天器件实现全球的量子保密通信网络, 建造这个网络困难重重, 除了密钥安全性及高速率的密钥生成器的问题之外, 还有如何实现全天候量子密钥高速分配. 国家是否需要建设这种网络应当慎重研究.

总之, 量子技术时代解决信息安全有两个途径:

(1) 物理方法 (适用于私钥体系). 不断提高实际量子密码系统的安全性, 能够抵抗当下各种手段的攻击, 确保密钥的安全性, 再加上“一次一密”加密, 可以使得私钥体制获得实际应用.

(2) 数学方法 (适用于公钥体系). 寻找能抵抗量子计算攻击的新型公开密钥体系. 其原理是, 目前无法证明量子计算机可以改变所有复杂函数的计算复杂度, 因而可以找到新的不被量子计算机攻破的新型公开密钥体系. 当然, 量子计算机的攻击能力依赖于量子算法, 当前最强攻击的首推 Shor 算法. 如果有比它更强大的量子算法出现, 那么这种新型公开密码体系有可能被攻破, 进而促使数学家再去寻找抵抗能力更强的公钥体系. 这将导致从“电子对抗”发展到“量子对抗”.

结论: 量子技术时代没有绝对安全的保密体系, 也没有无坚不摧的破译手段, 信息安全的攻防将进入“量子对抗”的新阶段.

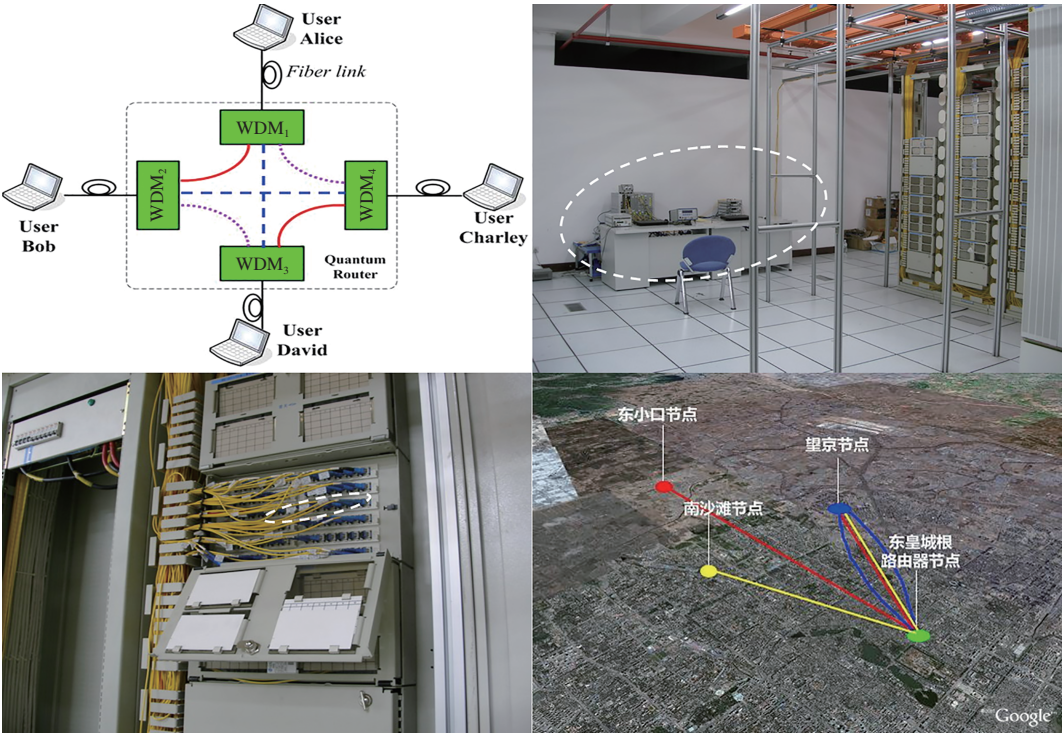


图 8 (网络版彩图) 2007 年北京 4 节点量子保密通信演示网  
Figure 8 (Color online) 4-nodes QKD demo network, Beijing, 2007



图 9 (网络版彩图) 2009 年安徽芜湖量子政务网  
Figure 9 (Color online) QKD network for government, Wuhu, Anhui, 2009



## 参考文献

- 1 von Neumann J. Mathematical Foundations of Quantum Mechanics. Princeton: Princeton University Press, 1955
- 2 Feynman R P. Simulating physics with computers. *Int J Theory Phys*, 1982, 21: 467–488
- 3 Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. In: *Proceedings of the Royal Society of London*, 1985. 97–117
- 4 Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science*, Santa Fe, 1994
- 5 Waldrop M M. The chips are down for Moore's law. *Nature*, 2016, 530: 144–147
- 6 Nielsen M A, Chuang I L. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000
- 7 DiVincenzo D P. The physical implementation of quantum computation. *Fortschr Phys*, 2000, 48: 771–783
- 8 Li C Z. *Quantum Communication and Quantum Computation*. Changsha: National University of Defense Technology Press, 2000 [李承祖. 量子通信与量子计算. 长沙: 国防科技大学出版社, 2000]
- 9 Schlosshauer M A. *Decoherence and the Quantum-to-Classical Transition*. Berlin: Springer, 2007
- 10 Brassard G. Brief history of quantum cryptography: a personal perspective. In: *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security*, Awaji Island, 2005. 19–23

## Research status and future of quantum information technology

Guangcan GUO

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

E-mail: gcguo@ustc.edu.cn

**Abstract** Quantum information technology is an emerging interdisciplinary field of quantum mechanics and information science, whose birth will promote a new era of human intelligence from classical technology to quantum technology. This paper elaborates on the research status and future of the field of quantum information technology. Moreover, this paper shows the vision of quantum technology, i.e., the construction of various types of quantum networks, including quantum cloud computing networks, distributed quantum computing, quantum sensor networks, and quantum key distribution networks. Quantum computers have transformed research from the laboratory to the development of practical devices led by these enterprises. Currently, research and development of quantum computers have shifted to the stage of noisy intermediate-scale quantum computers (NISQ). In the era of quantum technology, there is no absolutely secure secrecy system or omnipotent way of deciphering Information and information security has entered a new stage of “quantum offense and defense.”

**Keywords** quantum information technology, quantum networks, quantum computers, quantum cryptography



**Guangcan GUO** was born in 1942. He graduated from the Department of Radio Electronics, University of Science and Technology of China (USTC) in 1965. He was elected as a member of the Chinese Academy of Sciences in 2003 and a member of the Academy of Sciences for the Developing World in 2009. His major research interests involve theoretical and experimental studies of quantum optics, quantum cryptography, quantum communication, and quantum computing.