摩石观察

密码是保障网络安全的核心技术和基础支撑，在维护国家安全、促进经济社会发展、保护人民群众利益中发挥着不可替代的重要作用。云物移大智的蓬勃发展，5G、智慧城市、互联网＋政务服务的全力推进，离不开用密码技术来保障网络安全、保护数据安全、保证网上诚信，需要密码学与其它学科深入合作，需要密码产业与其它产业的深度融合，需要产学研管用的真诚协作，需要全社会共同传播密码知识与政策、研究密码应用技术、推进密码应用方案。

为激浊扬清，构建以密码技术为核心、多种技术相互融合的新网络安全体系，推进密码技术科学规范应用，长期深耕于信息安全一线的卫士通公司凝聚了一批国内顶尖的密码专家于2016年建立了摩石实验室。依托密码基础理论，探索密码创新实践，解决密码应用难题，培养密码专业人才，摩石实验室致力于让密码技术更好地服务于网络强国、数字中国和智慧社会。

本着共同的愿景，《信息安全与通信保密》杂志社与摩石实验室精诚合作，专门开辟《摩石观察》栏目。立足于密码本真，反思密码实践，《摩石观察》将以密码人的细致严谨叩问密码创新的真理之门，为广大读者了解、认识、掌握、使用密码技术提供准确规范的参考依据；同时我们期望以密码会友，与理想作伴，热忱邀请有志之士共同探索密码理论与应用的最佳实践，为推动金融等重要领域密码应用与创新发展而奋斗。

量子计算机能否改变世界?

陈克非[1,2]
（1 杭州师范大学理学院；2 卫士通摩石实验室）

编者按：量子计算是一种利用量子特性的新型计算技术。目前，量子计算机的计算能力正在逐步提高，但受限于理论及技术问题，目前距离建造出真正的通用量子计算机还较遥远。本文介绍了量子计算、量子算法及量子计算机的研究进展，并对量子计算的未来进行了展望。

1 量子计算机能否分解大整数?

去年夏天，在引人瞩目的 2017 国际密码大会 (Crypto2017) 上，加州大学圣巴巴拉分校约翰·马提尼斯（John Martinis）教授的特邀报告“量子整数分解计算机展望（Prospects for a quantum factoring machine）”中介绍了他所领导的 Google 量子计算机团队的工作 [图 1]，他坦承要真正做出稳定实用高效的量子计算机还有很多的路要走，想要使用量子计算机破解现在主流采用的 RSA 密码，10 年之内几乎不可能实现，因为有太多的技术问题需要解决， 在他看来这些真的很困难。

图 1. 约翰·马提尼斯教授在做“量子整数分解计算机展望”的特邀报告

经典计算机，利用 1 和 0 来表示经典物理量（如电流、电压等）的有与无，因而 1 和 0 组成的比特（bit，信息量单位）就可用来存储和处理信息。比特的值要么是 1，要么是 0。任何经典信息都只不过是由“1”和“0” 组成的一个长序列。

在量子力学中，光子偏振态、电子的自旋态、离子的能级、量子纠缠等物理量都具有两个状态。这两个状态可以编码成量子比特（qubit）的 1 和 0， 但另一方面这些系统遵循量子叠加原理，一个量子位可以同时处于 1 状态和 0 状态，即处于一种叠加状态 [图 2]。若用量子比特来存储数据，由于量子特性，n 个量子比特的存储器可以存储 2^n 个数据，数据存储能力随着量子比特数的增多而呈指数级增长。

量子计算机利用量子特性来完成计算。由于量子叠加效应，n 比特的量子计算机可同时处于 2^n 种状态，当量子计算终止时，2^n 种状态因为测量而坍塌到一种确定的状态，从而完成计算 [1]。量子计算机的一次操作同时完成了对 2^n 个数据的操作，相当于经典计算机完成了对 2^n 个数据的并行处理。所以说，这种叠加性让量子比特能够比比特编码处理多得多的信息，这就是量子计算机相对于经典计算机的优势。

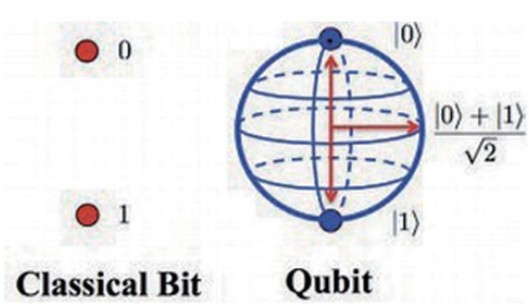

图 2. 经典比特与量子比特

量子叠加特性使得量子计算具有极强的并行处理能力，但另一方面，该特性也导致量子态的不稳定和难以操控。很多人往往只注意到量子计算的空前竞争是比谁能够操控更多量子比特数，而实际情况是做到稳定精确有效地操控量子比特，降低量子比特运算过程中所产生的误差，这可能是更难的。由于量子计算机错

误率高的问题，一些科学家和数学家质疑它们的实用性。谷歌和其他的公司称该问题可通过纠错算法来解决，但那些算法需要更多的量子比特来检查进行运算的量子比特的工作。有的专家估计，检查单个量子比特的工作将需要额外增加 100 个量子比特。

2 量子计算机研究进展

上面提到量子力学原理是下一代计算革命的关键所在。在加州圣巴巴拉的一个小型实验室里，马提尼斯领导的谷歌物理学家和工程师在利用量子力学来打造运算潜力令人瞠目结舌的计算机 [图 3]。可靠的规模化量子计算机有望改变从 AI 到化学的各行各业，加速机器学习的发展，带来新型的材料、化学物和药物。

2017 年 10 月 17 日 Intel 公司发布了包含 17 个量子位的超导测试芯片 [图 4]，之前只有 IBM 公司推出相同规模量子计算芯片。同一天，IBM 宣布量子计算已经突破了 49 量子比特的障碍（Quantum computing—breaking through the 49 qubit simulation barrier）[图 5]，在全球范围量子计算机领域的公认领跑者是 IBM 和 Google。2017 年 4 月份，Google 开发出具有 9 个量子位的计算芯片；2017 年 5 月，IBM 展示了首个包含 17 个量子位的芯片。IBM 的成果基于耶鲁大学教授罗伯特·施罗科夫（Robert Schoelkopf）的研究，而 IBM 的团队中也有他的多名博士生和研究生。Google 的工作则基于加州大学圣巴巴拉分校教授约翰·马提尼斯（John Martinis）的研究，他的研究团队自 2014 年获得了谷歌的支持，并开展合作研究。

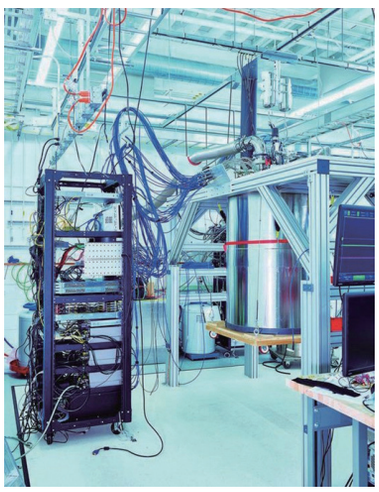

图 3.Google 位于加州圣巴巴拉的实验室里，量子芯片被冻结在悬在空中的低温恒温器里

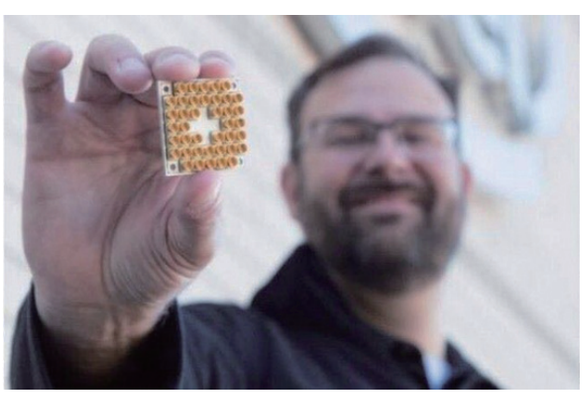

图 4.Intel 公司展示的 17 个量子位的超导测试芯片

2017 年 5 月，中国科技大学研究团队宣布通过电控可编程的光量子线路构建出可用于多光子“玻色取样”任务的光量子计算模拟机。有人认为中科大的工作应该还属于实验室里的原理机，还算不上通用的量子计算机。

目前，各大科技公司的研究员都在开发包含 50 个量子位的芯片。这样的芯片计算能力将超过当前所有超级计算机。目前还不清楚，在获得如此强大的计算能力之后，我们可以做些什么，解决什么样的问题。不过，目前的挑战主要是开发规模更大的量子计算机。

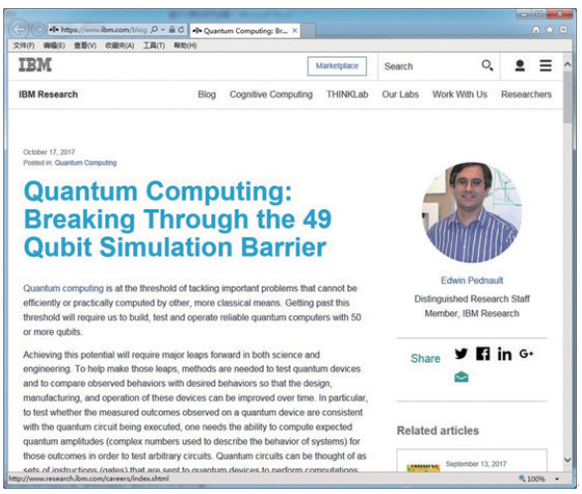

图 5.IBM 公司宣布量子计算突破 49Qubit

Intel 研究人员表示，量子位极其脆弱， 任何噪声或无意的干扰都会令量子位丢失数据。此外，量子位依靠超导体金属，而这样的超导体必须处于极低的温度下。Intel 表示， 量子位的运行温度为“20 毫开尔文”，比太空冷 250 倍，制造并维持这样的环境难度很大。除了低温之外，量子位的开发还有其他问题。随着量子计算机的规模越来越大，可能发生的故障类型也越来越多。

3 量子计算与量子算法

1936 年，Alan Turing 提出 Turing 机模型，通过机器来模拟人们的计算过程。该模型隐含的观点是一台装有足够资源的计算机能实现任何合理的算法。

1982 年， Richard Feynman 发现在经典计算机上难以模拟量子过程，该模拟过程需要超指数级的存储空间和运行时间，指出 Turing 机的功能也许并没有人们所想的那么强大。Feynman 提出将量子力学与经典计算机结合起来，引入量子计算的概念。

关于量子计算，目前已经取得了很多进展，如开发建造量子比特数越来越大的芯片等，这使人们感觉似乎只要工程技术进步就可以实现大型通用量子计算机的建造。然而，事实上关于量子计算机的基础物理问题并没有得到完全解决，而这些与量子计算技术的实现紧密相关。

量子比特所能做的事情与电子比特所能做的事情并无本质上的区别。只是由于量子特性，量子比特能够同时处于两种叠加状态，且处于相干态的多个量子比特在执行特定的计算任务时，一个量子比特的变化会影响所有其它量子比特，从而使量子计算相比于经典计算机具有极大的并行加速能力。

要实现量子加速，参与计算的量子比特必须处于量子相干状态中。当前，受限于工程技术能力，人们所建造的量子相干系统所能维持的相干状态时间不超过一秒，且随着量子比特数的增多，系统与周围环境相互影响越来越大，保持相干态也越来越困难。

除了要保持相干态外，环境中的各种噪音都可能干扰量子计算，因此它还面临着噪声干扰导致的出错问题。由于量子比特一旦观测就会坍塌到一个特定状态，无法通过直接观测特定的量子比特来确定是否出错。为建造一个具有自我纠错能力的逻辑量子比特，需要更多的实际量子比特，距离建造出可实用的量子计算机还有很大的距离。

经典计算问题本质上是一系列算符操作，可以通过门电路来实现。谈到量子计算也是类似，

我们对应着 n 个 qubit，对其执行一系列算符操作，最后执行测量得到计算结果。如图 6，我们常常画出横着并排的 n 条直线，从左到右代表着时间顺序，而不同的直线代表不同的 qubit；在这些直线上排列着各种小方块大方块还有竖线，代表着各种不同的单 qubit 或多 qubit 幺正算符，每一个幺正算符被称为一个（量子）门 U；主要的几种量子门如翻转门 σ X，Hadmard 门 H、控制非门等，人们可以将一些简单的量子门组合成更复杂的量子门；整张图就被称为一个量子网络 / 量子电路 [图 6]。

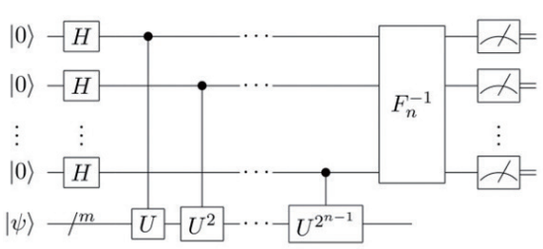

图 6. 由量子门组成的复杂量子电路

1994 年，Peter Shor 提出了一个能在多项式时间内分解给定整数的量子算法 [2]。这意味着，一个具有足够量子比特数的量子计算机可以破解 RSA 算法。2001 年，IBM 的研究人员在基于核磁共振的 7 量子比特计算机上实现整数 15 的素因子分解，到 2014 年人们已可在量子计算机上运行 Shor 算法分解整数 56153。RSA 算法是当前广泛使用的公钥密码体制之一，随着量子计算机能力的增强，此类公钥密码体制的安全性将受到严重威胁。

1996 年，贝尔实验室科学家 Lov Grover 提出 Grover 量子搜索算法 [3]。对于一个无序数据库，最优的经典算法的搜索复杂度为 O(N)，而该搜索算法可将搜索复杂度降低至 $O(\sqrt{N})$，从而对于经典分组密码算法的穷举攻击可以起到平方加速的作用。例如，对 AES-128 算法的穷举攻击，经典计算机下的复杂度为 2^{128}，而使用 Grover 算法在量子计算机的复杂度可降低至 $\sqrt{2^{128}} = 2^{64}$。

4 结束语

自从经典计算机出现，模拟电子电路就以促进更快的计算机设计为其任务之一。同时，计算机的高速发展也加快了模拟电子电路的进步。这一反馈循环一直在促进计算机工业半个世纪以来爆炸式的发展。量子计算机具有潜力把这一爆炸式的发展转变得更具活力，如同量子计算机用于创造更快更有力的量子计算元件一样。

自上世纪八十年代初人们提出量子计算以来，从最初的质疑到最近几年 IBM、微软、谷歌、D-Wave 等公司不断刷新量子计算机的量子比特数、计算能力，量子计算热潮持续不断。然而到目前为止，人类还没造出真正意义上的通用量子计算机，主要原因在于量子比特的质量比数量更重要：量子比特数做大并非难事，真正的困难是如何在芯片做大的同时保证每个量子比特的相干时间以及量子逻辑门和量子测量的保真度。限于当前量子计算机的发展水平，量子计算机对传统密码学的威胁还较小，且人们针对性地设计了一些能抵御量子计算机攻击的密码算法，储备了大量的相关密码技术，可缓解量子时代的信息安全问题。另一方面，目前关于量子密码的研究还

仅局限于量子密钥分发，对基于量子特性的量子密码算法研究还较少。在大型通用量子计算机出现时，新型量子算法可能出现井喷，人们可以利用量子特性来提高密码算法的安全性，也可以利用量子特性对密码算法进行攻击。事实上，从可计算性的角度看，图灵机模型下的可计算问题与量子计算模型下的可计算问题是等价的，也就是说量子计算机的优势可能只是在计算复杂度方面；但是从目前几个有效的量子加速算法看，在大幅度降低计算复杂度的同时，其空间复杂度却呈现快速增长。在处理很多规模巨大的实际问题时，我们关心的复杂度 = 时间复杂度 × 空间复杂度，在这个意义下如果某种加速算法虽然时间很快，但同时带来空间复杂度指数级增长，那么要想突破解决实际问题计算上瓶颈的作用就非常有限。因此，未来量子计算机能给人类社会带来怎样的冲击，我们将拭目以待。

参考文献

[1] 维基百科 . Quantum computing[EB/OL].
https://www.wikipedia.org/(2018-09-05)
https://en.wikipedia.org/wiki/Quantum_computing.

[2] 维基百科 . Shor’s algorithm[EB/OL].
https:/www.wikipedia.org/(2018-09-01)
https://en.wikipedia.org/wiki/Shor%27s_algorithm.

[3] 维基百科 . Grover’s algorithm[EB/OL].
https://www.wikipedia.org/(2018-08-21)
https://en.wikipedia.org/wiki/Grover%27s_algorithm.

作者简介：

陈克非，杭州师范大学教授，卫士通摩石实验室兼职专家，主要研究方向为密码理论与应用。

名词解释：

幺正算符：对一个矩阵，如果该矩阵乘以它的伴随矩阵等于单位阵，则称该矩阵为幺正算符。

量子纠缠：量子纠缠是是一种量子力学现象，它描述了两个粒子互相纠缠，即使相距遥远距离，一个粒子的行为将会影响另一个的状态 。