量子计算是把双刃剑

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Quantum Computing Brings Promise and Threats		
原文作者	Lisa Morgan	原文发布日期	2017 年 10 月 26 日
作者简介	Lisa Morgan 是一位自由撰稿人，负责大数据和商业智能领域。https://www.informationweek.com/author-bio.asp?author_id=2250		
原文发布单位	InformationWeek		
原文出处	https://www.informationweek.com/strategic-cio/quantum-computing-brings-promise-and-threats/d/d-id/1330230?		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

量子计算是把双刃剑

Lisa Morgan

2017 年 10 月 26 日

量子计算机更快，更好，具有潜在的危险性，能够超越传统计算机的边界，但是能到什么程度呢？本文将探索一些可能性。

数字计算有一些严重的局限性。虽然过去几十年来的技术进步令人印象深刻，如体积更小、处理器更快、用户界面（UI）更人性化、内存和存储空间更大，但是量子计算机可以更好地解决一些问题。

一方面，量子计算机比传统的计算机更快。它们也能够解决传统计算机在合理的时间内处理不好或不能处理的问题。

英特尔实验室量子硬件总监吉姆·克拉克（Jim Clarke）说："量子计算利用物理学的基本原理，以新的方式解决复杂的计算问题，如发现疾病如何发展并创造更有效的药物来对抗它们等。一旦量子系统上市，人们就可以用它们模拟自然，以促进化学、材料科学和分子建模方面的研究。例如，帮助创建新的催化剂（以螯合二氧化碳）或室温超导体。"

量子计算还将推动业务优化，有利于机器学习和人工智能的发展，并改变密码学的格局。

Deloitte 董事总经理大卫·沙茨基（David Schatsky）表示，常见的是有多个可能答案的优化问题，任务是找到正确的答案。例如投资管理、投资组合管理、风险缓解以及通信系统和运输系统的设计。物流公司正在探索路线优化，而国防工业正在考虑通信应用。

沙茨基说："一年前，量子计算被更多地认为是一种物理实验，但是这种观点迅速改变。在过去的三个月中出现了突破性的进展，包括基础工程突破和商业产品公告。"

测试驱动着量子计算机

可以确定的是，我们无法很快地拥有量子计算机，但是任何使用浏览器的人都可以通过云访问 IBM 的 5 和 16 量子位（qubit）计算机。今年早些时候，IBM 宣布将推出世界首个商用量子计算系统 IBM Q。IBM 还宣布，它已经构建并测试了两个量子计算处理器，包括 16 量子位开放处理器，供公众使用，并为客户提供了 17 量子位商用处理器。

根据《自然》杂志上的 IBM 文章，科学家们成功地使用了一个 7 量子位处理器来解决氢化铍（BeH2）的分子结构问题，这是迄今为止在量子计算机上模拟的最大分子。

IBM Systems 的量子计算技术战略与转型副总裁兼首席技术官斯科特·克劳德（Scott Crowder）说："量子计算目前还处于早期阶段，但它将会迅速扩展。当您开始谈论数百或数千个量子位时，您就可以解决传统计算机处理不好的问题了，如量子化学和某些类型的优化问题（指数问题）。"

指数问题是指随着元素数量呈指数级变化的问题。例如，根据目标，可以以多种方式优化涉及 50 个地点的路线，例如识别最快的路线。这个看似简单的问题实际上涉及到一千万亿种不同的可能性，传统计算机很难处理，克劳德说。

英特尔也取得了进展

2015 年，英特尔与荷兰学术伙伴 QuTech 合作。此后，英特尔实现了多个里程碑，例如演示集成低温 CMOS 控制系统的关键电路块、开发了自旋量子位制造流程和超导量子位的独特封装解决方案（在 2017 年 10 月 10 日推出的 17 位量子超导测试芯片中进行了展示）。一周之后，在加利福尼亚拉古纳的《华尔街日报 D.Live 大会上，英特尔首席执行官布莱恩·科兹安尼克（Brian Krzanich）说计划在 2017 年年底之前推出 49 量子位量子芯片。

英特尔公司的克拉克表示："最终目标是开发一种商业化的量子计算机，一种通用的、能够影响英特尔底线的量子计算机。"

为此，英特尔与 QuTech 的合作涵盖了从量子位设备到整体硬件架构、软件架构、应用和互补电子产品的领域。

克拉克说："量子计算本质上是并行计算，能够解决传统计算机无法处理的问题。但是，实现量子计算需要将优秀的科学、先进的工程技术和持续发展的传统计算技术结合起来，英特尔正在通过各种合作伙伴关系和研发计划朝着这一方向努力。

解密等威胁

关于量子计算机是否会使当前的加密方法过时，是有争议的。以暴力破解攻击为例，黑客不断猜测密码，并使用计算机加速这一过程。量子计算将进一步加速这种攻击。

"几乎今天使用和部署的所有安全协议都容易受到量子计算机的攻击，" IEEE 量子标准

工作组主席威廉·赫利（William Hurley）说，“量子信息可以让我们以完全无法攻破的方式来保护信息，甚至是对抗量子攻击。”

按照这些原则，我们正在努力开发一种不利用量子力学的新型安全协议。赫利表示，他们正在使用非常困难的数学问题，即使是量子计算机也无法解决，这被称为“后量子加密”。

IEEE 量子标准工作组正在研究其它量子技术，包括量子传感器和量子材料。该研究所汇集了物理学家、化学家、工程师、数学家和计算机科学家，以确保研究所能够迅速适应变化。

Deloitte 的沙茨基表示，合成生物学和基因剪辑也有潜在的危险性，主要是因为这些能力的发展速度比人们理解如何明智地应用这些技术的能力更快。许多新兴技术也是如此。

警惕量子计算

量子计算正在迅速发展，所以明智的做法是思考这种能力对企业能够带来什么好处。现实情况是，没有人知道量子计算的所有使用方式，但它最终会影响到许多不同行业的企业。

量子计算机是否会取代传统计算机？还是说两者会共存？在可预见的未来，共存是这个问题的答案，因为二进制和量子计算机各自擅长不同的问题。

您有什么看法？

您认为量子计算的“杀手锏”是什么？做过实验吗？您想解决什么问题？我们很乐意在评论部分与您讨论可能性。

[仍然在纠结量子计算到底是什么？]

以下是来自《麻省理工科技评论》的最简洁的定义之一：

“量子计算的核心是量子位（qubit），这是一种基本的信息单元，类似于您的计算机中由晶体管表示的 0 和 1。由于两个独特的属性，量子位比传统的位数多得多：它们可以同时表示 1 和 0，它们可以通过称为量子纠缠的现象影响其它量子位，这使得量子计算机在某些类型的计算中能够更快地获得正确答案。”