引用格式:郭光灿. 量子计算优势对信息安全的影响[J]. 信息对抗技术,2024, 3(1):1-2. [GUO Guangcan. The impact of quantum computing advantages on information security[J]. Information Countermeasure Technology, 2024, 3(1):1-2. (in Chinese)]

特 邀 评 述

量子计算优势对信息安全的影响

郭光灿

(中国科学技术大学,安徽合肥 230036)

摘 要 经过 40 多年的发展,量子计算已处在一个从实验室到实际场景的应用阶段,意味着量子技术时代即将来临。量子计算的巨大优势就是其指数级增长的算力,它将为信息技术带来革命性的变化,但也为现有信息安全体系带来挑战。

关键词 量子计算;信息安全;量子纠缠

中图分类号 TP 385 ; TP 393.08 **文章编号** 2097-163X(2024)01-0001-02

文献标志码 A **DOI** 10.12399/j.issn.2097-163x.2024.01.001

The impact of quantum computing advantages on information security

GUO Guangcan

(University of Science and Technology of China, Hefei 230026, China)

Abstract After more than forty years of development, quantum computing has entered a stage from laboratory to practical application, meaning that quantum era is coming. The huge advantage of quantum computing is its exponentially increasing computing power, which will bring revolutionary changes to information technology but also pose challenges to existing information security systems.

Keywords quantum computing; information security; quantum entanglement

量子计算是基于量子力学,利用量子叠加、量子纠缠等特性发展起来的技术体系。相对于经典计算,它具有超级算力的巨大优势,这必然对未来的整个信息技术产生深远的影响。

1 量子计算的物理基础

与经典世界的确定性和局域性相比,量子世界具有不确定性和非局域性,也正是这 2 个特征构建了量子计算强大算力的物理基础,使其算力呈现出指数级增长。

量子世界的不确定性是指某个时刻量子客体的物理量不具有确定值,而是概率分布的值。经典信息是确定精准的信息,非“0”即“1”。而量子信息单元是不确定的,处在 0 和 1 叠加之后的状态,即量子态或量子比特,量子信息的单元是量子比特,是叠加态。1 个量子比特编制了 2 个经典数据(α、β);同理,含有 N 个量子比特的芯片含有 2^N 个经典数据。当操作此量子芯片时,芯片中 2^N 个经典数据可能变换成 2^N 个新数据。这是量子计算机具有并行运算能力的基础,也是量子算力呈指数级上升的原因。正是将这种不确定原理的量子态作为信息单元,量子计算机的 1 次操作相当于超算中心的 2^N 次操作,这就是叠加态带来的计算速度优势。

收稿日期:2023-11-15 **修回日期**:2023-12-30

非局域性是客体之间即使没有相互作用，也会互相影响，量子纠缠就是其生动的体现。2 个纠缠粒子不论相距多远，一旦其中一个粒子的状态发生变化，另一个粒子必将瞬时地随之产生变化。这种变化和影响来自于关联，它不需要信息的传递。量子计算机处理某个函数的速度，取决于量子算法。应用量子纠缠可以开发出更高效的量子算法，将量子计算机的并行运算能力体现在实际的信息处理过程中，使量子计算机的算力超越电子计算机。

可以看出，量子计算要用到量子的叠加和纠缠 2 个性质，而这正是量子计算机超算能力的根源。

2 量子计算面临的技术难题

当前，量子计算机的研制面临两大技术难题。一是量子计算机是宏观的量子器件，不可避免地受到环境影响，环境影响会破坏量子相关性、量子性质（即消相干），从而导致量子计算机丧失并行运算的能力。为了解决这个问题，科学家提出量子纠错容错编码原理，即使在有噪声的环境下，也可以确保量子计算机能够可靠正确地运行，但就目前情况来看，实现起来仍有相当大的难度。二是量子的操控能力有限，人类尚未掌握精确操控量子状态和演化的技术，因此无法制备和精确操控量子比特数较多的量子芯片。为解决这 2 大技术难题，科学家正致力研究量子编码技术。量子编码用逻辑比特作为单元，逻辑比特没有噪声，编码若干个有噪声的量子物理比特得到一个无噪声的逻辑比特。逻辑比特就是把 N 个物理比特编成一种特殊的纠缠态，这种特殊的纠缠态在环境作用下不会消相干。通常用来编码的物理比特质量越好，编成一个逻辑比特所需要的物理比特数目就越少。简而言之，解决这些问题一定有办法，但需要做大量工作。

3 信息安全受到的影响及应对方法

量子计算的强大计算能力是显而易见的，但科学技术的两面性在量子计算方面也十分突出。人类社会一旦进入到以量子计算为主导的量子技术时代，以目前经典信息技术为基础构建的信息安全将面临巨大的挑战。这是因为，量子计算是利用量子叠加效应实现的并行计算，极大地提高计算速度和信息处理效率。量子计算被证明能指数级或多项式量级加速某些有重要应用价值的计算问题的求解，具有指数级增长的算力，可能攻破现有的信息安全体系。例如，1994 年被提出的 Shor 算法，可以在多项式时间内解决大整数分解和离散对数求解等复杂数学问题，能够高效破解广泛使用的公开密钥加密方法（如 RSA、ECC 等算法）。

为了对抗量子计算对信息安全体系的威胁，科学家构建了量子编码体系，比较典型的有 2 个：一是基于量子物理原理的量子密钥分配（quantum key distribution，QKD）。现在已经做到可以在数百千米范围里保证光纤网络甚至卫星通信的信息安全，并且有商业化产品部署的实际案例。二是基于数学的方法，提出抗量子密码算法（post quantum cryptography，PQC），即能够对抗量子计算机攻击的新型公开密钥。它的研究进展非常快，美国花了 7 年时间，从 84 个可能的方案中逐步筛选出最后 4 种方案，并于 2022 年开始实施。最近国内相关单位也共同组织了实施 PQC 量子密码的方案。当前在 QKD 与 PQC 相结合的方向上，我国的科研和产业化团队已经迈出了他们的步伐。但 PQC 算法的抗量子性是基于格和编码等底层数学问题的量子困难性假设，这一假设还有待时间的检验，在政策及企业层面，我国应该增加抗量子算法的研究和关注，才能够在国际上获得更多的话语权。

以上 2 种密码体系只是相对安全，并不是绝对安全。量子计算对一个没有绝对安全的保密系统，有可能达到无坚不摧的地步，这种影响将是非常深远的。因此，进入到量子时代，信息安全领域的攻防将进入新阶段，量子计算超级计算能力与信息安全防护必然是一对矛盾，两者如何演绎，让我们拭目以待。

作 者 简 介

郭光灿

男，1942 年生，教授，博士研究生导师，中国科学院院士，第三世界科学院院士，中国量子信息学的开拓者和奠基人。研究方向为量子光学与量子信息。曾获国家自然科学奖二等奖 2 项、何梁何利奖 1 项，省部级、军队科技进步奖一等奖励 7 项，获评 2013 年度 CCTV 年度科技创新人物

E-mail：gcguo@ustc.edu.cn

责任编辑 钱 静