量子计算与域名系统 (DNS)

ICANN 首席技术官办公室

保罗 • 霍夫曼 (Paul Hoffman)
OCTO-031
2022 年 2 月 11 日

ICANN

目录

本文是 ICANN 首席技术官办公室 (Office of the Chief Technical Officer, OCTO) 文档系列的一部分。如需查看 OCTO 系列文档，请参阅 OCTO 出版物页面。如果您对任何这些文件存有任何问题或建议，请将您的反馈发送至 octo@icann.org。

本文支持 ICANN 的战略目标，即通过与利益相关方合作来强化域名系统 (Domain Name System, DNS) 协调性，提高相关各方维护 DNS 安全性与稳定性的共同责任意识。加强 DNS 和 DNS 根服务器系统 (root server system, RSS) 的安全性是 ICANN 战略目标的一部分。

执行摘要

近年来，量子计算机引起了安全界的关注，因为量子计算机有可能破解当前普遍使用的加密算法。虽然迄今为止还没有量子计算机能够做到这一点，但随着技术逐渐发展，可能在未来的某一天，这种新型计算机将可以轻松破解当今使用的一些算法。然而，鉴于量子计算技术仍处于起步阶段，而且构建和运行量子计算机的成本非常高昂，因此很难预测这一天究竟何时到来。

目前，人们正在为设想的不受量子计算机影响的新算法制定标准。本文将审查近期开展的相关工作，这些工作有助于更好地预估 DNS 社群何时需要考虑从当前的加密算法更改为新的加密算法。

1 简介

现代密码学中的一些算法依赖于某些需要大量时间来求解的数学问题的难度。量子计算机也许能够更快地解决这些数学问题，因而会削弱这些算法的安全保障力度。基于量子原理的计算机与过去 70 年内广泛使用的计算机存在本质上的差别。量子计算机中的数据处理依赖于量子位（简称“*qubit*”），而不是当今所有计算机使用的二进制位。

如果能够构建大规模的量子计算机，它们或许能够解决一些当前计算技术无法解决的问题，因为量子计算机可以同时处理许多复杂进程。虽然当今的计算机（称为“*传统计算机*”）可以处理并行进程，但量子计算机可以利用所分析数据各部分之间更为紧密的联系来做到这一点。

量子计算机背后概念的理论化已有近 50 年时间，但即使是规模非常小的量子计算机也很难构建。以量子位存储的信息非常脆弱，因此必须在计算过程中将量子位保持在接近零开氏度的温度，从而将其与外部环境完全隔离；而这样做需要大量的计算机空间和物理空间。然而，量子位在处理过程中也很容易出错。为此，量子计算机需要数百或数千个额外的冷却量子位来纠正计算过程中每个量子位的错误；鉴于冷却和通信方面的要求，可能无法构建具有数百万量子位的量子计算机。