简译版

量子计算迫在眉睫，企业需要加密敏捷性

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 is imminent, and enterprises need crypto agility now		
原文作者	托德·摩尔（Todd Moore）	**原文发布日期**	2021年6月11日
作者简介	托德·摩尔是Thales公司加密解决方案副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/06/11/crypto-agility/		
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		
摘要	随着第二次量子革命的爆发，网络安全威胁以及用于保护数据和通信的工具将出现巨大的变化。后量子技术将在保护骨干网络和边缘的数据和通信方面发挥至关重要的作用。安全行业必须齐心协力，迅速采取行动，以跨整个价值链和全套用例开发基于后量子技术的解决方案。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

量子计算迫在眉睫，企业需要加密敏捷性

托德·摩尔

2021 年 6 月 11 日

近 100 年前，第一次量子革命带来了巨大的技术进步，使我们的现代化生活成为可能。量子物理学的进步促进了晶体管、激光和原子钟的发展，而这些正是半导体、GPS、医疗成像设备和光纤通信等科技创新的基石。

如今，第二次量子革命即将到来。第一次量子革命使用量子力学原理开发新应用，而第二次量子革命将为工程师赋能，使其能够自己管理量子力学，从个人层面控制量子系统。就像第一次量子革命塑造了 20 世纪一样，量子计算的突破将定义下一个百年。

量子计算将带来我们尚无法预测的进步，但无疑也将对企业及其保护信息和通信的能力带来挑战。当前的网络安全实践依赖于经典加密算法，这些算法容易受到量子计算机的攻击。随着量子技术的不断进步，安全行业必须开发量子计算机无法破解的后量子加密工具。

量子计算的前景和挑战

第二次量子革命将利用量子物理学最先进和最细微的特性，掌握这些技术已经成为领先的政府实体和企业的首要任务。特别是，拥有关键系统的大型组织已经认识到，为量子计算的安全影响做好准备至关重要。

第二次量子革命可能会使当前的网络安全实践过时。现在，攻击者已经开始收集加密数据，以便为未来的后量子攻击做准备。幸运的是，企业可以采取一些措施，来应对量子革命及随之而来的新兴威胁。

在过去的五年中，政府、企业和网络安全公司一直在预测量子安全威胁的挑战。抗量子解决方案的关键技术是后量子加密工具，这些工具将使企业获得加密敏捷性，帮助其部署量子计算机无法破解的算法。

竞相开发量子解决方案

美国国家标准与技术研究院（NIST）指出，领先的工程师预测道，能够破解目前所有加密解决方案的大型量子计算机将会在 20 年内被开发出来。为了应对这种威胁，NIST 启动

了一项计划，以征求至少一种抗量子公钥加密算法并将其作为标准。

在过去的五年中，领先的工程团队一直致力于开发后量子加密算法，这些算法将成为未来网络安全的支柱。NIST 已经确定了标准后量子加密算法（用于公钥加密和数字签名）的候选者（包括 Thales），获胜解决方案将于 2022 年选出。

追求加密敏捷性

虽说在网络安全方面从来没有灵丹妙药，但是量子攻击的处理能力带来的挑战只能通过加密敏捷性来解决。加密敏捷性不仅能够提供针对量子黑客工具的重要保护，还能为企业赋能，帮助其为未来的威胁和解决方案做好准备。

加密敏捷性使企业能够采用灵活的方法来部署新算法，且不需要对系统基础架构进行重大改动。如果原始加密失败，企业可以以相同的方式部署更新的算法。从长远来看，这种方法意味着企业可以跟上不断增长的计算能力，而无需对其基础架构进行改动。

量子计算与数据所有权、数据处理和通信有关，有可能会颠覆我们对“信任”的理解。加密敏捷性将使企业能够确保，只有那些受信的人员才能访问数据资产。新的网络安全威胁即将出现，企业和组织必须立即采取行动保护其最重要的信息。

未来之路

随着第二次量子革命的爆发，网络安全威胁以及用于保护数据和通信的工具将出现巨大的变化。后量子技术将在保护骨干网络和边缘的数据和通信方面发挥至关重要的作用。安全行业必须齐心协力，迅速采取行动，以跨整个价值链和全套用例开发基于后量子技术的解决方案。

如果安全行业还未认识到这种威胁并支持后量子计算，就会将组织及其关键数据置于风险之中。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com