面向未来

通往量子安全保障之路

前沿报告

2022 年 4 月

委托方

IBM

451 Research

S&P Global
Market Intelligence

作者简介

John Abbott

4SIGHT 首席研究分析师

John Abbott 在标普全球市场情报部 (S&P Global Market Intelligence) 下属 451 研究所负责系统、存储器和软件基础架构等版块的研究报告。在三十多年的职业生涯里，他在许多专家级技术领域开拓耕耘，内容涵盖 Unix、超算、系统体系结构、软件开发、存储器等领域。

作为 1999 年 10 月成立的 451 集团联合创始人之一，John 在集团位于旧金山的办公室从事分析运维工作。他是很多 451 研究所特别报告文章的第一作者，其中包括有关存储器虚拟化和刀片服务器这两项主题首次公之于众的全面调查分析文章。就在最近，John 开始专注于融合式基础架构、新系统体系结构、人工智能和深度学习加速器等主题的研究报告。他协助建立起了 451 研究所新兴技术前瞻性长期报告机制——4SIGHT。

早在 1984 年，John 就结合自己之前担任技术文章作者和使用大型计算机、早期个人计算机及 Unix 工作站的经历，开始从事技术领域的报告工作。作为一名自由撰稿人，他的文章曾被包括 Computing、Computer Weekly、《金融时报》、《泰晤士报》等报刊公开发表。1987 年，他曾担任 ComputerWire 的 Unix 通讯周刊——Unigram.X 的编辑，接着又先后在伦敦和旧金山任职公司旗下报业 Computergram International 日报的编辑。他在旧金山成立了 451 研究所办公室，并在那里生活了十多年。

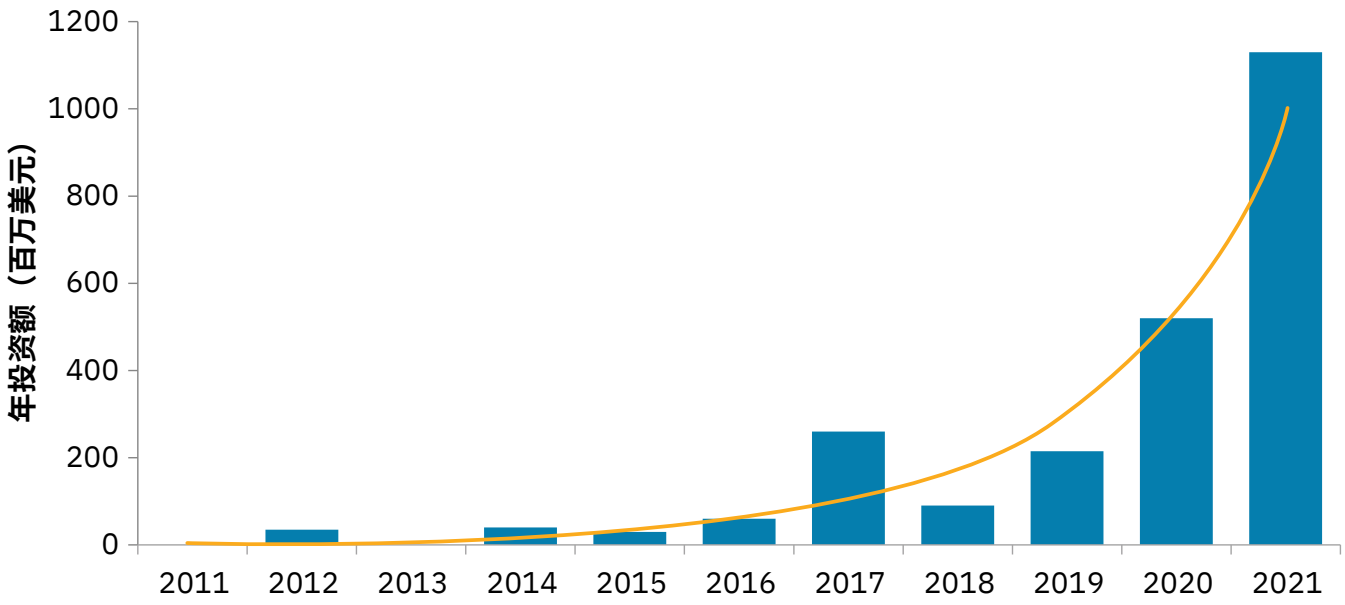
John 曾在基尔大学 (University of Keele) 主修音乐课，并在伦敦大学 (University of London) 获得了现代英语文学硕士学位。

简介

今天，量子计算堪称是一个高风险、高回报的投资领域。谁也不能保证在我们有生之年能看到一台通用的实用型量子计算机真正投入使用。不过，该技术领域的诸多研究实验室以及越来越多的私人公司都一直在不断突破，努力实现这一科学前沿的技术革新。而由此获得的回报也非常可观，解决了很多当前任何（传统）超级计算机都无法解决的问题。这也是为何卖家和用户纷纷试水这一可能带来颠覆性影响的技术。标普资本 IQ 专业版数据（图 1）显示，在过去十年里，量子初创公司融资金额达 24 亿美元。2021 年，投资者的兴趣呈井喷态势，流入量子公司的投资额高达 11 亿美元。以上数据还不包含像 IBM、亚马逊、谷歌、霍尼韦尔等成熟 IT 公司投入的巨额资金。

伴随这一机遇而来的还有引发大家担忧的几大问题。最紧急的问题当属现今的安全措施。有了量子计算，恶意玩家就能够伪造数字签名，破译当前保密级别的密码技术和加密技术，包括与全球 IT 系统深度融合的公共密钥基础设施。更严重的是，一旦实用型量子计算手段出现，就算是当前受保护的加密数据也会被破译掉。这是当务之急，必须马上解决。等待的时间越长，面临风险的数据就会越多。

图 1：量子计算初创公司融资情况



来源：标普资本 IQ 专业版

451 观点

对于量子计算机普遍可以高效运行舒尔算法 (Shor’s algorithm) 因而被恶意玩家利用的准确时间节点，我们无法预测。截止到目前，没有一家 IT 厂商可提供量子计算在实质上超过传统计算机能力的准确时间表。但从过去五年技术飞速发展、巨额投资如今已经落地的情况来看，这一天迟早要来，很可能在这一个十年快结束的时候就能实现。届时，目前受公钥算法保护的所有信息全部都有泄露的危险。对国防和情报机构以及客户来自受监管行业的云服务供应商和系统厂商来说，这一风险已经足够大了，必须引起重视。不管是有过去的错误警报作为前车之鉴（回忆下千年虫 (Y2K) 事件，当时间从 1999 年跨越到 2000 年时，一个大规模使用的计算机编程快捷方式就几乎造成严重破坏），还是面对充满未知的将来，有一点是肯定的：今天，网络攻击风险是一项重大问题，施害方和受害方一直都在不断演变。安全政策需要实时检查和更新；量子安全加密技术，以及推行密码灵活度和加密清单等措施等，如今已成为制衡双方力量的重要砝码。

抗量子技术与量子安全场景

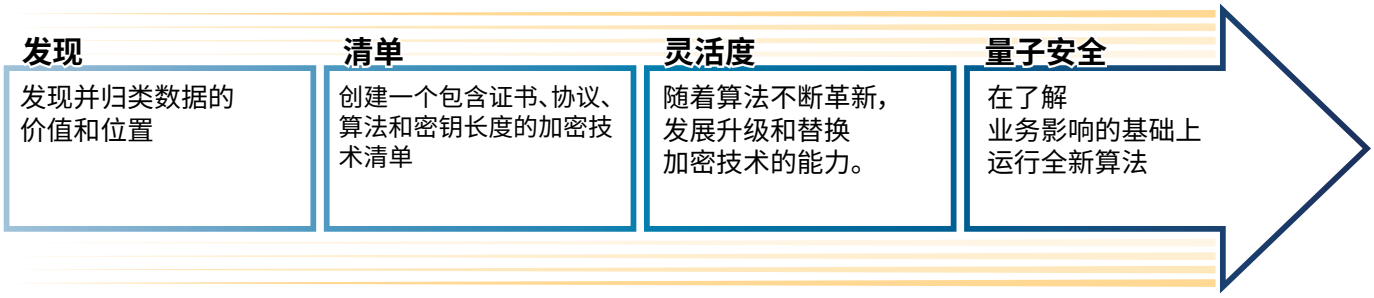
问题在于：当前大规模使用的安全算法是基于数学难题开发的，传统计算机很难突破。不过，一台电力充足的量子计算机可以轻松解决这些难题，早在 1994 年这一假设就已被广泛认同，那一年，美国数学家皮特·舒尔 (Peter Shor) 发现了多项式时间算法，也就是今天大家所说的舒尔算法。三年后，第一台量子计算机问世。过去十年，量子安全算法的发展日新月异。不过，要想把政府和各行业目前广泛应用的公钥加密系统换成另一套全新算法，可能要花费数十年。

这也是为什么像美国国家标准技术学会 (NIST) 和美国国土安全局这些机构在已经着手制定算法标准化流程的同时，还要为企业准备转向后量子加密技术提供建议。这项工作还促使美国白宫在 2022 年 1 月份起草了一份备忘录，要求国防及情报部门开始实施转换工作。

如果要通过找到质因数将一个 2048 位的复合整数分解，即便使用当今世上最强大的计算机，也可能要耗时几百万年。而如果换成量子计算机，理论上几个小时就能完成。被舒尔算法破解的现有公钥方案包括：问世了 45 年但依旧活跃在几乎所有互联网交易中的古老 RSA 算法、数据安全标准、Paillier 加密系统、椭圆曲线数字签名算法，以及椭圆曲线 Diffie-Hellman 和 ElGamal 加密法。由 NIST、ISO/IEC、ETSI 和 IETF 建立的一长串标准都受到了影响，也就意味着这是一个全世界都存在的问题：中国 SM2 数字签名算法和 SM9 国家加密标准同样遭到了破解。

在 2016 年开始征集提案的 NIST 标准化程序已经识别出一套新的抗量子密码候选方案。在分成诸如网格、多变量、基于散列或编码的密码术等不同方案后，这些方案包含基于网格的 CRYSTALS-Kyber 密钥封装机制 (KEM)、McEliece（基于编码的 KEM）以及 Falcon（基于网格）和 Rainbow（基于多变量）后量子签名方案。在现已结束的第三轮角逐之后，这些方案和其他终极方案都会被列入标准化草案。包含替代算法和附加签名方案征集工作的第四轮研究在今年启动，并将于 2024 年底前完成。

图 2：量子安全成熟度里程碑事件



来源：451 研究所

通往量子安全密码术之路

当前，各机构应该采取哪些行动为其信息安全体系结构在下一个十年融合量子安全密码术做准备？第一步已经开始，即参与到标准化流程当中。参与标准化流程，以确保最终算法、处理器及工具批准清单满足要求，对任何一个志在防止虚假认证、保护密码完整性和避免损害数字签名的组织来说都至关重要。尽管标准化主体进展顺利，但这是一项持续进行的工作：需要投入更多的算法。除此之外，下述成熟度里程碑事件也是实现量子安全的必经之路。

- **数据识别与分类：**对关键数据进行盘点。哪一种数据值最大？数据存放在哪？合规要求是什么？了解这些信息很关键，因为很多组织并不完全清楚自己到底拥有哪些数据以及这些数据的价值所在。不了解这些信息，他们就无法识别出最薄弱的环节。他们必须利用给定的所有权创建并管理一个数据清单。
- **加密技术清单：**加密技术清单详细阐述了易破解公钥密码术用在哪里以及如何使用，包含证书、加密协议、算法及密钥长度等细节内容。清单必须经常维护，以便囊括证书及加密密钥的整个生命周期。
- **加密技术灵活度：**相关组织在制定计划和实施转换工作过程中要把加密技术灵活度考虑进去，这样就可以在技术革新、环境发生变化的时候适时作出调整，以免伤筋动骨。他们应该设计并植入流程，以便在明确规定的交付时间内，较为轻松地升级或替换当前一代加密技术，然后紧接着完成测试工作。
- **量子安全：**在应用新的算法时，相关组织必须要意识到量子安全加密技术对业务运营的潜在影响。

每个组织都不尽相同，也并不是所有的组织都处于需要改变一切的处境（或思维方式），比如他们所面临的成本压力或生命周期管理问题等，都会有所不同。不过，无论是从短期还是长远来看，升级或替换安全协议能力的设计都至关重要。鉴于该工作与系统基础架构密切相关，要想实现加密技术灵活度，需要系统设计方、应用开发方和安全专家通力合作。而目前还缺少能促进此合作模式的合适工具。

相关组织将利用各种要素优先保证量子安全加密技术的替换工作：受保护资产价值；受保护数据（即密钥存储库和密码）风险等级；受影响的连接系统（即与包括联邦机构在内的外界实体共享的信息）；以及数据需要被保护的时长。在长时间转换过程中，融合传统算法和量子安全算法相结合的方案很有必要。

实施、动力与驱动程序

对于系统供应商和大型云服务提供商（其设备和基础设施承载着关键任务型企业的工作负载）来说，他们无法一直等到量子安全加密技术标准化工作完全结束的那一天。他们已经在这个问题上苦心钻研多年，为 2024 年制定出最终标准清单创造了前沿的算法和协议选择。一批基于云服务的密钥管理厂商已经为第二轮和第三轮算法提供了强有力的支持。客户开始利用这些服务来衡量给应用程序带来的潜在性能影响，其主要源自带宽使用率和等待时间等因素可能产生的额外开支；同时还利用它们来缓解传输级安全代理层连接失败等可能出现的问题。不过，大家都认为随着标准和技术不断革新，向量子安全转换将是一项耗时多年的工作，而且这项工作是从保障核心基础架构安全开始。

在系统领域，大型计算机仍旧被视为可用性高且十分安全的核心基础架构，广泛用于各大银行、保险公司、电信提供商、零售商以及交通运输业务，大型计算机的这种地位已经维持了半个多世纪。最新一代大型计算机将搭载具备量子安全属性的硬件安全模块，与升级后的操作系统组件、密钥管理 APIs 和一套新兴抗量子算法支持模块协同工作。带有硬件信任根的量子安全保障引导技术将被用于保护系统根固件完整性，而用于业务合作伙伴之间安全交换密钥的量子安全机制将通过应用程序编程接口提供。

在帮助客户转换到量子安全加密技术方面，云服务提供者和厂商必须发挥关键作用。光有监管部门自己的声明还不够，部分原因是他们在自己没有真正意义上的专家的情况下，通常不能规范地为用户组织提供清晰的准则。通过在不作额外的系统级启动更改前提下提供核心业务系统保护，已经处于任务关键型基础架构核心的厂商可以让流程变得更加简单。他们还可以提供更急需的发现工具，以用于加密应用程序分析工作。数据管理组织需要确保他们的数据从当前到未来的全生命周期都处于被保护状态，因为现在使用传统算法加密的数据，在以后可能就会被更先进的量子计算机破解。如果数据要完好保存 20 年，那就将是 2040 年以后了。即使是坚信实用型量子计算还需要很多年才能问世的怀疑论者也必须清楚，照目前的发展速度来看，到那时，这个可能性将大大增加。

总结

量子计算的商业案例越来越多，一台得以完全实现性能的量子计算机将给化工、机器学习、金融、交通运输、医疗等行业带来跨越式发展的机遇。量子计算机将推动公式处理能力呈指数级增长，而目前在用的传统型、确定式计算机还不具备这种实用运行的能力。

而另一方面，由于网络攻击的存在，数据保护和隐私威胁本来就呈增长态势，量子计算可能也会让这种不利情况雪上加霜。随着数据的商业价值增长，数据保护需求规模和成本也会跟着增加。而由于数据价值会维持很长一段时间，量子计算在不远的将来就会成为现实，这种可能性越来越大，必须要考虑进去。越早行动，转向量子安全核心基础架构、部署能够发现当前应用层风险的工具、保护各组织密钥交换系统以及持续保护数据中长期隐私信息等工作开展起来就会越有把握。

联系方式

美洲地区
+1 877 863 1306
market.intelligence@spglobal.com

欧洲、中东及非洲地区
+44 20 7176 1234
market.intelligence@spglobal.com

亚太地区
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence