Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

News & Highlights

量子密码学竞赛产生下一代标准算法

Chris Palmer

Senior Technology Writer

未来短短十年内，我们目前使用的加密密钥很可能会被量子计算机所破解，而这些密钥的保护范围从安装在智能手机中的银行应用程序到日常使用的电子邮件。面对这一威胁，美国商务部国家标准与技术研究所（NIST）于2022年7月公布了第一批用于抵御该类攻击的加密工具，而这批工具是一场始于2016年的竞赛的胜出者[1–2]。

这批加密工具包括一种用于保障公共网络信息交流的一般加密算法，以及三种用于管理数字签名的算法，数字签名用于身份认证。这四种加密算法被NIST合并列入其后量子加密标准中，最终标准将于两年后确定颁发[1]。

NIST于2016年发起了一场后量子密码算法标准全球征集竞赛，呼吁世界各地的密码学家投身于后量子加密方法的设计中，以抵御未来量子计算机的攻击，因为量子计算机的计算能力将远超目前的量子机器[3–4]。这批加密算法的发布便是本场竞赛的一个重要里程碑。来自全球六大洲近50个国家学术界和产业界的团队共提交了82种算法，其中69种算法接受了全球专家的全面测试[1]。

经典计算机，即使是世界上最强大的超级计算机，也很难对大数进行分解计算。现有的公钥加密系统便是利用这一特性来对网上银行交易以及其他敏感信息进行保护（图1）。虽然用于数据加密和解密的共享密钥很容易生成，但别有居心之人却几乎不可能推导出使密码有效的数字。

早在1994年，AT&T贝尔实验室研究员Peter Shor便表示这些计算对于未来的量子计算机来说根本微不足道[5]。

图1. 目前在线数据以及通信加密密钥可能会被未来的量子计算机的强大运算能力所破解。为了为应对该威胁，美国商务部国家标准和技术研究所最近选定了一批可在未来几年内投入使用的安全工具，以抵御量子计算机的攻击。图片来源：Pixabay（CC0）。

2001年，Shor算法已经被科学家们成功运行，但也仅止步于对15的质因数推导[6]。虽然从彼时起量子计算技术已经取得较为显著进步[3–4]，但通过Shor算法来进行大数字密钥计算依旧道阻且长。但“量子计算工程师们都持有一个共识：Q-day，即量子计算机破解公共加密密钥的那一天，不是是否会到来的问题，而是何时到来的问题。”Cloudflare研究以及密码部主管Nick Sullivan说道，Cloudflare是一家总部位于美国旧金山的互联网安全公司。

“人们会好奇，为什么在量子计算机还不存在的当下我们就要进行后量子加密算法的标准化。这么说吧，现在的你可能已经面临着‘先收集，后破解’（harvest now, decrypt later）的威胁。”NIST计算机安全部的数学家

英文原文：Engineering 2023, 21(2): 6–8
引用本文：Chris Palmer. Quantum Cryptography Competition Yields Next-Generation Standard Algorithms. *Engineering*, https://doi.org/10.1016/j.eng.2022.12.002

Dustin Moody说道。这种威胁背后的逻辑是：目前可以先将互联网上的加密数据复制保存，待到量子计算机发展到足够强大之后再将它们一一破解。“在这种逻辑的驱使下，美国的对手正在积极地进行数据收集。这无疑会成为一个大隐患。”主导NIST后量子密码学项目的Moody表示。

Moody表示，NIST选出的后量子加密算法主要基于其应对当前经典攻击表现出的安全水平、应对量子计算机攻击表现出的预期安全水平以及其速度和紧凑性等效率因素来进行判断。“我们受到了很多公众监督，”Sullivan表示道，“提交的算法也受到了许多密码学家的审查，其弱点也进行了确认。”

对于一般加密，NIST选择了CRYSTALS-Kyber算法，因为这种算法整体速度较快且其生成的加密密钥相对较小，可以轻松被双方用来进行数据交换[7]。对于数字签名，NIST选择了CRYSTALS-Dilithium、FALCON和SPHINCS+三种算法。NIST将CRYSTALS-Dilithium作为主要数字签名算法。而对于某些需要比Dilithium更小签名的应用，FALCON依旧被列为首选[7]，虽然Moody表示其实现难度巨大。

尽管相较于其他两种数字签名算法，SPHINCS+算法要更大更慢，但作为备份也不失为上乘之选。因为包括一般加密算法在内的其他选定算法，均属于结构化格子数学结构（将数据映射到任意维度矩阵内的向量的函数），而SPHINCS+使用的是完全不同的哈希函数数学结构（将任意大小的数据映射到固定大小值的函数）[5]。

“格子结构很有吸引力，因为它们性能全面且优越。基于格子机构的算法速度非常快，甚至比我们现有的用于加密的算法速度还要快，而且运用时效率非常高。”Moody说道，“高效率非常重要，因为我们希望将这些加密系统应用于所有地方。”

NIST目前已经开始制定针对这些算法的应用标准。NIST将在未来一年内从密码学界获得更多反馈，并于2024年发布其正式标准。Moody同时表示，这些算法在实际应用中的建立和使用将由一个名为互联网工程任务组（Internet Engineering Task Force，位于美国加州弗里蒙特市）的志愿者国际互联网协议标准机构决定。该项工作完成后，互联网公司即可将这些算法整合到网络浏览器中，而技术供应商则可通过定期的软件更新对这些算法进行部署。

在过去的几年中，Cloudflare与互联网巨头谷歌（美国加州山景城）多次协作，致力于将一些后量子算法纳入选定的谷歌Chrome网络浏览器测试版本以及服务器软件，并对其进行实际测试[8]。测试很关键，因为要保障互联网通信的顺利进行，仅拥有完全兼容的服务器和浏览器是远远不够的，数据必须能够在各网络设备中顺利传输，而网络设备可能会对使用了陌生加密协议的数据流量进行阻拦。

谷歌母公司Alphabet [9]以及Cloudflare [10]可以协助全球为数不多的浏览器开发商和服务器提供商更换加密系统。但对于为数众多的连网的物联网（IoT）设备[11]，如汽车、安全摄像机以及“智能家居”小工具来说，更换加密系统就难得多，因为这些设备的安全模块是硬连接到芯片中的，而且通常不会进行更换。

算法的具体实施并没有中央部门进行监督。但NIST会提供在线工具对已获得批准的加密算法的实施进行验证。虽然这些验证测试是免费的，但要在互联网范围内进行全面落实，成本也不在少数。Sullivan说：“当然，升级会产生成本，但这些升级都在传统在线产品的生命周期之内，尤其是在‘软件即服务’的范式下。另一方面，如果某些设备的密码是通过硬件内部设定的，如物联网设备，那么解决方案只能是淘汰旧设备，然后重新购置新一代设备。”

Sullivan表示，尽管成本很高，但更新换代已是刻不容缓，尤其是在五到十年内Q-day就会到来的情况下。他说：“在五到十年间对整个互联网进行技术升级困难重重，特别是当这些升级目前尚无法利用时。”即便更新换代的好处显而易见或政府进行强制要求整改，一些公司和组织也可能会对信息技术更新产生抵抗心理，而对那些有目共睹的益处选择视而不见[12]。

业内见证的更为广泛的加密技术升级之一，即哈希函数安全哈希算法-1（SHA-1）升级为SHA-2 [13]，为后量子加密算法的实现提供了一个行之有效的路线图。哈希函数可通过任意长度的数据串生成一个固定长度的哈希值或数字指纹。SHA-1由美国国家安全局（NSA）设计，并在1995年由NIST作为标准发布。意识到该算法总有一天被破解，NSA的软件工程师从2002年便开始开发更强大的SHA-2。从2015年开始，SHA-2开始被广泛应用，该时间比SHA-1被成功破解早了两年[14]。SHA-2的最终替代算法为SHA-3，也是NIST通过公开竞赛开发获得，并在2015年被采用，目前可随时投入使用。“业界花了五年多的时间才使SHA-2普遍化。这还是在该算法经历了非常积极且实用的攻击之后。”Sullivan说道，“在进行了大规模的数据迁移后，目前仍有一些应用采用SHA-1算法。”

在后量子加密算法全面替代现有的加密算法之前，两者可能会共同运行十年左右。“有些人认为，两种算法的

混合运行将永远行之有效，”Sullivan说道，“另一些人则认为，一旦后量子算法发展的时间足够长，它们就会像传统算法一样经过重重考验，届时也便无需再进行混合运行。归根结底，这取决于我们对新算法的信心有多大。”

无论全球密码学专家对NIST的选择如何有信心，中国与俄罗斯在内的一些国家仍将继续坚持自己的研发之路[15]。一直以来，中国使用的加密算法与世界其他国家不同。2018年和2019年，中国举办了自己的后量子加密竞赛，并于2020年公布了少数获胜者，而这些算法也均基于结构化格子[15]。“中国的竞争规模较小，且节奏比我们快得多，”Moody说，“但他们最终选择的一些算法与我们选定的算法非常相似。”

“我们经历了一个漫长且严格的选择过程，因为我们没有回头路可走。如果一个算法在数学方面相对薄弱，那么实施后再去改变是非常困难的。”Sullivan说道，“不过，我们非常肯定，我们选定的这些算法非常优秀，这些算法将会在很多年里为我们提供数据保护。”

随着量子互联网的出现，后量子加密的概念某天也可能面临淘汰，在这种情况下，量子物理学原理基本上可以保障信息交换免受黑客的攻击[16–17]。近期超奇异同源密钥封装（SIKE）算法被人用简单的经典计算机进行了破解[18]，SIKE算法入围了NIST加密算法半决赛。Moody表示，鉴于此，目前NIST正在对另外四种不基于格的后量子加密算法进行评估，SIKE和这四种算法是NIST选定的备用算法。NIST还发起了一项新的竞赛，为数字签名选定其他备份算法[19]。“如果在该领域实现了一些突破后，已选定算法被发现存在新的漏洞，我们希望有其他一些加密算法可以随时顶上去快速扭转局面。”Moody说道。

References

[1] Castelvecchi D. These ‘quantum-proof’ algorithms could safeguard against future cyberattacks [Internet]. London: Nature; 2022 Jul 11; [cited 2022 Oct 30]. Available from: https://www.nature.com/articles/d41586-022-01879-6.

[2] Boutin C. NIST asks public to help future-proof electronic information [Internet]. Gaithersburg: NIST; 2016 Dec 20 [cited 2022 Oct 30]. Available from: https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information.

[3] Palmer C. Google takes a big step toward quantum computing. Engineering 2020;6(4):381–3.

[4] Palmer C. Quantum computing quickly scores second claim of supremacy. Engineering 2021;7(9):1199–200.

[5] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science; 1994 Nov 20–22; New Mexico. New York: IEEE; 1994. p. 124–34.

[6] Vandersypen LMK, Steffen M, Breyta G, Yannoni CS, Sherwood MH, Chuang IL. Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance. Nature 2001;414(6866):883–7.

[7] O’Shea D. NIST picks initial post-quantum security standards [Internet]. New York: Fierce Electronics; 2022 Jul 7 [cited 2022 Oct 30]. Available from: https://www.fierceelectronics.com/electronics/nist-picks-initial-post-quantum-security-standards.

[8] Venables P. How Google is preparing for a post-quantum world [Internet]. Mountain View: Google; 2022 Jul 6 [cited 2022 Oct 30]. Available from: https://cloud. google. com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world.

[9] Smith DI. Data is vulnerable to quantum computers that don’t exist yet [Internet]. New York: IEEE Spectr; [cited 2022 Oct 30]. Available from: https://spectrum.ieee.org/post-quantum-cryptography.

[10] Westerbaan B, Rubin CD. Defending against future threats: Cloudflare goes post-quantum [Internet]. San Francisco: Cloudflare; 2022 Oct 3 [cited 2022 Oct 30]. Available from: https://blog.cloudflare.com/post-quantum-for-all/.

[11] Carlson EK. New standards release sets stage for 5G future. Engineering 2021;7(3):275–6.

[12] Leslie M. Legacy information technology compounds pandemic pain. Engineering 2021;7(4):415–7.

[13] Grimes RA. All you need to know about the move from SHA-1 to SHA-2 encryption [Internet]. Needham: CSO; 2017 Jul 6 [cited 2022 Oct 30]. Available from: https://www.csoonline.com/article/2879073/all-you-need-to-know-about-the-move-from-sha1-to-sha2-encryption.html.

[14] Lomas N. Security researchers announce “first practical” SHA-1 collision attack [Internet]. San Francisco: TechCrunch; 2017 Feb 23 [cited 2022 Oct 30]. Available from: https://techcrunch.com/2017/02/23/security-researchers-announce-first-practical-sha-1-collision-attack/.

[15] Liu N. China, Russia to adopt ‘slightly different’ PQC standards from US [Internet]. Denver: SDX Central; 2022 Oct 19 [cited 2022 Oct 30]. Available from: https://www.sdxcentral.com/articles/analysis/china-russia-to-adopt-slightly-different-pqc-standards-from-us/2022/10/.

[16] Whalen J. Chicago scientists are testing an unhackable quantum internet in their basement closet [Internet]. Washington DC: Washington Post; 2022 Oct 9 [cited 2022 Oct 30]. Available from: https://www.washingtonpost.com/technology/2022/10/09/quantum-internet-chicago-argonne/.

[17] Leslie M. Quantum cryptography via satellite. Engineering 2019;5(3):353–54.

[18] Ropek L. Supposedly quantum-proof encryption cracked by basic-ass PC [Internet]. New York: Gizmodo; 2022 Aug 2 [cited 2022 Nov 13]. Available from: https://gizmodo.com/quantum-encryption-algorithm-nist-broken-single-core-pc-1849360898.

[19] Post-quantum cryptography: digital signature schemes. Gaithersburg: NIST; 2022 Aug 29 [cited 2022 Nov 16]. Available from: https://csrc.nist.gov/Projects/pqc-dig-sig/standardization.