量子安全世界杯结果揭晓

2016 年，82 种算法参加了由美国国家标准与技术研究院（NIST）主办的量子安全世界杯。这 82 支 “队伍 ” 代表了学术界和工业界最先进的密码学研究成果。但是，在八年的时间里，这些算法中的每一种都经历了艰苦的考验，世界上最优秀的密码分析师用尽了一切办法来破解它们。它们一个接一个地失败，直到最后只剩下寥寥几种。

2024 年 8 月中旬，NIST 的世界杯落下帷幕。四名决赛选手脱颖而出： CRYSTALS-Kyber、CRYSTALS-Dilithium、SPHINCS+ 和 Falcon。NIST 正式对前三种算法进行了标准化，而第四种算法 Falcon 也即将标准化。

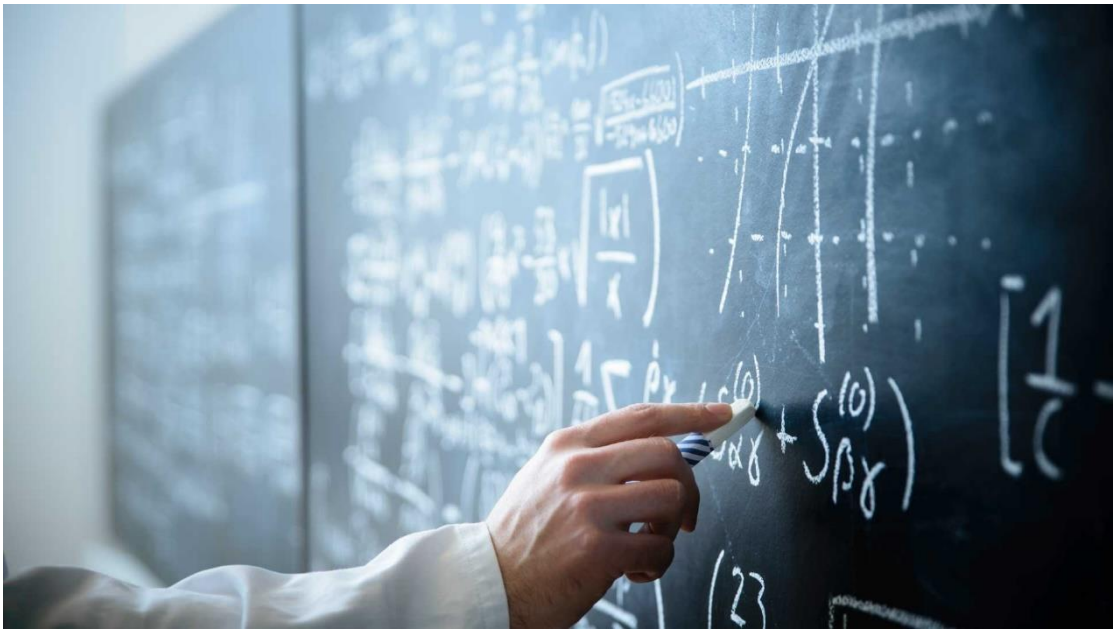
这对后量子密码学（PQC）领域来说是一个重大决定。NIST 批准这些算法意味着它们现在可以进入不同的行业标准化机构，成为保护世界信息的互联网、网络和数据加密标准的一部分。这些 PQC 标准将成为创建量子安全网络和产品的关键。这些新算法将成为我们日益强大的量子安全武器库中的有力武器，抵御未来不可避免的量子计算攻击。

为 Q-Day 做准备

量子计算仍处于初级阶段。如今，我们正处于所谓的嘈杂的中等规模量子时代，这意味着我们可以制造出基本的量子计算机。然而，这些计算机无法解决实际问题，因为它们缺乏稳定性，会产生过多的错误或噪声，从而无法高效地执行计算。

但随着量子计算机容错能力的进一步突破，它们将有能力解决难度越来越高的数学问题。最终，这些计算机将强大到足以破解保护我们数据和通信的最广泛使用的加密系统。这种与密码学相关的量子计算机（CRQC）上线之日被称为 Q-Day，也就是所有经典加密方法过时之时。

Q-Day 将是 10~25 年后的事，这取决于你问的是谁。不过，虽然我们可能至少还要再过十年才能看到 CRQC，但量子安全是我们今天需要认真对待的威胁。原因很简单。我们今天用非对称经典加密方法保护的任何信息，在 Q-Day 发生时都会暴露无遗。密码学专家认为，有魄力的黑客正在收集和存储大量加密的敏感数据，涵盖从消费者身份信息到国家机密，不一而足。这些黑客今天可能无法解密这些数据，但他们打赌，当 CRQC 上线时，这些信息仍将具有巨大价值。



这正是 PQC 等量子安全网络技术发挥作用的地方。像 NIST 刚刚批准的 PQC 算法将创造出新一代非对称加密技术，而 CRQC 理论上是无法破解的。从根本上说，加密算法基于非常困难的数学问题，传统计算机需要数千年才能解决这些问题。然而，CRQC 的计算能力可以将这一间隔缩短到几天，甚至几小时。PQC 算法所要做的，就是利用我们对量子计算的理解，创造出 CRQC 需要很长时间才能解决的新数学问题。从技术上讲，这些后量子加密算法并非不可破解，但从理论上讲，破解这些算法需要数万年的时间，这将使这种加密在所有实际用途上都是不可破解的。

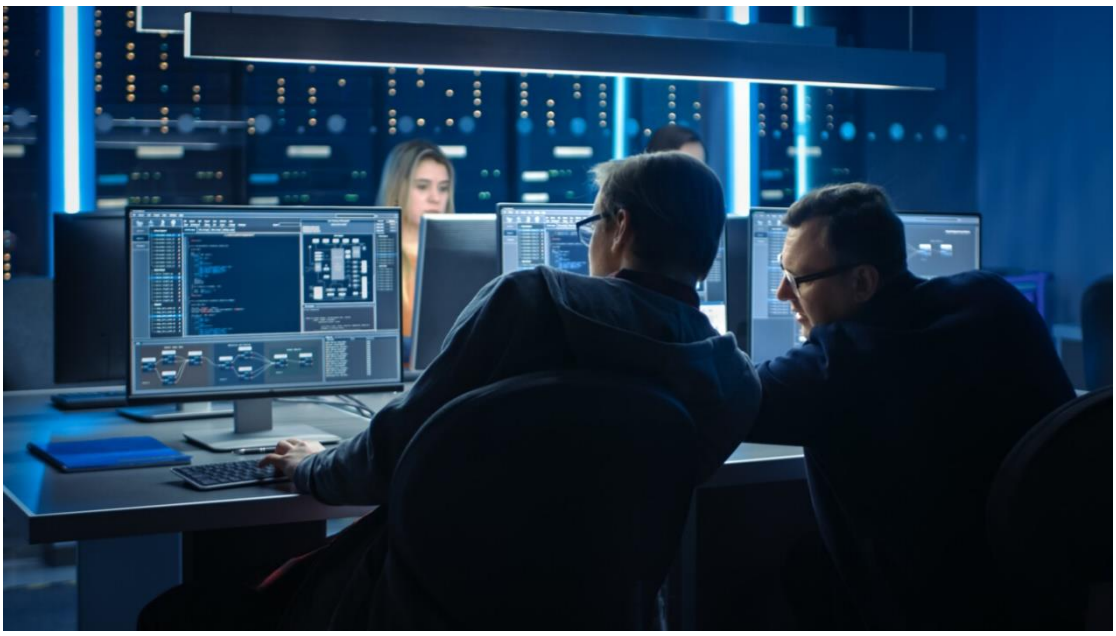
PQC 的下一步

随着 NIST 对首批 PQC 算法的批准，我们希望看到量子安全领域取得更多有意义的进展。一些公司已经开始将这些算法整合到特定应用和服务的安全协议中。例如，苹果公司正在使用 Kyber 在 iMessage 中创建后量子加密，而亚马逊正在 AWS 中使用 Kyber。

但 PQC 的大规模普及将在全球标准机构的参与之后才能实现。3GPP 和互联网工程任务组（IETF）等组织目前正在研究量子安全算法，并将其纳入未来标准版本的安全协议中。**诺基亚是许多正在研究 PQC 的行业标准化机构中的佼佼者，我们计划确保这些算法在未来的网络和通信标准中占据重要位置。这对我们的客户至关重要。**

这种标准化对于电信和互联网服务等行业至关重要，因为这些行业有数百家不同的公司提供网络的不同硬件、设备和软件组件。与任何安全协议一样，PQC 必须在网络中的所有暴露网元中一致实施，因为任何不符合量子安全的链接都将成为任何数据采集攻击的焦点。

未来几年，我们将看到越来越多的 PQC 增强型产品进入市场。起初，它们可能会像苹果和亚马逊那样，采用混合安全方法，同时使用经典和后量子加密方案。但随着量子安全技术的进步和市场的进一步检验，PQC 将有可能取代经典的非对称加密方法。



需要明确的是，我们还有更多的测试和验证工作要做。在 NIST 的试验中，安全专家让 Kyber、Dilithium、SPHINCS+ 和 Falcon 经受了各种经典和量子黑客的攻击，击败了数十种其它算法。但是，我们永远无法百分之百地确定这些算法能够真正抵御量子攻击。我们早已了解量子计算机在未来解密数据的方法，并利用这些知识在理论层面对 PQC 进行了严格测试。但一个简单的事实依然存在：目前还没有一台量子计算机强大到足以让我们对这些算法进行实证测试。

此外，数据安全一直是一个不断变化的目标，并将继续如此。虽然我们可以确定，这些最初的 PQC 算法可以保护我们免受第一波量子攻击，但量子威胁只会越来越复杂。聪明的黑客可能会开发出更好的方法来破解后量子加密密钥，或者出现更强大的 CRQC。此外，最近发表的几篇学术论文已经证明，可以利用人工智能中的概念来攻击 PQC。这些人工智能方法还远远无法破解 PQC 算法，但它们的存在意味着我们不能低估人工智能作为未来密码分析工具的威力。

因此，**信息和通信技术行业正在探索多种手段来保护我们的网络免受量子攻击，而不仅仅是 PQC 这样的数学方法。这种深入防御的量子安全策略包括基于物理的解决方案，如对称分发的预共享密钥和量子密钥分发（QKD），这将使攻击者无法截获加密密钥。通过实施多道防线，我们可以确保即使一道防线被攻破，我们的数据仍然受到保护。**

至于 PQC，我们的工作并没有因为有了第一波 PQC 算法而结束。

NIST 已经在为下一届世界杯做准备，接受包括诺基亚在内的全球各地团队提交的更多 PQC 算法。我们是创建数字签名算法 ALTEQ 的团队成员之一，该算法利用同构问题的数学难度，生成 CRQC 难以解决的加密算法。

ALTEQ 和其他许多新的 PQC 算法都将面临与 Kyber、Dilithium、SPHINCS+ 和 Falcon 一样的严峻挑战，此外还有安全界能想到的任何新的试验。几年后，我们完全有可能为新的获胜者加冕。这将是一件好事。我们的创新和改进越多，未来我们的数据就越安全。