简译版

为“后量子”时代做准备：五种安全策略

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	Start Preparing Now for the Post-Quantum Future		
原文作者	Tim Hollobeek	**原文发布日期**	2018 年 12 月 28 日
作者简介	Tim Hollobeek 是 DigiCert 公司的行业和标准技术战略专家。 https://www.darkreading.com/author-bio.asp?author_id=5102		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/perimeter/start-preparing-now-for-the-post-quantum-future/a/d-id/1333517		
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		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

为“后量子”时代做准备：五种安全策略

Tim Hollobeek

2018 年 12 月 28 日

“量子计算”（quantum computing）将会攻破我们目前所依赖的大多数加密方案。本文将介绍量子计算环境下的五种安全策略。

搜索“量子计算”一词，你会发现一场激烈的争论。支持者认为，人工智能、基因组学、经济学以及几乎所有领域都会取得突破性进展。反对者则认为，这些都是炒作。他们认为：即使大型量子计算机有可能出现，那也是几十年以后的事了。即使量子计算机出现，除了在一小部分问题上，它们也不会比标准计算机快多少。

然而，有一个观点双方都认同：量子计算将会攻破我们目前所依赖的大多数加密方案。如果你是企业的 IT 或安全系统负责人，这话一定会让你寒毛倒立。为了应对“后量子”（post-quantum）时代，现在是时候开始准备了。

量子计算围绕加密问题

关于量子计算机“可以做什么”的大部分争论仍然是推测性的，但在一些领域，它们的确会出类拔萃。早在 1994 年，数学家彼得·秀尔（Peter Shor）就提出了一种量子算法，该算法可以执行某些类型的计算，例如找到大数的质因子，而且计算速度远超过传统计算机。然而，目前最广泛使用的加密系统正是依赖于此类计算的。

云安全联盟的量子安全防护工作组（Quantum Safe Security Working Group）指出：

大型量子计算机将使用秀尔的算法，攻破所有采用 RSA（基于整数因子分解）、Diffie-Hellman（基于有限域离散对数）和 Elliptic Curve（基于椭圆曲线离散对数）加密算法的公钥系统。**目前使用的所有密钥交换和数字签名系统都依赖于这些算法。一旦出现能够处理数万个逻辑量子比特（qubit）的、尺寸合理的量子计算机，这些公钥算法将形同虚设。**

目前，上述规模的量子计算机仍然处于假设阶段。目前的量子计算机（如 IBM 和谷歌开发的量子计算机）可以处理的量子比特数有限。但是，研究人员每天都在推进这一数量。

麻省理工学院的艾萨克·庄（Isaac Chuang）说：“创建量子计算机还需花费大量资金。

但是，现在的问题在于工程工作，而非基本的物理问题。”

企业不具备时间优势

量子计算将会攻破 RSA 和其他常见的加密方案，这听起来非常糟糕。但是，如果大型量子计算机还有 10 到 15 年的时间才能出现，就像乐观的研究人员所认为的那样，我们就有足够的时间来开发后量子加密解决方案了，是吧？其实并不是，原因有两个。

首先，如果你认同 10 到 15 年的时间窗口，那么当第一台大型量子计算机上线时，现在发货的产品仍在使用中。以物联网（IoT）设备为例，如联网汽车、智能水电表、电力控制系统和交通基础设施；其中许多设备设计的运行时间长达 10 年或更长，而且它们几乎都使用 RSA 加密。

其次，虽然世界上一些最聪明的人正在研究“量子安全”加密机制，但这是需要时间的。实施他们最终推荐的新标准则需要更长的时间。

清点一下企业中依赖于公钥系统的各个流程和设备，如电子邮件、身份验证、在线金融交易等。更改和更新这些系统需要多长时间呢？很可能需要若干年。如果你处于受到严格监管的行业（如金融服务），并且面临复杂且具体的合规要求，则需要更长时间。

“部署现代公钥加密基础设施花费了近 20 年的时间，”美国国家标准与技术研究院（NIST）在其《后量子加密报告》中指出，“要从目前广泛使用的加密系统顺利、安全地迁移到量子计算对抗加密系统，需要付出很大的努力。因此，无论我们是否可以估计量子计算时代到来的确切时间，我们都必须立即开始为信息安全系统做准备，以对抗量子计算。”

五种安全策略

行业团体可能需要一段时间来确定后量子加密和身份验证的最佳方法，但企业无需等待，可以采取以下五种策略：

- **密切关注：**关注量子计算机和后量子标准/协议的开发，尤其是在设计具有 10 年以上寿命的物联网设备时。
- **将密钥长度加倍：**如果你认为量子计算机出现时当前系统仍在使用，建议你将对称算法的密钥长度加倍。AES-256 就是一个不错的起点，它的效率远低于短密钥。对于抗碰撞哈希函数，请使用 SHA-512。

- **采用基于哈希函数的签名：**基于哈希函数的签名是一种可行的量子安全信任机制。NIST 希望在 2019 年将其作为一项标准，届时企业可以采用该机制。这些签名还可用于安全部署更先进的量子安全技术。
- **混合加密：**金融行业的一些人正在探索混合加密技术，将传统的 RSA 或椭圆曲线加密与一种或多种新的“量子对抗”算法相结合。在该模型中，攻击者要想破解密钥交换，需要同时攻破多个加密方案。
- **与加密提供商讨论：**与你的加密提供商讨论其适应量子计算环境的计划，特别是如果你正在生产长寿命的物联网产品。经验丰富的提供商能够帮助你构建适应量子计算环境的加密方案，例如使用公钥基础设施执行基于证书的身份验证。

关于量子计算的争论很可能会继续下去，而且我们可能几年内都不会得到明确的答案。但是，智能 IT 和网络安全专家正采取积极主动的方法。企业现在就应该着手为后量子时代做准备了，只有这样，当量子计算浪潮袭来时，企业才可以掌控它，而非被拍死在沙滩上。

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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*