Sectigo 2024 年预测二：后量子密码将成为明年的热点

零信技术国际 SSL 证书战略合作伙伴 Sectigo 本月在其官网博客栏目发布了 2024 年数字安全领域的六大预测，笔者利用周末时间翻译并解读了这六大预测。

今天解读预测二：后量子密码将成为明年的热点。

后量子密码在我国已经是一个热门研究课题，北京雁栖湖国际后量子密码论坛已经成功举办了三届国际后量子密码标准化与应用研讨会。《信息安全与通信保密》2023 年第 9 期发布了文章《后量子密码发展综述》，讲的内容还是比较全面的，推荐有兴趣的读者查阅。

国际组织-PKI 联盟(PKIC)今年成立了一个后量子密码工作组(PQC WG)，专门讨论后量子密码相关的技术、产品和监管等相关话题，并负责维护一个 PQC 能力矩阵(PQCCM)，这是一个软件应用程序、库和硬件的 PQC 功能支持列表，让大家能了解全球有哪些厂商的产品正在或已经支持后量子密码。PKI 联盟正在积极致力于促进后量子密码的采用，维护 PQC 能力矩阵是 PKI 联盟的关键工作之一。零信技术非常重视后量子密码的研究工作，于今年 2 月份正式成为国际 PKI 联盟的成员单位，也是最早加入后量子密码工作组的成员之一。

PKI 联盟今年 11 月 7 日-8 日在荷兰阿姆斯特丹成功举办了第二届混合后量子密码工作会议，为期两天的工作会议讨论的话题非常丰富，笔者在这里推荐三个笔者认为非常精彩的演讲 PPT，有兴趣的读者可以下载学习。第一个是来自美国国家标准技术研究院(NIST)的 Bill Newhouse 先生和 Dustin Moody 博士的《NIST PQC 相关标准更新》，提供全面的 PQC 标准更新、对标准化现状的解读、以及简化从易受量子攻击的公钥密码体系到抗量子公钥密码体系的迁移实践的发展情况。第二个是来自 Cloudflare 研究工程师 Bas Westerbaan 的《后量子互联网的诞生》，浏览器正在准备默认启用后量子加密，以应对“先存储密文后解密”的威胁。加密只是故事的一半，后量子证书的部署更具挑战性。第三个是来自 Entrust 全球销售副总裁 Robert Hann 的《如何通过与零信任之旅相结合来销售后量子密码就绪》，从销售的角度讨论了如何利用零信任安全的热点优势，为 PQC 提供令人信服的应用，并分享一些最佳实践和技巧，介绍如何规划和执行与零信任安全相一致的成功实现 PQC 过渡。

鉴于笔者对后量子密码研究甚少和相关知识非常有限，本篇解读只能为有兴趣的读者提供一点与后量子密码相关的资讯，希望也能有所帮助。

<下面请读者朋友仔细阅读原文译文>

(C) 2023 零信技术（深圳）有限公司

后量子密码、加密敏捷性不再只是一个流行语，将成为明年相关企业高管们的重点关注点。这一转变得到了美国国家标准技术研究院(NIST)对抗量子加密技术的开发及其针对量子解密威胁的富有影响力的教育活动的大力支持。量子威胁不再只是理论上的讨论，而是已成为主流焦点。

随着 2024 新年的临近，一个关键的转变即将到来，它将把后量子密码学从 IT 行业首席信息安全官的小众关注提升到董事会层面来讨论。向抗量子加密技术过渡的必要性不再属于技术团队和安全专家的范畴，这将成为跨行业高管对话的主导因素。明年将见证组织如何实施网络安全战略的范式转变。

美国国家标准技术研究院大力支持

这一转变的催化剂可以追溯到美国国家标准与技术研究院，它是国际密码标准领域的关键参与者。为了应对量子计算对传统加密方法日益增长的威胁，NIST 率先开发了抗量子加密算法。曾经是关于当前加密模型漏洞的理论讨论现在已经转化为切实关键行动。

从利基讨论到主流业务焦点

在接下来的 12 个月里，组织将不再将抗量子密码视为一个流行词或一个可以顺便简单讨论的话题。相反，如何实现加密敏捷将成为高管层的关键战略重点。这种紧迫性源于这样一个事实：量子计算机的处理能力呈指数级增长，有可能使当前的密码系统变得过时。从本质上讲，数字安全的基础正受到威胁。

在整个 2023 年，人们越来越意识到量子计算对传统解密方法构成了迫在眉睫的威胁。曾经的小众领域和理论讨论正在转变为主流业务焦点。量子计算被认为比当今的计算机快 1.58 亿倍，因此真正的问题不应该是“为什么高管层应该谈论量子”，而是“为什么他们还没有谈论

(C) 2023 零信技术（深圳）有限公司

量子？”

数字时代的生存：量子时代企业的利害关系

这种紧迫性背后的主要驱动因素之一是量子计算机有能力在多项式时间内破解广泛使用的加密算法，如 RSA 和 ECC，这意味着曾经被认为是安全的机密数据可以被毫不费力地被破解。随着企业努力应对这种量子威胁的影响，采用抗量子密码技术的需要不仅是谨慎的问题，也是数字时代生存的问题之一。

曾遭受 SSL 证书中断的企业所报告的财务损失从每分钟几百美元到每小时 100 万到 600 万美元不等。如果这就是短时间离线的代价，那么不难想象，当敏感数据在几秒钟内容易受到未经授权的访问时，企业和政府将会面临什么后果，赌注从未如此之高。

董事会将需要讨论什么？

企业领导者需要重新评估当前的加密基础设施，并制定抗量子解决方案的路线图。这种转变并非没有挑战，因为实施新的加密协议需要仔细规划、资源分配以及对不断变化的威胁形势的敏锐理解。主动采用抗量子加密的组织不仅可以加强其网络安全态势，而且可以在日益数字化和互联的世界中获得竞争优势。 包括客户、投资者和监管机构在内的利益相关者可能会积极看待此类主动措施，从而对组织保护敏感信息的承诺建立信任和信心。

后量子密码将是 2024 年的积极姿态

Sectigo 相信，后量子密码的兴起将成为 2024 年董事会的主流讨论话题，不仅仅是对潜在威胁的回应，而且是确保数字通信未来的积极立场。NIST 在塑造这一叙事中发挥的关键作用强调了应对抗量子加密的复杂性所需的协作努力。随着企业做好准备迎接量子挑战，明年有望成为网络安全持续发展的转折点，适应性和远见将成为在不断变化的数字环境中取得成功的关键。

王高华

2023 年 12 月 20 日于深圳

(C) 2023 零信技术（深圳）有限公司

请关注公司公众号，实时推送公司 CEO 精彩博文。

(C) 2023 零信技术（深圳）有限公司