解读 Sectigo 2024 年预测六：RSA 将受到围攻

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 年数字安全领域的七大预测，笔者利用周末时间翻译并解读了这七大预测。

今天解读预测六：RSA 将受到围攻。

笔者不是密码算法专家，只是密码算法在 PKI/CA 中的应用专家，笔者能从 Sectigo 博文中读出 Sectigo 专家对破解 RSA 算法的担忧，这个担忧不是大家所知的量子计算将能破解 RSA 算法，而是大家已经从量子计算如何破解 RSA 算法中获得了灵感，可以参考这种思路找出采用目前的算力来破解 RSA 的方法。

本文对我国商用密码算法的启示是：我国必须加强对商用密码算法 SM2/SM3/SM4/SM9 可能遭遇破解的研究，这种研究不能只是抗量子的研究，同时也要研究在当前的算力下是否有可能破解商用密码算法，这是本文的最大启示。

笔者作为一个密码算法的 CA 应用工作者，非常期待我国能及时启用更长密钥位数的商密算法，因为国际 CA 已经纷纷启用了 521 位和 384 位的 ECC 算法根证书，以及开始签发 384 位的 ECC 用户证书，而我国仍然停留在 256 位 SM2 算法根证书和用户证书中。

<下面请读者朋友仔细阅读原文译文>

研究人员和黑客都在抓紧努力破解 RSA 加密。后量子密码给了大家启示，其实可以不用等量子计算机出来就可以尝试破解 RSA。2024 年，将出现大量的 RSA 破解尝试。尽管预计 RSA 不会被攻破，但它将面临巨大的压力。

数字安全格局的特征是不断变化和动态变化，2024 年有望标志着一个重要的转折点。这

个关键的一年将使 RSA 加密算法面临前所未有的审查，因为世界各地的研究人员都在加强努力打破这个互联网的安全支柱。我们应该准备好迎接破解 RSA 的新捷径，我们正站在加密漏洞新时代的边缘。此预测可作为您对迫在眉睫的威胁的独家先睹为快，并指导您在未来一年内应对加密漏洞和数字安全的复杂领域。

后量子密码：为研究人员指明方向

对 RSA 加密的围攻迫在眉睫的催化剂是对量子计算机对 RSA 构成的威胁以及对后量子密码(PQC)的需求的广泛理解。随着 RSA 破解的想法越来越受到关注，它促进了对击败 RSA 的基本原理的研究，而无论有没有量子计算架构的参与。

2024 年，密码专家将继续探索 RSA 漏洞，以寻求新方法来缩短发现 RSA 密钥的时间。长期以来，RSA 不可攻破的假设已成为过去。我们预计该算法不会在 2024 年被破解，但我们确实预计更多实用攻击的尝试将进一步削弱这种长期服务的算法。

研究 RSA 的漏洞

量子计算机将击败 RSA 和 ECC 算法，研究人员正在投入精力寻找最有效的策略。这项研究也可以借鉴如何用传统计算机击败 RSA。毕竟，任何能够访问量子计算的攻击者也能够访问它需要的所有传统计算架构。

这一事实不仅是探索基于量子计算的攻击的动力，也是探索传统攻击以及两者如何协同工作的动力。我们应该期待未来几年的持续启示，这将在各个方面缩短破解 RSA 的时间。虽然这些攻击本身不太可能将计算时间缩短到代表我们今天常用的密钥大小的可行攻击向量的程度，但它们将推动更多的研究，并最终有助于优化基于量子的攻击，我们有一天会理解这一点。

期待

虽然对 RSA 加密的围攻正在进行中，但必须承认加密方法本身是强大的，并且经受住了 40 多年的技术创新。这没有受到挑战。

然而，我们将看到对这种算法的持续审查，为量子计算机可以执行这种攻击的那一天做准备。我们将看到对将传统方法应用于量子平台的想法的持续审查，我们将看到对同时使用两种架构的混合攻击的充分考虑。虽然我们预计没有一台计算机能在 2024 年完成这些攻击，但随着更多已发表的论文和关于如何打破数字安全堡垒的启示，最终有一天被破

解的趋势正在加速。

王高华

2023 年 12 月 27 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。