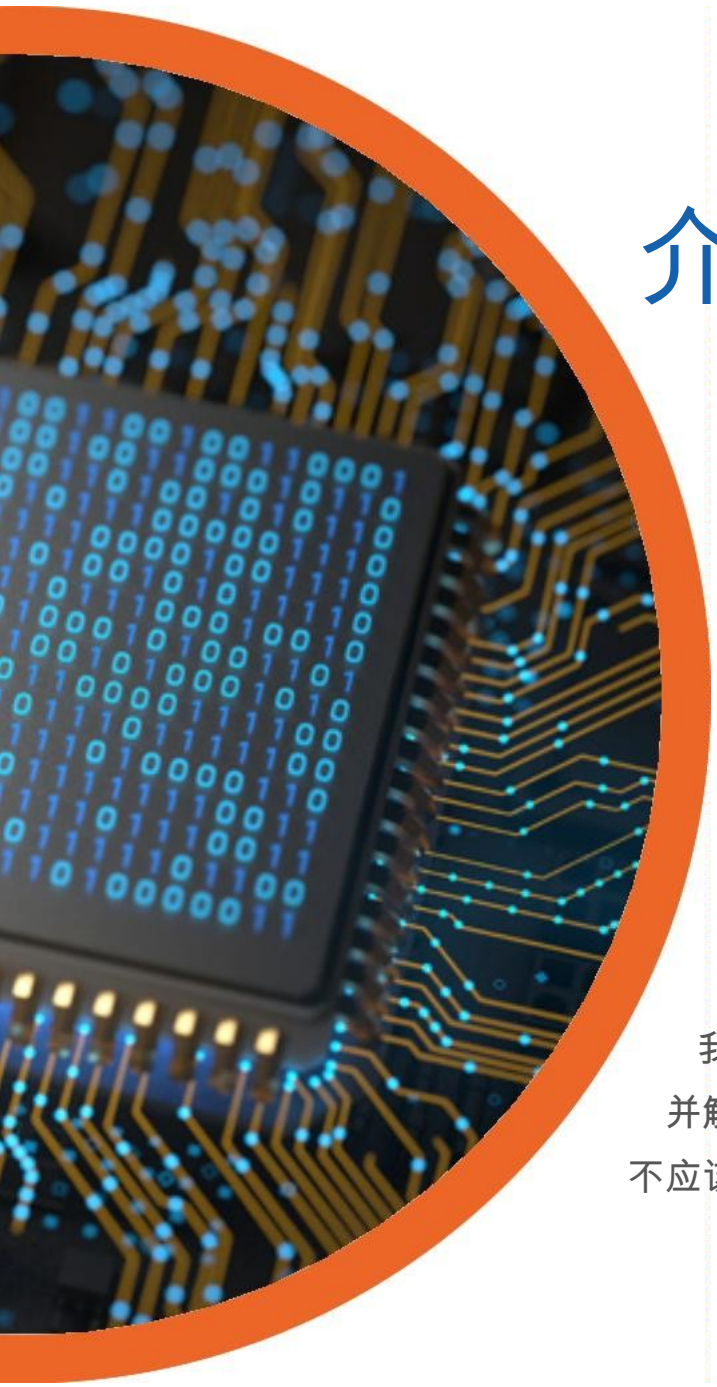
GlobalSign by GMO

后量子计算和证书颁发机构

探索密码学的未来

目录



介绍

在技术飞速发展的时代，对于证书颁发机构（ CA ）客户来说，

了解可能影响其数字证书安全性的新趋势至关重要。

其中一个趋势是

后量子计算（ PQC ）的发展，它有可能

颠覆当前的密码算法。

在这本电子书中，

我们将讨论围绕 PQC 的问题，

并解释为什么 CA 客户

不应该担心它对他们证书的影响。

了解后量子计算的基础知识

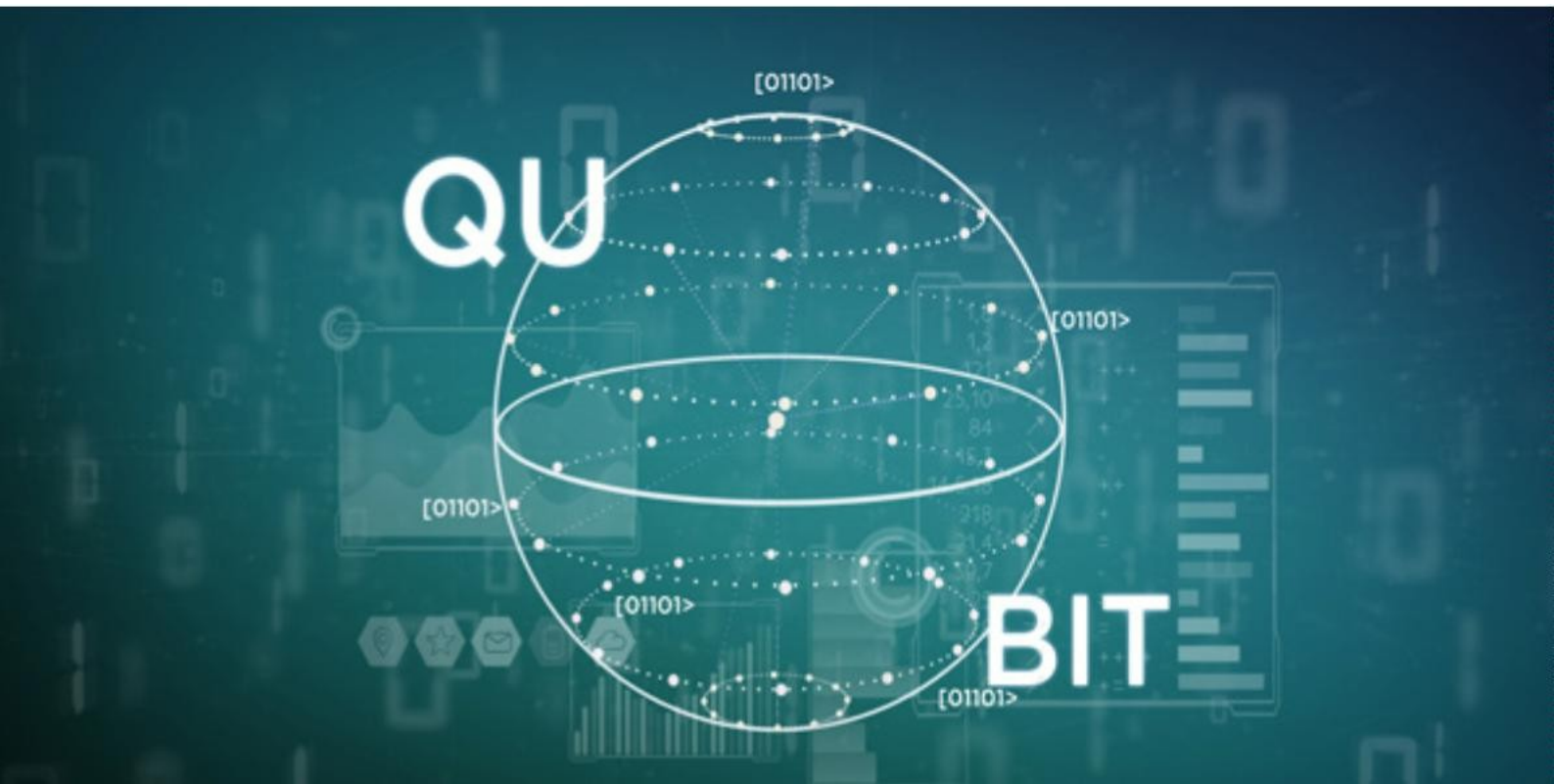
为了理解它的含义，让我们首先深入研究量子计算的概念以及它在密码学世界中引起轰动的原因。

量子计算：计算能力的范式转变

我们每天使用的传统计算机利用比特来处理信息。这些比特可以代表 0 或 1 ，构成了驱动我们数字世界的二进制代码的基础。另一方面，量子计算机使用量子比特或量子位工作。与经典比特不同，量子比特可以同时以 0 和 1 两种状态的叠加存在。这种独特的特性使量子计算机能够并行处理大量信息，使某些复杂的计算比经典计算机快得多。

量子密码的威胁

量子计算的强大也有它的另一面。虽然量子计算机在解决某些问题（如模拟分子相互作用或优化复杂系统）方面具有巨大的潜力，但它们也具有破解目前保护我们数字通信的密码系统的能力。这种威胁主要影响非对称加密算法，而我们的网络安全很大程度上依赖于非对称加密算法。



非对称密码学，也称为公钥密码学，涉及
密钥对的使用——一个用于加密的公钥和一个用于
解密的私钥。 RSA （ rivests - shamir – adleman ）和 ECC
（ Elliptic Curve Cryptography ）等广泛使用的算法依赖于
某些数学问题的难度，如大数因式分解或
求解离散对数问题。传统计算机
很难有效地解决这些问题，使
加密和数字签名变得安全。

量子优势

如果以足够大且稳定的
规模实现量子计算机，则可以利用它们执行
某些计算的能力以指数级速度加快。例如，
一种名为 Shor 算法的算法可以
在量子计算机上在多项式时间内分解大数，
从而破解 RSA 加密的
数学基础。类似地，量子版本的
离散对数算法也可能危及 ECC 。

后量子密码的诞生

这就是后量子密码学进入图像的
地方。该领域的目标是开发新的
密码算法，保持抵抗量子攻击。
研究人员正在探索量子计算机无法
显著更快地解决的数学问题，
从而确保即使在量子驱动的世界中的安全性。

有趣的是，这些新算法通常来自不同的
数学学科，如格理论、基于码的密码学、
多元多项式等。他们的任务是建立一个新的
密码基础，能够抵御量子攻击。

介绍后量子计算思想（PQC）

到目前为止，我们已经揭示了量子计算的迷人世界，以及它颠覆我们所知的安全格局的潜力。现在，让我们深入探索 PQC 的领域，并探索它在确保我们的密码系统的弹性方面的关键作用。

抵御量子威胁

想象一个场景，一个足够强大的量子计算机出现在技术的地平线上。目前为安全在线通信提供基础的算法——保护我们的个人数据、金融交易和机密信息的算法——可能会变得脆弱。这一量子威胁促使全球密码学界共同呼吁采取行动。

进入后量子计算时代

PQC 不仅仅是一个流行词；这是对量子挑战的战略性回应。 PQC 的核心目标非常明确：开发能够抵御量子计算机发起的攻击的密码算法。本质上， PQC 是一个数字堡垒，在这个量子计算机可能摧毁我们所依赖的安全保障的时代，它将加强我们的信息。

让 PQC 格外引人注目的是其雄心勃勃的范围。这是一项前瞻性的努力，需要在数学和计算机科学的各个领域进行创新。 PQC 不是试图修补现有的密码算法，而是创造全新的方法，利用量子计算机无法以闪电速度破解的数学问题。

抗量子搜索

PQC 领域的研究人员正在探索挑战量子计算优势的各种数学挑战。这些挑战来自编码理论、数论等领域。基于格的密码学、基于代码的密码学、基于哈希的密码学和多元多项式的算法是这场密码学探索中的一些竞争者。

是马拉松，不是短跑

重要的是要理解 PQC 是一个持续的过程。研究人员正在精心开发和测试新的密码算法，对它们进行严格的审查，以确保它们的量子抵抗能力。此外，这些算法还必须在更广泛的安全性、可用性和性能背景下证明自己，才能被认为是现有系统的有价值的接班人。

过渡的桥梁

随着我们冒险走向量子计算机时代，向 PQC 的过渡将是一个慎重和周到的过渡。密码学社区，以及机构和组织，将需要协调从经典密码方法到后量子密码方法的平稳转变。这种转变需要仔细的计划、标准化和协作。

PQC 的现实：仍在研究阶段

当我们深入 PQC 的迷人领域时，将我们的探索锚定在当前的现实中是至关重要的。 PQC 是量子计算机的潜力和当今技术景观的实用性之间的桥梁。

未来的展望和正在进行的演变

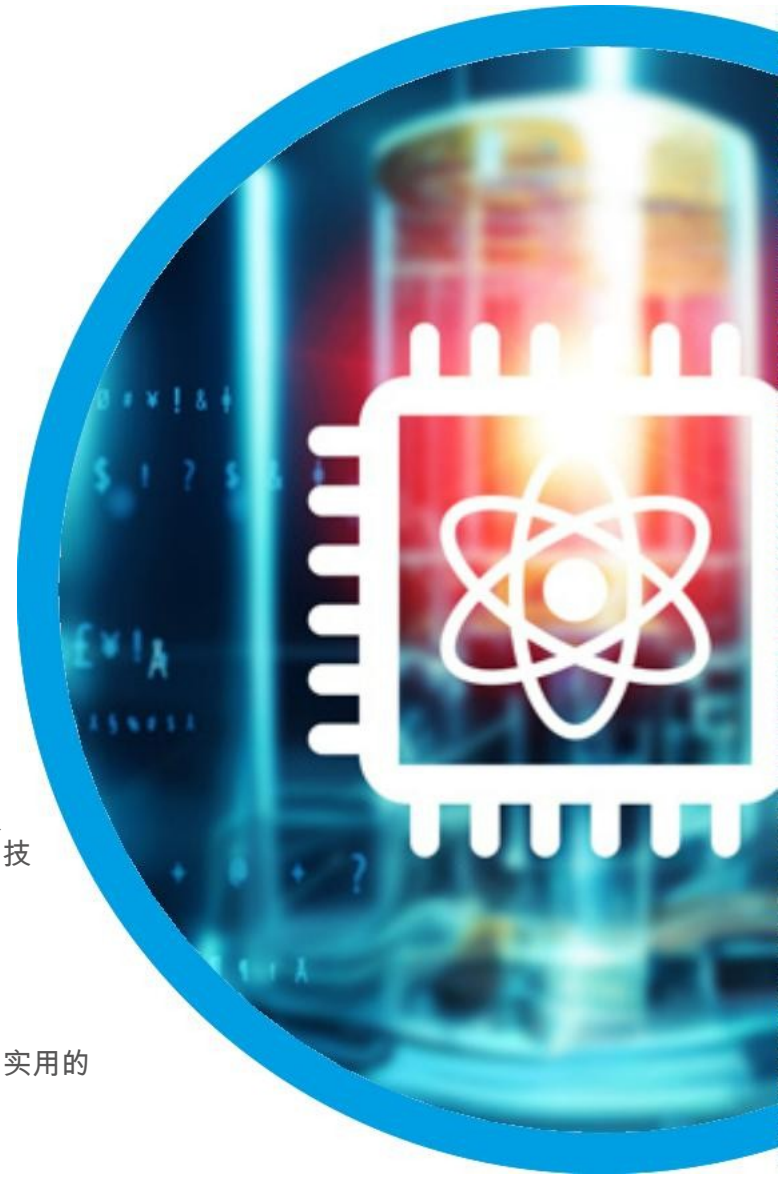
在我们进一步讨论之前，重要的是要注意，能够挑战现有密码系统的实用量子计算机仍然处于正在进行的研究领域。由于复杂的技术挑战，这些强大的机器尚未实现。

几十年来，量子计算机的概念一直吸引着研究人员。然而，构建和维护量子计算机，将量子比特（量子位）操作用于复杂操作，存在巨大的障碍。量子系统对噪声、干扰和“量子退相干”很敏感，它会破坏微妙的量子态。

后量子密码学是量子领域的重要组成部分。预测了量子计算机对经典密码方法的潜在影响。全球研究人员合作开发可以抵御量子攻击的密码算法。

迈向实用量子计算的旅程

目前，量子计算机主要用于研究和实验。它们远没有达到高效执行 Shor 算法所需的计算能力，这对现有的加密方法构成了威胁。量子计算机面临着诸如量子比特一致性、错误纠正和可扩展性等挑战。



认识到研究阶段在 PQC 中的关键作用。新的密码算法不仅要通过理论测试，还要证明其实用性、高效性和现实世界的弹性。

当我们深入研究 PQC 对证书安全性的影响时，请记住，我们正站在量子地平线的边缘。量子计算机可以重新定义计算，但它们的全面实现需要经历科学发现、工程壮举和技术创新的多方面旅程。

对于那些对即将到来的量子革命感到好奇的人：请放心，实用的量子计算机仍然是未来的领域。

当前证书的强度

当前证书的稳健性：建立在坚实的基础上

在我们穿越 PQC 错综复杂的地形的旅程中，至关重要的是将我们自己锚定在现在。构成安全在线通信基石的证书不仅仅是代币；它们被久经考验的加密算法加固，多年来一直保护着数字交互。

这些证书的核心是非对称加密，这是现代网络安全的基石。非对称加密，也称为公钥加密，使用一对加密密钥：一个用于加密的公钥和一个用于解密的私钥。这种巧妙的机制可以实现安全的数据传输、数字签名以及在互联网上建立安全连接。

当我们面对复杂的密码学潮流时，认识到当前的加密算法是为了抵御经典攻击而构建的是很重要的。在面对无数的计算挑战和详尽的数学分析时，这些算法已经证明了它们的弹性。

你的证书：安全的证明

可信证书颁发机构签发的证书由这些久经考验的加密算法支撑。它们能够实现安全的在线交易，保护敏感数据，并在数字交互中建立信任。放心吧，这些算法一直是数字领域的守护者，即使技术在不断发展。

充满信心地展望未来

当您在数字领域遨游时，重要的是要记住，虽然量子时代正在地平线上招手，但当前的加密基础设施仍然强大。在接下来的章节中，我们将深入探讨后量子计算对这些证书的潜在影响，以及证书颁发机构正在采用的策略，以确保你在不断变化的世界中数字安全。

证书：您在数字领域中值得信任的守护者

当我们开始探索密码学及其不断发展的格局时，我们希望向您提供充分的保证。由可信的证书颁发机构签发的证书就像永不动摇的哨兵，以对安全的坚定承诺守护着您的数字资产。

坚不可摧的加密之盾

每当你访问一个安全网站，进行数字身份验证，或者发送加密通信时，证书就是加密力量的体现。 RSA （ Rivest-Shamir-Adleman ）和 ECC （ Elliptic Curve Cryptography ）
等加密算法支撑着这些证书，它们不仅仅是一行代码；它们是数十年研究、改进和经过验证的安全性的结晶。

RSA 和 ECC 的强度不仅在于它们的数学复杂性，还在于它们能够抵抗最复杂的经典计算攻击。这些算法以分解大数或求解离散对数等数学挑战为基础，确保你的数字资产得到安全保护，即使在技术进步的情况下。

数字证书不仅仅是加密数据；它们验证个人、组织和网站的身份。当你在浏览器地址栏中看到挂锁图标或收到数字签名的电子邮件时，你正在见证证书在互联世界中验证真实性和建立信任的力量。

让您安心：我们的首要任务

在一个不断发展的数字环境中，内心的平静仍然是至关重要的。放心，您的证书，通过强大的加密算法加强，是保护您的数字资产的坚定盟友。随着未来的发展和技术的进步，证书颁发机构对你安全的承诺不会动摇。

探索量子领域

当量子计算的前景和后量子密码学的地平线在召唤你时，请记住，你所依赖的证书根植于此时此地。它们被设计成能够抵抗当前的经典计算攻击。

一个充满弹性的未来等待着我们

保护你在线互动的数字证书不仅仅是符号；它们有力地保证了您的数据、通信和交易都得到了可用的最佳工具的保护。当我们冒险进入量子领域时，您对这些证书的信任一如既往地有根据。

后量子密码学：一个持续的过程

当我们站在密码学和量子可能性的交叉点上时，必须认识到进入后量子密码学领域的旅程是一个动态的旅程。让我们深入研究正在进行的研究、集体努力以及定义这一旅程的逐步过渡。

蓬勃发展的研究领域

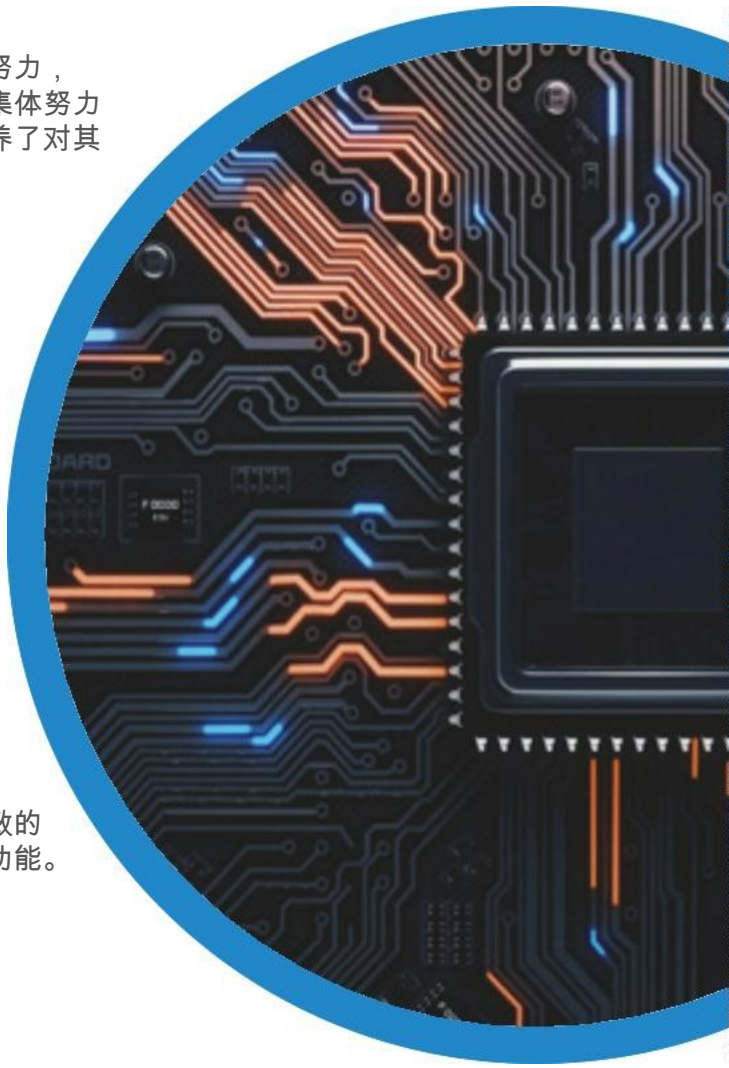
后量子密码学领域充满了研究人员、数学家和计算机科学家的合作，以挖掘新的密码算法。这些算法不仅旨在阻止来自经典计算机的攻击，还旨在阻止即将出现的量子武器库的攻击。该研究涵盖了从格到编码再到多元多项式的各种数学概念。

对量子阻力的追求

后量子密码背后的驱动力是追求能够抵抗量子计算机潜在威力的算法。研究人员正在探索即使在量子计算优势面前仍保持其复杂性的数学问题。我们的目标是确保我们所依赖的安全始终不变，无论未来的技术如何进步。

合作交响曲

后量子算法的发展是一支多人创作的交响乐。这是一项协作努力，汇集了来自学术界、行业专家和标准组织的研究人员。这种集体努力确保了新的加密方法受到严格的分析、审查和验证，从而培养了对其有效性的信任感。



安全标准

标准组织在后量子密码学领域发挥着关键作用。正如他们指导采用现有的密码标准，他们在确保后量子算法满足安全性、实用性和互操作性的严格标准的最前沿。这一标准化过程对于构建安全的数字未来至关重要。

导航过渡效果

后量子密码学旅程的一个关键方面是过渡本身。从经典密码算法到后量子密码算法是一个精心策划的过程。它涉及到细致的计划、测试和实现，以确保无缝转换，而不会影响安全性或功能。

渐进的演变

需要注意的是，向后量子密码的过渡将是渐进的。
随着新的算法从研究熔炉中诞生并经历严格的验证，组织和系统将逐渐将它们纳入他们的加密基础设施。这确保了在适应不断变化的密码学环境的同时安全性保持不变。

为量子时代做准备

虽然实用的量子计算机仍然是未来的可能，但为它们到来的准备工作正在进行中。今天正在进行的努力——从研究和开发到合作和标准化——正在为未来的安全数字奠定基础。

CA 在确保未来安全方面的作用

当我们在错综复杂的密码学领域中穿行时，必须认识到证书颁发机构（ CA ）在确保未来数字交互安全中所起的不可或缺的作用。让我们探索 CA 如何保持在密码学进步的前沿，监控后量子密码学的进展，并为无缝过渡到量子可能性时代做好准备。

领先潮流

证书颁发机构不仅仅是旁观者；他们是数字安全的积极保管人。 CA 深入密码学领域，不断监控进展、突破和新出现的威胁。这种警惕确保他们准备好适应行业的变化，并为客户提供尖端的解决方案。

后量子密码学的兴起对 CA 来说并不是一个谜；这是他们战略愿景的组成部分。中科院认识到量子计算机对当前密码方法的潜在影响，并努力跟踪后量子密码研究的进展。他们致力于了解新算法是如何形成的，以及它们如何与客户不断发展的安全需求保持一致。

为量子安全铺平道路

向后量子密码算法的过渡并不是一个孤立的努力；这是 CA 和他们的客户之间的伙伴关系。 CA 有助于确保迁移过程无缝、安全、协调。他们在密码学、安全协议和数字证书管理方面的专业知识将成为组织向抗量子方法过渡的基石。

可信赖的伙伴

作为证书颁发机构的客户，在这段加密之旅中，你并不孤单。CA 理解后量子密码等新兴技术带来的担忧和不确定性。作为 CA ， GlobalSign 致力于通过提供准确的信息、明确的指导和坚定的支持来缓解这些担忧。

量子未来等待着我们

量子未来不是一个遥远的梦想；这是一个正在迅速逼近的领域。当您踏上这条道路时，请放心，GlobalSign 配备了导航您身边的量子地形。 CA 、研究人员和行业专家之间的协作精神确保您的数字安全始终坚定，无论前方面临的挑战如何。

结论

虽然后量子计算代表了一个令人兴奋的技术前沿，但围绕其对证书安全影响的担忧不应掩盖当前密码算法的强度和可靠性。通过了解正在进行的后量子密码学研究并及时了解情况，客户可以对其证书的安全性有信心。作为值得信赖的合作伙伴， GlobalSign 将与我们的客户一起引领向后量子加密的过渡，确保一个安全和无缝的未来。

关于 GMO GlobalSign

作为全球最具影响力的认证机构之一，GlobalSign是全球领先的可信身份和安全解决方案提供商，使全球的组织、大型企业、云服务提供商和物联网创新者能够进行安全的在线通信，管理数百万已验证数字身份以及自动化认证和加密。其大规模的PKI和身份解决方案支持构成物联网的数十亿项服务、设备、人和物。GMO GlobalSign是日本GMO云KK和GMO互联网集团的子公司，在美洲、欧洲和亚洲设有办事处。欲了解更多信息，请访问https://www.globalsign.cn。

GlobalSign CN

上海市普陀区陕西北路 1438 号财富时代大厦 706 室

+86 021 60952260

www.globalsign.cn