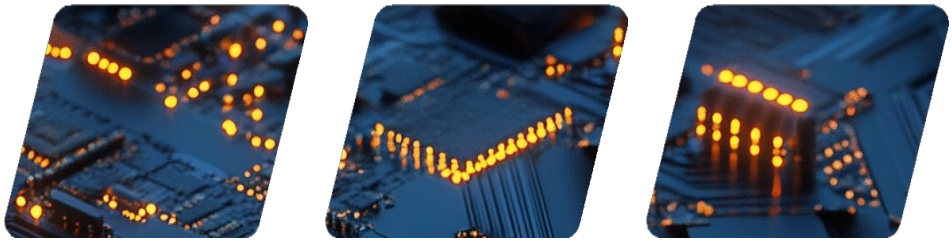
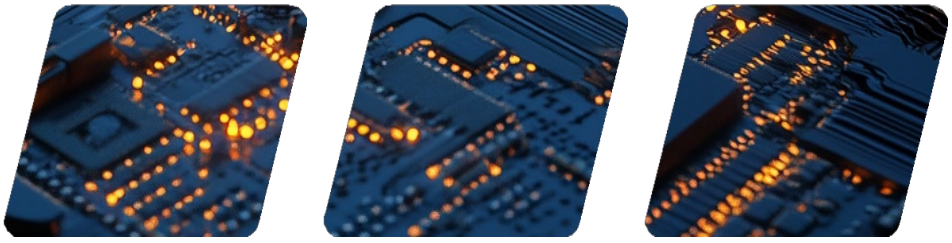


后量子加密（PQC）：

为量子时代的未来保驾护航



白皮书

作者：

莱迪思半导体公司安全、电信和数据中心战略业务开发部高级总监Mamta Gupta

莱迪思半导体安全解决方案总监Jordan Anderson

莱迪思半导体产品安全架构师Temoc Chavez Corona

莱迪思半导体产品安全架构师Mehryar Rahmatian

免责声明

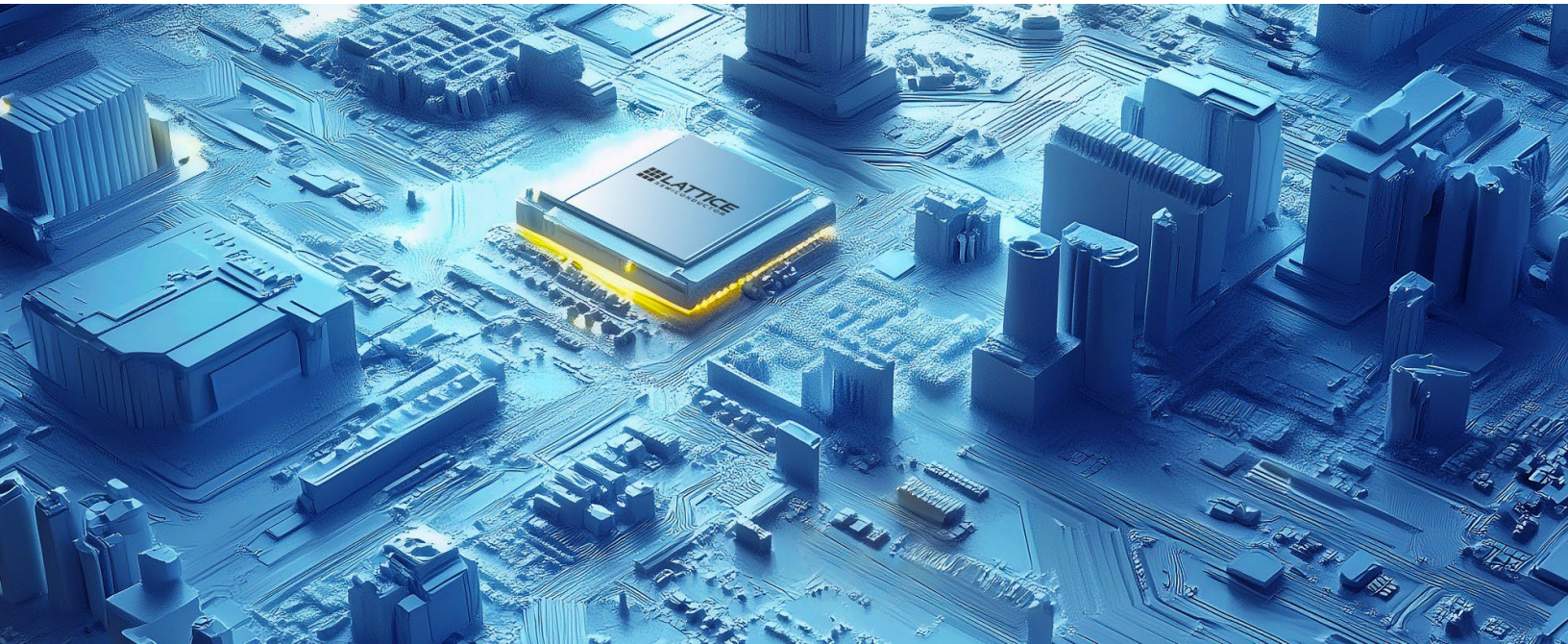
包容性用语

本文档的创建符合莱迪思半导体的包容性用语政策。在某些情况下，基础工具和其他项目中的语言可能尚未更新。请参阅莱迪思的包容性用语常见问题解答6878，获取术语的交叉参考。请注意，在某些情况下，如寄存器名称和状态名称，有必要继续使用旧的术语以保证兼容性。

摘要

量子计算的快速发展对传统密码系统构成了重大威胁。

在量子计算可能颠覆传统密码系统的时代，采取行动迫在眉睫。本白皮书深入探讨了当前加密协议的漏洞，介绍了最新标准化的PQC算法，为那些希望采取措施对抗量子威胁的组织提供了战略路线图。通过采用莱迪思半导体的创新解决方案，您可以保护您的数字资产，在量子时代保持领先。



目录

1.引言

1.1. 当前加密方案面临的挑战

量子计算不仅仅是一个理论概念，它正快速融入现实，可能动摇全球数字安全的基础。从确保金融交易安全到保护私人通信，当今几乎所有的安全系统都使用RSA和ECC加密算法。面对能够轻松破解这些算法的量子算法，这些传统加密方法濒临淘汰边缘[1]。向量子抗性加密技术的转变不仅是一项建议，而且必不可少。虽然量子计算机仍在开发之中，但抵御其攻击的时间窗口正在快速关闭。

现在是时候采取行动加强防御、维护全球数字安全完整性了。

1.2. PQC的采用和加密敏捷

从RSA和ECC加密算法迁移到后量子算法需要更新整个安全基础设施。这影响到从公钥基础设施（PKI）系统和硬件安全模块（HSM）到通信协议和硬件加密引擎的方方面面。PQC作为一项新技术，将会持续发展。加密解决方案必须支持“加密灵活性”，以适应新标准。

在多数情况下，迁移到PQC算法需要在硬件层面进行更改。使用现场可编程门阵列（FPGA）设计的系统在采用PQC算法方面具有显著优势。FPGA固有的适应性使其成为PQC算法移植的理想选择。随着PQC算法的不断发展，FPGA通过可重新配置特性进行调整的能力具有显著优势，可确保加密实现与最新和最安全的标准保持同步。面对快速发展的量子计算能力，这种灵活性对于保持系统的完整性至关重要。

莱迪思半导体的FPGA产品为NIST批准的PQC算法提供内置支持，且支持加密敏捷，是安全关键操作和PQC迁移工作的理想选择。

1.3. 量子计算的进步

量子计算已从早期的理论探讨发展到实际应用。研究人员已经证明了量子的优越性[2]。本节重点介绍量子计算机的优势及其带来的威胁。量子算法，如用于因式分解的肖尔算法和用于搜索的格罗弗算法，对加密算法构成的威胁迫在眉睫，因此转向PQC十分有必要。由于其独特的运行特性，量子计算机擅长解决某些类型的问题，而这些问题对经典计算机来说极具挑战性。量子计算显示出巨大潜力的一些领域包括：

优化问题：通过高效探索多种组合，优化送货车辆的路线安排、航班调度或供应链管理。

量子系统模拟：在材料科学和药理学等领域，研究人员可以利用量子计算机了解复杂分子，从而发现新材料和新药物。

机器学习和人工智能：更高效地处理大型数据集，从而在自动驾驶和个性化医疗等领域建立更强大的预测模型，缩短处理时间。

解决理论物理学中的难题：量子计算可以帮助研究人员深入了解量子力学和其他复杂的物理理论，为理论物理学做出重大贡献。这将提高人们对高能物理、引力、化学和宇宙学的理解。

1.4. 量子威胁

加密：量子计算机可以高效地解决公钥加密的基础问题，如整数因式分解和离散对数，从而破解当前的许多密码系统。这种能力将危及数据安全系统。

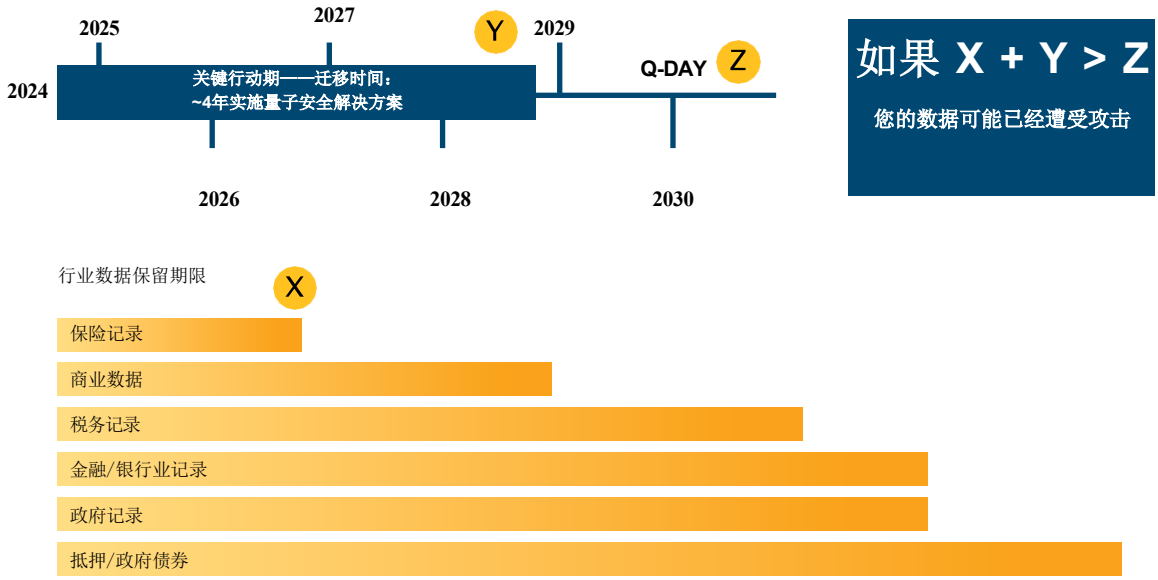
量子计算技术的发展和扩展有望在许多领域取得重大突破，有可能带来目前经典计算技术无法想象的解决方案。然而，解决这些问题的潜力也凸显了对量子安全加密方法的需求，以保护敏感信息免受未来量子技术的威胁。

2. 采用PQC迫在眉睫

2.1. 哪些领域会受影响

如果没有量子安全加密技术，所有在公共信道上传输的信息（无论是现在还是将来）都易受攻击。一旦量子计算机技术进一步发展，当前存储的加密数据以后就能被轻易解密。传输信息的完整性和真实性将受到损害，从而违反数据隐私和安全方面的监管要求。这种风险的影响范围包括：政府和军事通信、金融和银行交易、医疗数据和医疗记录、云端存储的个人数据以及企业机密网络的访问权限。见图1。

图1：立即采取措施至关重要



现在就是行动的最好时机。你为抵御量子攻击准备了什么计划？

2.2. “先收集，后解密”式攻击

“先收集，后解密”（HNDL）式攻击，又称“先存储、后解密”（SNDL）攻击，是一个迫在眉睫的安全问题。攻击者当下存储窃取的加密数据，然后在量子计算取得进展后再进行解密。对于需要保证长期数据安全的组织来说，这是一个严重的威胁，需要立即采取行动。见图 2。

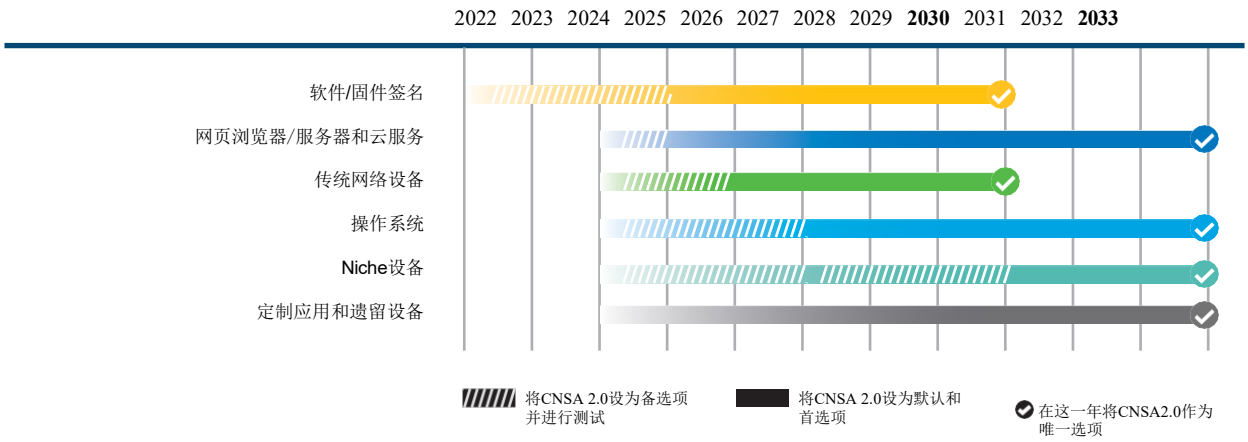
2.3. CNSA 2.0时间表

2022年9月7日，美国国家安全局发布了《商用国家安全算法套件2.0》（CNSA 2.0）[3]。该文件规定了与国家安全相关的系统中应使用的加密算法。不符合标准不仅存在风险，更是完全不可接受的。对于任何处理美国基础设施敏感数据的组织而言，遵守这些标准至关重要。见图2。

CNSA 2.0强制要求使用以下PQC算法，在某些场景下最早自2025年生效：

- XMSS/LMS
- ML-DSA (CRYSTALS-Dilithium)
- ML-KEM (CYRSTALS-Kyber)
- XMSS和LMS已被批准用于代码签名和代码验证用例

图2：CNSA 2.0时间线

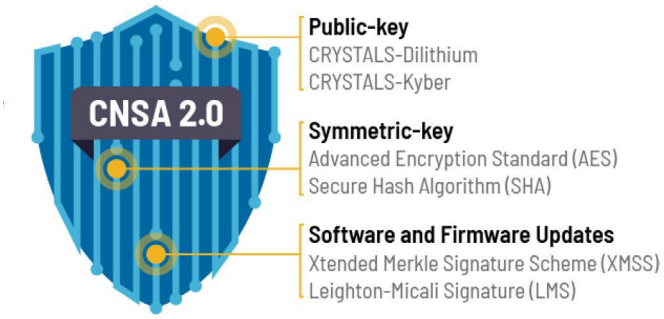


ML-DSA和ML-KEM获批成为新的公钥加密算法，取代RSA、Diffie-Hellman密钥交换、椭圆曲线Diffie-Hellman（ECDH）和椭圆曲线数字签名算法（ECDSA）。AES-256仍是对称加密标准。安全散列算法SHA-384或SHA-512仍是标准的散列算法。

CNSA 2.0算法套件如图3所示。CNSA 2.0要求中的关键日期包括：

- **软件/固件签名：**到2025年，PQC算法必须作为默认算法和首选算法使用
- **网络浏览器/服务器和云服务：**到2026年，PQC算法必须作为默认和首选算法使用
- **传统网络设备：**到2025年，PQC算法必须作为默认和首选算法使用
- **操作系统：**到2027年，PQC 算法必须作为默认算法和首选算法使用

图3: CNSA 2.0算法套件



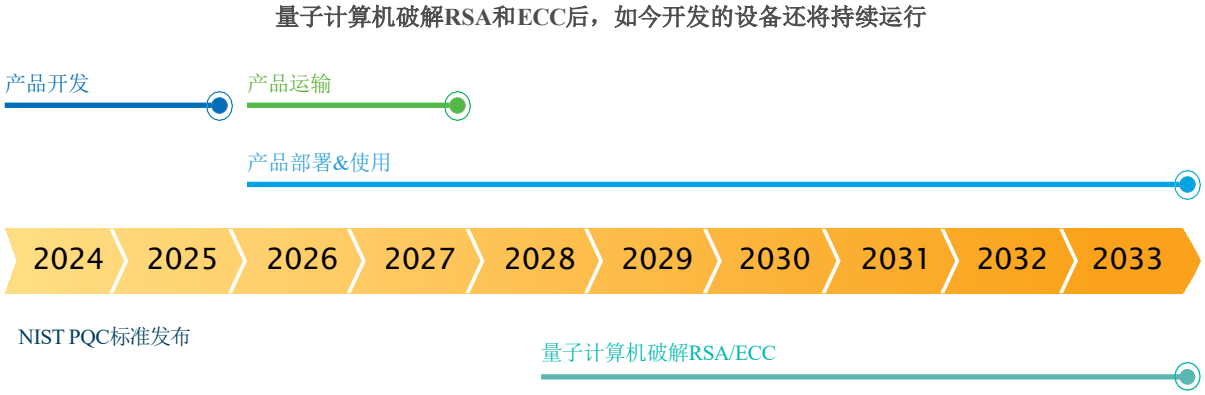
资料来源：美国国家安全局网络安全委员会，宣布商用国家安全算法套件2.00

2.4. 设备寿命和量子计算机开发时间表

如今设计的设备在未来15至20年内可能仍在使用，因此当下实施的安全措施必须能够抵御未来的量子威胁。预计在未来十年内，能够破解现有加密算法的量子计算机将投入实用，这对长期数据安全构成的威胁迫在眉睫。

汽车以及电网等关键基础设施中使用的设备，其使用寿命普遍长达15至20年，这意味着它们将在量子计算时代长期运行。这将带来一个危险的安全漏洞 ——当前部署的采用传统加密技术的系统，在其使用期限内会因量子攻击而变得脆弱。因此，必须在这些设备中**集成抗量子攻击密码技术**，以确保其在整个生命周期内的安全性。见图4。

图4：设备生命周期vs.量子计算机的发展



2.5. 量子计算机发展路线图

大多数专家认为，量子计算机能在未来十年内破解RSA和ECC加密。作为推动新型后量子加密算法研发与应用的核心机构之一，美国国家标准与技术研究院（NIST）预测这一时间最早可能出现在2030年[4]。全球风险研究所的《量子威胁时间线报告》指出：实现大规模量子计算不存在已知的根本性障碍，因此网络风险管理者应考虑这一情况“何时发生”而非“是否发生”[5]。

研究人员和领先的科技企业正大力投入量子计算技术，推动量子计算取得重大进展。例如，谷歌于2024年12月推出了105量子比特的量子计算机，并计划在2030年前实现100万量子比特的突破。IBM、D-Wave、Rigetti和富士通等企业已开发出商用化量子计算机，并在系统性能提升方面取得快速进展。

3. 全球PQC相关举措

各国政府和国际标准机构正在制定指导方针与法规，明确后量子密码（PQC）算法的技术要求和采用时间表。这些标准既规定了需使用的PQC算法，也划定了算法落地的时间节点。美国国家标准与技术研究院（NIST）的后量子加密标准为全球相关算法的应用奠定了基础——即使是考虑采用NIST标准以外算法的国家，也在很大程度上受其影响。具体实践中，法国和德国等国家选择同时采用NIST指定的算法，以及部分NIST曾评估但未最终标准化的算法；而中国等国家则在探索研发国家专用算法。见图5。

图5：全球各国采取的PQC举措

国家/地区	正在考量的PQC算法	已发布的指南	采纳时间线
澳大利亚	NIST算法	CTPCO (2023)	开始实施 (2025/2026)
加拿大	NIST算法	Cyber Centre (2021)	开始实施 (2025)
中国	中国特有算法	CACR (2020)	开始规划 (2025)
欧盟	NIST算法	ENISA (2022), 欧盟委员会 (2024)	现在开始规划和实施 (2025)
法国	NIST、FrodoKEM、LMS、XMSS	ANSSI (2023)	开始实施 (2025)
德国	NIST算法、LMS、XMSS, FrodoKEM、ClassicMcEliece-KEM	BSI (2022)	开始实施 (2025)
日本	Monitoring NIST	CRYPTREC (2022, 2024)	开始规划 (2025)
荷兰	AES、NIST、SHA-DSA-256、XMSS	NCSC (2023)	目前的行动计划草案有明确的时间框架（关于时间框架没有硬性规定）。
新西兰	NIST算法	NZISM (2022)	开始规划 (2025)
新加坡	Monitoring NIST	MCI (2022), 新加坡金融管理局 (2024)	开始规划 (2025)
韩国	KpqC	MSIT (2024)	2024年选择更多韩国特有的算法
英国	NIST算法、LMS、XMSS	NCSC (2023)	开始实施 (2025)
美国	NIST算法、LMS、XMSS	CISA (2021, 2022, 2023) NIST (2023) NSA (2022, 2024) 白宫 (2022, 2024) 议会 (2022)	现在开始实施 (2025); 要求从2025年开始实施

4. 哪些算法会受到量子计算机的影响

了解哪些算法容易受到攻击是确保系统安全的第一步。量子计算机会破解现有的非对称加密算法，如RSA和ECC。增加算法的密钥长度并不能有效抵御量子攻击。必须按照NIST的定义和各监管机构的要求，用抗量子算法替换这些算法。见图6。

AES等对称加密算法也会受到影响，但程度较轻。在这里，将所有对称加密算法升级到AES 256将提供抗量子攻击能力。已获批准的算法根据所使用的底层数学进行分类。

基于格的算法：ML-KEM（Kyber）、ML-DSA（Dilithium）和FN-DSA（Falcon）基于复杂格结构提供安全性，这些结构会给量子计算机的计算带来很大挑战。

基于哈希的签名：LMS（Leighton-Micali Signature）、XMSS（eXtended Merkle Signature Scheme）和SLH-DSA（SPHINCS+）都是基于哈希值的签名方案，以安全著称。

图6：受量子计算机影响的算法

加密功能	经典算法	后量子状态	后量子替代
随机数生成	TRNGs	量子安全	无需替代
对称加密	AES-128、AES-256	AES-256是量子安全的 AES-128易受量子攻击	需要AES-256
加密哈希	SHA2、SHA3	需要更大的输出	需要SHA2-384/512或 SHA3-384/512
密钥交换	RSA、Diffie-Hellman、ECDH	不安全	ML-KEM (Kyber)
数字签名	RSA、ECDSA	不安全	ML-DSA (Dilithium) SLH-DSA (SPHINCS+) FN-DSA (Falcon) LMS、XMSS (仅代码签名)

5. PQC算法和NIST标准

2024年8月13日，美国国家标准与技术研究院（NIST）敲定了第一套后量子加密标准，标志着网络安全领域的一个重要里程碑。

NIST标准为全球PQC算法的迁移奠定了基础。这些标准由全球安全研究人员和公司的合作制定，目前正在被世界各国采用。大多数国家直接采用NIST标准。少数国家采用本国的特有算法，但这些算法都源自NIST标准。还有一些国家在采用NIST算法的同时，也接受了一些其他算法。这些算法是NIST标准化进程中的入围算法，未被NIST选为标准化算法。

在2024年8月发布的版本中，NIST批准了四种旨在确保数字通信安全的算法。这些算法包括:

- ML-KEM (CRYSTALS-Kyber)
- ML-DSA (CRYSTALS-Dilithium)
- SLH-DSA (SPHINCS+)
- FN-DSA (Falcon)

实施与过渡：这些算法旨在立即集成到数字系统中，以抵御量子攻击，增强安全性。NIST提供了实施这些算法的详细指南，目的是在不影响当前操作标准的情况下实现平稳过渡。

未来考虑：NIST未来将继续评估更多标准化算法。将对更多算法进行标准化，进一步增强加密防御的稳健性，并提供针对各种用例进行优化的算法。

过渡到新算法是一项重大工程，会影响PKI系统、TLS和VPN协议、加密库、HSM、TPM以及其他许多系统。在整个生态系统和供应链中推广这些新算法需要数年时间。公司需要立即采取行动，向PQC迁移。莱迪思半导体提供专业技术和解决方案，带来无缝、高效的迁移体验。

6. 迁移到PQC算法

PQC算法现已标准化，开发人员可以开始迁移到这些新的、经NIST批准的算法。利用莱迪思先进的FPGA技术，您可以实现无缝和面向未来的迁移，确保您的系统始终受到最新加密标准的保护。参见图7。

图7. 迁移到PQC算法

算法	CNSA 2.0套件算法	NIST标准化情况	类型	目的	替代算法
LMS	是	是	基于哈希的状态签名	代码和固件签名	ECDSA, RSA
XMSS	是	是	基于哈希的状态签名	代码和固件签名	ECDSA, RSA
ML-DSA (Dilithium)	是	是	基于格	所有的数字签名使用案例	ECDSA, RSA
ML-KEM (Kyber)	是	是	基于格	密钥交换和加密	ECDH, RSA, Diffie-Helman
SLH-DSA (SPHINCS+)	否	是	基于哈希的无状态	所有的数字签名使用案例	ECDSA, RSA
FN-DSA (Falcon)	否	否	基于格	所有的数字签名使用案例	ECDSA, RSA

LMS和XMSS都是基于哈希的状态数字签名算法，这意味着私钥包括了一个必须保持的状态值。每次生成签名时，都必须更新状态值。这些算法非常适合代码签名用例。标准要求在HSM中执行签名操作和状态管理，以确保安全性和正确的状态管理。因此，这些算法实际上只适用于代码签名，并不适合用作通用数字签名算法。

ML-DSA（Dilithium）和ML-KEM（Kyber）都是基于格的算法，已被NIST全面标准化，并通过CNSA 2.0认证。ML-DSA是一种通用数字签名算法，可用于所有用例，包括代码签名。ML-KEM是一种密钥交换机制，将被TLS和IPSec等协议用于交换AES密钥。

SLH-DSA（SPHINCS+）是一种无状态哈希数字签名算法。该算法已被NIST完全标准化，可用于所有数字签名用例。然而，它并非CNSA 2.0批准的算法。此外，SLH-DSA的性能也比其他后量子数字签名算法更差[6]。尽管有一些适用场景，但它不适用于对性能要求严苛的应用。

FN-DSA（Falcon）已被NIST选为标准化项目，但FN-DSA标准预计要到2025年才能完成。

6.1. 实施PQC算法的挑战

实施PQC算法并非没有挑战。企业在采用新算法时会面临学习曲线。PQC算法的密钥大小、签名大小和性能特征与传统算法有很大不同。不同PQC算法之间也存在很大差异。

组织必须熟悉这些新算法，以便理解不同算法之间的权衡。例如，ML-DSA和LMS这两种算法的签名验证速度都非常快，而且签名尺寸都相对较大。但它们在其他方面存在显著差异。例如，LMS的公钥尺寸非常小，而ML-DSA的公钥尺寸则相对较大。

组织应该选择像莱迪思半导体这样在后量子加密算法（PQC）领域具备经验与专业知识的可信合作伙伴，并着手实施概念验证（POC）解决方案，以积累必要的知识，推动其设备与系统向后量子加密算法迁移。

莱迪思半导体提供的产品已将后量子加密算法集成至器件上的加密引擎中，帮助客户快速、便捷地升级解决方案以支持后量子加密技术。针对正在实施概念验证的客户，公司还提供开发板，助力其加速向后量子加密技术的迁移进程。

7. 在主要应用案例中实现量子抗性

7.1. 传输层安全（TLS）与安全通信

TLS和其他安全通信协议利用三种不同的加密操作来确保数据安全：

- **身份验证**：用ML-DSA、SLH-DSA或FN-DSA代替RSA/ECDSA
- **密钥交换**：ML-KEM代替RSA、ECDH或Diffie-Helman
- **批量数据加密**：AES-128或AES-256，确保使用AES-256

对于需防范HNDL攻击的应用场景，企业应优先在通信协议中部署Kyber（ML-KEM）。采用ML-KEM可确保会话密钥无法被量子计算机破解，从而使HNDL攻击失效。

7.2. 代码签名

LMS、XMSS和ML-DSA可用于代码签名。

7.3. 可信根

可信根（RoT）解决方案将在设备上执行签名操作，以实现对配置数据的验证，以及对更广泛系统中其他组件的校验。ML-DSA是可信根应用场景的最佳算法，因其支持在设备端进行签名。

7.4. 对加密敏捷的需求

后量子加密技术的发展仍处于起步阶段。随着该领域的不断演进，加密解决方案保持高度灵活性以适应新标准和新发现至关重要。这种对“加密敏捷性”的需求之所以必要，是因为它使系统能够迅速整合加密领域的进步，无需进行大规模改造，从而确保持续抵御新出现的量子威胁。

8. 莱迪思半导体：您可靠的PQC合作伙伴

现场可编程门阵列（FPGA）在现代应用中扮演关键角色，而莱迪思半导体凭借能够抵御现有和新兴威胁的安全能力引领行业。我们的可信根（Root of Trust）解决方案可在器件加电启动直至整个运行周期内提供防护。

FPGA自身具备灵活性，支持重新编程以适配不断演进的标准。这种适应性确保了设备的长生命周期和成本效益，使其成为构建安全、面向未来解决方案的理想选择。莱迪思FPGA可用于“加密敏捷性”解决方案，这对向PQC标准过渡至关重要。借助莱迪思技术，您可以采用后量子加密算法无缝升级硬件，并修补现有系统中的安全漏洞。

莱迪思半导体已在后量子加密领域牢固确立了领军者地位，我们在先进FPGA平台上成功实现的概念验证即印证了这一点。依托值得信赖的可信根解决方案这一成熟传统，当我们的安全器件用于电源时序控制时，可提供不可绕过的强大安全防护。我们的后量子加密解决方案基于这些安全控制FPGA中的硬核安全算法构建，并具备分层的加密敏捷特性，能够随着标准的演进实现后量子加密算法的无缝现场升级。这确保您的系统始终安全且灵活适应，为抵御新兴的量子计算威胁提供长期保护。

此外，莱迪思半导体正在积极推出采用所有NIST批准和符合CNSA 2.0要求的PQC算法的解决方案。其中包括:

- **ML-KEM (CRYSTALS-Kyber)**：替代RSA、Diffie-Hellman和ECDH
- **ML-DSA (CRYSTALS-Dilithium)**：替代RSA和ECDSA
- **XMSS (eXtended Merkle Signature Scheme)**：经批准用于代码签名和验证的有状态哈希数字签名算法
- **LMS (Leighton-Micali Signature)**：另一种用于代码签名和验证的有状态哈希数字签名方案

我们的开发路线图严格遵循监管时间表，确保我们的客户能够在规定的截止日期之前达到或超越合规要求。通过将这些先进的标准化算法集成到我们的FPGA解决方案中，我们为企业提供了平稳过渡到抗量子加密的基本工具。选择莱迪思，即选择了一个致力于交付及时、合规且强大的安全技术的值得信赖的合作伙伴，为您的资产抵御当前及未来的量子威胁提供保障。

8.1. 降低过渡风险：莱迪思对混合加密策略的支持

除了我们先进的后量子加密产品，莱迪思半导体继续支持所有经典非对称算法，包括最高512位的椭圆曲线密码算法（ECC）和最高4096位的RSA算法，以及用于对称加密的AES-256算法。我们还全面支持SHA-2和SHA-3等密码哈希算法。这种广泛的算法支持使我们的客户能够在必要时实施混合加密流程。在向PQC标准过渡期间，实施结合经典算法与抗量子算法的混合流程是一种明智的策略。该策略确保与现有系统和协议的向后兼容性及互操作性，同时采用新的抗量子安全算法。它提供了额外的安全性，使组织能够降低因立即全面改造其加密基础设施而带来的风险。

莱迪思半导体通过同时支持经典算法与PQC算法（包括关键哈希函数），帮助客户根据自身运营需求和监管时间表，平稳、安全地过渡到抗量子加密体系。

莱迪思注重PQC和经典加密算法的稳定性和可靠性。我们将来自行业顶尖IP供应商的软硬件算法融入解决方案。这些供应商在加密技术领域的卓越表现广受认可，其算法通过了NIST的严格验证，并在客户系统级环境中接受了全面渗透测试，确保在实际应用场景中具备足够的安全性和抗攻击能力。

我们与这些受信任的IP供应商保持紧密合作，他们正积极为算法申请更多认证，这进一步提升了我们安全产品的可信度。这种严谨的态度不仅证明了莱迪思加密解决方案的强度，也有助于客户实现自身的合规目标。通过集成经过认证和充分测试的加密算法，企业可以放心地保护其系统，并可能更轻松地获得高级安全认证。对于那些追求系统级FIPS 140-3 Level 2等认证的客户而言，这种技术支持为满足严格的监管标准提供了坚实基础。

9. 结论

美国国家标准与技术研究院（NIST）完成后量子密码学标准的制定，标志着数字安全领域的关键转折点。量子计算的进步已不再是遥远的可能性，而是迫在眉睫的现实，传统密码系统的大厦将倾。全球组织必须紧急升级其加密基础设施，以符合这些新标准。行动刻不容缓。

从RSA和ECC等经典加密算法迁移到抗量子替代方案是一项需持续数年的重大任务。企业在规划这一过渡时，拥抱“加密敏捷性”—— 即随着PQC的发展快速适应新算法的能力 —— 变得至关重要。现场可编程门阵列（FPGA）因其固有的灵活性和可重配置性，将发挥关键作用。

与固定功能硬件不同，FPGA允许快速更新以实施最新密码标准，确保安全系统在量子计算的快速发展中保持未定且有能力面对未来的威胁。

莱迪思半导体已准备好支持组织度过这一变革期。凭借在后量子加密领域的成熟专业知识和值得信赖的安全解决方案，莱迪思提供先进的FPGA技术，实现向抗量子加密的无缝迁移。通过支持NIST批准的后量子加密算法和经典加密方法（包括 ECC、RSA、AES-256以及SHA-2和SHA-3等哈希算法），莱迪思能帮助客户实施混合加密流程。这种方法在采用新的抗量子安全算法的同时，促进与现有系统的向后兼容性和互操作性，降低因全面改造基础设施而带来的风险。主动采用抗量子标准，辅以莱迪思FPGA等适应性技术，对于在后量子时代维护数字基础设施的完整性和安全性至关重要。通过集成经过认证和充分测试的加密算法，组织可以自信地保护其系统并实现合规目标。

现在是保障数字未来的关键时刻。向弹性加密措施的转变将保护敏感信息和系统免受日益增长的量子威胁和HNDL攻击，在我们日益数字化的世界中增强信任和安全性。各组织应迅速采取行动，采用后量子加密解决方案，并与值得信赖的领导者合作，确保其关键数据和基础设施受到保护。

10. 参考资料

1. Shor, W (1995) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. https://arxiv.org/abs/quant-ph/9508027
2. Quantum Supremacy is the ability to perform calculations that are too difficult for a classical computer to perform in a reasonable amount of time, for narrowly defined tasks. https://www.nature.com/articles/s41586-019-1666-5
3. Announcing the commercial national security algorithms ... National Security Agency. (2022). https://media.defense. gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
4. Chen, L., Jordan, S., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D., & Liu, Y.-K. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf
5. Mosca, Michele, Piani Marco (2024). Quantum Threat Timeline Report 2023, Global Risk Institute. https://globalriskinstitute.org/ publication/2023-quantum-threat-timeline-report/
6. Westerbaan, B., Meunier, T., Rubin, C. D., Faz-Hernández, A., Tholoniat, P., Kozlov, D., & Wang, M. (2024, July 29). NIST's Pleasant Post-quantum surprise. The Cloudflare Blog. https://blog.cloudflare.com/nist-post-quantum-surprise

11. 附录

XMSS、LMS和NIST PQC标准

2024年8月13日，美国国家标准与技术研究院（NIST）最终确定了第一套后量子加密（PQC）标准。被标准化的算法包括：

- ML-KEM (CRYSTALS-Kyber)
- ML-DSA (CRYSTALS-Dilithum)
- SLH-DSA (SPHINCS+)
- FN-DSA (Falcon)

这是NIST首次标准化的通用PQC算法，但在它们之前，NIST已于2020年10月29日发布了LMS和XMSS这两种状态哈希签名方案的标准。

NIST将XMS和LMS算法描述为“.....可安全对抗量子计算机的发展，但不适合广泛使用，因为它们的安全性取决于谨慎的状态管理。它们最适合私钥使用可被严格控制的应用.....”。

这使得XMS和LMS非常适合用于代码签名/代码验证场景，如安全启动和安全软件更新，但不适用于大多数其他场景。对于代码签名，私钥及相关的状态管理可由具备状态管理能力的硬件安全模块（HSM）执行。

PQC算法家族

后量子加密采用与RSA和ECC不同的数学方法来创建算法，这些算法可在传统计算机上运行，且不受量子计算机或传统计算机攻击的威胁。

NIST在标准化过程中考虑了利用多种不同数学方法的算法，具体类型包括：

- 基于代码的（经典McEliece）
- 基于格的（CRYSTALS-KYBER、NTRU、SABER、CRYSTALS-DILITHIUM、Falcon）
- 基于同源的（SIKE）
- 多变量的（Rainbow）
- 零知识的（Picnic）
- 基于哈希（SPHINCS+）
- 有状态哈希（XMSS、LMS）（虽不在NIST本轮标准化流程中，但此前NIST已发布标准）

每种算法类型均通过不同数学方法实现安全性，确保在合理时间内无法被经典或量子计算机破解。NIST选择对基于格、基于哈希和有状态哈希的算法进行标准化。

基于格的算法：ML-KEM（Kyber）、ML-DSA（Dilithium）和FN-DSA（Falcon）基于复杂格结构提供安全性，这类结构对量子计算机而言具有极高计算难度。基于格的加密技术因其假定对量子和经典计算机均具备安全性，且运算效率高而备受青睐。最短向量问题（SVP）和最近向量问题（CVP）是基于格的数学问题，构成了格基方法安全性的基础。

有状态哈希签名：LMS和XMSS属于有状态哈希签名方案，以简单性和安全性著称。顾名思义，这些方案依赖SHA2或SHA3等哈希函数实现安全。其「有状态」特性意味着私钥包含必须维护的状态值 —— 每次生成签名时，状态值必须更新。这类算法非常适合代码签名场景（如安全启动、软件更新验证），但标准要求签名操作和状态管理需在硬件安全模块（HSM）内执行，以确保安全和正确的状态维护。因此，它们仅适用于代码签名，不适用于通用数字签名场景。

基于哈希的签名：SPHINCS+（SLH-DSA）是无状态的哈希签名方案。与LMS、XMSS一样，其安全性依赖SHA2或SHA3等哈希函数，但由于无需维护状态值，私钥中不包含需持续更新的状态参数。这一特性消除了状态值维护需求，使该算法适用于**通用签名场景。**

对HNDL攻击的解释

HNDL攻击会存储整个通信会话的所有数据包，包括密钥交换操作。然后，这些攻击将使用量子计算机尝试破解密钥交换操作中使用的加密。如果成功，攻击将恢复会话密钥（AES密钥），然后可用于解密通信会话期间传输的数据。

换句话说，即使AES-256是量子安全的，但在TLS中使用它并不足以确保该协议是量子安全的。量子计算机将破解用于交换会话密钥（AES密钥）的非对称加密（RSA、ECDH或Diffie-Helman）。一旦非对称加密被破解，就可以获得AES密钥，并且可以解密用AES加密的数据。

为了防范HNDL攻击，通信协议必须使用ML-KEM，这是目前唯一用于密钥交换操作的标准化后量子加密算法。

准备好了解更多信息了吗？

欲了解更多有关基于莱迪思低功耗FPGA解决方案如何应用于工业、汽车、通信、计算和消费市场，请访问www.latticesemi.com或通过www.latticesemi.com/contact或www.latticesemi.com/buy与我们联系。

技术支持

通过www.latticesemi.com/techsupport提交技术支持案例。有关常见问题，请参阅莱迪思答案数据库www.latticesemi.com/Support/AnswerDatabase。

V.2 WP0041