筑牢未来之信：

依托莱迪思 RoT FPGA 与完整 CNSA 2.0，

为数字系统构建可信根基

作者：
Ramya Chandrasekaran，高级产品营销经理，莱迪思半导体公司
Temoc Chavez Corona，安全架构工程师，莱迪思半导体公司

免责声明

莱迪思不对本文档所含信息的准确性或其产品用于任何特定用途的适用性作出任何担保或保证。本文件中的所有信息均按原样提供，不保证无任何纰漏，所有相关风险完全由买方承担。此处提供的信息仅供参考，可能包含技术上的不准确或遗漏，也可能因多种原因而变得不准确，莱迪思不承担更新或以其它方式更正或修订这些信息的义务。莱迪思销售的产品已经过有限的测试，买方有责任独立确定其产品的适用性，并进行测试和验证。莱迪思产品和服务的设计、制造或测试并非用于生命或安全关键系统、危险环境或任何其他要求故障安全（fail-safe）性能的环境，包括产品或服务故障可能导致死亡、人身伤害、严重财产损失或环境损害的任何应用（统称“高风险用途”）。此外，买方必须采取谨慎的措施来防止产品和服务故障，包括提供适当的冗余、故障安全功能和/或关闭机制。莱迪思声明不对产品或服务在高风险用途中的适用性作出任何明示或暗示的保证。本文档中提供的信息为莱迪思半导体所有，莱迪思保留随时更改本文档信息或任何产品的权利，恕不另行通知。

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。

目录

引言

随着数据泄露事件激增和攻击者手段日益精进，量子计算的兴起带来了新的紧迫性——它使攻击者能够利用窃取加密数据并在未来将其解密，从而威胁所有数字系统的长期可信度。为此，各国政府和行业正加速制定法规，并采用《商业国家安全算法套件2.0》（CNSA 2.0）和美国国家标准与技术研究院（NIST）的 FIPS 203/204 等后量子加密（PQC）标准保护关键基础设施和确保合规性。如今，数字系统依靠加密敏捷性和基于硬件的可信根应对不断进化的威胁，其可信度也取决于此。本白皮书将介绍为何采用 PQC 刻不容缓、各国及行业如何应对以及莱迪思半导体公司支持 PQC（后量子加密）的 RoT（可信根） FPGA 如何帮助组织在量子计算时代保障其未来安全。

为何采用后量子加密（PQC）刻不容缓

后量子安全基础必须建立在可信硬件之上，莱迪思的 RoT FPGA 提供了这样的安全基础。凭借独特的设计，莱迪思的 RoT FPGA 可执行后量子算法并具有业界最完整的 CNSA 2.0 算法覆盖，支持包括 ML-KEM、ML-DSA、LMS 和 XMSS 在内的所有强制性标准。这使客户不仅具备了保障未来安全的保障能力，而且能够满足美国国家安全局（NSA）等机构设定的合规期限。

不同于传统微控制器或通用硬件安全模块，莱迪思的 RoT FPGA 结合了以下特性：

- 全面符合 CNSA 2.0：支持所有获批的后量子加密（PQC）算法
- 硬件强制的 RoT 机制：保障启动链安全、保护固件并消除拒绝服务的风险
- 加密敏捷性：支持经典、混合及 PQC 算法间的无缝迁移
- 高效性能：安全启动速度提升高达 10 倍，功耗较竞品降低了 50%-75%
- 这使莱迪思的 RoT FPGA 成为当下部署 PQC 技术的实用基础平台。

刻不容缓的真正原因

关于大规模量子计算机何时问世的争论仍在持续，但关于“先收集，后解密”（HNDL）式攻击风险已迫在眉睫这一点已无争议。攻击者正在不断收集加密通信、财务记录、医疗数据及机密信息，计划等到量子技术成熟后再进行解密。

这是各国政府加速采取行动的真正原因。NSA 的 CNSA 2.0 要求到 2025 年在软件和固件签名中采用 PQC 技术，到 2027 年实现全面普及。欧盟及其他地区也制定了同样紧迫的时间表。转型窗口所剩无几，延迟转型的企业将面临敏感数据在未来遭到泄露的风险。

显然，PQC 已不是未来的问题，而是当下要务。依托莱迪思的 RoT FPGA 构建安全基石，企业可以部署符合 CNSA 2.0 的解决方案，为今日产生当下创建的数据筑起抵御明日量子威胁的防护墙。

解析“先收集，后解密”式攻击

尽管对称分组加密方案一般被认为能够抵御量子攻击，但用于交换或建立共享密钥的协议往往依赖易受量子威胁的非对称加密技术。“先收集，后解密”（HNDL）式攻击

指攻击者（通常是国家行为体或高级网络犯罪分子）截获并存储当前加密数据，待量子计算能力成熟后再行解密。

该攻击手段的危险性在于，其瞄准的是具有长期战略价值或个人价值的敏感数据，例如医疗记录、金融协议、知识产权、机密通信信息等，这些数据往往具有数十年的保存价值。不同于具有即时威胁的传统攻击，HNDL 产生的是长期威胁。被窃取的数据始终处于加密状态，表面看似安全，使企业产生虚假的安全感。

为降低此风险，组织必须着手规划向量子抗性密钥交换机制（如 ML-KEM（FIPS 203)）过渡，尤其是针对最敏感的通信。尽早采用 PQS 标准对保障当前加密的数据在未来的安全性至关重要。

量子计算领域的进展

2025 年，量子计算在软硬件领域均取得重大突破。谷歌的 105 量子位 Willow 芯片将错误率降低了几个数量级，仅用数分钟便完成经典超级计算机需耗时万亿年的基准测试任务；微软推出首个基于拓扑量子位的量子处理器 Majorana 1，为构建容错量子系统开辟了扩展路径；NVIDIA 与 Quantum Circuits 通过将 CUDA-Q 集成至 Aqumen 推进混合量子-经典计算技术的发展；亚马逊与 NVIDIA 联合推出了 DGX Quantum，该平台结合了 AI 超级芯片与量子控制系统，支持实时性错误纠正以及可扩展的量子工作负载。

根据当前进展，首台实用后量子计算机（指能破解 RSA-2048 等主流加密系统的设备）预计将在 2030 至 2035 年间问世，具体时间取决于技术进步与实现条件。届时，任何长度的经典公钥加密方案都将面临风险。

行业与监管机构的应对之策

全球网络安全行业正积极应对量子计算迫在眉睫的威胁。各国政府及企业正加速采用 PQC 防范未来量子攻击对敏感数据的威胁。例如 NIST 发布了 NIST SP 800-208 建议，推荐两种基于哈希的状态化签名方案：Xtended Merkle Signature Scheme（XMSS）和 Leighton-Micali Signature（LMS）。该机构还正式确立了首套 PQC 标准，包括 FIPS 203 基于模块-格的密钥封装机制（ML-KEM）和 FIPS 204 基于模块-格的数字签名（ML-DSA）等算法标准。

欧盟已启动协调路线图，计划到 2030 年通过量子抗性加密保障关键基础设施的安全。

NSA 发布的 CNSA 2.0 是对国家安全系统（NSS）加密标准的全面更新。该标准强制要求向量子抗性算法过渡，用基于格和哈希的替代方案取代 RSA 和 ECC 等易受攻击的方案。

该文件明确了转型时间表：到 2025 年，软件和固件签名须开始采用 CNSA 2.0 算法，到 2027 年在 NSS 系统全面推广。预计到 2035 年所有 NSS 技术将实现全面合规，因此对于处理敏感或机密数据的组织而言，提前规划与实施至关重要。

莱迪思提供怎样的解决方案

莱迪思的 RoT FPGA 提供的功能包括安全启动、低功耗运行、防篡改保护、位流与数据安全、实时固件防护及端到端 IP 保护——所有这些功能均基于不可篡改的硬件安全功能。目前这些基础功能均已推出，而 PQC 构建于此坚实基础之上，能够更好地抵御新兴威胁。

莱迪思 PQC FPGA 器件通过提供广泛的支持算法套件满足 PQC 技术发展需求，涵盖基于格的加密（ML-DSA 和 ML-KEM）及基于哈希的签名（LMS/XMSS）等，可适应多元市场需求与应用场景。

鉴于加密技术发展的动态性，这些器件以加密敏捷性为核心设计目标，可快速适应新兴协议与技术改进。

为简化向后量子标准的过渡，莱迪思器件支持混合加密模型，通过实现经典算法与抗量子算法的并存增强安全保障。

此外，这些器件经过精心设计，可与量子随机数生成器（QRNG）等新兴量子技术组合成更加强大、与时俱进的安全解决方案。

经典 + PQC 密钥层次结构

在公钥签名方案中，私钥的保密性是安全性的基础。但多年来反复发生的密钥泄露事件表明，密钥外泄是真实且持久的威胁，因此必须建立后备机制。

为此，设备必须支持多个有效公钥，以实现安全的密钥轮换和遭泄露凭证的快速撤销。

莱迪思 PQC 器件通过强大的密钥分层架构实现了该功能，支持多个有效公钥同时并存。

配置的密钥可混合采用 ML-DSA、XMSS 或 LMS 等后量子方案及经典算法，为系统设计者带来了高度灵活性。

密钥一经配置，即可根据请求进行启用、延长或撤销，从而支持密钥的良性轮转与稳固的生命周期管理。

这一架构能够确保在那些将弹性与敏捷性置于首位的环境中，实现可扩展、安全且能否灵活适应的密码运算。

采用 PQC 方案的位流认证与用户数据签名

LMS 和 XMSS 是 IETF 提出的基于哈希的数字签名算法，而由 NIST 标准化的 ML-DSA（FIPS 204）被 CNSA 2.0 认定为有效的 PQC 选项。

莱迪思 PQC 器件系列中，CNSA 2.0 算法已支持用于位流认证。该认证功能是这类设备的核心安全特性。

客户可在硬件安全模块（HSM）生态系统中使用其 LMS、XMSS 或 ML-DSA 私钥对位流映像进行签名。该映像在设备中通过预先配置的对应公钥进行编程时将被验证。

客户还可使用 ML-DSA 对莱迪思 FPGA 器件上的用户数据进行签名，确保敏感信息除位流认证外还能获得后量子数字签名保护。

采用 ML-KEM 的安全信道——防范“先收集，后解密”式攻击

如前文所述，量子计算带来的最大威胁之一是“先收集，后解密”（HNDL）式攻击，即窃取并长期存储加密数据，待量子计算机性能足以破解经典加密方案时再行解密。

传统 Nexus 器件虽支持创建采用 RSA 或 ECDH 的安全信道，但这些方法易受 HNDL 攻击。

为此，莱迪思 PQC 器件采用基于硬件的 ML-KEM 实现抗量子密钥封装。

这些器件支持整个 ML-KEM 套件，通过两种方式实现安全通信：使用第三方公钥封装共享密钥，或发起密钥交换并解封由其他可信代理生成的密钥。

共享密钥建立后，可立即通过板载 AES 引擎创建抵御未来量子攻击的安全信道。

此外，莱迪思 PQC 器件支持（符合 CNSA2.0 要求）所有 ML-KEM 安全等级，包括 ML-KEM-512、ML-KEM-768 和 ML-KEM-1024，使用户可根据具体应用需求定制安全级别与性能。

支持 ML-DSA/ML-KEM 的 SPDM

由分布式管理任务组（DMTF）制定的安全协议与数据模型（SPDM）规范是一项标准化协议，专门用于实现跨平台及传输层的安全通信、设备身份验证及认证，从而构建零信任安全环境。

SPDM 促进了组件间的加密和验证通信，其功能类似于 TLS 1.3.，但针对嵌入式和固件级环境进行了优化。

该模型支持相互身份验证、密钥交换和会话保密性，非常适合芯片到芯片和设备到主机的交互。

SPDM 的核心功能是能通过固件认证等机制核验硬件组件的身份与完整性，设备可向验证方提供其固件状态的加密证明。

随着 SPDM 1.4 的发布，该协议现已支持 ML-KEM 和 ML-DSA 等 PQC 算法，为抵御未来的量子威胁提供了保障。

莱迪思 PQC 器件全面支持 SPDM 兼容系统，提供了必要的密码学原语（包括 ML-KEM、ML-DSA、AES-GCM）及 MCTP 传输支持，实现了所有平台组件的安全集成。

莱迪思器件中的 DICE

设备标识符组合引擎（DICE）是由可信计算组（TCG）制定的安全规范，用于为资源受限设备建立具有强加密特性且不可篡改的身份标识。

在莱迪思器件中，通过将加载的位流、其配置信息及固有硬件密钥进行密码学组合，生成称为“复合设备标识符”（CDI）的唯一标识。该 CDI 反映设备当前状态，并作为生成唯一非对称密钥对的基础。

当该密钥对在制造过程中获得莱迪思证书颁发机构的认证时，即可生成设备专属证书。这些 DICE 证书可与 SPDM 协同使用，在零信任环境中建立设备间安全通信。设备可通过莱迪思器件正品追溯签名凭证共享配置数据。

此外，系统设计者可使用莱迪思 PQC 器件的功能，将认证基础设施的安全性提升至能够抵御量子攻击的新高度。

莱迪思 PQC 器件的平台固件弹性（PFR）

平台固件弹性（PFR）是专为保护关键平台固件（例如 BIOS、引导加载程序及其他底层系统组件）而设计的安全框架，可抵御网络威胁、未经授权的修改及运行故障。

莱迪思 PQC 器件率先实现了基于 NIST 特别出版物 800-193 指南的 PFR 解决方案，并结合了 CNSA 2.0 定义的高级加密技术。

随着 PQC 算法的持续开发，融合经典与抗量子方法的混合方案为未来发展提供了切实可行的安全路径。这种模型在保持成熟算法可靠性的同时，实现了 PQC 的实际应用测试，从而增强了可信度并促进了该技术的普及。

莱迪思 PQC 器件可以很好地支持该混合 PFR 模型。这些器件可结合 ECDSA 等经典算法与 ML-DSA、LMS、XMSS 等抗量子算法进行固件身份验证，并结合 ML-DSA/ML-KEM 与 ECDSA 和 AES-GCM 用于认证和安全信道服务。

这种分层加密策略能够保证当某一算法因量子技术突破或未知漏洞而失效时，其余算法仍能持续提供保护。这种冗余设计大幅增强了整体系统弹性。

使用 PQC 技术保证制造安全

本文档阐述的多数安全功能，均依赖于器件制造阶段预置的敏感数据。这些数据可能包含用于认证运行时密钥的密码密钥、配置文件、策略设置或 X.509 证书。

但制造过程在安全评估中常被忽视，导致这一关键阶段面临潜在威胁。

而莱迪思 PQC 器件在受保护的测试设施中，通过“最后一英寸安全”配置协议启动其生命周期。其制造过程采用的硬件安全模块（HSM）均以后量子密码技术（如 ML-DSA 与 ML-KEM 的组合方案）进行强化，这为敏感配置数据构筑了一道安全传输并能抵御量子级别攻击的坚固防线。

结论

量子计算带来的威胁已不再是理论层面的推演，而是真实存在且迫在眉睫的挑战，尤其是能够利用当前加密技术漏洞的“先收集，后解密”式攻击。

为应对这一威胁，全球政府与组织正积极推动从经典公钥密码学向后量子公钥密码学的转型，以保护数字基础设施的安全。

莱迪思的 PQC 器件恰逢其时地提供了有效的解决方案，满足了不断演进的安全需求。这些器件凭借对大量密码算法的支持及内置的密码敏捷性，能够很好地适应 PQC 的未来发展。

此外，FPGA 固有的灵活性使其能够集成 PFR 和 SPDM 等高级安全服务，进而使用现有密码原语构建能够抵御量子时代威胁的弹性架构。

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 或者 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。