信息安全导论作业四

Project Leap

量子攻击下的安全金融系统

学　　生：XXX，XXX

学　　号：2021XXXX，2021XXXX

指导教师：XXX

助理指导教师：XXX

专　　业：软件工程

重庆大学大数据与软件学院

2023 年 12 月

BIS Innovation Hub

Project Leap

量子攻击下的安全金融系统

2023 6月

BANQUE DE FRANCE EUROSYSTÈME

DEUTSCHE BUNDESBANK EUROSYSTEM

执行摘要

量子计算机对金融系统构成了严重威胁。如果它们变得可行，它们可能会用于破坏当前主流的加密协议，这些协议是金融系统用来保护数据和交易安全的关键依赖项。在 20 世纪 90 年代中期，研究人员创建了量子算法，这些算法至少在理论上和在有足够强大的量子计算机的情况下，可以破解当今广泛使用的公钥加密方案。这将立即使许多当前的加密技术过时，威胁到我们金融服务基础设施的基础，并严重影响金融稳定性。

虽然功能性量子计算机尚不可用，但安全威胁需要得到紧急解决。恶意行为者已经可以拦截和存储机密的、经典加密的数据，以便在量子计算机变得足够强大时进行解密。这意味着今天存储或传输的数据实际上面临着未来量子计算机的“现在收集，以后解密”的攻击。金融数据的长期敏感性意味着量子计算机的潜在未来存在有效地使今天的系统不安全。

Project Leap 的目标是帮助金融系统应对这一威胁。实现量子安全的加密协议已经是可行的。然而，在金融系统中实现它们会带来许多挑战。具体而言，遗留系统中缺乏灵活性意味着需要进行重大的过渡工作。Project Leap 解决了实现金融系统量子安全 IT 环境的一些具体挑战，旨在为这一过渡做好准备并加速过渡。

BIS 创新中心欧洲系统中心、法国银行和德国联邦银行的这项联合实验旨在从央行流程开始，为金融系统创建量子安全的 IT 环境。Project Leap 的第一阶段探索了将后量子加密协议应用于中央银行使用案例（如支付）的实现。创建了一个量子安全环境，以保护基础设施免受数据在传输过程中的拦截。这种解决方案可以保护高度敏感的通信。该项目的两个关键目标是量子安全金融系统和提高央行社区的意识，旨在为金融系统的量子之旅提供有价值的见解。

Project Leap 的第一阶段解决的一个具体挑战是密码敏捷性，即在不影响应用程序的情况下在加密方案和算法之间切换的能力。由于新的量子抗性加密标准仍在讨论中，密码敏捷性在过渡到量子抗性加密中将是至关重要的。另一个重要发现涉及安全强度和性能之间的权衡。在后量子加密领域，安全性可能需要根据应用程序要求进行配置。这些和其他技术发现在第 6 章中总结。

Project Leap 的第一阶段在金融系统环境中成功建立了一个量子安全环境。由于这是在测试环境中实现的，因此需要更多的工作来探索复杂的现实环境。因

此，计划了 Project Leap 的第二阶段，以研究更多的网络架构，测试不同类型的硬件，并包含其他通信层，以构建完整的信任链，以及包括其他央行流程。

目录

1 引言

量子计算已经成为一个重要的研究领域。自 20 世纪 90 年代初以来，关于量子计算的出版物数量显著增加（Scopus（2021）），仅 2020 年就有超过 48,000 篇出版物，表明了人们对这种快速发展的技术的兴趣。领先的科技公司以及初创公司一直在开发量子计算机，其量子比特数不断增加。在不久的将来，量子计算机可能能够显著超越今天的经典计算机在某些任务上的能力。

量子计算机的潜在能力可能对许多行业都是一个福音。这包括金融行业，量子

计算机可以支持金融服务中的人工智能应用或改进金融建模。例如，在银行业中，越来越多的人对使用量子算法加速蒙特卡罗模拟感兴趣。

由于今天的金融系统严重依赖于传统的加密安全协议来保护数据和通信，因此量子计算机可能会使金融系统面临新形式的网络攻击。事实上，一个完全功能的量子计算机将对当前广泛使用的加密算法产生重大影响。金融稳定委员会在其有关金融部门网络安全的报告中指出，网络攻击是金融系统的一种破坏性威胁。全球各地的监管机构和监管工作已经缓解了金融部门所遭受的网络风险。然而，对金融数据的恶意使用将对重要的金融服务产生破坏性影响，威胁安全和数据机密性，对金融稳定性产生破坏性影响（FSB（2017））。此外，在其最近的全球风险报告中，世界经济论坛将量子计算机的网络威胁列为主要的新兴全球技术风险之一（WEF（2022））。这种情况需要集体行动，包括开发能够保护金融服务 IT 系统的新加密标准。

虽然功能性量子计算机尚不可用，但安全威胁是即时的，需要紧急解决。恶意行为者已经可以拦截和存储机密的、经典加密的数据，以便在量子计算机变得足够强大时进行解密。这意味着今天存储或传输的数据实际上面临着未来量子计算机的“现在收集，以后解密”的攻击。金融数据的长期敏感性意味着量子计算机的潜在未来存在有效地使今天的系统不安全。

这种紧迫性在图 1 中得到了进一步说明，其中 Y 线显示了可能会出现可以破解当前加密算法的量子计算机的时间。相应地，X 表示完成过渡到量子抗性加密的时间。即使 X 早于 Y，以便过渡“及时”完成，这只能保护存储或传输之后的数据。所有今天存储或传输的数据实际上都面临着未来量子计算机所代表的威胁。

图1

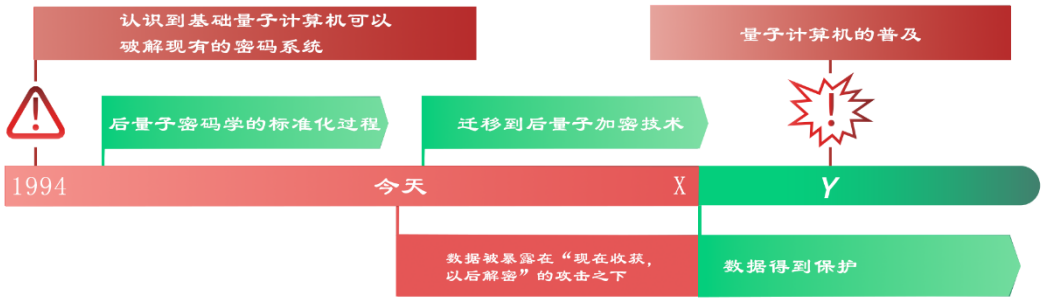


图 1

央行了解量子网络威胁的紧迫性以及迁移到量子抗性加密的复杂性至关重要。同时准备尽快实施新的加密协议也至关重要。Project Leap 旨在为这一过渡提供

见解，从而为成功迁移到量子抗性系统铺平道路。

2 量子解密技术对中央银行 IT 系统的威胁

2.1 量子计算产生解密威胁的原因

想要理解量子网络威胁，那么了解量子计算机的运作方式就至关重要。在传统的计算机系统中，信息被转换为一系列称为比特的二进制数字。每个比特只有一个可能的值，即 0 或 1。使用这种二维经典系统，计算机可以执行各种任务，并为整

个基于 Web 服务的经济体提供基础，包括金融服务。

量子计算机通过使用量子粒子来表示数据来处理信息，与经典计算机的运作方式非常不同（请参见附录 A 框 1）。量子计算机中的基本信息单元不是比特，而是量子比特，简称 qubit。像经典比特一样，qubit 可以具有 0 或 1 的值。与经典比特不同，qubit 还可以处于超位置状态，其值同时为 0 和 1。这种超位置状态使量子计算机在某些任务上比经典计算机具有更强大的处理能力。

在成功构建量子计算机方面仍然存在相当大的挑战。其中一个主要挑战是“噪声”。在计算过程中，量子计算机内外存在的所有原子和亚原子粒子都可能干扰 qubit，从而产生不完美的状态，从而抵消它们的计算优势。尽管物理实现的量子计算机在高度隔离的环境中接近绝对零度以最小化干扰，但目前很难创建足够数量的完美 qubit，从而限制了量子设备的实现。

由于这个噪声问题，今天的量子计算机仅限于五十到几百个 qubit。这促使加州理工学院的理论物理学教授 John Preskill 将量子计算的当前最先进技术称为嘈杂的中间规模量子（NISQ）时代（Preskill（2018））。由于量子计算机不断发展，因此预计这些限制终将被克服。

在量子计算领域工作的公司和组织通常遵循两种不同的方法，以生成更多的 qubit。一些人一直在尝试稳定物理 qubit 并创建完美的 qubit。其他人则应用纠错技术来抵消不稳定性。这涉及添加更多的 qubit，称为逻辑 qubit。尽管 NISQ 设备在能力方面受到限制，但嘈杂的量子计算机已经可以成功地执行某些特定任务[1]。

目前还不确定何时将建造出足够强大的操作量子计算机，以破解当前的加密协议。然而，专家意见是，这可能会在未来 10-15 年内发生（Mosca（2021））。行业的快速发展使得预测变得困难：任何时候都可能出现完全改变前景的新突破。2022 年 12 月，中国研究人员在一篇有争议的论文中声称，使用当前一代量子机器可能会破解广泛使用的 RSA-2048（Rivest-Shamir-Adleman）加密方案（Yan 等人（2022））。2023 年 2 月，量子计算领域的一位重要人物报告了 qubit 误差率的降低，生成了噪声更小的量子计算机。这些快速的性能提升显著增加了量子攻击的风险。

同样令人担忧的是当前的“现在收获，以后解密”的量子网络威胁，恶意行为者可能会拦截和存储机密的、经典加密的数据，以便在量子计算机变得足够强大时进行解密。任何需要长期加密保护（即必须保持安全和私密超过 10 年的所有数据）

[1] 量子计算领域一直存在着关于何时以及是否能够达到“量子至高”时刻的许多争论——即量子计算机超越经典计算机的时刻。2019 年，谷歌宣布其 53 位 qubit 的“Sycamore”处理器完成了一项特别复杂的计算，比世界上最强大的经典计算机快了 1.58 亿倍，将所需时间从 1 万年缩短到不到四分钟。尽管后来发现该任务是为实验目的而人为设计的，但这清楚地表明 50 比特是一个显著的门槛——量子机器可以在比经典计算机更短的时间内执行特定任务的起点。2020 年底，中国合肥的中国科学技术大学的研究人员宣布，他们的量子计算机能够解决目前最强大的计算机无法解决的问题。2022 年，IBM 的研究人员提出了一个量子路线图，目标是在 2025 年实现 4,158 个嘈杂 qubit。

的数据都需要尽快采取后量子保护措施，特别是如果这些数据存储在离线位置（例如云中）。

这种网络风险将对金融系统产生破坏性后果。考虑到这种风险和可能影响金融稳定性的后续漏洞是至关重要的。

2.2 当前加密技术面临的潜在威胁

密码学是基于计算复杂性的。今天的密码学可靠地保护着今天的计算机系统，确保了安全的互联网通信等。它是一种确保在线通信的机密性、完整性和身份验证的基本工具。这意味着信息只应该对预定的接收者可用，接收者可以确信信息来自正确的发送者，并且这些信息在传输过程中没有被更改。

目前有两种加密系统正在使用：对称加密和非对称加密（也称为公钥加密）。在两个不同的 IT 系统之间创建安全通道通常是通过使用对称和非对称加密系统的多步过程来完成的（请参见图 2）。首先，在称为密钥交换机制（KEM）的过程中交换秘密密钥，使用非对称加密加密秘密密钥，然后使用对称加密使用共享秘密密钥加密发送给两个方之间的消息。这种组合方法的一个原因是非对称加密比对称加密慢得多。

非对称加密依赖于复杂的数学问题，例如质因数分解。这种方法的思想是，虽然经典计算机可以通过将两个足够大的数字相乘来生成一个数字，但将该数字分解回原始质数是极具挑战性的。

1994 年，数学家 Peter Shor 设计了一种量子算法，理论上能够计算大数的质因数。网络安全专家立即确认了 Shor 算法对非对称加密的威胁，例如 RSA 加密算法，它依靠有效地分解非常大的数字来保证其安全性。如果在具有足够 qubit 的量子计算机上运行，Shor 算法可以使质因数分解挑战变得微不足道，将在今天的经典计算机上需要数百或数千年的操作时间缩短到在足够强大的量子计算机上只需要几小时甚至几分钟。第二个量子算法 Grover 也对对称加密算法（如高级加密标准 AES 或 SHA）构成威胁，后者用于加密货币挖掘过程。对于 AES，解决方案是将密钥长度从 128 位增加到 256 位，使其免受基于 Grover 算法的攻击。

此外，重要的是要了解，这种网络威胁不仅会影响公钥算法，还会影响生成加密密钥的方式。为了防范这种威胁，必须加强所有使用非对称加密的加密协议，包括身份验证。数字签名是一种用于验证数据完整性和身份验证的加密机制。在数字签名方案中，签名者拥有一个秘密签名密钥，签名验证器拥有相应的公钥。当签名者使用其秘密密钥签署消息时，可以使用相应的公钥验证签名。数字签名广泛用于

支付系统。

随着量子计算研究的快速发展，紧迫的问题是量子计算机何时能够破解当前的加密方案。为了回答这个问题，需要精确了解需要多少个完美稳定的 qubit 才能有效地应用 Shor 或 Grover 算法，以便对非对称加密方案发动攻击。由于已经发表了关于需要多少个 qubit 才能破解 RSA 加密算法的不同估计，因此很难预测它将过时的确切日期。更加复杂的是，量子机器何时开始运行的估计通常会因预测人员来自研究社区还是涉足构建（并试图销售）量子计算机的公司而大相径庭。毫无疑问的是，没有任何组织，尤其是中央银行，愿意通过不作为而冒量子计算机网络攻击的风险。

为了应对这种网络安全威胁，科学界一直在研究新的加密协议，以创建量子抗性环境。Project Leap 探索了这些新的加密方案。

图2 设置一个传统VPN

图 2

3 如何抵御量子解密威胁

3.1 一个由 NIST 组织的国际合作项目

研究人员和国家标准机构一直在努力解决保护互联网信息的问题。2016 年，美国国家标准与技术研究院（NIST）宣布了一项公开竞赛，以选择量子抗性公钥加密算法。通过涉及来自世界各地的专家的协作过程，开发了 80 多种算法（23 种签名

方案和 59 种密钥加密机制方案）。随后，科学界进行了一系列竞争性回合，测试了所提出的算法。这个过程导致了不同的算法被同行或 NIST 专家的工作所排除[1]。

图3

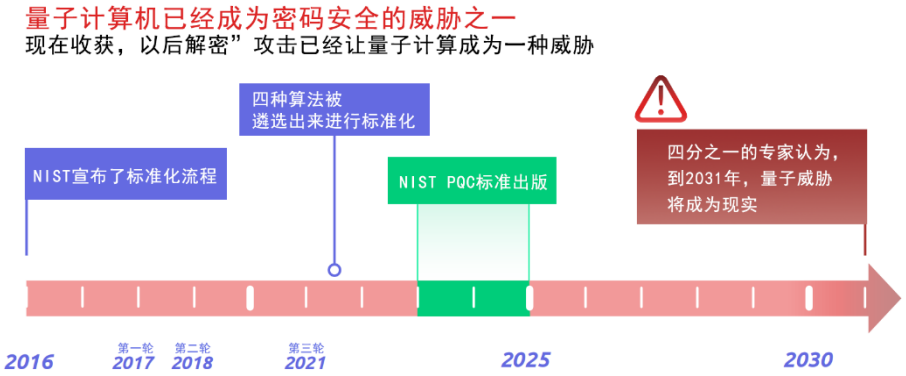


图 3

2022 年 7 月，在三轮竞赛之后（图 3），第一组四个算法被选中进行标准化。这意味着现在可以实现和测试这些算法以用于实际应用。

在 Project Leap 中，一个主要目标是实现所选算法并了解迁移到新加密标准时的影响。在该项目中，NIST 选择的所有算法都经过了测试。此外，还实施和测试了 FrodoKEM 算法，该算法[2]被法国和德国当局视为与 NIST 选择的其他标准化算法一样可靠（请参见表 1）。

表 1

[1] 例如，在 2022 年，有两个算法经过测试，它们的弱点暴露了出来。一个名为 Rainbow 的数字算法被提交给 NIST 用于消息验证，但被破解了。另一个被称为超奇异同源密钥封装（SIKE）的加密算法在使用 2013 年 Intel Xeon 处理器的一个核心约一个小时内被破解。因此，这些算法随后被排除在竞争过程之外。

[2] ANSSI 和 BSI（见术语表）。

表1 Project Leap中测试的算法

算法名称	算法类型	基于的问题族	轮次
CRYSTALS-Kyber	公钥加密	基于格	经过了标准化筛选
CRYSTALS-Dilithium	数字签名	基于格	经过了标准化筛选
FALCON	数字签名	基于格	经过了标准化筛选
SPHINCS+	数字签名	基于哈希	经过了标准化筛选
FrodoKEM	公钥加密	基于格	被德、法专家认定为优秀选择

*附录B详细解释了这些算法的问题族

密码学算法通常基于特定的数学问题族。NIST 为标准化选择的四种算法中，三种来自基于格的问题族，一种来自基于哈希的问题族（有关完整列表，请参见附录 B）。

NIST 过程的一个重要目标是采用多样化的数学问题族作为算法的基础。这是因为，虽然一种算法可能被认为足以保护今天的 IT 系统，但随着网络威胁的快速发展，它是否能够在长期内保持可靠性还不确定。为了鼓励更广泛的问题族算法，NIST 在 2022 年启动了第四轮。这一轮包括基于诸如同构和基于代码的算法族的公钥加密机制。同时，NIST 呼吁提出新的数字签名提案，旨在鼓励数字签名标准所基于的数学问题的多样性。长期目标是标准化为不同的用例设计的不同类型的算法。

这个标准化过程的结果，欧洲网络安全机构正在依赖的这个结果，将在 2024 年最终确定。与此同时，国家机构已经发表了他们对后量子密码学实施的看法。法国网络安全机构指出，安全应该是主要优先事项，如果一种算法不在 NIST 标准化选择中，但证明比 NIST 标准提供更高的安全级别，也应该被接受（ANSSI（2022））。

3.2 当前可实施的解决方案

准备迎接量子时代是网络安全部门的主要关注点。不同的方法已经被定义并且是可行的。本报告旨在提供对其中一些方法的理解，但并不详尽。Project Leap 采

用的策略已被标准机构和国家网络安全机构推荐。具体而言，NIST 认识到混合方法在迁移阶段维护互操作性的重要性（NIST（2023））。它包括使用传统和后量子算法的混合模式。这种双层实现方案为使用公钥加密时的预共享密钥提供了解决方案。为了实现这样的解决方案，通过测试一系列算法开发了成本效益分析。

4 如何准备和创建量子安全环境

4.1 后量子密码 VS 量子密码

目前，研究人员正在探索两种方法，以确保通过网络发送的数据免受潜在的量子计算机攻击。这些方法被称为后量子密码学和量子密码学。尽管它们的名称相似，但这是两种根本不同的方法，因此重要的是能够区分它们。

后量子密码学涉及使用新的数学问题族（请参见附录 B）作为算法的基础，以加强当前使用的加密协议的安全性。这些可以部署在现有的 IT 基础设施上。由于无法预测可能会设计出什么新技术来破解这些新算法，因此这种方法始终存在一定的网络风险。尽管如此，使用后量子密码学保护 IT 系统被认为是非常可靠的，因为我们可以假设，如果可能的话，破解这种量子抗性密码学仍需要耗费极大的时间和金钱。

与依赖于数学的复杂性不同，量子密码学依赖于量子力学的基本原理，例如不确定性原理，以创建抗量子系统。例如，为了保护密钥分发，可以使用粒子来确保所选密钥的随机性以加密数据。称为量子密钥分发（QKD），这种方法允许发行一次性密钥交换。虽然是一种非常有前途的技术，但量子密码学需要专门的硬件，而且无法解决身份验证问题。这需要在实践中将其与后量子密码学相结合。实施它将意味着对全球 IT 基础设施进行重大升级，从而显着增加了向安全环境的过渡成本。

因此，国家网络安全机构支持尽快部署后量子密码学，因为这可能允许在足以破解当前加密协议的量子计算机开始运行之前进行迁移。在今天的基于 Web 的经济体中，机构（如中央银行）更容易尝试新型经典密码学，而不是使用量子密码学，因为他们可以更轻松地适应浏览器和服务器以添加对新协议的支持。在金融领域等行业范围内适应系统始终是棘手的，因为只有几乎每个参与者都进行了过渡，移动才能变得可操作。

因此，ANSSI、BSI 和 NIST 等国家机构主张尽快开始过渡到混合模式的后量子密码学方案。Project Leap 假定在过渡期间旧协议和新协议共存。

4.2 中央银行需要未雨绸缪

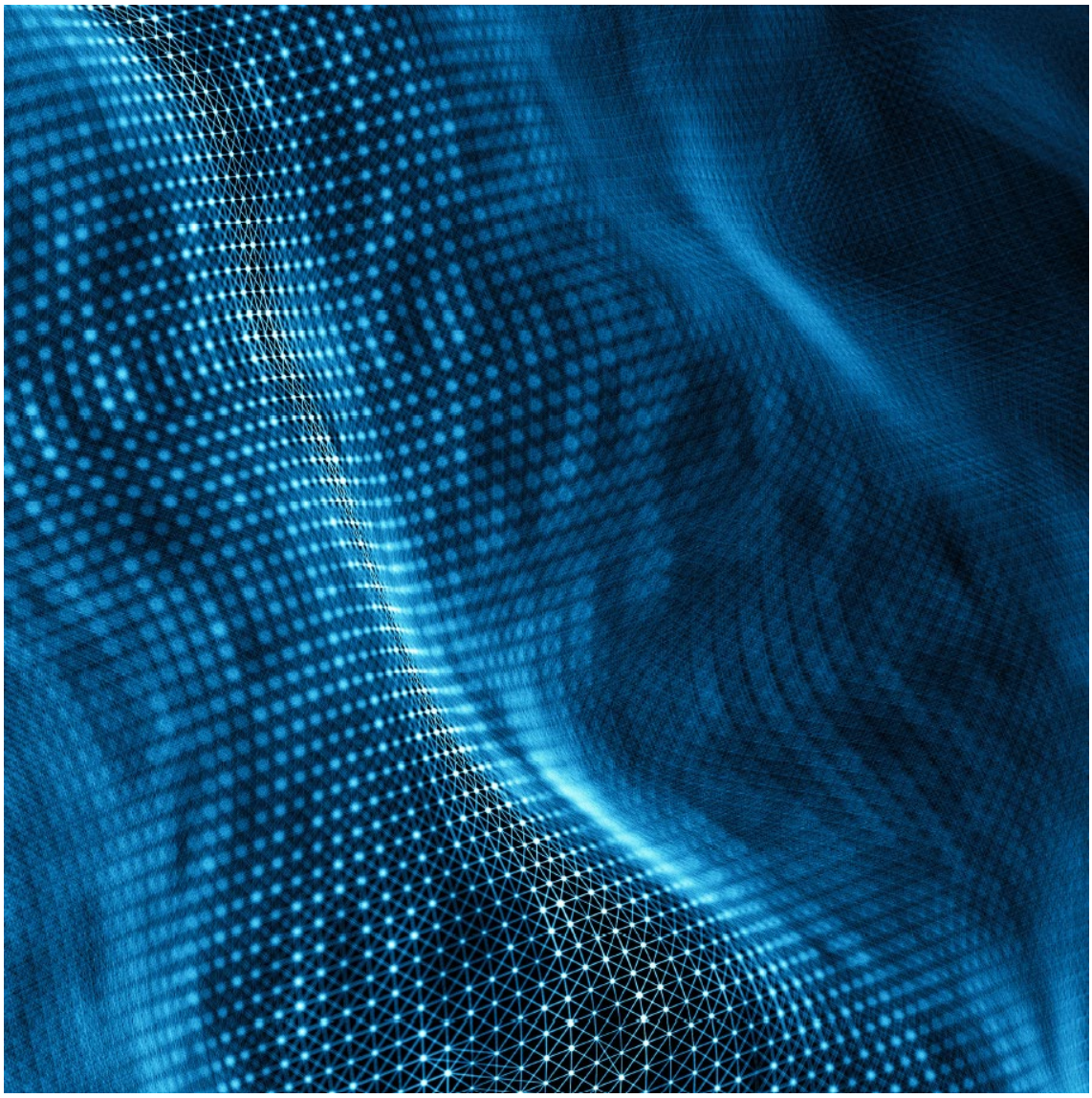
毫无疑问，量子计算对金融稳定性构成了重大风险。金融行业一直面临着常规网络攻击的威胁，这可能导致偿付能力和流动性冲击。Eisenbach 等人（2021）表明，对中型银行的网络攻击可能会产生大规模影响。金融市场基础设施的相互关联结构也容易受到传染效应的影响，这可能影响整个金融行业。与传统攻击相比，量子计算机攻击对金融系统的影响可能更加严重和昂贵。考虑到金融数据的长期敏感性和当今 IT 系统的复杂性，更不用说从重大网络入侵中恢复的潜在成本，中央银行需要提前解决这一威胁。

鉴于互联网通信、数字签名、密码、合同和其他文件的数据保护机制在足够强大的量子计算机开始运行时将立即过时，风险很高。除此之外，这将破坏今天数字签名合同的完整性，因为签署者身份的有效性将无法得到保证。

好消息是，许多组织和政府开始做出回应。2022 年 11 月，白宫发布了一份备忘录，计划实施后量子密码学，概述了一个具体的时间表，将易受攻击的系统转移到量子抗性加密。与此同时，法国 ANSSI 等国家机构一直在向政府和企业发布有关将系统迁移到量子安全密码学的指导。

然而，在面对这种威胁时变得自满是危险的，中央银行需要立即采取行动，因为替换当前的加密标准可能需要数十年，正如 NIST 所警告的那样（NIST（2021））。经验表明，新标准发布后可能需要数十年才能完成迁移。过渡规划应从量子风险评估开始，以确定和清点易受量子计算机攻击的系统。然后应制定战略性和长期的量子路线图，包括过渡阶段，因为这将是保护和加强关键中央银行基础设施的关键。

在 Project Leap 中，创建了一个量子安全环境，以保护基础设施免受数据在传输过程中的拦截。这个解决方案可以保护高度敏感的通信，防止其被拦截后被解密。考虑到这种转变对中央银行 IT 系统的影响，不仅需要实施新的算法，还需要更改整个密码协议集。到目前为止，在设置 VPN 隧道时，协议仅能依赖 RSA 方案。但是，使用量子安全协议后，保护数据的方式将会发生变化。迁移到新的密码协议需要提前定义，以确保新协议所涉及的所有复杂性都将得到解决。



5 Project Leap

5.1 目标和范围

Project Leap 旨在通过在混合加密中实现传统的公钥算法和量子抗性算法来创建量子安全环境，以确保在两个不同的 IT 系统之间发送的消息的机密性，以及数据的完整性、身份验证和防重放，确保任何交换的数据都无法被重发。该连接是

在公共云和本地基础设施之间建立的。然后，通过使用供应商修改的开源互联网络协议安全（IPsec）VPN 解决方案 strongSwan 配置的虚拟专用网络（VPN）在法国银行和德意志联邦银行之间传输付款消息。

图4 Leap计划 - 量子混合加密的安全VPN隧道

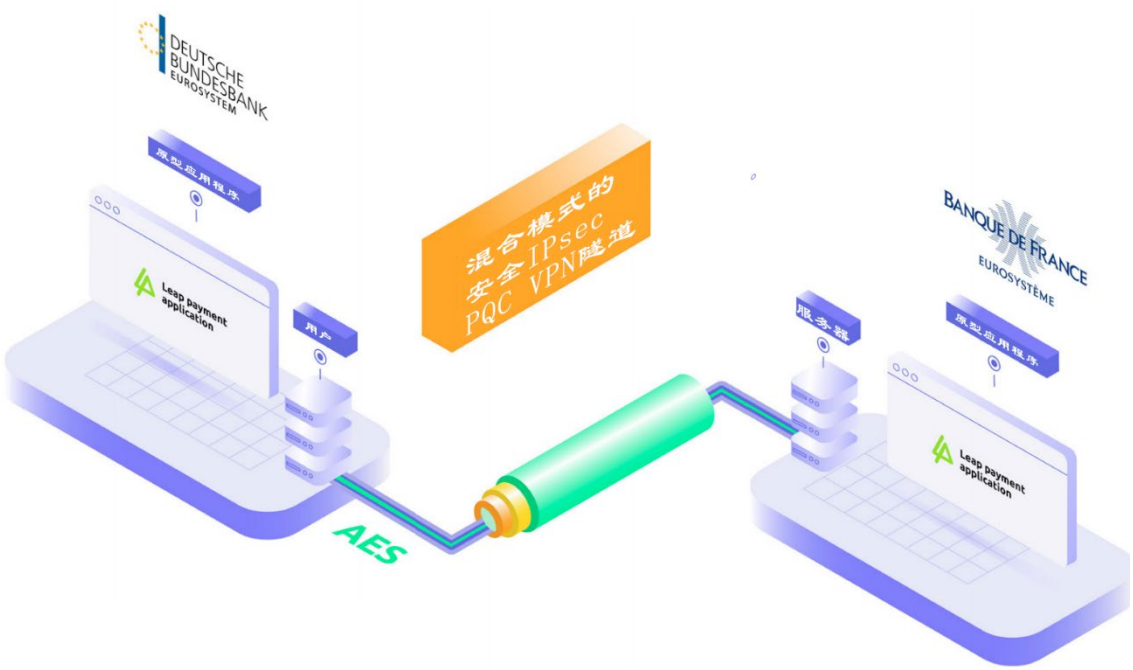


图 4 Leap 计划-量子混合加密的安全 VPN 通道

在中央银行系统中，VPN 被广泛用于在公共网络上连接并安全地传输数据。为了在两个位置之间创建安全隧道，VPN 会加密数据，使其在不受信任的网络上传输，并保持用户身份的机密性，从而隐藏 Internet 流量。Project Leap 专注于建立量子安全的站点到站点 VPN。

测试阶段的重点是测试密码敏捷性、性能和安全性。最初的范围是证明新的密码协议可以为量子时代的中央银行系统提供所需的安全级别。随着后量子密码学领域的快速发展，项目团队还测试了当前密码系统适应新加密方案的能力。一个主要目标是证明后量子密码学与公共网络的使用是兼容的。

该项目与技术合作伙伴一起，专注于集成后量子算法库。另一个目标是向中央银行社区介绍如何建立此类项目。其中一个重要的教训涉及人员配备。目前，具备所需技能和专业知识的人员仍然很少。随着需求的增加，将需要大量培训网络安全专家和密码学家的量子安全相关技能。在 Project Leap 的情况下，一支网络安全专家团队接受了特殊培训，以掌握测试所需的特定能力。

图5 Project Leap的涉及范围

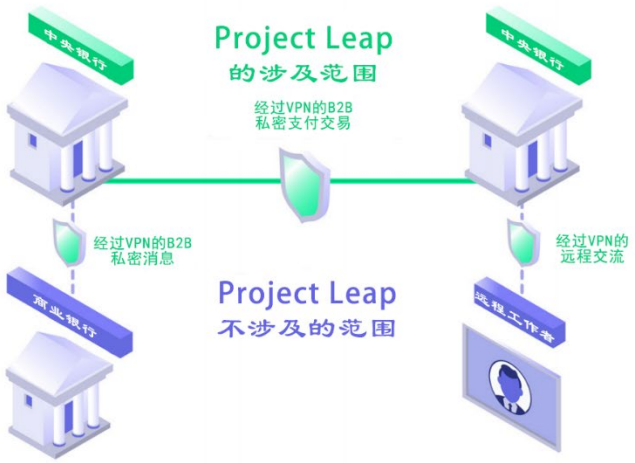


图 5 Project Leap 的涉及范围

5.2 解决方案设计

在一个混合量子抗性虚拟专用网络(VPN)Internet 协议安全(IPsec)隧道中，使用后量子算法库，实现了安全的通信渠道，包括密钥交换和身份验证，以在两个中央银行之间发送符合 ISO 20022 标准的 XML 付款消息。作为测试的一部分，还开发了一个名为 Leap payments 的前端应用程序，具有高级用户界面。

在这个项目中，虚拟机在不同的位置上设置，提供足够的灵活性，以允许在使用供应商软件和不同的 IT 环境时进行技术集成。在德国方面，云环境支持 AVX2（高级矢量扩展），从而实现了后量子算法的最有效实现。在法国方面，虚拟机在基于传统 IT 系统的私有云中设置。

在该项目的第一阶段，测试了不同的算法(Kyber 和 FrodoKEM 用于密钥交换；Crystals-Dilithium、Falcon 和 Sphincs+用于数字签名)，重点关注高水平的安全性（见表 2)。在选择算法时，考虑到中央银行环境的安全要求和正在进行的标准流程的演变。此外，供应商配置的解决方案用于生成 x.509 后量子证书。

表 2 已实现的算法组合

表2 已实现的算法组合

测试ID	KEM	PQC安全强度类别	DS	PQC安全强度类别
Legacy	RSA 2048	0*	RSA 2048	0*
Kyber3_dilithium5	Crystals-Kyber	3	Crystals-Dilithium	5
Kyber5_dilithium5	Crystals-Kyber	5	Crystals-Dilithium	5
Kyber5_falcon5	Crystals-Kyber	5	Falcon	5
Frodoa5_dilithium	FrodoKEM (AES)	5	Crystals-Dilithium	5
Frodos5_dilithium	FrodoKEM (Shake)	5	Crystals-Dilithium	5
Kyber5_sphincs1	Crystals-Kyber	5	Sphincs+	1
Kyber5_sphincs5	Crystals-Kyber	5	Sphincs+	5

*后量子安全强度类别不适用于传统密码学，因为 RSA 安全级别指的是不同的标度。安全级别的标度详见上表 4。

5.3 实施和测试

一旦建立了多层 VPN 隧道，测试就会按照混合化的新协议的不同步骤执行。与传统 VPN 相比，构建量子安全 VPN 所需的额外步骤增加了协议的复杂性并提出了性能问题。实际上，在设置传统 VPN 时，第一步是交换密钥，然后传输证书以进行验证。客户端使用公钥创建对称密钥加密，然后使用对称密钥加密会话。最后，服务器端使用私钥解密对称密钥。这种协议今天被广泛使用，更为简单。新的混合 VPN 设置包括额外的步骤，因为经典算法与后量子算法一起使用。

测试阶段的第一阶段是证明该解决方案完全可操作：通过运行完整的用例场景，展示了打开隧道并具有从发送方向接收方发送付款消息的能力（见图 6）。

Graph 6 Screenshots of Leap application

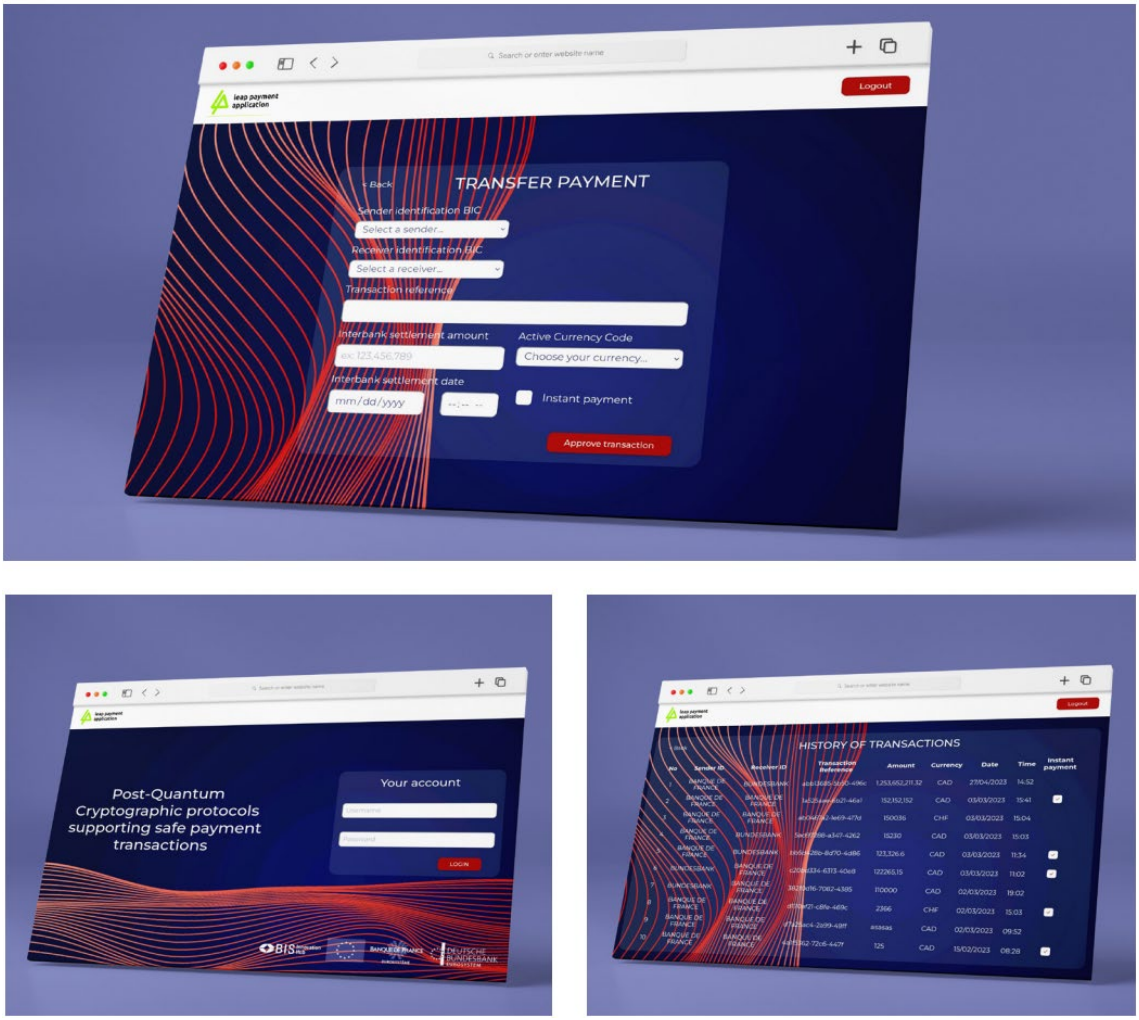


图 6 Leap 应用程序的截图

为了验证在混合模式下使用后量子密码协议建立安全隧道是否能够在两个不同位置和不同 IT 环境的情况下提供完全功能的解决方案，制定了一项战略测试计划（表 3）。测试阶段重点关注网络安全的三个方面：密码敏捷性、性能和安全性。一些测试，例如测试 4，涉及这两个主题，同时提供有关性能和安全性的见解。测试是通过脚本自动化的，使测试过程可重复。

表 3 已进行的测试

表3 已进行的测试

序号	描述
1	能够使用后量子协议在两个中央银行之间建立 VPN 安全隧道
2	经过后量子密码和传统密码的比较
3	经过两种不同后量子算法的比较
4	通过从头开始设置 VPN 来测试灾难恢复案例
5	在一整个工作日内测试安全隧道的性能稳定性
6	考察安全性和性能之间的权衡
7	识别证书交换中使用的算法
8	测试虚假证书

5.3.1 密码敏捷性

一旦建立了多层 VPN 隧道，测试就会按照混合化的新协议的不同步骤执行。与传统 VPN 相比，构建量子安全 VPN 所需的额外步骤增加了协议的复杂性并提出了性能问题。实际上，在设置传统 VPN 时，第一步是交换密钥，然后传输证书以进行验证。客户端使用公钥创建对称密钥加密，然后使用对称密钥加密会话。最后，服务器端使用私钥解密对称密钥。这种协议今天被广泛使用，更为简单。新的混合 VPN 设置包括额外的步骤，因为经典算法与后量子算法一起使用。

图7 ANSSI预设的迁移计划时间线

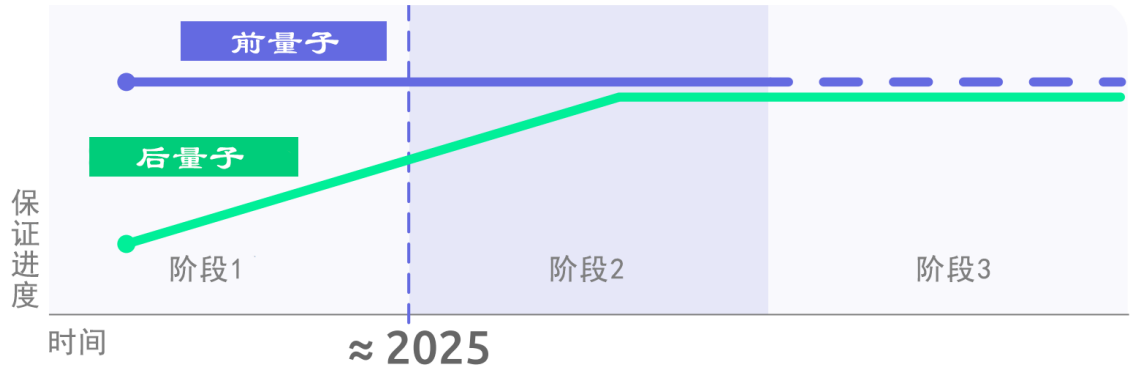


图 7 ANSSI 预设的迁移计划时间线

在这种情况下，测试了不同的传统和后量子密码学组合以确保敏捷性。由于算法经常被切换以测试不同的配置，因此 Project Leap 能够清楚地证明从一个算法切换到另一个算法是容易、快速和可靠的。

5.3.2 性能表现

该项目团队设计了测试计划，以收集不同算法组合之间的性能比较。不同的测试允许团队通过测量仅实现经典密码学（例如 RSA 加密算法）时的性能时间，然后测量添加额外的后量子密码学层的影响来比较延迟。性能测试在不同算法和单个算法的不同变体之间以及在不同安全级别下进行。测试协议配置以使结果能够进行公正比较而定义；具体而言，增加了一些参数以限制强 Swan 中数据包和片段的大小。还测试了隧道的性能稳定性以及从头开始构建 VPN 时的影响。

5.3.3 安全性

密码算法的安全强度因算法和密钥大小而异。后量子算法的安全强度类别在 1 到 5 的范围内定义（5 为最安全）。NIST（2016）根据对称密码学标准定义了这些安全类别，作为任何需要计算能力等于或大于破解确定对称密钥所需计算能力的攻击。

表 4 由 NIST 定义的安全强度类别

表4 由NIST定义的安全强度类别

安全强度类别	破解对称密钥所需要的算力量级	对称密钥
1	使用 128 位密钥在分组密码上进行密钥搜索	AES 128
2	对 256 位哈希函数进行碰撞搜索	SHA256/SHA3-256
3	使用 192 位密钥在分组密码上进行密钥搜索	AES192
4	对 384 位哈希函数进行碰撞搜索	SHA384/SHA3-384
5	使用 256 位密钥在分组密码上进行密钥搜索	AES 256

在设置 VPN 隧道时，测试了由 NIST 选择用于标准化的算法以及 FrodoKEM，包

括 1 到 5 之间的不同安全级别的时间测量结果的比较。还进行了其他测试，以识别所使用的证书并测试虚假证书。

为了彻底测试密码敏捷性、性能和安全性，进行了八个测试系列，并对每个配置进行了至少 100 次测试（有关测试的更多详细信息，请参见附录 D）。测试阶段证明，实现后量子密码协议已经是可行的。下面专门介绍了有关发现的部分，提供了有关根据中央银行流程的性能和安全要求的不同可能算法组合的更多见解。

6 研究发现

6.1 密码敏捷性

如今，大量信息系统由于没有考虑易于替换而缺乏密码敏捷性。转向新的协议需要进行深入的基础设施修改。因此，后量子算法需要在集成适应的密码解决方案的当前混合系统中进行测试。在 Project Leap 中，选择了开源解决方案 strongSwan，

因为它提供了所需的灵活性。在混合模式下实现后量子密码学允许新算法与传统算法并存，并具有放弃不再被国家网络安全机构推荐的任何特定算法所需的灵活性。

国家标准化机构（如 NIST）和国家网络安全机构（如 BSI 或 ANSSI）建议采用混合化（BSI（2023）），这意味着后量子算法应与基于密码敏捷性的传统密码学方案相结合。在这种设置中，客户端和服务器在一开始就协商并同意将实施哪些附加密钥交换。在 Project Leap 首次尝试使用量子安全密码学构建 VPN 时，证明了密钥协议和数字签名都可以在混合模式下实现。

采用绿灯方法来检测信息是否通过量子安全 VPN 传输。一旦建立了量子安全连接，Leap Payment Application 标志的颜色就会变为绿色，这意味着 VPN 隧道已经建立并以混合模式进行了加密。这与现有的 VPN 应用程序相似，其中使用的密码类型是完全透明的。这也类似于浏览器中的小锁形状，表示用户与 Web 服务器之间存在安全连接。Project Leap 测试的目的与子网相同，但仅限于子网。显示绿灯的屏幕截图可以在附录 C 中找到。

关于所使用的密码协议的敏捷性，注意到密钥交换机制可以轻松接受任何后量子算法。但是，数字签名的情况并非如此，标准配置未预先配置以检测算法。尽管如此，这样的配置是可能的。X.509 证书是一种基于非对称密码学的数字签名的公钥管理标准格式[1]。它因其密码敏捷性而被选中。

测试阶段的最终的功能性发现是，具有高度密码敏捷性的系统将更好地应对即将到来的转变。中央银行应检查其系统，以确定缺乏此类灵活性的系统的使用情况并计划其替换。这很可能适用于某些类型的硬件，例如 HSM、防火墙和智能卡。

6.2 性能表现

实现后量子密码学可能会涉及潜在的性能成本，因为需要生成密钥并验证签名所需的时间。在 Project Leap 中，这些方面也进行了测试。

在设置 VPN 时，使用时间测量测试了密码算法的性能。测试是使用传输 1 Mb 文件进行的。此外，约 1 Mb 的标准 Pacs.008 付款消息在法国银行和德意志联邦银行之间通过 VPN 传输。

无论数据大小如何，通过 VPN 隧道发送数据时都不会对性能产生影响，因为当设置后量子 VPN 隧道时，信息使用传统密码学（AES-256）进行加密。发送的消息的计时指标与使用传统密码学设置 VPN 所需的时间长度相同。由于加密层的额外

[1] X.509 证书涉及由 CA 证书生成其他证书或终端用户证书。这些证书由 IETF 标准化，参考 RFC 5280。

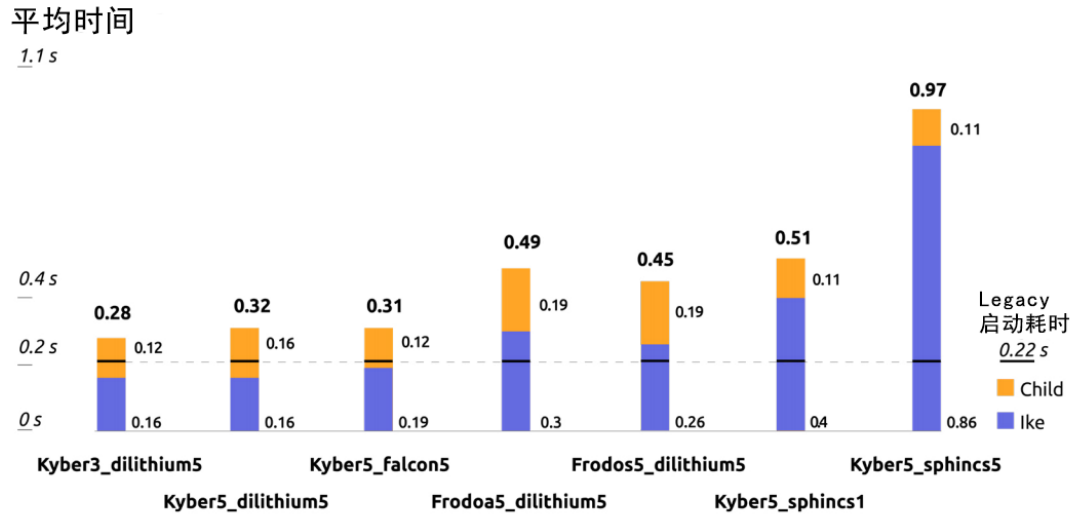
增加，初始设置隧道时性能受到影响，但数据传输的性能不受影响。在实际应用中，初始隧道只会在一天的业务中设置一次或两次。

在测试阶段，测试了不同 IT 系统上的算法，包括遗留系统以及具有更新配置的云环境。在遗留系统中执行 FrodoKEM 的两个版本（AES vs Shake）的性能受到轻微影响。如预期的那样，测试表明，硬件加速（例如 AVX2）可以提高设置隧道的速度，特别是与 FrodoKEM Shake 相比，FrodoKEM AES 版本的速度更快。

在中央银行 IT 系统中，拥有多样化的算法范围有助于处理不同的用例。在这个阶段，所有经过测试的后量子算法都适用于中央银行流程，并且后量子算法的各种安全强度类别都被认为是强的。然而，需要考虑性能方面的差异。具体而言，关于数字签名 Sphincs+，注意到其性能较其他算法慢。这种类型的算法在性能不是高优先级的应用程序中使用时将受到赞赏。另一方面，作为基于哈希的算法，Sphincs+不必以混合模式实现，因为该算法族的可靠性是众所周知的。在 Project Leap 中，Sphincs+被配置为混合化。即使考虑到协议遗留部分所需的时间，该算法的时间仍较长。

在 Project Leap 的第一阶段进行的测试需要继续探索更多流程。测试结果（请参见附录 D 中的表格）表明，在设置隧道时，不同算法之间的性能特征存在广泛的差异。

图8 在德意志联邦银行（客户）和法国银行（服务器）之间建立后量子VPN隧道所需的时间



标记为 IKE 的蓝色条表示交换非对称密钥和身份验证所需的时间。
标有 CHILD 的橙色条表示交换密钥所需的时间。
协议的这些不同步骤在图4中表示为隧道的叠加层。

图 8 在德意志联邦银行（客户）和法国银行（服务器）之间建立后量子 VPN 隧道所需的时间

通过记录从头开始构建新 VPN 隧道所需的时间来测试隧道的可靠性和一致性。一旦数据通过隧道发送，隧道将重新生成密钥以便再次交换密钥。然后，重复启动该过程以了解连接中断的后果。在这个特定测试的开始，项目团队注意到重新生成密钥没有性能影响。观察到协议发送重新生成密钥命令，但不会立即执行。一旦系统被告知重新生成密钥，它就会发送确认以表明命令已注册。这类似于 IT 系统问题的票务。这并不意味着问题会立即得到处理和解决。在这种情况下，重新生成密钥稍后执行，然后可以进行测量。通过这个具体的测试，观察到隧道的性能稳定性没有受到影响。在隧道重新生成密钥期间，性能的影响仅涉及密钥交换，对于客户端来说完全是异步的。这个测试重复了 100 次，并显示出稳定的结果。

VPN 隧道的稳定性也通过每小时验证进行了测试，当隧道仍然设置时，进行了完整的工作日验证。验证的频率可以根据需要进行更改。项目团队认为，一个完整的工作日足以证明隧道完全可用。结果表明，连接稳定，并且与遗留 VPN 隧道一样有效。

6.3 安全性

虽然 ANSSI 等各种机构建议仅实施第五个安全类别，但 Project Leap 团队选择测试了 NIST 定义的几个不同安全类别。在混合实现和非混合实现之间进行了比较。在混合模式下使用后量子密码学可以缓解两个与安全相关的风险：

- 如果遗留的非对称密码系统被破解，后量子层将保护数据传输，从而保持系统的安全性。实施混合模式可以防止任何退化。
- 混合化使系统具有敏捷性：随着传统方案变得过时，更换传统方案变得更加容易。

在安全性和性能之间总是存在权衡。如果使用高级别安全版本的算法来增加安全强度，则设置 VPN 隧道所需的时间也会增加。因此，必须根据应用程序要求配置安全性，考虑到处理速度的重要性以及需要操作公钥和密文的频率。性能测试的结果显示，除了后量子算法 Crystals-Kyber 之外，其他算法在 3 级和 5 级之间的速度差异在几秒钟之内，Crystals-Kyber 的速度差异微不足道。测试结果表明，在具有高性能约束的用例中，Crystals-Kyber 似乎比 Frodo 更适合。Crystals-Dilithium 和 Falcon 之间的性能差异较小。尽管如此，Falcon 表现更好。基于这些结果，如果需要性能，则可能更喜欢使用 Crystals-Kyber 和 Falcon 的算法组

合，但用户应首先在其系统上进行内部测试，以确认是否在其特定设置中实现了相同级别的结果。

使用 X.509 标准测试了几种类型的签名算法，以查看是否可以识别正在使用的证书。实际上，由于数字签名的不同可能的后量子算法，识别它是很重要的，以验证所使用的特定算法。一旦接收到证书，OID（对象标识符）描述了证书所使用的算法。因此，使用当前工具可以确定使用的 OID，证明在后量子密码学中确实可以获取有关正在使用的算法的信息。

使用已更改的虚假证书进行了最终测试。这凸显了协议的可靠性：由于无法验证后量子签名，因此证书被拒绝。

测试阶段强调了所使用的密码协议的可靠性，表明提供密码敏捷性至关重要。在传统协议中，识别所使用的算法并不是很重要，因为只有一个算法。这一系列测试证明了在使用不同算法时考虑密码协议的整体效果的重要性[1]。

[1] 更详细的技术信息可以在附件 D 中找到。

7 总结和后续

Project Leap 已经证明了应用后量子协议已经是可行的。因此，现在可以开始迁移过程。中央银行需要在其网络安全路线图中允许过渡阶段，以便在最终标准发布后做好准备。通过提供见解和技术发现，本报告为中央银行在后量子密码协议上的未来合作铺平了道路。Project Leap 从网络层面实现了量子安全环境，通过后量子 VPN 隧道建立了安全的通信渠道，用于发送数据和付款消息。在未来的阶段中，将探索其他中央银行用例，以总体目标为量子证明金融系统的工作做出贡献。

7.1 迁移计划的需求

关键问题是量子计算何时变得实用，因此组织应该准备好应对攻击。通常，这个问题的答案是由 Michele Mosca（Mosca（2021））的定理给出的。迁移计划需要根据以下变量实施（见图 9）：

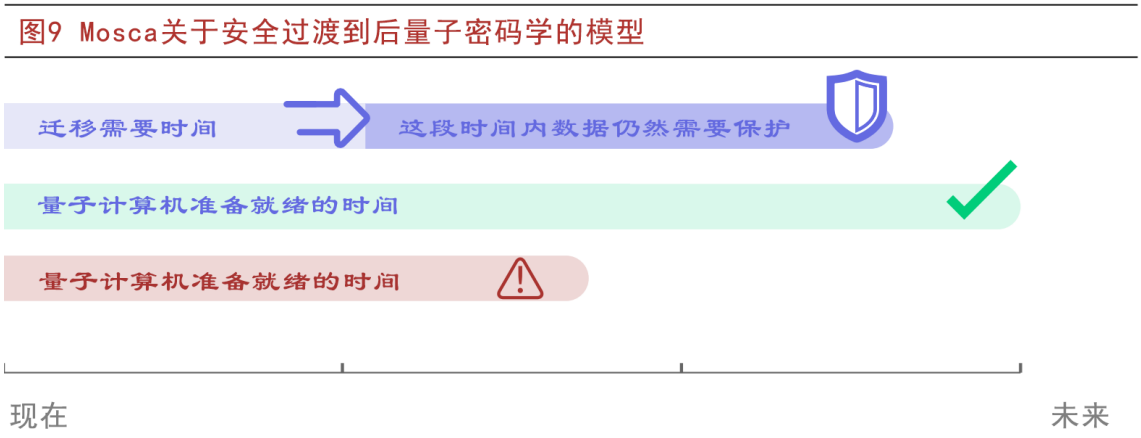


图 9 Mosca 关于安全过渡到后量子密码学的模型

完成这些变量的分析后，中央银行可以制定实施量子安全性的路线图。这个过程将从清点其 IT 系统开始，以确定和评估其漏洞，并确定可能需要替换或升级的安全方法。应尽快建立加密的持续监控过程（CSA（2021））。此外，中央银行需要确定他们正在使用的密码协议是否保护需要长时间存储的机密数据，这些数据可能会受到对手的攻击。如果确定在传统密码学被攻破时信息仍然具有价值，则需要部署新的加密系统。为了有效，必须提前完成。特别是需要检查使用潜在弱加密算法（例如 RSA 和 ECC）以及使用这些算法的易受攻击的协议（例如 VPN IPsec、SSH、TLS 等）。

一旦定义了路线图，实施阶段将开始，通过部署量子抗性加密来升级基础设施。

图10 完成迁移计划所需要的步骤

图 10 完成迁移计划所需要的步骤

迄今为止，中央银行社区只进行了少数测试和实施后量子密码学的倡议。这些新的密码协议在更改广泛部署的密码方案方面存在一些挑战和限制。管理自己的密码基础设施并需要长期密码保护的组织应将量子计算机攻击的威胁纳入其长期路线图中。通过建立安全的 VPN 隧道以保护两个中央银行之间的通信，Project Leap 的合作工作为构建量子抗性基础设施铺平了道路。

7.2 部署面临的挑战

后量子密码学应用的转换将是一项重大任务。正如之前所看到的，中央银行和所有其他组织面临的挑战是需要编制当前在其 IT 系统中使用的密码学清单，并确定威胁的密码学方案的实施位置。一旦审核了所有系统，组织将不得不开始使用新的量子安全密码协议替换易受攻击的密码学方案。另一个挑战是这项工作的规模和所需的时间。转换将影响大量协议、方案和基础设施。迁移到新协议需要时间，因为算法的替换需要新的密码库。不仅硬件会受到影响，操作系统和应用程序代码也会受到影响。这反过来意味着更新所有相关文档。最后但并非最不重要的是人力资源挑战，组织应该在过程的最开始考虑这一点。在今天的劳动市场上，具备所需技能的专家很少。如果需要满足需求，需要培训网络安全专家。尽快开始迁移过程将使中央银行提前组织，为其网络安全部门升级必要的技能留出时间。

7.3 后续

Project Leap 表明，实施后量子解决方案已经是可行的。对于 VPN，已经清楚地证明了对性能没有显著影响。然而，对于性能至关重要的应用程序，例如即时支付应用程序或央行数字货币（CBDC）系统，安全和性能之间需要权衡。还表明，安全级别可以适应不同的中央银行流程，并且实施 strongSwan 解决方案提供了足够的灵活性以进行混合。未来的工作可能包括在更复杂的环境中测试后量子密码学，解决更多的中央银行使用案例，以确保中央银行与其他机构之间的通信安全。在量子证明金融系统方面，量子抗性密码学不仅需要在网络层实现，还需要在应用程序和传输层实现，以建立完整的信任链（图 11）。

图11 Project Leap的后续步骤

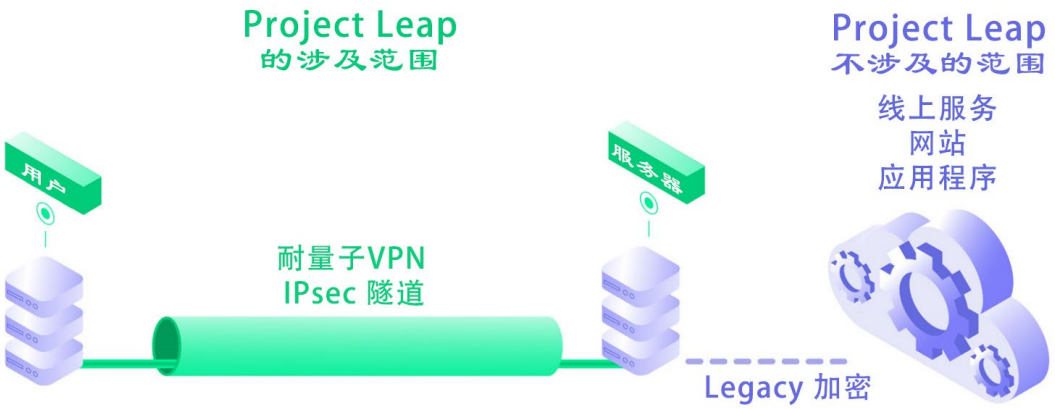
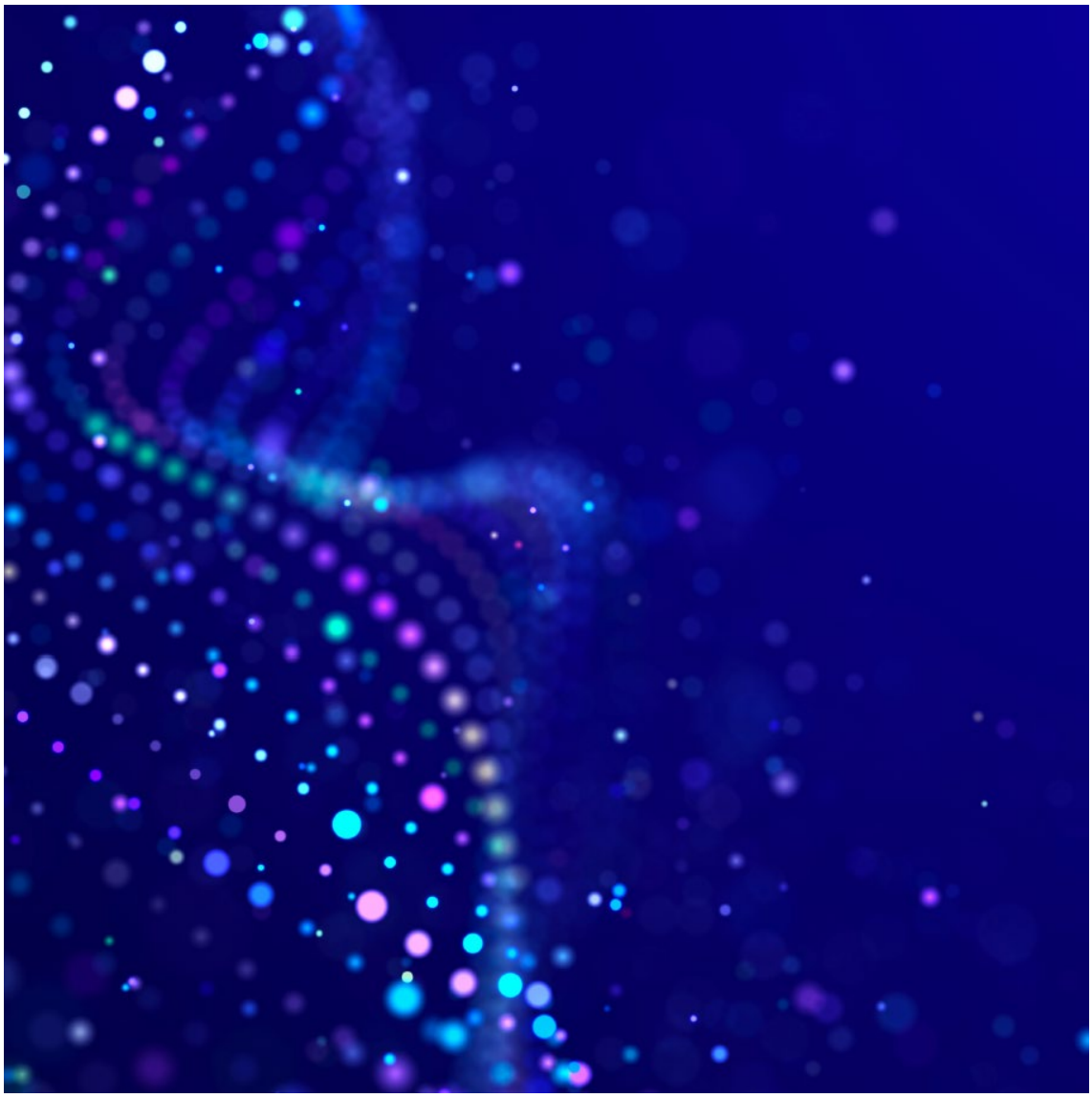


图 11 Project Leap 的后续步骤



附录

术语表

A

ANSSI：信息系统安全国家局是法国的一个机构，负责信息系统的安全。

B

BSI：德国联邦信息安全办公室。

C

Child：IPsec VPN 协议的一个阶段，无需进行身份验证。

D

DS：数字签名是一种用于验证消息的加密过程。

E

ECDSA：或椭圆曲线数字签名算法，是一种基于 ECC 的具有密码学安全性的数字签名方案。

ECDH：椭圆曲线 Diffie-Hellman。

ECC：椭圆曲线密码学。

I

IKE：旨在在两个对等方之间建立安全隧道（完整性和机密性）的协议。

IKEv2：互联网密钥交换协议的第二个版本标准，使用密钥交换算法和数字签名。

IPsec：用于 IP 流量的安全架构，允许在网络层保护数据，并在应用层（OSI 模型）透明。

K

KEM：密钥交换机制（也称为密钥建立）允许使用加密算法在两个方之间交换密钥。

N

NIST：国家标准与技术研究所。

O

OID：代表对象标识符，用于命名 X.509 证书中的几乎每种对象类型。

P

PKE：公钥加密是一种混合加密方案，提供三个基元，即公钥/私钥生成算法、加密算法（使用公钥）和解密算法（使用私钥）。

Q

Qubit：量子位是量子计算机的基本构建块。

R

Rekey：在 VPN 会话期间，密钥交换将在不进行身份验证的情况下更新。

RSA：一种公钥密码体制，其缩写代表 Rivest-Shamir-Adleman，是设计该算法的团队。

S

StrongSwan：是一种基于 IPsec 的开源 VPN 解决方案，使用 X.509 证书进行强身份验证。

T

TLS：传输层安全性的架构。

V

VPN：虚拟专用网络是一种通过不安全的网络创建安全连接的机制，用于在服务器和客户端之间建立安全连接。

参考文献

ANSSI (2022): ANSSI Views on the post-quantum cryptography transition, March.

BSI (2023): Cryptographic mechanisms: recommendations and key lengths, January.

Castelvecchi, D (2023): “Google’s quantum computer hits key milestone by reducing errors”, Nature, 22 February.

CSA (2021):): Practical preparations for the post-quantum world, October.

Eisenbach, T, A Kovner and M Lee (2021): “Cyber risk and the US Financial System: a pre-mortem analysis”, Federal Reserve Bank of New York, Staff Reports, n° 909, May.

Financial Stability Board (FSB) (2017): Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices, October.

Preskill, J (2018): “Quantum computing in the NISQ era and beyond”, Quantum Physics, Cornell University, July.

Mosca, M and M Piani (2021): Quantum threat timeline report, Global Risk Institute, January.

NIST (2016): Submission requirements and evaluation criteria for post-quantum cryptography standardization process, December.

——— (2021): Migration to post-quantum cryptography, August.

——— (2023): Migration to post-quantum cryptography: preparing for considering the implementation and adoption of quantum safe cryptography, April.

Scopus (2021): Quantum computing research trends report, Elsevier, February.

White House, Memorandum for the heads of executive departments and

agencies, November 2022.
World Economic Forum (WEF) (2022): The Global Risks Report 2022, 17th edition.
Yan, B, Z Tan, S Wei, H Jiang, W Wang, H Wang, L Luo, Q Duan, Y Liu, W Shi, Y Fei, X Meng, Y Han, Z Shan, J Chen, X Zhu, C Zhang, F Jin, H Li, C Song, Z Wang, Z Ma, H Wang and G-L Long (2022): "Factoring integers with sublinear resources on a superconducting quantum processor", Quantum Physics, Cornell University, December.

附录 A 技术盒

盒子 1-量子计算

尽管它们对我们对世界的直觉理解提出了挑战，但量子理论的定律是基本的，并且据我们目前的知识，适用于每个物理对象。然而，如果材料由许多基本组成部分组成，则可以使用更直观的定律来描述它们的集体行为。这些定律称为经典定律，这些定律是我们日常计算机所利用的定律。量子计算机一词指的是一种使用物质的量子行为而不是经典定律进行计算的设备。在量子计算机中操作的量子对象称为"qubits"，这是"量子位"的缩写。如今的量子计算机仍然是一项新兴技术和研究努力，而不是已经建立的工程学科。

量子计算这个术语不应与量子计算机技术混淆。量子计算方法是一种完全新的算法方法，涉及只能在量子计算机上执行的算法。量子计算需要一种可以利用和操作某些物理对象的量子行为的设备。最初，人们惊讶地发现，在设计算法时不能忽略物理定律。然而，一旦克服了这个概念上的障碍，量子计算的发展就开始了。正如算法先于现代数字计算机一样，量子算法也先于量子计算机。量子计算基于这样一个假设，即未来量子计算机的 qubits 只能以两个值观察，类似于位可以是 0 或 1。

量子计算经常被简化为超级位置的概念，这是误导性的。量子理论是一个将观察放在其核心的数学构造。量子对象的某些属性仅在有限数量的值中观察到，称为纯态。量子理论的一个基本属性是超级位置，它允许量子对象进化为纯态的混合状态。每当一个 qubit 处于超级位置状态时，对其值进行测量或观察将给出 0 或 1。超级位置不能直接看到，但可以通过概率行为推断出来。因此，qubit 的超级位置

状态意味着观察到的状态将具有一定的概率 P 为 0，概率 1-P 为 1。不确定性不是量子计算机或观察者的实验限制，而是物体量子性的基本属性。使用 qubit 的超级位置状态，可以在一次执行中对两个纯态执行类似的计算。这种方法类似于在具有不同输入的经典多处理器计算机上并行执行相同的代码。但是，如果超级位置只能将算法的执行时间减半，那么其好处将是微不足道的。

超级位置只是使量子计算如此高效的第一个行为。纠缠的概念是第二个概念，在我们对世界的经典概念中没有相应的概念。这个定律使得两个量子对象可以以一种方式纠缠在一起，以至于所得到的化合物不能被描述为每个单独对象的组合。正如谚语所说：整体大于部分之和。这个扩大的潜在配置集随着纠缠 qubits 的数量呈指数增长，并允许自然并行化，这是经典计算机所无法达到的。这是超级位置和纠缠的结合，使得量子算法能够高效地执行某些计算任务。

在讨论物质的量子行为在计算方面的优势时，也很重要提到它的限制。在使用量子计算和构建量子计算机时，最大的挑战与观察或测量有关。一般来说，在微观尺度上，我们假设我们刚刚观察到的物体的状态将被保留。在量子世界中，情况完全不同。如前所述，即使量子对象处于超级位置状态，也只观察到纯态。此外，在观察之后，物体不再处于超级位置状态，而是已经坍塌到观察到的纯态。在量子世界中，“观察是干扰”的话，引用天体物理学家和生态学家 Hubert Reeves 的话。对于量子计算，后果是严重的。这意味着在不干扰最终结果的情况下，无法观察到计算的任何中间结果。甚至可以证明，无法复制量子超级位置状态。

这个规则被称为测量假设，也对构建可行的量子计算机提出了重大挑战。具体而言，与外部粒子的相互作用是可能影响算法并终止其执行的潜在测量。为了按预期执行，量子计算机因此需要一个严格隔离的环境，量子算法肯定需要要求严格的错误纠正步骤。由于量子理论中的测量性质，量子计算机不太可能在所有应用程序类别中取代我们的经典计算机，特别是那些严重依赖复制和存储信息的应用程序。量子计算可能仍然是解决某些计算密集型任务的工具。

量子理论保留信息。这个额外的属性要求量子算法始终是可逆的。在这种情况下，“可逆性”一词的意思是算法中没有单个步骤会删除信息，并且计算的输出应足以重建输入。当微处理器变得越来越难以冷却时，人们考虑了可逆的经典计算机。由于删除信息会增加温度，因此可逆计算机不会像经典计算机那样迅速升温。从可逆计算机的研究中获得的知识在第一个量子算法的开发中非常有用。

盒子 2-RSA 和 Shor 算法

RSA 方法是一种公钥加密方案，基于这样的想法：一个消息可以使用一个密钥（加密密钥）加密，但只能使用另一个密钥（解密密钥）解密。数论等提供了实现这种加密机制的实用模式[1]。

典型的 RSA 方法依赖于两个大质数。使用这两个质数，定义了一个具有与两个质数的乘积相对应的周期性的第一个时钟。然后，使用这两个质数的乘积定义另一个时钟，从中删除了 1。加密是将消息的数字化版本提高到公共加密密钥的幂的过程。计算在第一个时钟上执行，因此第一个时钟的周期性也必须公开。公共加密密钥需要符合某些数学属性，但几乎可以视为任意的。

解密密钥由加密密钥和第二个时钟确定。在第二个时钟的模算术中，解密密钥是加密密钥的倒数。通过在第一个时钟上将编码的消息提高到解密密钥的幂，可以解码消息。

知道编码的消息、公共加密密钥和第一个时钟的周期性就足以解密消息了。该过程非常简单：将第一个时钟的周期性分解为两个原始质数；从这两个质数中减去 1 并将它们相乘，以获得第二个时钟的周期性。使用第二个时钟和公共加密密钥可以确定解密密钥。

虽然该过程可能很简单，但第一步——将数字分解为它所包含的两个质数的乘积——是一个非常耗时的过程。截至今天，没有已知的算法可以有效地执行这种分解，特别是对于大数。缺少这样的算法是使 RSA 如此可靠和强大的原因。

然而，有一种量子算法可以有效地分解大数。这种算法称为 Shor 算法，该算法及其众多变体基于这样的想法：可以通过在第一个时钟上评估编码消息的所有幂来确定第二个时钟的周期性。

Shor 算法有四个主要步骤，它们是：

• 首先，通过在纠缠 qubits 上使用超级位置原理，可以将系统带入表示自然数的二进制表示形式的大序列的状态。

• 其次，需要将任意数字提高到第一步中表示的所有自然数的幂。由于它们处于超级位置状态，因此只需要通过这第二步进行一次通行。在这个阶段，我们知道 qubits 表示一个复杂但周期性的函数。

• 第三步，采取措施使系统强制定居在此周期函数的一个值上。现在，该函数更简单，因为其状态已经坍塌为仅具有少量幂的子集，但仍无法使用。

[1] 在 RSA 中采用的方法基于模算术，它简单地是时钟的算术。使用传统算术，11+2 等于 13。然而，当考虑传统时钟，并假设现在是上午 11 点，再加两个小时会得到下午 1 点，而不是 13 点。尽管传统时钟在 12 点时重新开始计数，但可以使用任何其他自然数设计无数的模算术。这被称为模数或周期性。

• 最后，第四步是使用称为（离散）傅里叶变换的经典过程转换此函数，以确定周期性。了解此周期性允许分解第一个时钟的大周期性并推断第二个时钟的周期性。必须说，这个过程并不总是有效的。在它不起作用的情况下，必须在此算法的第二步中选择不同的任意数字。

如果已知第二个时钟的周期性和公共加密密钥，则消息不再受保护。Shor 算法的改编也可能使其他公钥加密方案易受攻击。

附录 B 后量子算法分类家族

• 基于格的算法：

基于格的算法是建立在寻找最短向量问题或最近向量问题的复杂性上的。基于格的签名方案使用专门构建的格来包含私有短向量和使用特定类别的随机格的带误差学习（LWE）或模块带误差学习（MLWE）方案。

• 基于代码的算法：

基于代码的算法基于设计编码方案的科学，这些方案允许两个参与方在嘈杂的信道上通信。发送方对消息进行编码，以便接收方即使信道添加了有界噪声也可以解码它。已知对于某些编码方案，最佳解码算法在经典计算机上需要指数时间。此外，即使对于量子计算机，解码问题似乎也很困难。

• 基于哈希的算法：

哈希函数允许将具有千兆字节数据的重要消息计算为输入并输出为短哈希值。哈希函数广泛用于密码管理或区块链上。其中最常用的哈希函数之一，SHA256，输出一个 256 位的哈希值，与输入的大小无关。不希望哈希函数受到量子计算机的威胁，但取决于密钥的大小和量子计算的进展，基于哈希的函数可能会受到应用 Grover 算法的攻击。

• 基于多元的算法：

基于多元的算法的安全性取决于解决多元多项式系统的难度。多元密码学用于数字签名的构造，而不是用于 PKE 方案或 KEMs。

• 基于同构的算法：

这些方案的安全性依赖于恢复一对椭圆曲线之间的同构的难度。与多元方案相反，同构基础方案更适合于 PKE 方案和 KEMs。

附录 C Leap 支付应用首页截图

Graph 6 Screenshots of Leap application

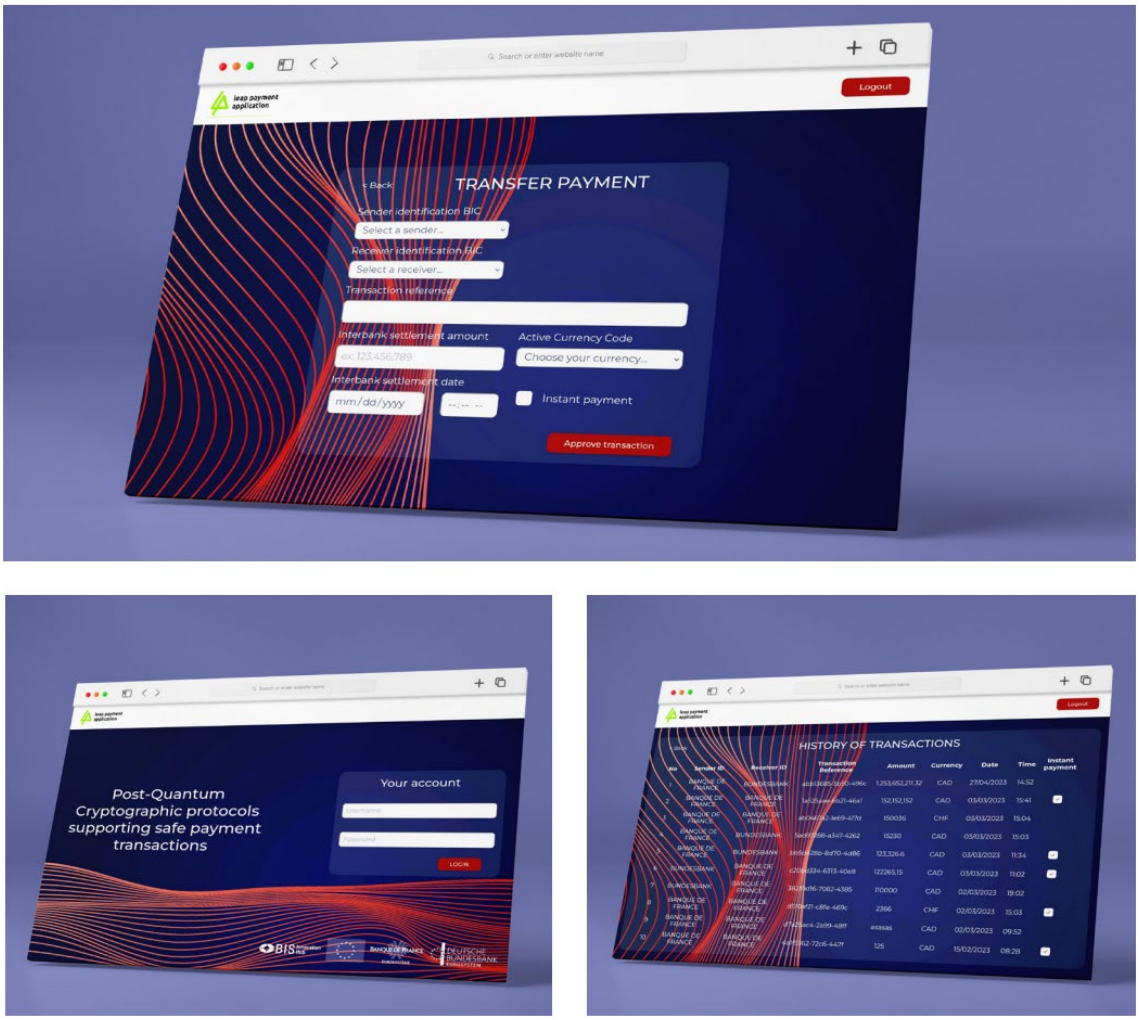


图 6 Leap 应用程序截图

附录 D 测试的技术描述

测试协议

用于测试的工具：

- 包括解决方案提供商（C-QST-STR）设计的后量子库的 strongSwan 版本。

- 使用 OpenSSL 和 Open Quantum Safe（OQS）OpenSSL 分析后量子（PQ）证书。
- 供应商量子安全库（C-QSL）。
- 实施了 strongSwan PKI 工具以生成后量子密钥和证书。

每组性能测试中的一个测试中执行的操作：

- Ping vpn ip before: KO
- strongSwan start Charon
- strongSwan init IKE
- strongSwan init nit child all
- Ping vpn after: OK
- Download 1MB file (wget): OK
- Send file 1 Mb file (scp): OK
- strongSwan Rekey chilld all
- strongSwan Rekey ike
- strongSwan Terminate IKE
- strongSwan Terminate child
- strongSwan kill Charon
- Ping after closing: KO

每个测试都在日志文件中验证了算法、安全强度类别和密钥大小，以及 strongSwan 控制命令（charon 守护程序）。

每个测试都执行了 100 次，并且是连续执行每个算法。

当在没有硬件加速的内部基础设施上测试 FrodoKEM 的 AES 版本时，性能会受到影响。

测试执行

- 在德国联邦银行和法国银行之间建立 VPN，包括生成 PQ 密钥和交换证书。
- 通过后量子 VPN 连接到 Web 门户。
- 测试不同的算法。
- 测试 VPN 的可靠性和一致性。
- 在 24 小时连接期间测试 VPN 的稳定性（自动重新密钥）。
- 在德国联邦银行一侧的云和法国银行的场地上进行测试（在两个中央银行之间

建立了 VPN，以及在它们自己的 IT 环境内）。

- 测试虚假证书。

确定的限制

时间记录是通过 Linux 命令“date”在执行命令之前和之后注册的，这意味着它不反映算法的计算时间。它显示软件完全处理操作所需的时间。

要注册计算时间需要修改 strongSwan 库。

在 strongSwan 中，某些操作是异步的，例如重新密钥。因此，无法记录重新密钥时间。尽管如此，它指出了这个特定操作对客户端没有影响。

由于 Sphincs+签名的大小，Sphincs+的数据包和片段大小已增加。

收集的数据和信息

结果显示，在每次测试中都表现出一致性，即使比较了法国银行和德国联邦银行的特定 IT 环境的结果。

图 A：在 Bank of France 系统上设置 VPN 隧道所需的时间，累积 IKE 和 CHILD 层。除了 Crystals-kyber 和 Sphincs+的组合外，这需要不到一秒钟。

图A

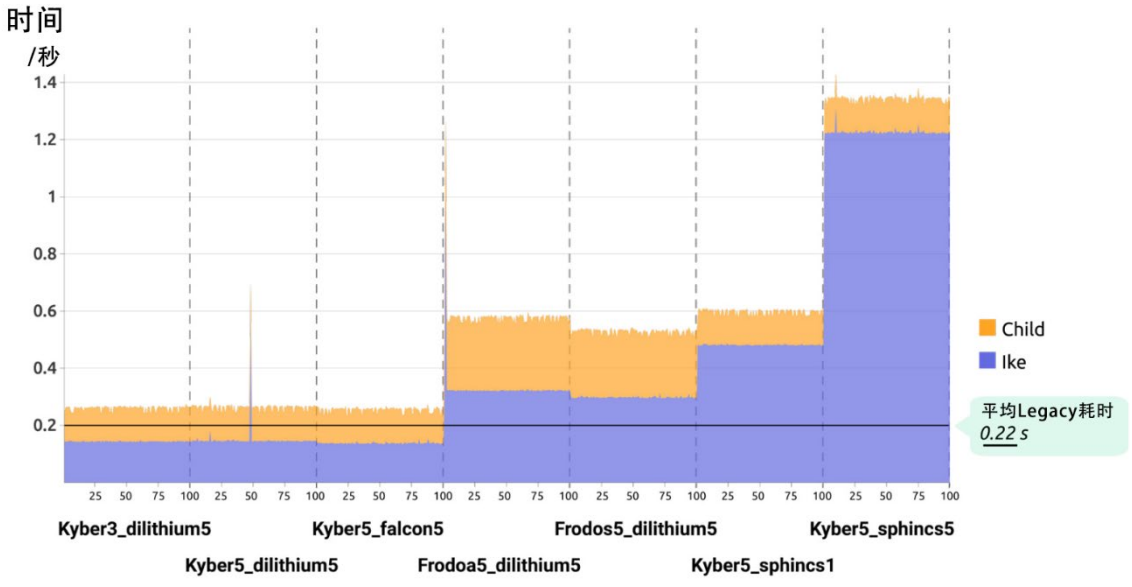


图 A

图 A 显示了每个测试的一致结果（测试了每个算法的每个组合 100 次）。

图B

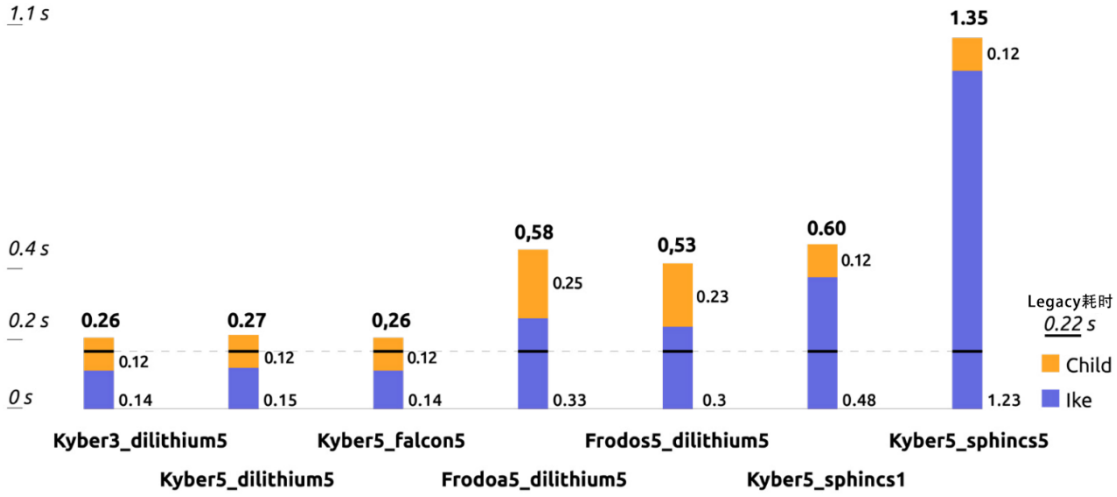


图 B

图 B 显示了使用 Sphincs+5 与另一种算法相比对性能的影响。

图C 没有 Crytal-Kyber 和 Sphincs+ 的组合的情况下
法国当地银行的时间测量

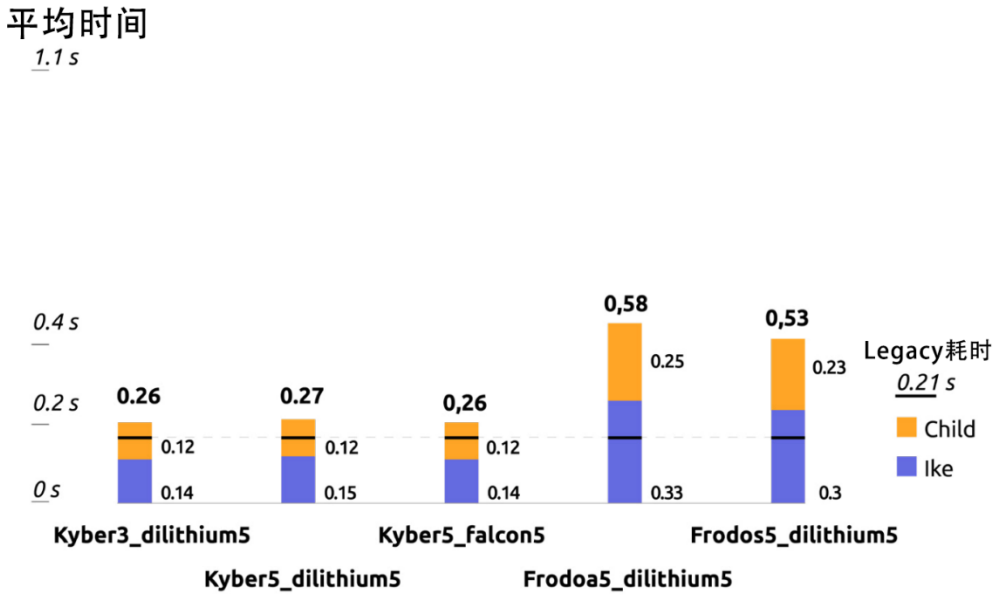


图 C 没有 Crytal-Kyber 和 Sphincs+的组合的情况下法国当地银行的时间测量

图 C 显示了 FrodoKEM 和 Crystals-Kyber 之间性能差异。

图D.1 法兰克福当地时间测量结果
比较 FrodoKEM AES 和 FrodoKEM Shake

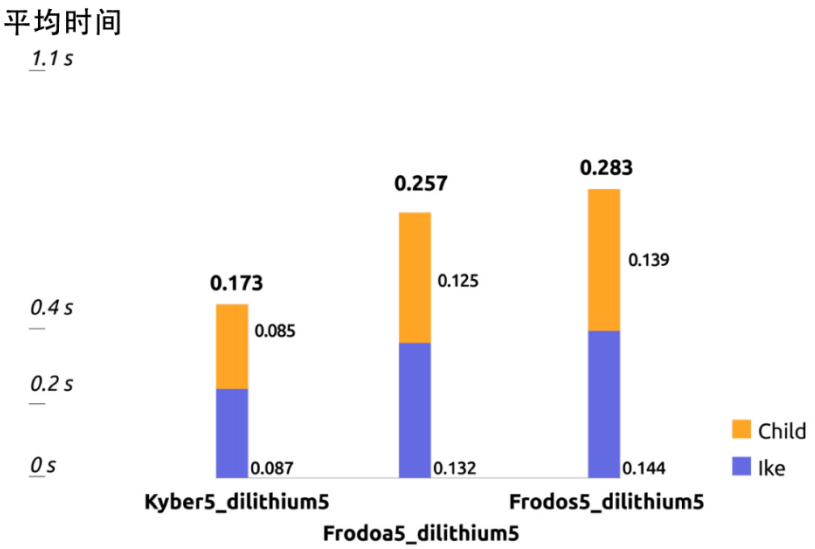


图 D.1 法兰克福当地时间测量结果比较 FrodoKEM AES 和 FrodoKEM Shake

图 D.1 显示了在德国联邦银行服务器上实现 AES 加速的测量。

图D.2

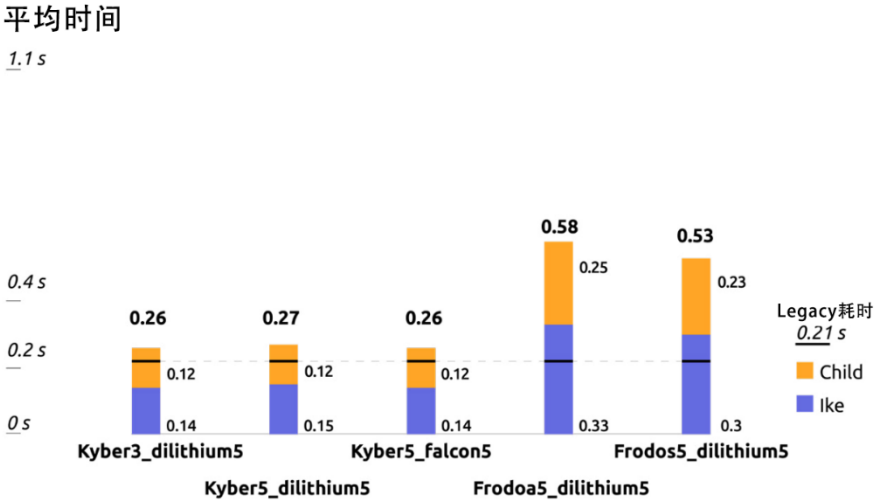


图 D.2

在图 D.2 中，没有硬件加速的法国银行服务器上进行的测试表明，Shake 比 AES 更快，因此我们可以期望，一旦 Shake 协议的硬件加速可用，将观察到更好的性能结果。

在法国银行方面，FrodoKEM AES 在 IKE 层上需要超过 0.3 秒的时间，而在德国联邦银行方面只需要不到 0.14 秒的时间。在子层也观察到了差异。

图E 发送和接收数据的平均时间

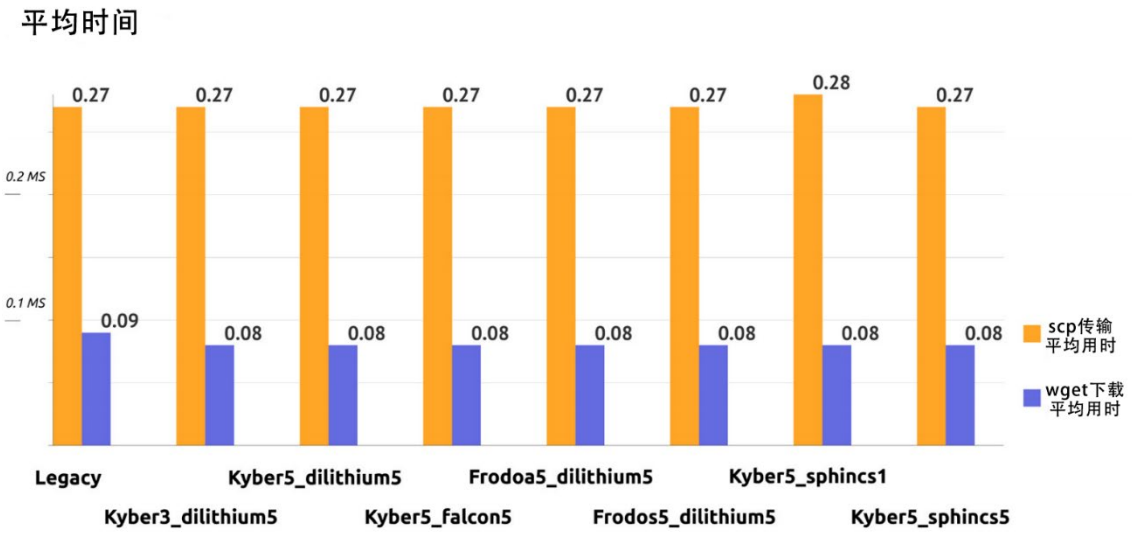


图 E 发送和接收数据的平均时间

正如预期的那样，应用后量子密码学对发送的数据性能没有影响，因为它是使用对称协议（AES-256）加密的。

表 5 OID 认证表

OID认证表

算法	OID（由OpenSSL显示）	OID（由OQS OpenSSL显示）
FALCON_LEVEL5	1.3.9999.3.4	1.3.9999.3.4
DILITHIUM_LEVEL5	1.3.6.1.4.1.2.267.7.8.7	dilithium5
SPHINCS+_LEVEL1	1.3.9999.6.7.4	sphincsshake256128fsimple
SPHINCS+L_LEVEL5	1.3.9999.6.9.3	sphincsshake256256fsimple

为了破解证书的签名，测试了一个修改过的证书。为了创建这样的伪造证书，修改了一个位。目的是确认无效证书不能被识别为真实证书。

由于此工具未配置为识别算法，因此该证书未经 OpenSSL 验证。但是，使用 OQS OpenSSL 版本可以识别证书。

技术发现

成功的测试阶段表明，实现后量子算法而没有任何严重缺陷是可能的。

密码敏捷性：

- 密钥交换由密钥提议很好地管理。
- 目前没有签名提议的机制，因此客户端必须知道所使用的算法或尝试不同的算法。

性能表现：

Sphincs+是测试的数字签名中表现最差的算法之一，时间和大小都不如其他算法。该算法目前也是唯一一个基于非格问题的算法，提供了有价值的备份解决方案。将 Sphincs+包含在库中似乎是明智的选择。

正如预期的那样，Crystals-Kyber 的性能优于 FrodoKEM，对于许多用例也是可以接受的。它可能更适合具有高安全级别要求的应用程序。

尽管 Falcon 签名的大小小于 Crystals-Dilithium 的大小，但对性能记录没有显着影响。Falcon 可能更适合需要存储大量签名的应用程序。

重新密钥是异步的，并且对于过渡数据是透明的。

项目参与者与致谢

BIS 创新中心

Raphael Auer，欧洲体系中心主任

Angela Dupont，顾问和项目负责人

Andras Valko，顾问

BIS 主题专家

David Whyte，网络安全协调中心主管

Christophe Laforge，财务运营主管

法国银行

Marc Fasquelle，高级经理

Olivier Lantran，高级经理

Benjamin Delpy，高级经理，网络安全专家

Nicolas Margaine，经理，网络安全专家

David Viatgé，顾问，网络安全专家

Erwann Legeleux，开发人员

Blandine Leal，UI 设计师

德意志联邦银行

Julia Biesen，高级经理

Thomas Kraus，高级经理

Florian Stock，高级经理

Henrieke Grimm，创新经理，敏捷教练

Max Grytz，创新经理 Vasileios Rentoumis，创新经理

欧洲中央银行

Sjoerd Van der Vaart，国际创新经理

供应商

Jean-Charles Faugere，创始人兼首席技术官

Christian d’Orival，首席营收官

Pascal Maudet，专业服务总监

Julien Prat，高级密码工程师

致谢

作者非常感谢 Christophe Laforge, Miguel Diaz, Baltazar Rodriguez, David Whyte 和该项目的私营部门合作伙伴 CryptoNext Security 对本报告的贡献。

Bank for International Settlement (BIS)

ISSN 978-92-9259-661-3 (Online)