量子计算机能够破解支撑金融稳定的密码技术

何塞·德奥多罗、迈克尔·戈尔巴尼奥夫、马吉德·马拉卡、塔赫辛·萨阿迪亚·西迪克

在古希腊，士兵们会通过在一根棍子上缠绕一张羊皮纸，然后在羊皮纸上写下文字来传递加密信息。只有拿着同样粗细棍子的人才能破译这些加密信息。这是密码学最早的应用案例之一。如今，互联网通信、数字银行和电子商务等领域的加密信息，都需要通过强大的计算机算法来为其提供保护，以防他人窥探。但是，这些我们现在还无法破解的密码可能很快会成为历史。

目前，我们的密钥主要生成于传统的数字计算机，而量子计算机所达到的最优化水平，能够破解我们今天使用的大多数密钥，且破译时间比密码生成时间更短。金融机构应当立即为网络安全系统做好未来防护，否则，恐将危及金融稳定。

量子革命

量子计算是指利用叠加和纠缠等量子现象来执行计算。量子计算机的基本单位是量子位（简称 qubit）。通常，量子计算需要通过亚原子粒子的量子特性来实现，例如，电子的自旋或光子的偏振。在我们现在使用的数字计算机中，每一个二进制位代表的值要么是 0，要么是 1，而量子位同时代表 0 和 1（或者两者的某种组合）。这种现象叫做叠加。

量子计算机有可能会让遵循经典物理学定律的数字计算机大规模退役。

量子纠缠是一对或一组量子元素之间的一种特殊联系。无论两者相距多远，改变一个元素的量子态会立即影响另一纠缠元素。

增加量子位的数量，会使量子计算机的计算处理速度呈指数级别增长。两个传统二进制位相当于一个量子位的算力；四个二进制位相当于两个量子位；八个二进制位相当于三个量子位，以此类推。想要制造一台仅有 54 个量子位的量子计算机模型，大约需要 1.8x1016 比特的传统内存。一台 100 量子位的量子计算机需要的比特数比地球上的原子还要多。而一台 280 量子位的计算机需要的比特数比已知宇宙中的原子数量还要多。

量子计算机有可能会让遵循经典物理学定律的数字计算机大规模退役。诺贝尔奖得主、物理学家威廉·菲利普斯认为，从目前的技术水平到量子计算的飞跃发展，就相当于从算盘发展到了今天的数字计算机。此前，所谓的量子优势或量子“霸权”都还只是一种理论。但在 2019 年，谷歌公司曾使用量子计算机在 200 秒内完成了一次特定的计算任务，并表示如果使用算力最强的超级数字计算机来完成同样的任务，需要花费 1 万年的时间。

机遇

复杂的计算任务就像寻找迷宫出口。传统计算机会按顺序跑完每一条逃跑路径，直到到达迷宫出口。相比之下，量子的叠加现象，使得量子计算机可以同时跑遍所有路径，大大减少求解的时间。与数字计算机相比，量子计算机的运算速度更快、准确率更高，因此，量子计算机很可能会让人类加速实现科学发现和科学创新，彻底颠覆金融市场的建模和模拟形式，有助实现机器学习和人工智能。量子计算机还可以用来模拟亚原子粒子、分子间相互作用以及化学反应，推动化学工程和材料科学的升级，设计出固态电池等新材料。此外，量子计算机还可以帮助我们了解气候变化。

量子计算机还可能会改变金融体系。在金融行业，人们一般会使用蒙特卡罗模拟，通过定价和风险模拟来预测市场行为，而量子计算机几乎可以实现实时模拟，且精度更高。借助量子计算机，我们不需要再用一些不切实际的假设来简化模型。量子计算机还可以解决最优化任务，例如，资本配置、确定投资组合或者管理 ATM 网络中的现金等，所花费的时间远低于数字计算机。量子计算机还可以加快机器学习算法的训练。每增加一个维度，数字计算机完成计算任务所花费的时间就会呈指数级别的增长。但量子计算机完全不存在这种问题。

关于风险

但量子计算机也存在风险。强大的量子机器算力很可能会威胁到现代密码技术，对金融稳定和隐私产生深远影响。现代密码技术主要基于三类算法：对称密钥、非对称密钥（也称为公钥）和哈希函数。对于对称密钥而言，消息加密和消息解密会使用同一密钥。非对称密码技术一般会使用一对相关密钥（一个私钥，一个公钥）。由一个密钥加密的消息只能由该密钥的另一个配对密钥解密。数字认证、数字签名、数据安全等领域，使用的都是这种算法。哈希函数可以将数字输入转换为一组唯一的固定长度的字节。通常，哈希函数主要用来保存密码，确认数字身份。

这些密码算法基本上都能保护数据安全。即便是现在最先进的超级数字计算机以及密码分析技术也无法快速破解它们。但是，相比超级数字计算机，量子计算机在解决数学难题时的速度会呈指数级别的增长。这不仅会让非对称密码技术

照片：GETTY IMAGES/ PICTURE ALLIANCE/ JULIAN STRATENSCHULTE

金融机构必须立即采取措施，为加密转型做好准备。

彻底丧失加密作用，而且还会削弱其他加密密钥和散列的安全性。从理论上来说，一台正常运转的量子计算机可以在几分钟内破解一个非对称密钥。其中，公钥尤其容易破解，在非对称密钥中，公钥大多数都是基于分解问题，而数字计算机很难从它们的乘积中找到两个质数，但量子计算机可以轻松做到这一点。

非对称密钥广泛应用于互联网安全通信领域。非对称加密算法被破解，将会危及金融系统所使用的连接，例如手机银行、电子商务、支付业务、ATM 提现和 VPN 通信等等。比特币和以太坊等最近大热的数字资产，它们所使用的应用程序，以及由密码保护的网页应用程序，使用的都是极易被破解的公钥加密。在这些协议中，最著名的就是 HTTPS，在世界前 100 名网站中，有 97 个使用的都是 HTTPS 协议。

对某些应用程序而言，也许已经为时太晚。我们今天认为安全的任何信息，都可以被捕获并存储起来，等到功能足够强大的量子计算机被创造出来时，就可以进行解密。事实上，对我们今天发送以及存储的几乎所有经过加密的个人信息以及金融信息，功能强大的量子计算机可以回溯解密。目前，大多数金融机构和监管机构都还没有对这些新的风险引起足够警惕。

与机器赛跑

比赛已经拉开帷幕，目前，我们已经在着手制定新的量子安全加密标准以及算法。在美国，国家标准与技术研究院正在举办一场关于开发量子安全加密算法的竞赛。希望能够在 2024 年之前出现获胜者。欧洲电信标准学会也率先展开了相关工作。美国和欧洲在这方面所做的努力，也促使其他标准制定机构采取了行动。但是，由于存在追溯风险，留给金融机构实施新标准的窗口期会十分短暂。

金融机构必须立即采取措施，为加密转型做好准备。首先，金融机构应当评估量子计算机所带来的可追溯风险和未来风险，包括已经被捕获且可能在多年后被利用的信息。其次，金融机构应当制定计划，将当前的密码学迁移到量子抵抗算法上。其中包括盘点金融机构自己使用的公钥密码，以及第三方供应商使用的公钥密码。对于易于破解的算法，我们必须将其转变为后量子密码技术。为了顺利升级算法，金融机构还应当创建加密敏捷性。尽管替换算法比过渡到后量子标准简单得多，但有关经验显示，算法的替换可能具有极大的破坏性，而且，通常需要花费数年甚至数十年才能完成。

在提高成员国的风险意识，加深对量子计算机所造成的金融稳定风险的理解，推动建立量子安全标准及实践方面，IMF 发挥着重要作用。IMF 应当鼓励成员国开展紧密合作，共同制定量子安全加密标准，保障操作性，为本国的金融行业制定加密迁移计划。

当前的量子计算机十分脆弱。热、光或振动等任何环境扰动都会将量子位元拉出它们的量子态，并将它们变成常规位元，导致计算错误。但是，距离能够以高准确率破译密码的量子计算机的出现，已为时不远。金融机构应当充分认识这种风险，及早对系统采取安全措施。毕竟，原以为牢不可破的密码被新技术破解的情况，在历史上屡见不鲜，应当加以警示。FD

何塞·德奥多罗 (JOSÉ DEODORO) 数据收集平台所有人；**马吉德·马拉卡** (MAJID MALAIKA) IMF 信息技术部数字化转型与网络安全风险首席专家；**迈克尔·戈尔巴尼奥夫** (MICHAEL GORBANYOV) IMF 战略、政策及检查部高级经济学家；**塔赫辛·萨阿迪亚·西迪克** (TAHSIN SAADI SEDIK)IMF 亚太部副处长。

本篇文章是根据 IMF 工作文件 21/71《量子计算机与金融系统：鬼魅般的超距作用》编写而成。