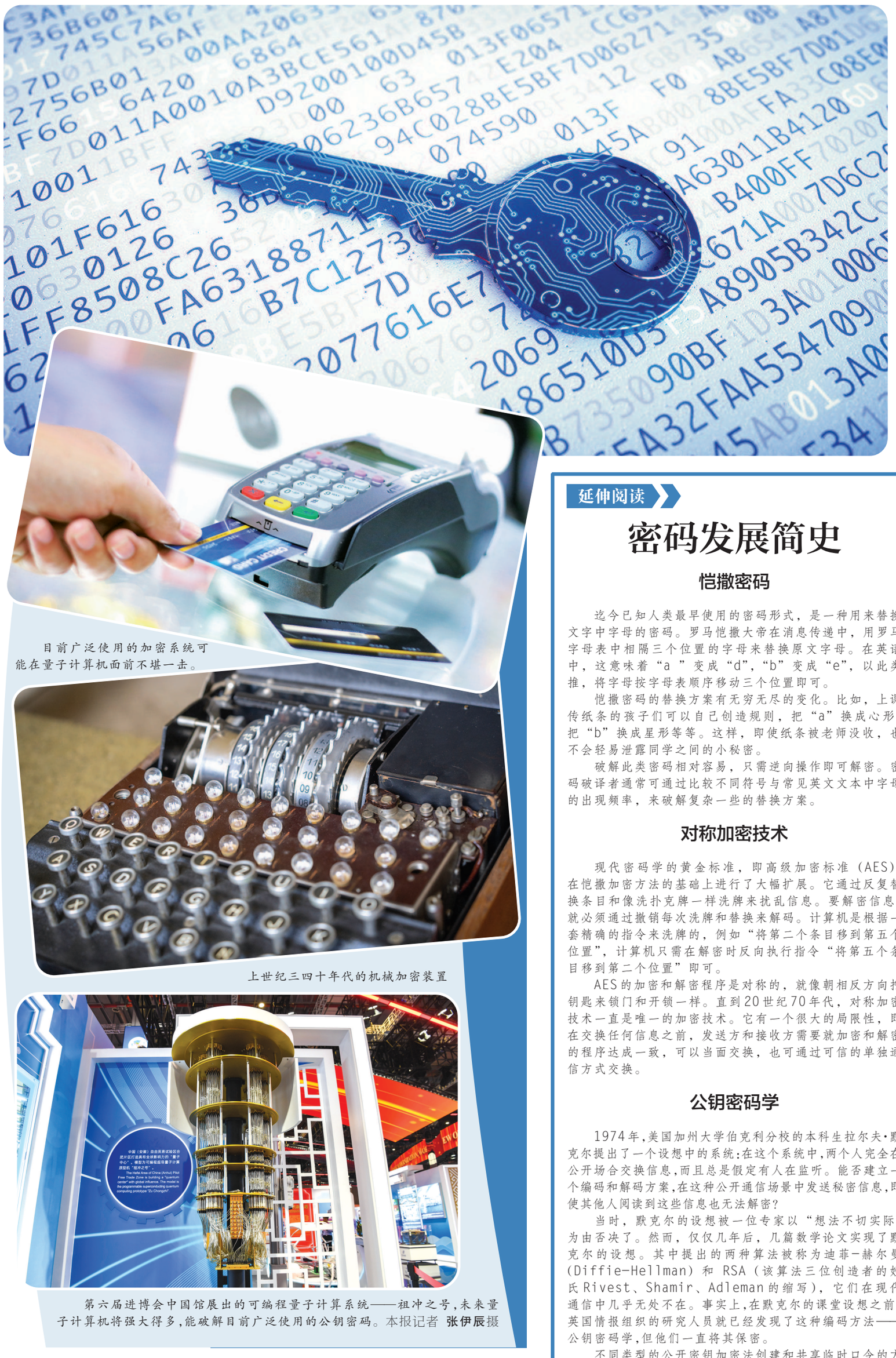
现代加密技术面临量子计算机破解威胁，今年将有三种“后量子密码”算法标准投入使用

“量子年”时钟逼近，如何保护今天的秘密？

在网络信息传输过程中，公钥密码算法是最重要的技术保障，也是互联网时代网络信息安全的基石。然而，随着量子计算机技术的迅猛发展，公钥加密技术正面临巨大安全威胁。为了提醒人们关注这一巨大隐患，数字安全专家设立了“量子年”时钟，其代表的量子计算机攻破现代密码技术的日期正在不断提前。

站在这场新技术变革的边缘，发展“后量子密码”变得刻不容缓。美国国家标准与技术研究院自2016年12月起发出后量子密码学标准化流程的公开征集，今年将有三种新算法标准投入使用，各类系统将开始向后量子密码技术切换。不过，问题似乎还未就此解决。科学家仍在不懈努力，希望“量子年”危机能像“千年虫”危机一样顺利渡过。



目前广泛使用的加密系统可能在量子计算机面前不堪一击。

上世纪三四十年代的机械加密装置

第六届进博会中国馆展出的可编程量子计算系统——祖冲之号，未来量子计算机将强大得多，能破解目前广泛使用的公钥密码。本报记者 **张伊辰**摄

■**章珂**/编译

如果有一台计算机，能在眨眼间解决当今速度最快的超级计算机也无法解决的数学问题；如果有一种技术，可以让观察者透过墙壁看到墙后的事物，或者看到最黑暗的海洋世界深处，还可以在构建完全不可攻破的网络的同时，破解对手最机密的数据——这就是量子计算机和量子技术。今后几十年甚至几个世纪内，它们将重新界定全球信息技术的未来。

当这一天到来，当前广泛使用的加密技术将在量子计算机面前不堪一击。为此，全世界的数字安全专家都在关注 “量子年”（Years to Quantum，Y2Q）时钟，它指向的时间对应的是通用量子计算机可以攻破非对称加密技术（*现代密码学的一种重要加密形式*）的预计日期。

非对称加密技术又称公钥加密技术，因能在公开场合共享密码而得名。这种加密技术可以保证网上购物时信用卡的安全，也可确保手机软件更新来自手机公司而非黑客。但是，量子计算机会让目前广泛使用的公钥加密技术形同虚设。

“量子年”时钟 传统密码“最后期限”将至

云安全联盟（CSA）量子安全工作组联合主席布鲁诺·胡特纳说，如果明天就有一台量子计算机出现，那所有人都将无法找到一种安全的方式在一起交谈，“这确实非常严重”。

胡特纳是Y2Q时钟的创造者之一。Y2Q时钟的命名是为了纪念那个可能导致计算机崩溃但最终在技术人员努力下得以避免的Y2K（*千年虫*）危机。这一危机之所以得以天衣无缝地顺利渡过，主要是因为企业和政府都在抓紧时间，及时修复了“千年虫”。

与“千年虫”危机不同的是，没有人确切知道，足以打破现有密码标准的量子计算机何时才能研制成功。目前，Y2Q时钟的结束日期被设置在2030年4月14日。但这只是一个猜测，胡特纳说，“Y2Q时钟是一个提醒，有助于引起人们的关注。”

实际上，对保密有长期需求的政府及相关机构来说，真正的“最后期限”会比Y2Q时钟设定的早很多年到来——如果今天发送的加密数据被存储起来，那么未来的量子计算机就可追溯性地解密这些信息。

美国密歇根大学的计算机科学家克里斯-佩克特说，如果一些信息需要保密20年，破解这种加密技术的量子计算机可能在20年内出现，那么现在为这些信息加密时，就不得不考虑这个问题了。

正是预见到了这种威胁，美国国家标准与技术研究院（NIST）于2016年12月发起了公开竞赛，征集“后量子”或“抗量子”密码学方案——这些密码可以在目前使用的计算机上运行，但却可以强大到连量子计算机也无法破解。

经过四轮提交和评审，NIST最终于2022年7月选定了四种算法作为“后量子密码学”标准化流程的成果，其中公钥封装机制为CRYSTALS—Kyber，数字签名方案为CRYSTALS—Dilithium、FALCON和SPHINCS+。NIST正在与研究人员合作，将获奖算法标准化，以便程序员可以此为基础，研发能够抵御量子计算机的密码技术。

专家们确信，它们肯定都是非常难以破解的，但谁也不能保证未来的量子计算机不会破解它们。

经典计算机运行的是一长串0和1，被称为“比特”，而量子计算机使用的是可以处于叠加状态的“量子比特”——通过在0和1这两种状态之间徘徊，量子计算机能够以比经典计算机快得多的速度执行某些任务。

现在的量子计算机看起来就像巨大的金色吊灯一样悬挂在天花板上——令人印象深刻，但功能却还不够强大。科学家们只能控制数量不多的量子比特进行计算。2012年，英国布里斯托尔大学的研究人员利用量子计算机推算出21是7的3倍。

尽管如此，许多专家还是认为，足以破解目前使用最广泛的RSA和迪菲-赫尔曼这两种加密算法的量子计算机，将在未来几十年内问世，不过时间线还不确定。

对于需要与量子计算机“赶时间”的密码学家来说，这种不确定性令人担忧。IBM公司的雷-哈里尚卡尔说，几乎每个行业都会涉及到信息保密和安全。比如，医疗公司需要确保他们医学研究的数据安全，而电力公司则必须保护电网免受黑客攻击，“而最坏的情况是，这些系统一旦遭受量子计算机攻击，它们就会完全暴露”。

拣选加密“基石” 新算法何以青睐格理论

每一种公钥密码学都会以一个困难的数学问题为基础。为了确保密码系统不受未来量子计算机的影响，研究人员在设计后量子密码时，需要使用那些即使量子计算机也无法在合理时间内破解的难题。

NIST发起的征集要求所提交的方案必须是可以在标准计算机上广泛实施的公钥加密算法，从而能够替代目前的RSA和迪菲-赫尔曼算法。NIST的数学家陈莉莉表示，这种新型密码必须满足人们在许多不同网络系统和设备上都能互相交流的需求。

在征集所规定的第一轮截止日2017年11月前，研究人员共提交了82份不同方案。此后一年，研究人员对这些算法进行了测试，NIST专家从中选出了26种算法在2019年1月进入下一轮测试。

在NIST的测试过程中，研究人员会试图从候选算法中不断找出漏洞。有一种候选算法使用了“基于同源性”的加密技术，这种技术已经被研究了十年，似乎很有前途。但两位研究人员注意到，利用一个已经被确认25年的数学定理就能破解这种算法——他们使用一台笔记本电脑，仅花了一个小时就完成了破解。

在被选出的四种算法中，有三种基于的都是格理论。CRYSTALS-Kyber的作者之一、IBM公司的瓦迪姆·柳巴舍夫斯基认为，选择格理论作为后量子密码算法基础很自然，因为“20多年来，人们一直在以各种形式研究这个问题”。

在格理论中，格点是由点组成的重复阵列，其中最简单的格子看起来就像一块钉板——圆点排列在一个正方形网格中。数学家认为，这种“格”是由两条基本线构成的：等长的垂直线和水平线。

假设有人在一张纸上画了两条线，并告诉你这两条线是网格的组成部分，然后再在纸上某处画一个点，你能找出离那个点最近的格点吗？

或许在一张纸这样的二维平面上最终可以找到，但如果将这个点放在三维空间中呢？人类的视觉想象力一般仅限于三维空间，但数学家却可以描述数百维的网格。在这些网格中，要找到最近的点是非常困难的。

研究人员利用这种巨型网格构建密码系统。例如，在一个1000维的网格中，从这些点中选择一个点，这个点的精确位置代表秘密信息，然后从这个点开始一点点移动，浮出网格，进入环境空间。你可以在不泄露秘密点位置的情况下公开分享新位置——寻找附近的网格点是一道非常难的数学题。

几十年来，计算机科学家一直在研究这类问题，并相信它们很难解决。但在设计新算法时，密码学家还需要考虑安全性之外的许多其他问题，并在这些问题间取得平衡，例如两台计算机需要交换的信息量以及加密和解密信息所需的计算难度。在这方面，基于格理论的密码学非常出色。有学者调侃说，格理论之于新型密码学就像一位“金发女郎”恋人——没什么太差，也没什么太好，一切都在合理的点上。

密码代际切换 “后量子”时代即将开启

然而，没有人能保证基于格理论的加密技术永远安全。为了防止数学基础研究上某次根本性突破使得“抗量子”密码全线覆灭，密码学家需要使用各种类型的算法。

NIST的竞赛征集为数字签名算法设立了一个类别。数字签名算法可以保证信息是由谁发送的，并且没有被修改过。美国加州蒙特雷海军研究生院的密码学家布里塔·黑尔解释，加密算法回答的是“我可以知道没有其他人会读到这个信息”，而数字签名回答的是“我能相信这些数据没有被修改过”。

此次，NIST选择将三种数字签名算法标准化，其中有两种基于格理论。然而，如此严重依赖单一类型的数学问题是有风险的。首先，没人能保证数学家最终不会破解它。其次，它也没有给用户提供任何选择余地——或许另一种加密技术更契合他们的特定需求。出于以上这些原因，NIST希望标准化方案可以拓展到基于格理论以外的其他数学基石上。

即使是已经被选中进行标准化的算法，也需要不断调整。德国马普安全与隐私研究所的彼得·施瓦贝是CRYSTALS-Kyber的创建者之一。第一轮提交后，研究人员发现该算法有一个小问题，随后作者就把它解决了。在下一轮竞赛中，作者又找到了一些方法来对算法进行微调。

去年8月，NIST正式发布了三种入选算法的标准化草案，第四种算法FALCON的标准化草案则会在今年发布。

目前，NIST正在制定前三种算法的标准，这些标准将逐条详细地描述程序员应如何实现这些算法。“互联网上的一切都必须有极其具体、详细的标准。否则，计算机之间就无法相互对话。”柳巴舍夫斯基说。

这些标准制定后，每个计算机系统都将开始向后量子加密技术切换。各大软件公司也得开始升级相关产品的协议，不少硬件设备也需要更换。

整个社会系统要完成向后量子加密技术的过渡，可能需要很多年。在此之前，任何使用旧式加密技术发送的信息都有可能被未来的量子计算机读取。你期望的保密时限是多久？或许，“量子年”时钟忽然就提醒你“密码过期了”。

“量子年”时钟目前被设置在2030年4月14日，其对应的是通用量子计算机可以攻破公钥加密技术的预计日期。 **（本版图片除署名外均视觉中国）**

延伸阅读

密码发展简史

恺撒密码

迄今已知人类最早使用的密码形式，是一种用来替换文字中字母的密码。罗马恺撒大帝在消息传递中，用罗马字母表中相隔三个位置的字母来替换原文字母。在英语中，这意味着“a ”变成“d”，“b”变成“e”，以此类推，将字母按字母表顺序移动三个位置即可。

恺撒密码的替换方案有无穷无尽的变化。比如，上课传纸条的孩子们可以自己创造规则，把“a”换成心形，把“b”换成星形等等。这样，即使纸条被老师没收，也不会轻易泄露同学之间的小秘密。

破解此类密码相对容易，只需逆向操作即可解密。密码破译者通常可通过比较不同符号与常见英文文本中字母的出现频率，来破解复杂一些的替换方案。

对称加密技术

现代密码学的黄金标准，即高级加密标准（AES），在恺撒加密方法的基础上进行了大幅扩展。它通过反复替换条目和像洗扑克牌一样洗牌来扰乱信息。要解密信息，就必须通过撤销每次洗牌和替换来解码。计算机是根据一套精确的指令来洗牌的，例如“将第二个条目移到第五个位置”，计算机只需在解密时反向执行指令“将第五个条目移到第二个位置”即可。

AES的加密和解密程序是对称的，就像朝相反方向拧钥匙来锁门和开锁一样。直到20世纪70年代，对称加密技术一直是唯一的加密技术。它有一个很大的局限性，即在交换任何信息之前，发送方和接收方需要就加密和解密的程序达成一致，可以当面交换，也可通过可信的单独通信方式交换。

公钥密码学

1974年，美国加州大学伯克利分校的本科生拉尔夫·默克尔提出了一个设想中的系统：在这个系统中，两个人完全在公开场合交换信息，而且总是假定有人在监听。能否建立一个编码和解码方案，在这种公开通信场景中发送秘密信息，即使其他人阅读到这些信息也无法解密？

当时，默克尔的设想被一位专家以“想法不切实际”为由否决了。然而，仅仅几年后，几篇数学论文实现了默克尔的设想。其中提出的两种算法被称为迪菲-赫尔曼（Diffie-Hellman）和RSA（该算法三位创造者的姓氏Rivest、Shamir、Adleman的缩写），它们在现代通信中几乎无处不在。事实上，在默克尔的课堂设想之前，英国情报组织的研究人员就已经发现了这种编码方法——公钥密码学，但他们一直将其保密。

不同类型的公开密钥加密法创建和共享临时口令的方式各不相同，一般都会使用数学函数来混合秘密数字。函数就像一台机器，输入数字、搅动数字，然后吐出新的数字。公钥密码学中使用的函数非常特殊，它们既要能轻松混合数字，又要让数字很难被混合。

例如，RSA密码术就是基于乘法函数及其相反的因数分解。通过乘法混合数字对计算机来说相对容易，即使数字非常大。但如果数字很大，撤销乘法或因数分解就非常困难。要解密用RSA创建的密码，需要对一个大数进行因数分解。最好的方法是过滤掉许多数字，找到其中的特定组合——这需要计算机花费很长的时间。

肖尔算法

1994年，时任美国贝尔实验室研究科学家的应用数学家彼得·肖尔发现，量子计算机可以破解任何用RSA或迪菲-赫尔曼加密的代码。

肖尔参加过一个关于使用量子计算机解决具有周期性或重复性结构的数学问题的讲座，这让他想起了“离散对数”问题。对数函数是指数函数的倒数。例如，在方程$2^x=16$中找到x。通常情况下，求对数很容易，但离散对数问题是用另一种算术形式计算对数。在这种算术形式中，人们像在时钟上一样绕圈计数。

正如RSA是基于因数分解，迪菲-赫尔曼是基于离散对数问题。计算机科学家普遍认为，经典计算机无法快速找到离散对数，但肖尔找到了在量子计算机上实现这一目标的方法。随后，他又运用类似的逻辑，证明了如何使用量子计算机快速找到大数因数。这些解决方案被称为肖尔算法。

不过，肖尔并没有想象过为真正的量子计算机编程，他只是在黑板和纸上做数学题。毕竟，量子计算机在当时似乎还是遥不可及的未来。但他的算法却对公钥密码学产生了重大影响，因为量子计算机可以利用它破解目前使用的几乎所有密码系统。 **（章珂/编译整理）**