天津大学讲席教授宗传明：

数学奠定“后量子密码”的基础

■本报记者 韩扬眉

今年，美国国家标准与技术研究院（NIST）公布了 4 项后量子密码标准，旨在抵御未来量子计算机的攻击。

科学家普遍认为，基于量子科学原理建造的量子计算机将大大超越电子计算机，而现代通信所利用的许多密码体系在量子计算的攻击下将不堪一击。抵抗这一攻击则需要“后量子密码”。

此次公布的 4 项后量子密码标准中的 3 项，是基于一个古老的数学学科——格理论。换句话说，假如量子计算机在不远的将来投入使用，格理论将是量子计算时代信息通信安全的“保护神”。

如何理解后量子密码？什么是格理论？《中国科学报》近日专访了格理论专家、天津大学讲席教授宗传明。

数学已成为现代密码学的基础

《中国科学报》：很多公众都会好奇，究竟什么是后量子密码？

宗传明：简单地说，密码是一种防范第三方窃取信息的通信保护手段。早在古罗马时期，凯撒大帝和他的将军之间就用密码传送命令，这就是著名的“凯撒密码”。他们的语言当时只有 23 个字母，情报官将命令内容的每一个字母依照字母表的次序后移固定的位置（比如 5 个位置），然后写成新的形式交给传令兵，前线将军收到命令后再由情报官还原回去。

第二次世界大战期间，密码成了某些重要战役胜负的决定因素，例如中途岛海战和击落山本五十六的座机等。为了破译密码，电子计算机应运而生。

随着计算机技术的快速发展，密码学也得到了空前发展。特别是进入互联网时代以来，密码学逐渐成为一项跨数学与计算机科学的科学技术。

现在，科学家普遍认为，不论是计算速度还是智能性，基于量子科学原理建造的量子计算机将大大超越电子计算机。许多电子计算机无法解决的科学问题对量子计算机来说易如反掌。特别是，现代通信所利用的许多密码体系在量子计算的攻击下将不堪一击。所以，科学家们在加速量子科学研究和量子计算机研制的同时，也在加速构建量子计算机时代安全的密码体系。这就是所谓的后量子密码。

《中国科学报》：我们能否设想有两个敌对国家，其中一国秘密发展了量子计算机，而另一国还在使用普通电子计算机的密码体系。如果前者利用量子计算机对后者的密码体系发动攻击，那么后者的信息安全体系将会瞬间崩溃。

宗传明：是的，就像科幻小说《量子间谍》描写的那样。

《中国科学报》：我们要研究密码学，数学是基础对吗？

宗传明：数学是最讲究逻辑、最精确的一门学问。无论是加密还是解密的过程都需要精确的规律性，而为了避免被破译，加密规律在计算上具有高度复杂性。因此，数学中的某些复杂问题成为密码学的基础是必然的。事实上，密码学的“鼻祖”凯撒密码就是基于数论中最简单的同余方程得来的。

随着电子计算机和互联网的高速发展，密码也变得越来越复杂。

1976 年，两位密码学家惠特菲尔德·迪菲和马丁·赫尔曼提出了革命性方案“密钥交换协议”，改变了原来单一密钥的设计，进而提出加密密钥和解密密钥不同的密码思想，并因此荣获 2015 年度“图灵奖”。该方案为基础数学进入密码学开启了大门。

1977 年，基于大整数分解的密码体系 RSA 诞生了，它是由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）3 位提出者的首字母而命名。早在两千多年前，古希腊数学家欧几里得就已经证明：每一个自然数都可以被唯一地分解为素数方幂的乘积。但是，具体分解一个大整数在计算上非常复杂耗时，正是其复杂性成就了 RSA 密码体系的安全性。他们由此荣获 2002 年度“图灵奖”。

随后，又有多种基于基础数学的密码体系相继被发现，比如基于椭圆曲线的密码体系、基于格理论的密码体系、GGH 密码体系、NTRU 密码体系等。

毫不夸张地说，数学已成为现代密码学的基础。

《中国科学报》：您提到的这些密码体系都能抵抗量子计算机的攻击吗？

宗传明：当然不是。

1994 年，当代著名数学家和计算机科学家彼得·肖尔首次提出了大整数分解的多项式时间量子算法，并应用于密码学。他的工作表明，在量子计算时代，基于大整数分解和离散对数问题的公钥密码体系将被攻破。

随着量子科技的快速发展，以及多项广泛应用的密码体系在量子计算环境下被逐一攻破，各国科学家意识到，量子计算机可能给信息安全带来危机。

2016 年，NIST 向全世界征集抵抗量子计算机攻击的后量子密码标准。历经 4 轮遴选淘汰，2022 年 7 月 5 日 NIST 公布了 4 项后量子密码标准。其中 3 项基于格理论、1 项基于编码理论。

基于格理论的后量子密码标准

《中国科学报》：什么是格理论？

宗传明：1831 年，高斯提出了格的概念。它是 n 维空间中最有规律的离散结构。历经高斯、厄尔密特、闵科夫斯基、西格尔等大数学家近两个世纪的系统研究，格理论已发展成为数论、代数与几何相交叉的一个重要数学分支。

在这一领域中，2021 年洛瓦兹由于 LLL 算法的工作荣获“阿贝尔奖”，今年 7 月维亚佐夫斯卡由于 8 维堆球和 24 维堆球的工作荣获“菲尔兹奖”。三维格理论奠定了晶体学的基础，高维格理论则成就了 NIST 公布的 4 项后量子密码标准中的 3 项。

《中国科学报》：为什么格理论独占四分之三？格密码能抵抗量子计算攻击吗？

宗传明：一个给定的格必定有最短的向量。早在 100 多年前，闵科夫斯基就已经给出估计。给定一个格，空间中的任一点一定有一个最近的格点。但要找到一个好的算法来确定格的最短向量（SVP）或离给定点最近的格点（CVP）却极其困难。

而格密码在量子计算环境下的安全性都可以递归到这两个数学问题的计算复杂度上。20 世纪 80 年代，众多著名数学家深入系统的研究证明，在电子计算机环境下求解这两个数学问题是非常困难的。

格密码最早由美国数学家米克劳斯·阿杰泰于 1996 年提出。由于上述数学家们的理论工作，格密码显然能够抵抗电子计算机的攻击。那时，彼得·肖尔的量子算法刚刚被提出，在其他密码体系纷纷被量子算法攻破的情况下，世界各地的密码专家更是使出“洪荒之力”试图利用量子算法攻破格密码，特别是在美国开始征集后量子密码标准以来的 6 年。

其实，在过去的近 10 年当中，每届世界密码学的三大会议（美密会、欧密会和亚密会）都会设一个分会专门研讨格密码。但是，人们至今没有找到有效的量子算法攻击格密码。数学家和密码学家反倒形成了一个共识（猜想）：不存在多项式时间的量子算法能在多项式误差下求解格的最短向量问题和最近格点问题。

换句话说，格密码是能够抵抗量子计算机攻击的。

中国数学家需尽快迎头赶上

《中国科学报》：1994 年还没有量子计算机的模型机，当时彼得·肖尔为什么能提出量子算法？人们又如何检验一个密码体系是否可以抵抗量子计算机的攻击？

宗传明：在科学技术的发展过程中，有时候是技术推动科学，而大多数情况下是科学推动技术。在没有公开运行的量子计算机模型机的情况下，彼得·肖尔依照量子科学的原理理论设计出量子算法，而其他数学家和密码学家也是如此设计攻击算法，来检验一个密码体系能否抵抗量子计算机的攻击。

假如把计算机比作一个人，硬件如同躯体，软件则如同智力。在物理学家和计算机工程师致力于设计建造量子计算机的同时，数学家和计算机科学家也在努力赋予它智能，并且防范其智能可能给信息安全带来的破坏。

《中国科学报》：在当下复杂的国际环境下，我们该如何应对量子科技可能带来的挑战？

宗传明：我不懂物理，也不懂计算机，只懂一个很小的数学分支——格理论。碰巧格理论成了后量子密码的数学基础，我有责任向公众科普这一可能的危机，以唤起大家的共识和重视。

欧美构建后量子密码标准是基于大批一流数学成果，没有“弯道超车”，也不靠“黑科技”，完全是水到渠成。

我国现代科学技术起步晚，现代数学进入中国仅一个多世纪。但大家已有共识，要摆脱被“卡脖子”困境，成为科技强国，就要有一流的基础科学，而一流的基础科学必须有一流的数学。

在量子计算机已成为各国竞争潜在战场的今天，我国急需一批数学家尽快迎头赶上，搞懂欧美数学家为后量子密码所奠定的基础，与我国的密码学家密切合作，共同打造我国的信息安全之盾。

集装箱

我国首个“三抗”优质杂交稻品种通过国审

试点种植的“科贵优 4302”。 李望君 / 摄

本报讯（记者王昊昊 通讯员邓力华）近日，记者从中科院亚热带农业生态研究所（下称亚热带生态所）获悉，由该所申报的杂交稻新品种“科贵优 4302”通过国家农作物品种审定委员会审定。

病虫害是影响水稻高产稳产的重要因素之一，水稻常见的病虫害有稻瘟病、白叶枯病及褐飞虱等。“水稻资源中本身就具有稻瘟病、白叶枯病及褐飞虱的抗性基因，培育抗稻瘟病、抗白叶枯病、抗褐飞虱的水稻品种，是防治这 3 种病虫害最经济、有效的方法。”亚热带生态所水稻分子育种团队负责人肖国樱表示。

“科贵优 4302”（国审稻 20220226）由亚热带生态所领衔，与广东省农业科学院水稻研究所和中国种子集团有限公司合作选育。它在长江中下游稻区晚稻区试中表现为中抗稻瘟病、中抗白叶枯病、中抗褐飞虱，品质达到部标优质三级，比对照组增产 1.9%，是我国通过审定的第一个抗这 3 种病虫害的优质水稻品种。

海洋经济监测智慧管理平台在青岛正式上线运行

本报讯（记者廖洋）近日，2022 中国海洋经济博览会上，青岛市海洋发展局举行了“青岛市海洋经济运行监测与评估智慧管理平台”发布会。该平台为全国首个上线运行的海洋经济运行监测评估关键数据全链条全流程治理和应用平台。

据介绍，该平台以“海洋经济运行监测评估关键数据全链条全流程治理和应用”为核心，构建了“经济总览”“区域透视”“产业透视”“决策评估”“海洋项目”等五大数字化应用场景。五大场景通过对涉海企业联网直报数据、政务开放数据和互联网大数据进行集成和挖掘，实现海洋经济数据空间可视化、海洋产业全景透视、海洋经济统计数据初步测算、海洋项目“一张图”管理等功能。

青岛市海洋经济运行监测与评估智慧管理平台于 2020 年底建设完成，并通过验收。2021 年平台启用试运行。本次发布会是平台完善相关功能后的首次亮相，标志着青岛市海洋经济运行监测与评估智慧管理平台正式上线运行，将为推动青岛市海洋经济运行监测与评估工作迈向数字化发展新阶段提供技术支撑，助推引领型现代海洋城市建设。

科大讯飞 AI 研究院副院长高建清：

一款好用的智能办公本是怎样炼成的

■本报记者 赵广立

11 月，科大讯飞推出了一款大尺寸的墨水屏办公本——讯飞智能办公本 MAX，被认为是“人工智能语音技术与墨水屏手写的完美结合”。作为智能办公本 MAX 的第一批体验用户和智能办公本家族系列背后的技术支撑者，科大讯飞 AI 研究院副院长高建清称，这是科大讯飞“用核心技术打造的核心产品”“一款好用的智能办公本”。

打造一款好用的智能办公本，需要集成多少核心技术？高建清在接受《中国科学报》专访时作了详细回答。

“我们认为智能办公本主要有三大功能——会议记录、手写书写、阅读 / 听书，讯飞智能技术主要关注这些功能的实现。”高建清说。

它首先要“听”得懂——不仅要能听懂普通话，还要能听懂方言、外语，并尽可能准确地将其转成文字。这需要语音识别、方言识别、机器翻译等技术。据了解，智能办公本 MAX 支持粤语、四川话、河南话等 12 种方言识别，英、德、日等 7 种外语和两种民族语言的实时互译。

如果是多人会议，使用场景变得复杂，它还要在多人发言的会议中区别发言人，以便更准确地识别。这要用到声纹识别、多麦克风阵列等技术，实现“说话人分离”。

在阅读 / 听书的使用场景，智能办公本 MAX 要会“读”书。高建清告诉记者，为了减少 AI 读书的“机械感”，讯飞在语音合成技术上下足了功夫，打造了 AI 模拟真人朗读功能，并且支持声音复刻、定制私人声库，让用户听得自然舒适。

另外，讯飞希望将智能办公本 MAX 打造成为“科研人员的第一款智能办公本”，因此专门配齐了专业文献阅览功能——办公本尺寸与 A4 纸张大小相近，阅览视野几乎与纸质文献无异；AI 排版优化，对 PDF 文件爱好者非常友好。更重要的是，阅览文献过程中要批注圈画、记笔记、写心得，Wacom 磁吸电磁笔和墨水屏相得益彰，更有 OCR 识别技术助阵中英文及符号图文转换。高建清说，智能办公本 MAX 写字和擦除仅 23 毫秒延迟，人类肉眼难以察觉，这背后是工程技术上的精益求精。

高建清告诉记者，讯飞智能办公本 MAX 承载着科大讯飞多项不断迭代精进的智能技术。同时，讯飞会不断根据产品端反馈的问题，优化技术。

他举例说，一开始，技术端小伙伴觉得“离线转写”这个功能并不太重要，但产品端对这一功能的需求反馈却非常高。“后来我们结合边缘计算技术，采用高性能计算处理单元（如 NPU）逐步实现了这一功能，现在几个小时的离线转写的准确率非常高，并且通过极致的工程优化，我们解决了办公本由于持续运算导致设备发烫的问题。”

另一个代表性功能是“说话人分离”。高建清说，复杂场景下的语音识别在业内一直都是个难啃的“硬骨头”，这要求智能终端有准确判断不同说话人所处方位、区分不同声纹的能力。对此他们除了在优化麦克风阵列上做文章、提高声纹识别能力外，还开创性引入自然语言处理技术，利用语义信息分析辅助 AI 更准确地区分说话人。

通过将语音识别与墨水屏手写相结合，科大讯飞集成多种技术打造了一款可以同时保存语音和手写两种记录的智能办公本，这在高建清看来不仅是效率的提升，同时标记着这个时代。他说，技术探索没有止境，针对智能办公本的优化改进将持续。“下一步，我们将借助技术和工程，不仅帮助人们保存信息，而且协助大家更高效地挖掘信息背后的价值，真正打造一款无可替代的时代精品。”

按图索技

不接触测心电图

本报讯（见习记者王敏）中国科学技术大学吴曼青院士团队陈彦教授、孙启彬研究员等在无线人体感知研究中取得重要进展，实现了基于毫米波雷达的非接触人体心电图实时监测，突破了百余年来心电图仅能通过接触式传感器获取的局限。相关研究成果日前发表于《IEEE 移动计算汇刊》。

陈彦介绍，通常心电图监测需要一直将电极连接到人的皮肤上，以捕捉反映心脏状态的电活动变化。而新方法中，被测者不需要佩戴电极，也不需要去除衣物，以无感的方式完成心电图监测。

陈彦等人利用心脏电活动与机械活动是心脏活动同源不同表征的特性，使用毫米波雷达以非接触形式测量体表的心脏机械活动，提取四维心脏机械活动信号，并利用深度神经网络模型构建心脏机械活动与电活动之间的非线性映射关系，通过数据驱动的方式求解该域转换问题，最终还原出心电波形。

研究人员在 0.5 米非接触感知距离、不同生理状态和人体相对静止躺姿约束的实验设计下，对 35 名实验对象实现了非接触心电图监测。

“非接触心电图实现了时间中位数精度小于 14 毫秒、形态中位数精度大于 90%的监测性能。”陈彦说，此外，该方法的监测结果支持对心血管疾病诊断中的关键指标——心跳间期的稳定监测，其误差在 9 毫秒以内。该指标对心律紊乱、心肌梗死等疾病诊断具有重要价值。

相关论文信息：https://doi.org/10.1109/TMC.2022.3214721

毫米波雷达非接触心电图实时监测。 中国科学技术大学供图

生物控害！不同植物品种间作好处多

■本报记者 李晨

华东理工大学研究员万年峰课题组与国内外科研人员合作，提出了利用植物基因多样性调控有害生物的下行控害假说。相关研究近日发表于《自然－通讯》。

基于该假说，在农业、森林、草原、湿地、海洋等生态系统增加植物的基因多样性，就能提高植物生产力和品质，增加天敌昆虫，控制和减少病虫害发生。

基因多样性与控害效果

“植物是人类赖以生存与发展的物质基础。”论文通讯作者万年峰说，保护植物免受有害生物危害，即植物保护工作，是科学家和决策者需要关注的课题。

目前，利用生物多样性防控植物有害生物（生物控害），是安全可行的生态环保技术途径之一。

生物多样性是生物及其与环境形成的生态复合体，以及与此相关的各种生态过程的综合，由遗传（基因）多样性、物种多样性和生态系统多样性 3 个层次组成。其中，物种多样性指群落中物种的数目和每一物种的个体数目。

“此前我们团队研究发现，增加田块中植物物种多样性，如在水稻田旁边种上大豆、玉米等农作物，可以有效实现控害。”万年峰说，但在实际生产中，很少看到不同品种的水稻种在一起。这促使他们思考，假如将不同水稻品种、不同马尾松品系或者不同高羊茅品种混种在一起，会不会也有控害效果。

万年峰解释说，同一个物种内的不同亚种、品种等种群的多样性，其实就是遗传（基因）多样性，是生物体内决定性状的遗传因子及其组合的多样性。

然而目前基于基因多样性的控害理论和假说相对较少。

间作两个品种足可增强控害效果

鉴于此，研究团队整合了涵盖全球农业、森林、草原、湿地、海洋等生态系统的 413 个植物多基因与单纯基因的比较试验数据。

“我们筛选了那些用多基因类型和单基因类型做比较的实验结果。”论文共同第一作者、首都医科大学付利宛博士说，例如，实验组为扬麦 3 号、扬麦 4 号和扬麦 5 号间作，对照组为单一品种如扬麦 3 号，两组实验的对比结果作为该项研究采纳的一组数据。

结果显示，在所有生态系统中，增加植物的基因多样性，可提高捕食性和寄生性天敌的丰度和捕食寄生率，降低植食性昆虫、杂草以及植物病害、线虫的侵害，提升植物产量与品质。

论文作者、复旦大学教授胡跃清介绍，进一步研究发现，就农业、森林、草原等生态系统中的控害效果而言，增加一种基因型和增加两种以上基因型并无显著差别。也就是说，在这些生态系统中，同一个田块间作 2 个品种和间作 3 个及 3 个以上品种，其控害效果差异不明显。

该研究提示，农林草种植者、海洋植物种植者、政府决策者可通过植物间套作实施植物基因多样化种植，如不同水稻品种、林木品系或牧草品种间作，充分利用基因多样性增强植物对病虫草害的抵抗能力以及巧用天敌自然控害的本领。

万年峰强调，这种间作不需要种太多品种，增加一个品种即可。间作过多的品种不但不会增加控害效果，而且不利于机械化种植，增加种植成本。

这项研究表明，增加植物的基因多样性，与增加植物的物种多样性一样，也能够起到在生态系统中控害的效果。

相关论文信息：https://doi.org/10.1038/s41467-022-35087-7