实现历史突破，复旦斩获全国密码技术竞赛特等奖

▶ 赵运磊教授介绍项目成果

◀ 特等奖获得者：郑婕妤 沈诗羽 赵一凡

国内级别最高、影响力最大的密码技术大赛第六届全国密码技术竞赛11月27日落下帷幕。我校计算机科学技术学院赵运磊教授带领两支学生队伍勇夺特等奖1项、二等奖1项，实现了我校在该项比赛中的历史突破。

从国家安全到日常生活 大国重器护卫网络和信息系统安全

密码技术是网络空间安全的关键基础技术，是国之重器。“没有网络安全，就没有国家安全”，密码技术与核技术、航天技术并称为“国家安全三大支撑技术”。

密码算法的运用，看似离生活遥远，其实就在我们身边。每一次手机支付，每一笔网银转账，正在走入百姓生活的数字人民币，背后都有密码技术的“保驾护航”，融入我们日常生活的点滴进程。而党政军外交领域的密码机要保护更是国之“命门、命脉”。

此次赵运磊带教项目斩获特等奖，其核心技术“抗量子密码算法设计”是我国计算机加密算法防护升级的有效手段，堪称网络安全的“护国神盾”。

面对量子计算机快速发展对现役公钥密码技术的颠覆性影响，研发和尽快部署抗量子计算机攻击的新型密码技术是密码代际发展进化的战略方向，是国内外密码技术学术界和产业界的研究热点，我国科协也将抗量子密码技术列为亟待解决的60项科技难题之一。如何抓住密码技术这一代际发展进化的窗口机遇期，研发出性能超越美国和国际同类水平的密码系统，服务国家重大战略需求一直是赵运磊课题组所关注和努力的方向。

师生同心，勇夺特等奖

“为了这次比赛，我们团队准备了近一年。更是五年多来持续不懈科研的结晶。我们研究成果不仅涉及算法数学理论基础、算法设计优化及相应的证明，同时提供了软件和硬件优化实现。”完备成体系的项目成果，同样也得益于一个汇聚了来自各学院、各年级、各研究领域优秀学生的复合型团队。

团队分工有序。曾获第五届全国密码技术竞赛一等奖的沈诗羽负责软件，微电子学院的赵一凡负责软硬协同，沈诗羽和郑婕妤一起负责硬件。他们进入团队时，有的是硕士研究生，有的是博士，有的当年甚至还是本科生。

赵运磊称这支队伍“是国内极少数把抗量子密码研究中的数学、算法、软件硬件融合到一起的团队”。特等奖，实至名归。

教研相融，行“三全育人”

“其实没有非常专门准备这个比赛”，赵运磊认为，科研是持之以恒、自然而然的成果而不仅仅是为了一个奖项，“时间精力花销巨大，只为冲个奖，这与我本身科研理念所偏离。”

赛事要求参赛作品必须是未发表的、未公开的首次取得的科研成果。因此，赵运磊团队把备赛过程融入日常科研教学。一块奖牌，绝非他们的最终目标。

在研究过程中，学生们收获灵感、成果并发表论文，不仅培养了他们的科研能力，更培养了他们的科研兴趣，奠定了坚实的研究基础。是学校积极推进“三全育人”，全力服务学生成长成才的生动诠释。

发挥特长，融汇交叉学科

此次比赛，赵运磊充分运用学校各学科交叉融合的优势，结合数学、计算机软硬件和微电子等多种综合力量，打造交叉融合团队，其中有硕士、卓博的优秀学生，也有本科生中的佼佼者，他们有的算法能力比较强，有的软件硬件实现能力比较强，而有的工程设计能力比较强。如何有机融合成一个体系一直是他指导团队重点考虑的问题。

整个备战过程综合数学和计算机算法的框架以及具体的调优，软硬协同的实现，将近一年拿出了两套成果：格基密钥封装算法优化与软硬件高效实现、Aigis-ake密钥交换协议的高效实现。相对于国际上美国标准化局NIST正在推进的后量子密码标准竞赛的决赛明星算法Kyber，在增强安全性、降低错误率的同时，效率提升约30%，在综合性能上全面超越了美国NIST后量子密码标准明星算法Kyber，发展的优化技术也可以应用于其它Kyber的变体算法。

“如何将各学科捏合到一起，就像作曲家把各个音符组合到一起发出最强音，是困难比较多的点”，整个项目从指令集到硬件的实现，如何发挥交叉优势，是赵运磊无时不刻在解决的问题。

复旦在密码领域具有悠久的历史和优良的传承，先后培养了蔡吉人、林永年、黄民强等密码学院士。赵运磊坦言，正因为在复旦，得以利用顶尖综合性大学的优势，调动各学科力量，“让工科有机地结合起来，才使这件事大有文章，让我们能在此次大赛中创造历史佳绩”。

密码学并不复杂神秘 关键要有百折不挠的韧劲

赵运磊在博士后出站后，主要聚焦计算复杂性理论，随后转向零知识、认证密钥交换、数字签名、提出匿签密新型密码原语。多项研究成果被密码学国际著名教材多个章节单独介绍。在五年前转到抗量子密码研究。他说：“每一次转变，就像又读了一个博士。”2007年，他参与了姚先生和王小云院士主持的973项目，后来在密码学领域与姚期智院士合作了多篇论文。赵运磊表示：姚先生是对他一生学术影响最深远的科学家。

密码学并不复杂神秘，赵运磊认为“这是我团队持之以恒要做的事情”，他希望通过从事相关领域的研究，把国家需要和科研结合在一起，同时培养后继人才，为国家的新一代抗量子密码技术贡献复旦智慧、上海经验——这是复旦机要密码研究的目标和使命。

比赛结束，赵运磊团队又回归实验室，继续工作。这日常的背后，是一代代复旦密码人为党和国家的密码机要工作做出的卓越贡献，融入复旦百年红色基因。 文/汪祯仪 王泽群等

■ 背景链接

全国密码技术竞赛主要面向全国高等院校和信息安全企业。2021年第六届竞赛历时三月，共有来自全国60个高校和企业、333个团队、1332名选手参加。123支队伍晋级总决赛，分成六组评比，每组推荐1支队伍角逐最终的特等奖评选。本届竞赛设置2个特等奖名额。

数学学院六位教师入选“金锝特聘教授”

数学科学学院“金锝特聘教授”聘任仪式11月23日举行，六位教师入选“金锝特聘教授”。这是学院首个冠名教授项目，支持潜心科学研究和教书育人的教师成长为学科领军人才，优先支持创新能力强、发展潜力大的优秀青年人才。首批“金锝特聘教授”设置6个岗位，聘期三年。由个人提出申请，经金锝特聘教授遴选委员会根据“好中选优、宁缺勿滥”的原则审核推荐，报学校人事处批准聘任。

来源：数学科学学院

光子晶体课题组实现光束在垂直入射情况下的横向位移

物理学系/应用表面物理国家重点实验室光子晶体课题组近期提出了利用光子晶体的动量空间偏振场和动量空间几何相位梯度操控光束实空间偏振依赖位移的新机制，并在实验上直接观测了垂直入射光束的线偏振依赖的横向移动。相关研究成果以《通过控制动量空间几何相位实现正入射光束的横向位移》（“Shifting beams at normal incidence via controlling momentum-space geometric phases”）为题，在线发表在《自然通讯》（*Nature Communications*）。

光子晶体因其特殊的周期结构和对光的调控作用面在新型高效光学器件方面呈现出广泛的应用前景。该项研究工作提出了利用光子晶体调控光束实空间位移的新机制，即利用光子晶体动量空间的偏振场去调控光束的动量空间相位梯度，进而实现对光束实空间的位移调控。这个工作扩展了光子晶体对光束的调控维度，进一步证实了光子晶体动量空间的偏振结构可以作为一个有效的光场调控新自由度。

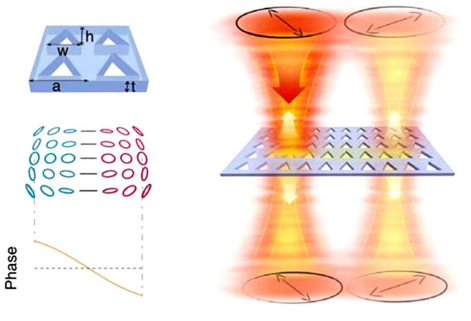
光束在介质界面处发生反射或者透射时，除了几何光学描述的传播方向的改变，同时还可能伴随光束重心位置的移动。光束的实空间位移反映了光束在界面处非凡的传播行为，蕴涵了丰富的物理内容。常见的光束位移主要分为两类：一类是位移方向沿着入射面内的位移，被称为Goos－Hänchen位移，其位移的产生是由于Fresnel系数的角度色散；另一类是位移方向垂直于入射面的位移，被称为Imbert－Fedorov位移，这类位移体现了光的自旋轨道相互作用，其位移方向一般是圆偏振依赖的。以往观察到的光束位移一般都非常小，位移大小远小于光束的束腰半径，需要精密的探测方法才能测量到，并且不能在不改变光束传播方向的同时实现对垂直入射光束的位移。进一步探索光束位移的物理机制，探索有效的调控方法，是推进光束位移调控和应用的关键。

基于动量空间和实空间互为倒易空间的这一关系，研究团队得出光束在界面处的实空间位移是由于光束的动量空间引入了额外的相位梯度。在该项工作中，研究团队提出利用面内反演对称性破缺的光子晶体来调控动量空间相位梯度。通过破坏四方光子晶体的面内反演对称性，会出现左右镜面对称分布的偏振场，对于这样的偏振场，通过入射线偏振入射的交叉极化转换，相对于入射光偏振正交的光束部分，其动量空间便引入了几何相位梯度。如此，便可对垂直入射的光束实现位移调控。

研究团队制备了理论设计的光子晶体，实验上直接测量到了光束通过光子晶体交叉极化转换在动量空间引入的相位梯度，进一步直接观察到了垂直入射的光束在光子晶体上的实空间位移。实验测量得到的光束位移大小和光束的束腰半径接近，切换入射光和交叉极化偏振的偏振方向，光束的位移方向也切换到相反方向。

文章链接（https://doi.org/10.1038/s41467-021-26406-5）。

文/刘岍琳



■ 利用光子晶体引入动量空间相位梯度以及垂直入射的光束在光子晶体发生位移示意图