

1101  
0011  
0100  
0011  
0100  
1001  
0101  
1110  
0101  
0101

HASH  
FUNCTION

a04558c  
1523465  
878e6a8

近日，第27届“欧莱雅—联合国教科文组织世界杰出女科学家奖”颁奖典礼在位于巴黎的联合国教科文组织总部举行。5位科学家因其在自然科学、数学和计算机科学领域的开创性研究以及在解决当今重大挑战方面作出的卓越贡献获得表彰。其中，中国科学院院士、清华大学高等研究院教授王小云荣登榜单，成为该奖设立以来第九位获奖的中国科学家。

从通信协议到电子支付，从网络加密到人工智能安全……现代密码是保障网络安全和信息安全的核心技术，成为数字时代安全体系的基石。与密码打交道数十年，王小云凭借一系列突破性研究成果，为中国在国际密码学领域赢得一席之地。

“我的工作就是专注于密码理论研究，包括密码分析数学理论和密码设计数学理论。”在获奖感言中，王小云说道，“我希望通过密码学界的共同努力，让我们的数字世界更安全、社会更和谐、人们生活更幸福。”

# 王小云：攀登世界密码学巅峰

本报记者 刘 峥

## 破解全球顶级密码算法

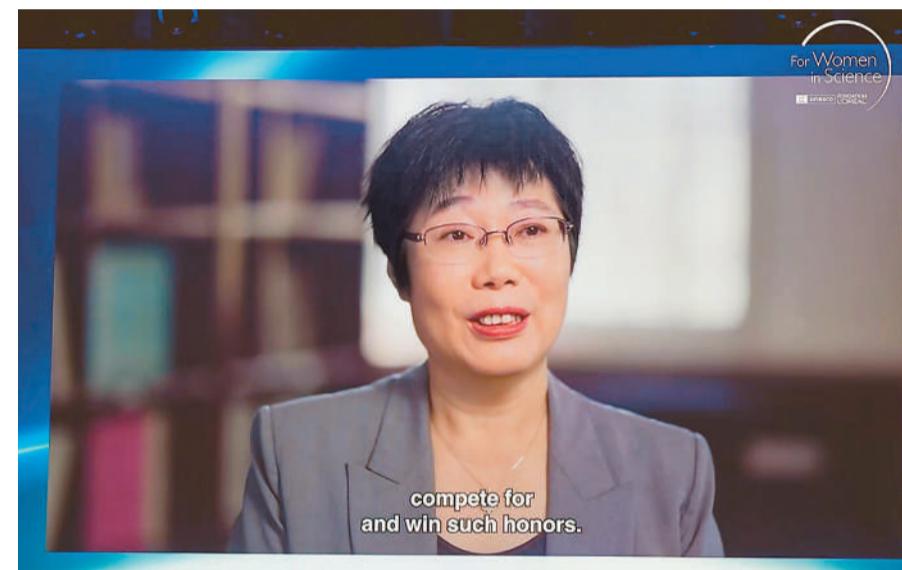
联合国教科文组织在今年评奖的新闻公报中写道，王小云在密码学及其相关数学问题领域的重大研究成果，为安全的数据通信和存储提供了坚实保障。她的突破性研究揭示了被广泛应用于通信协议的哈希函数所存在的根本性漏洞，推动了新一代哈希函数标准的制定。如今，这些标准广泛应用于银行卡、计算机密码与电子商务领域。她的变革性研究成果激励着众多女性投身数学与网络安全研究。

密码学是研究信息加密与解密技术的学科，旨在保障数据的保密性、完整性和可认证性。在王小云看来，“密码学的目的就是保障信息世界是安全的，保护我们的信息隐私、银行信息等敏感数据，实际上我们生活中有很多密码的产品。”

1983年，王小云考入山东大学数学系，师从中国数论学派的重要代表，在“哥德巴赫猜想”研究中取得突出成就的中国科学院院士潘承洞。在导师的引导和建议下，她将研究方向由纯理论的解析数论，转向当时尚属新兴的应用领域——密码学。

上世纪90年代的国际密码界，MD5和SHA-1几乎是全球网络安全系统的“标配”，广泛应用于银行、政府、军事、电子商务等系统。作为两种哈希函数算法，它们的作用就像是给一份电子文件生成“指纹”——哪怕只改动了文件中的一个字母或像素，生成的指纹也会完全不同。

2004年在美国举行的国际密码大会上，王小云带领团队公布了对MD5等算法的攻击路径与完整验证，这一成果震惊了全球密码学界。1年后，她又同团队一起，进一步攻破了被称为“白宫密码”，当时广泛应用于美国政府、金融、国防等高敏感系统的SHA-1。这一研究成果直接推动了全球新一代哈希函数标准的制定进程。



王小云通过视频在颁奖仪式上发布获奖感言。

主办方供图

## 密码为国家服务

密码研究是一个需要“坐冷板凳”的领域，需要极大的耐力和钻研精神。一种密码算法的破解往往需要花费10余年甚至更久的时间，即便如此，成功率也只有1%左右。破解MD5时，王小云用手写推导的方式，写了400多页纸、几百个方程，推导了两三个月才得到结果。

在全球密码界一鸣惊人后，多位国际著名密码学家邀请王小云到国外工作，但她坚定不移地留在国内。39岁时，她被聘为清华大学高等研究院杨振宁讲座教授，51岁当选中国科学院院士。

在王小云看来，密码为国家服务，国家利益放在第一位。在哈希函数两大支柱算法遭受重创后，美国向全球密码能的安全、可控、可靠。”

学者征集新的国际标准哈希函数算法，王小云没有参与这项设计研究计划，而是将精力投入到设计国内的密码算法标准上。她与国内其他专家设计了第一个哈希函数算法标准SM3，其安全性得到国内外密码专家高度认可，在金融、国家电网、交通等国家重要经济领域广泛使用。

如今，王小云正带领团队攻关“后量子密码”，设计更强大的密码算法。在这一研究领域持续攻关近20年，团队已取得国际领先成果。

“今天，人工智能的时代到了，我也带领我的团队从事人工智能安全的很多重要问题研究。”王小云说，“我希望更多的年轻人喜欢密码学并从事密码科研工作，期待更多的密码学家积极投入到人工智能安全研究，以密码分析视角构建人工智能安全新理论，保障人工智能的安全、可控、可靠。”

## 助力科研人才成长

在获奖感言中，王小云说：“展望未来，我将以这份荣誉为契机，全力支持新一代年轻科研人才的成长，积极倡导科研领域的性别平等。我坚信，通过构建包容、友好的科研环境，提供公平、平等的教育与职业发展机会，科技女性将会越来越强大。”

“世界杰出女科学家奖”由联合国教科文组织和欧莱雅企业基金会在1998年联合设立，该奖项每年从全球五大地区（非洲及阿拉伯国家、亚太、欧洲、拉丁美洲、北美）各遴选一位获奖者，其设立初衷在于弥合科学领域的性别差距，提升女性科研人员的能见度与影响力。截至2025年，共有超过125位女性科学家获得该奖。

近年来，随着中国女性科研力量的不断崛起，已有包括王小云在内的9位中国女科学家荣膺该奖，近4年内更是有3人获奖。今年，与王小云一同获得世界杰出女科学家奖的还有南非西开普大学化学系教授普莉西拉·贝克、德国马克斯·普朗克固体化学物理研究所所长克劳迪娅·费尔泽、阿根廷拉普拉塔国立大学精密科学院物理系教授玛丽亚·特蕾莎·多瓦以及美国加利福尼亚大学欧文分校化学系杰出荣誉退休教授芭芭拉·芬莱森-皮茨。

“这份荣誉不仅是对其个人科技成就的高度认可，更是对全球女科学家非凡韧性与智慧的礼赞。”王小云说，“希望这个奖项在未来的教育、工作过程当中鼓励更多女性，以很高的热情从事科研工作。希望我团队中特别优秀的女性将来能够承继这一类的奖项。”

## 科教人物坊

湖南省长沙市望城区建设德育一体化品牌

# 在雷锋故乡， 有十万名“雷小锋”

欧阳军

“我是092897号雷小锋，我叫谢皓宇。”

“我是092901号雷小锋，我叫周瑾瑶。”

走进湖南省长沙市望城区丁字镇的一所村小——车桥小学，二年级的孩子们争先恐后地介绍起自己。如今，这里的10万名中小学生有一个共同的称呼——“雷小锋”。

望城是雷锋同志的故乡。2022年以来，该区深挖本土红色资源，构建具有鲜明雷锋精神标志的区域德育品牌——“雷小锋”，引导全区少年儿童传承雷锋精神，建立起区域基础教育德育一体化体系。同时，为深入提炼雷锋精神时代内涵，该区提出了3个口号：“向阳（忠诚于党、坚定信念）”“向上（奉献祖国、敬业进取）”“向善（服务人民、助人为乐）”。雷小锋”000001号授予从渣土车车轮下勇救3岁幼童的全国道德模范周美玲。

“‘雷小锋’德育品牌强调全员参与、全员育人，不落下一所学校、不落下一名教师，不落下一个学生。”望城区教育局党组书记张红元说。

据介绍，“雷小锋”德育品牌设计了“亮号行动”“青锋计划”“超级课程”“争章工程”“养成教育”等行动内容，推出了“雷小锋”德育示范校、特色校、标准校创建工作。

“让孩子理解并认同自己的身份，是德育的关键问题。”望城区教育局局长戴金利说，“雷小锋”德育品牌突破灌输性模式，不断加强孩子们对“雷小锋”的身份理解和身份认同，让孩子实现自我教育、自我成长、自我蜕变。

以“青锋计划”为例。该计划的微信小程序设有微心愿、图书角、社会实践、希望小屋等板块。中小学生注册后，可进行“微心愿”认领、社会实践活动报名等。截至2024年底，“青锋计划”微信小程序中注册的“雷小锋”已达9万余人，为农村学校募集超100个班级图书角。

此外，贯穿全年的“超级课程”（超级运动会、超燃文艺节、炫科创展、超能阅读季）和养成教育，建立了“雷小锋”全面发展的平台。“超级运动会”的比赛项目多达40个大项、400多个小项，已经开展了3届。数据显示，近3年，望城学生的学业水平明显提升，一批学生走向了国家乃至国际领奖台。

# 中外科学家揭秘蚂蚁在恐龙时代的组织架构

据新华社电（记者白瑜）近日，由浙江大学、中国科学院、丹麦哥本哈根大学、德国明斯特大学、南昌大学、华大生命科学研究院科学家共同组成的研究团队在国际学术期刊《细胞》上联合发表研究成果，揭示了蚂蚁适应性辐射与社会性演化的遗传基础。

身长不足一厘米的蚂蚁，竟拥有足

以令人类佩服的组织能力。它们不靠语言沟通，却能协同建造惊人大巢穴；它们没有领袖意识，却有最严密的分工体系。联合研究团队通过整合全球163种不同蚂蚁的全基因组数据，重构了蚁科的生命之树，涵盖现生蚂蚁16个亚科中的12个，343个属中的97个。这项成果不仅澄清了蚁科物种复杂的亲缘关系，更是

将蚂蚁的共同祖先追溯到约1.57亿年前的侏罗纪晚期，揭秘蚂蚁在恐龙时代的组织架构。

研究团队发现，在蚂蚁共同祖先的基因组中，与嗅觉感知相关的基因家族发生了显著扩增，表明蚂蚁的共同祖先已经具备社会通信的关键分子机制。不同种类的蚂蚁在调节“谁当蚁后、谁当

工蚁”的过程中，这些信号通路的作用机制存在差异，反映出它们在自然选择下的适应性演化。

文章共同第一作者、南昌大学教师熊子军介绍：“以保幼激素和胰岛素信号为核心的保守通路在蚂蚁社会性演化中发挥着重要作用，蚂蚁中许多社会性状之间存在显著的相关性，共同塑造了蚂蚁表型的多样性。我们的研究从基因水平、基因家族、基因调控网络和保守信号通路等多维度揭示了驱动蚂蚁社会性演化的分子遗传基础。”



# 无人机 快送货

近日，飞行服务航线连接武汉三镇（武昌、汉口、汉阳）核心区域的汉商低空港正式投入运营。据了解，汉商低空港由汉商集团旗下汉商低空科技有限公司建设运营，目前形成由1个数字化实时调度平台、2个智慧指挥中心、10条低空航线、22个智能停机坪组成的专业化低空物流运营体系，主要服务于海鲜、鲜花、药品等商品的配送和应急保障，可实现飞行路径动态规划、设备状态实时监测与货物全流程追溯。

图为一架无人机在飞行中。  
新华社记者 伍志尊 摄

幼儿园的小朋友围坐一起，熟练地点触平板电脑上的互动游戏；四五岁的孩子在家中使用父母手机刷着短视频……这些生活中常见的场景提醒我们：网络并非成人世界的专属，而是进入了学前儿童的成长图景。

网络对于学前儿童而言，是新奇的“魔法盒”。不可否认，线上的早教动画、益智小游戏等，能在一定程度上激发孩子们的认知兴趣。但学前阶段的孩子，处在认知飞速发展、价值观萌芽的关键期，良莠不齐的网络内容，难免会对其成长造成困扰。比如，许多家长发现孩子在看动画时，会遇到不明所以的复杂广告、跳转链接。这些超出幼儿理解范畴的画面与信息，就像在搭积木时混入了形状怪异的零件，当孩子用纯真的眼光认识世界时，突然出现的干扰会打乱他们的认知逻辑。

电子设备使用的“度”很难把控——这对成年人来说也是个问题，何况学前儿童。有的幼儿园为了吸引孩子注意力，过度依赖动画教学；有的家长因为“别来烦我”，放任孩子玩手机游戏。这种情况下，短时间内孩子是安静了，但长期看，可能让孩子变得注意力难集中，对真实的绘本阅读、户外游戏兴趣降低，沉浸在虚拟画面营造的“快刺激”里，弱化了主动探索、人际互动的能力。这与学前教育倡导的“在真实体验中成长”背道而驰。

如何帮孩子在真实体验中成长？

学前教育工作者应该当好“把关人”。一方面是筛选优质、适龄的网络资源融入教学，比如利用科普动画辅助自然认知等；一方面也需要控制电子屏幕使用时长，多开展传统游戏、手工创作，让孩子在真实触摸、交流中发展感知力。

家长应该当好“同行者”。对孩子成长来说，家长陪伴的重要性不言而喻，家长需要了解学前儿童网络接触特点，学会设置电子设备儿童模式。其实，孩子也需要家长的“无网陪伴时光”，比如每晚睡前一起读绘本、玩角色游戏等。应该让家庭成为抵御不良网络影响的“安全岛”。

学前儿童的网络保护，是一场温柔且坚定的守护战，需要各方共同努力。网络平台要优化儿童内容生态，严格过滤不适宜信息，开发更多符合学前认知、寓教于乐的优质产品。监管部门需加强对学前教育类网络内容的审核，对违规推送不良信息的平台“零容忍”，从源头减少危害。

网络应当成为滋养幼苗的“雨露”，而非干扰成长的“风雨”。只有“科学用网”，才能引导孩子与网络“健康相遇”，让孩子们在网络与现实交织的世界里，纯真向阳，快乐启航。



内蒙古自治区巴彦淖尔市乌拉特中旗投资建成国防教育实训基地。基地集国防教育、校外实践、团体拓展、思政教育等为一体，整理修缮了二十世纪五六十年代在川井苏木建立的防空洞、地堡、供销社等，展现了国防发展历程。

图为参加研学的当地学生参观川井苏木供销社。

特日格乐摄