甘坐冷板凳者赢得“未来”

密码学家王小云：十年破解 MD5 和 SHA-1 两大国际密码

■王小云

清华大学杨振宁讲座教授，中国科学院院士，国际密码协会会士，2019未来科学大奖-数学与计算机科学奖获得者

王小云制定密码，为何又破解（破译）国际上的密码？破译的价值何在？密码界既认为王小云的破译是“密码学的危机”，为何又承认她的成就

“密码破解非常重要，没有破解，就很难有密码应用的标准化、规范化，商用密码体系也很难加强起来。”王小云眼中的密码学是矛与盾的交锋，攻与防的艺术

多年来，由美国国家标准技术研究院（NIST）颁布的基于Hash函数的MD5和SHA-1算法，是国际上公认最先进的两大重要算法，后者更被视为计算安全系统的基石，有着“白宫密码”之称，然而，却被王小云团队花十年时间破解

本报记者完颜文豪、李牧鸣

2019年11月17日，梳着干练短发、带着金边眼镜的王小云，走进“未来科学大奖周”的报告厅，用一口淳朴的山东口音，开始讲述她与密码的往事。

首个由中国民间发起的“未来科学大奖”，迎来了首位女性得主——今年53岁的清华大学高等研究院杨振宁讲座教授王小云。她获得了“数学与计算机科学奖”，因为她“在密码学中的开创性贡献，她的创新性密码分析方式揭示了被广泛使用的密码哈希函数的弱点，促进了新一代密码哈希函数标准”。

破解两大国际密码算法

偶然间看到的一条注释，让吴彦冰决定跟着王小云读博士。

5年前，四川大学信息安全专业本科生吴彦冰，在阅读公认世界第一黑客的凯文·米特尼克所著《欺骗的艺术》时，发现一段文字中有个中国人的名字，这是一条关于“MD5已被王小云教授破解”的注释。

了解这条注释背后的故事后，吴彦冰被密码学深深吸引了。毕业前他向王小云发了邮件，决定探索密码学这个迷人的世界。如今，他已师从王小云，漫游密码世界。

时间回到2004年，对于国际密码学界来说，这注定是不同寻常的一年。

这年的8月，在美国加州圣巴巴拉召开的国际密码大会上，王小云宣读了自己和研究团队对于MD4、MD5、HAVAL-128和RIPEMD四个国际著名密码算法的破译结果。

这被认为是2004年密码学界最具突破性的结果，堪称学术界的一场强烈地震。当年国际密码大会总结报告上写道：我们该怎么办？MD5被重创了，它即将从应用中淘汰。SHA-1仍然活着……

多年来，由美国国家标准技术研究院（NIST）颁布的基于哈希函数的MD5和SHA-1算法，是国际上公认最先进、应用范围最广的两大重要算法，后者更被视为计算安全系统的基石，有着“白宫密码”之称。

没多久，SHA-1的末日降临。2005年2月，在美国召开的国家信息安全研讨会上，5名著名密码学家公布了哈希函数发展史上的重要研究进展——他们收到了来自中国的王小云等3位女研究者对SHA-1全算法的攻击。

2005年，美国《新科学家》杂志在一篇文章中，用了颇具震撼力的标题——《崩溃！密码学的危机》，报道了王小云团队花10年时间取得的学术成果。

2006年，NIST颁布了美国联邦机构2010年之前必须停止使用SHA-1的新政策，并于次年向全球密码学者征集新的国际标准密码算法。

改变战争走向的古典密码

王小云从事的密码学，是一个既古老又新兴的学科。在1949年以前，人类社会经历了漫长的古典密码时期。

从古到今，密码被频繁应用在战争中，保护己方秘密并洞悉对方情报成了克敌制胜的重要条件。

中国古代兵书《六韬》中记录了阴符和阴书两种加密通信方式。国君和在外主将之间用阴符秘密联络，八种不同尺寸长度的阴符，隐藏着不同的军情秘密。如需传递军机大事则用阴书：把书信拆成三部分，分派三人发出，每人拿一部分，只有三部分合在一起才能读懂信的内容。

大约在公元前700年，古希腊军队用一种圆木棍进行保密通信。公元前405年，雅典和斯巴达之间的伯罗奔尼撒战争进入尾声，斯巴达军队截获了雅典信使的一条重要加密情报并破译，由此改变了作战计划，赢得战争的最后胜利。

这种加密方法中，加密方把纸条缠绕在特定的木棒上，写上原信息，木棒撤掉之后，纸条上的字母变成了乱码。解密方收到这个纸条后，用相同的木棒就可以恢复原信息。

聪明的古人，用简单的置换方式就设计出一个密码。不过，古典密码的加密方式不能让人知道，一旦泄露密码就被破解。

当王小云走进密码学的世界时，这门学科已经发展到了公开加密方法的现代密码时期。

▲王小云在2019未来科学大奖颁奖典礼上。 本报记者李牧鸣摄

家国情怀塑造密码天才

1966年，王小云出生于山东诸城一个教师家庭。童年时，做数学老师的父亲讲“鸡兔同笼”的故事，就是她最早的数学启蒙。1983年，17岁的王小云考入山东大学数学系，师从著名数学家潘承洞。读完了本科、硕士与博士，她留在山东大学任教。后听从导师建议，将研究方向从解析数论转向密码学。

39岁时，王小云被聘为清华大学高等研究院杨振宁讲座教授，之后曾获得中国密码学会“密码创新奖特等奖”以及“网络安全优秀人才奖”，51岁当选中国科学院院士。

多年后，王小云回忆起读书经历时，提到老师潘承洞对学生的一个特别要求，不管是出国深造，还是做访问学者，两年或者三年，到了时间就得回来，坚决立足于国内发展。

或许是耳濡目染了老一代学者身上的这种家国情怀，破解了两大国际密码算法后，王小云放弃了参与设计美国向全球征集的新国际标准密码算法，转而设计国内的密码算法标准。

此后，王小云和国内其他专家设计了我国首个哈希函数算法标准SM3。如今，SM3已为我国多个行业保驾护航，在金融、国家电网、交通等国家重要经济领域广泛使用。

“密码破解非常重要，没有破解，就很难有密码应用的标准化、规范化，商用密码体系也很难加强起来。”王小云眼中的密码学是矛与盾的交锋，攻与防的艺术。

“天书”哈希函数到底是什么

今天，计算机网络、移动网络、物联网、卫星网络还有大数据、云计算，这些人们已经熟知的科技场景，都离不开密码技术的支撑，需要密码来解决安全问题。

王小云曾将密码比作钥匙：“没有密码的保障，就相当于有人偷了家里的钥匙，可以随时自由进出你家，而你却浑然不知。”

密码学重要到何种地步？不得不从一个密码学中的基本工具说起，它就是王小云打了多年交道的哈希函数。

这个时代的所有网络信息安全，需要满足机密性、可认证性、不可抵赖性、完整性与有效性这五大安全属性，才可以有效防御黑客的攻击。其中，有效性是指效率问题，而前四个属性中，机密算法保障机密性，即不被窃取、看到；数字签名算法满足的是可认证性和不可抵赖性；哈希函数算法保证信息的完整性。

不过，数字签名算法必须和哈希函数一起才能保证可认证性和不可抵赖性。因此，五大安全属性里有三个，都离不开哈希函数。

密码上的哈希函数，可以将任意长度的消息压缩成固定长度的哈希值，而哈希值就像每个人都拥有唯一的“指纹”一样，哈希函数的重要之处就是能够赋予每个消息唯一的“数字指纹”，即使更改该消息的一个比特，对应的哈希值也会变为截然不同的“指纹”。

清华大学高等研究院数学博士吴彦冰打了个比方，就像把一本书里的某一页或一个字更改了，但看书的人很难判断更改的地方，即便全书通读一遍也未必能发现，“但通过哈希函数，输入稍有不同，输出结果就会完全不同”。

“严师”与“慈母”

在现代密码学中，哈希函数占据着基础而又重要的地位。上世纪90年代，王小云开始进行哈希函数研究，1994年开始尝试破解MD5和SHA-1。

一种密码算法的破解往往需要花费十年，甚至更久的时间，即便如此，成功率也只有1%左右。这注定是一个要“坐冷板凳”的研究领域，王小云就是用了整整十年的时间，破解了MD5和SHA-1两大密码算法。

清华大学密码学博士生丛天硕觉得，导师王小云似乎对密码有特别的直觉，做科研“就像是在跟着电影里的世界级大师一起工作”。

有一次，丛天硕和师兄尝试去攻击破解一个密码算法，想了很久不清楚是否可行，后来去找导师咨询，“王老师听完，说你们直接去做就行，她一眼就明白怎么回事儿了”。在丛天硕看来，王小云总能看到很远的地方，让学生去尝试前沿的研究。

学生眼中，这位导师在学术上要求“特别严厉”。学生的论文，一定要做到最好才能发表，“如果做到第二或有稍微的改进空间，她都是不能接受的，会让学生继续深入做研究”。

学术之外，王小云又很慈祥。丛天硕打算申请一个国外实践时，王小云会对出行住宿仔仔细细问个清楚，担心学生的安全。“刚读博时，王老师会和学生沟通，根据我们的兴趣，制定培养计划，还给出很多研究方向，让我们去尝试。”丛天硕说。

解密的惊心动魄更多在内心

在一些电影大片中，常有特工或黑客破解密码的惊险镜头，短短几秒钟就成功进入了对方的内部系统。当迈进密码学的大门后，吴彦冰发现很多人对密码的认识并不准确，或许是看电影后形成的刻板印象，误把破解银行卡或邮箱密码当成密码学家的工作，“其实那不是真正的密码，只是一个简单的‘口令’”。

王小云在一档节目中做了这样的科普：当你输入一串字符，如果不经过任何处理直接送到服务器来验证，它一定不是密码，只是一个口令；如果输进去的字符，通过密码运算得出另外一个结果，那么这个结果可以验证你是否为合法用户时，这个口令就变成了密码。

“比如战争中传输了一段密文，当这段密文被拦截后，如果让密码学家上场，他们就会根据各自的数学方法和手段，推导出原文是什么，比简单破解银行卡密码要复杂很多。”吴彦冰说。

现实中密码学家的工作，没有电影中那样惊心动魄。吴彦冰甚至觉得，这是一个很枯燥的过程，不停地推导公式、做编程，然后用大型计算机验证，等待结果，“想尽各种方法，一个个去尝试，失败了再重来”。

在吴彦冰看来，破解密码有时就像走进了一个巨大的迷宫，一套密码是经过密码大师在设计中一遍遍确认，没有问题后才公布出来，很多时候用传统的方法和思维破解不了，可能在迷宫中碰壁多次也找不到出口。

像很多科学突破一样，破解密码也需要勤奋和灵感，熬夜攻关亦是常态。吴彦冰跟着王小云做科研时，有过几次这样的经历，“白天忙了一天，晚上脑袋里突然蹦出来一个灵感，会亢奋得睡不着，就要顺着把理论推导完，不断尝试到底行不行”。

吴彦冰曾听老师王小云讲起破解MD5的经历，“那时候王老师还没学过编程，就用手写推导的方式，写了400多页纸，几百个方程，推导了两三个月才得到结果。”

王小云沉浸在密码的美妙世界中，享受着外人无法体会的乐趣。生活中她喜欢在家里和实验室养花，有时候思考一个数学问题，却找不到答案时，就会起来打扫打扫卫生，或者是给花浇浇水，干点别的事情，但实际上脑子里一直没有放下科学问题。

科研过程中，王小云也把这种乐趣传递给学生们。他们既扮演着“设谜者”的角色，设计一套巧妙的密码算法，弥补前人的不足，希冀让攻击者无法突破；同时还扮演着“猜谜人”的角色，把别人设计精妙的体系一举攻破。“参与者会有很大的喜悦感和成就感。”吴彦冰说。

就如王小云在未来科学大奖的获奖致辞中所说，虽然目前密码学只被少数人所熟悉，但未来会有更多的年轻力量为密码学的发展助力，愿意尽自己的全力去帮助年轻的科学家们开拓密码学这门神秘而又充满力量的学科。

◀扫描二维码，观看视频《2019未来科学大奖获奖者王小云报告会及对话青少年》

（上接10版）

刘艳芳说：“这些奶奶辈的人，不少人是家里的一把手，在家里都被伺候着。有时候教练批评一句都不行。”刘艳芳亲眼看过，教练指导动作的时候，一名队员双臂弯在胸前，和教练顶嘴。

没多久，教练就被气走了。

刘艳芳出面劝和，斩钉截铁地告诉对她来说是“奶奶辈”的“姐姐们”：“不团结的话，明天就解散模特队”。

刘艳芳请社区信息文化员王瑾纯“出山”当队长。王瑾纯才55岁，“姐姐们”也不服她。有人说，她还不如我们走得好，凭啥当队长。

王瑾纯不怕得罪人，也私下劝了不少人：“你是出来找气受，还是找乐的？”

后来，在社区的支持下，王瑾纯给队员们申请了三套表演服，还带着队员们找舞台，这才镇住了场。

没多久，社区请来了专业指导老师岳淑莲，杨星也磨平了自己的急脾气。王瑾纯说：“模特队的叛逆‘青春期’过去了。”

踏着模特步，走过天安门

10月1日，队员许建华守在电视机前，找姐妹们的身影，手机拍了直播画面，马上发到朋友圈。她又兴奋又遗憾——许建华自己本来也能上的。

6月17日傍晚，“姐姐们”接到一个通知。“当时只是说参加十一健步走，没提群众游行。”许建华记得很清楚。当时模特队20个人全报名了。随着一步步“过关斩将”，她们意识到“十一健步走”可能就是国庆群众游行。

竞争确实激烈，每次训练都刷人。仅霍营街道就报了53个人，别的街道也不少，最后只留了12个名额，而和谐家园社区模特队占了6个。

“姐姐们”训练确实拼。大太阳底下，正步走训练、十公里体能训练，这些“姐姐们”没掉链子。

肖莲的脚动过手术，脚前掌没肉，训练的时候一直垫着胶垫。60岁的队员李东平腰疼得厉害，一直戴着护腰。与她同龄的队员朱秀云平时追公交车都喘，十公里体能训练，愣是坚持下来了。

大晴天的时候，“姐姐们”脸被晒得像老农；赶上雨天，脚被泡得跟白猪蹄似的，训练完回家就得喝姜汤，生怕感冒打喷嚏被发现。

临近国庆的一次训练，李东平一直低烧不退，她硬是咬牙坚持，不敢和别人说。李东平觉得要是说了，就参加不了最终的方阵了。她趁没训练的时候，偷偷上医院输了液，身体才好了一些。

“这些都不算什么。”副队长杨秀云说，“我们都这么大岁数了，什么苦没吃过”。后来，“姐姐们”身板反而更结实了，护腰也撤了。

国庆期间，和谐家园社区也举办了“我和我的祖国”快闪系列活动，许建华、邢晓玲和其他被淘汰的姐妹们成了节目主力。邢晓玲说，“5个节目我上了4个”。

愿意来的，咱们都欢迎

模特队着实又火了一把。“姐姐们”成了圈子里的网红。同事、亲家、朋友发来的祝贺，“刷爆”了队员们的手机。她们反复播放国庆游行那段视频，看不腻，也说不腻，以至于杨秀云的小孙女说：“我奶奶还在电视上呢。”

国庆直播对模特队所在的“美好生活”方阵是这样介绍的：“美好生活是什么？是环卫工人清扫的整洁环境，是快递小哥便捷的物流服务，是医生护士的悉心照料，是最美家庭的幸福相伴，是老年模特队的神采奕奕……”

王瑾纯说：“老年模特队把我们从厨房里拉出来，是真正的老有所乐。一些队员懂缝纫，有手艺，在模特队里还能派上用场，是真正的老有所为。”

国庆之后，报名模特队的“姐姐”更多了，别的社区也有人申请。现在模特队有30多个队员，最大的70岁。居委会的楼道有些走不开了，刘艳芳忙着四处找场地。

“模特队本来就是图一乐，没有什么门槛。愿意来的，咱们都欢迎。”刘艳芳说，“以前岗位不同，那都是退休前的事了，现在大家一样，都是退休的人，应该两脚着地”。

从天安门广场回到社区，王瑾纯反复提醒队员们：“咱们不能老躺在山上回忆过去，该下山的时候下山，该爬新山的时候还要爬新山。”

现任教练岳淑莲确实有几下子，化妆、衣品、模特步，样样懂。队员们服气，也舍不得她，怕把她气走了。

65岁的岳淑莲在圈内小有名气，每周都得带3个老年模特队，不是在教学，就是在去教学的路上。周三下午给和谐家园社区模特队纠正动作的时候，又一个社区来了电话邀她去指导。

岳淑莲说：“很多人退休后想把自己修饰一下，变得更端庄一点，优雅一点。这是好事。”

王瑾纯说：“教练越忙，越说明更多人老有所乐了。”

（刘月、杨星均为化名）