王小云访谈录

王 涛 王 坤 / 访问整理

摘要：王小云，1966 年出生于山东诸城，1981 年进入诸城一中学习，1983 年起就读于山东大学数学系，先后获得学士、硕士、博士学位，师从潘承洞院士；1993 年毕业后留校任教，历任讲师、副教授、教授；2005 年 6 月受聘为清华大学高等研究院“杨振宁讲座教授”。现为第十三届全国人大代表、中国科协女科技工作者专门委员会委员、中国密码学会副理事长、中国数学会常务理事。

王小云的主要研究领域为密码学。在密码分析领域，她系统给出了包括 MD5, SHA-1 在内的系列 Hash 函数算法的碰撞攻击理论，提出了对多个重要 MAC 算法 ALPHA-MAC、MD5-MAC 和 PELICAN 等的子密钥恢复攻击，以及 HMAC-MD5 的区分攻击思想。在密码设计领域，主持设计了国家密码算法标准 Hash 函数 SM3，该算法在我国金融、交通、电力、社保、教育等重要领域得到广泛使用，并于 2018 年被成功纳入 ISO/IEC 国际密码算法标准。

由于杰出的科学成就，王小云于 2005 年获得国家自然科学基金杰出青年基金资助，2006 年被聘为清华大学“长江学者特聘教授”，同年获得陈嘉庚科学奖、求是杰出科学家奖、第三届中国青年女科学家奖，2008 年获得国家自然科学二等奖，2010 年获得苏步青应用数学奖，2014 年获得中国密码学会密码创新奖特等奖，2017 年当选为中国科学院院士。

受《数学文化》杂志委托，王涛博士于 2018 年 8 月 12 日和 2018 年 9 月 27 日采访了王小云院士。以下为访谈的主要内容。

早年教育

问：能否简单介绍一下您的家庭情况。

王：我出生于一个教师家庭。父亲毕业于诸城师范学校的数学与化学班，所以我们姐弟五人从小就对数理化比较感兴趣。父亲的兴趣比较广泛，他喜欢中国文化，对古代文学很有研究，对中医也有一些研究，他有特别有效的中药方，这些药方曾帮助过很多人。另外父亲还擅长书法绘画，我上小学时，曾来人请他到潍坊市文化局举办文化展览。父亲是一个传统的中国知识分子，家里收藏了很多古书籍，比如《康熙字典》《二十四史》等，其中《二十四史》在文革期间烧掉了。我很遗憾自己没能继承父亲的这些兴趣与爱好，但在艺术方面我的女儿继承下来了。

在母校诸城一中作报告（2018 年）

父亲常年在外教书，经常两周才能回来一次。为了让我们能安心学习，母亲承担起了全部的农活和家务，即便再苦再累她总能处理得井井有条。我们姐弟五人都先后考上了镇重点初中，每次离家返校，母亲都要几次起床看星星来判断时间给我们准备食物。后来家里买了钟表，母亲再也不用出屋看星星，可以安稳地多睡一会了。父亲当时感慨地说我们家里最重要的东西就是那个钟表。每当我们遇到想不通的事，母亲总是开导我们要想开，宰相肚里能撑船。当别人做的比我们好时，便教育我们不要嫉妒人家。母亲还告诉我们对待弱势群体要有善心和爱心。可以说，她的很多言行至今还在深深地影响着我，激励着我。母亲真的非常伟大，勤劳善良是她最优秀的品质。在我的记忆里，母亲每天都劳动到深夜，我很小时就陪母亲熬夜。也许正是这个经历，历练了我深夜工作的能力。

问：您从小就对数学感兴趣了吗？

王：我对数学有些兴趣，因为父亲给我讲过鸡兔同笼的问题。小学和初中时我基本上是边玩边学，偶尔去钻研一下，数学题也能做出来。我的数理化成绩不错，文科成绩不是特别好。中考的时候我学了 40 天，顺利地考入了诸城一中。其实我平常的成绩一般，那时最好的学生都上中专，到我们那一届改为最好的学生上高中。上高中后我进行了反思，40 天的学习成绩竟然能提高这么多，意识到自己的学习潜力可能很大，便开始了认真地学习。

问：高中有没有对您很有影响的老师？

王：我的物理成绩非常好，平常在班里一直都是第一名。我喜欢物理有两个原因，一是初中时的物理不错，做物理题很有感觉；二是上了诸城一中以后，教物理的戴恩浦老师不断地鼓励我，说女孩子能学好物理的不多，一定要好好学。因此我学习物理的兴趣很高又很用功，成绩一直都在前面。

与物理相比，数学成绩只能算得上比较好。数学老师是我的班主任吴世业老师，他总觉得我的数学潜力还没有完全挖掘出来。吴老师的教学经验很丰富，有一次我们模拟考试，他提醒同学们答题要注意方法，若难题花太多时间做不出来，前边的简单题又由于粗心而错了很多，这样会得不偿失，其实我就属于这一类学生。那次考试我把前面的题目都做完了，正在做最后两道难题，吴老师对我说：“你别做了，先把前面的那些题检查一遍。”我就认真地把前面的题检查了一下，然后再做后面的题。平常我数学考不到前几名，结果那一次考得很好，数学老师对我的指导方法很有帮助。等到高考时，我的数学成绩竟然是班里的第一名。当然，数学考得好还另有原因，就是当时我擅长的物理考砸了，所以把追分的希望放在了数学上，竟然能梦想成真。

问：那您物理考试不理想的原因是什么？

王：我也不知道。我擅长的物理题目是能量守恒、力的平衡等，这类题目我很有感觉，一般很快就做出来了。但那年高考的物理题与我平常做的不太一样，反正是感觉不太好，最后只考了 78 分。物理考砸之后，我心想一定要把剩下的科目考好，把平时的成绩发挥出来应该还能考上一个不错的大学。

问：您当年报考了山东大学。

王：高考后老师根据我们平时的成绩，给我们拟填报了志愿。我在班里一般