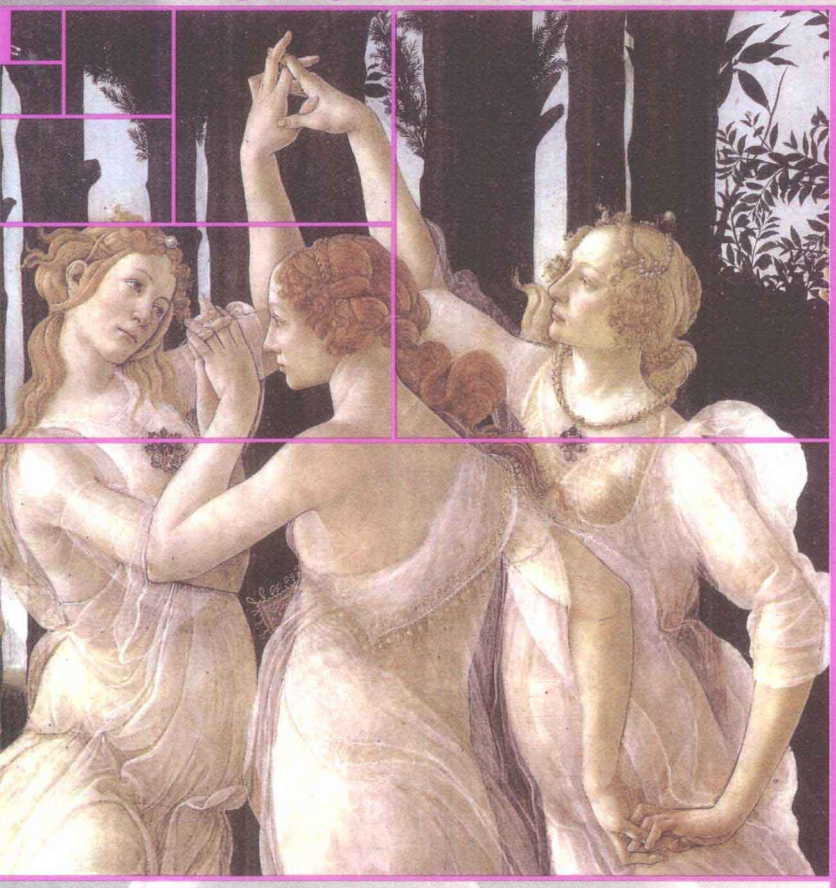
数学与人文 · 第四辑

Mathematics & Humanities

女性与数学



主编 丘成桐 杨乐 季理真
副主编 李文林

高等教育出版社
HIGHER EDUCATION PRESS

数学与人文·第四辑
Mathematics & Humanities

女性与数学

Nuxing yu Shuxue

主编 丘成桐 杨 乐 季理真
副主编 李文林

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING
International Press

图书在版编目（CIP）数据

女性与数学 / 丘成桐,杨乐,季理真主编. —北京：高等教育出版社，2011.6
（数学与人文.第4辑）
ISBN 978-7-04-032286-6

Ⅰ.①女… Ⅱ.①丘…②杨…③季… Ⅲ.①数学-人文科学-普及读物 Ⅳ.①O1-05

中国版本图书馆CIP数据核字（2011）第101849号

出 品 人 苏雨恒
总 监 制 吴 向
总 策 划 李冰祥
策 划 赵天夫
责任编辑 赵天夫
书籍设计 王凌波
责任印制 朱学忠

出版发行 高等教育出版社
社 址 北京市西城区德外大街4号
邮政编码 100120
购书热线 010-58581118
咨询电话 400-810-0598
网 址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.landraco.com
http://www.landraco.com.cn
印 刷 涿州市星河印刷有限公司
开 本 787×1092 1/16
印 张 13
字 数 230 000
版 次 2011年6月第1版
印 次 2011年6月第1次印刷
定 价 29.00元

物 料 号 32286-00

内容简介

《数学与人文》丛书第四辑将继续着力贯彻“让数学成为国人文化的一部分”的宗旨，展示数学丰富多彩的方面。

本辑主题栏目“数坛巾帼”，通过部分女数学家的评传，以历史实例来引发对“女性与数学”这一社会课题的思考。特别是，本专栏刊登了两位活跃在现代数学前沿的女数学家的访谈录，她们的成长经历一定会引起读者的兴趣。

本辑“数海钩沉”栏目刊发丘成桐先生“清末与日本明治维新时期数学人才引进之比较”，以史为鉴，发人深省；“数学星空”栏目特约文章冯端院士“纪念冯康院士诞辰90周年”，真切感人；新辟栏目“数学人生”，刊数学家们探求真理的人生感悟与经验之谈，本辑特载国家最高科技奖获得者谷超豪先生激励人心的讲演“请勿歌仰止，雄峰正相迎”；“数学家诗词”栏目，为数学家开辟发表诗作的园地；“数学之旅”栏目，发表数学家们在国内外访问的观感、见闻，以轻松的笔墨，与读者共享数学的文化魅力。

让数学贴近公众，让公众走近数学！

丛书编委会

《数学与人文》丛书序言

丘成桐

《数学与人文》是一套国际化的数学普及丛书，我们将邀请当代第一流的中外科学家谈他们的研究经历和成功经验。活跃在研究前沿的数学家们将会用轻松的文笔，通俗地介绍数学各领域激动人心的最新进展、某个数学专题精彩曲折的发展历史以及数学在现代科学技术中的广泛应用。

数学是一门很有意义、很美丽、同时也很重要的科学。从实用来讲，数学遍及物理、工程、生物、化学和经济，甚至与社会科学有很密切的关系，数学为这些学科的发展提供了必不可少的工具；同时数学对于解释自然界的纷繁现象也具有基本的重要性；可是数学也兼具诗歌与散文的内在气质，所以数学是一门很特殊的学科。它既有文学性的方面，也有应用性的方面，也可以对于认识大自然作出贡献，我本人对这几方面都很感兴趣，探讨它们之间妙趣横生的关系，让我真正享受到了研究数学的乐趣。

我想不只数学家能够体会到这种美，作为一种基本理论，物理学家和工程师也可以体会到数学的美。用一个很简单的语言解释很繁复、很自然的现象，这是数学享有“科学皇后”地位的重要原因之一。我们在中学念过最简单的平面几何，由几个简单的公理能够推出很复杂的定理，同时每一步的推理又是完全没有错误的，这是一个很美妙的现象。进一步，我们可以用现代微积分甚至更高深的数学方法来描述大自然里面的所有现象。比如，面部表情或者衣服飘动等现象，我们可以用数学来描述；还有密码的问题、电脑的各种各样的问题都可以用数学来解释。以简驭繁，这是一种很美好的感觉，就好像我们能够从朴素的外在表现，得到美的感受。这是与文化艺术共通的语言，不单是数学才有的。一幅张大千或者齐白石的国画，寥寥几笔，栩栩如生的美景便跃然纸上。

很明显，我们国家领导人早已欣赏到数学的美和数学的重要性，在 1999 年，江泽民先生在澳门濠江中学提出一个几何命题：五角星的五角套上五个环后，环环相交的五个点必定共圆，意义深远，海内外的数学家都极为欣赏这个高雅的几何命题，经过媒体的传播后，大大地激励了国人对数学的热情，我希望这个丛书也能够达到同样的效果，让数学成为我们国人文化的一部分，让我们的年轻人在中学念书时就懂得欣赏大自然的真和美。

前　言

编辑组

《数学与人文》丛书第四辑与读者见面了。

本辑副题“女性与数学”，缘起于丛书主编丘成桐先生的提议。早在丛书创办之初，丘先生就提议办一个关于女数学家的专辑或专栏，其成果就是本卷的主打栏目“数坛巾帼”。在整个数学历史上，女数学家可谓寥若晨星，即使到了提倡男女平等的现代，女性数学家所占比例仍然不足称道。究竟是什么原因导致男女性在数学方面发展的不平衡呢？是不同性别的生理和心理上存在差异的原因，还是主要受社会因素之影响？这已成为广受关注的人文学课题。我们的专栏组编了部分女数学家的评传，通过历史实例来引发对这一课题的思考。特别是，本专栏刊登了两位活跃在现代数学前沿的女数学家 —— 数论专家、台湾大学数学“五朵金花”之一李文卿和密码学家王小云的访谈录，她们的成长经历一定会引起读者的兴趣，激励有志于数学的女青年走上成功之路。随后转载的台湾大学数学系李莹英教授“女数学家论坛会后报道”，报道了台湾数学界人士对女性与数学问题的热烈和有意义的讨论。

本辑“数海钩沉”刊发丘成桐先生“清末与日本明治维新时期数学人才引进之比较”一文。该文通过对 19 世纪以来中国和日本两国数学发展轨迹的比较分析，探讨中国现代数学落后于日本的原因，可以说是“钱学森之问”的共鸣，文后附刘源张院士之读后感，更发人深省。接着的“数学星空”栏目特约文章“纪念冯康院士诞辰 90 周年”，由著名物理学家、冯康院士的胞弟、年近九旬的冯端院士亲自撰写，真切感人，文中指出国内外对冯康院士逝世的“报道、评价形成鲜明对比”之现象，亦令人感慨。

新辟栏目“数学人生”，刊载数学家们探求真理的人生感悟与经验之谈。这里我们要特别感谢国家最高科技奖获得者谷超豪先生慨允转载他的激励人心的讲演“请勿歌仰止，雄峰正相迎”。

魏尔斯特拉斯曾经说过：“一个数学家如果不是某种程度的诗人，就绝不是一个完美的数学家。”这当然不是说数学家个个都能诗，但事实是数学家中确不乏诗人。数学家的诗词，反映了他（她）们的情怀，体现着数学与艺术的统一。本卷新设“数学家诗词”栏目，为数学家开辟发表诗作的园地，让

数学家们的诗情画意跃然纸上。“数学之旅”栏目，则欢迎数学家们发表他（她）们在国内外访问的观感、见闻，以轻松的笔墨，与读者共享数学的文化魅力。

《数学与人文》丛书将继续着力贯彻“让数学成为国人文化的一部分”的宗旨，展示数学丰富多彩的方面，让数学贴近公众，让公众走近数学！

目　录

数坛巾帼

王小云和她的密码学团队

—— 王小云教授访谈录

王小云，清华大学高等研究院“杨振宁讲座教授”，清华大学密码理论与技术研究中心主任，2006 年入选“长江学者特聘教授”。1966 年出生于山东诸城，1983 年至 1993 年就读于山东大学数学系，先后获得学士、硕士和博士学位，师从著名数学家潘承洞院士和于秀源教授。1993 年毕业后留校任教。1995 年开始从事 Hash 函数研究，2004 年破解 MD5、HAVAL-128、MD4 和 RIPEMD，2005 年破解 SHA-1。先后获得密码学领域最权威的两大会议 EUROCRYPT 与 CRYPTO 的 2005 年度最佳论文奖、国家自然科学二等奖、陈嘉庚信息技术科学奖、求是杰出科学家奖、中国青年女科学家奖等奖项。

建于 1917 年的清华科学馆，保存着清华理科最古老的记忆，这座国家级文物建筑现在是清华大学高等研究院和周培源应用数学研究中心所在地。2010 年 5 月 6 日，春末夏初一个阳光明媚的日子，上午 9 点，我们如约来到这里，对著名密码学家王小云教授进行了近 3 小时的专访。

王小云教授本不愿再接受媒体采访，但当我们说明《数学与人文》是丘成桐先生创办的系列出版物，旨在向公众普及数学、传播数学文化时，她欣然同意接受采访。

十年磨剑——从数论到密码学

王小云（以下简称王）：密码学领域有其特殊性，它的专业术语以及它跟数学的关系，很多人，包括媒体报道，都不容易准确理解和把握。另外，密码学的概念基本都是近几十年提出的新概念，而密码工作由来已久，所以有时候人们对这些概念的理解也会有不同的认识，这都是很正常的。例如，我们的工作应该是叫“密码分析”而不是“破译”，因为就密码体制而言，成功地分析一个密码算法，就是把它归结为一个数学难题并对这个数学难题给出一个有效算法，这在国际上一般都叫“破解”，英文里对应的专业术语是

break 或者 attack；而“破译”一般来讲主要针对被加密信息的破解，是把一个密文恢复其明文的原意，但破译的过程往往很艰苦，因为有可能涉及很多非学术的工作，如信息的搜集等，这些工作已经超出了学术的范畴。由于密码破译容易被社会关注，不仔细了解，一般人很难分清“破译”与“破解”这两个概念之间的差异。

王丽霞问[1]（以下简称问）：数论是数学的皇后，听说您原来是学数论的，后来转到密码学领域，这个转变的原因是什么？

王：这主要还是老师把关、方向转得比较好。我的研究生导师有两位，一位是潘承洞老师，一位是于秀源老师。由于当时因式分解、离散对数等数论问题已经应用到密码领域，潘老师就想利用山东大学在数论方面的优势来发展密码学研究，他跟于老师、展涛博士等成立了一个密码研究小组。在他们的指导下，我在初步学习了解析数论等内容以后就转向密码学研究了。

李文林[2]问（以下简称李）：常言道：“十年磨一剑”。实际上您是十年磨了五剑——从 1995 年开始从事 Hash 函数研究到 2004 年成功破解 MD4，HAVAL-128，RIPEMD 和 MD5 四大密码体系，以及 2005 年破解 SHA-1，恰恰经历了 10 年，这个过程很艰苦吧？能介绍一下您这十年间的经历和感受吗？

王：我觉得这个经历是有一定的艰苦度，但是也没有感到特别艰苦。因为一是现在的生活比较好，另外家庭条件和工作条件都比以前好，而且一般来讲我们工作后不久都会有一定额度的科研经费支持，从这个角度来讲，我们这一代人与老一代专家相比确实谈不上什么艰苦。所谓艰苦，是在进密码学领域的时候以及科研攻关阶段。

密码学分公钥密码学和对称密码学。从长远来说，公钥密码学这个方向是很难的，因为它的设计理论基于算法数论、计算代数领域的一些数学难题以及计算复杂性理论的困难问题等，如分解因子问题、离散对数问题以及格的最短向量问题等。只看它的设计，不容易看出它的算法背后隐藏的真正数学问题的难度，跟它的安全强度之间的关联性，但是如果从各个角度来尝试分析它的安全性，就会了解它设计的理念与技巧。我原来是学解析数论的，初等数论的基础还是很好的，对公钥密码算法的设计比较容易理解，所以比较顺利地进入了密码学领域，这是一个跨越。但是我也跟其他密码研究人员一样，对于安全性分析也做不了很多。不久山东大学密码研究小组调整方向，需要有人研究对称密码，我就转到了对称密码体制这个方向。这个方向不管是跟我本科学的内容还是跟我研究生学的方向差异都是很大的，转入这个领

[1]王丽霞：2006 年获中国科学院数学与系统科学研究院博士学位，现任北京邮电大学理学院副教授。

[2]李文林：中国科学院数学与系统科学研究院研究员。

↑ 王小云教授（左一）和她的密码学团队在讨论问题

域对我来说是另一个跨越。因为我学的专业是基础数学，而对称密码领域涉及的概率问题、信息论的内容以及密码分析模型比较多，针对对称密码分析逐步建立起来的密码分析学对我来说是一个全新的领域，难度比较大，从这个意义上说，这个跨越是艰难些。

从理论上讲，一个密码算法可以归纳为布尔函数方程，而对称密码的设计引入 S 盒的概念。S 盒是一个随机置换，可以导出随机性良好的布尔函数方程。结合算法的其他变换，经过少数几步运算就可以导出非常复杂的布尔函数方程，根本不可能通过简单计算看出这些方程具有哪些数学特性或者一些非随机的统计规律。算法设计最重要的就是随机原理。密码算法对应的布尔函数方程是高次的，如果密钥的长度是 128 比特，那么它的布尔函数方程的次数就可能达到 128 或者 127，而且 128 个变量的所有的组合都有可能出现在这个方程里面，每个项出现和不出现的概率大约是 1/2，也就是说你不知道哪个项出现哪个项不出现，其中有些项可以通过特别选择的明文检测它是否出现，但因为组合数是指数阶的，所以不可能对每个项进行检测。如果不能把相当数量的项推算出来，通过求解布尔函数方程或者通过布尔函数的一些特性进行密码分析是很困难的。

一些常规的对称密码算法分析技术是 20 世纪 90 年代提出的，如差分分析、线性分析、不可能差分分析等，仅用这些分析技术分析算法的安全性是远远不够的，不容易做出好的分析工作。基本上每几年就有新的分析技术出现，这就需要密码分析人员不停地去探索，不停地跟踪国际密码分析新进展。

问：能谈谈您和您的团队在克服这些困难方面的建树吗？

王：公钥密码体制设计的目标是使得算法安全性等价于一个被广泛认可的数学难题。因此公钥密码体制的分析需要解决一些数学难题的快速求解算法或者结合各种环境下的攻击模型求解数学难题。而对称密码设计中的数学

难题很难做到与一个理想的数学问题完全吻合，这就导致密码分析人员和设计人员不停地在以前算法的基础上，根据以往的设计经验和分析经验对密码设计进行完善与提高，但无论怎样提高我们都要怀疑算法设计没有达到百分之百的完美，给我们的分析增加动力。那么我们在做分析的时候，就是希望能够研究它的非随机性，用概率统计方法或者高概率数学特征寻找破解路线。

每种密码体制都有安全属性的要求，实际上每一个安全属性的要求就是一个数学难题。一个算法一般要有几十步，我们在分析它的时候，要提炼能够反映整个算法安全属性的数学特征，这个工作很难。一个密码算法通常有几十步，如 Hash 函数算法 MD4 有 48 步，我最早做研究的时候，可以很容易提炼出 4 步的数学特征，扩到 8 步的时候还是能做到，…… 但是到了最后 16 步数学特征基本就提炼不出来了。这个时候我们既不能用纯数学的方法来做，也不能用纯密码分析技术来做。这个时候会有一些科学发现和一些新的理念。

值得说明的是，Hash 函数是一类基础密码算法，主要用于数据的完整性检测以及保证电子签名安全的关键技术。电子签名的安全性主要基于 Hash 函数的无碰撞性。我们的一个主要工作就是要找到 Hash 函数的碰撞攻击。

比特进位的概念是我们提出的一个开创性的方法。这个思想是受 1949 年 Shannon 提出的完全（perfect）安全概念的启发得到的。我觉得我们最幸运的一点就是能对 Shannon 理论有正确的认识并在密码分析中进一步发展。在安全保密系统中 Shannon 理论提出“雪崩效应”现象。“雪崩”体现了一种设计理念，同时也是分析理念，它指的是输入函数有一个微小的变化就会引起输出结果的随机变化，即雪崩似的巨大变化。我们是用比特来解释函数的，一个含有 128 比特变量的函数，如果它的随机性好，一个变量（也就是一个比特）改变，就会引起算法输出的许多比特位变化，每个输出的比特发生变化的概率约为 1/2。这就相当于雪山上一个点的变化引起了雪崩，…… 引起雪崩的这一个点，雪崩以后你就无法用数学方法追踪它了，同时这一个点导致了整个雪体崩塌。

在分析密码算法的时候，我就想密码算法一定是有雪崩现象的，但是这需要一个过程，而且一开始雪崩速度较慢。一个密码算法经过 4 步、8 步，基本就是有雪崩现象的，但速度比较慢，经过 16 步运算雪崩可能就很强了。我想既然开始雪崩比较慢，我们就先刻画它，也就是用数学现象来表达它。实际上很多问题都可以用数学现象来刻画，而且数学问题如果能表达得很清晰，那么数学研究方法自然也就可以确定下来了，否则就不可能有数学分析的方法。这是我们成功分析算法的第一个重要的思想理念。当时我想做不了 8 步就先做 4 步的刻画，刻画了 4 步再想办法刻画到 8 步，刻画了 8 步再刻画到 12 步，当然再到 16 步就已经无法刻画了。这个时候怎么办呢？我们又

想了一个思想。

因为给出一个 Hash 函数的碰撞攻击，就是要发现找到 Hash 函数的碰撞对的有效算法，即找到两份不同消息具有相同输出值。也就是从第一步的零雪崩开始，经过雪崩控制过程，到最后一步又出现零雪崩，才算破解了这个算法，所以自然有一个想法，既然能刻画一定程度的雪崩，那就可以控制这种雪崩。就像一个雪山，雪崩比较缓慢时，我们就可以在这个过程中借助外来的因素控制它、排除它。到最后，我们把雪崩全都排除了，就没有雪崩了。基本就是这种分析理念，就是使用比特进位产生雪崩抵消因子的思想。对称密码有三种基本体制，一种是流密码，一种是分组密码，一种是 Hash 函数。比特进位的思想，不仅对 Hash 函数而且对其他的密码体制都有很重要的借鉴与指导作用。

使用比特进位以后，我们就开始控制雪崩的复杂过程。控制过程到底需要 100 多个方程还是 200 多个方程，这些方程如何推导，怎样让雪崩（变化比特）相互抵消，所有这些复杂的工作都是以后慢慢地、一点一点做的。在分析的过程中可能会出现很多数学问题，出现什么问题就解决什么问题，或者放弃。因为密码算法有的是 48 步，有的是 64 步，有的是 80 步，一步过不去就又雪崩了、就出不了任何结果，必须从第一步走到最后一步出现零雪崩才能成功。面对众多的数学问题、数不清的坎，怎么越过去，那就要看你的耐力了。也许从科学贡献上讲你已经有 80% 成功了，但是因为太烦了，对于那么多方程不愿意控制了，不能够推导下去，可能也就失败了。所以说这个工作，确实需要坚持和毅力。

做密码数学分析的研究人员很多很多，能做出好的密码分析工作的比例，远比做设计的要少得多。欧密会、美密会每年有 70 多篇论文发表，这是密码领域最高水平的论文，基本上每次会议找到 10 篇、8 篇好的密码体制设计论文是比较容易的，但是要找到 2、3 篇比较好的分析论文很难。

密码理论涉及的数学领域跨度很大。首先是数论，我国王元院士、陈景润院士，还有我的导师潘承洞院士在数论方面做了杰出的工作。在公钥密码领域，总的来讲我们是从 20 世纪 80 年代中期开始进入这个领域的，最初能够做一些设计工作，分析工作我们现在也慢慢开始重视起来。还有一个方向就是计算代数，最为成功的应用可以说是编码。编码在密码算法设计中应用较早，尽管依它设计的一些密码算法被破解了，不过这个失败的经历又推动了密码分析技术的进步，分析技术又衍射到其他的密码设计领域。对一个在密码学中有重要应用的数学领域来讲，不能光看它的设计成败与否。如果分析是成功的，对密码学的发展也具有很大推动作用。

问：刚才您说到你们提出的分析理论来源于对 Shannon 信息论的正确理