丁石孙与中国密码学

徐茂智

丁石孙先生与中国密码学的渊源可以追溯到1974年。当时，担任北京大学数学力学系主任的段学复先生在北京大学组织了军队密码学人才的培养工作。这一年北京大学举办了第一届密码技术培训班并招收了部队学员40多人，学制一年半。由段学复、丁石孙、聂灵沼、王萼芳讲授《群论》、《高等代数》和《线性移位寄存器》等课程，同时还聘请了中国科学院的万哲先、曾肯成、戴宗铎、刘木兰、冯绪宁讲授《非线性移位寄存器》、《组合数学》、《有限域》、《高等代数》等课程，他们共同指导学生完成论文。其后又在1975年、1976年、1977年连续举办了三届密码技术培训班，1978年选留成绩优秀的数名学员继续深造3年。通过举办培训班，为军队培养了大批优秀专门人才，也开启了北京大学密码学人才培养的先河。

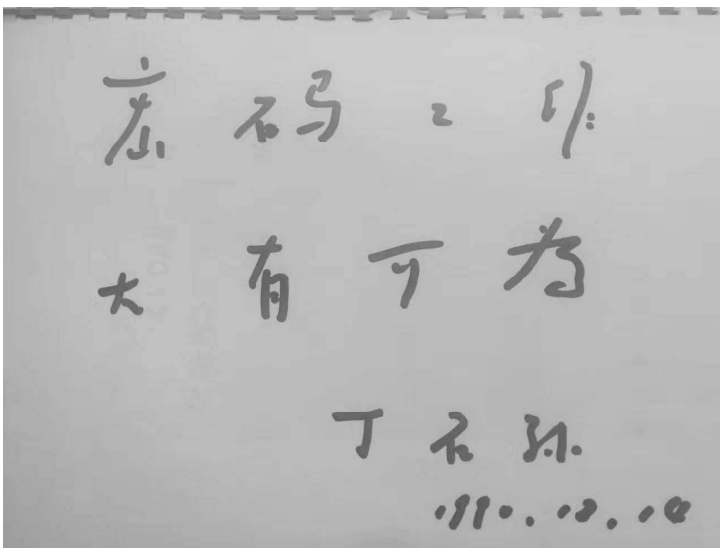
70年代，很多纯数学家都在寻找应用领域，而密码学是一个从纯数学到应用最短路径的分支。所以吸引了很多国内知名的数学家，如华罗庚、段学复、马大猷、柯召、丁石孙、聂灵沼、万哲先、曾肯成、戴宗铎、刘木兰、冯绪宁、肖国镇、王育民、王新梅、陶仁骥、

冯克勤等。他们的研究虽然仅涉及到序列密码方面，但是他们是中国高校和社会研究机构涉入密码研究的先驱。

2005年，在国家密码管理局的支持下，成立了中国密码学会正式的筹备组。筹备组由裴定一、冯登国、杨义先、吴成贵和我共五人组成，经过一年多的努力，在2007年正式成立，裴定一当选为第一届理事长。

谈到中国密码学会，人们一定会联想到丁石孙先生在1990年挂帅组成了“中国密码学会筹备组”。筹备组的核心成员包括丁石孙、曾肯成、裴定一、陶仁骥、肖国镇等，并在1990年12月份在中国科学院DCS中心召开了中国密码学会（筹）第一次大会，参会人员近150人。

会议议题包括学会筹备情况说明和学术交流。丁石孙在这次会议上被推选为理事长（筹）并为密码学会题字“密码工作，大有可为”表示祝贺。



丁石孙先生为中国密码学会（筹）题词

需要说明的是，尽管中国密码学会（筹）当时尚没有获得官方正式批复从而履行注册登记手续，但是从第一次会议开始，每两年一次的中国密码学会议一直开展到2006年，共举办了九次会议，对促进中国密码学的研究和密码技术的应用起到了重要作用。

听丁石孙先生讲课是一种最为愉快的享受。丁石孙、王元等在1990年冬天，在中科院举办了一个学习班。王元讲授初等数论、丁石孙主讲椭圆曲线密码。我当时在北京大学跟随段学复先生攻读代数和密码学的博士学位，对椭圆曲线还是刚刚接触，理解起来觉得有一定困难。但是，当丁先生开始讲授后，一切均出乎我的预料。他声音洪亮、从最初等的角度入手逐步深入，一切困难在他的讲座中全部化解。他仅用几次课就把椭圆曲线基础理论、椭圆曲线密码的算法理论等完全讲明白了。

丁石孙先生是一位在中国密码学发展史上做出了重要贡献的科学家。

（作者为北京大学教授、网络空间安全研究院院长）