国家出版基金资助项目

现代数学中的著名定理纵横谈丛书

丛书主编　王梓坤

Rivest-Shamir-Adleman System—Public Cryptography

Rivest-Shamir-Adleman体制
——公钥密码学

曹珍富　著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

国家出版基金资助项目

现代数学中的著名定理纵横谈丛书

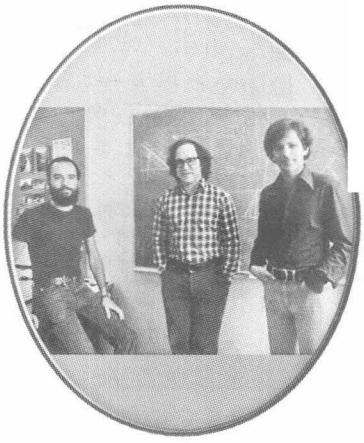
丛书主编　王梓坤

Rivest-Shamir-Adleman System—Public Cryptography

Rivest-Shamir-Adleman体制

——公钥密码学

曹珍富　著



哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书全面地总结了公钥密码学从1976年提出公钥密码体制(PKC)的概念到如今形成较为系统的公钥密码学的主要成果.通过本书读者可对各种密钥体制的构作方法、安全性分析以及用于数字签名讨论等有深刻地了解.

本书适合从事计算机科学、通信理论、密码学、计算复杂性理论、数论、组合数学、线性代数、有限域、编码理论等工作的科技人员及高等院校有关专业的师生参考.

图书在版编目(CIP)数据

Rivest-Shamir-Adleman体制:公钥密码学/曹珍富著.—哈尔滨:哈尔滨工业大学出版社,2016.1
(现代数学中的著名定理纵横谈丛书)
ISBN 978-7-5603-5100-1

Ⅰ.①R… Ⅱ.①曹… Ⅲ.①公钥密码系统—高等学校—教材 Ⅳ.①TN918.2

中国版本图书馆CIP数据核字(2014)第303521号

责任编辑 刘培杰 张永芹
封面设计 张永芹 关虹玲
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街10号 邮编150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 牡丹江邮电印务有限公司
开 本 787mm×960mm 1/16 印张15.25 字数200千字
版 次 2016年1月第1版 2016年1月第1次印刷
书 号 ISBN 978-7-5603-5100-1
定 价 98.00元

⊙作者简介

曹珍富，国家杰出青年基金获得者，享受国务院特殊津贴。现任华东师范大学特聘教授，第十二届上海市政协常委。作为第一完成人或独立完成人获得教育部自然科学一等奖等省部级奖7项。从1981年开始发表学术论文以来，已在各种学术期刊、会议上发表400余篇高质量学术论文，SCI检索150余篇，EI检索260余篇，引用超过6000次，出版专著7部（包括1部CRC出版的英文专著）、主编（或副主编）全国教材两部，先后担任SCI国际期刊Computers & Security，Fundamenta Informaticae，Peer-to-Peer Networking and Applications，Security and Communication Networks，IEEE Transactions on Parallel and Distributed Systems和Wireless Communications and Mobile Computing等的副主编、编委或客座编辑。主持完成国家或省部级科研项目50余项，包括国家自然科学基金A3前

瞻计划项目、重点项目、杰出青年基金项目等重要科研项目。在高校执教30余年里，为国家有关部门科研人员、中科院和众多高校做邀请报告100余次，参与制定相关国家标准10余项，历任国家自然科学基金专家评审组成员、国家自然科学奖评委、中国科学院杰出成就奖评委、国家重点实验室评估专家等。

⊙代序

读书的乐趣.你最喜爱什么——书籍.

你经常去哪里——书店.

你最大的乐趣是什么——读书.

这是友人提出的问题和我的回答.真的,我这一辈子算是和书籍,特别是好书结下了不解之缘.有人说,读书要费那么大的劲,又发不了财,读它做什么?我却至今不悔,不仅不悔,反而情趣越来越浓.想当年,我也曾爱打球,也曾爱下棋,对操琴也有兴趣,还登台伴奏过.但后来却都一一断交,"终身不复鼓琴".那原因便是怕花费时间,玩物丧志,误了我的大事——求学.这当然过激了一些.剩下来唯有读书一事,自幼至今,无日少废,谓之书痴也可,谓之书橱也可,管它呢,人各有志,不可相强.我的一生大志,便是教书,而当教师,不多读书是不行的.

读好书是一种乐趣,一种情操;一种向全世界古往今来的伟人和名人求

教的方法，一种和他们展开讨论的方式；一封出席各种社会、体验各种生活、结识各种人物的邀请信；一张迈进科学官殿和未知世界的入场券；一股改造自己、丰富自己的强大力量.书籍是全人类有史以来共同创造的财富，是永不枯竭的智慧的源泉.失意时读书，可以使人重整旗鼓；得意时读书，可以使人头脑清醒；疑难时读书，可以得到解答或启示；年轻人读书，可明奋进之道；年老人读书，能知健神之理.浩浩乎！洋洋乎！如临大海，或波涛汹涌，或清风微拂，取之不尽，用之不竭.吾于读书，无疑义矣，三日不读，则头脑麻木，心摇摇无主.

潜能需要激发

我和书籍结缘，开始于一次非常偶然的机会.大概是八九岁吧，家里穷得揭不开锅，我每天从早到晚都要去田园里帮工.一天，偶然从旧木柜阴湿的角落里，找到一本蜡光纸的小书，自然很破了.屋内光线暗淡，又是黄昏时分，只好拿到大门外去看.封面已经脱落，扉页上写的是《薛仁贵征东》.管它呢，且往下看.第一回的标题已忘记，只是那首开卷诗不知为什么至今仍记忆犹新：

日出遥遥一点红，飘飘四海影无踪.

三岁孩童千两价，保主跨海去征东.

第一句指山东，二、三两句分别点出薛仁贵（雪、人贵）.那时识字很少，半看半猜，居然引起了我极大的兴趣，同时也教我认识了许多生字.这是我有生以来独立看的第一本书.尝到甜头以后，我便千方百计去找书，向小朋友借，到亲友家找，居然断断续续看了《薛丁山西征》、《彭公案》、《二度梅》等，樊梨花便成了我心中的

女英雄.我真入迷了.从此,放牛也罢,车水也罢,我总要带一本书,还练出了边走田间小路边读书的本领,读得津津有味,不知人间别有他事.

当我们安静下来回想往事时,往往会发现一些偶然的小事却影响了自己的一生.如果不是找到那本《薛仁贵征东》,我的好学心也许激发不起来.我这一生,也许会走另一条路.人的潜能,好比一座汽油库,星星之火,可以使它雷声隆隆、光照天地;但若少了这粒火星,它便会成为一潭死水,永归沉寂.

抄,总抄得起

好容易上了中学.做完功课还有点时间,便常光顾图书馆.好书借了实在舍不得还,但买不到也买不起,便下决心动手抄书.抄,总抄得起.我抄过林语堂写的《高级英文法》,抄过英文的《英文典大全》,还抄过《孙子兵法》,这本书实在爱得狠了,竟一口气抄了两份.人们虽知抄书之苦,未知抄书之益,抄完毫末俱见,一览无余,胜读十遍.

始于精于一,返于精于博

关于康有为的教学法,他的弟子梁启超说:"康先生之教,专标专精、涉猎二条,无专精则不能成,无涉猎则不能通也."可见康有为强烈要求学生把专精和广博(即"涉猎")相结合.

在先后次序上,我认为要从精于一开始.首先应集中精力学好专业,并在专业的科研中做出成绩,然后逐步扩大领域,力求多方面的精.年轻时,我曾精读杜布(J. L. Doob)的《随机过程论》,哈尔莫斯(P. R. Halmos)的《测度论》等世界数学名著,使我终生受益.简言之,即"始于精于一,返于精于博".正如中国革命一

样，必须先有一块根据地，站稳后再开创几块，最后连成一片.

丰富我文采，澡雪我精神

辛苦了一周，人相当疲劳了，每到星期六，我便到旧书店走走，这已成为生活中的一部分，多年如此. 一次，偶然看到一套《纲鉴易知录》，编者之一便是选编《古文观止》的吴楚材. 这部书提纲挈领地讲中国历史，上自盘古氏，直到明末，记事简明，文字古雅，又富于故事性，便把这部书从头到尾读了一遍. 从此启发了我读史书的兴趣.

我爱读中国的古典小说，例如《三国演义》和《东周列国志》. 我常对人说，这两部书简直是世界上政治阴谋诡计大全. 即以近年来极时髦的人质问题（伊朗人质、劫机人质等），这些书中早就有了，秦始皇的父亲便是受害者，堪称“人质之父”.

《庄子》超尘绝俗，不屑于名利. 其中“秋水”、“解牛”诸篇，诚绝唱也.《论语》束身严谨，勇于面世，“己所不欲，勿施于人”，有长者之风. 司马迁的《报任少卿书》，读之我心两伤，既伤少卿，又伤司马；我不知道少卿是否收到这封信，希望有人做点研究. 我也爱读鲁迅的杂文，果戈理、梅里美的小说. 我非常敬重文天祥、秋瑾的人品，常记他们的诗句：“人生自古谁无死，留取丹心照汗青”，“谁言女子非英物，夜夜龙泉壁上鸣”. 唐诗、宋词、《西厢记》、《牡丹亭》，丰富我文采，澡雪我精神，其中精粹，实是人间神品.

读了邓拓的《燕山夜话》，既叹服其广博，也使我动了写《科学发现纵横谈》的心. 不料这本小册子竟给我招来了上千封鼓励信. 以后人们便写出了许许多多的

“纵横谈”.

从学生时代起，我就喜读方法论方面的论著. 我想，做什么事情都要讲究方法，追求效率、效果和效益，方法好能事半而功倍. 我很留心一些著名科学家、文学家写的心得体会和经验. 我曾惊讶为什么巴尔扎克在51年短短的一生中能写出上百本书，并从他的传记中去寻找答案. 文史哲和科学的海洋无边无际，先哲们明智之光沐浴着人们的心灵，我衷心感谢他们的恩惠.

读书的另一面

以上我谈了读书的好处，现在要回过头来说说事情的另一面.

读书要选择. 世上有各种各样的书：有的不值一看，有的只值看20分钟，有的可看5年，有的可保存一辈子，有的将永远不朽. 即使是不朽的超级名著，由于我们的精力与时间有限，也必须加以选择. 决不要看坏书，对一般书，要学会速读.

读书要多思想. 应该想想，作者说得对吗？完全吗？适合今天的情况吗？从书本中迅速获得效果的好办法是有的放矢地读书，带着问题去读，或偏重某一方面去读. 这时我们的思维处于主动寻找的地位，就像猎人追找猎物一样主动，很快就能找到答案，或者发现书中的问题.

有的书浏览即止，有的要读出声来，有的要心头记住，有的要笔头记录. 对重要的专业书或名著，要勤做笔记，“不动笔墨不读书”. 动脑加动手，手脑并用，既可加深理解，又可避忘备查，特别是自己的灵感，更要及时抓住. 清代章学诚在《文史通义》中说：“札记之功必不可少，如不札记，则无穷妙绪如雨珠落大海矣.”许多

大事业、大作品，都是长期积累和短期突击相结合的产物．涓涓不息，将成江河；无此涓涓，何来江河？

爱好读书是许多伟人的共同特性，不仅学者专家如此，一些大政治家大军事家也如此．曹操、康熙、拿破仑、毛泽东都是手不释卷，嗜书如命的人．他们的巨大成就与毕生刻苦自学密切相关．

王梓坤

⊙再版前言

写于二十多年前的《公钥密码学》了。

这本书写作较早，初稿写成于1989年10月。后来，给研究生开课，当时的研究生王立华（现在是日本NICT研究员）提出可以帮我将初稿誊写到稿纸上。于是，我一边修改、她一边抄写，除了书中第5章外，其他几乎全部章节均由她抄写到了稿纸上，至1992年9月全书完成、交稿。

那个时候，密码资料奇缺，信息不通畅。完全不知道，世界上与我同时在写作完全相同书名的一位学者——欧洲科学院院士Arto Salomaa教授，他也在像我一样“独创着”、“构思着”并于1990年出版了他的书。他的书在我的书出版了好几年后才看到。后来，他的书在国内还有了中文译本。提这件事的目的是，我们虽然天各一方，却独立地在构思和创作相同书名的书，确是很巧很巧的事情。正因为这样，这两本书

也有很大的不同。

Arto Salomaa 教授的书写了六章(经典双向密码学、公钥思想、背包系统、RSA 系统、密码系统的其他基础、密码方案:通信中的惊人应用)、两个附录(复杂度理论讲座、数论讲座),我的这本书写了十章(公钥密码学的理论基础、RSA 体制及其推广、基于二次剩余理论的 PKC、概率体制(PEC)、一次背包体制与分析、二次背包体制、基于编码理论的 PKC、基于离散对数的 PKC、其他形式的 PKC、密钥分散管理方案),两本书有交集,而且即使交集部分在材料的取舍上也有很大不同。Arto Salomaa 教授更多的是搜集整理,而我的更多的是以自己的工作为主。

所以,今天再读我的这本书感觉仍有几点内容向读者推荐:

(1)2 次密钥概念是国际上首次提出,可以看成无授权的重密钥方案,亦即重密码最早的雏形。现在分为授权的重密码(即代理重密码)和无授权的重密码。

(2)Eisenstein 环上的密码是国际上较早提出的新理论、新方法。

(3)K 次剩余密码至今还有重要的参考价值。

(4)关于二次背包的研究,许多思想是现今"格密码"的出发点。

事实上,那个年代有许多"好方案"是不发表的,例如,我提出的"加标识位的密码"、"多维 RSA"(这个后来发表在《中国科学》英文版上,见 Zhenfu Cao: The multi－dimension RSA and its low exponent security, Science in China (Series E), 43(4), 349-354, 2000)、"等价于 Eisenstein 整数分解的密码"等。在

30余年的教学和科研中，其实密码学的内容在不断扩大，除了上面提到的这些“好方案”均陆续教给了学生们外，连同后来新发现的密码方案、构造方法和可证明安全等内容，只要在课堂上能讲得清楚的，均毫无保留地教给了学生们。

哈工大出版社刘培杰先生是我几十年的朋友，他提出要重印我的这本书。这本是高兴的事，因为这本书在市场上绝迹应该有二十年了。当时出版数量就很小，而且大部分需要我购买和典当“稿费”，社会上能见到的极少。确如《太阳照在桑干河上》的作者在重印前言中所说，“只剩有极少几本收藏在黑暗尘封的书库里，或秘藏在个别读者的手中。”本想将这本书扩展后再出版，因为有太多的新内容需要放进去，听过我的课的同学都知道，有相当多的自创的新内容、新思想也值得放进去。但苦于没有太多的时间，只好一边答应重印、一边扩写本书内容。争取尽快完成扩展工作，将最新最好的公钥密码学呈现给读者。

心如此，还是不要期望太高。无论如何，都要感谢刘培杰先生和他的出版团队，使得今天的读者能够读到这本二十多年前出版的书。期望读者能提出宝贵意见，以便我在扩展版中改进和借鉴。

曹珍富（华东师范大学）

二零一五年七月七日于上海

⊙前言

在计算机的网络中，计算机之间以惊人的速度互相交换着信息.这些信息的每个用户都可以发送与接收.然而，很多时候，发送这些信息的用户希望只用合法的用户（接收者）才能读懂信息的内容，而其他用户均不能读懂.例如商业中，股票市场的“买进”与“卖出”，与外商谈判等，或国家安全、军事与外交部门的秘密指令等，均属于这类信息.所以，研究计算机网络中任一用户都可以和其中的一个用户进行秘密交换信息（秘密通道）就是一项重要的课题.

传统的密码体制是通过通信双方共同约定的密钥来加、解密的，这显然不适用计算机网络上的秘密通信.1976年，美国斯坦福大学的Diffie与Hellman在“密码学的新方向”一文中提出了公钥密码体制（Public Key Cryptosystem）的新概念，可用于解决前面提出的问题，因而开创了现代密码学的新

领域[71]. 1978 年，Rivest，Shamir 与 Adleman 基于大整数分解的困难性提出了第一个公钥密码体制(RSA 体制). 后来，关于这一领域的研究如雨后春笋，不仅提出了一系列公钥密码体制，还由此引出了很多应用与新的概念. 例如，公钥密码体制用于数字签名，概率加密体制，门限方案等等. 同时，也有一些公钥密码体制被先后破译. 这就形成了较为系统的公钥密码学.

研究公钥密码学，不仅需要传统密码学的一些知识，而且需要计算复杂性理论、数论、组合数学、线性数学、有限域、有限状态机、椭圆曲线算术以及编码理论等方面的知识. 这些知识都已经被成功地用于构造与分析公钥密码体制.

作者于 1986 年以“数论、公开钥密码体制”为题申报中国科学院首次对全国开放的青年奖励研究基金资助获得批准. 1989 年顺利完成这一课题，其中“公钥密码体制及其计算机实现”[77]获航空航天工业部科技进步三等奖. 自 1990 年起，国家自然科学基金对作者这方面的研究给予连续性资助.

本书试图较为系统地、全面地介绍公钥密码学已形成的成果与方法，其中作者的工作分别被写进了第 2、4、5、6、9、10 章. 下面扼要介绍一下本书 的主要内容.

第 1 章主要介绍密码学的基本理论，包括 Shannon 信息论与计算复杂性理论的基本概念与方法. 同时对公钥密码学的基本概念与产生的背景做了论述.

第 2 章在介绍欧几里得(Euclid)算法与欧拉(Euler)定理的基础上，进一步介绍了 RSA 体制，给出了 RSA 体制加、解密变换的严格证明. 同时分析了 RSA

体制的安全性与用于数字签名的方法.最后,介绍了RSA体制在代数整数环 $\mathcal{Z}[\theta]$ 上的推广与讨论.

第3章介绍RSA体制的各种修改.在介绍同余式、孙子定理与二次剩余理论之后,介绍了Rabin,Williams以及Kurosawa等建立的三类公钥密码体制.

第4章介绍各种与大整数有关的概率体制(PEC)与强数字签名方案,同时论述了对强数字签名的消息进行加密的方法.最后介绍利用公钥密码体制构作概率体制的一般方法.

第5章在介绍著名的MH背包体制之后,论述了在破译一次背包体制中起决定性作用的规约基L的3次方一算法.由此算法,不难证明大部分的一次背包体制均是可破译的(第5章5.3).

第6章论述了二次背包体制的构作方法,特别介绍了MC概率背包体制、线性分拆背包体制的构作以及构作二次背包体制的几种新的方法.这方面的公钥密码体制均是近年来才提出的,安全性尚需时间的考验.

第7章介绍有限域与Gpooоa码的基本知识,同时用于介绍McEliece与Niederreiter分别构作的两类基于编码理论的公钥密码体制.最后介绍纠错码用于数字签名的方法.

第8章论述了用离散对数构作公钥密码体制的方法.对其中用到的一般的离散对数问题、原根、离散对数的计算方法与椭圆曲线算术,也做了相应的介绍.最后介绍奇特的Chor-Rivest体制.

第9章论述用有限状态机、丢番图方程构作公钥