中国人民解放军
信息工程大学

博士研究生文库

对现代科学技术的
哲学思考

周效坤 米立根 主编

军事科学出版社

中国人民解放军
信息工程大学 博士研究生文库

对现代科学技术的
哲学思考

主　编　周效坤　米立根
副主编　王杰锋　周东方
魏　峰

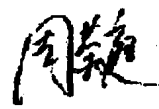
军事科学出版社

(京)新登字 122 号

对现代科学技术的哲学思考

军事科学出版社出版
(北京市海淀区青龙桥　100091)
信息安全学院印刷厂印刷　新华书店发行所经销
2000 年 8 月第 1 版　　2000 年 8 月第 1 次印刷
开本：850×1168　1/32　印张：13
字数：300 千字　印数：1－1000 册
统一书号：380137·010
定价：22.00 元
(军内发行)

序　言



当代科学技术革命及其辉煌成就，极大地改变了世界的面貌和人类的生活，改变和继续改变着社会的生产方式、生活方式和思维方式。世纪之交，以信息技术为先导，以生物技术、新材料技术、新能源技术、空间技术和海洋技术为主要内容的科学技术革命，突飞猛进，渗透于经济发展和社会生活的各个领域，成为现代生产力发展的最活跃因素，促使经济形态发生深刻变革，知识经济已见端倪，国力竞争日趋激烈，军事领域也正在发生着一场深刻的变革。当今世界，科学技术已成为对国家和民族兴衰起决定作用的一种力量。综合国力的竞争，主要是科学技术的竞争。实行科教兴国、科技强军战略，科技是关键，人才是根本，教育是基础。培养大批高素质的科学技术人才，是国家兴旺，民族振兴的根本大计。

为迎接世界军事变革的挑战，实现我军跨世纪战略目标，推进质量建设，顺应高等教育的发展潮流，中央军委作出了合并组建几所高水平综合大学的决策，我们

信息工程大学应运而生，担负着为全军培养高素质国防信息人才的任务。其中培养博士研究生，使他们成为我军新一代在信息战领域、数字化战场上的专家骨干是办好综合性大学的一项神圣使命。而要博士研究生承担起自己的历史责任，必须通过系统的教学实践来锻炼，使他们具有坚定的政治信仰、渊博的专业知识，具有独特的创新能力和辩证的思维方法。马克思主义作为科学的世界观和方法论，是人类一切优秀思想文化成果的结晶，是正确认识客观真理的思想武器，是科学技术研究的指南。在博士研究生中开设“现代科学技术革命与马克思主义”课程，结合科学技术革命的内容、影响和发展趋势深入进行辩证唯物主义和历史唯物主义的教学，不仅可以为坚定理想信念打下牢固的理论基础，而且有助于开阔知识的视野，提高理论思维的能力。

我校信息安全学院和信息技术学院自1994年招收第一届博士研究生以来，按照军委、总部和国家教委的要求，把“现代科学技术革命与马克思主义”课程作为必修课进行教学，至今已历六届，毕业生百余名。博士们在导师的指导下，认真学习辩证唯物论和历史唯物论，运用马列主义、毛泽东思想和邓小平理论的基本观点，分析研究现代科学技术革命的内容与特征、社会功能与影响、发展规律与趋势，探讨创造性思维的本质和形式，加深对党和国家发展科学技术事业路线方针政策的理解，提高辩证思维能力，增强社会历史责任感和科学道德修养，作了大胆的尝试，取得了良好效果。

这里收编结集的文章，是我校信息安全学院和信息技术学院历届博士研究生在学习了“现代科学技术革命与马克思主义”课程之后撰写的部分结业论文。他们运用唯物辩证法和历史唯物论的基本观点，结合自己学习和科研实践的体验，对现代科学技术革命及相关学科中的问题作了认真的哲学思考。他们在文章中回顾了相关学科的辩证发展过程，探讨和总结了发展的原因和动力，审视和概括了相关学术前沿的基本问题，预测了今后可能的发展方向，分析了我国相关技术和产业的发展现状、存在问题和相应对策，内容广泛，见解独到。这些文章，作为一个教学成果，所提问题和阐述的观点，不仅是对学习收获的检验，而且对以后的教学和研究也具有启发性和参考价值。

周荣庭　解放军信息工程大学校长、少将、教授、研究生导师。

目　录

略论数学对密码学发展的影响

戚文峰

【摘要】本文从五个角度分析了数学对现代密码学发展的影响：(1) 密码学广泛涉及的数学领域；(2) 数学理论和成果的直接应用；(3) 密码学研究过程中所产生的数学问题；(4) 总体数学思想对密码学发展的影响；(5) 数学对密码学发展的间接影响。在文章的最后还指出了数学不是研究密码的唯一工具。

一、密码学发展概况

在古代，人们已经意识到在传送消息过程中，某些消息需要采取保密措施。同时，人们也为了自己的利益，千方百计地获取他人的秘密情报，这样就逐渐形成了密码体制的编制和破译技术。

密码学的历史大致经历了以下几个阶段：从古代到本世纪20年代，密码体制的编制和破译能够用笔和纸或简单的器械来实现，那时的密码专家常常是凭直觉来进行密码设计和分析的，而不是靠推理证明，他们有丰富的经验，但缺乏系统的理论；20年代初至40年代末这个时期的密码与早期的密码相比，从设计思想来说并无多大差别，所不同的是采用了复杂的机械设备；1949年申农（Shannon）发表了划时代的论文《保密系统中的通信理论》（Communication Theory of Secrecy Systems），它证明了密码学如何能置于坚实的数学基础上。从而使密码学形成一整套系统的理论，而不再仅仅停留于经验和直觉上，从此密码成为一门真正的

科学，现代密码学随之诞生；60年代的微电子的发展为实现Shannon的思想提供了硬件设备，以数学中代数学为理论依据的电子密码随之产生，电子密码（或称流密码）至今仍是军事和外交上使用的主要加密体制；1976年Diffie和Hellman发表了著名的《密码学新方向》（New Directions in Cryptography）一文，导致了密码学上的一场革命，他们首次证明了在发端和收端无密钥传输的保密通信是可能的，这就是所谓的公开密钥体制，以后产生的一些公开密钥体制理论依据主要是数学中的大数分解理论和离散对数理论。

二、数学对早期密码的影响

不管是早期密码还是现代密码，不管是密码编制思想还是密码的破译思想，无不包含着丰富的数学思想和方法。从一定意义上说，数学的发展水平影响和制约着密码的发展水平。

我们以二千多年前意大利凯撒（Caesar）大帝使用过的密码来说明在古代，人们尽管还没有掌握丰富的数学理论，但早期的密码中已体现出丰富的数学思想。公元前100年，凯撒大帝所使用的是所谓的Caesar密码，在这种密码体制中，明文消息中的每个字母均用在它后面的第三个字母来代换，这种代换关系如下表所示：

明文字母表 a b c d e f g h i j k l m n o p q r s t u v w x y z

密文字母表 d e f g h i j k l m n o p q r s t u v w x y z a b c

例如下面的一条明文和对应的密文就是按照上述代换关系产生的，

明文 zhengzhou information engineering institute（郑州信息工程学院）

密文 ckhqjckrx lqirupdwlrq hqjlqhhulqj lqvwlwxwh

一条有明确意义的明文，经过上述加密代换，就变成了一条

表面上看去似乎毫无规律的乱七八糟的字母组合，脱密的办法是把每个密文字母向后移三位（其中 c→z，b→y，a→x）。事实上，这一加密和脱密过程可由数论中的同余运算表出，我们把 a 到 z 的字母与数字 1，2，…，25，0，按下表对应：

a	b	c	d	e	f	g	h	i	j	k	l	m
1	2	3	4	5	6	7	8	9	10	11	12	13
n	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	0

每个字母看作是 0 至 25 中的一个数，即用数字代表字母，那么 Caesar 密码的加密数学模型就是同余式：$\beta = \alpha + 3 \pmod{26}$ 其中 α 代表明文字母，β 代表密文字母。例如：$8 + 3 = 11 \pmod{26}$，而 8 代表 h，11 代表 k，从而 k 是 h 的密文字母，又如：$24 + 3 = 1 \pmod{26}$，而 24 代表 x，1 代表 a，从而 a 是 x 的密文字母。同样 Caesar 密码的脱密数学模型为：

$$\alpha = \beta - 3 \pmod{26}$$

对 Caesar 密码可稍作推广：设 N 是 1 至 25 中任一数，加密为

$$\beta = \alpha - N \pmod{26}$$

脱密为 $\alpha = \beta - N \pmod{26}$

这就是一般加法密码的数学模型。

Ceasar 密码是 2000 多年前人们使用过的密码，当时人们并没有数学中的同余知识，更没有用数学来处理保密问题的意识，人们是在无意识中把某些数学思想运用于密码中。

还有许多早期的密码，从表面上看似乎只是一些复杂的技巧，但经过仔细分析，可以发现其中包含着大量数学思想，也可以发现许多值得研究的数学问题。

三、数学对现代密码学发展的影响

下面谈谈数学对现代密码学的影响。

自 Shannon 于 1949 年发表了著名论文以后，数学对密码学的影响越来越大，当今的密码是置于现代数学理论之上，每个密码体制都经过严密的数学论证，破译者也是充分利用现有的数学工具对遇到的体制进行破析，在破译过程中有些问题归结为一个新的数学问题，然后对该问题作纯数学研究。这一正反过程包含了丰富的数学思想和方法。所以不论是密码的编制、破译还是一般的密码理论研究，都离不开数学这一强有力的工具。数学对现代密码学的影响主要有如下几个方面：

1. 密码学中所涉及到的数学领域非常广泛，几乎包括了当今数学的各个分支。最常用的数学理论有：代数学（包括有限域、群论、域论、环论、模论、交换代数等）、代数数论、代数几何、椭圆曲线、组合论、概率论、数理统计、运筹学、函数论、微分方程、拓扑学等。有些密码理论甚至应用了数学中的当前最高深的理论和最新的研究成果，有些密码问题与当今数学家们所研究的著名数学难题甚至与数百年来一直未能解决的数学难题有直接的联系。所以当今的密码工作者必须具备很高的数学造诣，这样才有可能做出高水平成果。

2. 许多现有的数学成果被直接应用于密码，对密码的发展产生巨大的推动作用。Shannon 于 1949 年证明了密码学如何能置于坚实的数学基础上，从此人们开始有意识地运用现有的数学理论研究和分析密码体制。受 Shannon 思想影响，60 年代出现的电子密码（也称流密码）就是数学成果直接应用于密码的一个例子，建立流密码体制的基础和研究流密码的主要工具是数学中的有限域理论，而这一理论在当时已相当完善。对于流密码体制中密钥序列的周期、随机特性等性质可由有限域理论中现有的成果直接

获得。

数学被许多人认为是与现实生活无关。很多数学理论确实非常抽象，这些理论在很长一段时期内对人类的现实活动不产生任何影响，最典型的例子是数学中的一个重要分支数论，著名数学家 G.H.Hardy 于 1940 年称“数论远离人类的实践活动”。然而，1976 年当 Diffie 和 Hellman 的《密码学新方向》一文发表后，数论不但进入了人类的实践活动，而且还导致了现代密码学上的一场革命，运用数论中大数分解和离散对数问题，成功地建立了公开密钥密码体制，使得通信中的发端和收端在无密钥传输下进行保密通信成为可能。

3. 随着现代密码学研究的深入，在密码的设计与分析过程中，经常遇到现成的数学理论无法直接解决的一些问题，也就是说，在研究密码过程中，往往会产生新的数学问题，有些问题是纯数学工作者难以遇到和难以想象的。密码工作者经常需要自己去解决这些难题，这也是我们时常看到研究密码的人发表一些优秀的数学论文的原因。许多密码问题抛开其背景后就是一个十足的数学问题，对这些问题的深入研究，有助于数学本身的发展。反过来数学运用于密码学，又将进一步影响密码学的发展。这一影响的程度之大有时是难以预料的，原因有二方面：一是因为某个密码问题所产生的数学问题可能与其它的密码问题也有关系，解决一个问题往往会影响一大片；二是因为在解决一个由密码问题引出的数学问题过程中，常常会引发并解决其它一些新的数学问题，因为许多密码问题都有内在的联系，问题中的问题很可能就是其它密码问题中所要解决的关键问题。由此看来一个密码工作者在具有较雄厚的数学基础同时，还必需具备解决数学难题和联想问题的能力。

4. 在密码的设计与分析过程中要使用大量技巧和构思，这些技巧和构思表面上看并不是数学成果的应用，更不属于哪个数

学分支，它实际上是整体数学思想的综合运用，这一点对密码学发展的影响要比一般数学结果的应用大得多，有时甚至是划时代的和革命性的。例如，公开密钥密码体制总体设想的提出归功于丰富的数学思想，用到的其中之一的数学思想就是单向性或逆问题的难解性，至于具体的各个体制的构造则由具体的数学理论或成果来实现和完成。只有具有很高数学造诣的学者才有可能运用这些数学思想于密码的研究中。

5. 想谈的最后一点就是数学对密码学发展的间接影响。现代密码不论编制还是破译，最后都是依赖于计算机来实现一切设想，计算机运行速度的快慢直接影响着所作的设想能否最终实现。而数学对计算机发展的影响是众所周知的，对计算机发展产生最大影响的一门学科数理逻辑，就是数学中的一门分支。另外代数学中的许多理论都已对计算机的发展产生重大作用，一些重大数学成果直接应用于计算机的设计中。每当计算机的运行能力增强时，一大批原有的密码体制要被淘汰或必须进一步被改进；计算机运行速度的提高也使原来难以实现的密码体制进入实用阶段。所以数学对计算机发展的影响并由此对密码学发展的影响是相当大的。

四、数学不是研究密码的唯一工具

前面已经谈了数学对密码学发展的影响，可以这么说：没有数学就没有现代密码学。然而密码是一项系统工程，在实现过程中还需要电子、通信、计算机等领域的知识。一个密码编制者或破译者只考虑数学上的完美性，而忽略或不懂实现中的技术问题，他将难以实现自己的设想。除了硬件工程外，还需有文字语言知识，每个国家都有自己的文字语言特点，这种特点必定会反映在密码的运用上，一个密码编制者应尽力克服这种语言文字特点的现象，而作为破译者要充分利用这一点。

因此我们可以认为数学是现代密码学的重要基础和研究工具，它对密码学的发展产生巨大的影响，但密码学并不是完全可由数学来处理。

参 考 文 献

[1]《现代科学技术革命与马克思主义文献选编》，厦门大学出版社，1993.

[2]C.E.Shannon,"Communication Theory of Secrecy System", Bell Sys.Tech.J.28 (1949),pp.657-715.

[3]W.Diffie and M.E.Hellman,"New Direction in Cryptography",Trans.IEEE Inform. Theory, IT-22(1976), pp.644-654.

[4]J.H.Loxton,《Number Theory and Cryptography》,Worl Publishing Corp.1990.

[5] N.Koblitz,《A Course in Number Theory and Cryptography》, Springer-Verlag, 1987.

作者简介：戚文峰，男，1963 年 7 月生，信息工程学院 94 级博士研究生，研究方向密码学，现为信息工程大学信息安全学院教授。博士论文被评为全国优秀博士论文，近年来先后有 6 篇论文被 SCI 检索，97 年获国家自然科学基金资助，2000 年获军队科技进步二等奖一项。

漫谈转化思想在数学解题中的应用

陈　晓

【摘要】本文阐述了数学解题中转化技巧的哲学根据；分析了费尔马最后定理证明中转化技巧的成功运用；提出了转化技巧的三种基本模式；对如何掌握转化技巧问题，提出了三条建议。

一、数学解题中转化技巧的哲学根据

数学是关于量和形的科学。从古到今，它是定量的描述和精确的研究所不可或缺的工具。作为一门学科，数学本身也是不断发展的，它揭示未知的量与量的关系，揭示未知的结构，从已知到未知的探索，使得数学工作者每时每刻都需要面对问题。所以，学习数学和研究数学都离不开解题。

所谓解题，就是要给出一个简洁明了的表示形式，突出地表现数学因素之间的内在联系。当然，这些内在的联系在解题前总是隐藏在内部，凭纯粹的观察或简单的演绎都难以揭示这些内在联系。那么怎么办呢？只有一条路，就是把问题进行适当的转化，把问题转化到我们的能力和知识能够把握的问题上来，这样，我们就可以用自己熟悉的结论或工具去解决一个并不太容易解决的问题。

这种转化技巧在数学解题中使用得非常普遍，这是符合事物存在和发展的规律的。数学研究对象量与形，关系与结构都是客观事物的概括和抽象。客观事物的矛盾反映在数学中，使得所有数学问题成为矛盾的统一体。它不仅包含诸多矛盾，其中有主要