完全映射及其密码学应用

Complete Mapping and Application in Cryptography

吕述望　范修斌
王昭顺　徐结绿　著
张　剑

中国科学技术大学出版社

当代科学技术基础理论与前沿问题研究丛书

完全映射及其密码学应用

Complete Mapping and Application in Cryptography

吕述望　范修斌
王昭顺　徐结绿　著
张　剑

中国科学技术大学出版社

内 容 简 介

本书对完全映射相关理论进行了系统的总结，在此基础上，进一步介绍了两类完全映射：正形置换与全向置换．书中给出了主要面向密码算法设计的几种正形置换发生器的研究结果，为完全映射在密码学中的具体应用做好了准备．

为阐述完全映射理论在密码算法设计中的应用，本书进一步给出了SP网络密码算法、Feistel网络密码算法的线性与差分安全性分析技术，并介绍了上述两种算法与正形置换之间的关系．

在上述工作的基础上，本书进一步介绍了P逻辑密码算法，并给出了其线性与差分安全性分析技术，从而使正形置换理论得到了比较系统的应用．

本书是专著《序列密码的设计与分析》(北京中软电子出版社，2003年1月)的姊妹篇．

本书可供信息安全、密码设计与分析等相关领域的研究和工作人员使用、参考．

Abstract

In this book, we introduce the theory of complete mapping, then the theory of orthomorphic permutation and omni-direction permutation. Several orthomorphic permutation generators are given.

We give the methods of linear and different analysis on the SP network cipher and Feistel network cipher, and the relations between the ciphers above and the orthomorphic permutation.

On the work above, the P logic cipher is studied, then the theory of orthomorphic permutation is used widely.

图书在版编目(CIP)数据

完全映射及其密码学应用 / 吕述望等著. —合肥：中国科学技术大学出版社，2008.12

(当代科学技术基础理论与前沿问题研究丛书；中国科学技术大学校友文库)

"十一五"国家重点图书

ISBN 978-7-312-02116-9

Ⅰ.完… Ⅱ.吕… Ⅲ.映射(数学)—应用—密码—理论 Ⅳ.TN918.1

中国版本图书馆CIP数据核字(2008)第062404号

出版 中国科学技术大学出版社

安徽省合肥市金寨路96号，邮编：230026

网址：http://press.ustc.edu.cn

印刷 合肥晓星印刷有限责任公司

发行 中国科学技术大学出版社

经销 全国新华书店

开本 710 mm×1000 mm 1/16

印张 17.5

字数 287千

版次 2008年12月第1版

印次 2008年12月第1次印刷

印数 1—2 000册

定价 58.00元

编　委　会

总　序

侯建国

（中国科学技术大学校长、中国科学院院士、第三世界科学院院士）

大学最重要的功能是向社会输送人才。大学对于一个国家、民族乃至世界的重要性和贡献度，很大程度上是通过毕业生在社会各领域所取得的成就来体现的。

中国科学技术大学建校只有短短的五十年，之所以迅速成为享有较高国际声誉的著名大学之一，主要就是因为她培养出了一大批德才兼备的优秀毕业生。他们志向高远、基础扎实、综合素质高、创新能力强，在国内外科技、经济、教育等领域做出了杰出的贡献，为中国科大赢得了“科技英才的摇篮”的美誉。

2008年9月，胡锦涛总书记为中国科大建校五十周年发来贺信，信中称赞说：半个世纪以来，中国科学技术大学依托中国科学院，按照全院办校、所系结合的方针，弘扬红专并进、理实交融的校风，努力推进教学和科研工作的改革创新，为党和国家培养了一大批科技人才，取得了一系列具有世界先进水平的原创性科技成果，为推动我国科教事业发展和社会主义现代化建设做出了重要贡献。

据统计，中国科大迄今已毕业的5万人中，已有42人当选中国科学院和中国工程院院士，是同期（自1963年以来）毕业生中当选院士数最多的高校之一。其中，本科毕业生中平均每1000人就产生1名院士和七百多名硕士、博士，比例位居全国高校之首。还有众多的中青年才俊成为我国科技、企业、教育等领域的领军人物和骨干。在历年评选的“中国青年五四奖章”获得者中，作为科技界、科技创新型企业界青年才俊代表，科大毕业生已连续多年榜上有名，获奖总人数位居全国高校前列。

鲜为人知的是，有数千名优秀毕业生踏上国防战线，为科技强军做出了重要贡献，涌现出二十多名科技将军和一大批国防科技中坚。

为反映中国科大五十年来人才培养成果，展示毕业生在科学研究中的最新进展，学校决定在建校五十周年之际，编辑出版《中国科学技术大学校友文库》，于2008年9月起陆续出书，校庆年内集中出版50种。该《文库》选题经过多轮严格的评审和论证，入选书稿学术水平高，已列为“十一五”国家重点图书出版规划。

入选作者中，有北京初创时期的毕业生，也有意气风发的少年班毕业生；有“两院”院士，也有IEEE Fellow；有海内外科研院所、大专院校的教授，也有金融、IT行业的英才；有默默奉献、矢志报国的科技将军，也有在国际前沿奋力拼搏的科研将才；有“文革”后留美学者中第一位担任美国大学系主任的青年教授，也有首批获得新中国博士学位的中年学者……在母校五十周年华诞之际，他们通过著书立说的独特方式，向母校献礼，其深情厚意，令人感佩！

近年来，学校组织了一系列关于中国科大办学成就、经验、理念和优良传统的总结与讨论。通过总结与讨论，我们更清醒地认识到，中国科大这所新中国亲手创办的新型理工科大学所肩负的历史使命和责任。我想，中国科大的创办与发展，首要的目标就是围绕国家战略需求，培养造就世界一流科学家和科技领军人才。五十年来，我们一直遵循这一目标定位，有效地探索了科教紧密结合、培养创新人才的成功之路，取得了令人瞩目的成就，也受到社会各界的广泛赞誉。

成绩属于过去，辉煌须待开创。在未来的发展中，我们依然要牢牢把握“育人是大学第一要务”的宗旨，在坚守优良传统的基础上，不断改革创新，提高教育教学质量，早日实现胡锦涛总书记对中国科大的期待：瞄准世界科技前沿，服务国家发展战略，创造性地做好教学和科研工作，努力办成世界一流的研究型大学，培养造就更多更好的创新人才，为夺取全面建设小康社会新胜利、开创中国特色社会主义事业新局面贡献更大力量。

是为序。

2008年9月

序

随着全球信息化进程的加快，信息安全问题凸现．密码作为信息安全的关键技术，其应用领域不断拓展，科研院所、高等院校纷纷进入密码研究领域，促进了密码科学的空前发展．

现代密码学沿着序列密码、分组密码、公钥密码和杂凑函数四个方向展开，构造安全高效的各类密码算法是密码研究的核心内容．吕述望教授领导的科研团队，十多年来坚持不懈，对密码算法中的最基本构件——置换进行了深入探索，在总结其研究成果的基础上，形成了颇具特色的《完全映射及其密码学应用》这本专著．作者从分析完全映射着手，对完全映射中的正形置换和全向置换这两类在密码学上有重要应用的置换展开研究，探讨了它们的基本性质、构造方法和计数问题，创造性地构造了 BCLL 正形置换发生器和 BDLL 正形置换发生器，并将其应用于密码算法 SMS4 的设计中．与此同时，他们将置换理论研究成果应用于分组密码的两类基本网络——SP 网络和 Feistel 网络中，探讨了它们各自的线性传播特性和差分传播特性，给出了一般计算公式，并将其结果推广于 P 逻辑中．著作较好地体现了密码理论与应用、编制与分析相结合的特色．

“山因势而变，人因思而变．”当前，面对日益增强的计算机处理能力和数学思想的进步，深入探索密码内在变换机理，拓展密码研究宽度和深度，发掘可用于密码构造的数学难题，丰富密码基础模块的构造、分析

方法，是密码学者所不懈追求的.希望《完全映射及其密码学应用》这本著作的出版，对大家有所帮助.

中国工程院院士

2008 年 5 月 15 日

前　言

众所周知，置换是一类在密码算法中使用相当广泛的特殊的密码函数.置换在密码算法中广泛使用的原因主要在于密码算法本身要求具有可逆性，即密文需要在密钥的作用下恢复出明文.所以在本书的第1章中，我们对密码学置换进行了介绍.

寻找具有良好密码学性质的置换类，显然具有重要的理论与实践意义.1942年，H. B. Mann为研究正交拉丁方而提出了“完全映射”这一概念.由于完全映射与正交拉丁方的构造有着密切的联系，在当时人们对完全映射已做过许多比较深入的研究.本书第2章是关于完全映射理论的介绍.

正形置换是一种完全映射，也是一种特殊的布尔置换.虽然完全映射的概念在半个多世纪之前就已经被提出，但将完全映射的概念和理论用于密码学，仅始于20世纪90年代初密码学界对正形置换的研究和讨论.关于密码学中正形置换的概念是由吕述望教授以及Mittenthal博士在各自的密码学研究工作中分别独立提出的.在我国，20世纪90年代初期，中国科学院DCS中心就提出并开始了正形置换的研究.到目前为止，已得到了不少有价值的研究结果，特别是基于正形置换的分组密码设计、分析的理论和技术已比较完善和自成体系.这是本书第3章中要介绍的主要内容.第4章简要介绍了另一类完全映射——全向置换.

在第5章、第6章SP网络以及Feistel网络研究结果的基础上，我们在第7章中进一步给出了P逻辑，该逻辑在实践中也得到了广泛的应

用，例如 SMS4、Fly 算法等都隶属于 P 逻辑.SP 网络以及 Feistel 网络皆为 P 逻辑的特例，即 SP 网络为“1”级 P 逻辑，Feistel 网络为“2”级 P 逻辑，从而使 SP 网络、Feistel 网络、SMS4 以及 Fly 算法等在 P 逻辑的概念上得以统一认识.书中同时给出了求 P 逻辑线性与差分 S-盒活动数的具体算法.在附录中给出了 SMS4 算法的原理、结构及实现.

在本书初稿的讨论过程中，一直得到徐克舰教授的指导、支持与帮助，在此表示衷心的感谢！他严谨的学风与治学态度使我们受益匪浅.

对孙同森、郭晓沛以及戈升波三位副教授在本书初稿的讨论过程中所付出的智慧与帮助表示衷心的感谢！

对博士研究生赵聆波、刘琦所付出的劳动表示衷心感谢！

衷心感谢硕士研究生刘广秀、戴照鹏、贺亮、刘秀玲以及张倩，他们在本书初稿历时两年的讨论过程中，放弃暑假，详细推导，逐字研读，使书稿更加严谨.他们那阳光般的微笑，驱走了我心灵的孤寂.

在该书的写作中，衷心感谢北京知识安全工程中心所提供的帮助与支持！

衷心感谢宋广娟女士所给予的理解与支持！

作 者

2008 年 5 月 30 日

目　录

第1章 引 论

随着计算机网络和通信技术的迅速发展与普及，信息安全在现代信息社会中占据着越来越重要的地位.信息安全已经成为国家安全、经济发展和社会稳定的重要保障和基本组成部分.然而，要构建安全的信息系统，必须使用密码技术，密码技术是安全信息系统的核心.密码技术主要由密码设计技术和密码分析技术两个分支组成.密码设计和密码分析都必须以一定的数学理论为基础，这在现代密码的设计与分析中表现尤为突出.由密码设计和密码分析的相互作用而逐渐发展和完善起来的密码设计理论具有极其丰富的内涵，其中密码函数的选取标准和设计技术是密码设计理论中讨论尤为广泛和持久的一类课题，它构成了密码设计理论的重要组成部分.

设计一个密码并不难，难的是如何分析清楚密码抗分析的复杂度.一个好的密码算法需要以构建好的密码函数为基础，密码体制或密码组件的设计是密码设计理论研究的基本内容.在这些基本内容的研究中，密码学安全性分析总是建立在各个密码组件的安全性分析基础之上的，因此，基本密码学映射或置换的研究对于构建好的密码算法具有重要意义.本章将从密码函数与置换、密码学对置换的需求等几个方面来讨论密码学中的有关置换理论.

1.1 密码函数与置换

密码函数在密码学中是一个涵盖内容相当广泛的概念，主要指用于构造密码算法的、具有密码学特征的数学函数.特别地，密码算法本身就是由若干基本密码函数复合而成的密码函数，此类密码函数的输入变元是明文和密钥，而输出的函数值是密文.密码学除了研究密码算法这类大的密码函数外，更基础的研究在于分析和构造具有良好密码学性质的基本密码函数，这类密码函数在密码算法中的使用，可以提高密码算法中运算的效率，降低制造成本，提高密码算法的安全性，同时又便于密码算法的安全性分析.一类密码函数的提出和研究往往是建立在某种密码安全性概念基础之上的，而某种密码安全性概念提出的目的又是为了防范某种形式的密码分析.如相关免疫函数的提出是基于相关免疫性概念，其目的是为了防范对序列密码的分别征服分析和线性分析等；Bent 函数概念的提出并不是基于密码学应用，但它更广泛和深入的研究正是因为其 Walsh 谱值的均匀分布特性切合了密码设计者防范线性分析和差分分析的需求.需要特别指出的是，具有单一密码学性质的密码函数在密码算法中的使用，并不能确保整个密码系统具有好的密码学特征，因而也就不能防范不同形式的密码分析.因此，研究具有各种不同密码学特征的基本密码函数以及它在密码算法中的综合应用，对于丰富密码学基础理论具有重要意义.

众所周知，置换是一类在密码算法中使用相当广泛的特殊的密码函数，其特殊性主要在于它的定义域中元素与值域中元素是一一对应的.置换在密码算法中广泛使用的原因主要在于密码算法本身要求具有可逆性，即密文需要在密钥的作用下恢复出明文.因此，从某种意义上看，密码算法本身就是在密钥控制下的置换.一般分组密码算法，其明密文的对应关系就是在密钥控制下的置换；一般序列密码算法，其明密文对应关系是在密钥以及时序逻辑控制下的置换；公钥密码算法的明密文对应关系是在一对密钥控制下的置换，其密码理论基础是陷门单向函数，密钥即为陷门信息.除密码算

法本身是置换外，密码算法中的许多组件也是置换.

然而，并不是所有的置换都可以作为密码函数，用于密码算法中的置换作为一类特殊的密码函数，必须具有良好的密码学性质.具有良好密码学性质的置换的研究是密码函数研究中的重要内容.

密码学对置换有着特殊的需求.由于密码学对所需置换使用的目的不同，对置换的性质需求也表现各异.密码学中所需的置换主要具有两种功能：扩散与混淆.扩散所需的置换主要是对密码函数输入地址的置换，混淆所需的置换主要是对密码函数输入内容的置换.

置换的混淆作用主要包括使密码函数输入输出的线性传播值和差分传播值必须足够小；输出分位必须几乎与所有输入分位相关；输入单分位符号的改变必须能够引起几乎一半的输出分位符号发生改变等.这就要求实现混淆作用的置换作为基本密码函数必须具有一定的非线性次数、足够多的项数、较强的免疫能力、平衡性等.

置换的扩散作用主要是使密码函数各输入分位信息均匀扩散到输出的每个分位之中.这就要求实现扩散作用的置换作为基本密码函数必须使各输入分位与各输出分位的互信息是均匀的.

由于完全映射具有良好的密码学特性，基于完全映射构造的基础置换具有良好的扩散或混淆作用，所以研究完全映射具有重要的理论与实践意义.

18 世纪，瑞士数学家 L. Euler 提出了拉丁方与正交拉丁方的概念，并提出了阶数 n 为 6，10，14，…，$4k+2$，…的正交拉丁方均不存在的猜想.1900 年，G. Tarry 证明了 $n=6$ 时 Euler 猜想是正确的.之后，拉丁方的研究引起了许多数学家的兴趣.20 世纪四五十年代，随着正交拉丁方在统计学和实验设计中应用需求的增加，数学界一度对正交拉丁方的研究引发过一阵新的热潮，并于 1959 年由 3 位数理统计学家 R. C. Bose，E. T. Parker 和 S. S. Shrikhancle 成功地证明了 $n>6$ 时 Euler 猜想不正确[1]，同时给出了 $4k+2$ 阶正交拉丁方的构造方法，从而彻底解决了 Euler 的猜想.“完全映射”[2]这一概念正是在此期间(1942 年)由 H. B. Mann 为研究正交拉丁方而首先引入的.由于完全映射与正交拉丁方的构造有着密切的联系，在当时关于完全映射已做过许多研究.本书将在引入一些相关概念的基础上，对完全映射的概念、存在性和性质等问题进行综述和讨论，同时给出基于完全映射所设计的分组密码的安全性分析.

为便于完全映射的讨论，我们在引论中先介绍关于密码学中置换的有关概念和性质.

1.2 布尔置换的表示

定义 1.2.1 2^n 个元素的有限集 G 到自身的双射 P 称为布尔置换.

布尔置换主要有如下表示法：

1. 真值表表示

P 是 2^n 个元素有限集 G 上的置换算子，令 $G = \{0, 1, 2, \cdots, 2^n - 1\}$，称

$$P = \begin{pmatrix} 0 & 1 & \cdots & 2^n - 1 \\ P(0) & P(1) & \cdots & P(2^n - 1) \end{pmatrix}$$

为布尔置换 P 的真值表表示.

2. 域上多项式表示

设 F_q 是有限域，φ 是 F_q 到 F_q 的任意函数，则必存在唯一的次数小于 q 的多项式 $g(x)$ 表示 φ，即对所有的 $c \in F_q$，$\varphi(c) = g(c)$. 这个多项式可由函数 φ 的 Lagrange 插值多项式计算，即

$$g(x) = \sum_{c \in F_q} \varphi(c)(1 - (x - c)^{q-1}).$$

若 $\varphi(x)$ 本身就是多项式，则

$$g(x) = \varphi(x) \bmod (x^q - x).$$

下面我们讨论有限域上的多项式函数生成置换的条件.

引理 1.2.2[3] 设 $g(x), f(x) \in F_q[x]$，那么对所有的 $c \in F_q$ 成立

$g(c) = f(c)$，当且仅当 $f(x) \equiv g(x) \bmod (x^q - x)$.

证明 设 $f(x) - g(x) = h(x)(x^q - x) + r(x)$，其中 $r(x), h(x) \in F_q[x]$，$r(x)$ 的次数小于 q. 因为对所有 $c \in F_q$ 成立 $g(c) = f(c)$ 当且仅当对所有 $c \in F_q$ 成立 $r(c) = 0$，即 $r(x) = 0$. 故该命题成立.

引理 1.2.3[3] 设 $a_0 = 0, a_1, \cdots, a_{q-1}$ 不为零是有限域 F_q 中的元素，则下列条件等价：

(1) $a_0, a_1, \cdots, a_{q-1}$ 互不相同；

(2) $\sum_{i=0}^{q-1} a_i{}^t = \begin{cases} 0 & (t = 0, 1, \cdots, q-2) \\ -1 & (t = q-1) \end{cases}$.

证明 给定 $1 \leqslant i \leqslant q-1$，考虑多项式 $g_i(x) = 1 - \sum_{j=0}^{q-1} a_i{}^{q-1-j} x^j$. 对 $b \in F_q, b \neq a_i$，有

$$g_i(a_i) = 1 - \sum_{j=0}^{q-1} a_i{}^{q-1-j} a_i{}^j = 1 - \sum_{j=0}^{q-1} a_i{}^{q-1}$$

$$= 1 - q a_i{}^{q-1} = 1.$$

令 $\lambda_i = \dfrac{b}{a_i}$，则

$$g_i(b) = 1 - \sum_{j=0}^{q-1} a_i{}^{q-1-j} b^j = 1 - \sum_{j=0}^{q-1} a_i{}^{q-1} a_i{}^{-j} b^j$$

$$= 1 - a_i{}^{q-1} \sum_{j=0}^{q-1} \lambda_i{}^j = 1 - \frac{1 - \lambda_i{}^q}{1 - \lambda_i} a_i{}^{q-1}$$

$$= 0.$$

令 $g_0(x) = 1 - \sum_{j=0}^{q-1} a_0{}^{q-1-j} x^j$，因而多项式 $g(x) = \sum_{i=0}^{q-1} g_i(x) = -\sum_{i=0}^{q-1} \sum_{j=0}^{q-1} a_i{}^{q-1-j} x^j$ 将 F_q 中的每个元素映射为 1 当且仅当 $F_q = \{a_0, a_1, \cdots, a_{q-1}\}$. 因为 $\deg(g) < q$，由引理 1.2.2 知 $g(x)$ 将 F_q 中的每个元素映射为 1 当且仅当 $g(x) = 1$，即

$$g(x) = -\sum_{i=0}^{q-1} \sum_{j=0}^{q-1} a_i{}^{q-1-j} x^j = -\sum_{j=0}^{q-1} \sum_{i=0}^{q-1} a_i{}^{q-1-j} x^j = 1,$$

故条件(2)成立.

定理 1.2.4[3] (Hermite 判据) 设 F_q 是特征为 p 的域，则 $f(x) \in$