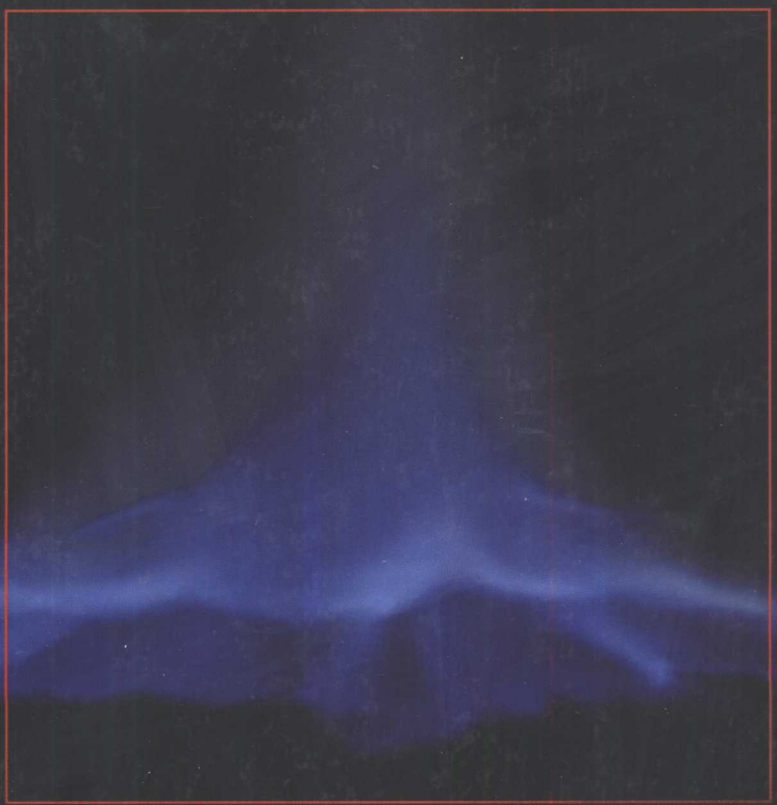
频谱理论及其在密码学中的应用

冯登国 著



科学出版社

内 容 简 介

本书系统而全面地介绍了频谱理论及其在密码学中的应用，内容主要包括：(1) 利用频谱技术对布尔函数的各种非线性准则之间的关系及其特征进行了深入的刻画，并在此基础上构造了一批满足某些密码学特性的布尔函数；讨论了非线性组合函数的最大相关分析问题，给出了一个非常有效的逼近算法。(2)介绍了广义一阶 Walsh 谱的概念，利用这种谱对多输出函数的密码学特性进行了深入的刻画；构造了一批具有差分均匀性较小、非线性次数较高的多输出函数；揭示了 S-盒的差分攻击和线性攻击之间的关系；给出了多输出函数的一种相关攻击方法。(3)利用频谱技术对多值逻辑函数(环上和域上)的密码学特性进行了系统而深入的刻画，给出了多值逻辑函数的相关免疫性、非线性性、退化性的特征；介绍了构造具有某些密码特性的多值逻辑函数的一些方法；给出了计算多值逻辑函数的谱值的快速计算方法。

本书可作为信息安全专业和应用数学专业的硕士生、博士生和本科高年级学生选修课教科书，也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

频谱理论及其在密码学中的应用/冯登国著，-北京：科学出版社，2000
ISBN 7-03-008659-7

Ⅰ. 频… Ⅱ. 冯… Ⅲ. 频谱-理论-应用-密码-理论 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字(2000)第 65342 号

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
源海印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2000 年 10 月第 一 版 开本：850×1168 1/32
2000 年 10 月第一次印刷 印张：6 5/8
印数：1—1 500 字数：171 000

定价：16.00 元

(如有印装质量问题，我社负责调换〈杨中〉)

前　言

虽然密码学的研究历史可追溯到几千年前，但是直到1949年Shannon发表了论文“保密通信的信息理论”[1]一文以后，它才真正成为一门科学。20世纪70年代中期，在密码学的研究中出现了两件引人注目的事件。一件是Diffie和Hellman发表了“密码学的新方向”[2]一文，提出了一种崭新的密码体制——双钥(公钥)密码体制，冲破了长期以来一直沿用的单钥(私钥)密码体制。新的双钥(公钥)密码体制可使发信者和收信者之间无须事先交换密钥就可建立起保密通信。该论文指明了Shannon在1949年所提出的将密码建立在解某个已知数学难题之上的具体实现途径。另一件是美国国家标准局(NBS)公开征集，并于1977年正式公布实施的美国数据加密标准(DES)[3]。公开DES加密算法，并广泛用于商用数据加密，这揭开了密码学的神秘面纱，大大地激发了人们对于密码学的研究兴趣。以上这两个事件标志着现代密码学的诞生。20多年来，现代密码学无论在理论上还是在应用上都得到了巨大发展。信息的安全与保密不仅与国家的政治、军事和外交等有关，而且与各个团体、单位和个人(如个人存款、医疗记录、财产数据等)密切相关，因此在今天的信息社会中，信息系统的安全与保密是至关重要的，从而给密码学的研究以巨大的推动力，为密码学的应用提供了广阔的前景。密码学主要由密码编码学和密码分析学两个分支组成。密码编码学的主要任务是寻求生成高强度密码的有效算法，满足对消息进行加密或认证的要求。密码分析学的主要任务是破译密码或伪造认证码，实现窃取机密信息或进行诈骗破坏活动。这两个分支既相互对立，又相互依存。正是由于这种对立促进了密码学的飞速发展。

自从密码技术诞生以来，密码系统的安全强度问题一直是引

人注目的，对这个问题的研究已有不少成果。密码按加密方式可分为分组密码和流密码。分组密码的典型代表是 DES 体制，DES 体制的安全强度主要取决于 S-盒的安全性能，比如 S-盒的非线性性、扩散特性、雪崩效应、平衡性、差分特性等性质。而 S-盒可用一组逻辑函数来实现，因此 DES 体制的安全强度的研究最终归于一组逻辑函数的非线性性、扩散特性、雪崩效应、平衡性、差分特性等性质的研究。不仅如此，美国最近公布的 15 个候选算法也可通过这种办法来研究。流密码现已有不少体制，最常用的是组合流密码系统和滤波流密码系统；这些系统的安全强度与所选用的组合和滤波函数的性能有着密切关系，因此研究这些系统的安全强度问题可归于组合或滤波函数的性能的研究，比如函数的相关免疫性、扩散特性、非线性性、雪崩效应、稳定性、差分特性等性能的研究。由此可见，研究逻辑函数和逻辑函数组的非线性性、相关免疫性、扩散特性、雪崩效应、平衡性、稳定性、差分特性等性质对密码的分析与设计有着重要的指导作用。研究密码函数的传统方法是在“时域”上直接对函数进行约化，用以分析与设计密码体制。直到 20 世纪 80 年代中期，肖国镇教授和 Massey 教授首次将频谱技术应用于密码学的研究[4]，并给出了布尔函数的相关免疫性的特征化定理，才为频谱技术在密码学中的应用开辟了一条广阔的道路。

作者从 1990 年起从事信息安全理论与技术方面的研究，受到了国内外一大批同行专家的精心指导和坦诚相助，作者的每一点成绩都与这些同行专家的辛勤培养分不开。在这里特别要感谢的有：西安电子科技大学的肖国镇教授、王育民教授和王新梅教授，是他们把作者带进了信息安全这个神圣的殿堂，在他们的指导下，作者所完成的博士论文“频谱理论及其在通信保密技术中的应用”被评为首届全国优秀博士学位论文；中国科技大学研究生院信息安全国家重点实验室的曾肯成教授、冯克勤教授、裴定一教授、戴宗铎教授、赵战生教授、吕述望教授和戴英侠教授，是他们使作者更加深化和拓宽了对信息安全的理解和认识，在他们的指导、参与和协助下，完成并出版了《密码学导引》和《信息安全技术浅谈》两

部著作，受到广大读者的一致好评；中国科学院信息安全技术工程研究中心的卿斯汉研究员，是他使作者了解了信息安全的具体应用环境并为作者提供了一个很好的学术环境，在他的指导和协助下作者参与了中心的大部分工作，很好地完成了中国科学院“九五”重大应用研究与开发项目，该项目产生了一定的经济效益，并获得了中国科学院科技进步一等奖。

本书收集了作者近10年来在频谱理论及其在密码学中的应用方面所做的一系列工作，以此献给辛勤培养过作者的专家们。

目　录

第1章 绪 论

本章简要介绍现代密码学的基本内容，概述频谱理论在密码学中的应用现状和本书的主要内容。

1.1 密码学简介

密码学是一门古老而又年青的科学，它用于保护军事和外交通信可追溯到几千年前。在今天的信息时代，大量的敏感信息如病历、法庭记录、资金转移、私人财产等常常通过公共通信设施或计算机网络来进行交换，而这些信息的秘密性和真实性是人们迫切需要的。因此，现代密码学的应用已不再局限于军事、政治和外交，其商用价值和社会价值已得到了广泛的重视。

密码学是研究密码系统的一门科学，它主要包括两个分支，即密码编码学和密码分析学。密码编码学的主要目标是寻求保证信息的机密性和可认证性的方法，密码分析学的主要目标是研究加密信息的破译和信息的伪造。这两个分支既对立，又统一；正是由于其对立的一面才促进了密码学的飞速发展。

采用密码技术可以隐蔽和保护需要保密的消息，使未授权者不能提取信息。被隐蔽的消息称作明文，隐蔽后的消息称作密文。将明文变换成密文的过程称作加密，其逆过程，即由密文恢复出原明文的过程称作解密。对明文进行加密时所采用的一组规则称作加密算法，对密文进行解密时所采用的一组规则称作解密算法。加密和解密算法的操作通常都是在一组密钥控制下进行的，分别称为加密密钥和解密密钥。

根据密钥的特点，将密码体制分为对称和非对称密码体制两种。对称密码体制又称单钥或私钥或传统密码体制，非对称密码体

制又称双钥或公钥密码体制。我们采用私钥和公钥密码体制这两个术语。在私钥密码体制中，加密密钥和解密密钥是一样的或彼此之间容易相互确定。按加密方式又可将私钥密码体制分为流密码和分组密码两种。在流密码中，将明文消息按字符逐位地加密。在分组密码中，将明文消息分组(每组含有多个字符)，逐组地进行加密。在公钥密码体制中，加密密钥和解密密钥不同，从一个难于推出另一个，可将加密和解密能力分开。现有的大多数公钥密码属于分组密码。

在信息传输和处理系统中，除了意定的接收者外，还有非授权者，他们通过各种办法如搭线窃听、电磁窃听、声音窃听等来窃取机密信息，称其为截收者。他们虽然不知道系统所用的密钥，但通过分析可能从截获的密文推断出原来的明文，这一过程称作密码分析。对一个密码系统采取截获密文进行分析的这类攻击称作被动攻击。密码系统还可能遭受的另一类攻击是主动攻击，非法入侵者主动向系统窜扰，采用删除、更改、增填、重放、伪造等手段向系统注入假消息。所谓一个密码是可破的，是指如果密码分析者无需花过高的代价诸如时间、空间和金钱就能通过密文能够确定明文或密钥，或通过明文-密文对能够确定密钥。破译密码的一种最朴素的方法是穷搜索方法，其基本观点是：给定一个明文-密文对(m,c)，试验所有可能的密钥K，直到$c=E_K(m)$为止。如果密钥的长度为b比特，那么为了找到正确的密钥K平均需要试验2^{b-1}次。这表明为了抵抗穷搜索攻击，密钥必须足够的长，但必须注意具有足够长密钥的密码未必安全。

密码分析中有一个基本的假设称为 Kerckhoff 假设；该假设假定密码分析者拥有所使用的算法的全部知识，密码系统的安全性完全寓于密钥之中，也就是说，密码分析者除了不知道所使用的密钥之外，他了解整个密码系统。

密码技术主要有三大技术即加密技术、认证技术和密钥管理技术，本节主要简要介绍这三种技术。对密码学感兴趣的读者请参阅文献[5]。

1.1.1 加密技术

信息的保密性是信息的安全性的一个重要方面。保密的目的是防止敌手破译信息系统中的机密信息。加密是实现信息的保密性的一种重要手段。加密技术可使一些重要数据存储在一台不安全的计算机上，或可以在一个不安全的信道上传送。只有持有合法密钥的一方才能获得“明文”。这里主要介绍目前国际上比较流行的几种加密技术。

1. 分组密码

一个分组密码有两个重要的参数：一个是密钥的大小，称作密钥长度；另一个是每次操作的组的大小，称作分组长度。在密钥 K 控制之下的加密算法 E 记为 E_K，明文消息 m 对应的密文记为 $E_K(m)$。类似地，在密钥 K 控制之下的解密算法 D 记为 D_K，密文消息 c 对应的明文记为 $D_K(c)$。显然，对所有的明文 m，都有 $D_k(E_K(m))=m$。

自从 1977 年美国公布其数据加密标准(DES)以来，人们提出了大量的分组密码，例如 IDEA、SAFER K-64、SAFER K-128、RC5、Skipjack、RC2、FEAL-N、REDOC-Ⅱ、LOKI、CAST、Khufu、Khafre、MMB、3-WAY、TEA、MacGuffin、SHARK、BEAR、LION、CA.1.1、CRAB、Blowfish、GOST、SQUARE、MISTY，以及美国 NIST 最近公布的十五个 AES 候选算法等。

迭代密码是最常用的一种分组密码，现有的分组密码大部分都是迭代密码，它以迭代一个简单的轮函数为基础，也就是通过选择某个较简单的密码变换，在密钥控制下以迭代方式多次利用它进行加密变换。例如，Feistel 型密码就是一种迭代密码，它发明于 1974 年，人们已利用这种结构设计了许多密码。现在我们来描述 Feistel 型密码的加、解密过程。

设 m 是一个长为 $n=2t$ 比特的明文组，记 $m=m_0m_1$，$m_i(i=0,1)$的长度为 t 比特。给定一个密钥 k，用它生成 r 个子密钥 $k_1,k_2,$

…，k_r，每一轮使用一个，共 r 轮。加密过程为

$$\text{for } i = 2 \text{ to } r+1 \text{ do}$$

$$m_i = m_{i-2} \oplus f(m_{i-1}, k_{i-1});$$

密文为 $m_{r+1}m_r$。其中 $f(\cdot,\cdot)$是轮函数。

解密过程与加密过程类似，其解密过程为：

$$\text{for } i = r \text{ to } 1 \text{ do}$$

$$m_{i-1} = m_{i+1} \oplus f(m_i, k_i);$$

最后获得明文 m_0m_1。

可见，在 Feistel 型密码的设计中，关键是轮函数 f 的设计。DES 就是一种 Feistel 型密码。在 DES 中，密钥长度为 56 比特，分组长度为 $n=64$ 比特，$t=32$。它的加密工作程序如下：

(1) 给定一个明文 $\boldsymbol{x}$，通过一个固定的初始转换 IP 置换 $\boldsymbol{x}$ 的比特获得 $\boldsymbol{x}_0$，记 $\boldsymbol{x}_0=\mathbf{IP}(\boldsymbol{x})=\boldsymbol{L}_0\boldsymbol{R}_0$，这里 $\boldsymbol{L}_0$ 是 $\boldsymbol{x}_0$ 的前 32 比特，$\boldsymbol{R}_0$ 是 $\boldsymbol{x}_0$ 的后 32 比特。

(2) 然后进行 16 轮完全相同的运算，在这里数据与密钥结合。我们根据下列规则计算 L_iR_i，$1\leqslant i\leqslant 16$：

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

这里⊕表示两个比特串的异或，f 是一个函数(f 将在下面描述)，$k_1, k_2, \cdots, k_{16}$都是密钥 k 的函数，长度均为 48 比特(实际上，每一个 k_i 是来自密钥 k 的比特的一个置换选择)，$k_1, k_2, \cdots, k_{16}$构成了密钥方案。

(3) 对比特串 $R_{16}L_{16}$应用初始置换 IP 的逆置换 IP^{-1}，获得密文 y，即 $y=\mathrm{IP}^{-1}(R_{16}L_{16})$。注意最后一次迭代后，左边和右边未交换，而将 $R_{16}L_{16}$作为 IP^{-1}的输入，目的是为了使算法可同时用于加密和解密。

函数 $f(A,J)$的第一个变量 A 是一个长度为 32 的比特串，第二个变量 J 是一个长度为 48 的比特串，输出是一个长度为 32 的比特串。f 的计算过程如下：

(1) 将 f 的第一个变量 A 根据一个固定的扩展函数 E 扩展

成一个长度为 48 的比特串。

(2) 计算 $E(A)\oplus J$，并将所得结果分成 8 个长度为 6 的比特串，记为 $B=B_1B_2B_3B_4B_5B_6B_7B_8$。

(3) 使用 8 个 S-盒 $S_1,S_2,\cdots,S_8$。每一个 S_i 是一个固定的 4×16 阶矩阵，它的元素来自 0 到 15 这 16 个整数。给定一个长度为 6 的比特串，比方说 $B_j=b_1b_2b_3b_4b_5b_6$，我们按下列办法计算 $S_j(B_j)$：用两个比特 b_1b_6 对应的整数 $r(0\leqslant r\leqslant 3)$来确定 S_j 的行(所谓两个比特 b_1b_6 对应的整数 r 意指 r 的二进制表示为 b_1b_6，以下的含义类同)，用四个比特 $b_2b_3b_4b_5$ 对应的整数 $c(0\leqslant c\leqslant 15)$来确定 S_j 的列，$S_j(B_j)$的取值就是 S_j 的第 r 行第 c 列的整数所对应的二进制表示。记 $C_j=S_j(B_j)$，$1\leqslant j\leqslant 8$。

将长度为 32 的比特串 $C=C_1C_2C_3C_4C_5C_6C_7C_8$ 通过一个固定的置换 P 置换，将所得结果 P(C)记为 $f(A,J)$。

下面我们来描述 DES 算法中所使用的具体函数和密钥方案的计算。

初始置换 IP 和其逆置换 IP^{-1}为

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

这意味着 x 的第 58 比特是 IP(x)的第 1 比特，x 的第 50 比特是 IP(x)的第 2 比特等等。初始置换 IP 及其逆置换 IP^{-1}没有密码意义，因为 x 与 IP(x)(或 y 与 $IP^{-1}(y)$)的一一对应关系是已知的。它们的作用在于打乱原来输入 x 的 ASCII 码字划分的关系，并将原来明文的检验位 $x_8, x_{16}, \cdots, x_{64}$变成 IP 的输出的一个字节。

扩展函数 E 为

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

置换 P 为

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

密钥方案的计算：每一轮都使用不同的、从初始密钥(又称种子密钥)k 导出的 48-比特密钥 k_i。k 是一个长度为 64 的比特串，实际上它只有 56-比特密钥，在第 8,16,…,64 位为校验比特，共 8 个，这主要是为了检错。在位置 8,16,…,64 的比特是按下述办法给出的：使得每一个字节(8 比特长)含有奇数个 1。因此在每一个字节中的一个错误能被检测出。在密钥方案的计算中，不考虑校验比特。密钥方案的计算过程如下：

(1) 给定一个 64-比特的密钥 k，删掉 8 个校验比特并利用一个固定的置换 PC-1 置换 k 的剩下的 56 比特，记 PC-1(k)$=C_0D_0$，这里 C_0 是 PC-1(k)的前 28 比特，D_0 是 PC-1(k)的后 28 比特。

(2) 对每一个 i，$1\leqslant i\leqslant 16$，计算$C_i=\mathrm{LS}_i(C_{i-1})$

$$D_i=\mathrm{LS}_i(D_{i-1})$$

$$k_i=\mathrm{PC\text{-}2}(C_iD_i)$$

其中 LS_i 表示一个或两个位置的左循环移位，当 $i=1,2,9,16$ 时，移一个位置，当 $i=3,4,5,6,7,8,10,11,12,13,14,15$ 时，移两个位置。PC-2 是另一个固定置换。

置换 PC-1 和置换 PC-2：

PC-1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC-2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	30	36	29	32

解密采用同一算法实现，把密文 y 作为输入，倒过来使用密钥方案即以逆序 $k_{16},k_{15},\cdots,k_1$ 使用密钥方案，输出将是明文 x。

8 个 S-盒为

	列																
行	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S_1
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	

0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	S_2
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	S_3
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	S_4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	S_5
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	S_6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	S_7
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	S_8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

2. 流密码

可将流密码分为两类，即同步流密码和自同步流密码。密钥流独立于明密文的流密码称作同步流密码。反之，密钥流与已产生的一定数量的密文有关的流密码称作自同步流密码。

同步流密码的加密过程可描述为

$$\sigma_{i+1}=f(\sigma_i,k)$$
$$z_i=g(\sigma_i,k)$$
$$c_i=h(z_i,m_i)$$

这里 σ_0 是初始状态，可以由密钥 k 确定，f 是状态转移函数，g 是产生密钥流 z_i 的函数，h 是组合密钥流和明文 m_i 产生密文 c_i 的函数。

在同步流密码中，只要发送端和接收端有相同的种子或实际密钥 k 和内部状态，就能产生出相同的密钥流。此时，我们说发送端和接收端的密钥生成器是同步的。

同步流密码的一个优点是无错误传播，一个传输错误只影响一个符号。不会影响后继符号，但这也是一个缺点，因为对手窜改一个符号比窜改一组符号容易。附加非线性检错码可克服这个缺陷。

目前已有的同步流密码，大多数是二元加法流密码；所谓二元加法流密码意指密钥流、明文和密文数字都是 0、1 数字，并且输出函数 h 是异或函数的流密码。

自同步流密码的加密过程可描述为

$$\sigma_i=(c_{i-t},c_{i-t+1},\cdots,c_{i-1})$$
$$z_i=g(\sigma_i,k)$$
$$c_i=h(z_i,m_i)$$

这里 $\sigma_0=(c_{-t},c_{-t+1},\cdots,c_{-1})$ 是非秘密的初始状态，k 是密钥，g 是产生密钥流 z_i 的函数，h 是组合密钥流和明文 m_i 产生密文 c_i 的输出函数。

从公开发表的文献来看，目前的绝大多数有关流密码的研究