随机置换表中闭合状态演化环的特征及其在分组加密中的应用

张申如① 郭 明②
①(解放军理工大学理学院 南京 211101)
②(解放军理工大学第63研究所 南京 210007)

摘 要 从Skipjack分组密码的F表出发，对随机置换表中闭合状态演化环的环数出现概率和期望值、闭合状态演化环的平均环长度等进行了研究，得到其封闭的计算式。为快速计算，分别寻找到它们的递推关系式。数值模拟的实验证实了理论结果的正确性。

关键词 Skipjack分组密码，随机置换表，状态演化环
中图分类号：TN918.3 **文献标识码**：A **文章编号**：1009-5896(2006)10-1870-04

The Properties of Closed State Evolutive Ring in Random Permutation-Table and Its Application to Block Encryption

Zhang Shen-ru① Guo Ming②
①(*Institute of Sciences*, *PLA University of Sci. and Tech.*, *Nanjing* 211101, *China*)
②(*The 63rd Research Institute*, *PLA University of Sci. and Tech.*, *Nanjing* 210007, *China*)

Abstract In this paper the concept of random permutation table is presented from F table in Skipjack block encryption. The probabilities and the expected values of closed state evolutive ring numbers and the average length of state evolutive rings are studied and their closed forms used in computation are given. For quick computation their recurrence forms are obtained. The theoretical results are proved experimentally by numerical simulation.

Key words Skipjack block encryption, Random permutation table, State evolutive ring

1 引言

分组加密方案中通常都有一个或多个非线性映射表。在DES中有8个S盒；在AES中有GF(2^8)上定义的字节代替变换所组成的一个共用“S盒”。分组加密总可以看作是多轮、多次查询非线性映射表的迭代过程。美国托管加密标准，又称Clippper建议中也采用了一个称为Skipjack的私钥分组密码[1,2]。该密码方案中使用了一个16×16非线性的F表，作为特定的代换网络。跟踪F表可以发现，256个8位输入和输出的F表，是由5个一对一映射组成的闭合状态演化环构成，它们分别是：

(1)00→A3→2C→E9→36→9A→DC→8B→D4→75→…→8E→67→69→00，环长为131；

(2)01→D7→A1→88→27→68→45→93→1F→28…→51→B9→FB→01，环长68；

(3)04→F8→BD→3E→6A→94→8D→C7→F0→5E→…→1E→44→C1→04，环长为45；

(4)25→F1→6C→6D→98→C8→29→B7→3B→F5→25，环长为10;

(5)9F→A4→9F，环长为2。

5个演化环按状态数加权的平均环长度，经计算为93.414。由此可以提出的一个数学问题是：这些数字特征与一个随机形成的16×16一对一置换表的一般性质相符吗？为此本文要研究一个随机形成的、长度为 N 的、由一对一映射组成的置换表。它们从一个输入起，将输出再次作为输入… 如此继续，所形成的闭合状态演化环有哪些期望的数字特征？

2005-01-20收到，2006-03-13改回

2 随机置换表的形成及其闭合状态演化环的特征

本文所指的随机置换表是一个长度为N (例如，N=256)的、状态一对一的映射表，它可用下述方法描述并由实验得到[3]：

(1)用 $T(\cdot)$代表映射，首先选 $T(i)=i\in(0,1,\cdots,N-1)$，构成一个对自身映射的置换表；

(2)产生一对(0,1,…,N–1)的随机整数 j，k，交换F表中 $T(j),T(k)$ 的值；

(3)重复步骤(2)足够次数，就可以得到一个随机的、由一对一映射组成的置换表，可表示为 $T(i)$, $(i,T(i)\in(0,1,\cdots,N-1),\ T(i)\neq T(j)\,|\,i\neq j)$。

性质 1(随机置换表的总数) 各不相同的随机置换表的总数为 N 个元素的全排列数 $A_N=N!$。从上述的产生方法知，此性质是显然的，证明从略。

性质 2(指定环数和环长下的状态演化环的概率) 随机置换表中出现 $k\,|\,k\in(1,2,\cdots,N)$ 个，长度分别为 $i_1,i_2,\cdots,i_k\ |\ i_1,i_2,\cdots,i_k\in(1,2,\cdots,N),\ i_1+i_2+\cdots+i_k=N$ 有序排列的、闭合的状态演化环的概率为 $p(k,i_1,i_2,\cdots,i_k)=1/(i_1i_2\cdots i_k k!),\ i_1+i_2+\cdots+i_k=N$。

证明　用构成 k 个长度分别为 $i_1,i_2,\cdots,i_k$ 闭合状态演化环的方法来加以证明。

(1) 从 N 个元素中选取 i_1 个元素，其排列数为 $A_N^{i_1}=N\times(N-1)\times\cdots\times(N-i_1+1)$，对 $a_1,a_2,\cdots,a_{i1}$ 建立循环的一对一映射，即 $T(a_i)=a_{i+1},(i=1,2,\cdots,i_1-1),T(a_{i_1})=a_1$，去除 i_1 个循环等价的闭合状态演化环，闭合状态演化环的总数为 $N\times(N-1)\times\cdots\times(N-i_1+1)/i_1$ (数学上也称称环状排列)；

(2)从余下 $N-i_1$ 元素中选取 i_2 个，其排列数为 $A_{N-i_1}^{i_2}=(N-i_1)\times(N-i_1-1)\times\cdots\times(N-i_1-i_2+1))$，对 $a_{i_1+1},a_{i_1+2},\cdots,a_{i_1+i_{12}}$ 建立循环的一对一映射，即 $T(a_i)=a_{i+1},(i=i_1+1,i_1+2,\cdots,i_1+i_2-1),T(a_{i_1+i_2})=a_{i_1+1}$，去除 i_2 个循环等价的闭合状态演化环，闭合状态演化环的总数为 $(N-i_1)\times(N-i_1-1)\times\cdots\times(N-i_1-i_2+1)/i_2$；

(3)按(2)的规则，如此继续… (数学上可看作多组环状排列)；

(4)第 k 次由于 $i_1+i_2+\cdots+i_k=N$，从余下 $N-i_1-i_2-\cdots-i_{k-1}=i_k$ 元素中选取最后剩下的 i_k 个，其排列数为 $A_{i_k}=i_k!$，对 $a_{N-i_k+1},a_{N-i_k+2},\cdots,a_N$ 建立循环的一对一映射，即 $T(a_i)=a_{i+1},(i=N-i_k+1,N-i_k+2,\cdots,N-1),T(a_N)=a_{N-i_k+1}$，去除 i_k 个循环等价的闭合状态演化环，闭合状态演化环的总数为 $i_k!/i_k$。

所以，随机置换表中出现 $k\,|\,k\in(1,2,\cdots,N)$ 个长度分别为 $i_1,i_2,\cdots,i_k\,|\,i_1,i_2,\cdots,i_k\in(1,2,\cdots,N),i_1+i_2+\cdots+i_k=N$ 有序排列的、闭合状态演化环的概率应为上述各步骤得到的闭合状态演化环总数的相乘，除以性质 1 给出的随机置换表的总数，此外还要除以不同次序、然而是等价的 $i_1,i_2,\cdots,i_k$ 排列选择数 $k!$，即

$$\begin{aligned}&p(k,i_1,i_2,\cdots,i_k)\\&=\frac{N\times(N-1)\times\cdots(N-i_1+1)(N-i_1)\cdots(N-i_1-i_2+1)\cdots i_k!}{N!\times i_1i_2\cdots i_k\times k!}\\&=\frac{1}{i_1i_2\cdots i_kk!}\end{aligned}$$

证毕

由此进一步不难得到下面的两条性质，由于篇幅关系，性质的证明从略。

性质 3(指定环数时，状态演化环出现的概率)　随机置换表中出现 $k\,|\,k\in(1,2,\cdots,N)$ 个闭合状态演化环的概率为

$$p(k)=\frac{1}{k!}\sum_{i_1=1}^{N-(k-1)}\sum_{i_2=1}^{N-(k-2)-i_1}\cdots\sum_{i_{k-1}=1}^{N-1-i_1-i_2-\cdots-i_{k-2}}\frac{1}{i_1i_2\cdots i_k},\quad i_1+i_2+\cdots+i_k=N$$

根据性质 3，显然长度为 N 的随机 F 表中平均环数为 $\sum_{k=1}^{N}kp(k)$。

性质 4(状态演化环的平均环长)　随机置换表中闭合状态演化环环以状态数为权的平均环长度为

$$L=\frac{1}{N}\sum_{k=1}^{N}\frac{1}{k!}\sum_{\substack{i_1=1\\k>1}}^{N-(k-1)}\sum_{\substack{i_2=1\\k>2}}^{N-(k-2)-i_1}\cdots\sum_{\substack{i_{N-1}=1\\k>N-1}}^{N-1-i_1-i_2-\cdots-i_{N-2}}\frac{i_1^2+i_2^2+\cdots+i_k^2}{i_1i_2\cdots i_k},\quad i_1+i_2+\cdots+i_k=N$$

式中 $\sum_{\substack{i_j=1\\k>j}}^{N-(k-j)-i_1-\cdots-i_{j-1}}\ (j=1,2,\cdots,N-1)$ 表示此求和号仅当 $k>j$ 时才出现。

3　典型的随机置换表的实验测试

上述演化环环数的概率给出的计算中，有两个值是预先可确定的，$p(1)=1/N,p(N)=1/N!$，要确定其它的 $p(k)$ 值，计算的复杂度是 $\propto N^k$，随 k 呈指数增大，当 N，k 较大时，实际上已无法完成。但是用计算机模拟实验的方法测试随机所形成的置换表，统计状态演化的特征量却是较容易的。所以，我们将首先用一个长度为 10、较短的随机置换表来验证上述结论的正确性，再用实验来验证或部分验证较长的随机置换表的特征。

用 Visual FORTRAN V5.1 的随机函数 RANDOM( )，按上节叙述的方法产生长度为 10 的随机置换表 10,000 个，测试闭合状态演化环的结果如表 1 所示。表 1 中列出了 10,000 次实测中各种环数出现的次数，并与性质 3 计算的理论概率值作了对比。置换表平均环数的实测值与依据性质 4 计算值的对比结果和概率的归一结果也列在表 1 中最后一列。可见理论与实验吻合得很好。

表 1　长度为 10 的随机置换表，闭合状态演化环数分布统计(测量次数=10,000)

Tab.1 Ring number statistical distributing of state evolutive ring in random permutation table with length 10 (metrical times=10,000)

环数	1	2	3	4	5	实测平均环数
实测平均次数	1007	2827	3244	1990	728	$2.924\sum_{k-1}^{10}p(k)=1$
性质 3 概率值(%)	10.00	28.29	32.32	19.94	7.422	
环数	6	7	8	9	10	性质 4 平均环数
实测平均次数	184	18	2	0	0	2.929
性质 3 概率值(%)	1.744	0.26	0.024	1.24×10^{-3}	2.76×10^{-5}	

用 Visual FORTRAN V5.1 的随机函数 RANDOM( )产生类似于 Skipjack 分组加密中的长度为 N=256 的随机置换表 10,000 个，实验测量了闭合状态演化环各环数出现的概率，其结果用“o”示于图 1 中。实验测到的平均环数约为 6.16，与实验点连成的曲线的峰值大体对应，略大于 Skipjack 的 F 表的环数。实验测得的平均环长度约为 128.12，逼近 F 表总长度的一半，比 Skipjack 的 F 表的平均环长度大。图 1 中还示出了按性质 3 计算得到的前 6 个理论上的概率值，用“+”示出。可见理论上的概率与实验概率也吻合得很好。一个明显存在的困难是：当 N 较大、环数 k 也较大时，理论概率值按性质 3 来计算，由于多重循环求和而耗时太大。如何才能简化计算的问题就出现了。

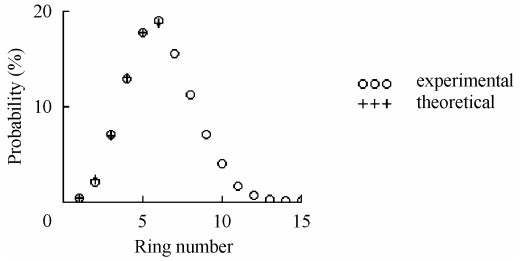

图 1 长度为 256 随机 F 表状态演化环各环数出现的概率（实验和理论）

Fig.2 Ring number probability of state evolutive ring in random F table with length 256 (experimental and theoretical)

4 演化环的概率和平均环长的递推计算

这一节我们要得到随机置换表闭合的状态演化环的环数出现概率和平均环长的递推计算公式。由性质 1，一个长度为 N 的随机置换表的总数为 $N!$，设环数为 k 的出现数为 R_N^k，那么环数为 $k \mid k \in (1,2,\cdots,N)$ 的闭合状态演化环的概率为 $p_N(k) = R_N^k / N!$。

定理 1 在长度为 N+1 的随机置换表中，环数为 k 的出现数 R_{N+1}^k 满足如下的递推关系：$R_{N+1}^k = NR_N^k + R_N^{k-1}$ $N \ge k \ge 1, N, k \in Z$。

证明 分析长度为 N+1 的随机置换表中环数为 k 的出现，可以分为下述两种情况：(1)在长度为 N 的、环数为 k 的所有 R_N^k 的随机置换表中，在各环任何两相邻元素间插入第 N+1 个元素，这样组成的长度为 N+1、环数为 k 的随机置换表有 NR_N^k 个。(2)在长度为 N 的、环数为 k–1 的所有 R_N^{k-1} 的随机置换表中，由第 N+1 个元素单独组成第 k 个环，这样组成的长度为 N+1 的、环数为 k 的随机置换表中随机置换表有 R_N^{k-1} 个。将(1),(2)两部分加起来就得到本定理的结果。 证毕

依据本定理，再利用 $p_1(1) = 1$，并补充定义 $p_N(0) = 0$，$p_N(N+1) = 0$ 就很容易得到一个长度为 N 的随机置换表环数为 k 出现概率 $p_N(k)$，如表 2，其中前 10 行为 $p_N(k)$, $1 \le k \le N = 1, 2, \cdots, 10$，即 N 不大于 10 的随机置换表的计算值，第 11 行为 $p_{256}(k), 1 \le k \le 10$，即 N 为长 256 的随机置换表的环数不大于 10 的计算值，最后一行为 10,000 次实验所得到 N 为长 256 的随机置换表的环数不大于 10 的测试值，可见计算结果与上一节计算和实验测定结果完全一致。表 2 中黑体数字代表概率最大的环数位置，括号内 e 后为 10 的幂次。

利用本定理，应用数学归纳法，容易证明下述推论叙述的归一特性，证明过程从略。

表 2 长度为 N 的随机置换表环数为 k 出现的概率 $p_N(k)$

Tab.2 Ring number k probability $p_N(k)$ of state evolutive ring in random permutation table with length N

$P_N(k)$	k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9	k=10
N=1	1.00									
N=2	0.500	0.500								
N=3	0.333	**0. 500**	0.167							
N=4	0.250	**0. 458**	0.250	4.17(e-2)						
N=5	0.200	**0. 417**	0.292	8.33(e-2)	8.33(e-3)					
N=6	0.167	**0. 381**	0.313	0.118	2.08(e-2)	1.39(e-3)				
N=7	0.143	**0. 350**	0.322	0.146	3.47(e-2)	4.17(e-3)	1.98(e-4)			
N=8	0.1.25	0.324	**0. 326**	0.168	4.86(e-2)	7.99(e-3)	6.94(e-4)	2.48(e-5)		
N=9	0.111	0.302	**0. 326**	0.185	6.19(e-2)	1.25(e-2)	1.50(e-3)	9.92(e-5)	2.76(e-6)	
N=10	0.100	0.282	**0. 323**	0.199	7.42(e-2)	1.74(e-2)	2.60(e-3)	2.40(e-4)	1.24(e-5)	2.76(e-7)
N=256	3.91(e-3)	2.39(e-2)	7.00(e-2)	0.131	0.178	**0. 188**	0.160	0.113	6.87(e-2)	3.61(e-2)
256(实验)	3.7(e -3)	2.35(e-2)	7.27(e-2)	0.127	0.168	**0. 192**	1.647	0.118	7.03(e-2)	3.49(e-2)

推论 1　长度为 N 的随机置换表中环数为 k 的闭合状态演化环的概率归一，$\sum_{k=1}^{N} p_N(k)=1$。

定理 2　长度为 N 随机演化表中闭合状态演化环的平均环长度的递推关系为 $\overline{l_{N+1}}=\frac{N^2+3N}{(N+1)^2}\overline{l_N}+\frac{1}{N+1}$，在 $\overline{l_1}=1$ 此迭代方程的解为 $\overline{l_N}=\frac{N+1}{2}$。

证明　分析长度为N+1 的随机置换表中环数为k的出现，可以分为下述两种情况：(1)在长度为N的、环数为k的所有 R_N^k 的随机置换表中，在第i_j个长度为 i_j, $j=1,2,\cdots,k$ 的环中任何两相邻元素间插入第N+1 个元素，这样插入有i_j种，每一次所增加的环长度为 $(i_j+1)^2-i_j^2=2i_j+1$。所以增加的总长度为 $(2i_j+1)i_j=2i_j^2+i_j$，考虑到 $i_1+i_2+\cdots+i_k=N$, $\overline{i_1^2+i_2^2+\cdots+i_k^2}=N\overline{l_N}$，平均将遍历所有可能的 k；而长度为 N 的、环数为 k=1,2 ,$\cdots$, N 的随机置换表总数为 $N!$，所以组成的长度为 N+1 随机置换表总的环长增加到 $L_{N+1}^1=\overline{l_N}N^2N!+(2N\overline{l_N}+N)N!$。(2)在长度为 N 的随机置换表中，将第 N+1 个元素单独组成一个对自身映射的新环，这样组成的长度为 N+1 的随机置换表中，每次环长增加 1，所以总的$N!$个随机置换表环长增加到 $L_{N+1}^2=N\overline{l_N}N!+N!$。最后将两部分加起来除以长度为 N+1 表的总数，并对长度 N+1 平均，就得到本定理的第一部分结果 $\overline{l_{N+1}}=\frac{L_{N+1}^1+L_{N+1}^2}{(N+1)(N+1)!}=\frac{N^2+3N}{(N+1)^2}\overline{l_N}+\frac{1}{N+1}$。

本定理的第二部分结果，则可在 $\overline{l_1}=1$，直接验证此迭代方程的解为 $\overline{l_N}=\frac{N+1}{2}$。　证毕

例如 N=256，$\overline{l_{256}}=128.5$, 与实际测量的平均环长度 128.12 很接近。

5　结束语

本文从理论得到了随机置换表中闭合的状态演化环，各环数出现的概率、平均环数以及平均环长，得到其封闭的计算式。为了快速计算，寻找到它们的递推关系式。数值模拟实验证实了理论结果的正确性。可以用上述理论检验分组加密算法中使用的置换表是否为随机置换表，Skipjack 加密算法中使用的 F 表，近似符合随机置换表的上述特性。

参 考 文 献

[1] Escrowed Encryption Standard (EES), Federal Information Processing Standards Publication 185, 1994 February 9.

[2] 冯登国，吴文玲. 分组密码的设计与分析. 北京：清华大学出版社, 2000.9: 12−14.

[3] 浙江大学数学系高等数学教研组. 工程数学——概率论与数理统计. 北京: 人民教育出版社, 1979: 42.

张申如：　男，1946 年生，硕士，教授，主要从事光电信息处理、扩展频谱通信及专用集成电路设计领域的研究.

郭　明：　男，1959 年生，高级工程师，主要从事跳频通信及专用集成电路设计领域的研究.