分组密码算法的测试方法研究

胡廉民，张九华

(乐山师范学院物理学与电子信息科学系 四川 乐山 614004)

【摘要】安全性是分组密码最重要的设计准则。该文基于分组密码算法，分析了算法的多种安全性测试方法和测试理论，提出相应的测试统计量。采用AES算法中的一个8×8 S盒，以一组长为1 048 576 b的随机数为测试序列，进行实际安全性测试。测试结果表明测试统计量符合实际测试结果，从而验证所提出的测试统计量具有实际可行性，有力地保证了分组密码的安全性设计。

关 键 词 AES算法； 分组密码； 随机性； S盒
中图分类号 TP309 **文献标识码** A

Research on Testing Method to Block Cipher

HU Lian-min，ZHANG Jiu-hua

(Department of Physics and Electronic Information, Leshan Teachers College Leshan Sichuan 614004)

Abstract Security is the most important principle of block cipher design. This paper analyses security-testing methods of block cipher, and proposes some statistically-testing variables. Finally, the random data with 1 048 576 b is used for the actual security-testing. The result shows that the presented statistically-testing variables agree with testing results and therefore are valuable to security design of block cipher.

Key words AES arithmetic; block cipher; randomicity; S-box

分组密码的研究从20世纪70年代开始，至今已经取得了很多研究成果[1-3]。分组密码的研究主要涉及分组密码的设计、安全性分析、统计性能测试等三个方面。由于差分密码分析[4]和线性密码分析[5]是攻击分组密码最有效的方法，因此现在的测试方法主要围绕随机性和S盒展开。本文从分组密码统计性能测试的角度出发，着重阐述随机性以及S盒的相关测试的一些典型方法，最后在分组密码的安全性评测方面，给出一个综合测试的方案。

1 随机性测试

在密码学的数据处理过程中，许多类数据都呈现了较好的随机二项分布特性，对于密码算法主要考察它对数据的随机化能力，因此在分组密码测试中主要的工具是二项分布的 χ^2 检验。对分组密码进行统计测试的目的是判断算法产生的输出是否在统计上难以与真随机数据区别开来。

1.1 频率测试

频率测试的目的是判断序列中的0、1个数是否基本相同。设需要测试的二进制比特流的长度为 n，n_0 代表含有0的个数，n_1 代表含有1的个数，则测试指标为：

$$X_1 = \frac{(n_0 - n_1)^2}{n} \tag{1}$$

如果 $n \geqslant 10$，且数据流是可证实的随机数据流，则 X_1 近似服从自由度为1的 χ^2 分布。

1.2 序列测试

序列测试的目的是判断序列中的00、01、10、11的个数是否基本相同。记 n_{00}、n_{01}、n_{10}、n_{11} 分别代表00、01、10、11的个数，由于子序列允许重叠，从而有 $n_{00} + n_{01} + n_{10} + n_{11} = (n-1)$，定义序列测试的指标为：

$$X_2 = \frac{4}{n-1}(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2) - \frac{2}{n}(n_0^2 + n_1^2) + 1 \tag{2}$$

如果 $n \geqslant 21$，且数据流是可证实的随机数据流，则 X_2 近似服从自由度为2的 χ^2 分布。

1.3 扑克测试

将长度为 n 的比特流分成长度为 m 的比特组，

收稿日期：2007－01－04
基金项目：四川省教育厅青年基金资助项目(2006B074)
作者简介：胡廉民(1969－)，男，硕士，讲师，主要从事计算机网络、信息安全方面的研究；张九华(1976－)，男，硕士，讲师，主要从事信息安全、信息处理等方面的研究.

共有 $k=\lfloor n/m \rfloor$ 个组，每组不重叠，有效扑克测试要求 $\lfloor n/m \rfloor \geqslant 5\times(2^m)$，$m$ 比特码组的状态共有 2^m 种，分别用 n_i 表示 k 个组中每种状态出现的次数，理论上希望每种状态出现的次数相同，相应的测试统计量定义为：

$$X_3=\frac{2^m}{k}\left(\sum_{i=1}^{2^m}n_i^2\right)-k \tag{3}$$

对于充分随机的序列，X_3 近似服从自由度为 2^m-1 的 χ^2 分布。m 通常取值3、4、8，当 $m=1$ 时即为频率测试。

1.4　游程测试

B_i、G_i 分别代表序列中长度为 i 的1、0游程的个数，$e_i=(n-i+3)/2^{i+2}$，k 等于满足 $e_i \geqslant 5^k$ 时最大的整数 i 值，相应的测试统计量定义为：

$$X_4=\sum_{i=1}^{k}\frac{(B_i-e_i)^2}{e_i}+\sum_{i=1}^{k}\frac{(G_i-e_i)^2}{e_i} \tag{4}$$

对于充分随机的序列，X_4 近似服从自由度为 $2k-2$ 的 χ^2 分布。

1.5　自相关测试

自相关测试的目的是考察非循环移位之后的序列与原序列之间的相关性。设 d 为一个固定的正整数，且满足 $1\leqslant d\leqslant\lfloor n/2 \rfloor$。设有长度为 n 的二进制序列 $s=(s_0,s_1,s_2,\cdots,s_{n-1})$，其中的一个二进制位表示为 s_i，与它延迟 d 位的二进制位表示为 s_{i+d}；自相关函数为 $A(d)=\sum_{i=0}^{n-d-1}s_i'\oplus s_{i+d}'$；$s_i'=(-1)^{s_i}$，相应的测试统计量定义为：

$$X_5=2\left(A(d)-\frac{n-d}{2}\right)\Big/\sqrt{n-d} \tag{5}$$

如果 $n-d\geqslant 10$，且测试序列充分随机，则 X_5 近似服从 $N(0,1)$ 分布。

2　S盒测试

S盒是许多密码算法的非线性部件，它的好坏直接影响密码算法的安全性[6]。一个 $n\times m$ 的S盒本质上可看作映射；其S盒函数：$S(x)=(f_1(x),f_2(x),\cdots,f_m(x))$：$F_2^n\to F_2^m$，如何全面准确地度量以及设计安全有效的S盒是分组密码设计与分析中的研究难题，本文结合已有的研究成果给出以下测试方法。

2.1　雪崩测试

严格雪崩准则包括完备性和雪崩效应。S盒函数 $S(x)=(f_1(x),f_2(x),\cdots,f_m(x)):F_2^n\to F_2^m$ 完备的是指其输出的任一比特和输入的每一比特相关。S盒函数 $S(x)=(f_1(x),f_2(x),\cdots,f_m(x)):F_2^n\to F_2^m$ 满足雪崩效应，是指改变输入的1个比特，大约有一半输出比特改变。

Webster和Tavares将完备性和雪崩效应合并成一个概念，严格雪崩准则，并且给出了相关的测试方法[7]。S盒函数 $S(x)=(f_1(x),\cdots,f_m(x)):F_2^n\to F_2^m$ 满足严格雪崩准则，是指改变输入的1 b，每个输出比特改变的概率为 $1/2$。

2.2　差分测试

差分测试的目的是度量一个密码函数抗差分分析的能力。

定义 1[8]　对 $S(x)=(f_1(x),f_2(x),\cdots,f_m(x))$：$F_2^n\to F_2^m$ 是多输出函数，令：

$$\delta=\frac{1}{2^n}\max_{\substack{\alpha\in F_2^n\\ \alpha\neq 0}}\max_{\beta\in F_2^m}\left|\{x\in F_2^n:S(x\oplus\alpha)-S(x)=\beta\}\right| \tag{6}$$

那么称 $S(x)$ 是差分 δ 均匀的，又称 δ 为 $S(x)$ 的差分均匀性，差分均匀性是针对差分密码分析而引入的统计量。代数次数与项数分布，代数中已经证明，任何 n 元布尔函数 $f(x):F_2^n\to F_2^m$ 都可以唯一的表示成如下正规形式[6]：

$$f(x)=a_0+\sum_{\substack{1\leqslant i_1\leqslant\cdots\leqslant i_k\leqslant n\\ 1\leqslant k\leqslant n}}a_{i_1i_2\cdots i_k}x_{i_1}x_{i_2}\cdots x_{i_k},x=$$
$$(x_1,x_2,\cdots,x_n),a_0,a_{i_1i_2\cdots i_k}\in F_2 \tag{7}$$

定义 2　令 $f(x):F_2^n\to F_2$ 是一个 n 元布尔函数，其代数正规形式中的最高项的次数为 $f(x)$ 的次数；它的代数正规形式中的 i 次项的个数称为 $f(x)$ 的 i 次项数；所有 i 次项数之和称为 $f(x)$ 的项数。如果代数次数低，就很难抵抗高阶差分密码分析；如果项数太少，也很难抵抗插值攻击。

2.3　线性与相关性测试

定义 3　$S(x)=(f_1(x),f_2(x),\cdots,f_m(x))$：$F_2^n\to F_2^m$ 是一个多输出函数，$\mu\cdot\nu$ 表示 μ 与 ν 的点积，$l(x)$ 是所有线性函数集合 l_n 中的一个函数，$d_H()$ 表示汉明距离。则 $S(x)$ 的非线性度为：

$$N_s=\min_{\substack{l\in L_n\\ 0\neq u\in F_2^m}}d_H(u\cdot S(x),l(x)) \tag{8}$$

在线性密码分析中，关键是构造单轮的有效线性逼近，而单轮总是离不开S盒的线性逼近[9]。令 $S:F_2^n\to F_2^m$，$x\to y=S(x)$ 是一个 $n\times m$ 的S盒，它的任意线性逼近都可以表示为 $a\cdot x=b\cdot y$，其中 $a\in F_2^n$；$b\in F_2^m$。而该式成立的概率 p 满足 $|p-1/2|\leqslant 1/2-N_S/2$，且称 $|p-1/2|$ 为线性逼近的

优势。显然，S 盒的非线性度越大就越能抗线性密码分析[10]。

3 测试实例

在Windows平台下，运用标准C语言可实现上述方案。对自相关测试中移位长度选取3；扑克测试中扑克长度选取4，所得结果如表1所示。

表1 1 048 576 b数据随机性检验结果

各分布典型值	频率测试临界值	序列测试临界值	扑克-4测试临界值	游程测试临界值	自相关性-3测试临界值
0.100	2.710	4.610	22.300 0	37.900 0	1.282
0.050	3.842	5.991	25.000 0	41.300 0	1.645
0.250	5.020	7.380	7.500 0	44.500 0	2.326
0.010	6.630	9.210	30.600 0	48.300 0	2.576
0.005	7.880	10.600	32.800 0	51.000 0	3.291
实测值	0.503	0.548	20.881 2	29.888	1.663

选取AES加密算法的一个8×8 S盒的数据如下：

82	9	106	213	48	54	165	56	191	64	163	158	129	243	215	251
124	227	57	130	155	47	255	135	52	142	67	68	196	222	233	203
4	123	148	50	166	194	35	61	238	76	149	1	66	250	195	78
8	46	161	102	40	217	36	178	118	91	162	73	109	139	209	37
114	248	246	100	134	104	152	22	212	164	92	204	93	101	182	146
108	112	72	80	253	237	185	218	94	21	70	87	167	141	157	132
144	216	171	0	140	188	211	10	247	228	88	5	184	179	69	6
208	44	30	143	202	63	15	2	193	175	189	3	1	19	138	107
58	145	17	65	79	103	220	234	151	242	207	206	240	180	230	115
150	172	16	34	231	173	53	133	226	249	55	232	28	117	223	110
71	241	26	113	29	41	197	137	111	183	98	14	170	24	190	27
252	86	62	75	198	210	121	32	154	219	192	254	120	205	90	244
31	221	168	51	136	7	199	49	177	18	16	89	39	128	236	95
96	81	127	169	25	181	74	13	45	229	122	159	147	201	156	239
160	224	59	77	174	42	245	176	200	235	187	60	131	83	153	97
23	43	4	126	186	19	214	38	225	105	20	99	85	33	12	125

S盒测试结果如表2～5所示：

表2 S盒的雪崩数据比特量分布

第1位改变数	第2位改变数	第3位改变数	第4位改变数	第5位改变数	第6位改变数	第7位改变数	第8位改变数
132	132	116	144	116	124	116	128
120	124	144	128	124	116	128	136
132	132	128	120	144	128	136	128
136	136	120	116	128	136	128	140
116	128	116	132	128	128	140	136
116	132	132	120	120	140	136	136
136	136	120	132	120	136	136	124
132	144	132	136	124	136	124	132

表3 S盒的雪崩数据比特量分布均匀度

第1位改变比	第2位改变比	第3位改变比	第4位改变比	第5位改变比	第6位改变比	第7位改变比	第8位改变比
0.515 6	0.515 6	0.453 1	0.562 5	0.453 1	0.484 4	0.453 1	0.500 0
0.468 8	0.484 4	0.562 5	0.500 0	0.484 4	0.453 1	0.500 0	0.531 2
0.515 6	0.515 0	0.500 0	0.468 8	0.562 5	0.500 0	0.531 2	0.500 0
0.531 2	0.531 2	0.468 8	0.453 1	0.500 0	0.531 2	0.500 0	0.546 9
0.453 1	0.500 0	0.453 1	0.515 6	0.500 0	0.500 0	0.546 9	0.531 2
0.453 1	0.515 6	0.515 6	0.468 8	0.468 8	0.546 9	0.531 2	0.531 2
0.531 2	0.531 2	0.468 8	0.515 6	0.468 8	0.531 2	0.531 2	0.484 4
0.515 6	0.562 5	0.515 6	0.531 2	0.484 4	0.531 2	0.484 4	0.515 6

注：分布均值：0.504 9；分布方差：0.001 0；Chi^2统计值：66.000

表4 S盒函数的项数分布

i次项数	i次项 C_8^i	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
0	1	1	1	0	0	0	1	1	0
1	8	4	4	4	4	5	3	3	4
2	28	16	14	12	11	17	7	10	10
3	56	30	30	38	29	29	32	31	26
4	70	33	33	36	39	32	32	30	33
5	56	30	31	33	33	34	27	4	24
6	28	15	16	17	16	11	10	11	11
7	8	3	4	5	4	3	2	2	2
8	1	0	0	0	0	0	0	0	0

表5 S盒函数的项数分布均匀度

i次项个数	1次项比例	2次项比例	3次项比例	4次项比例	5次项比例	6次项比例	7次项比例	8次项比例
i=0	1.000	1.000	0.000	0.000	0.000	1.000	1.000	0.000
i=1	0.500	0.500	0.500	0.500	0.625	0.375	0.375	0.500
i=2	0.571	0.500	0.429	0.393	0.607	0.250	0.357	0.357
i=3	0.536	0.536	0.679	0.518	0.518	0.571	0.554	0.464
i=4	0.471	0.471	0.514	0.557	0.457	0.457	0.429	0.471
i=5	0.536	0.554	0.589	0.589	0.607	0.482	0.429	0.429
i=6	0.536	0.571	0.607	0.571	0.393	0.357	0.393	0.393
i=7	0.375	0.500	0.625	0.500	0.375	0.250	0.250	0.250
i=8	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

平均值: 0.485 9 方差值: 0.010 7

(下转第736页)

同理也可以构造出负边沿触发的D触发器的完全模型，这里不再赘述。

3 结 束 语

该方案通过为时序元件建立完全模型，将时序电路中的时钟信号CLK引入，为非同步时序电路构建用于测试的单时钟同步电路模型，从而直接用同步时序电路测试生成算法解决非同步电路的测试生成问题。本文的研究已经以该方案为基础，结合成熟的同步时序测试生成算法完成了一个通用的时序电路的测试生成平台，在实际应用中取得良好的效果。该方案的基础是稳态下的确定性测试生成算法，在建模时也是基于稳态分析进行，未考虑动态因素，因此采用该方案生成的测试激励在时序配合上会有欠缺，有待进一步地研究和探讨。

参 考 文 献

[1] 杨士元. 数字系统的故障诊断与可靠性设计[M]. 第2版. 北京: 清华大学出版社, 2000.
[2] JHA N, GUPTA S. Testing of digital systems[M]. Cambridge UK: Cambridge University Press, 2003.
[3] LIN Xi-jiang, POMERANZ I, REDDY S M. MIX: A test generation system for synchronous sequential circuits[C]// VLSI Design, 1998 Eleventh International Conference. Los Alamitos: IEEE Comp Soc, 1998.
[4] 陈光禹; 潘中良. 基于遗传算法的数字电路测试生成方法[J]. 电子学报, 1997, 25(4): 111-113.
[5] 曾芷德. 特大规模组合电路高速测试生成系统ATGTA-1[J]. 国防科技大学学报, 1999, 21(2): 37-41.
[6] 李忠诚, 潘榆奇, 闵应骅. 一个基于电路结构分析的测试产生系统—SABATPG[M]. 中国科学(A辑), 1993, 2(2): 189-196.
[7] LIN Xi-jiang, THOMPSON R. Test generation for designs with multiple clocks[C]// Design Automation Conference. Anaheim: Institute of Electrical and Electronics Engineers Inc, 2003.
[8] GHOSH S, CHAKRABORTY T J, TGICAPP: An asynchronous distributed approach to test vector generation based on circuit partitioning on parallel processors[C]// Systems, Man, and Cybernetics, 1991 IEEE International Conference. Piscataway: IEEE, 1991.
[9] BANERJEE S, CHAKRADHAR S T, ROY R K. Synchronous test generation model for asynchronous circuits[C]// In Proc of the Int. Conf on VLSI Design. Bangalore. Los Alamitos: [s.n.], 1996: 178-185.
[10] GOLDSTEIN L, THIGPEN E. SCOAP: Sandia controllability / observability analysis program[C]// Proceedings of the Design Automation Conference. Minneapolis: IEEE Computer Society ATTN, 1980: 190-196.

编 辑 熊思亮

(上接第722页)

4 结 束 语

本文从分组密码随机性测试的角度出发，介绍了频率测试、序列测试、扑克测试、游程测试以及自相关测试等随机性测试理论，给出了相应的测试统计量。针对S盒测试，归纳了严格雪崩准则、代数次数与项数分布、差分、线性与相关性等测试方法，给出了各种测试方法与抵抗各种攻击之间的关系，并通过实例数据验证了各测试统计量的测试可行性和必要性。

参 考 文 献

[1] 冯登国, 吴文玲. 分组密码的设计与分析[M]. 北京: 清华大学出版社, 2000.
[2] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.
[3] 冯登国. 国内外密码学研究现状及发展趋势[J]. 通信学报, 2002, 23(5): 18-26.
[4] MATSUI M. Linear cryptanalysis method for DES cipher [C]//Prcceedings of Cryptology-EUROCRYPT'93, Berlin: Springer-Verlag, 1994: 386-397.
[5] KALISKI B J, Robshaw M. Linear cryptanalysis using multiple approximations and FEAL [C]//Prcceedings of The 2nd Fast Software Encryption workshop, Berlin: Springer-Verlag, 1995: 249-264.
[6] 温巧燕, 钮信忻, 杨义先. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000.
[7] WEBSTER A F, TAVARES S E. On the design of S-box [C]//Advances in Cryptology-Crypto'85, LNCS 218.Berlin: Spring-Verlag, 1985: 525-534.
[8] MENEZES A J, VANSTONE S A. Handbook of Applied Cryptography[M]. New York: CRC Press, 1996.
[9] STINSON D R.密码学原理与实践[M]. 冯登国 译. 北京: 电子工业出版社, 2003.
[10] KNUDSEN L, ROBSHAW M. Non-linear approximations in linear cryptanalysis[C]// Proceedings of Cryptology-EUROCRYPT'96. Berlin: Springer-Verlag, 1994: 252-267.

编 辑 税 红