文章编号:1671-8860(2010)05-0558-04　　文献标志码:A

S 盒的互相关测试算法设计

高　胜[1]　马文平[1]　郭　娜[1]　陈秋丽[1]

(1　西安电子科技大学 ISN 国家重点实验室,西安市太白南路 2 号,710071)

摘　要:S 盒是构成分组密码算法重要的非线性部件,其密码学性质直接影响整个密码算法的安全性,因此对 S 盒的安全性检测十分重要。以往对 S 盒的安全性评估大多数集中在检测分量函数的安全性上,本文考虑了分量函数之间的关系,并利用 Shannon 在对称密码系统设计中所提出的混淆和扩散的思想,提出了 S 盒的互相关测试指标,设计了测试算法,更好地评价了 S 盒的安全性能。对 DES 和 AES 的 S 盒分别进行了实验,给出了测试结果。

关键词:S 盒;互相关;测试;算法

中图法分类号:TP311

S 盒是现代分组密码体制中重要的组成部件。它本质上是一个多输出布尔函数,可以表示为 $S(x)=(f_1(x),f_2(x),\cdots,f_m(x)):F_2^n\to F_2^m$,其中,每个 $f_i(x):F_2^n\to F_2$ 是布尔函数。S 盒多被用于分组密码系统,以增强密码体制的安全性[1],也有学者建议将其用于流密码系统,以加快加解密速度[2]。S 盒的安全性关系到整个密码算法的安全性,因而制定安全性测试指标,进而对其安全性作出评价十分重要[3-9]。遗憾的是,以往的测评标准大都集中在构成 S 盒的分量布尔函数上,很少关注函数之间的关联程度。根据 Shannon 在对称密码系统设计中所提出的指导思想[10],若构成 S 盒的分量函数高度相关,那将是一个缺陷。文献[11]研究了任意两个布尔函数之间的相关性,文献[12]基于互相关函数,推广了文献[13]对单个布尔函数所提出的全局雪崩准则[14]。本文在此基础上,结合实际应用背景提出了 S 盒的互相关检测指标,设计了测试算法,更好地评价了 S 盒的安全性能。

1　预备知识

1.1　基本概念

定义 1　令 B_n 为全体 2^{2^n} 个 n 元布尔函数的集合。对任意的 $\alpha\in F_2^n$,α 与 x 的内积 $<\alpha,x>$ 表示 B_n 中的线性函数,$f(x)\in B_n$ 在 α 处的 Walsh 变换定义为:

$$W_f(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+<\alpha,x>}$$

定义 2　令 $wt(\cdot)$ 表示汉明重量,对 $f(x)\in B_n$,如果 $wt(f(x))=2^{n-1}$,则称 $f(x)$ 是平衡的。

定义 3　令 $\boldsymbol{I}_m$ 表示 m 阶单位阵,对 m 阶(1,-1)矩阵 $\boldsymbol{A}$,如果有 $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}=m\boldsymbol{I}_m$,则称 $\boldsymbol{A}$ 为 Hadamard 矩阵,其中,$\boldsymbol{A}^{\mathrm{T}}$ 表示 $\boldsymbol{A}$ 的转置矩阵。另外,阶为 2^n 的 Sylvester-Hadamard 矩阵 $\boldsymbol{H}_n$ 递归定义如下:

$$H_0=1,\boldsymbol{H}_n=\begin{bmatrix}\boldsymbol{H}_{n-1} & \boldsymbol{H}_{n-1}\\ \boldsymbol{H}_{n-1} & -\boldsymbol{H}_{n-1}\end{bmatrix},n=1,2,\cdots$$

定义 4　令 $f(x),g(x)\in B_n$,互相关函数定义为:

$$C_{f,g}(u)=\sum_{x\in F_2^n}(-1)^{f(x)+g(x+u)},u\in F_2^n$$

易知,对任意的 $u\in F_2^n$,都有 $C_{f,g}(u)=C_{g,f}(u)$。当 $f=g$ 时,互相关函数就变成自相关函数。众所周知,自相关函数可以反映布尔函数的扩散性能。

定义 5[12]　令 $f(x),g(x)\in B_n$,$u\in F_2^n$,定义

$$\delta_{f,g}=\sum_{u\in F_2^n}C_{f,g}^2(u)\qquad(1)$$

收稿日期:2010-03-15。

项目来源:国家 863 计划资助项目(2007AA01Z472);国家自然科学基金资助项目(60773002);国家教育部留学回国人员科研启动基金资助项目;高等学校创新引智计划资助项目(B08038)。

$$\Delta_{f,g}=\max_{u\in F_2^n}|C_{f,g}(u)| \tag{2}$$

定义 6　对 $n\times m$ 的 S 盒,令 f_i、f_j($1\leqslant i\leqslant j\leqslant m$)为 S 盒的任意两个分量布尔函数,定义 S 盒的平方和指标性能和绝对值指标性能如下:

$$\delta_S=\max_{1\leqslant i\leqslant j\leqslant m}\delta_{f_i,f_j},\Delta_S=\max_{1\leqslant i\leqslant j\leqslant m}\Delta_{f_i,f_j} \tag{3}$$

这两个指标的本质在于通过度量分量函数之间的关联程度,更好地反映 S 盒的混淆和扩散的性能。显然,两个指标值越小,S 盒的安全性越好。

1.2　相关理论

为了度量 S 盒的平方和指标性能,需要有效求解式(1)的方法。

定理 1[11]　令 $f(x),g(x)\in B_n$,$m=2^n-1$,则有:

$$[C_{f,g}(0)\cdots C_{f,g}(m)]\boldsymbol{H}_n=[W_f(0)W_g(0)\cdots W_f(m)W_g(m)]$$

推论 1　$$\delta_{f,g}=\frac{1}{2^n}\sum_{u\in F_2^n}W_f^2(u)W_g^2(u) \tag{4}$$

式(4)可在定理 1 的等式两边分别乘以各自的转置,再根据式(1)则可证明。因此,可利用式(4)求取平方和指标。但考虑到求一个布尔函数的 Walsh 谱计算量较大,为了提高效率,对文献[5]求谱值的方法稍作修改,给出如下快速计算布尔函数谱值的方法。

定理 2　令 $\boldsymbol{Y}=[y_0,y_1,\cdots,y_{2^n-1}]^{\mathrm{T}}$ 表示布尔函数 $f(x)\in B_n$ 的真值向量,$f(x)$ 的 Polarity 真值向量记为 $\boldsymbol{Y}_n=[(-1)^{y_0},(-1)^{y_1},\cdots,(-1)^{y_{2^n-1}}]^{\mathrm{T}}$,$f(x)$ 所有谱值构成的向量记为 $\boldsymbol{R}_n=[r_0,r_1,\cdots,r_{2^n-1}]^{\mathrm{T}}$,其中,$y_i=f(i)$,$r_i=W_f(i)$,$0\leqslant i\leqslant 2^n-1$,则 $f(x)$ 的全部 Walsh 谱值可快速递归计算如下:

$$\boldsymbol{R}_n=\boldsymbol{H}_n\boldsymbol{Y}_n=\begin{pmatrix}\boldsymbol{A}+\boldsymbol{B}\\ \boldsymbol{A}-\boldsymbol{B}\end{pmatrix}$$

其中,$\boldsymbol{A}=\boldsymbol{H}_{n-1}\cdot[(-1)^{y_0},(-1)^{y_1},\cdots,(-1)^{y_{2^{n-1}-1}}]^{\mathrm{T}}$,$\boldsymbol{B}=\boldsymbol{H}_{n-1}\cdot[(-1)^{y_{2^{n-1}}},(-1)^{y_{2^{n-1}+1}},\cdots,(-1)^{y_{2^n-1}}]^{\mathrm{T}}$。

证明　1)当 $n=1$ 时,由 Walsh 谱定义,有:

$$\boldsymbol{R}_1=[r_0,r_1]^{\mathrm{T}}=\boldsymbol{H}_1\boldsymbol{Y}_1=\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}(-1)^{y_0}\\(-1)^{y_1}\end{pmatrix}=\begin{pmatrix}\boldsymbol{A}+\boldsymbol{B}\\ \boldsymbol{A}-\boldsymbol{B}\end{pmatrix}$$

这里,$\boldsymbol{A}=H_0\cdot[(-1)^{y_0}]^{\mathrm{T}}$,$\boldsymbol{B}=H_0\cdot[(-1)^{y_1}]^{\mathrm{T}}$,所以,当 $n=1$ 时命题成立。

2) 假设 $n=k$ 时,命题成立,即

$$\boldsymbol{R}_k=[r_0,r_1,\cdots,r_{2^k-1}]^{\mathrm{T}}=\boldsymbol{H}_k\boldsymbol{Y}_k=\begin{pmatrix}\boldsymbol{A}+\boldsymbol{B}\\ \boldsymbol{A}-\boldsymbol{B}\end{pmatrix}$$

其中,$\boldsymbol{A}=\boldsymbol{H}_{k-1}\cdot[(-1)^{y_0},(-1)^{y_1},\cdots,(-1)^{y_{2^{k-1}-1}}]^{\mathrm{T}}$,$\boldsymbol{B}=\boldsymbol{H}_{k-1}\cdot[(-1)^{y_{2^{k-1}}},(-1)^{y_{2^{k-1}+1}},\cdots,(-1)^{y_{2^k-1}}]^{\mathrm{T}}$。那么,当 $n=k+1$ 时,$\boldsymbol{R}_{k+1}=[r_0,r_1,\cdots,r_{2^{k+1}-1}]^{\mathrm{T}}=\boldsymbol{H}_{k+1}\cdot\boldsymbol{Y}_{k+1}=$

$$\begin{pmatrix}\boldsymbol{H}_k&\boldsymbol{H}_k\\ \boldsymbol{H}_k&-\boldsymbol{H}_k\end{pmatrix}[(-1)^{y_0},\cdots(-1)^{y_{2^k-1}},(-1)^{y_{2^k}},\cdots,(-1)^{y_{2^{k+1}-1}}]^{\mathrm{T}}=$$

$$\begin{pmatrix}\boldsymbol{H}_k\cdot\boldsymbol{Y}_k+\boldsymbol{H}_k\cdot[(-1)^{y_{2^k}},\cdots,(-1)^{y_{2^{k+1}-1}}]^{\mathrm{T}}\\ \boldsymbol{H}_k\cdot\boldsymbol{Y}_k-\boldsymbol{H}_k\cdot[(-1)^{y_{2^k}},\cdots,(-1)^{y_{2^{k+1}-1}}]^{\mathrm{T}}\end{pmatrix}=\begin{pmatrix}\boldsymbol{A}+\boldsymbol{B}\\ \boldsymbol{A}-\boldsymbol{B}\end{pmatrix}$$

其中,$\boldsymbol{A}=\boldsymbol{H}_k\cdot[(-1)^{y_0},(-1)^{y_1},\cdots,(-1)^{y_{2^k-1}}]^{\mathrm{T}}$,$\boldsymbol{B}=\boldsymbol{H}_k\cdot[(-1)^{y_{2^k}},(-1)^{y_{2^k+1}},\cdots,(-1)^{y_{2^{k+1}-1}}]^{\mathrm{T}}$,证毕。

为了度量 S 盒的绝对值指标性能,需要有效求解式(2)的办法。文献[12]利用布尔函数的汉明重量刻画了 $\Delta_{f,g}$ 的计算。

引理 1[12]　令 $C'_u=\{x\in F_2^n:f(x)=1,g(x+u)=1\}$,$f(x),g(x)\in B_n$,$u\in F_2^n$,则可通过下式求得 $\Delta_{f,g}$:

$$\Delta_{f,g}=2^n-2wt(f)-2wt(g)+4\max_{u\in F_2^n}|C'_u| \tag{5}$$

引理 2[12]　$0\leqslant\Delta_{f,g}\leqslant 2^n$;$C_{f,g}^2(0)\leqslant\delta_{f,g}\leqslant 2^{3n}$。

在实际应用中,构成 S 盒的分量布尔函数一般都是平衡的,故在 S 盒中,引理 1 可以进行简化。

推论 2　令 $f(x),g(x)\in B_n$ 是 S 盒的任意两个分量布尔函数,则有:

$$\Delta_{f,g}=-2^n+4\max_{u\in F_2^n}|C'_u| \tag{6}$$

2　S 盒的互相关测试

2.1　互相关测试算法

1) 对给定的 $n\times m$ S 盒,计算构成 S 盒的 m 个布尔函数 $f_k(x)$($1\leqslant k\leqslant m$)的 Polarity 真值向量表,并存入 sbool[m][loop]中;

2) 将 S 盒的 Polarity 真值向量表两两按顺序与 $\boldsymbol{H}_1$ 相乘并保存,初始化 $s=2$;

3) 将第 2)步的保存结果按 s 个分组以后,依照顺序两两相加、相减,并将结果保存;

4) 以 $2s$ 更新 s 的值,并判断 s 是否等于 2^n,若不等,则跳回第 3)步;若相等,则可得谱值;

5) 重复第 2)~4)步,并利用式(4)求 δ_{f_i,f_j};

6) 对于给定的 $u\in F_2^n$,寻找使得 $f_i(x)=1$、

$f_j(x+u)=1$ 成立的 x 个数的最大值；

7) u 遍历 $0\sim2^n-1$，重复第6)步，求得所有 u 对应的 x 个数的最大值；

8) 重复第6)、7)步，并利用式(6)求得 Δ_{f_i,f_j}；

9) 对每个待测 S 盒求出 δ_{f_i,f_j}、Δ_{f_i,f_j} 的最大值，并输出 $\delta_S=\max\limits_{1\leqslant i\leqslant j\leqslant m}\delta_{f_i,f_j}$，$\Delta_S=\max\limits_{1\leqslant i\leqslant j\leqslant m}\Delta_{f_i,f_j}$。

注意，该算法只适用于分量函数平衡的 S 盒。当要求对分量函数不平衡的 S 盒测试时，只需将第8)步中的“利用式(6)”换成“利用式(5)”即可。

2.2 实验结果

对DES和AES的 S 盒分别进行互相关测试，记 $\delta_{f_i,f_j}=\delta_{f_{i,j}}$，$\Delta_{f_i,f_j}=\Delta_{f_{i,j}}$，表1表示DES S 盒的互相关性能测试结果，表2表示AES S 盒的平方和指标性能和绝对值指标性能测试。由于互相关函数的对称性，表2中空白部分的值实际上关于该正方形表格的主对角线对称。

一般称任意两个布尔函数在零点的互相关函数值为这两个函数的零相关度。本文还对DES和AES的 S 盒分别进行了零相关度的测试。实验结果表明，构成DES每个 S 盒的任意两个不同函数间的零相关度均为0，每个函数与自己的零相关度均为64；AES S 盒的任意两个不同函数间的零相关度均为0，每个函数与自己的零相关度均为256，这和预期的结果是一样的。

从实验结果还可以看出，DES S 盒的平方和指标值和绝对值指标值比较分散，而AES S 盒这两个指标值相对集中，体现出很好的混淆和扩散性能。因此，S 盒的互相关测试对 S 盒的安全性评价是一个较好的度量标准。

表1 DES前4个和后4个S盒性能测试结果

Tab. 1 Performance for DES S-boxes(S_1, S_2, S_3, S_4) and S-boxes(S_5, S_6, S_7, S_8)

	$(\delta_{f_{i,j}},\Delta_{f_{i,j}})$				$(\delta_{f_{i,j}},\Delta_{f_{i,j}})$			
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
f_{11}	(20 224,64)	(19 840,64)	(21 376,64)	(15 232,64)	(16 000,64)	(19 456,64)	(17 152,64)	(12 544,64)
f_{12}	(4 160,20)	(9 280,28)	(7 680,28)	(2 432,16)	(7 872,32)	(5 376,16)	(16 448,28)	(4 922,32)
f_{13}	(5 376,28)	(5 952,20)	(5 504,8)	(2 432,16)	(6 272,24)	(7 424,24)	(6 592,20)	(4 160,20)
f_{14}	(3 648,16)	(3 776,16)	(4 992,24)	(15 232,64)	(5 888,24)	(6 336,20)	(6 272,16)	(6 848,28)
f_{22}	(11 776,64)	(25 984,64)	(19 456,64)	(15 232,64)	(18 304,64)	(15 616,64)	(34 084,64)	(16 768,64)
f_{23}	(5 440,24)	(4 480,20)	(5 248,20)	(15 232,24)	(4 672,24)	(8 576,24)	(1 536,8)	(6 336,24)
f_{24}	(4 352,16)	(5 184,24)	(11 008,32)	(2 432,16)	(5 824,24)	(6 720,24)	(2 624,12)	(3 456,16)
f_{33}	(16 000,64)	(1 600,64)	(12 544,64)	(15 232,64)	(14 464,64)	(15 232,64)	(13 696,64)	(16 768,64)
f_{34}	(9 664,28)	(4 928,20)	(8 320,20)	(2 432,16)	(3 904,28)	(6 464,20)	(23 296,64)	(6 336,20)
f_{44}	(19 072,64)	(14 464,64)	(19 072,64)	(15 232,64)	(10 624,64)	(16 000,64)	(34 048,64)	(12 928,64)
性能	(20 224,64)	(25 984,64)	(21 376,64)	(15 232,64)	(18 304,64)	(19 456,64)	(34 048,64)	(16 768,64)

表2 AES S 盒平方和指标和绝对值指标性能测试结果

Tab. 2 Performance of Sum-of-squares Indicator and Absolute Indicator for AES S-box

	$\delta_{f_{i,j}}$								$\Delta_{f_{i,j}}$							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
f_1	133 120								256							
f_2	65 536	133 120							32	256						
f_3	65 536	65 536	133 120						32	32	256					
f_4	65 536	64 512	66 560	133 120					28	32	32	256				
f_5	64 512	64 512	64 512	64 512	133 120				32	32	32	32	256			
f_6	64 512	64 512	64 512	65 536	65 536	133 120			32	28	32	32	32	256		
f_7	65 536	66 560	65 536	66 560	64 512	66 560	133 120		32	32	28	32	32	32	256	
f_8	65 536	65 536	66 560	65 536	65 536	64 512	65 536	133 120	32	32	32	32	32	32	256	
性能	133 120	133 120	133 120	133 120	133 120	133 120	133 120	133 120	256	256	256	256	256	256	256	256

3 结 语

基于Feistel网络的分组密码算法，其安全性主要依赖于轮函数中使用的 S 盒。因此，人们对 S 盒设计了许多安全性测试方法，如平衡性测试、严格雪崩测试、线性方程测试、线性逼近测试、相关免疫测试、差分分布测试等。但是这些测试方法大都局限于 S 盒的分量布尔函数的性能上，而忽略了函数之间的关系。根据Shannon信息论的思想，如果存在高度相关的分量函数用于 S 盒时，即使每一个分量函数都很优秀，这样的 S 盒也将是不安全的。本文考虑这个问题，提出了度量 S 盒安全性能的互相关测试指标，设计了互相

关测试算法,弥补了原来测试方法的不足,更好地度量了 S 盒的安全性能。

本文互相关测试算法不仅可以比较同量级的 S 盒性能,还能比较直观地把握 S 盒各分量函数之间的关联程度,因而对 S 盒的设计和安全性评估都起到很好的作用。另外,针对目前不断出现的新的攻击方法,设计更多安全性测试指标,并开发一个自动化检测 S 盒安全性能的工具正在研究。

参 考 文 献

[1] Brickell E F, Moore J H, Purtill M R. Structures in the S-boxes of the DES[C]. Advances in Cryptology-CRYPTO'86. New York: Springer-Verlag, 1986:3-8

[2] Zhang M, Chan A. Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers[C]. Advances in Cryptology—CRYPTO'20. Berlin: Springer-Verlag, 2000: 501-514

[3] Mister S, Adams C. Practical S-box Design[C]. The 3rd Annual Workshop on Selected Areas in Cryptography(SAC'96), Kingston, Canada, 1996

[4] Knudsen L, Raddum H. Linear Approximation to the MARS S-box[OL]. http:/www. cosic. esat. kuleuven. be/nessie/reports/, 2000

[5] Porwik P. The Spectral Test of the Boolean Function Linearity[J]. Journal of Applied Mathematics and Computer Science, 2003, 13(4):567-575

[6] Xiao G Z, Massey J L. A Spectral Characterization of Correlation-immune Combining Functions[J]. IEEE Trans on Information Theory, 1988, 34(3): 569-571

[7] Biham E, Shamir A. Differential Cryptanalysis of DES- like Cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72

[8] Nyberg K. Perfect Nonlinear S-boxes[C]. Advances in Cryptolygy—EUROCRYPT'91. New York: Springer-Verlag, 1991: 161-173

[9] Webster A F, Tavares S E. On the Design of S-Boxes[C]. Crypto'85, New York, 1985

[10] Shannon C E. Communication Theory of Secrecy Systems[J]. Bell System Technical Journal, 1949, 28(4):656- 715

[11] Sarkar P, Maitra S. Cross-correlation Analysis of Crypto- graphically Useful Boolean Functions and S-boxes[J]. Theory Computer Systems, 2002, 35:39-57

[12] Zhou Yu, Xie Min, Xiao Guozhen. On the Global Avalanche Characteristics Between Two Boolean Functions and the Higher Order Nonlinearity[J]. Information Sciences, 2010, 180: 256-265

[13] Zhang X M, Zheng Y L. GAC—the Criterion for Global Avalanche Characteristics of Cryptographic Functions[J]. Journal for Universal Computer Science, 1995, 1(5): 316-333

[14] Forre R. The Strict Avalanche Criterion: Spectral Pro- perties of Boolean Functions and an Extend Definition[C]. Advances in Cryptology—CRYPTO'88. New York: Springer-Verlag, 1988:450-468

第一作者简介:高胜,博士生,主要研究方向为密码学、信息安全、密码安全性评估算法设计。

E-mail:gs14011@163.com

Design of Cross-Correlation Test Algorithm on S-Box

GAO Sheng[1]　*MA Wenping*[1]　*GUO Na*[1]　*CHEN Qiuli*[1]

(1　National Key Laboratory of ISN, Xidian University, 2 South Taibai Road, Xi'an 710071, China)

Abstract: In the past, security assesment on S-box is concentrated on examining the security of each component function, with little regard for the relationship between these functions. Considering this problem, using the idea of confusion and diffusion presented by shannon on symmetric cryptography, we propose the cross-correlation test indicators of an S-box. An algorithm of cross-correlation test is presented, which evaluates the security of the S-box better. Finally, experiments on the S-boxes of DES and AES were undertaken, and the test results are given.

Key words: S-box; cross-correlation; test; algorithm

About the first author: GAO Sheng, Ph. D candidate, majors in cryptology, information security and design of cryptographic security assessment algorithm.

E-mail: gs14011@163.com