提高S盒非线性度的有效算法*)

陈 华 吴文玲 冯登国

(中国科学院软件研究所信息安全国家重点实验室 北京 100080)

摘 要 S盒是分组密码算法中的重要的非线性部件。William Millan 曾给出一个能改善S盒非线性度的 Hill Climbing 算法,它通过交换S盒的两个输出向量来提高S盒的非线性度直到非线性度达到一个局部最优值,即交换任何两个输出向量也不能提高S盒的非线性度。本文研究了如何同时改变S盒的三个输出向量的位置来提高S盒的非线性度,并给出了 MHC 算法,它能在 Hill Climbing 算法的基础上进一步提高非线性度。实验证明,MHC 算法对随机S盒的优化效果明显大于 Hill Climbing 算法。

关键词 分组密码,S盒,非线性度

An Effective Algorithm to Increase the Nonlinearity of S-boxes

CHEN Hua WU Wen-Ling FENG Deng-Guo

(State Key Laboratory of Information Security, Institute of Software of Chinese Academy of Sciences, Beijing 100080)

Abstract A S-box is the important nonlinear conponent of block cipher algorithms. William Millian provied the Hill Climbing algorithm for improving the nonlinearity of S-boxes, which can increase the nonlinearity of a S-box by swapping two output vectors. Under the algorithm, the nonlinearity will reach a local maximum, which means that swapping any two output vectors can not increase the nonlinearity any more. In this paper, how to improve the nonlinearity of S-boxes by changing the positions of three output vectors simultaneously is explored. The MHC algorithm is given which can increase the nonlinearity on the basis of the Hill Climbing algorithm. The experimental results show that, the MHC algorithm is apparently more effective than the Hill Climbing to improve the nonlinearity of random S-boxes.

Keywords Block cipher, S-Box, Nonlinearity

S盒实质上是多输出布尔函数,是分组密码中重要的非线性部件,其好坏直接影响到分组密码的安全性。自从 DES[1] 被公布以来,如何构造满足各种密码特性的S盒一直是分组密码的一个研究热点。利用数学函数可以构造密码性能强的S盒,其中人们使用最多的是有限域上的幂指数函数,已有许多著名的密码算法采用幂指数函数来构造S盒,如 Aes[2],Shark[3], Square[4],它们的非线性度、差分均匀性和代数次数都能达到最佳值。但是由于幂指数函数的代数结构的简单而容易遭受不同类型的攻击如插值攻击[5]。除了数学函数,也可以按照一定的规则直接构造S盒,如 Serpent[6] 的S盒就是在 DES 的S盒的基础上构造的。

William Millian 提出了利用布尔函数的 Walsh 谱来改善布尔函数的非线性度的方法,也称之为 Hill Climbing 方法[7]。此方法的本质是研究改变布尔函数的局部输出可以改善非线性度的 Walsh 谱特征,使用这种方法,可以使随机生成的S盒的非线性度得到大大改善。文[7]研究了交换单输出布尔函数的两个输出能提高非线性度的谱特征。进一步地,在文[8]中,William 将文[1]的研究扩展到S盒中去,通过交换两个输出向量来提高S盒的非线性度直到交换任何两个输出都不能再提高S盒的非线性度,这时我们称S盒的非线性度达到了局部最优值。文[9]将文[8]的对S盒的 Hill Climbing 算法应用到生成S盒的遗传算法,实验证明使用 Hill Climbing 算法将会使遗传算法更加有效。文[10]在文[8]的基础上,对 Hill Climbing 算法进行了改进,它可以同时改善S盒的非线性度和差分均匀性。文[11]给出了一种演化策略,在这种策略下,利用基因算法可以有效生成高非线性度和低差分均匀性的S盒。

上述 Hill Climbing 算法都是考虑交换布尔函数的两个输出的情况,当算法迭代到一定程度后,交换任何两个输出都不会使非线性度提高,即达到了局部最优值。这时可以考虑三个输出的情况,将输出按逆时针或顺时针改变一下次序,可能会再次提高非线性度。本文研究了顺时针方向改变S盒的三个输出向量会提高非线性度所应呈现的谱特征。在此基础上,对文[8]的 Hill Climbing 算法进行了改进,它可以使S盒的非线性度在交换两个输出向量达到局部最优值后,通过改变三个输出向量的次序进一步提高非线性度,从而更加接近全局最优值。因为双射S盒被目前大多数分组密码算法所采用,本文和文[8]一样,将双射S盒作为研究对象。

1 基本概念与定理

定义 1.1 设 $f(x): F_2^n \to F_2$ 是 n 元布尔函数。称 $\hat{F}(w)$ 是 $f(x)$ 的 walsh-Halsh-Hadamard 变换(WHT),是指:

$$\hat{F}(w) = \sum (-1)^{f(x) \oplus L_w(x)}$$

其中 $L_w(x) = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus \omega_n x_n$, $w = (w_1, w_2, \cdots, w_n) \in F_2^n$。

定义 1.2 n元布尔函数的非线性度 $N_f = \min_{l \in L_n} d_H(f, l)$, $l \in L_n$,其中 L_n 表示全体 n 元线性和仿射函数之集,$d_H(f, l)$ 表示 f 与 l 之间的汉明距离。

*)基金项目:国家自然科学基金重大研究计划项目(90304007);国家自然科学基金资助项目(60373047);863 高科技发展计划(2001AA141010)。陈 华 博士生,主要研究方向为密码学与信息安全;吴文玲 研究员,主要研究方向为密码学;冯登国 研究员,博导,主要研究方向为密码学与信息安全。

若 WH_{max} 表示为 $\hat{F}(\omega)$ 的最大绝对值，则 $N_f=\frac{1}{2}(2^n-WH_{max})$，因此，通过降低 WH_{max}，就可以增加布尔函数的非线性度。文[7]就是采用这种方法来提高布尔函数的非线性度的。S盒的非线性度可以用类似的方法得到提高。

定义 1.3 令 $S(x)=(f_1(x),\cdots,f_m(x)):F_2^n\to F_2^m$ 是一个多输出函数，称 $N_s=\min d_H(u\cdot S(x),l(x))$ 为 $S(x)$ 的非线性度，其中，$l\in L_n$，$0\neq u\in F_2^m$，它等于S盒的各输出位的任意非零线性组合所形成的布尔函数与 l 之间的最小汉明距离。

如果对于每个非零线性组合所形成的布尔函数都进行Walsh-Hadamard变换。则可形成 WHT 矩阵，其中矩阵元素可表示为 $\hat{B}_\theta(\tilde{\omega})=\sum_x L_\theta(y)\cdot L_{\tilde{\omega}}(x)$，在这里，也用 WH_{max} 表示 $\hat{B}_\theta(\tilde{\omega})$ 的最大绝对值，因此，$N_s=\frac{1}{2}(2^n-WH_{max})$

显然，降低 WH_{max} 可以提高S盒的非线性度。我们定义如下集合：

$W_1^+=\{(\tilde{\omega},\theta):\hat{B}(\tilde{\omega},\theta)=WH_{max}\}$，

$W_1^-=\{(\tilde{\omega},\theta):\hat{B}(\tilde{\omega},\theta)=-WH_{max}\}$

$W_2^+=\{(\tilde{\omega},\theta):\hat{B}(\tilde{\omega},\theta)=WH_{max}-2\}$，

$W_2^-=\{(\tilde{\omega},\theta):\hat{B}(\tilde{\omega},\theta)=-WH_{max}+2\}$

$W_3^+=\{(\tilde{\omega},\theta):\hat{B}(\tilde{\omega},\theta)=WH_{max}-4\}$，

$W_3^-=\{(\tilde{\omega},\theta):\hat{B}(\tilde{\omega},\theta)=-WH_{max}+4\}$

$W_4^+=\{(\tilde{\omega},\theta):\hat{B}(\tilde{\omega},\theta)=WH_{max}-6\}$，

$W_4^-=\{(\tilde{\omega},\theta):\hat{B}(\tilde{\omega},\theta)=-WH_{max}+6\}$

定理 1.1[8] 设 $b(x)=y$ 是一个双射S盒，x_1 和 x_2 是两个不同的输入，并且 $y_1=b(x_1)$，$y_2=b(x_2)$，令 $b'(x)$ 是 $b(x)$ 交换 y_1 和 y_2 后得到的 S 盒。若 x_1 和 x_2 满足以下条件，则 $b'(x)$ 的 WH_{max} 就会降低。

a) $L_{\tilde{\omega}}(x_1)\neq L_{\tilde{\omega}}(x_2)$，对于所有的 $(\tilde{\omega},\theta)\in W_1^+\cup W_1^-$

b) $L_\theta(y_1)\neq L_{\tilde{\omega}}(x_2)$，$L_{\tilde{\omega}}(y_2)\neq L_{\tilde{\omega}}(x_1)$，对于所有的 $(\tilde{\omega},\theta)\in W_1^+$

c) $L_\theta(y_1)=L_{\tilde{\omega}}(x_2)$，$L_{\tilde{\omega}}(y_2)=L_{\tilde{\omega}}(x_1)$，对于所有的 $(\tilde{\omega},\theta)\in W_1^-$

d) 对于所有 $(\tilde{\omega},\theta)\in W_{2,3}^+$，下列式子不全为真：

$L_\theta(y_1)=L_{\tilde{\omega}}(x_2)$，$L_{\tilde{\omega}}(y_2)=L_{\tilde{\omega}}(x_1)$，

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_2)$

e)对于所有 $(\tilde{\omega},\theta)\in W_{2,3}^-$，下列式子不全为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_2)$，$L_{\tilde{\omega}}(y_2)\neq L_{\tilde{\omega}}(x_1)$，

$L_\theta(y_1)=L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)=L_{\tilde{\omega}}(x_2)$。

2 MHC算法

在定理2.1中，若 $b(x)$ 的任何两个不同输入 x_1 和 x_2 都不满足定理要求的条件，则意味着交换任意两个输出都不能提高 $b(x)$ 的非线性度，这时利用 Hill Climbing 算法不能再提高 $b(x)$ 的非线性度了。如果想在此基础上进一步地提高非线性度，可以考虑同时改变三个互不相同的输出向量次序而保持其它输出向量不变的情况。若 x_1，x_2 和 x_3 是三个互不相同的输入，并且，$y_1=b(x_1)$，$y_2=b(x_2)$，$y_3=b(x_3)$，若仅考虑改变 y_1，y_2 和 y_3 的值，则有两种可能，一种是顺时针方向变换 y_1，y_2 和 y_3 的位置，一种是逆时针方向变换 y_1，y_2 和 y_3 的位置。限于篇幅，本文只研究第一种情况。

令 $b'(x)$ 满足 $b'(x_1)=y_2$，$b'(x_2)=y_3$，$b'(x_3)=y_1$，并且对于 $x\neq x_1,x_2,x_3$，$b'(x)=b(x)$。如果要想 $b'(x)$ 的非线性度大于 $b(x)$，必须令 $b'(x)$ 的 WH'_{max} 小于 $b(x)$ 的 WH_{max}。这时对于每一个 $(\tilde{\omega},\theta)$，$\hat{B}'_\theta(\tilde{\omega})$ 的绝对值应该都小于 WH_{max}。因为 $\Delta\hat{B}_\theta(\tilde{\omega})=\hat{B}_\theta(\tilde{\omega})-\hat{B}'_\theta(\tilde{\omega})=L_0(y',)L_{\tilde{\omega}}(x_1)+L_\theta(y'_2,)L_{\tilde{\omega}}(x_2)+L_\theta(y'_3)L_{\tilde{\omega}}(x_3)-L_\theta(y_1)L_{\tilde{\omega}}(x_1)-L_\theta(y_2)L_{\tilde{\omega}}(x_2)-L_\theta(y_3)L_{\tilde{\omega}}(x_3)$

所以 $\Delta\hat{B}_\theta(\tilde{\omega})$ 的绝对值不大于6。不难证明对于 $(\tilde{\omega},\theta)\in\{(\tilde{\omega},\theta)\,|\,|\hat{B}_\theta(\tilde{\omega})|<WH_{max}-6\}$，$|\hat{B}'_\theta(\tilde{\omega})|<WH_{max}|<WH_{max}$，因此只需考虑对于 $(\tilde{\omega},\theta)\in\{(\tilde{\omega},\theta)\,|\,|\hat{B}_\theta(\tilde{\omega})|\geq WH_{max}-6\}$，$|\hat{B}'_\theta(\tilde{\omega})|<WH_{max}$ 成立需要满足的条件。定理3.1给出了我们的研究结论：

定理 3.1 设 $b(x)=y$ 是一个双射S盒，x_1，x_2 和 x_3 是三个互不相同的输入，并且，$y_1=b(x_1)$，$y_2=b(x_2)$，$y_3=b(x_3)$，，令 $b'(x)$ 满足 $b'(x_1)=y_2$，$b'(x_2)=y_3$，$b'(x_3)=y_1$，并且对于 $x\neq x_1,x_2,x_3$，$b'(x)=b(x)$。若 x_1，x_2 和 x_3 满足以下条件，则 $b'(x)$ 的 WH_{max} 就会降低。

1)对于所有的 $(\tilde{\omega},\theta)\in W_1^+$，条件 a)，b)至少一个成立：

a) $L_\theta(y_1)\neq L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$，并且下列式子不全为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_3)$

b)下列式子至少要有两项为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)\neq l_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$

并且下列式子也至少要有两项为真：

$L_\theta(y_1)=L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)=L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)=L_{\tilde{\omega}}(x_3)$

2)对于所有的 $(\tilde{\omega},\theta)\in W_1^-$，条件 a)，b)至少一个成立：

a)下列式子不全为真

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$

并且

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_3)$

b)下列式子至少要有两项为真：

$L_\theta(y_1)=L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)=L_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)=L_{\tilde{\omega}}(x_2)$

并且下列式子也至少要有两项为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_3)$

3)对于所有的 $(\tilde{\omega},\theta)\in W_2^+$，条件 a)，b)，c)至少一个成立：

a) $L_\theta(y_1)\neq L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$

b)下列式子至少要有两项为真：

$L_\theta(y_1)=L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)=L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)=L_{\tilde{\omega}}(x_3)$

c)下列式子至少要有两项为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$

并且下列式子不全为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_3)$

4)对于所有的 $(\tilde{\omega},\theta)\in W_2^-$，条件 a)，b)，c) 至少一个成立：

a)下列式子至少要有两项为真：

$L_\theta(y_1)=L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)=L_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)=L_{\tilde{\omega}}(x_2)$

b) $L_\theta(y_1)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_3)$

c)下列式子不全为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$

并且下列式子至少要有两项为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_3)$

5)对于所有的 $(\tilde{\omega},\theta)\in W_3^+$，条件 a)，b)至少一个成立：

a)下列式子至少要有两项为真：

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_3)$，$L_\theta(y_2)\neq L_{\tilde{\omega}}(x_1)$，$L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$

b)下列式子至少要有两项为真：

$L_\theta(y_1)=L_{\tilde{\omega}}(x_1)$，$L_\theta(y_2)=L_{\tilde{\omega}}(x_2)$，$L_\theta(y_3)=L_{\tilde{\omega}}(x_3)$

对于所有的 $(\tilde{\omega},\theta)\in W_3^-$，$x_1$，$x_2$ 和 x_3 要满足的条件和 $(\tilde{\omega},\theta)\in W_3^+$ 相似，所不同的是将符号取反。

6)对于所有的 $(\tilde{\omega},\theta)\in W_4^+$，下列式子不全为真：

$L_\theta(y_1)=L_{\tilde{\omega}}(x_1), L_\theta(y_2)=L_{\tilde{\omega}}(x_2), L_\theta(y_3)=L_{\tilde{\omega}}(x_3)$

$L_\theta(y_1)\neq L_{\tilde{\omega}}(x_1), L_\theta(y_2)\neq L_{\tilde{\omega}}(x_2), L_\theta(y_3)\neq L_{\tilde{\omega}}(x_3)$

对于所有的$(\tilde{\omega},\theta)\in W_4^-$，$x_1,x_2$ 和 x_3 要满足的条件和$(\tilde{\omega},\theta)\in W_4^+$ 相似，所不同的是将符号取反。

证明：对于 $b(x)=y, \hat{B}_\theta(\tilde{\omega})=\sum_x L_\theta(y)\cdot L_{\tilde{\omega}}(x)$，相应地，对于 $b'(x)=y', \hat{B}'_\theta(\tilde{\omega})=\sum_x L_\theta(y')\cdot L_{\tilde{\omega}}(x), \Delta\hat{B}_\theta(\tilde{\omega})=\hat{B}_\theta(\tilde{\omega})-\hat{B}_\theta(\tilde{\omega})$。因为 $\hat{B}_\theta(\tilde{\omega})$ 和 $\hat{B}'_\theta(\tilde{\omega})$ 仅在涉及 x_1,x_2,x_3 的项是不同的，所以：

$$\begin{aligned}\Delta\hat{B}_\theta(\tilde{\omega})=&L_\theta(y')L_{\tilde{\omega}}(x_1)+L_\theta(y'_2)L_{\tilde{\omega}}(x_2)+L_\theta(y'_3)L_{\tilde{\omega}}(x_3)-L_\theta(y_1)L_{\tilde{\omega}}(x_1)-L_\theta(y_2)L_{\tilde{\omega}}(x_2)-L_\theta(y_3)L_{\tilde{\omega}}(x_3)\\=&L_\theta(y_2)L_{\tilde{\omega}}(x_1)+L_\theta(y_3)L_{\tilde{\omega}}(x_2)+L_\theta(y_1)L_{\tilde{\omega}}(x_3)-L_\theta(y_1)L_{\tilde{\omega}}(x_1)-L_\theta(y_2)L_{\tilde{\omega}}(x_2)-L_\theta(y_3)L_{\tilde{\omega}}(x_3)\end{aligned}$$

令 $\Delta_1=L_\theta(y_2)L_{\tilde{\omega}}(x_1)+L_\theta(y_3)L_{\tilde{\omega}}(x_2)+L_\theta(y_1)L_{\tilde{\omega}}(x_3)$

$\Delta_2=-L_\theta(y_1)L_{\tilde{\omega}}(x_1)-L_\theta(y_2)L_{\tilde{\omega}}(x_2)-L_\theta(y_3)L_{\tilde{\omega}}(x_3)$

不难得知，$\Delta_1\in\{-3,-1,1,3\}$，$\Delta_2\in\{-3,-1,1,3\}$，$\Delta=\Delta_1+\Delta_2\in\{-6,-4,-2,0,2,4,6\}$

对于$(\tilde{\omega},\theta)\in W_1^+$，只有当 $\Delta\in\{-6,-4,-2\}$ 时，$\hat{B}_\theta(\tilde{\omega})$ 的绝对值才会降低。这时 Δ_1 和 Δ_2 的取值组合可以是$(-3,-1),(-3,-3),(-3,1),(-1,-3),(-1,-1),(+1,-3)$中的一种。其中组合$(+1,-3)$是不存在的，因为当 $\Delta_1=1$ 时，$L_\theta(y_1)=L_{\tilde{\omega}}(x_3), L_\theta(y_2)=L_{\tilde{\omega}}(x_1), L_\theta(y_3)=L_{\tilde{\omega}}(x_2)$ 中有两个等式成立，不妨假设 $L_\theta(y_1)=L_{\tilde{\omega}}(x_3), L_\theta(y_2)=L_{\tilde{\omega}}(x_1), L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$，当 $\Delta_2=-3$ 时，$L_\theta(y_1)=L_{\tilde{\omega}}(x_1), L_\theta(y_2)=L_{\tilde{\omega}}(x_2), L_\theta(y_3)=L_{\tilde{\omega}}(x_3)$，可以推出 $L_\theta(y_3)=L_{\tilde{\omega}}(x_2)$，这与 $L_\theta(y_3)\neq L_{\tilde{\omega}}(x_2)$ 相矛盾。因此 Δ_1 和 Δ_2 的取值等价于$(\Delta\neq-3,\Delta_2=3)$或$(\Delta_1>0,\Delta_2>0)$，它等价于条件(2)。

同理，对于所有的$(\tilde{\omega},\theta)\in W_1^-$，只有当 $\Delta\in\{6,4,2\}$ 时，$\hat{B}_\theta(\tilde{\omega})$ 的绝对值才会降低。这时 Δ_1 和 Δ_2 的取值组合可以是$(-1,+3),(+1,+1),(+1,+3),(+3,-1),(+3,+1),(+3,+3)$中的一种。其中$(+3,-1)$是不存在的，因为当 $\Delta_1=3$ 时，$L_\theta(y_1)=L_{\tilde{\omega}}(x_3), L_\theta(y_2)=L_{\tilde{\omega}}(x_1), L_\theta(y_3)=L_{\tilde{\omega}}(x_2)$，当 $\Delta_2=-1$ 时，$L_\theta(y_1)=L_{\tilde{\omega}}(x_1), L_\theta(y_2)=L_{\tilde{\omega}}(x_2), L_\theta(y_3)=L_{\tilde{\omega}}(x_3)$ 只有一个不成立，不妨假设为 $L_\theta(y_3)\neq L_{\tilde{\omega}}(x_3)$，但通过剩余的五个等式可以推出 $L_\theta(y_3)=L_{\tilde{\omega}}(x_2)$，得出矛盾。因此 Δ_1 和 Δ_2 的取值等价于$(\Delta_1=-3,\Delta_2\neq3)$或$(\Delta_1<0,\Delta_2<0)$，它等价于条件(1)。

对于所有的$(\tilde{\omega},\theta)\in W_2^+$，只有当 $\Delta\in\{-6,-4,-2,0\}$ 时，$\hat{B}_\theta(\tilde{\omega})$ 的绝对值才会降低。这时 Δ_1 和 Δ_2 的取值组合可以是$(-3,-1),(-3,-3),(-3,1),(-3,+3),(-1,-3),(-1,-1),(-1,+1),(+1,-1)$中的一种，它也可写成$(\Delta_1=-3)$或$(\Delta_2<0)$或$(\Delta_1<0,\Delta_2\neq3)$，等价于条件(3)。

对于所有的$(\tilde{\omega},\theta)\in W_2^-$，只有当 $\Delta\in\{6,4,2,0\}$ 时，$\hat{B}_\theta(\tilde{\omega})$ 的绝对值才会降低。这时 Δ_1 和 Δ_2 的取值组合可以是$(-3,+3),(-1,+1),(-1,+3),(+1,-1),(+1,+1),(+1,+3),(+3,-3),(+3,+1),(+3,+3)$中的一种，它也可写成$(\Delta_1>0)$或$(\Delta_2=3)$或$(\Delta_1\neq-3,\Delta_2>0)$，等价于条件(4)。

对于所有的$(\tilde{\omega},\theta)\in W_3^+$，只有当 $\Delta\in\{-6,-4,-2,0,2\}$ 时，$\hat{B}_\theta(\tilde{\omega})$ 的绝对值才会降低，因此 $\Delta\notin\{6,4\}$。不难证明，$\Delta=\{6,4\}$ 等价于 Δ_1 和 Δ_2 的取值组合为$(1,3),(3,3),(3,1)$，这时 $\Delta_1>0$ 并且 $\Delta_2>0$。因此 $\Delta\notin\{6,4\}$ 等价于 $\Delta_1<0$ 或 $\Delta_2<0$，它等价于条件(5)。类似可以证明，对于所有的$(\tilde{\omega},\theta)\in W_3^-$，$\Delta_1>0$ 或 $\Delta_2>0$，它相当于将条件(5)的符号取反。

对于所有的$(\tilde{\omega},\theta)\in W_4^+$，只有当 $\Delta\neq6$ 时，$\hat{B}_\theta(\tilde{\omega})$ 的绝对值才会降低，因此 $\Delta_1\neq3$ 或 $\Delta_2\neq3$，它等价于条件(6)。类似可以证明，对于所有的$(\tilde{\omega},\theta)\in W_4^-$，$\Delta_1\neq-3$ 或 $\Delta_2\neq-3$，它相当于将条件(6)的符号取反。证明完毕。

上述定理指出了提高 S 盒非线性度的充分条件，在此基础上，我们对文[8]提出的 Hill Climbing 算法进行了改进。为了简便起见，称文[8]的算法为 HC 算法，本文算法为 MHC 算法。以下是 MHC 算法的具体流程：

MHC(Sbox, WHT)

第一步：计算 WH_{max} 和集合 $W_1^+, W_1^-, W_2^+, W_2^-, W_3^+, W_3^-, W_4^+, W_4^-$；

第二步：对于 S 盒的每一个输入对(x_1,x_2)，检查(x_1,x_2)是否满足定理 1.1 的条件，若满足则交换(x_1,x_2)的输出得到一个新 S 盒，重新计算 WHT，跳到第一步；否则挑选一个新的输入对进行检查直到没有输入对满足条件；

第三步：对于 S 盒的每一个输入三元组$(x_1,x_2,x_3)$$(x_1,x_2,x_3$ 互不相同)，检查(x_1,x_2,x_3)是否满足定理 2.1，若满足则按照定理 2.1 将(x_1,x_2,x_3)的输出重新排序，并重新计算 S 盒的 WHT 矩阵，WH_{max} 和 $W_1^+, W_1^-, W_2^+, W_2^-, W_3^+, W_3^-, W_4^+, W_4^-$，否则再找一个输入三元组进行检查直到没有三元组满足条件；

第四步：输出当前的 S 盒。

4 实验结果

我们随机生成了 10000 个双射 S 盒来进行了实验，实验结果表明 MHC 算法比 HC 算法能更加有效地提高双射 S 盒的非线性度。

图 1 给出了这 10000 个 S 盒的初始非线性度分布和使用改进的 HC、MHC 算法后优化非线性度的分布。通过曲线分布可以看出 MHC 算法对初始 S 盒的优化效果明显大于 HC 算法。初始 S 盒的非线性度主要分布在 90、92、94、96，它们的比例分别是 12.27%、32.07%、38.88%、11.05%。经 HC 算法优化后的 S 盒的非线性度主要集中在 96 和 98，其比例分别为 52.59%和 45.02%。而经过 MHC 算法优化后的 S 盒的非线性度大都集中在 98，比例为 92.77%。

表 1、表 2 分别记录了 HC 算法和 MHC 算法对初始 S 盒的详细优化情况。不难看出，表 2 的每一行的优化结果都好于表 1。这与 MHC 算法的过程是相符的，因为它实质上是在 HC 算法基础上对 S 盒的进一步优化。

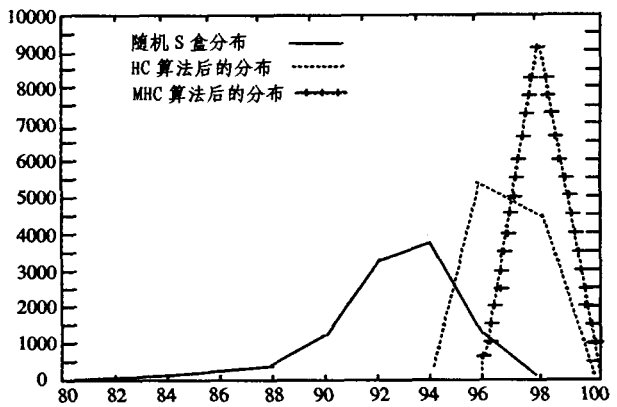

图 1 非线性度分布图

(下转第 86 页)

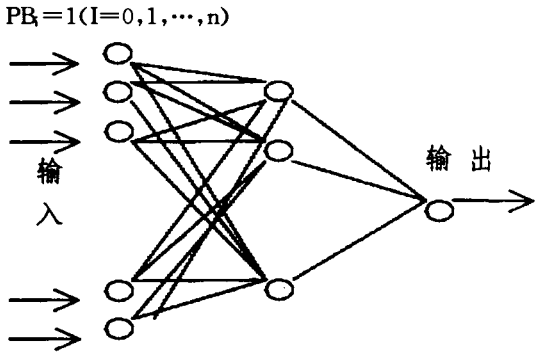

图 3 神经网络结构图

由审计事件计算得到 PA_i 与 PB_i 的值。将 PA_i 与 PB_i 进行权重计算得到 PE 的概率值。

本文中审计事项 E 是指客户端的可信度，将所有客户端的请求按照 PE 值的大小进行排序，改变服务器应答客户端的先后顺序。

(4)当代理收到客户端的"第三次握手"协议之后，结合其对客户端可信度的排序，受理客户端的请求，代理向服务器端发出连接中断请求，客户端和服务器端开始传输数据。

4.3 可行性论证

该方法有助于改善系统防范 SYN-Flooding 攻击的能力，它具有以下方面的品质。

(1)具有分布式均衡的能力。由于代理与服务器分别管理不同的服务，代理处理"第三次握手"协议，而服务器处理"第一、二次握手"协议，相当于增加了系统的处理器。

(2)适当缩小了 SYN-Timeout 值。由于代理将客户端的服务请求按照一定的原则进行了排序和优化，事实上缩短了 SYN-Timeout 时间，有助于加快网络的传输。

(3)利用了防火墙 QoS 的优点。其一，代理设计在防火墙内，没有暴露在客户端面前，增加了其安全性。其二，服务器端不存在大量消耗系统资源的中断申请，即客户端的连接响应由代理服务器按照时间统计概率 PE 值判断后排序提交。

4.4 前景

目前在 IPV4 的技术条件下，针对分布式入侵检测的方法很多，但是都没有一个完整的解决方案，特别是无法防御系列和重复攻击。随着 IPV6 技术的推广，使用该方法解决此问题将更加有效。

IPv6 具有实名认证机制。IP 地址与用户身份的一一对应性，使非法占用 IP 资源作为攻击其他计算机的平台的可能性大大降低，即没有大量的攻击资源的出现。进行 SYN-Flooding 攻击时，攻击者不能构造虚假的 IP 地址，换言之，IP 地址是真实而有效的。代理对于客户端的可信度排序的准确性，使从根本上解决 SYN-Flooding 攻击成为可能。

结束语 随着 Internet 的发展，最常见的拒绝服务攻击将是网络安全的一大劲敌，特别是 SYN-Flooding 攻击。根据实验验证，该方法是一种有效而经济的 SYN-Flooding 攻击防御方法。

参 考 文 献

1 叶芳，吴中福，刘永国．网络入侵的聚类算法研究与实现．重庆大学学报，2004，27(3)
2 Lee W, Stolfo S J, Mok K W. Mining audit data to build intrusion detection models. In: Proc. of the 4th Intl. Conf. 174 on Knowledge Discovery and Data Mining , New York, NY, AAAI Press, Aug. 1998
3 (美)Richard Stevens W.《TCP/IP 详解》卷一：协议[M]. 北京：机械工业出版社，2000
4 http://www. nsfocus. com/
4 http://www. xfocus. net/
5 Allen J, Christie A, et al. state of the pratice of Intrusion Detection Technologies, CMU/SEI, 2000. 6
6 方勇，龚海澎，胡勇，欧晓聪. 一种针对 SYN-Flooding 攻击的防范对策. 四川大学学报，2004(1)

(上接第 70 页)

表 1 HC 算法对初始 S 盒非线性度的改善情况

初始非线性度	改善后的非线性度					
	90	92	94	96	98	100
80	0	0	0	1	0	0
82	0	0	0	7	0	0
84	0	0	3	19	12	0
86	0	2	9	61	36	0
88	0	1	15	262	129	0
90	0	5	60	767	395	0
92	0	3	110	1966	1128	0
94	0	0	29	1922	1936	1
96	0	0	0	254	850	1
98	0	0	0	16	0	0

表 2 MHC 算法对初始 S 盒非线性度的改善情况

初始非线性度	改善后的非线性度					
	90	92	94	96	98	100
80	0	0	0	0	1	0
82	0	0	0	1	6	0
84	0	0	0	4	28	2
86	0	0	0	9	98	1
88	0	0	0	48	353	6
90	0	0	0	97	1123	7
92	0	0	0	222	2939	46
94	0	0	0	124	3682	82
96	0	0	0	6	1033	66
98	0	0	0	0	14	2

结束语 本文通过对双射 S 盒的 Walsh 谱的研究，给出了一个提高 S 盒非线性度的充分条件，并提出了 MHC 算法。与文[8]的 Hill Climbing 算法相比，它能更加有效地提高 S 盒的非线性度。同时，对 10000 个随机生成的双射 S 盒进行了实验，实验结果也证明了 MHC 算法对随机 S 盒非线性度的优化效果明显高于 Hill Climbing 算法。

本文的工作也可以和基因算法结合起来，演化地生成密码性能强的 S 盒。

参 考 文 献

1 Data Encryption Standard. FIPS PUB 46, National Tech. Infor. Service. VA, 1977
2 Daemen J, Rijmen V. The design of Rijndael: AES - The Advanced Encryption Standard. Springer, 2002
3 Rijmen V, Daemen J, Preneel B, et al. The cipher SHARK. Fast Software Encrytion, 1996. 99～111
4 Daemen J, Knudsen L R, Rijmen V. The Block Ciphe Squarer. Fast Software Encrytion, 1997. 149～165
5 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. 67～69
6 Anderson B J, Biham E, Knudsen L R. The Case for Serpent. In: AES Candidate Conf. 2000. 349～354
7 Millan W, Clark A, Dawson E. Smart Hill Climbing Finds Better Boolean Functions. In: Workshop on Selected Areas in Cryptology 1997, Works hop Record, 1997. 50～63
8 Millan W. How to Improve the Nonlinearity of Bijective S-boxes. ACISP '98, Berlin: Springer-Verlag, LNCS vol. 1438, 1998. 181～192
9 Millan W, Burnett L, Carter G, et al. Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes. ICICS' 99, Berlin: Springer-Verlag, LNCS vol. 1726, 1999. 263～274
10 陈华，冯登国，吴文玲. 一种改善双射 S 盒密码特性的有效算法. 计算机研究与发展，已录用
11 Chen H, Feng Deng-guo. An Effective Evolutionary Stategy for Bijective S-boxes. IEEE Congress on Evolutionary Computation, Accepted, 2004