第 34 卷 第 20 期 计 算 机 工 程 2008 年 10 月
Vol.34 No.20 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)20—0193—03 文献标识码：A 中图分类号：TP309

S 盒抗 DPA 能力与非线性度的关系

刘连浩[1]，沈增晖[1]，刘上力[1,2]，段绍华[1]
(1. 中南大学信息科学与工程学院，长沙 410083；2. 湖南科技大学计算机科学与工程学院，湘潭 411201)

摘 要：S 盒作为高级加密标准(AES)中的唯一非线性部件，是影响算法性能的重要因素之一，在研究其性质的基础上，将透明阶作为衡量密码系统抗差分功耗分析(DPA)能力的一个指标，推导出高非线性函数透明阶的下界计算公式。实验结果表明，该算法是有效的，在类似 AES 的分组密码中，S 盒非线性度与密码抗 DPA 能力成反比关系。

关键词：透明阶；非线性度；分组密码；差分功耗分析；高级加密标准

Relationship Between S-box's Resistance to DPA and Nonlinearity

LIU Lian-hao[1], SHEN Zeng-hui[1], LIU Shang-li[1,2], DUAN Shao-hua[1]
(1. School of Information Science and Engineering, Central South University, Changsha 410083;
2. College of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201)

【Abstract】S box, which is the only nonlinear component involved in Advanced Encryption Standard(AES), is one of the important ingredients that affect the algorithmic performance. Based on the research on its property, this paper uses the conception of transparency order as the target to measure the resistance to Differential Power Analysis(DPA), and educes a formula to calculate the lower boundary of transparency order of high-nonlinear function. Experimental results show that, the algorithm is effective, and the degree of the S box's nonlinearity inverses the resistance to DPA in the similar grouping cipher AES.

【Key words】 transparency order; nonlinearity; block cipher; Differential Power Analysis(DPA); Advanced Encryption Standard(AES)

1 概述

2000 年 10 月 2 日，Vincent Rijmen和Joan Daemen设计了AES的最终算法——Rijndael算法。1998 年，Paul Kocher等人[1]提出密码攻击方法——功耗分析(Power Analysis, PA)方法，该方法利用加密硬件系统运行时功耗的泄漏，进行统计、分析，并恢复出密钥。

一般地，可将功耗分析分为两类：

(1)简单功耗分析(Simple Power Analysis, SPA)；

(2)差分功耗分析(Differential Power Analysis, DPA)[2]。

类似 AES 的分组算法中的 S 盒是其唯一的非线性部件，它被用来设计防范线性分析和差分分析，DPA 这类统计学攻击方法对非线性函数的攻击效果却很好，因此，研究 S 盒抗 DPA 能力与非线性度之间的关系，可以设计出一种 S 盒或者给出一个 S 盒参考判别准则，使其同时具有抗差分功耗分析、线性分析和差分分析的能力。

文献[3]引入透明阶的概念，将其作为 S 盒抗功耗分析能力的衡量指标。本文根据透明阶下界计算公式，得出精确的 S 盒透明阶下限结果。S 盒函数非线性度越高，系统抗差分功耗分析的能力就越弱。

2 DPA 与 S 盒非线性度关系

与简单功耗分析相比，差分功耗分析更加有效，攻击者不需要知道算法实现的有关细节。DPA 通过采集加密设备所泄漏的边带信道信息，使用统计手段来恢复密钥。

在文献[4]中，当执行DPA攻击时，首先应该选择N组随机数据作为输入的明文，然后搜集明文分组X_i功耗信号即功耗采样信号$S_{i,j}$和对应的密文输出。功耗采样信号即加密过程中所泄漏的可被攻击的边带信道信息，X_i表示第i组明文；j表示采样时间。

构造功耗选择函数为

$D(X_i,K_t)_b$

其中，K_t表示猜测密钥；b表示位数。

应用 $D(\cdot)$函数将得到的 N 条采样功耗曲线分为如下 2 个集合：

$$T_0=\{S_{i,j}\mid D(\bullet)=0\}$$

$$T_1=\{S_{i,j}\mid D(\bullet)=1\}$$

下一步就是计算每个功耗信号集合的均值：

$$A_{0,j}=\frac{1}{|S_0|}\sum_{S_{i,j}\in S_0}S_{i,j}$$

$$A_{1,j}=\frac{1}{|S_1|}\sum_{S_{i,j}\in S_1}S_{i,j}$$

此时 $|S_0|+|S_1|=N$，然后计算 $A_{0,j}$ 和 $A_{1,j}$ 两个集合均值的差 $\Delta T_{K_t}[b]=A_{0,j}-A_{1,j}$，根据 ΔT_{K_t} 的大小变化趋势，向上判断，并猜测密钥是否正确：

(1)如果密钥猜测正确，在差分功耗曲线图上会出现明显的峰值；

(2)否则，峰值不明显。

作者简介：刘连浩(1959－)，男，教授、博士，主研方向：信息安全与密码学；沈增晖，硕士研究生；刘上力，工程师、硕士研究生；段绍华，硕士研究生

收稿日期：2007-12-25 **E-mail：**yixuehuishen@163.com

1 阶 DPA 的数学模型为

$$\Delta T_{K_t}[b]=\frac{\sum_{i\in[1,N]} S_i D(X_i,K_t)_b}{\sum_{i\in[1,N]} D(X_i,K_t)_b}-\frac{\sum_{i\in[1,N]} S_i\left(1-D(X_i,K_t)_b\right)}{\sum_{i\in[1,N]}\left(1-D(X_i,K_t)_b\right)} \tag{1}$$

2.1 S 盒相关知识

设一个(n,p)元函数为

$$F: GF\left(2^n\right)\to GF\left(2^p\right)$$

其中，n 元布尔函数为

$F=(f_1,f_2,\cdots,f_p)$的 $f_i: GF\left(2^n\right)\to GF(2)$

在分组密码中，S 盒用到的布尔函数 F 一般是 $n=p$。

定义 1[5] 对于每一个n元布尔函数f，Walsh谱变换为

$$S_{(f)}(w)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f(x)+wx}$$

定义 2 已知$F=(f_1,f_2,\cdots,f_p)$是 $GF(2^n)\sim GF(2^p)$ 的多输出布尔函数，若 $\varepsilon\in GF(2^n)$，满足 $F(x)+F(x+\varepsilon)=$ 常量，则函数F的线性结构为

$$D_\varepsilon F=F(x)+F(x+\varepsilon)$$

定义 3[5] 对于任何一个n元布尔函数f，它的非线性度为

$$N_f=2^{n-1}\left(1-\mathrm{MAX}\,|\,S_{(f)}(w)\,|\right)$$

其中，$w\in GF(2^n)$。

当一个 n 元布尔函数的非线性度等于 $N_f=2^{n-1}-2^{n/2-1}$ 时，即 $2^{8-1}-2^{8/2-1}=120$，它被称为 bent 函数也就是完全非线性函数。作为衡量密码算法抵抗线性分析能力大小的指标，S 盒函数非线性度越接近于 120，它抵抗线性分析的能力就越强，但当其非线性度达到最高时，其他性能将变弱。

AES的S盒非线性度为 112，其非线性度已经非常接近完全非线性函数的非线性度 120，但是该函数并不是完全非线性函数，它是一种几乎完全非线性函数(Almost Perfect Nonlinear, APN)[6]。

定义 4 给定一个布尔函数 F，其中 $\mu,\nu\in F_2^n$，$F(x)$ 的差分均匀度为

$$\delta_F(\mu,\nu)=\max_{\mu\in F_2^n-\{0\}}\max_{\nu\in F_2^n}|\{x\in F_2^n : F(x)+F(x+\mu)=\nu\}|$$

文献[5]指出，差分均匀度是用来衡量算法抵抗差分攻击能力的指标。从这个意义上来说，S 盒函数差分均匀度越接近最小值 1，抵抗差分分析的能力就越强。计算表明 AES 的 S 盒差分均匀度是 4，具有一定的抗差分分析的能力。

2.2 S 盒抗 DPA 能力指标

在差分功耗分析中，功耗均值差 ΔT_{K_t} 可以描述密码系统抗DPA攻击的能力。在文献[3]中，Prouff把分组密码S盒的这个新性质称作透明阶τ_F，该参数可表示为

$$\tau_F=\max_{\rho\in F_2^n}\left(|n-2H(\rho)|-\frac{1}{2^{2n}-2^n}\sum_{\varepsilon\in F_2^n-\{0\}}\Big|\sum_{i\in[1,n]}2^n(-1)^{\rho_i}S_{(D_\varepsilon f_i)}(0)\Big|\right) \tag{2}$$

其中，$\rho\in GF(2^n)$ 表示加密系统所使用S盒的非线性函数输出的状态字节；$H(\rho)$ 表示 ρ 的汉明重量。透明阶的大小满足关系：$0\le\tau_F\le n$，即如果函数F的每个布尔函数 f_i 都是bent函数，则τ_F的值为n，如果函数F的每个布尔函数 f_i 均为仿射函数，则τ_F的值为 0。τ_F值的大小反映了密码系统防范差分功耗分析能力的高低，可以看出，τ_F的值越小，密码系统防范能力就越强，反之就越弱。

定理 1 设$F=(f_1,f_2,\cdots,f_p)$是一个$(n,\ p)$元布尔函数，对于任意的 $i=1,2,\cdots,n$，每一个函数 $f_i: GF(2^n)\to GF(2)$ 都是n元布尔函数。则

$$\tau_F\ge n-\frac{1}{\sqrt{2^n-1}}\sqrt{\sum_{\varepsilon\in F_2^n-\{0\}}\sum_{i\in[1,n]}\left(S_{D_\varepsilon f_i}(0)\right)^2+2\sum_{\varepsilon\in F_2^n-\{0\}}\sum_{i,j\in[1,n]}S_{D_\varepsilon f_i}(0)S_{D_\varepsilon f_j}(0)} \tag{3}$$

证明

由 $\rho\in GF(2^n)$ 可得 $H(\rho)\in[0,n]$，当 $H(\rho)=0$ 或 $H(\rho)=n$ 时，有 $\mathrm{MAX}\,|\,n-2H(\rho)\,|\ =\ n$。

已知 τ_F 的定义如式(2)所示，根据柯西不等式可得：

$$\sum_{\varepsilon\in F_2^n-\{0\}}\Big|\sum_{i\in[1,n]}2^n(-1)^{\rho_i}S_{(D_\varepsilon f_i)}(0)\Big|\le\left((2^n-1)\sum_{\varepsilon\in F_2^n-\{0\}}\left(\sum_{i\in[1,n]}2^n(-1)^{\rho_i}S_{(D_\varepsilon f_i)}(0)\right)^2\right)^{\frac{1}{2}} \tag{4}$$

由(4)式得

$$\sum_{\varepsilon\in F_2^n-\{0\}}\left(\sum_{i\in[1,n]}2^n(-1)^{\rho_i}S_{(D_\varepsilon f_i)}(0)\right)^2=$$

$$2^{2n}\left(\sum_{\varepsilon\in F_2^n-\{0\}}\sum_{i\in[1,n]}\left(S_{(D_\varepsilon f_i)}(0)\right)^2+2\sum_{\varepsilon\in F_2^n-\{0\}}\sum_{i,j\in[1,n]}S_{(D_\varepsilon f_i)}(0)S_{(D_\varepsilon f_j)}(0)\right) \tag{5}$$

将式(4)、式(5)代入式(2)即得式(3)。

推论 1 按照透明阶的定义和定理 1 的假设，可以推出透明阶下限的另一种表示形式，如下式所示：

$$\tau_F\ge n-\frac{1}{\sqrt{2^n-1}}\sqrt{\sum_{\varepsilon\in F_2^n}\sum_{i\in[1,n]}\left(S_{D_\varepsilon f_i}(0)\right)^2+2\sum_{\varepsilon\in F_2^n}\sum_{i,j\in[1,n]}S_{D_\varepsilon f_i}(0)S_{D_\varepsilon f_j}(0)-n^2 2^{2n}} \tag{6}$$

证明

由定理 1 可知：

$$\sum_{\varepsilon\in F_2^n-\{0\}}\left(\sum_{i\in[1,n]}2^n S_{(D_\varepsilon f_i)}(0)\right)^2=$$

$$2^{2n}\sum_{\varepsilon\in F_2^n}\sum_{i\in[1,n]}\left(S_{D_\varepsilon f_i}(0)\right)^2+2^{2n+1}\sum_{\varepsilon\in F_2^n}\sum_{i,j\in[1,n]}S_{D_\varepsilon f_i}(0)S_{D_\varepsilon f_j}(0)-n^2 2^{4n} \tag{7}$$

将式(7)代入式(2)中，即得式(6)。

2.3 透明阶与非线性度的关系

透明阶与 n 元布尔函数的 Walsh 谱变换的关系由透明阶的定义可知，而 n 元布尔函数非线性度与 Walsh 谱变换的关系如定义 3 所示：

$$N_f=2^{n-1}\left(1-\mathrm{MAX}\,|\,S_{(f)}(w)\,|\right)$$

由此关系可得 $\mathrm{MAX}\,|\,S_{(f)}(w)\,|=1-2^{1-n}N_f$。

定理 2 设$F=(f_1,f_2,\cdots,f_p)$是一个(n,p)元布尔函数，对于任意的 $i=1,2,\cdots,n$，每一个函数 f_i： $GF(2^n)\to GF(2)$ 都是n元布尔函数，则

$$\tau_F\ge n-\sqrt{3n}\,|1-2^{1-n}N_f\,|$$

证明

由定理 1 可知

$$\because\ \Big|\sum_{i\in[1,n]}2^n(-1)^{\rho_i}S_{(D_\varepsilon f_i)}(0)\Big|\le\sum_{i\in[1,n]}|S_{(D_\varepsilon f_i)}(0)|\le$$

$$\sum_{i\in[1,n]}\mathrm{MAX}\,|S_{(D_\varepsilon f_i)}(w)|$$

$$\therefore\tau_F\ge n-\frac{1}{\sqrt{2^n-1}}\sqrt{3\sum_{\varepsilon\in F_2^n-\{0\}}\sum_{i\in[1,n]}\mathrm{MAX}\left(S_{D_\varepsilon f_i}(w)\right)^2} \tag{8}$$

又知

$$\mathrm{MAX}\,|\,S_{(f)}(w)\,|=1-2^{1-n}N_f \tag{9}$$

将式(9)代入到式(8)中得：

$$\tau_F \geq n - \frac{1}{\sqrt{2^n - 1}} \sqrt{3n(2^n - 1)(1 - 2^{1-n} N_f)^2} \quad (10)$$

化简式(10)得：

$$\tau_F \geq n - \sqrt{3n}\,|1 - 2^{1-n} N_f\,| \quad (11)$$

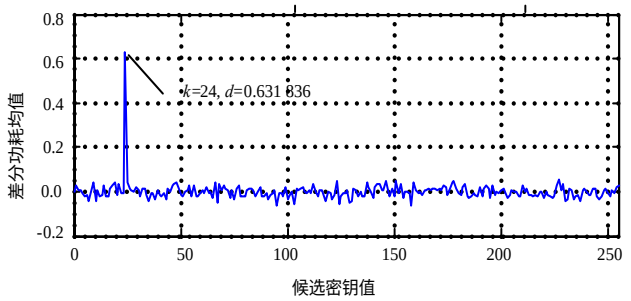
由式(11)可知，DES中第3个S盒布尔函数非线性度是16，τ_F值下限约等于 3.879；其AES中S盒布尔函数非线性度是112，τ_F值下限约等于 7.387；bent函数的非线性度是120，τ_F下限约等于 7.694。

随着非线性度的增大，透明阶τ_F也逐渐增大，系统抗DPA能力就变弱。由此可见，非线性度的大小对密码抗DPA能力好坏有着重要的影响。由于透明阶和S盒函数非线性度是线性关系，要取得抗DPA和抗线性差分分析性能的折中方案有一定的难度。

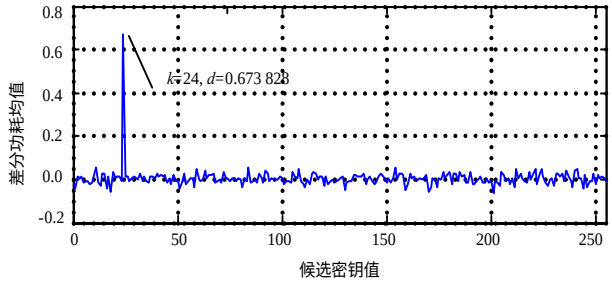
3 仿真实验结果

为了对比非线性度大小对 S 盒抗差分功耗分析能力的影响，本文使用软件仿真的方法，通过对不同透明阶大小的加密函数进行差分功耗分析实验，力求证明非线性度对密码系统抗差分功耗分析能力有很大的影响。实验仿真使用随机明文 $X_i \in F_2^n, i \in (0,255)$，密钥正确值为 24。

高级加密标准算法S盒布尔函数和改进的AES S盒布尔函数[7]的差分功耗对比见图 1。



(a)AES S盒的DPA



(b)改进的AES S盒的DPA

图 1　AES S 盒函数的 DPA 效果对比

高级加密标准算法 S 盒布尔函数、数据加密标准的第 3 个 S 盒布尔函数、线性函数的差分功耗对比见图 2。为了便于对比分析密钥正确时的峰值变化，其中，DES S 盒的纵坐标值加 0.3；AES S 盒的纵坐标值加 0.5。从图 1 可以看出，分别对两个 S 盒进行差分功耗分析，它们的差分功耗均值分别为 0.631 836 和 0.673 828，相差不大。也就是说虽然 S 盒的其他性质改善了，但是只要它的非线性度大小不变，它抵抗 DPA 的能力不会有太大变化。图 2 表明，随着加密函数的非线性度的增大，对应于正确密钥的差分功耗均值的峰值也是逐渐增大的。也就是说，对于具有高的非线性度的布尔函数来说，对它进行差分功耗分析，可以明显看出有峰值的出现，即正确密钥很容易被析出；而对于非线性度较低的函数，通过使用 DPA 手段进行攻击，对应于任何一个猜测密钥，均没有特别明显的峰值出现，即正确密钥很难被猜到。实验表明：S 盒函数的非线性度大小影响密码系统抵抗差分功耗分析的强度。

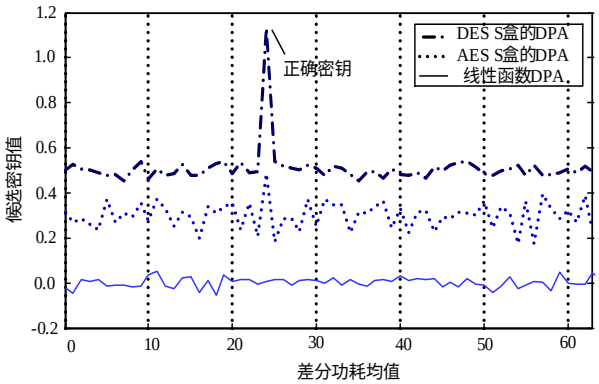


图 2　S 盒函数的 DPA 效果对比

4 结束语

本文借助透明阶概念，推导并证明了一个高非线性 S 盒的透明阶下界的计算公式，为 S 盒设计的优劣提供了一个参考判别准则：透明阶的下界与非线性度大小成正比，即非线性度越大，透明阶也就越大，迭代分组密码系统防范 DPA 攻击的能力就越弱。

透明阶作为S盒的一个新性质，能够更加准确地确定抗差分功耗分析能力，笔者将在如何确定其他APN函数的透明阶大小、如何更为精确地确定τ_F值的上下限等方面继续展开研究。

参考文献

[1] Analysis and Related Attacks[EB/OL]. (1998-10-09). http://www.cryptography.com/dpa/technical/.

[2] Kocher P. Differential Power Analysis[C]//Proc. of CRYPTO'99. California, USA: Springer-Verlag, 1999: 388-397.

[3] Emmanuel P. DPA Attacks and S-boxes[C]//Proc. of the 12th International Workshop on Fast Software Encryption. Paris, France Springer-Verlag, 2005: 424-441.

[4] Messerges T S. Examining Smart-card Seurity Under the Therat of Power Analysis Attacks[J]. IEEE Transactions on Computers, 2002, 51(4): 541-552.

[5] 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000: 9-19.

[6] Carlet C. On Highly Nonlinear S-boxes and Their Inability to Thwart DPA Attacks[C]//Proc. of INDOCRYPT'05. Paris, France: Springer-Verlag, 2005: 125-143.

[7] 刘连浩, 崔　杰, 刘上力. 一种 AES S 盒改进方案的设计[J]. 中南大学学报, 2007, 38(2): 339-344.