

引用格式: 杨正文, 郭箏. 抗相关性功耗分析的 DES 掩码方案[J]. 微电子学与计算机, 2019, 36(9): 1-6. [YANG Z W, GUO Z. Masking scheme against correlation power analysis on DES [J]. Microelectronics & Computer, 2019, 36(9): 1-6.]

抗相关性功耗分析的 DES 掩码方案

杨正文, 郭 箏

(上海交通大学 电子信息与电气工程学院, 上海 200240)

摘 要: 以相关性功耗分析为代表的旁路攻击技术对密码设备的安全性造成严重威胁, 针对这种情况, 本文提出了一种新型的抗相关性功耗攻击的掩码防护方案. 该方案是一种流水线式的“非对称掩码技术”, 通过流水线式操作, 使得加密过程中的每一轮都引入了不同的随机掩码, 功耗和操作数之间的相关性被扰乱, 从而抵御相关性攻击. 我们通过功耗仿真, 采集了标准 DES、对称掩码方案及本文提出防护方案对应的功耗仿真曲线, 并对其进行相关性功耗攻击. 实验结果表明, 标准 DES 需要 1 000 条可以攻击成功, 对称掩码方案需要 4 000 条功耗曲线可以攻击成功, 非对称防护方案则需要 50 000 条曲线才能攻击成功, 防护能力提升了 10 倍以上, 掩码方案可以有效抵抗相关性功耗分析.

关键词: 差分功耗分析; 掩码; 相关性功耗攻击; 流水线

中图分类号: TN918. 4

文献标识码: A

文章编号: 1000—7180(2019)09—0001—06

Masking scheme against correlation power analysis on DES

YANG Zheng-wen, GUO Zheng

(College of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract: With the situation that side channel attack poses a serious threat to the security of cryptographic devices, we propose a new scheme of pipelined “asymmetric masking technology” against correlation power analysis and implement it in DES algorithm. Through pipelined operation, different random masks are introduced in each round of the encryption process, so that the correlation between power consumption and processing data is disturbed and we can resist correlation power analysis. Through power simulation, we collected the standard DES, symmetric mask scheme and the power simulation curve corresponding to the proposed protection scheme, and conducted related power consumption attacks. The experimental results show that the standard DES requires 1000 power consumption curves, and the symmetric mask scheme requires 4000 power consumption curves to successfully attack. The protection scheme proposed in this paper requires 50,000 curves to successfully attack, and the protection capability is improved by more than 10 times. We can say that scheme can achieve great protection.

Key words: differential power analysis; masking; correlation power analysis; pipeline

1 引言

侧信道攻击(Side-Channel Analysis, SCA)自出现以来, 对嵌入式加密系统产生了致命威胁, 其利用加密硬件执行某种操作时泄露的关键信息^[1](如电磁信号、功耗、执行时间等)来进行攻击. 功耗分析

利用硬件执行时的功耗信息来攻击, 是当前对密码芯片威胁最大的攻击方式之一, 其原理是利用 CMOS 电路在翻转时产生的功耗和数据有关的特征, 通过猜测算法的中间结果来恢复密钥. 大量实验证明如果不采取防护措施, 几乎所有的密码电路都会受此类攻击的影响. 目前已有大量的分析方法被

收稿日期: 2018—12—20; 修回日期: 2019—01—14

基金项目: 国家自然科学基金(U1536103)

提出,其中应用最为广泛的就是差分功耗分析(differential power analysis,DPA)^[2]和由其衍生的基于相关系数的差分功耗攻击(correlation power analysis,CPA)^[3].Kocher 等在 1999 年提出 DPA 技术,通过测量约 1 000 条芯加解密操作时的功耗曲线,就可以破译当时市场上大部分智能卡.2004 年,Brier 等人在 CHES 会议上指出基于相关性系数的差分功耗分析(CPA)相比传统 DPA 的优势.随着各种各样分析方法的提出,差分功耗分析和相关性功耗分析对加密系统的威胁也越来越大.

2 掩码方案

为抵御功耗攻击,多种抗功耗攻击的方法相继诞生,例如在算法流程中插入随机操作^[4]、增加功耗噪声^[5]和采用双轨电路设计的方法^[6]等.这些操作都是想通过增加噪声降低信噪比,隐藏泄露信息.但是事实证明一旦攻击者采取一些预处理的操作,这些方法都将失效.后来,Chari^[7]提出掩码这一方法,在加密算法运算时,每一个中间值都与一个称为“掩码”的随机数进行变换,这使得功耗信息不仅与密钥操作有关,而且还与引入的随机数相关.随机数扰乱了功耗与密钥间的相关性,从而实现了抗功耗攻击.对数据实施随机掩码主要是消除猜测中间值与功耗的相关性,攻击者虽然同样可以采集到功耗值,但由于输入增加了随机掩码使得攻击者不能获取有效中间值.由于其不改变硬件设备的功耗消耗特征,所以很多防护方案都基于此展开.但是这些传统掩码技术只能抵御运用简单分类模型的 DPA 攻击,无法有效抵御基于数学模型进行相关性计算的 CPA 攻击.

针对这种情况,大量研究都致力于寻找有效的掩码防护方案.Akkar 等^[8]首先在 DES 上实现了一种掩码方案,通过引入随机数,保证了每一轮计算存在寄存器的中间值都带上了相同的掩码.蒋惠萍^[9]将掩码加在密钥上,同样达到了随机化功耗的效果.李杰,单伟伟等^[10]提出了一种 32 位随机数掩码方法,但是该方案左右 32 位带相同掩码使得攻击者完全可以通过左右中间值异或的方式消除掩码,存在缺陷.徐鹏,薛伟^[11]提出了改进方案,保证了左右 32 位带的掩码不相同,但是每一轮所带的掩码仍然与上一轮相同,前后两轮之间异或操作可以消去掩码的防护作用.

针对以上问题,本文提出了一种流水线式的非对称掩码方案.该掩码方案保证了在 DES 算法的每

一轮都加上了不同的掩码,并且左右 32 位所带掩码不同,最大可能保证了算法在整个计算过程中不出现真实值,从而有效地抵御相关功耗攻击.

3 DES 算法

DES 算法含有 16 轮($i=1,2,\dots,16$)加密操作,进入首轮操作前需进行的初始置换(Initial Permutation,IP),第 16 轮的输出需要进行最终置换(Final Permutation,FP).每一轮内的操作包括 E 盒置换、S 盒置换(S-BOX)、P 盒置换;轮间的加密子密钥为 K_i ;轮间数据被分为相同长度(32 位)的 L_i , R_i 两部分.标准的 DES 算法不带防护每一轮的加密流程如图 1 所示.

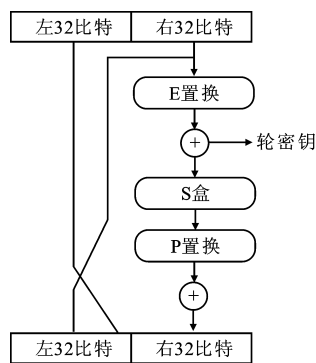


图 1 DES 算法结构

针对 DES 的 CPA 攻击的流程为:

(1) 选择 DES 执行过程的某个中间值.这个中间值可以看做是一个函数 $f(d,k)$,其中 d 是明文或者密文, k 是密钥的一部分(此次我们攻击 DES 算法的首轮,所以 d 代表的是明文).

(2) 测量 DES 加密过程的实际功耗迹.密码设备每次执行加密或者解密操作时,攻击者都需要记录相应的明文 d 值,密码设备若采集 D 次加密过程,每次加密都会记录一条功耗曲线,每条曲线含 P 个点,也就是功耗曲线的长度.经过 D 次加密我们将获得一个 $D \times P$ 的功耗矩阵,记为矩阵 T ;

(3) 计算假设的中间值.假设子密钥 k 有 K 种可能,对于每一次加密计算出中间值,可获得一个 $D \times K$ 的中间值矩阵 V ;

(4) 将中间值映射为假设功耗值.用功耗模型(汉明距离或者汉明重量模型)将中间值矩阵 V 映射成一个 $D \times K$ 的假设功耗矩阵 H ;

(5) 计算假设功耗矩阵 H 与实际功耗矩阵 T 之间的相关性,得出一个 $K \times P$ 的矩阵 R ,其每一行分别对应一种猜测的密钥,每一列对应在该时刻实际

功耗与假设功耗之间的相关系数,计算式为:

$$r_{i,j} = \frac{\sum_{d=1}^D (h_{d,i} - \bar{h}_i)(t_{d,j} - \bar{t}_j)}{\sqrt{\sum_{d=1}^D (h_{d,i} - \bar{h}_i)^2 \sum_{d=1}^D (t_{d,j} - \bar{t}_j)^2}} \quad (1)$$

式中, $h_{d,i}$ 为矩阵 $\mathbf{H}$ 的元素, $i = 1, 2, \dots, K; d = 1, 2, \dots, D; t_{d,j}$ 为矩阵 $\mathbf{T}$ 的元素, $j = 1, 2, \dots, P$.

(6) 将矩阵 $\mathbf{R}$ 按行绘制出曲线, 曲线的横坐标是 P 个点, 纵坐标是相关性的值. 图中将 K 条曲线放在一起, 为了更好地区分出正确密钥和错误密钥, 出现峰值的曲线表明猜测密钥值正确.

4 掩码方案的实现及功能仿真

4.1 掩码方案

CPA 攻击能成功的原因是密码设备的能量消耗依赖于密码算法的中间值, 所以掩码方案的目标就是消除这种依赖性. 通过对密码算法中间值加上掩码, 随机化后的中间值的能量消耗与处理实际中间值所需的能量消耗之间相互独立. Akkar^[8] 提出的掩码方案中左右 32 位所带的掩码是相同的, 可称其为“对称掩码”, 相对地本文左右 32 位所带掩码不同, 故我们称其为“非对称掩码”. 本文提出的流水线式的非对称 DES 掩码方案流程图如图 2 所示.

算法首先将明文 P 输入, 经过 IP 变换. 然后左边 32 位异或上 32 位的掩码 XL, YR , 结果作为 L'_0 , 右 32 位异或上 32 位的掩码 XR, YL , 以及固定掩码 M_1 , 结果作为 R'_0 . 后面第 1~16 轮每次进入的数据都同 L'_0 和 R'_0 中所带的掩码一样, 左 32 位带 XL 和 YR , 右 32 位带 XR, YL , 以及固定掩码 M_1 .

在本次掩码方案中, S 盒是唯一的非线性运算. 由于方案中我们引入了固定掩码, 所以计算中我们重新构造了掩码 S 盒, 定义为 SM 盒.

$$SM(IN \oplus E(M_{1(i-1)})) = S(IN) \oplus M_{3(i)} \quad (2)$$

我们掩码方案的整个计算流程的推导如下所示: 对同一明文, 同一密钥, 标准 DES 算法和我们的掩码方案的中间值分别定义为 L_i, R_i 与 L'_i, R'_i ($0 \leq i \leq 16$).

DES 每一轮中间值有如下规则:

$$L_i = R_{i-1} \quad (3)$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \quad (4)$$

式中, f 函数是 R_{i-1}, K_i 经过 E 扩展, S 盒, P 盒的运算过程的统称.

$$L'_0 = L_0 \oplus XL_{(0)} \oplus YR_{(0)} \quad (5)$$

$$R'_0 = R_0 \oplus XR_{(0)} \oplus YL_{(0)} \oplus M_{1(0)} \quad (6)$$

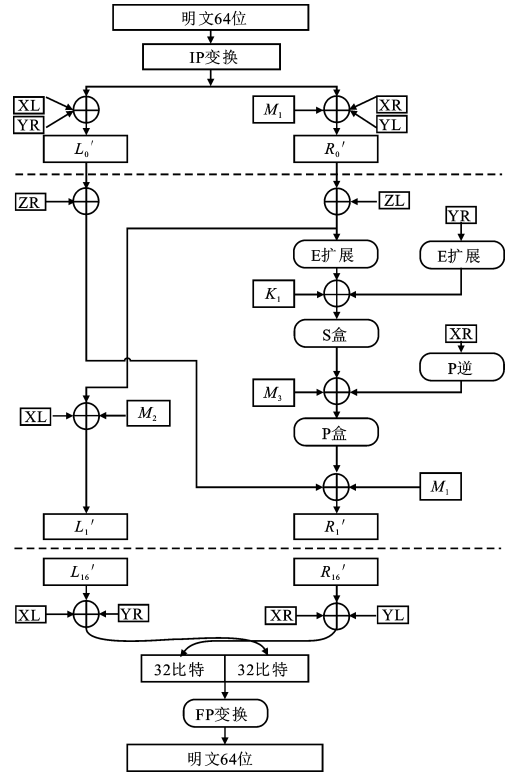


图2 流水线式的非对称 DES 掩码方案

第 1 到 16 轮加密:

$$L'_i = L_i \oplus XL_{(i)} \oplus YR_{(i)} \quad (7)$$

$$R'_i = R_i \oplus XR_{(i)} \oplus YL_{(i)} \oplus M_{1(i)} \quad (8)$$

推导过程如下:

$$L'_i = R'_{i-1} \oplus ZL_{(i)} \oplus XL_{(i)} \oplus M_{2(i)} \quad (9)$$

$$R'_i = L'_{i-1} \oplus ZR_{(i)} \oplus f(R'_{i-1}, K_i) \oplus M_{1(i)} \quad (10)$$

其中:

$$f(R'_{i-1}, K_i) = P(SM(E(R'_{i-1} \oplus ZL_{(i)}) \oplus E(YR_{(i)}) \oplus K_i \oplus M_{3(i)}) \oplus P^{-1}(XR_{(i)})) \quad (11)$$

由于本次实现随机数掩码是流水线的形式, X, Y, Z 都是 64 位的寄存器, 将寄存器 X 的值传递给寄存器 Y , 寄存器 Y 的值传递给寄存器 Z . 实现中随机数掩码的值由线性反馈移位寄存器产生. 则有如下:

$$Y_i = X_{i-1} \quad (12)$$

$$Z_i = Y_{i-1} \quad (13)$$

式中, L 代表左 32 位; R 代表右 32 位. 则 XL 表示寄存器 X 的左 32 位的值, XR 表示寄存器 X 的右 32 位的值, 依次类推. 同理固定掩码也是, 固定掩码放在寄存器 M_1 中, 经过时钟传递给寄存器 M_2 则有:

$$M_{2(i)} = M_{1(i-1)} \quad (14)$$

由式(9)得到:

$$L'_1 = R'_0 \oplus ZL_{(1)} \oplus XL_{(1)} \oplus M_{2(1)} \quad (15)$$

将式(6)代入得:

$$L'_1 = (R_0 \oplus XR_{(0)} \oplus YL_{(0)} \oplus M_{1(0)}) \oplus ZL_{(1)} \oplus XL_{(1)} \oplus M_{2(1)} \quad (16)$$

由式(12),(13),(14)得:

$$L'_1 = L_1 \oplus XL_{(1)} \oplus YR_{(1)} \quad (17)$$

由式(10)得到:

$$R'_1 = L'_0 \oplus ZR_{(1)} \oplus f(R'_0, K_1) \oplus M_{1(1)} \quad (18)$$

将式(5)代入得到:

$$R'_1 = (L_0 \oplus XL_{(0)} \oplus YR_{(0)}) \oplus ZR_{(1)} \oplus f(R'_0, K_1) \oplus M_{1(1)} \quad (19)$$

将式(1),(11),(12),(13),(14)代入式(19)得:

$$R'_1 = R_1 \oplus XR_{(1)} \oplus YL_{(1)} \oplus M_{1(1)} \quad (20)$$

2轮到16轮也是这样的.至此可以推出一般性公式:

$$L'_i = L_i \oplus XL_{(i)} \oplus YR_{(i)} \quad (21)$$

$$R'_i = R_i \oplus XR_{(i)} \oplus YL_{(i)} \oplus M_{1(i)} \quad (22)$$

经过16轮变换, L'_{16} 和 R'_{16} 所带掩码值如上所述,将 L'_{16} 异或上 $XL_{(16)}$ 和 $YR_{(16)}$, R'_{16} 异或上 $XR_{(16)}$ 和 $YL_{(16)}$,以及固定掩码 $M_{1(16)}$.得到两个32位的数据,左右交换后,合并成64位的数据进入FP变换得到最终的密文.

4.2 掩码方案功能仿真

本文使用verilog硬件描述语言,在Xilinx的ISE工具上实现功能仿真,仿真采用的时钟周期为 $clk=20$ ns.输入的是16进制的64位明文64'h0000000000000001F,密钥固定为64'h99EEF067A8100522,标准DES算法的结果应当是64'hAED8CB1812EE4B0D.设计中随机数掩码由线性反馈移位寄存器产生.图3是非对称掩码方案的功能仿真图,输出是64'hAED8CB1812EE4B0D,由此验证了非对称掩码方案的功能正确.

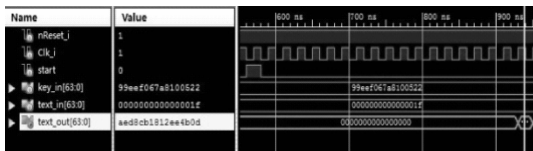


图3 流水线式的非对称DES掩码方案功能仿真

5 功耗仿真和结果分析

5.1 功耗仿真

本次实验是在仿真环境下进行,我们建立了基于EDA工具的功耗仿真测量平台.利用Synopsys

公司的综合工具Design compiler对RTL设计文件进行逻辑综合,得到相应的门级网表文件,然后用VCS工具对其进行时序仿真,生成多次加密过程中的功耗点的VPD文件并且记录与之对应的明密文,再利用PTPX工具对门级网表和VPD文件进行功耗仿真,生成out文件,最后我们利用曲线转换工具对out文件其进行格式转化,得到仿真功耗曲线,曲线是接近于真实测量结果去除噪声的结果.以上测试平台的优点在于:能够对电路设计进行较快地实现,检测其安全性,大幅度减少时间和成本.而且测试环境是无噪声的,更能体现测试的准确性.

为了充分说明我们提出的掩码方案抗CPA攻击的有效程度,我们将改进的掩码方案与标准DES算法以及对称掩码方案都进行了电路实现并且都进行了功耗仿真,最终选取标准DES算法的1000条曲线,对称掩码方案的4000条曲线,以及非对称掩码方案的50000条曲线,分别进行了抗CPA攻击测试实验.

5.2 CPA分析结果

对于DES算法攻击一般选择攻击首轮.对于标准DES方案,我们得到的功耗曲线是1000条,每条曲线的采样点数是6400个,因此生成的功耗矩阵T是 1000×6400 的.现在攻击首轮的48位子密钥,以每6位为一组,分为8组,逐组攻击.

首先攻击第一轮字密钥的前6位.取第一个S盒输出的中间值矩阵V,通过全比特模型映射成假设功耗矩阵H,将H和T两个矩阵的功耗数据导入matlab中,计算相关系数.得到一个 64×6400 的矩阵R.矩阵的每一个元素 $R_{i,j}$ 是H的第i列和T的第j列的相关系数,表示的是猜测密钥i的中间值和第j个功耗点的仿真功耗的相关性.将R矩阵的数据按行作图,得到第一个6位字密钥和功耗点的相关性.由于我们攻击的是第一轮,所以我们针对性地放大了DES的第一轮运算过程.第一轮的第1个6比特的相关性分析如图4所示.

图4和图5中(a)是标准的DES掩码方案1000条曲线做的相关性分析曲线,(b)是Akkar提出的对称掩码方案4000条曲线做的相关性分析,(c)是本文提出的流水线式的非对称掩码方案的相关性分析,曲线条数是50000条.黑色曲线是正确密钥与功耗的相关系数曲线,灰色是错误密钥与功耗的相关系数曲线.图中可以看出(a)(b)中正确密钥的相关系数与错误密钥的差距明显,而(c)中的正确密钥的相关系数和错误密钥差距不明显,非对称掩

码的正确密钥的相关性淹没于错误密钥中.

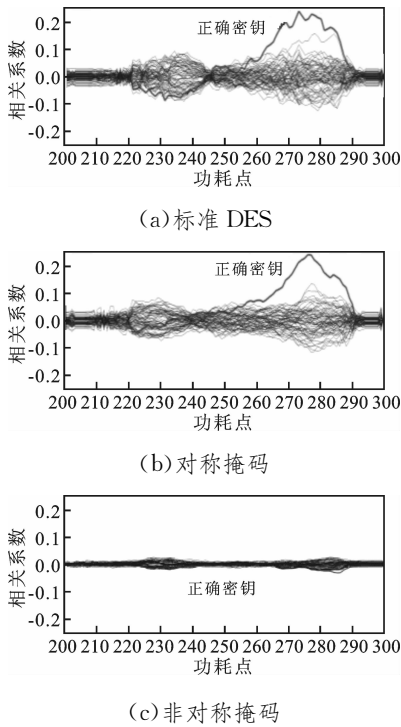


图 4 第 1 个 6 比特子密钥相关性分析
第一轮的第 5 个 6 比特的相关性分析结果如下
图 5 所示.

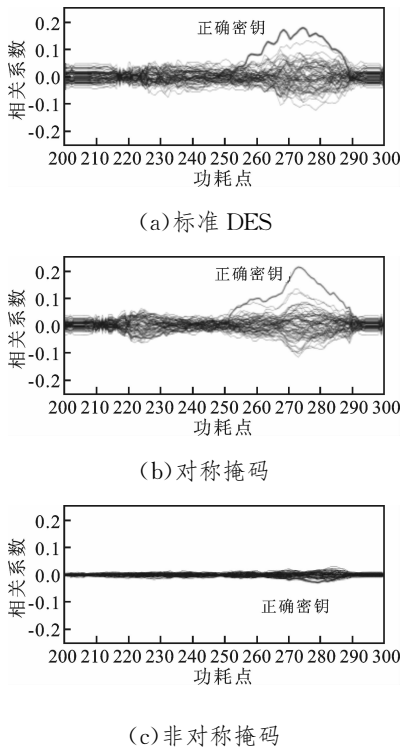


图 5 第 5 个 6 比特子密钥相关性分析
进一步地对 R 的每一行进行排序,将每一行的
最大值放在第一列.然后对 R 矩阵的第一列进行绘
图如图 6 所示,发现对于标准的 DES 算法,第一个 6

位的子密钥为 33(即 0×21)的值明显最大,即第一
个 6 位子密钥攻击成功.对称掩码方案同样攻击成
功,但是本文提出的非对称方案攻击不成功.

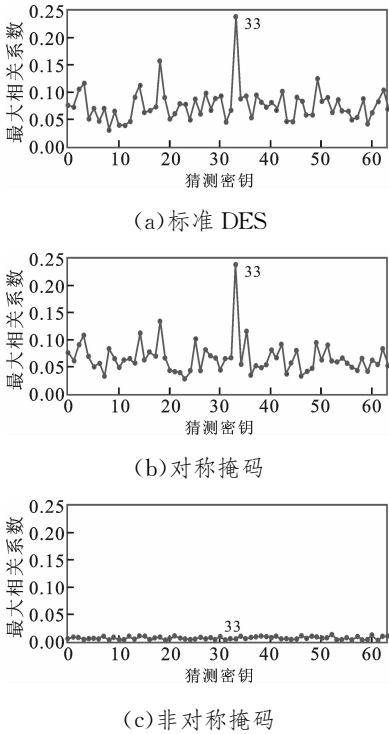


图 6 第 1 个 6 比特子密钥最大相关性
对于第 5 个 6 位子密钥 7(即 0×07)攻击结果如
图 7 所示,同样是标准 DES 算法和对称掩码方案都
能攻击出来,本文提出的方案攻击不出来.

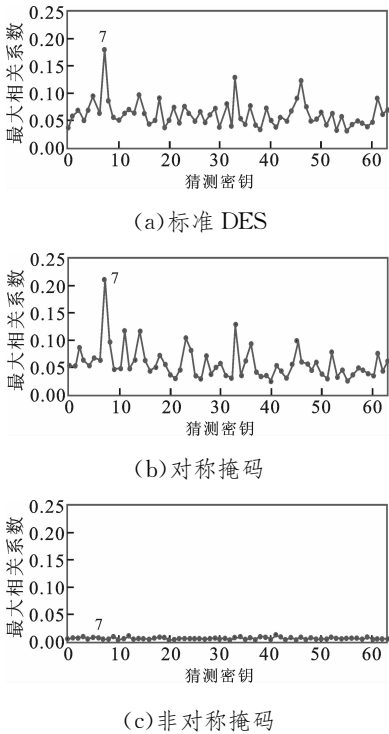


图 7 第 5 个 6 比特子密钥最大相关性

再用同样的方法去攻击剩下的 6 个 6 比特子密钥,实验结果与第 1 个和第 5 个 6 比特一致.我们发现当猜测子密钥与真实密钥相同的时候,标准 DES 和对称掩码方案的相关系数明显高于其他错误密钥,即相关系数为最大值,出现尖峰,因此可以用相关系数来恢复出真实的密钥值,故 CPA 攻击成功.而本文提出的非对称掩码方案的实验结果却表明正确密钥和错误密钥的相关系数并无较大差距,正确密钥的相关曲线同样没有显示出明显峰值,故无法从功耗中推测出正确密钥,攻击不成功.

由于我们引入了流水线式的非对称随机掩码,保证每轮的掩码都不一样,导致汉明距离模型没法表示出实际功耗.所以对于 CPA 攻击来说,即使猜测密钥正确,相关系数也达不到最大值,即使增加了仿真曲线数,正确密钥的相关性曲线仍然不理想.实验结果完全可以说明我们的掩码方案可以达到较好地抗 CPA 攻击的效果.

6 结束语

本文基于 DES 密码算法提出了一种抗 CPA 攻击的改进掩码方案.通过使用流水线的方式,改变每一轮所带的掩码,并且设计保证了每一轮左右 32 位所带的掩码不同.同时采取了掩码 S 盒,并且掩码所加的位置都提前了一个时钟,可以减少电路实现中可能由于路径长度不同导致组合逻辑产生的泄露.功能仿真保证了掩码方案功能的正确性,同时在仿真功耗平台下完成了功耗仿真,实验结果表明我们提出的流水线式的非对称掩码方案可以抵抗 CPA 攻击.后续如果想要增加安全性,可以从增加掩码 S 盒的个数的角度继续研究.

参考文献:

- [1] KELSEY J, SCHNEIER B, WAGNER D, et al. Side channel crypt analysis of product ciphers[J]. Journal of Computer Security, 2000, 8(2/3): 141-158.
- [2] KOCHER PAUL, JAFFE JOSHUA, JUN BENJAMIN. Differential power analysis[C]// 19th Annual International Cryptology Conference, California,

USA:Springer,1999: 388-397.

- [3] MANGARD STEFAN, OSWALD ELISABETH, POPP THOMAS. Power analysis attacks[M]. Berlin, Germany: Springer Science, 2007.
- [4] ZAFAR Y, PARK J, HARD D, et al. Random clocking induced DPA attack immunity in FPGA[C]// IEEE International Conference on Industrial Technology, Gwangju, Korea, IEEE, 2010: 1068-1070.
- [5] KAMOUN N, BOSSUET L, GHAZEL A. Correlated power noise generator as a low cost DPA countermeasures to secure hardware AES cipher[C]// 3rd International Conference on Signals, Circuits and Systems (SCS). Medenine, Tunisia, IEEE, 2009:1-6.
- [6] GUILLEY S, SAUVAGE L, HOOGVORST P, et al. Security evaluation of WDDL and SecLib countermeasures against power attacks[J]. IEEE Transactions on Computers, 2008, 57(11): 1482-1497.
- [7] CHARI S, JUTLA C S, RAO J R, et al. Towards sound approaches to counteract power-analysis attacks [C]// Annual International Cryptology Conference on Advances in Cryptology. Berlin, Springer-Verlag, 1999: 398-412.
- [8] AKKAR M L, GIRAUD C. An implementation of DES and AES secure against some attacks[C]// Third International Workshop on Cryptographic Hardware and Embedded Systems (CHES). Paris, France, Springer, 2001: 309-318.
- [9] 蒋惠萍,毛志刚. 一种抗差分功耗攻击的改进 DES 算法及其硬件实现[J]. 计算机学报, 2004, 27(3): 334-338.
- [10] 李杰,单伟伟,吕宇翔,等. 一种抗相关功耗攻击 DES 算法及 FPGA 电路实现[J]. 东南大学学报:自然科学版, 2012, 42(6): 1063-1068.
- [11] 徐鹏,薛伟. 抗差分功耗攻击的 DES 算法研究[J]. 计算机仿真, 2018(1): 282-286.

作者简介:

杨正文 男,(1995-),硕士研究生.研究方向为侧信道攻击、硬件掩码. E-mail:zhengwen_y@163.com.

郭 箴 男,(1980-),博士,工程师.研究方向为集成电路安全分析和测试.