一种轻量级数据加密标准循环掩码实现方案

王立辉② 闫守礼② 李 清*①②
①(复旦大学专用集成电路与系统国家重点实验室 上海 201203)
②(上海复旦微电子集团股份有限公司 上海 200433)

摘 要：随着智能卡技术的不断发展，智能卡芯片的安全性也面临越来越大的挑战。在众多加密算法中，数据加密标准(DES)算法是一种应用较广的对称加解密算法。为了抵御各种侧信道攻击，使用最为广泛的是在算法中通过掩码技术来消除真实密钥和功耗相关性，该文提出一种新的适用于DES的循环掩码方案，和之前文献中的预计算掩码方案相比，不仅预计算量大大减少，而且整个DES运算过程的中间数据都是带有掩码的，把掩码拆分后，还可以防护高阶攻击。

关键词：数据加密标准；侧信道攻击；掩码
中图分类号：TN918.4 **文献标识码**：A **文章编号**：1009-5896(2020)08-1828-08
DOI: 10.11999/JEIT190870

A Lightweight Implementation Scheme of Data Encryption Standard with Cyclic Mask

WANG Lihui② YAN Shouli② LI Qing①②
①(*State Key Laboratory of ASIC and System*, *Fudan University*, *Shanghai* 201203, *China*)
②(*Shanghai Fudan Microelectronics Group Company Limited*, *Shanghai* 200433, *China*)

Abstract: With the continuous development of smart card technology, the security of smart card chip is facing more and more challenges. Among many encryption algorithms, Data Encryption Standard(DES) algorithm is a widely used symmetric encryption and decryption algorithm. In order to resist all kinds of side channel attacks, the most widely used method is to eliminate correlation of the real key and power consumption through the masking technology in the algorithm. A new cyclic mask scheme for DES is proposed. Compared with the pre-calculated mask scheme in the previous literature, not only the pre-calculation amount is greatly reduced, but also the intermediate data in the whole DES operation process is masked. After the mask is split, it can also protect against high-order attacks.

Key words: Data Encryption Standard(DES); Side channel attack; Mask

1 引言

数据加密标准(Data Encryption Standard, DES)，是一种使用密钥加密的分组密码算法，1977年被美国联邦政府的国家标准局确定为联邦资料处理标准，并授权在非密级政府通信中使用，随后该算法在国际上广泛流传开来。由于DES的密钥较短，随着硬件计算能力的不断提升，其安全性逐步降低，后来逐渐被高级加密标准(Advanced Encryption Standard, AES)所替代。但是在算法过渡过程中，DES的一种安全变形模式3DES(Triple DES，相当于是对每个数据块应用3次DES加密算法)到目前为止仍然有着大量的应用。

一直以来，针对DES和AES等密码算法的攻击手段仅仅局限于寻找密码算法自身的缺陷，从而使得密码算法的破译变成一个繁冗的数学理论推理研究过程。但是近年来出现的侧信道攻击(Side Channel Attacks，SCA)突破了传统的密码算法攻击模式，成为最具威胁的攻击方法[1,2]。

侧信道攻击不同于传统的密码算法攻击方式，利用算法在硬件设备中运行时泄漏的各种信息，采用科学的分析手段，最终达到获取密钥信息的目的。密码设备在进行运算和工作时，不可避免地存在着某些信息的泄漏，比如：时间、功耗、电磁辐射和有意让其发生错误后产生的结果等等。把对以

收稿日期：2019-11-01；改回日期：2020-06-06；网络出版：2020-07-07
*通信作者： 李清 liqing@fmsh.com.cn
基金项目：十三五预先研究项目(3110105-09)
Foundation Item: The 13th Five-Year Plan Advance Reserch Projects Fund of China (3110105-09)

上这些泄漏信息的监测分析和对算法的数学分析结合起来，就成为获取密钥信息、揭示芯片工作原理和最终破译加密芯片的最强大工具，并由此产生了诸如时间攻击，功耗分析攻击，错误攻击和电磁辐射攻击等一系列侧信道攻击的方法，这比单纯的通过分析算法获得信息要容易的多。后来人们发现，在某些情形下，把数学分析和和侧信道分析结合起来会更加有效，例如代数侧信道攻击(algebraic side-channel attacks)[3]。

抵御侧信道攻击的核心思想是：消除算法执行过程中的秘密中间值与各种硬件泄漏信息之间的一一对应关系，一切可以达到此目的的手段，均为可行的防护措施，若能同时兼顾硬件成本、执行时间等因素，则为有效的防护措施。

一般地，针对DES或AES的防护可分为隐藏和掩码两大类。隐藏的目的是通过随机化功耗或固定功耗等手段来隐藏真实数据的功耗。主要方法有功耗平衡[4–7]、时钟抖动[8]、随机延时[9]、冗余操作[10]、乱序执行[11]等，很多涉及到硬件，暂不作为本文讨论的重点内容，具体可参考文献[12]。掩码的目的通过随机化密码算法处理的中间数据，使其和功耗无关，是一种使用最为广泛的防护方法。典型的掩码方法又包括复制法[13,14]、预计算掩码法[15–18]、在线计算掩码法[19,20]、固定掩码法[21]、隐藏掩码法[22]等。

其中最受广泛关注的是预计算掩码法和在线计算掩码法，他们本质相同，只是前者把预计算结果保存下来，在本次加密中可以反复使用；后者是当在线计算的结果使用完毕以后直接丢弃，以节省存储空间。两者的优点是存储空间和时间都在可接受范围内，且都可以通过把掩码拆分来升级防护等级，以防护高阶功耗分析攻击。其它的防护方法要么实现代价较大，要么理论上存在安全漏洞。

在文献[18]的基础上，本文提出了一种新的适用于DES的循环掩码方案，和之前文献中的预计算掩码方案相比，不仅预计算量大大减少，而且整个DES运算过程的中间数据都是带有掩码的。本文其它部分组织结构如下，第2节阐述DES算法及功耗分析攻击原理，第3节全面分析之前的预计算掩码方案及优缺点，第4节提出新的循环掩码方案并分析其性能及安全性，在第5节对全文进行总结。

2　DES算法及功耗分析攻击原理

DES采用了64 bit的分组长度和56 bit的密钥长度，其算法流程如图1所示。其中IP是初始置换，IP^{-1}是与初始置换互逆的置换；子密钥K_1，K_2，K_{16}长度均为48 bit。轮函数F如图2所示，其中E为32～48 bit的扩展操作，SBox1, SBox2, …, SBox8, …表示查表操作，又被称为S盒，P表示32 bit的置换操作。算法安全性主要依赖于非线性不可逆运算的S盒。

DES算法是完全对称的结构，一般硬件实现时仅需实现1轮的电路，然后进行16次迭代进行16轮的加密，因此，在硬件上每一轮对应数据都是存储在同一个寄存器中，每次运算结束后更新寄存器的内容。通过观察一个寄存器的指定位，可以判断电路翻转的大致情况，从而对功耗曲线加以区分。因为寄存器某一位的翻转意味着上一轮计算输出的变化，这种变化往往就反映了S盒电路相关的一系列电路的动作，所产生的功耗要比输出不发生变化的

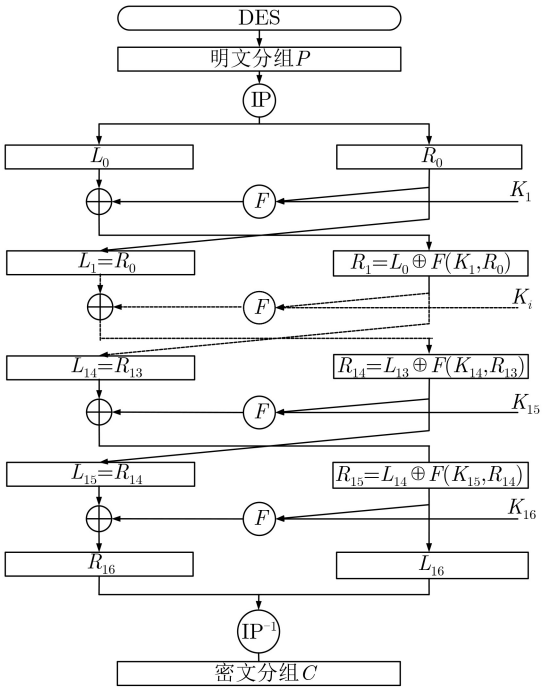


图 1 DES加密流程

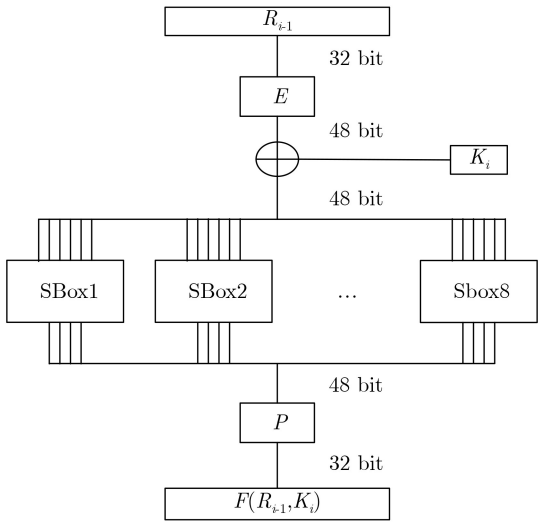


图 2 F函数

情况大一些，功耗分析攻击就是抓住了这种特征进行攻击的。

对于DES第16轮而言，由密文可以经过一系列逆运算得到R_{15}, L_{16}, R_{16}，如果要计算L_{15}，还需要知道子密钥K_{16}。在每轮运算中，48 bit子密钥与$R_{i\text{-}1}$扩展后的48 bit数据异或，结果分为8组，每6 bit经过一个S盒产生4 bit输出。因此R_i的每4 bit仅与相应的6 bit子密钥相关，与另外42 bit子密钥无关。因此，如果只计算L_{15}的某4 bit，则只需要知道子密钥K_{16}的6 bit即可，此6 bit密钥用Ks表示，这样需要猜测的Ks空间减少到2^6=64个。

假设需要计算L_{15}的第b bit，对相应的Ks分别使用0～63进行赋值，并计算L_{15}的第b bit，可能的结果为0和1。利用这个运算结果可以进行DES的功耗分析攻击，并确定Ks的真实值。

至此，可以得到如下的功耗分析破解流程：

(1) 猜测一个6 bit密钥Ks。

(2) 取出一组(C_0, W_0)，利用C_0推导出相应的L_{16}, R_{16}，与猜测的Ks一起代入区分函数，计算得到区分函数值d。

(3) 根据d的取值对功耗曲线W_0进行分类，$d=0$对应寄存器不翻转，W_0归入集合S_0；$d=1$对应寄存器翻转，W_0归入集合S_1。

(4) 重复(2)操作，直至遍历所有密文功耗曲线对(C_i, W_i)，得到两个集合S_0, S_1。

(5) 对S_0, S_1集合内的所有曲线分别求平均值，各自得到一条代表本集合功耗特性的曲线$\overline{W}_{S_0}$和$\overline{W}_{S_1}$。

(6) 对两条平均功耗曲线做差分，得到对应于这个猜测密钥的差分功耗曲线$\Delta W_{k_1}=\overline{W}_{S_1}-\overline{W}_{S_0}$。

(7) 重复(1)操作，遍历所有可能的64种密钥，得到64条差分功耗曲线，找到其中峰值最高的一条曲线，其对应的猜测值k就应该是正确密钥。

(8) 以上步骤分别针对8个S盒进行攻击，可破解全部48 bit子密钥，根据子密钥生成算法，可以推导出56 bit密钥中的48 bit，剩下的8 bit可通过简单的穷举攻击破解。

以上的区分函数只考虑了最常见的寄存器翻转，也就是汉明距离模型，也可以对寄存器状态进行攻击，即汉明重量模型，还可以对S盒输出的状态进行攻击。但是在同等条件下，区分函数选择寄存器翻转的攻击效果最好。

攻击首轮的方法与尾轮类似，本文不再赘述。

3 预计算掩码法

最早的针对DES的预计算造表掩码法是由Akkar等人[15]提出的。算法通过引入掩码随机数，改变S盒的结构来达到掩盖真实数据的目的。后由于存在叠加攻击，经过作者的不断改进加以完善[16]，提出了所谓的UMM掩码方案：

给定任一32 bit值α，定义两个基于原始S盒的新函数$S1(x)$,$S2(x)$，满足对任一$x\in[0,\ 1]^{48}$：$S1(x)$=$S(x+E(\alpha))$; $S2(x)$=$S(x)$ +$P^1(\alpha)$。f_{K_i}是E扩展、密钥异或、S盒及P置换的组合；f_{1,K_i}是用$S1(x)$代替原始S盒；f_{2,K_i}是用$S2(x)$代替原始S盒。定义了5种轮函数，如图3所示。

DES的加密过程为$(\text{BCDCDCE})_{\alpha 1}$(BCDCDCDCE)$_{\alpha 2}$或$(\text{BCE})_{\alpha 1}$AAAAAAAAAA$(\text{BCE})_{\alpha 2}$。这两种加密过程中第2轮的S盒输出均为真实值

$$\begin{aligned}&S(E(P(S(K_1\oplus E(\text{IP}(M)_{32-63})))\oplus \text{IP}(M)_{0-31}\\&\quad\oplus\alpha_1)\oplus K_2\oplus E(\alpha_1))\\&=S(\underline{E(P(S(K_1\oplus E(\text{IP}(M)_{32-63}))))\oplus K_2}\\&\quad\oplus E(\text{IP}(M)_{0-31}))\end{aligned}\tag{1}$$

可以被选择明文攻击，攻击流程如下：

(1) 选择不同的特殊明文M，即固定$\text{IP}(M)_{32-63}$为M_A，而对$\text{IP}(M)_{0-31}$进行随机。猜下划线部分的6 bit值，利用功耗分析攻击可以得到

$$\theta_A=K_2\oplus E(P(S(K_1\oplus E(M_A))))\tag{2}$$

(2) 选择不同的特殊明文M，即固定$\text{IP}(M)_{32-63}$为M_B，而对$\text{IP}(M)_{0-31}$进行随机。猜下划线部分的6 bit值，利用功耗分析攻击可以得到

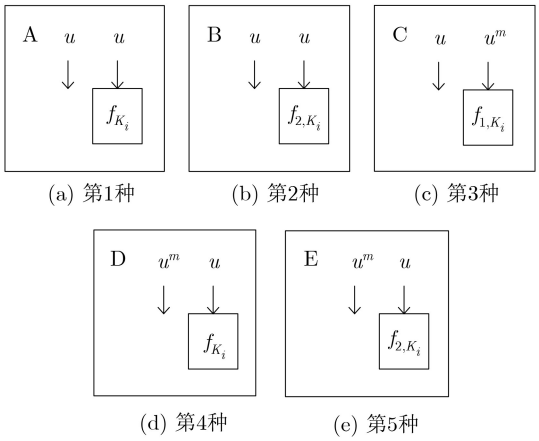
$$\theta_B=K_2\oplus E(P(S(K_1\oplus E(M_B))))\tag{3}$$

(3) 把式(2)和式(3)进行异或运算，可以得到

$$\begin{aligned}&S(K_1\oplus E(M_A))\oplus S(K_1\oplus E(M_B))\\&\quad=P^{-1}(E^{-1}(\theta_A\oplus\theta_B))\end{aligned}\tag{4}$$

(4) 求解式(4)可以得到K_1，平均每个S盒可以得到4个不同的K_1值。对8个S盒重复上述过程，最后需要穷举猜测$4^8\times2^8=2^{24}$种可能的key值。

因此Akkar等人在文献[17]又对UMM掩码方案进行了改进：定义函数$S3(x)$，满足对任一$x\in[0,$



(a) 第1种 (b) 第2种 (c) 第3种

(d) 第4种 (e) 第5种

图 3 5种不同的轮函数

1][48]: $S3(x+E(\alpha))=S(x)+P^{1}(\alpha)$。$f_{3,K_i}$是用$S3(x)$代替原始S盒，并使用$f_{3,Ki}$来掩码第2轮运算。

不幸的是，该方案仍然可以被选择明文的2阶功耗分析所攻击[18]。此时第2轮S盒输出的值为

$$\begin{aligned}&S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63})))\\&\quad\oplus\mathrm{IP}(M)_{0-31}\oplus\alpha_1)\oplus K_2)\\&=S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\\&\quad\oplus E(\mathrm{IP}(M)_{0-31})\oplus E(\alpha_1)\oplus K_2)\\&=S(E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\\&\quad\oplus K_2\oplus E(\mathrm{IP}(M)_{0-31}))\oplus P^{-1}(\alpha_1)\end{aligned}\tag{5}$$

第1轮S盒输出的值为

$$S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))\oplus P^{-1}(\alpha_1)\tag{6}$$

式(5)和式(6)异或以后，可以削去掩码，得到

$$\begin{aligned}\hat{T}=&S(\underline{E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\oplus K_2}\\&\oplus E(\mathrm{IP}(M)_{0-31}))\oplus S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))\end{aligned}\tag{7}$$

注意到，给定K_1，且选取明文使得低32 bit固定不变，则$S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))$是固定不变的。因此可以针对$S(\underline{E(P(S(K_1\oplus E(\mathrm{IP}(M)_{32-63}))))\oplus K_2}\oplus E(\mathrm{IP}(M)_{0-31}))$进行分类。

具体攻击流程如下：

(1)选择不同的特殊明文M，即固定$\mathrm{IP}(M)_{32-63}$为M_A，而对$\mathrm{IP}(M)_{0-31}$进行随机。猜下划线部分的6 bit值，利用功耗分析攻击可以得到

$$\theta_A=K_2\oplus E(P(S(K_1\oplus E(M_A))))\tag{8}$$

(2) 选择不同的特殊明文M，即固定$\mathrm{IP}(M)_{32-63}$为M_B，而对$\mathrm{IP}(M)_{0-31}$进行随机。猜下划线部分的6 bit值，利用功耗分析攻击可以得到

$$\theta_B=K_2\oplus E(P(S(K_1\oplus E(M_B))))\tag{9}$$

(3) 把式(8)和式(9)进行异或运算，可以得到

$$\begin{aligned}&S(K_1\oplus E(M_A))\oplus S(K_1\oplus E(M_B))\\&\quad=P^{-1}(E^{-1}(\theta_A\oplus\theta_B))\end{aligned}\tag{10}$$

(4) 求解式(10)可以得到K_1，平均每个S盒可以得到4个不同的K_1值。对8个S盒重复上述过程，最后需要穷举猜测$4^8\times2^8=2^{24}$种可能的key值。

基于之前的攻击经验，文献[18]认为要想构造一个安全的DES，需要满足以下5点：

(1)关键的中间值需要被掩码；

(2)第1轮和第16轮的S盒输出的异或值需要被掩码；

(3)第1、第2轮(或第15、第16轮)的S盒输出的异或值需要被掩码；

(4) 第2轮和第16轮(或第1、第15轮)的S盒输出的异或值需要被掩码；

(5) 第1、第2、第16轮(或第1、第15、第16轮)的S盒输出的异或值需要被掩码。

因此，提出了用3个随机数来预计算6组不同的带掩码S盒，记为$\overline{S}(x)$，其中每一轮所使用的$\overline{S}(x)$如式(11)所示

$$\left.\begin{aligned}&\text{Round }1,6,11,12:\ \overline{S}(x)=S(x)\oplus P^{-1}(X_1)\\&\text{Round }2,5,10,13:\ \overline{S}(x\oplus E(X_1))=S(x)\oplus P^{-1}(X_2)\\&\text{Round }3,4:\ \overline{S}(x\oplus E(X_2))=S(x)\oplus P^{-1}(X_1\oplus X_2)\\&\text{Round }7,16:\ \overline{S}(x)=S(x)\oplus P^{-1}(X_3)\\&\text{Round }8,15:\ \overline{S}(x\oplus E(X_3))=S(x)\oplus P^{-1}(X_2)\\&\text{Round }9,14:\ \overline{S}(x\oplus E(X_2))=S(x)\oplus P^{-1}(X_1\oplus X_3)\end{aligned}\right\}\tag{11}$$

虽然该方案每一轮的S盒输出都带有掩码，且首尾几轮相互之间无法抵消，可以抵御之前的所有功耗攻击，但是仔细观察会发现，第1轮的S盒输入是明文，轮密钥直接参与了异或运算，在某些情况下也是可以被极性DPA攻击的[23]，存在一定的安全隐患。另外，该方案需要每次计算DES之前都要预计算出6组掩码S盒，需要$6\times8\times2^6\times4$ bit=1536 Byte的存储空间，在资源受限的智能卡芯片中可能会存在问题。

4　循环掩码法

4.1　掩码方案

基于以上考虑，本文提出的循环掩码法本质上也是一种预计算掩码方案，只用4个随机数，只造4组表，和之前的预计算掩码方案一样，在预计算新的掩码S盒时已经考虑到了寄存器上的掩码更新问题，结构简单，不需考虑延时泄漏问题，理论上可防所有的1阶功耗攻击。

具体方案流程如图4所示。其中，P为明文输入，C为密文输出。F_1, F_2, …, F_{16}为每一轮计算使用的F函数，所使用的S盒只有4种：S_1, S_2, S_3, S_4，每轮使用情况为

$$\left.\begin{aligned}&\text{Round }1,5,9,13:\ S_1(x)=S(x\oplus E(X_0))\\&\quad\oplus P^{-1}(X_1\oplus X_3)\\&\text{Round }2,6,10,14:\ S_2(x)=S(x\oplus E(X_1))\\&\quad\oplus P^{-1}(X_2\oplus X_0)\\&\text{Round }3,7,11,15:\ S_3(x)=S(x\oplus E(X_2))\\&\quad\oplus P^{-1}(X_3\oplus X_1)\\&\text{Round }4,8,12,16:\ S_4(x)=S(x\oplus E(X_3))\\&\quad\oplus P^{-1}(X_0\oplus X_2)\end{aligned}\right\}\tag{12}$$

由于以上的掩码方案为每4轮一个循环，因此可称之为循环掩码。相较于之前的掩码方案，只需要每次计算DES之前预计算出4组掩码S盒，不仅存储空间($4\times8\times2^6\times4$ bit=1 kByte)大大减少，预计算的时间也相应减少了。

4.2　安全性分析

通过上述技术方案，在整个DES加密处理过程

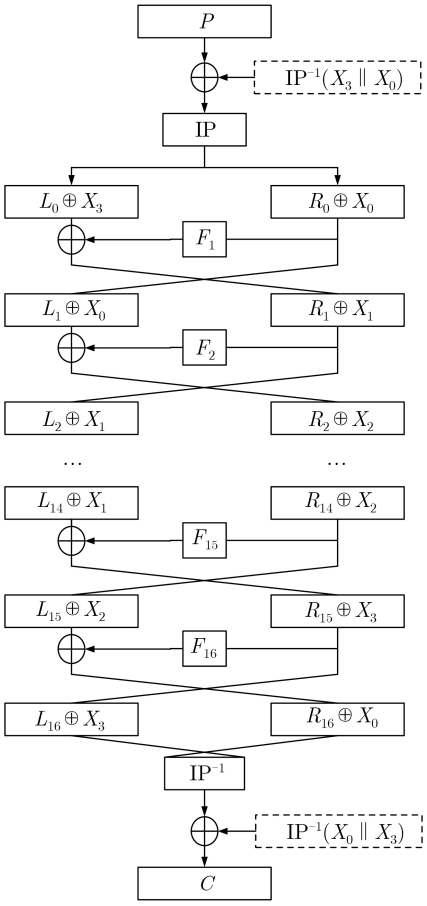


图 4 循环掩码方案

中，所有中间数据都是带有掩码的，也就是说，所述中间数据都是以密文形式存在，因此安全性相对较高，可以抗功耗分析攻击。

本文的DES循环掩码，关于S盒输出满足了以下4点：

(1) 掩码在明文输入以后即被加入，因此所有的中间值均被掩码。

(2) 第1轮和第16轮的S盒输出的异或值被掩码。

(3) 第1、第2轮(或第15、第16轮)的S盒输出的异或值被掩码。

(4) 第1、第2、第16轮(或第1、第15、第16轮)的S盒输出的异或值被掩码。

关于轮寄存器输出满足了以下5点：

(1) 掩码在明文输入以后即被加入，因此所有的中间值均被掩码。

(2) 相邻两轮的寄存器输出的异或值被掩码。

(3) 第2轮和第16轮(或第1、第15轮)的寄存器输出的异或值被掩码。

(4) 第1、第2、第15、第16轮的寄存器输出的异或值被掩码。

需要注意的是由于造表的循环使用，第2轮和第16轮的S盒输出带有相同的掩码。如第3节所述，虽然普通的2阶功耗攻击对其不构成威胁，可是选择明文的2阶功耗分析理论上可以，但由于相对于轮寄存器的翻转，S盒输出的信噪比都较低，一般很难对其进行2阶攻击。另外也可以采用8个S盒的循环掩码方案从根本上解决该问题，但是所需的存储空间是现在的2倍，同时预计算的时间也会相应地增加到两倍。

另外，由于轮寄存器上的中间数据只有1个掩码，因此理论上可以对其进行2阶功耗分析。为此可以将掩码拆分来进行防护。

5 实验分析

5.1 实验平台

本文利用日本AIST的RCIS小组所研发SASEBO-GII评估板进行安全性评估实验，该评估板在学术界获得广泛认可且并大量使用，其中搭载着两块FPGA芯片：SpartanXC3S400A作为控制芯片，负责与计算机进行通讯以及对其他模块进行控制；Virtex-5 LX50作为密码电路的计算芯片，具有强大的计算性能。如图5所示。

在实验过程中，将带有循环掩码法防护的DES电路下载到V5芯片中，并在Spartan芯片中加入了控制逻辑，同时提供了伪随机数作为掩码。本文采用了32 bit线性反馈移位寄存器来生产伪随机数。

功耗采集通过SMA电缆连接SASEBO-GII的J2接口和LeCroy示波器WaveRunner625Zi完成，电路工作频率为2 MHz，采集频率为1 GHz。数据采集完成后在荷兰Riscure的Inspector平台上做了对齐、重采样的数据预处理，并做进一步的攻击实验。

5.2 攻击结果

为了保证该防护方案的安全性，其中主要采用的攻击模型主要包括以下6种:

(1) 对于S盒输出的数据采用汉明重量模型，即计算S盒的输出数据的汉明重量与功耗曲线的相关性。

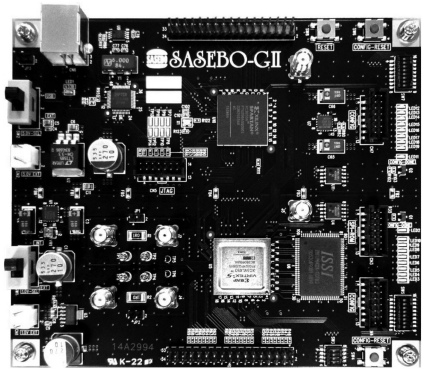


图 5 SASEBO-GII开发板

(2) 对于轮计算结果采用汉明重量模型，即计算本轮寄存器数据的汉明重量与功耗曲线的相关性。

(3) 对于轮计算结果采用汉明距离模型，即计算相邻两轮寄存器数据的汉明距离与功耗曲线的相关性。

(4) 对于第1轮和第16轮的S盒输出的汉明距离模型，即计算第1轮和第16轮S盒输出数据的汉明距离与运算后功耗曲线的相关性。

(5) 对于第1轮和第2轮的S盒输出的汉明距离模型，即计算第1轮和第2轮S盒输出数据的汉明距离与运算后功耗曲线的相关性。

(6) 对于第2轮和第16轮的寄存器输出(或S盒输出)的汉明距离模型，即计算第2轮和第16轮寄存器输出(或S盒输出)数据的汉明距离与运算后功耗曲线的相关性。

本实验中首先采集了10^6次DES随机明文加密的功耗曲线，并对其首轮和尾轮分别进行了以上前3种攻击模型的安全性测试，如图6和图7所示，选择阴影区域进行分析。

最终根据计算出的相关系数，无法区分出正确密钥及错误密钥。说明采用本文防护方案的DES实现方案可以有效防护1阶功耗分析攻击。再对其首轮和尾轮进行了第4种攻击模型的安全性测试，仍然无法区分出正确密钥及错误密钥，说明本方案可以有效防护前文所述的叠加攻击，即首尾轮的2阶功耗分析攻击。

接下来重新采集了10^6次DES选择明文加密的功耗曲线，对其进行了第5种和第6种攻击模型的安全性测试，仍然无法区分出正确密钥及错误密钥，说明本方案可以有效防护选择明文的2阶功耗分析攻击。

基于以上实验分析，相比于文献[17,18]，本方案不仅硬件实现需要的存储空间更小，还可提供更高的安全性。详细对比情况如表1所示。

6　结论

对于针对DES实现的功耗攻击，可以通过加入掩码来进行防护。本文提出了一种新的适用于DES的循环掩码方案，通过构造可循环使用的掩码

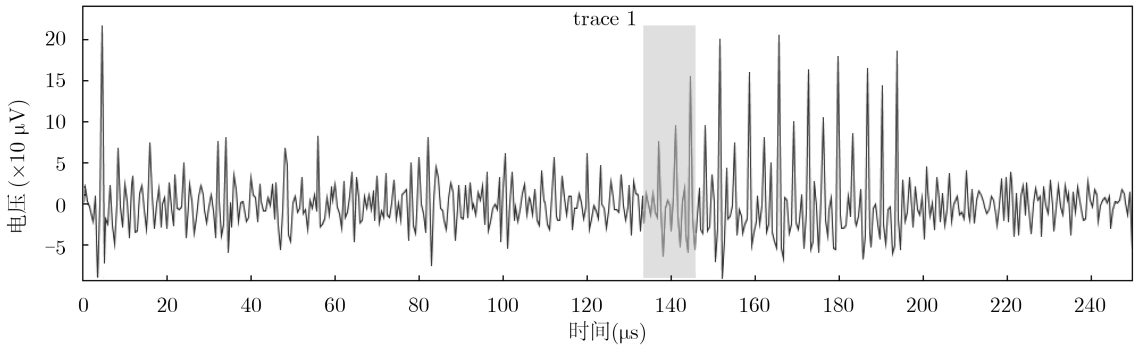


图 6 DES的首轮攻击位置

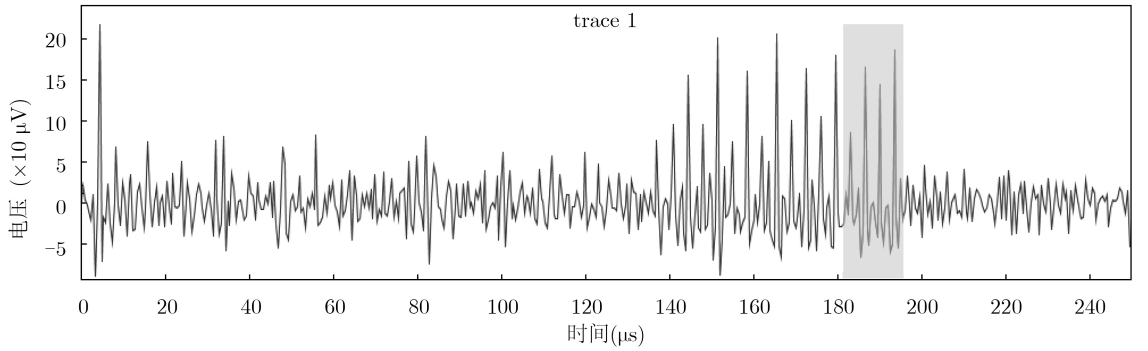


图 7 DES的尾轮攻击位置

表 1　不同方案的详细比较

方案	存储空间(Byte)	预计算时间(clk)	安全风险
文献[17]方案	1536	384	极性DPA，选择明文的2阶攻击
文献[18]方案	1536	384	极性DPA
本文方案	1024	256	无

S盒，不仅使预计算量大大减少，而且整个DES运算过程的中间数据都是带有掩码的，可以防护1阶功耗攻击和叠加攻击。进一步地，通过拆分掩码，该方案还可以抵御2阶攻击。该方案同时考虑了安全性和性能开销，是一种轻量级掩码方案，对其它类似加密算法的防护也具有重要借鉴意义。

参 考 文 献

[1] KOCHER P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]. The 16th Annual International Cryptology Conference, Santa Barbara, USA, 1996: 104–113. doi: 10.1007/3-540-68697-5_9.

[2] KOCHER P C, JAFFE J, and JUN B. Differential power analysis[C]. The 19th Annual International Cryptology Conference, Santa Barbara, USA, 1999: 388–397. doi: 10.1007/3-540-48405-1_25.

[3] RENAULD M and STANDAERT F X. Algebraic side-channel attacks[C]. The 5th International Conference on Information Security and Cryptology, Beijing, China, 2010: 393–410. doi: 10.1007/978-3-642-16342-5_29.

[4] TIRI K, AKMAL M, and VERBAUWHEDE I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards[C]. The 28th European Solid-State Circuits Conference, Florence, Italy, 2002: 403–406.

[5] TIRI K and VERBAUWHEDE I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation[C]. Design, Automation and Test in Europe Conference and Exhibition, Paris, France, 2004: 246–251. doi: 10.1109/DATE.2004.1268856.

[6] GUILLEY S, FLAMENT F, HOOGVORST P, *et al*. Secured CAD back-end flow for power-analysis-resistant cryptoprocessors[J]. *IEEE Design & Test of Computers*, 2007, 24(6): 546–555. doi: 10.1109/MDT.2007.202.

[7] 乐大珩, 李少青, 张民选. 基于LBDL逻辑的抗DPA攻击电路设计方法[J]. 国防科技大学学报, 2009, 31(6): 18–24. doi: 10.3969/j.issn.1001-2486.2009.06.004.

YUE Daheng, LI Shaoqing, and ZHANG Minxuan. An LBDL based VLSI design method to counteract DPA attacks[J]. *Journal of National University of Defense Technology*, 2009, 31(6): 18–24. doi: 10.3969/j.issn.1001-2486.2009.06.004.

[8] YANG Shengqi, WOLF W, VIJAYKRISHNAN N *et al*. Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach[C]. The Conference on Design, Automation and Test in Europe, Munich, Germany, 2005: 64–69. doi: 10.1109/DATE.2005.241.

[9] CORON J S and KIZHVATOV I. An efficient method for random delay generation in embedded software[C]. The 11th International Workshop on Cryptographic Hardware and Embedded Systems, Lausanne, Switzerland, 2009: 156–170. doi: 10.1007/978-3-642-04138-9_12.

[10] CORON J S. Resistance against differential power analysis for elliptic curve cryptosystems[C]. The 1st International Workshop on Cryptographic Hardware and Embedded Systems, Worcester, USA, 1999: 292–302. doi: 10.1007/3-540-48059-5_25.

[11] 黄海, 冯新新, 刘红雨, 等. 基于随机加法链的高级加密标准抗侧信道攻击对策[J]. 电子与信息学报, 2019, 41(2): 348–354. doi: 10.11999/JEIT171211.

HUANG Hai, FENG Xinxin, LIU Hongyu, *et al*. Random addition-chain based countermeasure against side-channel attack for advanced encryption standard[J]. *Journal of Electronics & Information Technology*, 2019, 41(2): 348–354. doi: 10.11999/JEIT171211.

[12] 汪鹏君, 张跃军, 张学龙. 防御差分功耗分析攻击技术研究[J]. 电子与信息学报, 2012, 34(11): 2774–2784. doi: 10.3724/SP.J.1146.2012.00555.

WANG Pengjun, ZHANG Yuejun, and ZHANG Xuelong. Research of differential power analysis countermeasures[J]. *Journal of Electronics & Information Technology*, 2012, 34(11): 2774–2784. doi: 10.3724/SP.J.1146.2012.00555.

[13] GOUBIN L and PATARIN J. DES and differential power analysis the “duplication” method[C]. The 1st International Workshop on Cryptographic Hardware and Embedded Systems, Worcester, USA, 1999: 158–172. doi: 10.1007/3-540-48059-5_15.

[14] STANDAERT F X, ROUVROY G, and QUISQUATER J J. FPGA implementations of the DES and triple-DES masked against power analysis attacks[C]. 2006 International Conference on Field Programmable Logic and Applications, Madrid, Spain, 2006: 1–4. doi: 10.1109/FPL.2006.311315.

[15] AKKAR M L and GIRAUD C. An implementation of DES and AES, secure against some attacks[C]. The 3rd International Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, 2001: 309–318. doi: 10.1007/3-540-44709-1_26.

[16] AKKAR M L and GOUBIN L. A generic protection against high-order differential power analysis[C]. The 10th International Workshop on Fast Software Encryption, Lund, Sweden, 2003: 192–205. doi: 10.1007/978-3-540-39887-5_15.

[17] AKKAR M L, BÉVAN R, and GOUBIN L. Two power analysis attacks against one-mask methods[C]. The 11th International Workshop on Fast Software Encryption,

Delhi, India, 2004: 332–347. doi: 10.1007/978-3-540-25937-4_21.

[18] LÜ Jiqiang and HAN Yongfei. Enhanced DES implementation secure against high-order differential power analysis in smartcards[C]. The 10th Australasian Conference on Information Security and Privacy, Brisbane, Australia, 2005: 195–206. doi: 10.1007/11506157_17.

[19] PROUFF E and RIVAIN M. A generic method for secure SBox implementation[C]. The 8th International Workshop on Information Security Applications, Jeju Island, Korea, 2007: 227–244. doi: 10.1007/978-3-540-77535-5_17.

[20] RIVAIN M, DOTTAX E, and PROUFF E. Block ciphers implementations provably secure against second order side channel analysis[C]. The 15th International Workshop on Fast Software Encryption, Lausanne, Switzerland, 2008: 127–143. doi: 10.1007/978-3-540-71039-4_8.

[21] ITOH K, TAKENAKA M, and TORII N. DPA countermeasure based on the “masking method”[C]. The 4th International Conference on Information Security and Cryptology—ICISC 2001, Seoul, Korea, 2002: 440–456. doi: 10.1007/3-540-45861-1_33.

[22] MAGHREBI H, GUILLEY S, and DANGER J L. Leakage squeezing countermeasure against high-order attacks[C]. The 5th IFIP International Workshop on Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, Heraklion, Greece, 2011: 208–223. doi: 10.1007/978-3-642-21040-2_14.

[23] TANG Ming, QIU Zhenlong, GAO Si *et al*. Polar differential power attacks and evaluation[J]. *Science China Information Sciences*, 2012, 55(7): 1588–1604. doi: 10.1007/s11432-012-4588-5.

王立辉：男，1982年生，博士，高级工程师，研究方向为密码芯片安全设计.

闫守礼：男，1972年生，硕士，工程师，研究方向为密码芯片安全设计.

李　清：女，1968年生，硕士，教授级高级工程师，研究方向为密码芯片安全设计.

责任编辑：马秀强