doi: 10.7690/bgzdh.2013.02.013

一种针对 DES 密码芯片的 M-DEMA 攻击方法

柏代军[1]，范黎恒[1]，余浩[2]
（1. 总装重庆军代局，重庆 400060；2. 军械工程学院计算机工程系，石家庄 050003）

摘要：为探究电磁信号泄漏的秘密信息，将多比特差分电磁分析（M-DEMA）应用于密码芯片的电磁旁路攻击。在分析 CMOS 电路直接电磁辐射机理的基础上，设计并搭建了 DES 微控制器（AT89C52）密码系统的近场电磁辐射信号采集与分析平台。在详细阐释 M-DEMA 攻击方法的同时，完成了针对该密码系统的攻击实验及实验效果分析，实验结果表明该方法是有效的，与传统 DEMA 方法相比，该方法能用更少的样本成功恢复 DES 密码芯片的密钥，并能提高攻击成功率。

关键词：密码芯片；差分电磁分析；近场；电磁辐射；数据加密标准
中图分类号：TJ02　　**文献标志码：**A

M-DEMA Attack Method for DES Code Chip

Bai Daijun[1], Fan Liheng[1], Yu Hao[2]
(1. *Military Representative Bureau of General Armament Department in Chongqing, Chongqing* 400060, *China*;
2. *Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang* 050003, *China*)

Abstract: In order to research for secret information leakage by electromagnetic signal, use multiple-bit differential electromagnetic analysis (M-DEMA) is applied to side channel attacks (SCA) in code chip. Based on analysis the principle of direct electromagnetic radiations for complementary metal-oxide-semiconductor (CMOS) circuit. A near-field electromagnetism radiations signals acquisition and analysis platform of DES microcontroller (AT89C52) code system is designed and constructed. Introduce M-DEMA attack method in detail, realize the attack test and test results analysis. The experimental results show that the method is effective, compared with conventional DEMA method, this method can use less traces successfully extract the secret key of DES cryptographic device, and can improve the success rate of attacks.

Key words: code chip; M-DEMA; near-field; electromagnetism radiations; DES

0 引言

在旁路攻击领域中，目前研究最为广泛，成果最为突出的当属功耗分析攻击[1](power analysis attacks)，它是利用密码设备在进行密码运算时产生的功耗信息，来推导出运算中的秘密参量。然而，在针对嵌入式密码芯片进行功耗攻击时，由于实际电路中设置的一些解耦电容以及电路中其他电子元器件对电路板内电流变化的额外作用，往往很难测量核心部件的功率消耗，即使获取到功耗信号，由于信号中包含的是整个电路中所有元器件的功耗泄漏，还需将密码运算核心部件产生的功耗与其它大量辅助部件产生的功耗进行逻辑上的剥离，这也是非常困难的。此外，如果密码设备采用内置电源方式，甚至会使得功耗分析攻击变得不可行。

电磁分析攻击又称电磁辐射攻击，是通过测量密码芯片在运算期间发射的电磁信号，依据电磁场与内部处理数据之间的相关性而获取内部秘密参量。电磁分析攻击[2]分为简单电磁分析（simple electro magnetic analysis，SEMA）攻击和差分电磁分析（differential electro magnetic analysis，DEMA）攻击。电磁分析攻击在大多数情况下无需分解密码系统设备和改动电路，并且通常密码系统的电磁辐射泄漏信息更为丰富，获取较为容易，其应用前景也更为广阔；因此，笔者以 AT89C52 微控制器 DES 密码系统为实验原型，参考传统 DEMA[3]攻击方法，提出选取多比特位中间值构造分割函数，借助均值差分统计方法，完成多比特差分电磁分析（Multiple-bit DEMA，M-DEMA）攻击，最终获取 DES 密码芯片的密钥。

1 CMOS 电路电磁辐射机理

当前，超大规模集成电路（very large scale integration，VLSI）芯片中应用最多的是互补金属氧化物半导体（complementary metal oxide semiconductor，CMOS）技术，它被广泛运用在微控制器以及其他数字逻辑电路中。对 CMOS 电路而言，电磁辐射源自于控制、I/O、数据处理或器件其他部

收稿日期：2012-08-29；修回日期：2012-09-13
基金项目：国家自然科学基金（60940019）；河北省自然科学基金（F2012506008）资助
作者简介：柏代军（1969—），男，四川人，工学硕士，高级工程师，从事信息安全研究。

分的电流，按照类型常将其分为直接辐射与间接辐射[4]。对直接辐射，电磁场的特性取决于辐射源、源周围的介质和源到观测点的距离，根据距辐射源的远近，其相应的辐射区域分别称作近场和远场。文中实验所获电磁信号为芯片的近场电磁辐射。

根据电磁场理论[5]，导体上存在随时间变化的电荷和电流时，它的周围就有随时间变化的电场和磁场。电场和磁场是一个不可分割的整体，它们相互联系、相互激发组成一个统一的电磁场。电磁场间的相互作用，在一定的条件下离开导体向远处运动，形成向自由空间传播的电磁波，被称为电磁辐射。CMOS 数字电路的基本组成单元是反相器，如图 1 所示，反相器可以看作是一个推拉开关：输入接地时切断下面的晶体管，产生高电平输出。高电平输入时刚好相反，将输出接地拉到低电平。当一个比特位从 0 翻转到 1，或者从 1 翻转到 0 同样成立，反相器的 NMOS 管和 PMOS 管会导通一小段时间，这就导致一个从 V_{DD} 到 V_{SS} 的短暂的电流脉冲，而这个在 CMOS 门的输出变化时产生的电流会在芯片周围产生一个变化的电磁场，这个变化的电磁场可以用感应探头检测到。

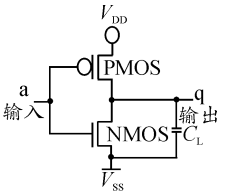

图 1 反相器原理

根据楞次定律，变化的磁场将在闭合导体中产生电流，探头中的感应电动势取决于磁通量的变化率，其表示如下：

$$V=\oint_s \boldsymbol{E}\cdot\mathrm{d}\boldsymbol{l}=-\frac{\mathrm{d}\boldsymbol{\Phi}_B}{\mathrm{d}t}=-\frac{\mathrm{d}(\oint_A \boldsymbol{B}\cdot\mathrm{d}\boldsymbol{A})}{\mathrm{d}t} \tag{1}$$

其中：V 表示探的输出电压；$\boldsymbol{\Phi}_B$ 表示探头感应的磁通量；t 表示时间；$\boldsymbol{B}$ 表示磁场；而 $\boldsymbol{A}$ 表示磁力线穿透的区域面积。基于安培定理的麦克斯韦方程将磁场的产生表示如下：

$$\boldsymbol{\nabla}\times\boldsymbol{B}=\mu\boldsymbol{J}+\varepsilon\mu\frac{\delta\boldsymbol{E}}{\delta t} \tag{2}$$

其中：$\boldsymbol{J}$ 表示电流密度；$\boldsymbol{E}$ 表示电场；ε 表示电导率；μ 表示磁导率。式 (1) 和式 (2) 说明探头的输出电压 V 与电流密度 $\boldsymbol{J}$ 和电场 $\boldsymbol{E}$ 成正比，也就是和翻转的晶体管数量成正比，即在一定时间内通过物理旁路泄漏的数据取决于该时间内从一个状态到另一个状态的翻转数[6]。

2 密码系统平台设计与搭建

数据加密标准(data encryption standard，DES)是典型的对称密钥算法，使用 56 位有效密钥将 64 位的明文输入经过一系列变换得到 64 位的密文输出。解密使用相同的步骤和相同的密钥，详细的 DES 算法描述可见文献[7]，其第一轮的加密过程如图 2。

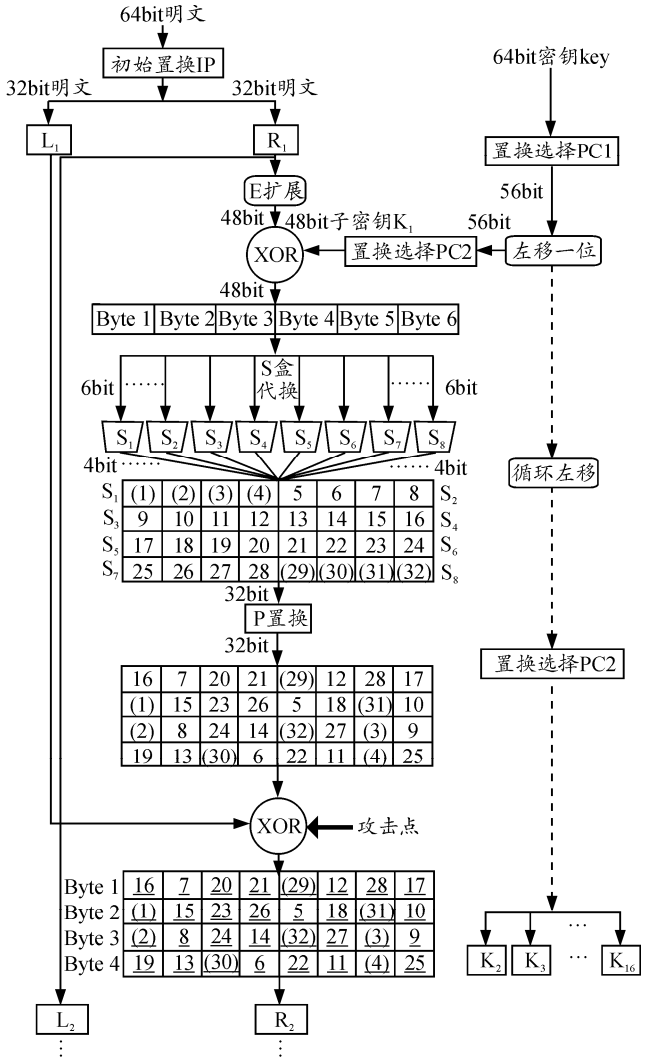

图 2 DES 第一轮的加密过程

差分电磁分析攻击需要采集大量样本来完成统计分析，笔者搭建微控制器 DES 密码系统的电磁采集、分析平台如图 3 所示。平台由微控制器 DES 密码系统、示波器(Tektronix DPO4032)、稳压电源、近场电磁探头(RF-R 400-1 磁场探头)、放大器(PA303，放大倍数 30 dB)及计算机组成。其工作过程为：电磁探头将接收到的电磁信号传送给示波器进行采集，并通过 USB 传输到 PC 机存储(随机明文与加密返回的密文也被同步存储)；示波器的采集过程由 PC 机上用 LabView 编写的虚拟仪器控制平台实现自动控制；在采集数据完成以后，在 PC 机

上用C++和Matlab编写的信号处理与分析软件进行数据分析，从而获取密钥。

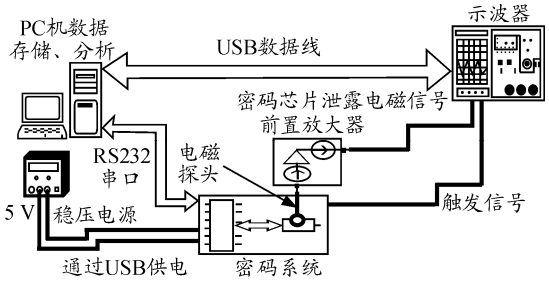

图 3　微控制器密码系统采集与分析平台

3　M-DEMA 攻击方法

以 DES 算法为例，M-DEMA 攻击方法步骤为：

1) 基于目标器件的密码算法运算过程中，选择一个可计算的、依赖于密钥的中间值函数作为 DPA 攻击的攻击点，如图 2 所示，可表示为 $H(f, k)=d$，其中 $H()$是一个确定函数，f 是已知非常量明文，k 是子密钥或者猜测密钥，d 是对应的可能子密钥所计算的假设中间值，即：$d=H(f, k)$。

2) 计算中间值。对要攻击的每一 S 盒 6 比特子密钥值 k 进行猜测，将猜测值记为矢量 $\boldsymbol{k}=(k_1,\cdots,k_i,\cdots,k_K)$，$i\in(1,\cdots,K)$，对 6 比特子密钥值进行猜测共有 64 种情况，即 K=64。针对每一种猜测，可计算出其所对应的假设中间值。

3) 对采集的大量电磁信号曲线进行分组。采用汉明模型[8]，对每个猜测密钥 k_i，选择一个分割函数来对实际采得的电磁信号进行分组，其原则为：根据假设中间值 d 的多个比特位的汉明距离的和值与阈值 Value 的大小关系，将基于采样时间点 j 的电磁信号曲线分为 3 组，可记为 S_0、S_1 和 S_2，其中 N 为所采明文数量，t_i 为对应于第 i 个明文的电磁信号曲线。

$$\begin{cases} S_0=\{\mathrm{t}_i[j]\mid D(.)<\mathrm{value}/2,\ 1\leqslant i\leqslant N\} \\ S_1=\{\mathrm{t}_i[j]\mid D(.)>\mathrm{value}/2,\ 1\leqslant i\leqslant N\} \\ S_2=\{\mathrm{t}_i[j]\mid D(.)=\mathrm{value}/2,\ 1\leqslant i\leqslant N\} \end{cases} \tag{3}$$

4) 求电磁信号曲线均值差。对每一猜测密钥，计算子集合 S_0 与 S_1 平均值，并进行差分，由式 (4) 计算。

$$\begin{cases} A_0[j]=\dfrac{1}{|S_0|}\sum_{t_i[j]\in S_0}t_i[j],\quad A_1[j]=\dfrac{1}{|S_1|}\sum_{t_i[j]\in S_1}t_i[j] \\ T[j]=A_0[j]-A_1[j] \end{cases} \tag{4}$$

根据 2 组信号曲线的均值差曲线是否出现尖峰，判断猜测密钥的正确与否，即猜测正确的密钥对应的差分曲线会出现尖峰，猜测错误密钥对应的差分曲线无明显尖峰出现。据此，可得出某一 S 盒所对应的 6 比特子密钥值，其他 7 个 S 盒的子密钥可同理得出，共得到 48 位有效子密钥。最后，通过强力攻击对剩余的 8 位子密钥进行穷举获取。

4　攻击实验及结果分析

如图 2 所示，以 DES 密码算法的第一轮进行攻击，由于 AT89C52 微控制器采用的是 8 位总线预充电结构串行工作模式，其电磁辐射能量依赖于总线上数据的汉明重量，因此只需考虑相关比特位的汉明重量(此时汉明距离可简化为汉明重量)来进行电磁信号曲线集合的划分。根据 M-DEMA 分析方法，笔者基于攻击点(异或操作)后的输出把电磁信号曲线分为 3 组，阈值 Value=4。

S_0 包含基于异或操作输出中汉明重量的和值较小的电磁信号曲线集合，即 $D(.)<2$；S_1 包含基于异或操作输出中汉明重量的和值较大的电磁信号曲线集合，即 $D(.)>2$；S_2 为剩余的电磁信号曲线集合，即 $D(.)=2$。

这样，所有电磁信号曲线几乎平分到了这 3 个组中，敌手仅仅利用 S_1 与 S_0 就能得到最大的差分电磁曲线结果，与此同时 S_2 中包含的电磁信号曲线被舍弃。

图 4、图 5 所示为对 DES 中 S_1 盒进行 M-DEMA 攻击后的情况图，分别列出了正确猜测子密钥(也即是真实子密钥)及错误猜测子密钥所对应的差分电磁曲线。由图 4、5 可以观察到，在正确猜测子密钥对应的电磁差分曲线上出现了明显的尖峰，而错误猜测子密钥对应的差分曲线则趋于平缓。

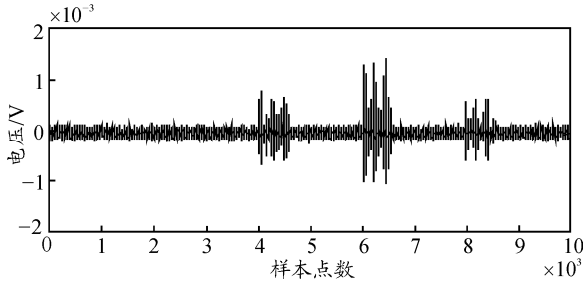

图 4　S_1 盒正确子密钥对应的 M-DEMA 攻击曲线

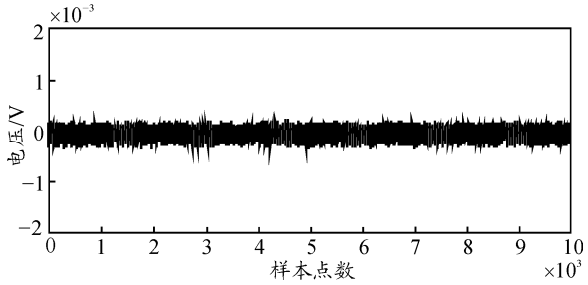

图 5　S_1 盒错误子密钥对应的 M-DEMA 攻击曲线

(下转第 54 页)