数据加密标准的相关电磁分析

丁国良 赵 强 张政保 杨素敏

(军械工程学院计算机工程系 石家庄 050003)

摘 要 分析了CMOS逻辑门电路在运行时的电流特征,阐明了集成电路中数据与电磁辐射的相关性,建立了寄存器级电磁信息泄漏汉明距离模型。通过针对P89C668单片机实现的DES密码系统的攻击实验,介绍了相关电磁分析(Correlation Electromagnetic Analysis,CEMA)算法的设计与实现,分析了攻击点D的选择和计算方法,成功获得了DES第16轮48位子密钥,验证了电磁信息泄漏汉明距离模型。实验结果表明,工作状态下的CMOS集成电路存在电磁信息泄漏现象,相关分析比差分攻击更有效,DES每一轮的异或操作可以成为攻击点,为密码系统实施相关防护措施提供了依据。

关键词 相关电磁分析,电磁信息泄漏,数据相关性,数据加密标准,旁路攻击

中图法分类号 TP309.7 **文献标识码** A

Research on Correlation Electromagnetic Analysis for DES

DING Guo-liang ZHAO Qiang ZHANG Zheng-bao YANG Su-min

(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract The article analyzed the CMOS logical gate's electric current characteristic under the active status, explained data and electromagnetic emissions correlation of ICs, established the electromagnetic information leakage hamming distance model in registers level. Aimed at the data encryption standard (DES) cryptographic system realized by the P89C668 microcomputer, correlation electromagnetic analysis (CEMA) algorithm was described, the choice of attack point D and the computational method were analyzed, an attack experiment was processed by CEMA, thereby which made us obtain 48-bit sub-key of the 16th round of DES. The result shows that EM information leakage exists in CMOS integrated circuit during work, XOR operation in each round of DES is an attack point. The correlation analysis is more effective than the differential attack. It can provide a basis for implementing protective measures in the cryptographic systems.

Keywords CEMA, EM information leakage, Data correlation, DES, SCAs

1 引言

旁路攻击(Side Channel Attacks,SCAs)是一种利用密码设备在工作期间自身产生的物理信号。它是通过统计方法分析其中的泄漏信息而获取敏感数据的密码分析技术,已对信息安全提出了严重的挑战。旁路攻击技术根据统计方法的不同,除了Paul Kocher提出的差分功耗分析(Differential Power Analysis,DPA)[1]外,主要还有Eric Brier等人提出的相关功耗分析方法(Correlation Power Analysis,CPA)[2]。根据攻击手段不同又可分为功耗攻击[3]、电磁攻击[4]和计时攻击等。由于电磁泄漏的信息丰富,因此利用电磁攻击已成为该领域研究的热点。

本文针对PHILIPS P89C668单片机实现的DES密码系统采用相关电磁分析(Correlation Electromagnetic Analysis,CEMA)的方法,在2500组样本量的情况下,用时约58min获得了DES第16轮加密的48位子密钥。实验结果表明,CMOS集成电路在工作时确实存在电磁信息泄漏现象。比较而言,相关分析比差分分析所需样本数量较少,且能有效避免奇异峰值现象的发生,密钥的破译更为高效和精确。同时采用电磁攻击方法无需分解设备和改动电路,具有更强的实用性和攻击能力。

2 集成电路电磁信息泄漏分析

2.1 集成电路电磁辐射

目前大规模数字集成电路主要由CMOS门电路实现。在CMOS器件中,操作对象为数字信号,所有操作都是在时钟的控制下进行的,每个时钟上升沿或下降沿触发各部件动作,使之逻辑状态发生变化。以CMOS反向器为例,典型的输入和输出电压波形以及负载电容、电流波形如图1所示。

到稿日期:2008-10-31 返修日期:2009-01-21 本文受国家高技术研究发展计划(863)(2007AA01Z454),国家自然科学基金(60571037)资助。

丁国良(1968-),男,副教授,主要研究方向为嵌入式系统及信息安全,E-mail:DGL998@163.com;赵 强(1945-),男,教授,主要研究方向为信息安全;张政保(1965-),男,教授,主要研究方向为网络与信息安全;杨素敏(1971-),女,博士,主要研究方向为网络与信息安全。

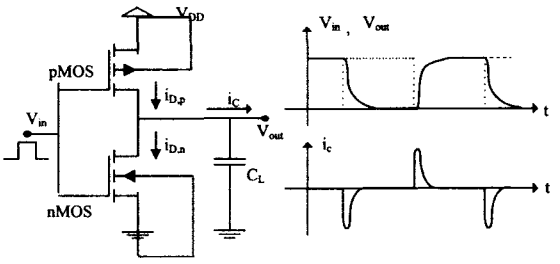

图 1 CMOS反向器开关过程输入输出电压和电容电流波形

由于数字集成电路芯片的开关特性，其工作电流一般为瞬态脉冲电流形式。电流的大小是输出电压的函数[5]，可表示为 $i_c=i_{D,p}-i_{D,n}=C_L\frac{dV_{out}}{dt}$。

根据电磁场理论，时变电流是产生辐射电磁场的源[6]。因此，数字集成电路在工作状态下会产生大量的电磁辐射信号，特别是与数据操作有关的控制器、运算器和总线等部件，这些部件在时钟信号控制下，其状态变化取决于运算、操作对象以及运算结果，这些状态信息和电磁辐射信号之间存在着一定的联系。利用这种相关性，通过分析两者之间的关系，就可能获得其中的数据，从而造成敏感信息的泄漏。

2.2 电磁信息泄漏汉明距离模型

Eric Brier 等人针对静态 CMOS 门电路的功耗与门电路状态变化过程的关系提出了汉明距离模型[2]。该模型假定 CMOS 门电路发生翻转时，状态由低变高和由高变低有能量消耗，且耗能相同，而由低变低和由高变高时 CMOS 门无能量消耗，因此 CMOS 门电路的电能消耗与状态翻转变化可用汉明距离描述，即 $E=aH(x\oplus x')+b$。其中 x 为门电路的先前状态，x' 为后来状态，E 为从 x 转换至 x' 过程的电能消耗，$H(x\oplus x')$ 为两状态间的汉明距离，a 为电能消耗比例系数，b 为与所处理数据不相关的电能消耗及噪声。由于电磁辐射的能量是整个 CMOS 门电路能耗的重要组成部分，且与之成正比，因此可将该模型推广至电磁辐射模型。

引理 1 对于 n 位处理器，寄存器 D 的数值可记为 $D=\sum_{i=0}^{n-1}d_i2^i$，$d_i\in\{0,1\}$，汉明重量记为 $H(D)=\sum_{i=0}^{n-1}d_i$，$d_i\in\{0,1\}$，其中 d_i 为寄存器 D 中第 $i+1$ 位的值。

定义 1 对于寄存器 D 在一次运算过程中产生的电磁辐射能量，可用寄存器中原始操作数和运算结果之间的汉明距离描述，其能量大小可表示为

$$E=aH(D\oplus D')+b \tag{1}$$

在这个电磁信息泄漏汉明距离模型中，D 和 D' 为寄存器 D 运算前后的状态，也就是原始操作数和结果，$H(D\oplus D')$ 为原始操作数与运算结果之间的汉明距离，E 表示为该运算产生的电磁辐射能量。以异或操作为例，该操作在寄存器 D 中产生的结果是 $D'=D\oplus R$，其中保存变量 D 的目的寄存器 D 可能发生翻转，而保存变量 R 的寄存器并不发生变化，则异或操作产生的电磁辐射能量可以用寄存器 D 运算前后的汉明距离 $H(D\oplus D')$ 描述。

3 电磁相关性分析

根据上述的电磁信息泄漏汉明距离模型，在寄存器一级，密码系统的电磁辐射能量与相关运算数据之间存在着线性关系，因此可以将运算数据作为被猜测密钥通过相关系数计算估计两者的相关程度，相关程度越高者则更有可能为密钥。

引理 2 对于 n 位处理器，当寄存器 D 的值为独立随机变量时，其中每一位 d_i 的数学期望为 $E(d_i)=1/2$，方差为 $\sigma^2(d_i)=1/4$，其汉明重量的数学期望为 $E(H(D))=n/2$，方差为 $\sigma^2(H(D))=n/4$。

假设寄存器 D 的真实值为 D，猜测值为 D'，猜测值与真实值之间差异位的数量为 m，m 可表述为 $m=H(D\oplus D')$。当寄存器 D 与另一寄存器 R 进行运算时，用猜测值 D' 去估计真实值 D，其接近程度可用两者的相关系数 $\rho_{HH'}$ 评价[2]：

$$\rho_{HH'}=\frac{\mathrm{cov}(H,H')}{\sigma_H\sigma_{H'}}=\frac{n-2m}{n},0\leqslant m\leqslant n \tag{2}$$

其中，寄存器 D 的数值和汉明重量的表示方法同引理 1。H 和 H' 分别表示 $D\oplus R$ 和 $D'\oplus R$ 的汉明重量，可表示为 $H=H_{n-m}+H_m$，$H'=H'_{n-m}+H'_m=H_{n-m}-H_m+m$。$H_{n-m}$ 和 H'_{n-m} 相等且表示 $D\oplus R$ 和 $D'\oplus R$ 的相同部分的汉明重量。H_m 和 H'_m 表示 $D\oplus R$ 和 $D'\oplus R$ 的不相同部分的汉明重量，并有 $|H'_m-H_m|=m$ 的关系。

证明：由协方差定义可得

$$\begin{aligned}\mathrm{cov}(H,H')&=\mathrm{cov}(H,H'-m)\\&=\mathrm{cov}(H_{n-m}+H_m,H_{n-m}-H_m)\\&=E((H_{n-m}+H_m)(H_{n-m}-H_m))-E(H_{n-m}+H_m)E(H_{n-m}-H_m)\\&=E(H_{n-m}^2)-E(H_m^2))-E^2(H_{n-m})+E^2(H_m)\end{aligned}$$

根据引理 2 及方差性质，可得

$$\rho_{HH'}=\frac{\mathrm{cov}(H,H')}{\sigma_H\sigma_{H'}}=\frac{n-2m}{n},0\leqslant m\leqslant n$$

如果要根据电磁辐射能量判断密钥，则需要计算实际电磁辐射能量与被猜测密钥之间的相关系数 $\rho_{EH'}$，可表示为

$$\rho_{EH'}=\frac{\mathrm{cov}(E,H')}{\sigma_E\sigma_{H'}}$$

根据电磁信息泄漏汉明距离模型及式(2)，则有

$$\rho_{EH'}=\frac{\mathrm{cov}(E,H')}{\sigma_E\sigma_{H'}}=\frac{\mathrm{cov}(aH+b,H')}{\sigma_E\sigma_{H'}}=\rho_{EH}\rho_{HH'}$$

从上式可以看出，ρ_{EH} 是电磁辐射能量与真实值之间的相关系数，为一固定值。因此 $\rho_{EH'}$ 值的大小取决于 $\rho_{HH'}$，而 $\rho_{HH'}$ 与 m 成反比，且 $-1\leqslant\rho_{HH'}\leqslant1$。当 $m\to0$ 时，$\rho_{HH'}\to1$，相关系数 $\rho_{EH'}$ 越大，则说明猜测值与实际值越接近，因此可以分析出参与运算的密钥。在实际计算时，$\rho_{EH'}$ 表示为如下形式[2]：

$$\rho_{EH'}=\frac{N\sum E_iH_i'-\sum E_i\sum H_i'}{\sqrt{N\sum E_i^2-(\sum E_i)^2}\sqrt{N\sum H_i'^2-(\sum H_i')^2}} \tag{3}$$

其中，N 为输入随机明文加密的次数，E_i 为第 i 次加密过程中采集的电磁辐射信号($1\leqslant i\leqslant N$)，H_i' 为第 i 次加密过程中猜测的密钥值参与运算后的汉明重量。由于在 N 次加密过程中，输入的明文为随机数，因此采集的电磁辐射信号可以认为是随机信号，其数学期望可用 N 次采样信号的平均值表示。

4 攻击实验与结果分析

4.1 实验装置

本实验攻击的对象为 PHILIPS P89C668 单片机构成的最小系统，其上运行 DES 密码算法[7]。电磁信号采集传感器采用 Langer EMV-Technik 公司的近场探头 RF-R400，测量

时水平放置于被测 CPU 上方约 0.5cm 处。数据采集装置为泰克 DPO4104 存储式数字示波器，采样深度设置为 100000 点，采样频率 250MSa/s。整个采集过程及分析均在 PC 机的控制下完成。攻击时，PC 机随机生成 N 组 64 位二进制明文，通过串口传至单片机系统。单片机收到明文后，运行 DES 加密程序，对明文进行加密。同时，单片机触发示波器开始采集信号。示波器通过近场探头 RF-R400 获取电磁辐射信号并保存在自身的存储器中。采集完成后，通过 USB 将数据上传至 PC。每次加密完成后，单片机将加密产生的 64 位二进制密文传送至 PC 机。PC 机在整个攻击过程中共获得 N 组一一对应的明文、密文和在加密过程中采集的电磁辐射信号。

4.2 攻击点的选择和计算

攻击点 D 的选择和计算是相关性分析的关键。一方面，D 要与密钥相关，因为只有相关，才能利用加密过程产生的电磁辐射信号分析出密钥。同时，D 点计算产生的值 H 是进行相关统计的依据，只有当密钥猜测正确，由密文和密钥反推出的 H' 才能计算正确，所计算的相关系数 $\rho_{EH'}$ 才能最大。

为此，在 DES 加密第 16 轮中选择异或运算作为攻击点 D，攻击点 D 的位置如图 2 所示。由于密文已知，反向计算逆初始变换可得 R_{16} 和 L_{16}，由 $R_{16}=L_{15}\oplus f(R_{15},K_{16})$，则有

$$L_{15}=R_{16}\oplus f(R_{15},K_{16})$$

可令 H 值为 R_{16} 与 L_{15} 异或之后的汉明距离，则有

$$H=H(R_{16}\oplus L_{15})=H(R_{16}\oplus R_{16}\oplus f(R_{15},K_{16}))$$

因此，$H=H(f(R_{15},K_{16}))$

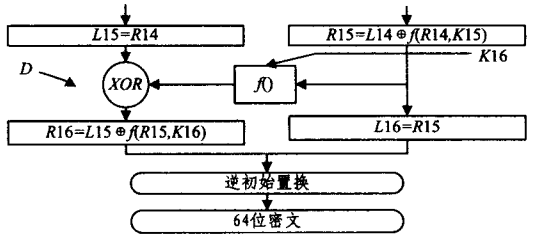

图 2 CEMA 攻击 DES 的攻击点选择和计算

$f(R_{15},K_{16})$ 计算过程如图 3 所示。R_{15} 可由密文反推得到，K_{16} 就是要破译的密钥。根据 8 个 S 盒的计算特点，首先取 K_{16} 中 6 位子密钥块（记为 K_{16}^6，其猜测值记为 K_{16}^{6*}）作为被攻击对象，与 R_{15} 中对应 6 位（记为 R_{15}^6）经 E 扩展置换、S 盒变换和 P 置换等运算后得到 $f(R_{15}^6,K_{16}^{6*})$，则可得到 $H_4'=H(f(R_{15}^6,K_{16}^{6*}))$。攻击完第一个子密钥块后，依次攻击其它子密钥块，即可得到第 16 轮的全部 48 位密钥 K_{16}。

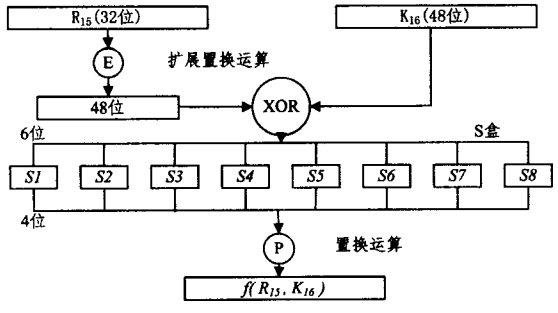

图 3 DES 的 f()函数的计算过程

CEMA 算法描述如下。

步骤 1 首先进行 N 次加密运算，经采样获取 N 条电磁辐射信号曲线：

(1)产生 N 个随机的明文 PT_i，$1\leqslant i\leqslant N$；

(2)对每一次加密运算过程进行采样，得到离散化电磁辐射曲线数组 $E_i[j]$，其中 $1\leqslant i\leqslant N$，j 表示采样的时间点；

(3)同时得到对应明文 PT_i 加密产生的密文 CT_i，$(1\leqslant i\leqslant N)$；

(4)计算式(3)中的 $\sqrt{N\sum E_i^2-(\sum E_i)^2}$ 项；

步骤 2 令子密钥块 $K_{16}^{6*}=0$，$(K_{16}^{6*}\leqslant 63)$，计算 H_4'；

步骤 3 计算式(3)得到 $\rho_{EH'}$；

步骤 4 令 $K_{16}^{6*}=K_{16}^{6*}+1$，转步骤 2，循环运行直到 K_{16}^{6*} 猜测完成；

步骤 5 按上述方法计算所有的子密钥块以后，判断所有 $\rho_{EH'}$ 的大小，从而得到整个密钥。

4.3 实验结果及分析

实验中，共采集电磁辐射信号样本量 2500 组，采样时间约 50min，分析时间约 8min。攻击目标为 DES 算法第 16 轮的 K_{16}，相关分析算法、攻击点的选择和计算如上所述。攻击时以 S 盒中的 6 位子密钥 K_{16}^6 为单位，猜测值从 0 至 63，依次计算与实际电磁辐射信号的相关系数。

图 4 为 S_1 盒 K_{16}^6 最大相关系数 $|\rho_{max}|$ 分布情况。可以看出在猜测值 $K_{16}^{6*}=3DH$ 时相关系数比其它猜测值都大，说明 3DH 极有可能为正确子密钥，事实也确实如此。

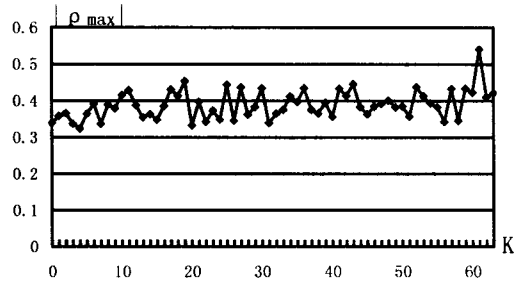

图 4 第 16 轮 S_1 盒 6 位子密钥最大相关系数

图 5 为 K_{16}^6 两个猜测值的攻击效果。A 图是 $K_{16}^{6*}=3DH$ 时相关系数计算结果，从中可以看到有明显的尖峰，最大尖峰处 $|\rho_{max}|=0.541$。而 B 图 $K_{16}^{6*}=23H$ 的 $|\rho_{max}|=0.397$。前者的 $|\rho_{max}|$ 大于后者，可认为 3DH 更有可能为正确的子密钥。其他 7 个 S 盒的攻击方法同 S_1 盒一样，也都成功猜测出了正确密钥。

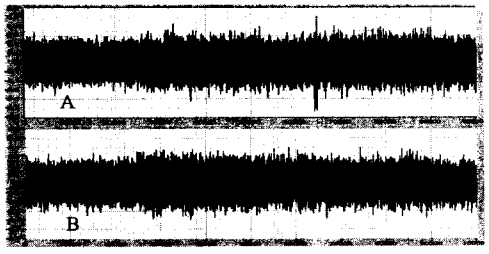

图 5 第 16 轮 S_1 盒攻击效果对比

在实验中的 DES 加密程序采用 C 语言编写，并利用 Keil-51 集成开发环境编译成 51 机器代码。第 16 轮 D 点运算为异或指令 rxtmp[0]^=lx[0]，该指令经编译变成 5 条 51 单片机的机器指令：

```
MOV  R0,#0xAF   ;L15的地址送入 R0 寄存器
MOV  A,@R0      ;L15送入 A 寄存器
```

(下转第 114 页)

低了 Web 服务匹配的搜索空间。

下一步，将进一步对该方法进行完善，其中对于抽象服务规划，由于 HTN 方法必须基于封闭世界假设(closed world assumption)，即实现动态服务组合的前提是给出完备的语义信息，当语义信息不够完备时，规划结果将不尽人意。而描述逻辑[13]在推理过程中是基于开放世界假设(open world assumption)，可以有效解决信息不完备的问题，并成为当前的一大研究热点，现拟采用描述逻辑对该部分进行进一步的研究；另外，服务接口匹配中，为了提高匹配效率，目前采用的接口匹配方法也稍显简单。为此，我们也将对该部分的方法进一步地进行完善。

参 考 文 献

[1] OASIS . Web Services Business Process Execution Language Version 2. 0[EB/OL]. [2007-4-11]. http: // docs. oasis-open. org/wsbpel/2. 0/OS/wsbpel-v2. 0-OS. html

[2] Aggarwal R, Verma K, et al. Dynamic Web Service Composition in METEOR-S[EB/OL]. [2004]. http: // Isdis. cs. uga. edu/lib/download/ IEEE-SCC-2004. pdf

[3] Wang S, Sheng W, Hao Q. Agent based workflow ontology for dynamic business process composition[C] // Proceedings of the Ninth International Conference on Computer Supported Cooperative Work in Design, 2005. New York: IEEE Press, 2005: 452-457

[4] Martin D, Burstein M, Lassila O, et al. OWL-S: S emantic Markup for Web Services [EB/OL]. [2004 -11]. http: // www. daml. org/services/owl -s/1. 1/overview/

[5] Narayanan S, McIlraith S. A Simulation, verification and automated composition of Web services[C] // Proceedings of the 11th Int'l World Wide Web Conference. Honolulu: ACM, 2002: 77-88

[6] Medjahed B, Bouguettaya A, Elmagarmid A K. Composing Web Services on the Semantic Web[J]. The VLDB Journal-The International journal on Very Large Data Bases, 2003, 12(4): 333-351

[7] Liu Jiamao, Fan Chenhui, Gu Ning. Web services automatic composition with minimal execution price Web Services[C] // Proceedings of the IEEE International Conference on Web Services. Washington DC: IEEE Computer Society, 2005: 302-309

[8] Sirin E, Parsia B, Wu D, et al. HTN planning for Web service composition using SHOP2[J]. Journal of Web Semantics, 2004, 1(4): 377-396

[9] Li M, Wang D Z, Du X Y, et al. Dynamic composition of Web services based on domain ontology[J]. Chinese Journal of Computers, 2005, 28(4): 644-650

[10] ActiveBPEL , LLC. ActiveBPEL-BPEL Execution Engine[EB/OL]. [2007-3]. http: // www. activebpel. org

[11] Martin K, Jonathan C, et al. BPEL4WS Business Processes with WebSphere Business Integration: Understanding, Modeling, Migrating [EB/OL]. [2004-12-22]. http: // www. redbooks. ibm. com/redbooks/pdfs/sg246381. pdf

[12] Nau D , Au T , Ilghami O , et al . Applications of SHOP and SHOP2[J]. IEEE Intelligent systems, 2005, 20(2): 34-41

[13] 王杰生，李舟军，李梦君. 用描述逻辑进行语义 Web 服务组合[J]. 软件学报，2008，19(4)：967-980

(上接第 102 页)

```
MOV   R1, #0xBA   ;f(R15, K16)地址送入 R1 寄存器
XRL   A, @R1      ;计算 L15⊕f(R15, K16)
MOV   @R0, A
```

通过分析指令的执行时间发现，图 5A 中 $|\rho_{max}|$尖峰出现在第 4 条异或指令 XRL 处。该指令中 A 寄存器保存有 L_{15} 的值，R1 寄存器指向的存储单元保存有 $f(R_{15}, K_{16})$的计算结果，异或运算的结果送给 A 寄存器，因此 A 寄存器的内容在异或运算前后发生了变化。$|\rho_{max}|$出现明显尖峰说明寄存器 A 中数据变化同电磁辐射能量之间存在相关性，验证了电磁信息泄漏汉明距离模型 $E=aH(D\oplus D')+b$ 能够正确反映出这种线性关系，同时也说明了 XRL 指令存在电磁信息泄漏。

在与差分攻击比较中发现，相关分析使用 2500 组数据就可全部猜测正确。而使用 1 位差分攻击虽然也能攻击成功，但需要约 3000 组才能出现尖峰，用时约 70min。此外，由于实验中相关分析算法每次同时攻击 6 位子密钥，因此在实验结果中没有发现奇异峰现象。而在 1 位差分攻击中，D 函数以 1 比特位作为攻击目标位，因此单独判读某位出现的尖峰容易造成误判。为了避免这种奇异峰值造成的误判，需要在 $f(R_{15}^6, K_{16}^6)$中的 4 位同时出现尖峰时才能判断子密钥猜测正确，这是 1 位差分攻击本身的缺陷造成的。

结束语 本文实验结果表明，大规模数字集成电路在工作过程中的瞬态脉冲电流可产生电磁辐射信号。寄存器中的数据变化与电磁辐射之间存在着线性关系，可用汉明距离描述。利用这种线性关系，通过相关性分析可以获得集成电路中的敏感数据。此外，与差分攻击相比，相关分析对集成电路密码系统进行旁路攻击需要的样本数量较少，破译更为高效和精确。而对于 DES 密码算法，每一轮的异或操作都可能成为密钥攻击点，在设计和实现中必须加以注意。

参 考 文 献

[1] Kocher P, Jaffe J, Jun B. Differential Power Analysis[C]// Proceeding of the Advances in Cryptology(CRYPTO' 99). Santa Barbara, USA, 1999

[2] Brier E, Clavier C, Olivier F. Correlation Power Analysis with a Leakage Model [C] // Proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES-2004). Boston, USA, 2004

[3] Messerges T S, Dabbish E A, Sloan R H. Investigation of power analysis attacks on smartcards[C]// Proceedings of the USENIX Workshop on Smartcard Technology. Chicago, Illinois, USA, 1999

[4] Agrawal D, Archambeault B, Rao J R, et al. The EM side-channel(s): Attacks and assessment methodologies[C] // Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems(CHES-2003). Cologne, German, 2003

[5] Kang Sung-Mo, Leblebici Y. CMOS 数字集成电路分析与设计(第 3 版)[M]. 王志功，窦建华，译. 北京：电子工业出版社，2005

[6] 孟昭敦. 电磁场导论[M]. 北京：中国电力出版社，2007

[7] Menezes A J, van Oorschot P C, et al. 应用密码学手册[M]. 胡磊，王鹏，李学俊，译. 北京：电子工业出版社，2005