DES 密码电路的抗差分功耗分析设计 *

韩 军 曾晓洋 汤庭鳌

(复旦大学专用集成电路与系统国家重点实验室, 上海 200433)

摘要: 提出一种互补结构的寄存器电路设计方案,用于减小 DES 加密电路的差分功率信号,防御差分功耗分析. 提出了一种误导攻击者的干扰电路,在保证加密电路安全等级的前提下,大幅度降低了电路的硬件开销. 为节约成本与缩短设计周期,文中使用了一套高效的抗攻击电路的设计流程.

关键词: 差分功耗分析; 互补结构; 抗攻击电路; DES

EEACC: 1265; 2570D; 6120B

中图分类号: TN492 **文献标识码**: A **文章编号**: 0253-4177(2005)08-1646-07

1 引言

随着智能卡和计算机网络的迅速发展与不断普及,信息安全问题日益突出,因此各种形式的专用密码电路和密码算法处理器被广泛地应用于各类产品中. 目前,常用的密码算法大致可以分为两类:以 DES,AES(高级加密标准)为代表的对称算法和以 RSA,ECC 为代表的非对称算法. DES[1] 是目前使用非常广泛的数据加密方法,它于 1977 年被美国国家标准局作为第 46 号联邦信息处理标准而采用.

任何安全产品或者密码系统都必须面对一个如何防御攻击和窥测的问题. 传统攻击方法是一种数学攻击手段,通过大量的数学计算来搜索密码系统的密钥. 该类攻击方法的一个直接的例子就是强力攻击(brute force attack):尝试所有可能的密钥,直至找到正确的密钥. 随着计算机性能的增强,这种方法也越来越具有可行性,但是仍需要耗费大量的时间和物力,而且如果密钥的长度增加,攻击难度则会急剧增加. 近些年来,出现了一种新的强有力的攻击方法,人们称之为旁道攻击(side-channel attack). 一个实际应用的密码系统,其硬件部件在运行过程中不可避免要泄露一些信息,诸如功耗、时间、电磁波、以及差错信息等. 利用上述信息对密码系统进行攻击和窥测已成为信息安全芯片产品的巨大威胁,其危害远远大于传统的攻击手段.

差分功耗分析(differential power analysis, DPA)就是一种极为有效的旁道攻击[2,3],它对内嵌 DES 算法的智能卡的成功攻击也被广泛报道. 关于如何抵御差分功耗分析,研究者提出了多种方案,比如增加电路噪声、数据屏蔽[4]、采取基于敏感放大器的逻辑[5]和异步逻辑[6]来设计电路等,但是这些方案需要引入额外的噪声和随机数,改变算法流程,甚至更改主流的设计逻辑. 基于差分功耗分析的基本原理和物理基础,本文提出在 DES 加密电路中设计互补电路和干扰电路来屏蔽和扰乱差分功耗分析,该方案的特点是在保证电路安全性的同时,不影响运行速度,硬件成本较小,易于实现. 将操作数转化为互补的形式,在抗差分功耗分析的软件方法中已有应用的先例[7],但是这种软件方法明显地降低微处理器的数据吞吐率,而如果将微处理器数据通路扩展一倍,那么硬件电路资源和整体功耗的浪费将极为可观,因此必须从具体的 VLSI 设计的角度来解决这一问题. 本文详细研究了应用于 DES 的互补

* 上海市重点实验室产学研基金(批准号:036511003),集成电路设计创新基金 SDC(批准号:037062016)和国家自然科学基金(批准号:90407002)资助项目

韩 军 男,1977 年出生,博士研究生,主要研究方向为信息安全芯片设计,芯片防御攻击技术.

曾晓洋 男,1972 年出生,副教授,研究方向为信息安全、密码系统电路设计和集成电路测试. Email:xyzeng@fudan.edu.cn

汤庭鳌 男,1939 年出生,教授,博士生导师,从事半导体器件、抗攻击集成电路研究.

2004-10-05 收到,2005-03-17 定稿

电路设计方法和其在 DPA 攻击下的功耗特性,并进一步提出了一种干扰电路的设计方案,在能够防御攻击的前提下降低硬件及功耗的开销. 通过对电路的仿真和分析,验证了其良好的抗攻击性能,同时本文还探索了信息安全芯片抗功耗分析设计和验证的基本流程和方法.

2　差分功耗分析的原理和物理基础

差分功耗分析能够成功攻击密码系统的前提是:加密电路的功率信号与密码系统的密钥及敏感数据存在相关性. 目前多数集成电路采用 CMOS 工艺,而 CMOS 门级电路的功耗模型可表示为

$$P_{\text{total}} = P_{\text{switch}} + P_{\text{short\_circuit}} + P_{\text{leakage}} \quad (1)$$

式中　$P_{\text{short_circuit}}$为短路电流导致的功耗; P_{leakage}为漏泄电流导致的功耗; P_{switch}为逻辑门翻转引起负载电容充放电导致的功耗,相对前两项, P_{switch}是电路功耗的主要部分.

$$P_{\text{switch}} = C_L V_{DD}^2 P_{0\to 1} f \quad (2)$$

式中　C_L 为负载电容; V_{DD}为电源电压; $P_{0\to 1}$为逻辑门发生从 0 到 1 翻转的概率; f 为输入更新的频率. 由于逻辑门功耗大小与其是否翻转密切相关,因而电路中运行的数据的 0,1 状态与电路的功率信号必然具有一定的相关性.

DES 加密电路的差分功耗分析,其基本思想是:输入若干组明文(PTI),收集相应的加密电路若干组功率信号 $S_i[j](i = 1 \sim m)$, i 表征了不同的输入明文, j 表征信号采样的时间点. 然后定义一判决方程 $D(\text{CTO}, K_b) \to \{0,1\}$, CTO 为密文, K_b 为 b 位子密钥. 依据假定的 K_b,计算方程的值将功率信号分为两类

$$S_0 = \{S_i[j] \mid D = 0\} \quad (3)$$

$$S_1 = \{S_i[j] \mid D = 1\} \quad (4)$$

令

$$T[j] = \frac{1}{|S_1|}\sum_{S_i[j]\in S_1} S_i[j] - \frac{1}{|S_0|}\sum_{S_i[j]\in S_0} S_i[j] \quad (5)$$

$$|S_0| + |S_1| = m \quad (6)$$

如果 $T[j]$出现明显的尖峰值则说明猜到了正确的子密钥(确切地说是密钥的一部分),反之则说明猜测的子密钥错误.

DES 算法的判决方程 D 如下[8]:

$$D(C_1, C_6, K_{16}) = C_1 \oplus \text{SBOX1}(C_6, K_{16}) \quad (7)$$

其运算过程可以如图 1 所示.

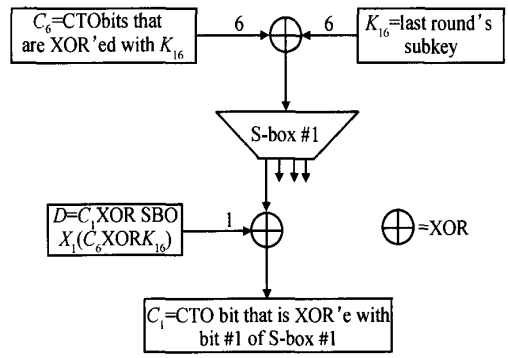

图 1　DES 判决方程示意图

Fig. 1　A partitioning function for DES

C_1 代表密文 CTO 的某一比特位, K_{16}为最后一次循环(第十六次)的子密钥进入第一个 S 盒子的六个比特位, C_6 代表 CTO 的六个比特位,其与 K_{16}相异或. 参照 DES 算法,可以发现判决方程 D 的值反映了第十五次循环加密结果的某一比特位的值. 具体地说,也就是某一时刻某一寄存器的值,因此下面首先研究电路中寄存器功率信号的统计规律.

3　寄存器功率信号分析及互补寄存器结构

考虑 n 比特的寄存器,其最初处于清零状态,在时钟上升沿对其随机赋值,记录每次赋值过程功率的变化,然后对收集的功率信号进行统计分析. 根据寄存器某一位的赋值状态(0 或 1)将记录的功率信号分为两类

$$S_0 = \{S_i[j] \mid \text{Reg} = 0\} \quad (8)$$

$$S_1 = \{S_i[j] \mid \text{Reg} = 1\} \quad (9)$$

计算 S_0 和 S_1 的平均值 $E(S_0)$ 与 $E(S_1)$,得到两者之差 $T[j]$. 根据差分功耗分析理论, $E(S_1)$ 与 $E(S_0)$ 在某一时刻必然存在明显的差异,本质原因在于寄存器赋 1 时,寄存器内部的逻辑门和与寄存器输出相连的逻辑门(负载)都发生了翻转,由于篇幅所限,本文不给出详细的理论证明,有关内容可参阅差分功耗分析的资料. 下面通过具体的 Hspice 仿真和相应的统计分析来验证这一结论. 基于 0.25μm 的 CMOS 工艺库设计一 4 位寄存器电路,每位寄存器的负载相同,都为 6 个 INVHD1X 反相器,电源电压为 3.5V. 下面是仿真和统计得到 $T[j]$的变化曲线.

如图 2 所示,在时间点 11ns 处,4 位寄存器发生赋值操作,正方形标注的曲线为按照寄存器其中 1 位的 0,1 状态分类得到的差分功率信号 $T[j]$(j 为时间点),而三角形、圆、星号标注的曲线为随机分类得到的 $T[j]$. 可见准确分类的 $T[j]$出现了明显的偏置尖峰值,而随机分类的 $T[j]$只是在零值附近出现微小波动. 差分分析能将功率信号中随机变化的因素消除,而体现电路某一部分不同状态的差异. 只要分类方法和电路的真实状态相一致,则功率差异就能体现出来,否则功率差异接近于零.

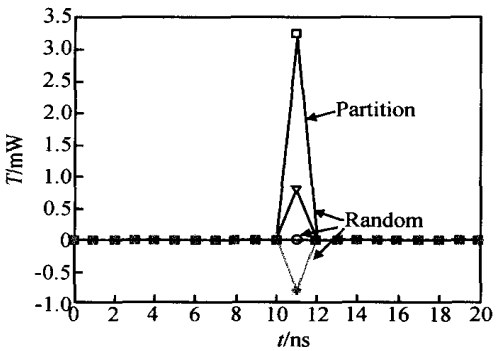

图 2 寄存器电路差分功率信号

Fig. 2 Differential power signal of register

针对差分功耗分析,有人提出增加电路噪声的防御方案[9],目的是降低差分功耗分析的信噪比,但是噪声产生电路会增加电路的功耗,而且确定防御差分功耗分析需增加多大噪声也是一个非常困难的问题. 如果采用逆向思维:努力减小差分功率信号的值,同样可以降低差分功耗分析的信噪比,若电路不同状态下的功率差异趋于零,则差分功耗分析将失效. 基于这样的思路,本文提出如图 3 所示的互补结构寄存器电路.

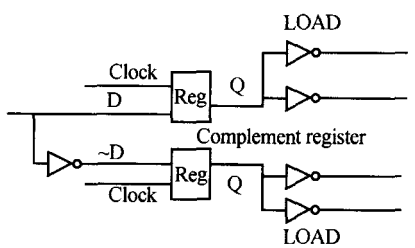

图 3 互补结构寄存器电路

Fig. 3 Complement structure for register

如图 3 所示,设寄存器初始状态相同,输出负载相同,时钟沿赋值. 可见,不论输入为 0 或是 1,两个互补寄存器必是一个翻转,另一个不翻转,因此总的功耗在两种情况下没有差别. 图 4 给出了采用互补结构的 4 位寄存器电路的仿真和统计分析结果.

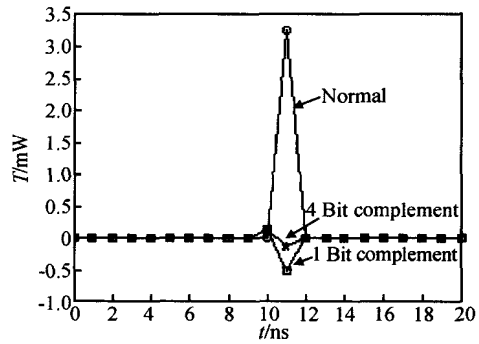

图 4 不同结构寄存器电路差分功率信号的比较

Fig. 4 Differential power signal comparison between different structures

如图 4 所示,圆形标注的曲线为普通结构 4 位寄存器电路的差分功率信号,正方形标注的曲线为 4 位中的 1 位寄存器采用互补结构时的差分功率信号,星号标注的曲线为 4 位寄存器完全采用互补结构后的差分功率信号. 与普通结构相比,互补结构能有效地减小差分功率信号,使之接近于零.

4 互补结构在 DES 密码电路中的应用

下面研究应用互补结构提高 DES 密码电路防御差分功耗分析的能力. 为便于研究且能说明问题,本文设计了一个简易的 DES 密码电路模型,主要模拟第 16 轮循环和产生加密结果的过程,其结构如图 5 所示. L15,R15,L16 和 R16 都为 4 比特寄存器,L15,R15 分别存放第 15 轮循环加密结果高 4 比特和低 4 比特,而 L16,R16 分别存放第 16 轮循环加密结果高 4 比特和低 4 比特,SK 为密钥. 电路中只有一个 S 盒子,而且省略其中一步置换操作. 运算过程的方程为

$$R16 = L15 \oplus SBOX1(R15 \oplus SK) \quad (10)$$

$$L16 = R15 \quad (11)$$

这一模型体现了 DES 密码算法的关键步骤,也是攻击者实施差分功耗分析的主要区域. 该电路设计和仿真流程为:先完成 Verilog 语言的描述,然后采用 0.25μm CMOS 工艺库进行综合,再将综合后的网表转化为 Hspice 电路,结合 0.25μm CMOS 工

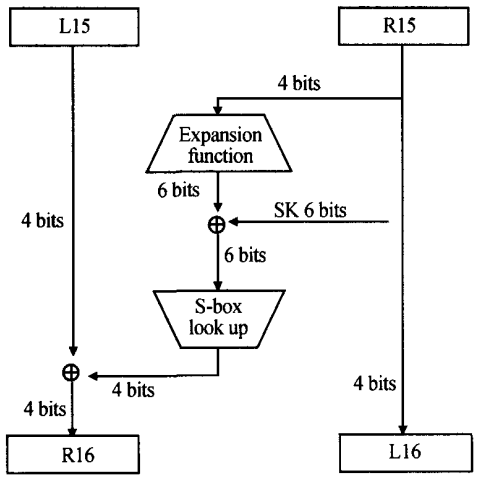

图 5　简化的 DES 电路模型

Fig. 5　Simple DES model

艺模型参数进行 Hspice 仿真,然后对仿真的功率信号完成统计分析. 这样做的优点在于:能够结合具体的工艺,电路性能十分接近于实际制造出来的电路,而在软件环境下模拟差分功耗分析过程,在流片以前就可检验它的防御攻击能力,减少了反复流片的次数,显然能缩短设计周期和减少研发费用. 因此这一设计流程可作为抗攻击设计的一种行之有效的重要途径.

本文对 L15 寄存器采用普通结构和互补结构的 DES 加密电路分别作了差分功耗分析.

图 6(a),(b)分别示出了 160 组和 200 组明文输入统计得到的电路差分功率信号(L15 寄存器为普通结构). 圆形标注的曲线为根据正确的密钥分类得到的 $T[j]$. 正方形标注的曲线为根据错误的密钥分类得到的 $T[j]$. 判决方程如(7)式所示. 由图 6(a),(b)可见,正确分类的差分功率信号与错误分类的差分功率信号相比始终具有更大的偏置峰值,差分功耗分析能够区分这两类信号,因此密钥的猜测过程也能顺利完成.

图 7(a),(b)分别示出了 160 组和 200 组明文输入统计得到的电路(L15 寄存器为互补结构)的差分功率信号. 圆形标注的曲线为根据正确的密钥分类得到的 $T[j]$. 正方形标注的曲线为根据错误的密钥分类得到的 $T[j]$. 判决方程如式(7)所示.

由图 7(a),(b)可见,正确分类的差分功率信号的值有了大幅度的减小,偏置峰值甚至能够小于错误分类的差分功率信号,两类信号已经达到难以区分的程度. 因此通过差分功耗分析对密钥进行猜测

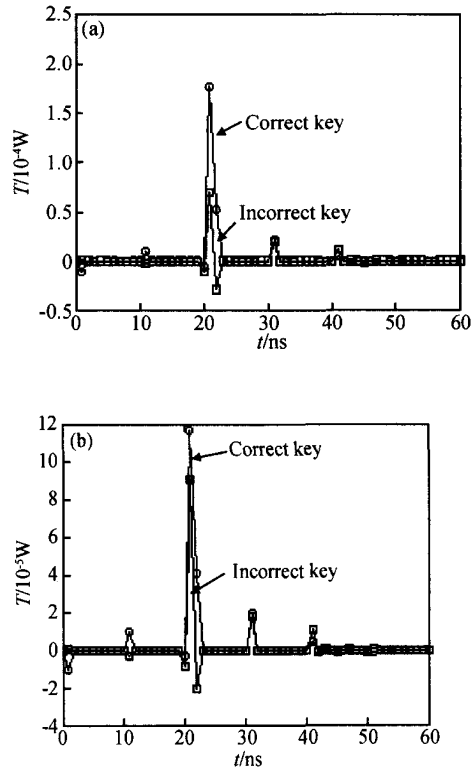

图 6　应用普通寄存器结构的 DES 电路差分功率信号　(a) 160 组样本;(b) 200 组样本

Fig. 6　Differential power signal of DES circuit with normal structure register　(a) 160 samples; (b) 200 samples

是无法进行的. 这说明 L15 寄存器采用互补结构设计能够有效地减小 DES 加密电路的差分功率信号,从而使攻击者无法通过 DPA 获取密钥.

互补结构能够提高电路的抗攻击能力,但是它也带来电路面积增大和平均功耗上升的问题. 实际的 DES 加密电路有 8 个 S 盒子,L15 寄存器也为 32 比特,如采用互补结构,需要增加 32 个寄存器以及相应的负载电路,显然这一开销不小. 综合考虑抗攻击性能和硬件开销,可以对 L15 的部分位采用互补结构,即对进入 S 盒子的 8 段密钥中的若干段进行保护. 当然如果被保护的密钥位数较少的话,攻击者可以先通过差分功耗分析获得未保护部分的密钥,然后用穷举搜索的办法对剩余密钥进行强力攻击,因此被保护的密钥位数必须足够多,使得强力攻击不可行或者不合算. 针对这个问题,下面提出另一种电路设计,可大幅度地降低电路的硬件开销,并有效防御差分功耗分析和强力攻击.

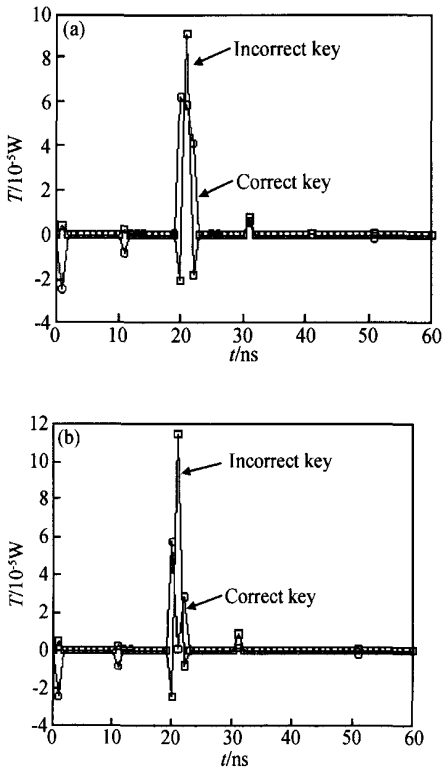

图 7 应用互补结构寄存器的 DES 电路差分功率信号 (a) 160 组样本;(b) 200 组样本

Fig. 7 Differential power signal of DES circuit with complement structure register (a) 160 samples; (b) 200 samples

5 应用干扰电路实现 DES 加密电路的抗攻击

由 DES 差分功耗分析的判决方程可知,若有一个错误的密钥 K'_{16}(进入第一个 S 盒子的 6 比特子密钥),那么可得

$$D'(C_1, C_6, K_{16}) = C_1 \oplus \mathrm{SBOX1}(C_6, K'_{16}) \tag{12}$$

显然 D 的值是不能正确反映电路中某一位寄存器的赋值状况的,因而由 D 分类得到的差分功率信号不会产生明显的偏置尖峰. 但是如果在电路中设置这样的一个一位寄存器,使得该寄存器的赋值与 D 相一致,即 Reg = D',那么根据 D 的 0,1 状态分类的差分功率信号必然出现明显的偏置尖峰. 同时对于与第一个 S 盒子的输出相异或(XOR)的 4 位寄存器采用互补结构进行保护,这样攻击者在选中正确密钥时反而无法观察到偏置尖峰,于是攻击者会认为 K'_{16} 就是正确密钥. 这样,当攻击者完成对 8 个 S 盒子的攻击后,得到的是一个错误密钥,而且攻击者也无法知道在攻击哪 6 比特子密钥时发生了错误,因此也不能进行有针对性的强力攻击以获得这一子密钥.

下面给出 Reg = D 的电路实现. 考察 DES 算法可知

$$C_1 = P_1 \oplus \mathrm{SBOX1}(C_6, K_{16}) \tag{13}$$

P_1 为第 15 轮循环加密结果的其中一个数据位,K_{16} 为正确的密钥,因此可得:

$$\begin{aligned}\mathrm{Reg} &= D' \\ &= P_1 \oplus \mathrm{SBOX1}(C_6, K_{16}) \oplus \mathrm{SBOX1}(C_6, K'_{16})\end{aligned} \tag{14}$$

该表达式很容易用组合逻辑电路实现. 电路运行时,在 P_1 存入寄存器的同时将 D' 存入 Reg. Reg 寄存器和相关的组合逻辑电路形成一个干扰电路. 下面给出添加干扰电路后 DES 加密电路的仿真和统计结果.

图 8(a),(b)分别示出 200 组明文输入按不同密钥统计得到的电路差分功率信号(添加干扰电路,且 L15 寄存器为互补结构). 图 8(a)中圆形标注的曲线为根据随机选择的密钥分类得到的 $T[j]$,正方形标注的曲线为根据干扰电路设置的错误密钥分类得到的 $T[j]$. 图 8(b)中圆形标注的曲线为根据正确的密钥分类得到的 $T[j]$,正方形标注的曲线为根据干扰电路设置的错误密钥分类得到的 $T[j]$.

由图 8(a),(b)可见,在 21ns 时间点附近(寄存器进行赋值操作),与按照正确密钥或其它随机选择的密钥进行分类得到的差分功率信号相比,按照预设的错误密钥进行分类得到的差分功率信号具有更明显的偏置尖峰,因此干扰电路能够导致攻击者发生误判. 干扰电路的设置使得只需对 4 位寄存器(与一个 S 盒子相关的)采用互补结构进行保护,而抗攻击的能力并不低于 32 位寄存器完全采用互补结构的方案.

6 结论

从防御差分功耗分析的角度出发,提出通过平衡电路不同状态的功率差异来减小攻击者获得的差分功率信号;针对 DES 密码电路的抗攻击设计,提出了一种互补结构的寄存器电路. 仿真和分析表明,改进后的电路具备了防御差分功耗分析的能力. 另外,为了降低硬件开销,同时充分保证电路的安全等

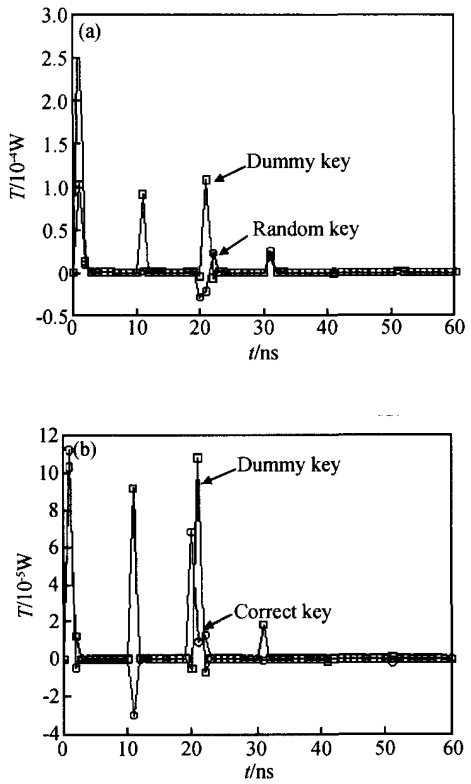

图 8　加干扰电路后 DES 电路差分功率信号　(a) 错误密钥与随机密钥; (b) 错误密钥与正确密钥

Fig. 8　Differential power signal of DES with disturbing circuit　(a) Dummy key and random key; (b) Dummy key and correct key

级,又提出了一种干扰电路设计方案. 仿真分析表明,该设计也具有良好的防御攻击能力. 本文提出的互补电路平衡功耗,干扰电路示错误导的思想可以适当推广到 AES 和 RSA, ECC 等密码电路设计中,可以对这些密码电路的算术逻辑运算单元采用互补结构进行改进,平衡其功耗信息,而干扰电路则需要结合具体的算法来进行设计. 目前各种密码系统的算术逻辑运算单元的 VLSI 设计已得到较为广泛的研究[10],而如何在其设计中实现抗攻击是值得进一步深入研究的问题.

对于抗攻击密码电路的设计,在普通数字电路的验证流程之外还必须增加对其抗攻击能力的测试,而反复流片测试会造成设计成本和周期急剧增加. 将电路设计与具体工艺参数相结合,在仿真环境下模拟差分功耗分析,对建立一套经济有效的防御攻击设计流程具有一定的普遍意义.

参考文献

[1] ANSI X9. 32-American National Standard for Data Encryption Algorithm (DEA). AM. Standards Inst, 1981

[2] Kocher P, Jaffe J, Jun B. Introduction to differential power analysis and related attacks. http://www.cryptography.com/dpa/technical

[3] Kocher P, Jaffe J, Jun B. Differential power analysis. Proceeding of Advances in cryptography (CRYPTO '99), 1999: 388

[4] Akkar M L, Christophe Giraud. An implementation of DES and AES, secure against some attacks. CHES, 2001: 309

[5] Tiri K, Verbauwhede I. Securing encryption algorithms against DPA at the logic level: next generation smart card technology. CHES, 2003: 125

[6] Fournier J J A, Moore S, Li H Y. Security evaluation of asynchronous circuits. CHES, 2003: 137

[7] Daemen J, Rijmen V. Resistance against implementation attacks: A comparative study of the AES proposals. Second Advanced Encryption Standard Candidate Conference, 1999, http://www.nist.gov/aes

[8] Messerges T S, Dabbish E A, Sloan R H. Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers, 2002, 51(5): 541

[9] Wayner P. Code breaker cracks smart cards' digital safe. New York Times, 1998, 22: C1

[10] Zhou Haohua, Li Zhiyong, Xie Wenlu, et al. A regular time-efficient VLSI architecture for multiplication modulo $2^n + 1$. Chinese Journal of Semiconductors, 2000, 21(10): 1032 (in Chinese) [周浩华,李志勇,谢文录,等. 一种规整高速的费马数模乘的 VLSI 结构. 半导体学报, 2000, 21(10): 1032]

VLSI Design of Anti-Attack DES Circuits *

Han Jun, Zeng Xiaoyang, and Tang Ting'ao

(State Key Laboratory of ASIC & System, Fudan University, Shanghai 200433, China)

Abstract: A complement register structure is proposed for a DES circuit. The structure can reduce the differential power signal of a DES circuit and lead to the failure of differential power analysis. A circuit design, which can mislead the attacker, is also presented. The circuit can ensure a high enough security level with reasonable area and power consumption. To save time and money, an effective design flow for an anti-attack circuit is also discussed.

Key words: differential power analysis; complement structure; anti-attack circuit; DES
EEACC: 1265; 2570D; 6120B
Article ID: 0253-4177(2005)08-1646-07

* Project supported by the National Natural Science Foundation of China (No. 90407002), the Key Laboratory Foundation of Shanghai (No. 036511003), and the IC Design Innovation Foundation of Shanghai (No. 037062016)

Han Jun male, was born in 1977, PhD candidate. His research interests include information security chip design and anti-attack technologies for chip.

Zeng Xiaoyang male, was born in 1972, associate professor. His research interests include VLSI design of cryptosystems, design testing, and information security. Email: xyzeng@fudan.edu.cn

Tang Ting'ao male, was born in 1939, professor. His research interests include semiconductor devices and IC design for anti-attack circuits.

Received 5 October 2004, revised manuscript received 17 March 2005