第 26 卷 第 8 期
2005 年 8 月

半 导 体 学 报
CHINESE JOURNAL OF SEMICONDUCTORS

Vol. 26 No. 8
Aug. ,2005

用于密码芯片抗功耗攻击的功耗平衡加法器*

李翔宇 孙义和

(清华大学微电子学研究所, 北京 100084)

摘要: 给出了一种用于密码芯片以提高芯片抗功耗攻击能力的"功耗平衡"加法器,它运行时工作功率与运算数据无关. 对新设计与相关原设计芯片的功率样本进行显著性检验,在样本数为 283 的情况下,前者的最低显著性水平比后者高 10 个数量级. 功耗平衡加法器比现有的采用"n 分之一"编码的抗功耗攻击加法器少 13 个以上的晶体管.

关键词: 专用集成电路设计; 数据安全; 加法器; 差分功耗攻击; 功耗平衡

EEACC: 2570D; 1265B

中图分类号: TN492 **文献标识码**: A **文章编号**: 0253-4177(2005)08-1629-06

1 引言

差分功耗攻击(DPA)是一种针对密码芯片在处理不同数据时功率变化存在的差异,通过统计方法攻破密钥信息的方法[1,2]. 减小处理不同数据时的功率分布差别是抵抗 DPA 的重要方法. 由此可引出功耗平衡电路的概念,定义如下:

定义 1:一个电路,在特定工作条件下,某种状态(包括电路内部状态和外部输入)下产生的瞬态功率曲线与另一状态下产生的瞬态功率曲线的差值的绝对值组成的曲线称为两个状态的功率差分曲线(简称功率差分曲线),差分曲线的最大值称为这两个状态的功率差分. 所有状态两两间的功率差分的最大值定义为该电路的功率差分.

定义 2:如果一个电路的功率差分为 0,称该电路是功耗平衡的.

实际情况中,往往只要一个电路具有某些给定特征的状态集合间的功率差分小于一定的值,就可以认为它是功耗平衡的.

采用功耗平衡电路处理敏感数据可使攻击者无法分辨被处理的数据,从而提高密码电路的安全性.

现有方法通过增加冗余电路或冗余操作来补偿功耗差值. 其中大部分方案是在算法级或结构级进行冗余设计. 但是,电路各个层次的不对称都会引起功率差异,因此采用这些方法的同时还要采用其他措施来掩盖底层电路的信息泄露. 更为有效的一种解决途径是采用"n 分之一"编码逻辑[3]. 但这种逻辑级的平衡措施同样不能消除门级以下层次的功率差分,普通逻辑门电路引起相同输出变化的不同输入变化之间可能存在功率差分,而且"n 分之一"编码逻辑会成倍地增加电路规模.

本文介绍的加法器从晶体管到逻辑结构综合考虑平衡电路功耗,不仅消减了电路级的功率差分,而且电路规模比已有方法的规模更小.

2 功耗平衡加法器设计

双轨编码的 DI 电路因逻辑对称实现了功耗平衡[3]. 本文给出了一种新的实现功耗平衡的 DI 超前进位加法器 PBDICLA.

设 A_{n-1},A_{n-2},…,A_0 和 B_{n-1},B_{n-2},…,B_0 是两个 n 位加数,S_{n-1},S_{n-2},…,S_0 表示和,C_n,C_{n-1},…,C_0 表示各位进位. 输入输出采用双轨编码,双轨编码的"0"线标以上角标 0,"1"线标以上角标 1. 例如: A_i^0 表示信号 A_i 的"0"线,A_i^1 表示 A_i 的"1"线. 定义位进位控制信号 K_i,P_i,G_i 依次分别表示进位消除、传递、生成信号;定义 $P_{i,k}$,$K_{i,k}$ 和 $G_{i,k}$ 依次分别表示

*国家自然科学基金资助项目(批准号:60236020)

李翔宇 男,1977 年出生,博士研究生,研究方向为密码芯片的硬件安全. Email:lixy00@mails.tsinghua.edu.cn

孙义和 男,1945 年出生,教授,博士生导师. Email:sunyh@tsinghua.edu.cn

2004-09-22 收到,2005-03-20 定稿

第 k 位到第 i 位的块进位控制信号,同一组 K_i, P_i, G_i 信号用 I_i 表示,一组 $P_{i,k}$, $K_{i,k}$, $G_{i,k}$ 用 $I_{i,k}$ 表示. 它们被统称为进位控制信号. C_i 的值是由进位控制信号 $I_{i-1,k}$ 和进位输入信号 C_k 得出的.

2.1 原先的 DI 加法器 DICLA[4]

这是一种 DI 超前进位加法器,它的进位链为树状结构. 图 1 是一个 8 位 DICLA 结构.

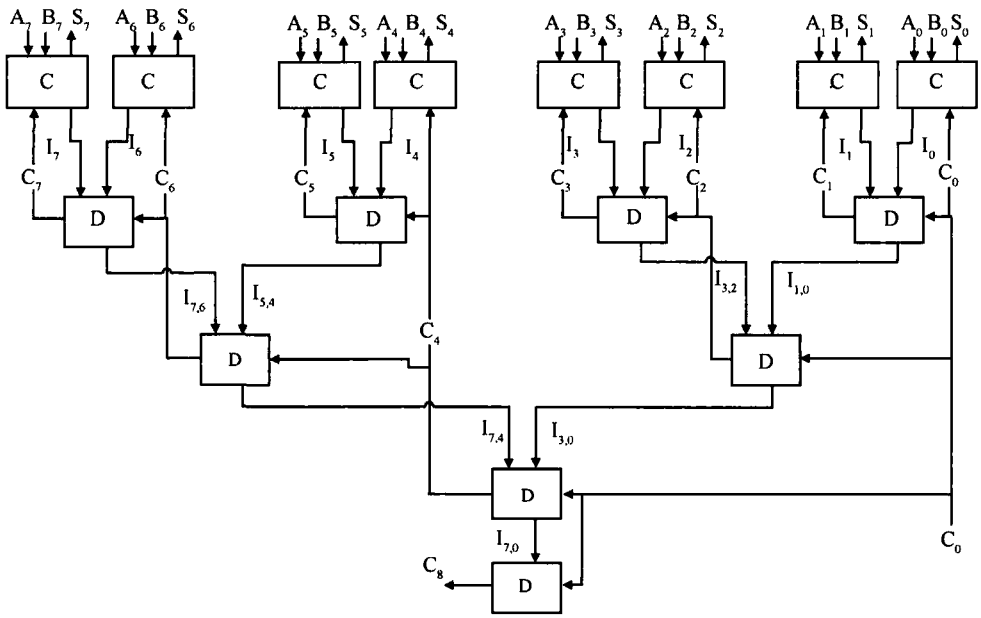

图 1 8 位 DICLA 结构图

Fig. 1 Structure of 8-bit DICLA

DICLA 共有两种基本模块,C 模块和 D 模块. C 模块实现求和和位进位控制信号的产生. D 模块组成进位链,实现块进位控制信号产生和进位计算.

此加法器产生进位信号的关键路径与加数的值有关,则相关电路节点的翻转时刻具有数据相关性,对应的功耗也具有数据相关性;况且 D 模块和 C 模块的功耗并不平衡,因此 DICLA 是一个功耗不平衡的电路.

2.2 功耗平衡加法器 PBDICLA

为了叙述方便,做如下定义:

共轭信号:如果一组信号线的取值或者同时为 0(无效状态),或者有且只有一个为 1(有效状态),则称这组信号是彼此共轭的.

显然,双轨编码的 0 线和 1 线是共轭的, K_i, P_i, G_i 和 $P_{i,k}$, $K_{i,k}$, $G_{i,k}$ 分别共轭. 一组共轭的信号线从无效变为有效时总是有且只有一个信号由 0 变 1,其余信号不翻转,从有效变为无效时也总是有且只有一个信号由 1 变 0,其余信号不翻转,如果这组信号线的负载和驱动完全相同,则它们的总翻转功耗是数据无关的.

关键信号:定义一个逻辑单元所有输入中最后到达的一个为关键信号,即只要且只有关键信号有效后电路输出才有效. 双轨编码电路只有在输入信号有效后才开始求值,所以关键信号的到达时刻决定了输出信号的翻转时刻.

2.2.1 结构

图 2 是 8 位 PBDICLA 的结构图(与图 1 不同的部分被加粗标出). DICLA 中产生 C_3, C_7 的 D 模块用进位控制的 D 模块(Dc 模块)代替. Dc 与 D 模块的进位控制信号产生电路相同,进位产生电路不同(分别用 CG 和 CGc 表示). CGc 的输出是在进位输入有效后才产生的,即其关键信号总是进位信号,与输入信号值无关.

PBDICLA 中 C_7, C_6, C_5 的产生采用了进位选择结构: C_4 作为选择信号, C_{70}, C_{60}, C_{50} 对应 $C_4 = 0$ 的结果; C_{71}, C_{61}, C_{51} 对应 $C_4 = 1$ 的结果. C_{60}, C_{61}, C_{50}, C_{51} 的关键信号变成了各自的进位产生信号,所以它们的产生时刻相对原始输入是固定的. 为了减小电路规模, C_{70}, C_{71} 和 C_3 的产生没有采用进位选

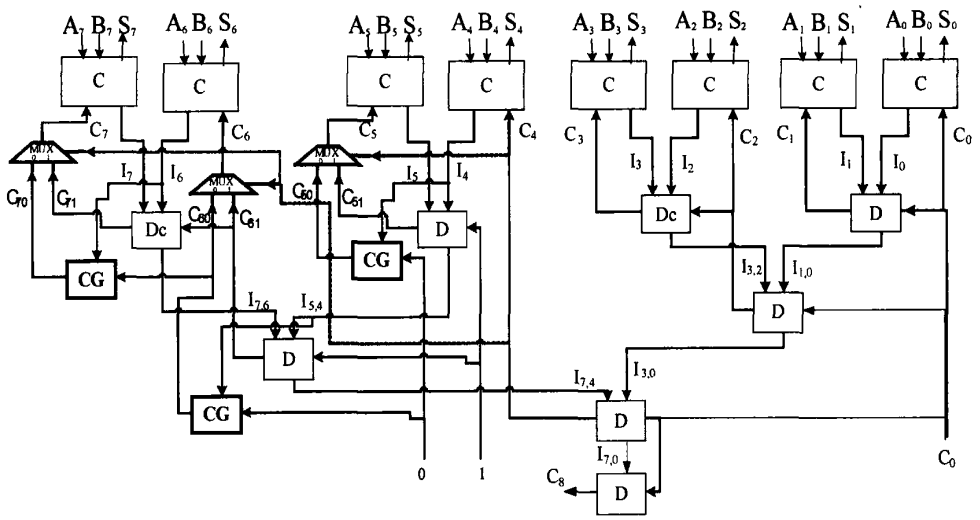

图 2　8 位 PBDICLA 结构

Fig. 2　Structure of 8-bit PBDICLA

择结构,而是由 Dc 单元产生. C_{70} ,C_{71} 和 C_3 的关键信号总是 C_{60} ,C_{61} 和 C_2 ,所以 C_{70} ,C_{71} 和 C_3 的产生时刻也是固定的. 而且由于 Dc 单元不在加法器的关键路径上,所以等待进位信号并不会减慢运算速度. PBDICLA 所有进位信号的产生时刻都是相对固定的,则以它们为关键信号的求和电路的翻转时刻也相对固定,又由于信号具有共轭性,所以每个时间步的信号翻转的总数量是数据无关的.

2.2.2　模块电路的 CMOS 实现

PBDICLA 的 C 模块和 D 模块都采用了 CMOS 交叉耦合的差分 Domino 逻辑. N 型 Domino 电路的充电部分不受输入控制,充电电流与数据无关. 交叉耦合的上拉结构用以补偿求值网络内部节点和输出端的电荷分配造成的电平下降. 图 3 是 PBDICLA 中块进位控制信号产生电路的 CMOS 实现. 其中 ϕ 是时钟,其他信号的定义与前面相同.

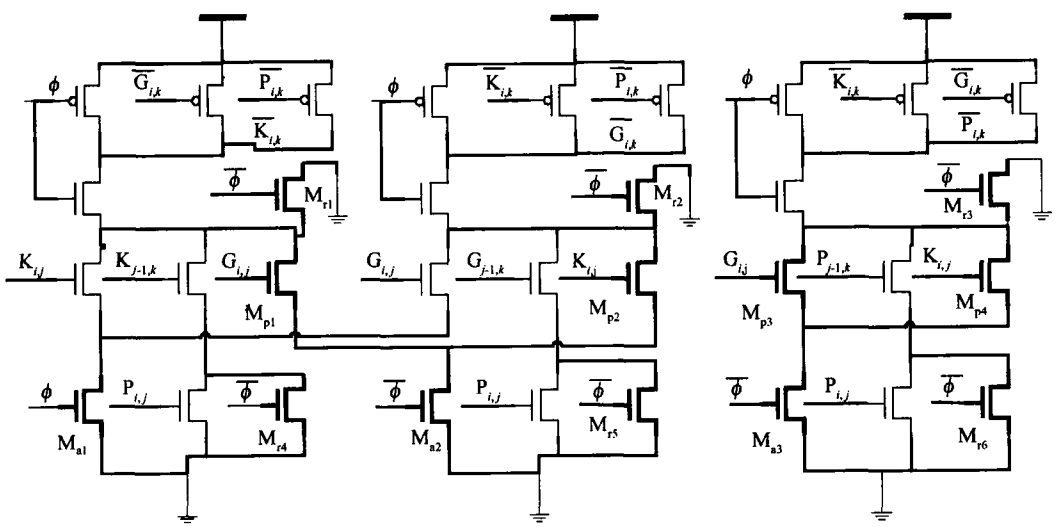

图 3　D 模块进位控制信号产生电路 CMOS 实现

Fig. 3　CMOS implementation of the carry-control signals generator in D-Module

图 3 的电路除了实现逻辑功能的器件之外,还有一些冗余晶体管(图中用粗线条表示). 它们的作用可以分成两类:

一类晶体管用于平衡负载和充放电网络,如图

3 中的 M_{p1} ,M_{p2} ,M_{p3} ,M_{p4} 以及 M_{a1} ,M_{a2} ,M_{a3} . 它们一方面使得 $K_{i,j}$,$P_{i,j}$,$G_{i,j}$ 三个输入负载相同,另一方面使电路在任何输入情况下等效的充放电 RC 网络相同,从而避免了由于 RC 网络的不同造成电容充放电电流出现差异[5]. 在版图设计中,这些对称节点采用相同的图形,共轭信号的互连线等长,以保证这些节点的电容相同.

另一类晶体管是内部节点的复位管,如图 3 中的 M_{r1} ,M_{r2} ,M_{r3} ,M_{r4} ,M_{r5} ,M_{r6} . 它们在电路的预充相位将内部节点电平置为 0. 这样可以保证每次运算开始时初始状态相同,避免了内部节点由于初始电平差异造成的功率差分.

3 流片结果

芯片采用 0. 18μm 的 CMOS 工艺(内核工作电压 1. 8V ,IO 工作电压 3. 3V). 表 1 是两种加法器的版图面积和流片测量得到的运算时间. 图 4 是 8 位 PBDICLA 和 DICLA 的芯片照片(包括各自的外围异步流水线电路).

表 1 DICLA 与 PBDICLA 的性能比较

Table 1 Performance of DICLA and PBDICLA

加法器	面积/μm ×μm	运算时间/ns
DICLA	94 ×144	1.8
PBDICLA	247 ×148	2.3

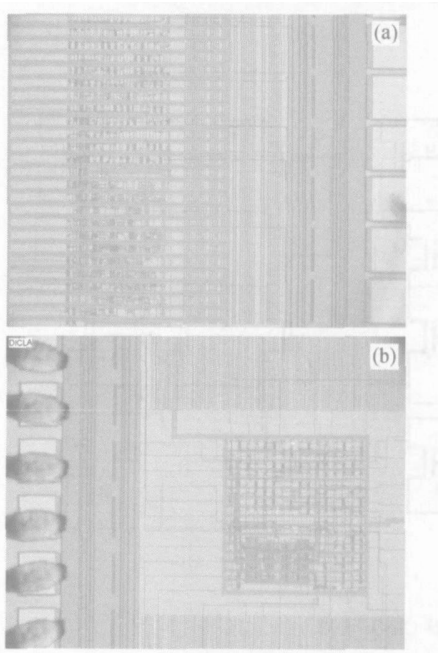

图 4 芯片内核照片 (a) PBDICLA 流水线;(b) DICLA 流水线

Fig. 4 Microphotographs of the chips (a) PBDICLA; (b) DICLA

从表中数据可知,PBDICLA 的面积大约是 DICLA 的两倍,运算时间比 DICLA 增加了将近 1/3. 这是由增加了冗余电路和保证版图中一些图形或布线的对称造成的.

3.1 抗差分功耗分析性测试

瞬态功率的测量方法是在芯片与电源间串联采样电阻,测量电阻两端电压再计算出电源电流. 为了降低信号变化速率,芯片采用低电源工作电压(1. 4V). 数据采集设备是一数字采样示波器,采样率为 2GSa/ s.

两个加法器分别运算 283 种不同的加数和进位组合,对每种输入组合重复 47 次运算,共采集到 13301 个功率波形样本.

将这些输入向量分别按照下面三种分组方式分组(冒号前是组名,冒号后是该组输入的特征):

(1) 组 A1 : A_0B_0 = 11 ,其他位随机选取,共 77 条向量;组 A2 : A_0B_0 = 00 ,其他位随机选取,共 101 条向量;组 A3 : A_0B_0 = 01 或 10 ,其他位随机选取,共 105 条向量;

(2) 组 B1 : I_1 = g 或 k *,其他位随机选取,共 181 条向量;组 B2 : I_1 = p ,其他位随机选取,共 102 条向量;

(3) 组 C1 : I_6 = g 或 k ,其他位随机选取,共 140 条向量;组 C2 : I_6 = p ,其他位随机选取,共 143 条向量.

其中分组方式 1 考察加数最低位取值对功耗的影响,能够反应 C 模块的功耗平衡情况;分组方式 2 考察块进位控制信号 I_1 对功耗的影响,反映 D 模块的功耗平衡情况;分组方式 3 考察 C_7 进位产生的关键信号对功耗的影响和 CGc 单元的功耗平衡情况.

3.2 结果分析

按照 3 种分组方式对两个芯片的功率样本分别进行显著性检验,即估计每种分组方式下的各个组两两服从相同分布的概率[2]. 采用常用的均值差值检验(t 检验):假设两个分组的样本数分别为 n_1 和 n_2 ,它们的平均功率曲线相减取绝对值得到差分曲线,差分曲线的最大值就是两个分组的功率差分的估计值,用 D 表示;两组样本在差分曲线最大值对

* $I_{i,j}$ = k 表示 $K_{i,j}$ = 1 ,$G_{i,j}$ 和 $P_{i,j}$ 均为 0 的情况. $I_{i,j}$ = g ,$I_{i,j}$ = p 与此类似.

应的时刻的样本方差分别用 s_1^2, s_2^2 表示,则检验统计量如下:

$$t = \frac{D}{s_w \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}}, s_w^2 = \frac{(n_1 - 1)s_1^2 + (n_2 - 1)s_2^2}{n_1 + n_2 - 2}$$

t 服从于自由度为 $n_1 + n_2 - 2$ 的 t 分布,由于 $D \geq 0$,所以采用单边检验, t 对应的 t 分布概率(用 α 表示)即是两个被检分组对应的总体分布的显著性水平,即两组样本服从同分布的概率. α 越大的芯片被攻破的概率越低. 表 2 列出了由测量结果计算的两个芯片 A1-A2, A2-A3, A1-A3, B1-B2 和 C1-C2 之间的功率差分和对应的 s_1^2, s_2^2, n_1, n_2 (此处忽略了相同输入各次计算间的功耗差别,表中列出的 s_1^2 和 s_2^2 是各对输入数据对应的平均功率曲线的样本方差, n_1 和 n_2 是 3.1 节给出的各分组的向量数)以及得到的 t 值和相应的显著性水平 α.

表 2　DICLA 与 PBDICLA 的功率差分与功率显著性水平

Table 2　Power differences and power significances of DICLA and PBDICLA

$n_1 - n_2$		A1-A2	A1-A3	A2-A3	B1-B2	C1-C2
		77-101	77-105	101-105	181-102	140-143
DICLA	D/mW	1.75	1.86	1.64	0.575	0.429
	s_1^2/mW^2	2.267	7.318	7.451	1.553	2.690
	s_2^2/mW^2	1.632	10.311	7.539	1.760	2.347
	t	8.38	4.12	4.30	3.64	2.27
	α	8.17×10^{-15}	2.89×10^{-5}	1.32×10^{-5}	1.62×10^{-4}	1.20×10^{-2}
PBDICLA	D/mW	0.599	0.473	0.316	0.285	0.206
	s_1^2/mW^2	1.710	1.005	0.309	2.353	2.015
	s_2^2/mW^2	1.191	1.223	0.366	2.902	2.433
	t	3.31	2.96	3.89	1.44	1.16
	α	5.66×10^{-4}	1.75×10^{-3}	6.78×10^{-5}	7.55×10^{-2}	1.24×10^{-1}

表中加粗边框的格子中分别是两个芯片最小的显著性水平,它们对应的输入组合特征最易被攻击者识别,它们的大小决定着芯片的安全性. 从中可以看出: PBDICLA 的 5 项功率差分都小于 DICLA,最小显著性水平比 DICLA 提高了 10 个数量级. DICLA 考察的三方面输入特征中,第 1 种分组方式的组间差别的显著性水平最低,说明 C 模块的功率差分是主要的功率差分来源,由此可见,平衡底层模块功耗是重要的.

4　比较与结论

在已检索到的文献中,功耗平衡运算单元的设计方法只有引言中提到的采用"n 分之一"编码 SI 的逻辑方法. DICLA 就是一种"2 分之一"编码加法器. 文献[3]中给出了一个对称 DI 逻辑的全加器电路. DICLA 共有 552 个晶体管, PBDICLA 共有 941 个晶体管,规模大约是其 2 倍,被攻破的概率比 DICLA 低 10 个数量级;文献[3]中没有给出全加器电路的功率差分,但通过逻辑分析可知其功耗平衡情况要好于 DICLA,至少需要 144 个晶体管,按此方法搭建的 8 位加法器,至少需要 1152 个晶体管,数量要多于 PBDICLA 13 个以上. 这是由于 PBDICLA 利用了内部信号的共轭性质,采用小粒度补偿,节省了器件.

综上所述,通过从顶层到器件层综合考虑的全定制设计,可以实现低功率差分的运算单元. 这种单元解决了上层设计无法解决的底层功耗信息泄露问题,而且相对于限于逻辑级的解决方案具有更小的电路规模.

参考文献

[1] Kocher P, Jaffe J, Jun B. Differential power analysis. Advances in Cryptology-19th Annual International Cryptology Conference Proceedings, 1999: 388

[2] Coron J S, Kocher P, Naccache D. Statistics and secret leakage. Financial Cryptography (FC2000), LNCS, Springer-Verlag, 2001, 1962: 157

[3] Moore S, Anderson R, Cunningham P. Improving smart card security using self-timed circuits. The Eighth International Symposium on Advanced Research in Asynchronous Circuits and Systems, 2002

[4] Cheng Fuchiang, Unger S H, Theobald M, et al. Delay-insen-

sitive carry-lookahead adders. Proceedings of the Tenth International Conference on VLSI Design. IEEE Comput Soc, 1997:322

[5] Elmore W C. Transient response of damped linear networks with particular regard to wideband amplifiers. J Appl Phys, 1948,19:55

DPA Resistant Power-Balanced Adder for a Cryptographic IC*

Li Xiangyu and Sun Yihe

(Institute of Microelectronics, Tsinghua University, Beijing 100084, China)

Abstract: A power-balanced DI carry-lookahead adder, whose power is influenced little by the input data, can be used in a cryptographic IC to counter the power analysis. Power significances of implementations of this circuit and a contrasted DI adder are tested, yeilding a significant probability of the former of about 10^{10} times of that of the later. The number of transistors of this adder is to a lesser degree 13 over than the existing logic level solutions.

Key words: ASIC; data security; adder; differential power analysis; power-balanced

EEACC: 2570D; 1265B

Article ID: 0253-4177(2005)08-1629-06

* Project supported by the National Natural Science Foundation of China (No. 60236020)

Li Xiangyu male, was born in 1977, PhD candidate. His research interests focus on hardware security of cryptographic ICs. Email: lixy00@mails.tsinghua.edu.cn.

Sun Yihe male, was born in 1945, professor and advisor of PhD candidates. Email: sunyh@tsinghua.edu.cn

Received 22 September 2004, revised manuscript received 20 March 2005