

CMOS 门电路电磁信息泄漏评估

丁国良¹, 常小龙¹, 陈家文¹, 武翠霞²

(1 军械工程学院 计算机工程系, 河北 石家庄 050003; 2 河北工业大学, 天津 300130)

摘 要: 通过将 CMOS 工艺中的导线转化为电偶极子模型, 提出了一种对 CMOS 工艺的门电路进行电磁信息泄漏评估的方法. 仿真实验采用 TSMC0.18 μm 工艺, 实现了基于单轨逻辑以及 SABL 双轨逻辑的与非门, 并用提出的评估方法对门电路的电磁信息泄漏进行评估. 仿真结果表明, 该评估方法能够对 CMOS 门电路的电磁信息泄漏程度进行量化评估, 同时还表明了双轨门电路电磁信息泄漏弱于单轨门电路.

关键词: 电磁信息泄漏; 差分电磁分析; 电偶极子模型

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2011)05-0067-04

The Electromagnetic Information Leakage Evaluation on Basic CMOS Gate

DING Guo-liang¹, CHANG Xiao-long¹, CHENG Jia-wen¹, WU Cui-xia²

(1 Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China;

2 Hebei University of Technology, Tianjin 300130, China)

Abstract: A method of evaluating electromagnetic information leakage of the CMOS gate circuit was presented by changing the lead in CMOS technology into dipole model. The simulation adopted TSMC0.18 μm process technology, and implemented the NAND gate based single rail logic and SABL double rail logic, meanwhile, the electromagnetic information leakage was evaluated by the given method. The results showed that this method was able to quantitative evaluate the electromagnetic information leakage of the CMOS gate, and that the electromagnetic information leakage of double rail logic gate was much weaker than single logic gate.

Key words: Electromagnetic Information Leakage (EMIL); Difference Electromagnetic Analysis (DEMA); Electric Dipole Model (EDM)

1 引言

旁路攻击是一种针对密码芯片十分有效的密码分析技术, 并对密码芯片的设计方法和生产流程产生了极大的影响^[1]. 为了有效抵抗旁路攻击, 设计者一般通过算法级或者电路级进行抗旁路攻击密码芯片的设计和实现. 其中电路级防护较为有效, 它可以从根本上切断旁路信号与敏感信息的相关性.

标准单元是具有基本功能的与非门、或非门等逻辑门电路, 是数字集成电路设计的最小单元模块. 在 ASIC 密码芯片设计过程中, 一般采用基于标准

单元的半定制设计流程, 对标准单元及模块电路的信息泄漏程度进行反复评估, 通过改进电路降低其泄漏量, 最终设计出安全的密码芯片. 因此, 信息泄漏程度评估是芯片设计的关键环节之一, 并得到科研人员的广泛关注. Kris 等人针对功耗泄漏提出了恒定功耗逻辑电路 DDCVSL、SABL, 并定义了一组功耗泄漏评估尺度 NED、NCD^[2], 对逻辑门单元的防 DPA 特性进行比较分析. 国防科技大学的童元满等人对芯片设计不同阶段进行功耗模拟, 对不同设计层次下密码运算部件抗功耗攻击能力进行量化评估, 为密码运算部件的设计与实现提供有效的指

收稿日期: 2010-07-19; 修回日期: 2010-09-01

基金项目: 国家“八六三”计划项目(2007AA01Z454)

导信息^[3].

除了功耗泄漏外,电磁辐射也是密码芯片信息泄漏的主要途径之一^[4-6].但电路功耗泄漏不能完全等同于电磁泄漏,功耗与流入电路网络的总电流有关,而电磁辐射是电路网络中各个支路的电流共同作用的结果^[7].剑桥大学 Li 提出了一种在设计阶段评估整个芯片的电磁信息泄漏特性的方法^[8],该方法利用芯片总的消耗电流的变化率表示电磁辐射的变化.但是仅对芯片做整体的电磁信息泄漏评估,不能准确定位泄漏点,安全芯片设计效率较低.

文中基于基本逻辑门单元提出了一种电磁信息泄漏的评估方法,为设计具有抗电磁分析标准单元提供评价尺度.设计芯片时,使用该评估方法可确定信息泄漏较强的单元,进而重新设计该单元,提高了安全芯片的设计效率.

2 CMOS 门电路的电磁辐射及计算

2.1 CMOS 门电路电磁辐射

CMOS 电路中电容效应对电路功能和性能的影响是至关重要的.如图 1(a)所示,一个 CMOS 反相器的寄生电容包括晶体管自身的寄生电容(C_{gs} , C_{gd} , C_{sb} , C_{db}),输出线的负载电容(C_{int})和下一级的输出电容(C_g).电路工作时,寄生电容根据不同的输入输出信号进行充放电,形成充放电电流.在这些电流的作用下,金属导体不断产生电磁辐射.

门电路上产生的电磁辐射可以分为两部分.电路对晶体管自身寄生电容的充放电产生的电磁辐射记为 EM_{mos} ;输出线上的寄生电容和下一级输出电容,统一作为负载电容 C_{load} ,即 $C_{load} = C_{int} + C_g$.那么负载电容充放电在输出线上产生的电磁辐射记为 EM_{load} .因此,反相器工作时总的电磁辐射记为 EM .

$$EM = EM_{mos} + EM_{load} \quad (1)$$

随着集成电路制造工艺的进步,晶体管沟道长度不断减小,自身寄生电容也越来越小,因此电路内部寄生电容对电路的性能影响变小,而负载电容影响增强^[9].此时,反相器的等效电路可用图 1(b)表示.通过对 DDCVSL 和 SABL 与非门的仿真对比发现,当工艺达到 $0.18 \mu m$ 以后,负载电容的影响将起主要作用.此时可以得出结论,CMOS 门电路的电磁辐射将主要由 EM_{load} 构成.即:

$$EM \approx EM_{load} \quad (2)$$

2.2 CMOS 门电路电磁辐射计算

从图 1(b)中可以看出,负载电容的充放电情况与电路的输入和输出数据是直接相关的,因此其上

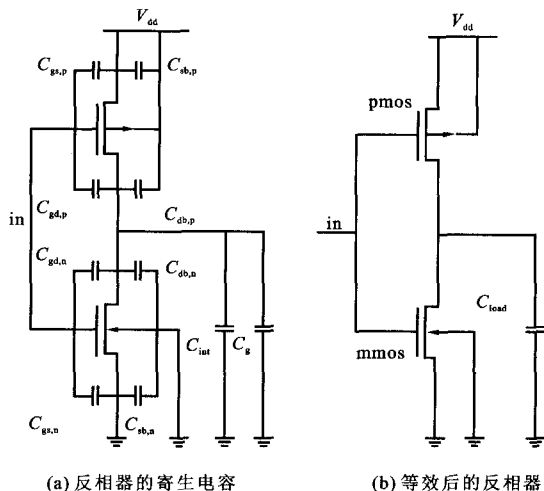


图 1 CMOS 反相器

的电磁辐射存在数据相关性.式(2)表明,只要能够计算出输出负载线上的电磁辐射就能够对门电路上整个电磁辐射的信息泄漏进行评估,问题关键在于如何计算输出线上产生的电磁辐射.

集成电路的金属层一般作为电路的引脚,传输线和导线等,其长度在微米数量级且远小于电磁辐射的波长.电偶极子是一种基本的辐射单元,它是一段长度 dl 远小于波长的直线电流元,因此可以利用电偶极子模型分析金属层的电磁辐射特性,如图 2 所示.在某一时刻,线上的电流是均匀的,且相位相同.此时, $I(t)dl$ 即为 $I dl$.

在电偶极子模型里,近场电磁场计算公式为^[10],

$$H = H_\varphi \approx \frac{I dl}{4\pi r^2} \sin\theta, \quad (3)$$

$$E_r \approx -j \frac{I dl}{2\pi\omega\epsilon r^3} \cos\theta, \quad (4)$$

$$E_\theta \approx -j \frac{I dl}{4\pi\omega\epsilon r^3} \sin\theta, \quad (5)$$

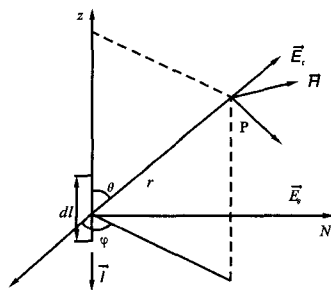


图 2 电偶极子的电磁辐射

该组公式反映电磁场与导线中电流 I 的内在关系,即近场区磁场 H 与电流 I 的相位完全相同,幅度 $|I|$ 的大小反映了磁场辐射的大小.虽然近场电场与电流没有这种直接的线性关系,从式(4)、(5)中

也可以看出电场 E 与 I 电流是密切相关的。

在近场区磁场和电场是分开的而且相互转化,因此为了计算的方便,可以通过磁场变化特性来反映电路的电磁辐射特性. 假设 t 时刻输出线上的电流为 I , 普通 CMOS 门电路的近场磁场可以近似表示为

$$\mathbf{H} = \frac{Idl}{4\pi r^2} \sin\theta, \quad (6)$$

r 为观测点 P 到门电路的距离, θ 为导线与 r 之间的夹角.

3 CMOS 门电路的电磁信息泄漏评估

3.1 单轨 CMOS 门电路电磁信息泄漏评估

单轨 CMOS 门中的输出信号线一般仅有条, 因此可通过式(6)来计算输出线上的磁场辐射, 进而分析整个门的电磁辐射的变化. 为评价门电路电磁信息泄漏程度, 文中定义门电路的电磁信息泄漏系数 ELC (Electromagnetic Leakage Coefficient):

$$ELC = |\max(\mathbf{H}) - \min(\mathbf{H})| / \max(|\mathbf{H}|), \quad (7)$$

式中, $\mathbf{H}$ 是门电路每个时钟周期的磁场峰值.

从定义式中可以看出, ELC 的值反映了通过门电路电磁场区分电路状态的能力, ELC 越大电磁信息泄漏越强, 电路越容易遭到差分电磁分析的攻击. 当电路所有时钟周期的电磁辐射都相等时, $ELC = 0$. 此时, 门电路没有信息的泄漏达到了防电磁分析的目的.

3.2 双轨 CMOS 门电路电磁信息泄漏评估

双轨门电路的特点是所有的信号都是由一对互补的信号线表示. 故对于双轨门单元电路, 计算出两条互补输出线上的电磁辐射就能估算出整个门单元的电磁辐射.

这里首先要解决的问题是, 如何计算两条互补输出线上的电磁辐射. 实际测量芯片电磁辐射时, 观测点一般放置在芯片的垂直正上方, 与芯片的距离 r 约 $0.5 \sim 1$ cm. 其中, 同一个门单元上两条导线的长度 l 和距离 d 都是在微米数量级上 $l \ll r, d \ll r, r_1 \approx r_2 \approx r, \theta_1 \approx \theta_2 \approx \pi/2$. 即, 观测点是在两个输出线所在的平面的垂直正上方. 当把两条互补的输出导线看作电偶极子模型时, 这两个电偶极子在观测点的电磁辐射就可以看作是二者的矢量之和.

因此, 研究双轨门电路的电磁辐射特性时可以得到首先得到互补输出端的瞬态电流 I_1 和 I_2 , 通过电偶极子模型计算两个互补输出线叠加的电磁场, 然后

使用定义式(7) 分析门电路的电磁信息泄漏程度.

两互补输出线在某一观测点的磁场强度为

$$\mathbf{H} = \mathbf{H}_1 + \mathbf{H}_2 = \frac{I_1 dl}{4\pi r_1^2} \sin\theta_1 + \frac{I_2 dl}{4\pi r_2^2} \sin\theta_2 \quad (8)$$

式中, $l \ll r, d \ll r, r_1 \approx r_2 \approx r, \theta_1 \approx \theta_2 \approx \pi/2$. 所以, 两条平行互补输出线在观测点的磁场计算可进一步简化得

$$\begin{aligned} \mathbf{H} &= \frac{I_1 dl}{4\pi r_1^2} \sin\theta_1 + \frac{I_2 dl}{4\pi r_2^2} \sin\theta_2 \\ &\approx \frac{I_1 dl}{4\pi r^2} \sin \frac{\pi}{2} + \frac{I_2 dl}{4\pi r^2} \sin \frac{\pi}{2} = (I_1 + I_2) \frac{dl}{4\pi r^2} \end{aligned} \quad (9)$$

当电路存在预充求值机制, 时每个时钟周期分为预充和求值两个阶段, 叠加后的磁场在预充和求值阶段方向不同, 可以具体求出预充和求值阶段的电磁泄漏系数 ELC_p 和 ELC_e :

$$ELC_p = |\max(|\mathbf{H}_p|) - \min(\mathbf{H}_p)| / \max(|\mathbf{H}_p|) \quad (10)$$

$$ELC_e = |\max(|\mathbf{H}_e|) - \min(\mathbf{H}_e)| / \max(|\mathbf{H}_e|) \quad (11)$$

$\mathbf{H}_p, \mathbf{H}_e$ 分别是预充和求值阶段门电路的磁场峰值.

4 仿真实验与分析

图3所示为门电路电磁信息泄漏评估流程. 使用 Cadence 进行原理图和物理版图的设计, 校验后进行寄生参数提取, 使用 Cadence Spectre 对电路进行仿真得到输出线上的电流 $I(t)$, 使用 Matlab 计算输出线的磁场 H , 根据定义式计算 ELC 值. 值得注意的是, 单轨和双轨门电路应选择不同的磁场计算公式. 另外, 在设计数字门电路版图时, 为了方便布局布线, 同一层的金属层一般保持平行或者垂直. 实验得到的磁场, 是以互补输出线平行为例计算得到的. 当互补输出线垂直时只需把计算公式稍作调整即可.

仿真实验基于 TSMC0.18 μm 工艺, 实现了 DDCVSL、SABL^[10] 和动态单轨的与非门, 并分别计算出了它们的 ELC 值, 取输出端导线长度 $dl = 1 \mu\text{m}$, 距离观测点距离 $r = 0.5$ cm, $\theta \approx \pi/2$. 式(6)、(9)可以分别简化为

$$\mathbf{H} = \frac{Idl}{4\pi r^2} \sin\theta = I \cdot 0.3185e-2 \quad (12)$$

$$\mathbf{H} = (I_1 + I_2) \frac{dl}{4\pi r^2} = (I_1 + I_2) \cdot 0.3185e-2 \quad (13)$$

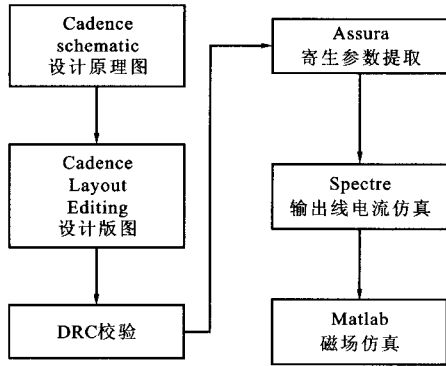


图 3 门电路电磁信息泄漏评估流程

DDCVSL、SABL 都是动态双轨逻辑,根据输出结果的不同,每个时钟周期相应的一个输出端负载电容将会进行充放电.表 1 给出了 DDCVSL、SABL 以及动态单轨与非门在预充和求值阶段的观测点磁场模的峰值(A/m)和 ELC 值.

表 1 DDCVSL 和 SABL 在预充和求值阶段磁场峰值模和 ELC

		Max H _p	Min H _p	Max H _e	Min H _e	ELC _p	ELC _e
1	SABL	0.0869e-5	0.0764e-5	0.0938e-5	0.0884e-5	12.08%	5.86%
2	DDCVSL	0.1105e-5	0.0974e-5	0.1240e-5	0.1075e-5	11.85%	13.31%
3	动态单轨	0.0979e-5	0.0012e-5	0.1074e-5	0.0043e-5	98.77%	95.99%
4	SABL	0.0933e-5	0.0764e-5	0.1019e-5	0.0884e-5	18.11%	13.25%

注:1、2 中互补输出端的负载电容均取 10f F; 4 中互补输出端负载电容分别取 10f F 和 12f F

从仿真结果中以看出(表 1),动态单轨与非门有较强的电磁信息泄漏,双轨门电路的抗电磁分析性能优于单轨的门电路.

动态双轨与非门两个互补的输出线上的负载电容相等时,虽然 SABL 和 DDCVSL 内部结构不同,内部寄生电容不相等,但它们的 ELC_p 十分接近,也即是这两种防护逻辑的电磁信息泄漏程度近似;当互补输出线上负载电容分别取 10 fF 和 12 fF 时,SABL 与非门的 ELC 值变大,电磁信息泄漏增强.这表明输出负载电容对电路的电磁辐射产生主要影响,双轨门电路中要保证输出端有近似的负载电容才能有较好的防电磁分析攻击的性能.

5 结束语

文中从 CMOS 基本单元出发分析了电路信息泄漏的机理,提出电磁信息泄漏的评估方法,为设计具有抗电磁分析性能的门标准单元提供评价标准.和文献[6]提出的芯片电磁信息泄漏整体评估方法相比,该方法能够对电路的单元模块的信息泄漏提供更为精细的评估,两种方法相互结合,可为安全芯

片的设计提供完整的电磁信息泄漏评估方案.但是,还应看到集成电路电磁信号的复杂性,未来应该通过引入电路不同结构间的干扰和耦合,寻找更为精确的计算门 CMOS 电路电磁辐射方法,提供更为精确的电磁信息泄漏评估模型.

参考文献:

[1] Kris Tiri, Ingrid Verbauwhede. A digital design flow for secure integrated circuits[J]. IEEE Transactions on Computer - Aided Design of Integrated Circuits and Systems, 2006,25(7):1197-1208.

[2] Tiri K, Akmal M, Verbauwhede I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards[C]// Process of the 28th European Solid-State Circuits Conference. Florence, Italy: IEEE, 2002:403-406.

[3] 童元满,王志英,戴葵,等. 不同设计层次下密码运算部件抗功耗攻击能力量化评估技术[J]. 计算机研究与发展,2009,46(6):940-947.

[4] 丁国良,赵强,陈家文,等. 电磁信息泄漏研究及进展[J]. 军械工程学院学报,2008,20(6):65-67.

[5] 郭华,丁国良,刘昌杰,等. DES 加密算法的差分电磁攻击实现[J]. 微电子学与计算机,2009,26(12):34-37.

[6] 陈光达,邱扬,田锦,等. 计算机防视频泄漏专用视频处理系统设计研究[J]. 微电子学与计算机,2004,21(3):37-40.

[7] Agrawal D, Archambeault B, Rao J, et al. The EM side-channel(s)[C]// Proceedings of Cryptographic Hardware and Embedded Systems - CHES2002, London, UK: Springer-Verlag, 2003:29-45.

[8] Huiyun Li, A. Theodore markettos and simon moore, "Security evaluation against electromagnetic analysis at design time"[C]// proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES2005). Edinburgh, Scotland: Springer, 2005:280-292.

[9] 石伟,戴葵,童元满,等. 防 DPA 攻击的两种不同逻辑比较研究[J]. 计算机工程与科学,2007,29(5):19-22.

[10] 谢处方,饶克谨. 电磁场与电磁波[M]. 北京:高等教育出版社,2008.

作者简介:

丁国良 男,(1968-),副教授.研究方向为集成电路防护与安全设计.

常小龙 男,(1986-),硕士研究生.研究方向为集成电路防护与安全设计.