

集成电路电磁辐射与数据相关性研究

常小龙, 丁国良, 尹文龙, 王创伟

(机械工程学院 计算机工程系, 河北 石家庄 050003)

摘要:为了减少集成电路密码芯片工作时的电磁信息泄漏,设计具有防护能力的加密芯片。在研究 CMOS 集成电路电磁辐射原理的基础上,分析了电磁辐射产生数据相关性的机理。以电偶极子为模型,简化了电磁计算的方法,对基本的 CMOS 电路工作过程进行分析。采用 TSMC 0.18 工艺设计 CMOS 反相器,并对该反相器进行电磁辐射仿真。建立评估模型并对金属层电磁辐射的信息泄漏进行评估。结果表明,电路工作时 NMOS 金属层、PMOS 金属层和输出线的金属层产生的电磁辐射均会导致信息泄漏,长度相等时,输出线金属层的电磁信息泄漏更强。

关键词:CMOS 集成电路;金属层;电磁信息泄漏;数据相关性;电偶极子

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2010)07-0156-04

Research on Correlation Between ICs Electromagnetic Radiation and Data

CHANG Xiao-long, DING Guo-liang, YIN Wen-long, WANG Chuang-wei

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

Abstract: In order to reduce electromagnetic information leakage of IC cipher chip, design encryption chip which has defending ability. The principles of electromagnetic radiation produced by IC is analyzed. Study the mechanism of data correlation caused by electromagnetic emissions on the basis of pre-principles. At the same time, the model which computes the value of EM field of electric dipole is predicted. The work process of basic CMOS circuit is analyzed in detail. According to TSMC0.18 design rule, a CMOS inverter is designed and electromagnetic radiation of the inverter is simulated and a evaluation model is established to evaluate the degree of electromagnetic information leakage of metal layer. Results indicate that the metal layer of NMOS, PMOS and output line of inverter will bring electromagnetic radiation when circuit is working and cause information leakage. Electromagnetic information leakage of the metal layer of transmission line is stronger than PMOS and NMOS with the same length.

Key words: CMOS integrate circuits; metal layer; electromagnetic information leakage; data correlation; electric dipole

0 引言

集成电路芯片在工作时将会向外部空间发出电磁辐射,这些电磁辐射可能会泄漏与数据相关的敏感信息,即产生了电磁信息泄漏。利用这些电磁辐射,采用统计学方法可以获取集成电路工作时的数据信息,从而给智能卡、加密芯片的安全构成巨大的威胁^[1-4]。文献[5,6]中以最简单的磁场传感器——环形线圈为基础,对 COMS 集成电路电磁辐射做了简单的分析,指出了电路电磁辐射与数据存在相关性,但并没有说明集成电路产生电磁辐射而导致信息泄漏的根本原因。

文中从 CMOS 集成电路的物理结构和工作原理出发,分析集成电路电磁辐射的基本原理。以 COMS 反相器为研究对象,指出电磁辐射源主要包括 PMOS、NMOS 和输出线的金属层(即与输出引脚相连的金属层)。当输入信号在(0→1)和(1→0)两种情况下跳变时电路会对负载电容进行充放电,导致在这两种情况下流过金属层的电流不相等,进而产生电磁辐射与数据的相关性,引起电磁信息泄漏。

同时研究表明电路的集总负载电容越大电路产生的电磁辐射越明显;同样长度金属层,在输出线上的电磁信息泄露更强,为以后集成电路芯片的抗电磁分析设计提供理论依据。

1 集成电路电磁辐射

1.1 电磁辐射原理及计算

根据麦克斯韦方程,随时间变化的电场会在周围

收稿日期:2009-10-31;修回日期:2010-01-29

基金项目:国家 863 计划项目(2007AA01Z454)

作者简介:常小龙(1986-),男,硕士,研究方向为集成电器防护与安全设计;丁国良,副教授,研究方向为集成电路防护与安全设计。

空间产生磁场,随时间变化的磁场也会在周围空间产生电场,在时变情况下 $I(t)dl$ 是产生电磁波的一种基本的“矢性点源”^[7]。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。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 $I dl$ 。集成电路的金属层一般作为电路的引脚,传输线和导线等,它们的长度都是在微米数量级上且远小于电磁辐射的波长,集成电路中长度 dl 的金属层可等效为一个电偶极子。因此可以利用电偶极子模型分析金属层的电磁辐射特性。

在球面坐标中长度为 dl 电偶极子的正弦时变辐射场的计算公式为^[6]:

$$\begin{cases} H_r = H_\phi = 0 \\ H_\theta = \frac{Idl e^{-jkr}}{4\pi r} \left(jk + \frac{1}{r} \right) \sin\theta \end{cases} \quad (1)$$

$$\begin{cases} E_r = -j \frac{Idl}{2\pi\omega\epsilon} \cdot \frac{e^{-jkr}}{r^2} \left(jk + \frac{1}{r} \right) \cos\theta \\ E_\theta = -j \frac{Idl}{4\pi\omega\epsilon} \cdot \frac{e^{-jkr}}{r} \left(-k^2 + \frac{jk}{r} + \frac{1}{r^2} \right) \sin\theta \\ E_\phi = 0 \end{cases} \quad (2)$$

实际对集成电路芯片攻击时,信号采集点一般处于近场区。 r 是观测点距场源的距离,此时 $r \ll \lambda$, $kr = \frac{2\pi}{\lambda}r \ll 1$,即 $e^{-jkr} \approx 1$,所以电偶极子近场电磁辐射场可简化为:

$$H_\theta \approx \frac{Idl}{4\pi r^2} \sin\theta \quad (3)$$

$$\begin{cases} E_r \approx -j \frac{Idl}{2\pi\omega\epsilon r^3} \cos\theta \\ E_\theta \approx -j \frac{Idl}{4\pi\omega\epsilon r^3} \sin\theta \end{cases} \quad (4)$$

公式(1)和公式(2)给出了电偶极子的电磁场,从公式可以知道,磁场 $H = H_\theta$ 、电场 $E = E_r + E_\theta$ 。用近场电场计算方法进行分析电场辐射特性较为复杂,而用磁场计算方法分析磁场辐射特性相对容易。当观测点一定时,可知在公式(3)中 r, θ, dl 为固定值,(3)式可进一步简化,

$$H = H_\theta \approx \frac{Idl}{4\pi r^2} \sin\theta = I \cdot \frac{dl}{4\pi r^2} \sin\theta = I \cdot M = |I| \angle \alpha \cdot M \quad (5)$$

简化的算式(5)更加直接地表示了磁场辐射与电流 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,从公式(2)、(4)中也可以看出电场 E 与电流 I 是密切相关的,电流 I 是分析电路电磁辐射与数据相关性的

桥梁。

1.2 CMOS 集成电路电磁辐射

图 1A 是一个反向器的电路,电容 C_{gd} 和 C_{gs} 主要是由栅极对扩散区的交叠引起, C_{db} 和 C_{sb} 是随电压改变的结电容, C_{int} 是集总的互联线电容, C_g 是下一级电路的扇出电容。

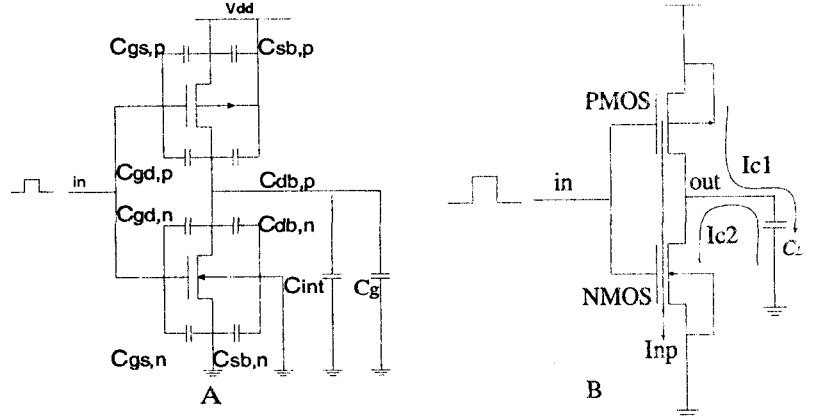


图 1 CMOS 反向器电路

这样的电路里包含许多非线性的压变电容,分析瞬态特性时相当复杂。为了简化,将输出与地之间的电容等效为一个集总的线性电容 C_L :

$$C_L = C_{gd,n} + C_{gd,p} + C_{db,n} + C_{db,p} + C_{int} + C_g \quad (6)$$

式(6)中有些寄生电容没有出现, $C_{sb,n}$ 和 $C_{sb,p}$ 两端电压不会变化,不影响瞬态特性。 $C_{gs,n}$ 和 $C_{gs,p}$ 的两端连在输入端和地(或 Vdd 端),因此也不会影响反相器的瞬态特性。所以,具有集总输出负载电容 C_L 的 CMOS 反相器如图 1B 所示^[8]。

在集成电路的版图中金属层起着至关重要的作用。它通常作为输入输出线,晶体管之间的金属连线,以及不同功能模块之间的传输线。

这些金属层在芯片工作时就会有电流通过,由电磁辐射的原理可知,每一段金属层就是一个电偶极子天线向空间发射电磁辐射。在数字电路中输入输出信号通常是脉冲信号,在这些信号的作用下,伴随着元器件的导通和截止,将产生时变脉冲电流,金属层在这些电流作用下会产生电磁辐射,可以用电偶极子模型计算和分析它们的电磁辐射。虽然某一段金属层电磁辐射十分微弱,但是集成电路芯片内部集成了大量元器件和 CMOS 门电路,工作时整个芯片的电磁辐射会达到可探测的程度。

2 CMOS 电路电磁辐射和数据的相关性

如图 1B 所示,当 CMOS 反相器电路在瞬态工作状态时(输入信号由高到低(1→0)或由低到高(0→1)跳变),必须考虑负载电容的影响。此时,有三种电流

存在:

1) NMOS 和 PMOS 同时导通时, 流经 NMOS 和 PMOS, 从电源流向地的短路电流 I_{np} , 当电路的负载电容较大且输入信号转换时间较短时, 短路电流 I_{np} 可以忽略不计^[5];

2) PMOS 导通时的负载电容充电电流 I_{C1} ;

3) NMOS 导通时的负载电容放电电流 I_{C2} 。

因此在 CMOS 反相器中产生电磁和数据相关性主要有三个部分, 即 NMOS 的金属层、PMOS 的金属层以及输出线相连的金属层。

2.1 PMOS 电磁辐射与数据相关性

经分析可知, 流过 PMOS 金属层的电流 I_{dsp} 主要由 I_{np} 和 C_L 的充电电流 I_{C1} 组成, $I_{dsp} = I_{np} + I_{C1}$ 。如前所述, 短路电流 I_{np} 可以忽略不计, $I_{dsp} \approx I_{C1}$ 。当输入信号 (1→0) 跳变时 C_L 处于充电状态, $I_{C1} \neq 0$, $I_{dsp} \approx I_{C1}$ 。而信号 (0→1) 跳变时 C_L 处于放电状态, $I_{C1} = 0$, $I_{dsp} \approx 0$ 。所以 $I_{dsp}(1 \rightarrow 0) \neq I_{dsp}(0 \rightarrow 1)$, 由式 (3)、(4) 可知 I_{dsp} 在 NMOS 金属层上产生的电磁辐射在信号 (1→0) 和 (0→1) 两种情况幅值必然不等, 存在数据相关性。

2.2 NMOS 电磁辐射与数据相关性

同样, 流过 NMOS 金属层的电流 I_{dsn} 主要由两部分构成: 1) NMOS 和 PMOS 同时导通时从电源到地的短路电流 I_{np} ; 2) C_L 经 NMOS 的放电电流 I_{C2} 。因此有 $I_{dsn} = I_{np} + I_{C2}$ 。 I_{np} 可忽略不计, $I_{dsn} \approx I_{C2}$ 。在 (1→0) 的跳变时, $I_{C2} = 0$, $I_{dsn} \approx 0$ 。相反, 信号 (0→1) 跳变时 C_L 处于放电状态, $I_{C2} \neq 0$, $I_{dsn} \approx I_{C2}$ 。因此, 可知 $I_{dsn}(1 \rightarrow 0) \neq I_{dsn}(0 \rightarrow 1)$ 。同样可以得到结论 NMOS 的金属层产生的电磁辐射也具有数据相关性。

2.3 输出线电磁辐射与数据相关性

如图 1B 所示, 与输出线相连的金属层电流 I_C 主要包含充电电流 I_{C1} 和放电电流 I_{C2} , $I_C = I_{C1} + I_{C2}$ 。 I_{C1} 和 I_{C2} 是两个方向相反的电流, (1→0) 时 $I_{C1} \neq 0$, $I_{C2} = 0$ 。 (0→1) 时 $I_{C1} = 0$, $I_{C2} \neq 0$ 。所以 $I_C(1 \rightarrow 0) \neq I_C(0 \rightarrow 1)$ 。由式 (3)、(4) 可知, 金属层在 I_C 的作用下, 两种情况信号跳变时将产生方向相反的电磁辐射, 同样具有数据相关性。

当反相器工作在稳定的状态时, 流过 NMOS、PMOS 和输出线的电流几乎为零, 产生的电磁辐射十分微弱, 可以忽略不计。当反相器工作在瞬态时会产生电磁辐射, 因此, 可以通过分析有无产生电磁辐射来区分反相器的工作状态。

3 仿真结果与分析

3.1 仿真结果

反相器电路采用 TSMC 0.18 工艺进行设计, 使用

Cadence 公司的集成电路设计工具进行前端设计、版图设计、寄生参数提取和后端仿真。经过寄生参数提取和后端仿真后, 得到的仿真结果十分接近电路工作的实际情况^[9]。

按照图 1B 进行原理图设计, 然后进行版图设计, 其中, $W_p = 2\mu\text{m}$, $L_p = 0.3\mu\text{m}$, $W_n = 1\mu\text{m}$, $L_n = 0.35\mu\text{m}$ 经过寄生参数提取后, 使用 Hspice 仿真。设定输入信号周期为 100ns, 瞬态扫描时间为 300ns。可以分别得到流经 NMOS、PMOS 和输出线的电流 I_{dsn} 、 I_{dsp} 和 I_C , 使用式 (5) 在 MATLAB 计算得到相应的近场磁场。

设 $r = 1\text{cm}$, $dl = 1\mu\text{m}$, $\theta = \pi/2$, 所以 $M \approx 10^{-3} \text{ m}^{-1}$ 。用式 (5) 计算出 NMOS、PMOS 和输出线上长度等于 $1\mu\text{m}$ 的金属层产生的磁场, 如图 2 所示。

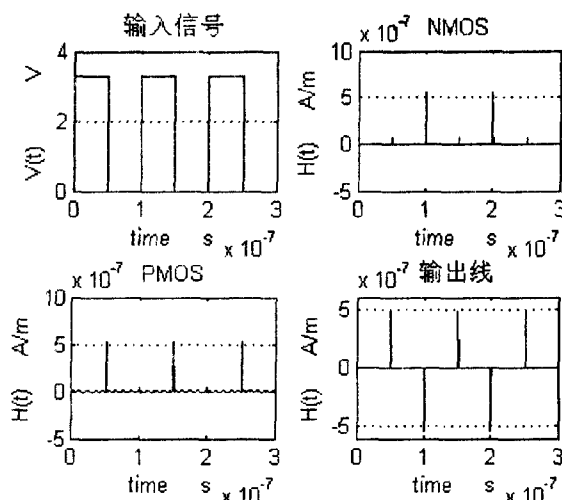


图 2 $C_L = 50\text{fF}$ 时 PMOS、NMOS 和输出线上磁场辐射场

3.2 结果分析

CMOS 反相器中输入数据有四种转换状态, (0→0)、(0→1)、(1→0)、(1→1), 当各个转换状态下产生的电磁辐射都相同时, 便无法区分这四种转换状态, 否则将能够区分这四种状态, 产生电磁信息泄漏。可以用电磁泄漏系数 ELC (Electromagnetic Leakage Coefficient) 来描述任意两种转换状态下产生电磁辐射差别, 它表明了通过电磁辐射来区分两种转换状态的难易程度, 也反映了电磁的信息泄漏程度。

定义:

$$ELC_{\text{stage1, stage2}} = \frac{|\max(W) - \min(W)|}{\max(|\max(W)|, |\min(W)|)}$$

W 是所考察的金属层的电磁辐射, $\max(W)$ 表示相比较的两种转换状态下电磁辐射的最大峰值, $\min(W)$ 表示相比较的两种转换状态下电磁辐射的最小峰值, $ELC = 0$ 说明无法区分两种转换状态, $ELC \neq 0$ 说明两种转换状态下电磁辐射不同, 产生了电磁信息泄漏, 能够区分这两种转换状态。ELC 值越大, 转换状

态越容易区分,电磁信息泄漏越明显,电磁辐射与数据的相关性就越强。

计算金属层近场电磁辐射 ELC 值时,长度取 $1\mu\text{m}$, W 是磁场 H 。从仿真结果可以看出 CMOS 反向器的各种辐射源在 $(0 \rightarrow 0)$, $(1 \rightarrow 1)$ 两种转换状态下产生的磁场为零,在 $(0 \rightarrow 1)$, $(1 \rightarrow 0)$ 两种转换状态下均有辐射产生。通过计算可知, $\text{ELC}_{(0 \rightarrow 0), (1 \rightarrow 1)} = 0$, 说明无法区分 $(0 \rightarrow 0)$ 和 $(1 \rightarrow 1)$ 两种转换状态。 $\text{ELC}_{(0 \rightarrow 0), (0 \rightarrow 1)} = 1$, $\text{ELC}_{(0 \rightarrow 0), (1 \rightarrow 0)} = 1$, 说明能够区分 $(0 \rightarrow 0)$ 和 $(0 \rightarrow 1)$, $(0 \rightarrow 0)$ 和 $(1 \rightarrow 0)$; $\text{ELC}_{(1 \rightarrow 1), (0 \rightarrow 1)} = 1$, $\text{ELC}_{(1 \rightarrow 1), (1 \rightarrow 0)} = 1$ 这说明也能够区分 $(1 \rightarrow 1)$ 和 $(0 \rightarrow 1)$, $(1 \rightarrow 1)$ 和 $(1 \rightarrow 0)$ 。反相器工作时,如果存在某两个转换状态的 $\text{ELC} \neq 0$ 就会产生电磁的信息泄漏。

表 1 清楚地表明 $(0 \rightarrow 1)$ 和 $(1 \rightarrow 0)$ 两种转换状态下, NMOS、PMOS 和输出线的金属层在长度等于 $1\mu\text{m}$ 时电磁辐射和 ELC 值,此时 W 为磁场 H 。

表 1 NMOS、PMOS 和输出线在 $(0 \rightarrow 1)$ 和 $(1 \rightarrow 0)$ 下的磁场辐射(A/m)和 ELC 值

辐射源	$(0 \rightarrow 1)$ 时 磁场峰值	$(1 \rightarrow 0)$ 时 磁场峰值	$\text{ELC}_{(0 \rightarrow 1), (1 \rightarrow 0)}$
NMOS 金属层	$5.60245\text{e}-7$	$0.67862\text{e}-7$	0.879
PMOS 金属层	$0.40407\text{e}-7$	$5.525792\text{e}-7$	0.878
输出线金属层	$4.88556\text{e}-7$	$5.11349\text{e}-7$	1.954

NMOS、PMOS 和输出线的金属层均产生了电磁辐射与数据的相关性,信号在 $(0 \rightarrow 1)$ 和 $(1 \rightarrow 0)$ 两种情况下跳变时 NMOS 和 PMOS 金属层的 ELC 值近似,二者电磁的信息泄漏程度近似;输出线产生的电磁辐射方向相反,ELC 值较大,因此同样长度的金属层,输出线对信息的泄漏明显强于前两者。

综上所述,电路对负载电容的充放电,是金属层产生电磁信息泄漏的根本原因。负载电容越大,充放电时的电流越大,金属层上的电磁辐射也越强,分别取 $C_L = 50\text{fF}$, $C_L = 10\text{fF}$, $d_l = 1\mu\text{m}$ 时,输出线金属层上产生的磁场辐射如图 3 所示。

4 结束语

CMOS 门电路对负载电容的充放电是产生电磁辐射与数据相关性的主要原因,通过改变电路的电容效应可以降低金属层的电磁辐射。在设计加密芯片的过程中,设计者设计与密钥紧密相关的运算电路单元时,可采用具有动态双轨特性的防护电路,使得电路在不同转换状态下产生相等的电磁辐射,力求做到去除电路电磁辐射和数据的相关性,达到抗电磁分析的目的。

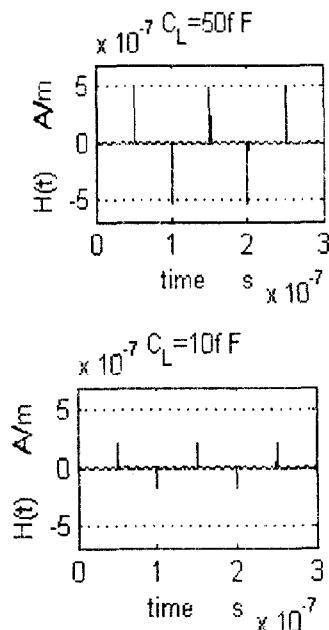


图 3 C_L 取不同值时的输出线上磁场的变化

参考文献:

- [1] 丁国良,郭华,陈利军,等. 密码系统差分电磁分析研究[J]. 计算机工程与设计, 2009, 30(12): 2892-2894.
- [2] 曹建国,王丹,王威. 基于 RSA 公钥密码安全性的研究[J]. 计算机技术与发展, 2007, 17(1): 172-173.
- [3] 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, 2009, 20(6): 65-67.
- [4] Gandolfi K, Mourtel C, Olivier F. Electromagnetic analysis: Concrete results[C]// Proc. of Cryptographic Hardware and Embedded Systems (CHES 2001). [s. l.]: Springer, 2001: 251-261.
- [5] Peeters E, Standaert Francois - Xavier, Quisquater Jean - Jacques. Power and Electromagnetic Analysis: Improved Model, Consequences and Comparisons[J]. Integration, the VLSI Journal, 2007, 40(1): 52-60.
- [6] Li Huiyun, Markettos A T, Moore S. Security Evaluation Against Electromagnetic Analysis at Design Time[C]// in proceedings of Workshop on Cryptographic Hardware and Embedded Systems(CHES2005), 7th International Workshop. Berlin, Heidelberg: Springer, 2005: 280-292.
- [7] 谢处方,饶克瑾. 电磁场与电磁波[M]. 北京: 高等教育出版社, 2008.
- [8] Kang Sung - Mo, Leblebici Y. CMOS 数字集成电路——分析与设计[M]. 王志功, 宴建华, 等译. 北京: 电子工业出版社, 2005.
- [9] 韩雁,洪慧,马绍宇,等. 集成电路设计中 EDA 工具实用教程[M]. 杭州: 浙江大学出版社, 2007.