物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

物理型硬件木马失效机理及检测方法

骆扬　王亚楠

Physical hardware trojan failure analysis and detection method

Luo Yang　Wang Ya-Nan

引用信息 Citation: Acta Physica Sinica, 65, 110602 (2016)　DOI: 10.7498/aps.65.110602
在线阅读 View online: http://dx.doi.org/10.7498/aps.65.110602
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2016/V65/I11

物理型硬件木马失效机理及检测方法*

骆扬† 王亚楠

(中国信息安全测评中心安全检测处, 北京 100876)

(2016 年 2 月 16 日收到; 2016 年 3 月 8 日收到修改稿)

对两种物理型硬件木马造成芯片退化或失效的机理进行了详细分析. 通过使用 ATLAS 二维器件仿真系统并结合 SmartSpice 电路逻辑仿真器, 模拟了两种物理型硬件木马对反相器逻辑电路输出特性的影响. 使用 ATHENA 工艺仿真系统模拟了掺杂离子注入工艺过程, 实现了掺杂型硬件木马的金属-氧化物-半导体场效应管 (MOSFET) 器件; 使用热载流子注入退化模型对 ATLAS 仿真器件进行热载流子压力测试, 以模拟热载流子注入型硬件木马注入 MOSFET 器件并造成器件退化失效的过程, 分别将上述掺杂型硬件木马和热载流子注入型硬件木马的 MOSFET 器件与另一个正常 MOSFET 器件组成同样的反相器逻辑电路. 反相器使用 Spice 逻辑电路仿真输出 DC 直流、AC 瞬态传输特性以研究物理型硬件木马对电路输出特性的影响. 为了研究 MOSFET 器件的物理特性本身对硬件木马的影响, 在不同温度不同宽长比 (W/L) 下同样对反相器进行 Spice 电路逻辑输出仿真. 本文分析了离子掺杂工艺、热载流子注入压力测试形成的物理型硬件木马随压力强度、温度的变化对逻辑电路输出特性的影响. 通过结果对比分析得出了含有物理型硬件木马的逻辑电路在 DC 直流输出特性上的扰动比 AC 瞬态传输特性更明显的结论. 因此, 本文提出了一种针对物理型硬件木马的检测流程. 同时, 该检测流程是一种具有可操作性的检测物理型硬件木马的方法.

关键词: 硬件木马, 热载流子注入, 器件退化, 失效分析

PACS: 06.60.Mr, 06.90.+v, 07.05.Fb **DOI:** 10.7498/aps.65.110602

1 引 言

缩短开发周期、整合优势技术、降低制造成本成为 IC 芯片制造全球化的主要动力, 随着集成电路全球化合作的发展, 芯片设计公司常购买第三方 EDA 工具或雇佣芯片代工厂, 整个 IC 芯片生成过程存在诸多不安全因素. 攻击者可能会恶意修改 IC 芯片原始电路, 插入额外功能的电路、器件或改变生产工艺等统称为注入硬件木马. 硬件木马的最终目的是泄露信息、改变寄存器信息或使芯片器件功能退化或失效.

自从 2005 年美国国防部先进研究项目局首次提出硬件系统安全的概念以来, 已经超过一百多种检测硬件木马的方法 [1], 其中基于功耗分析和路径延时分析的侧信道分析受到了广泛关注 [2−7]. 但直到现在, 没有任何基于侧信道分析硬件木马的技术作为评估标准或被认定是评估对象的测试指导 [8]. 对于逻辑级硬件木马的检测, 采用对芯片开封、剖片等逆向工程后, 再通过光学图像识别系统 (包括扫描电子显微镜, SEM) 与原有版图进行对比可以找出被篡改的电路部分, 但物理型硬件木马改变的是器件物理特性而非电路结构. 物理型硬件木马使得部分器件在一定时间内逐步退化或快速退化致功能失效. 例如, 利用 AES 加密模块产生随机数的逻辑电路模块, 在注入掺杂型硬件木马后, 使得某些比特位恒为 0 或 1, 进而使得产生随机数质量降低, 造成后续破解密钥的难度大幅降低. 因此, 研究物理型硬件木马对逻辑电路传输特性的影响及其造成芯片退化失效的物理机理, 对提出检测应对物理型硬件木马的方法和国家信息安全具有深远的意义.

* 国家自然科学基金 (批准号: 61402536) 资助的课题.

† 通信作者. E-mail: mddr@163.com

本文通过使用ATLAS二维器件仿真系统并结合SmartSpice电路逻辑仿真器, 使用Spice逻辑电路仿真输出DC直流、AC瞬态传输特性以研究物理型硬件木马对电路输出特性的影响. 分析了离子掺杂工艺、热载流子注入压力测试形成的物理型硬件木马随测试压力强度、温度的变化对逻辑电路输出特性的影响. 通过结果对比分析得出了含有物理型硬件木马的逻辑电路在DC 直流输出特性上的扰动比AC瞬态传输特性更明显的结论. 探索了物理型硬件木马造成逻辑电路输出错误及芯片模块失效的物理机理, 提出了一种针对物理型硬件木马的检测方法及流程.

2 物理型硬件木马模型

2.1 掺杂型硬件木马

攻击者通过改变离子注入掩膜区域, 在晶体管的特定位置上注入其他离子杂质, 改变器件的掺杂离子或浓度达到改变原始门电路逻辑特性的目的. 例如, 在p型掺杂掩膜时注入n型掺杂, 这时有源区变成了带有n掺杂的n阱, n阱常被用于连接供电电源$V_{\rm dd}$的接口, 再通过金属膜做金属接触后就会制造出一条从n阱到$V_{\rm dd}$的连接线. 从图1的右

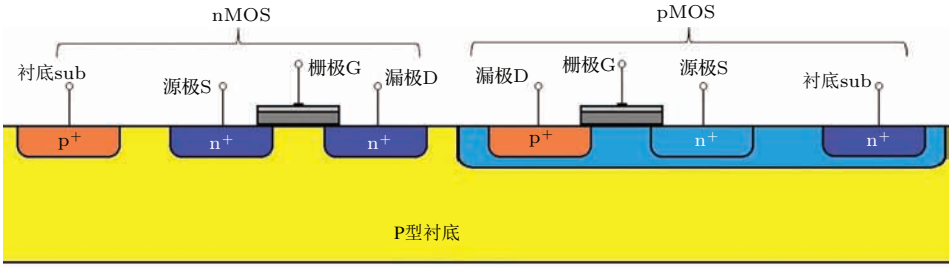

图1 反相器金属氧化物半导体(MOS)器件掺杂结构改变示意图

Fig. 1. MOSFET inverter device dopant trojan schematic.

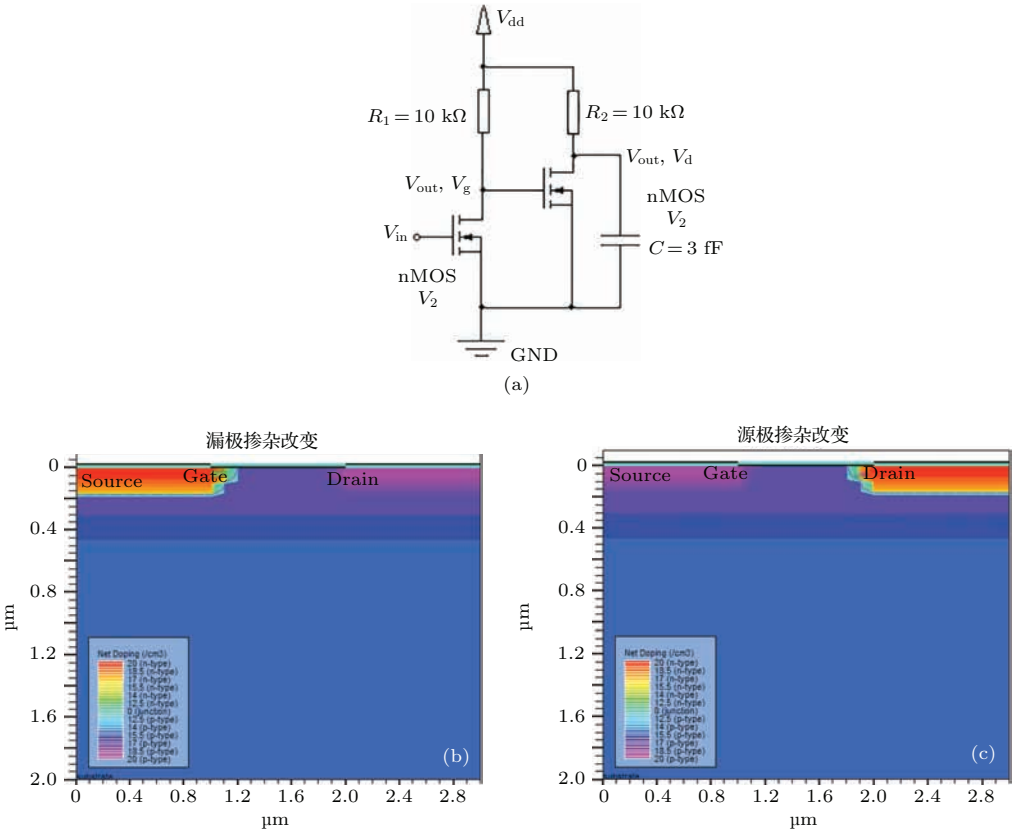

图2 (a) 反相器原理图; (b) 漏极掺杂改变的器件; (c) 源极掺杂改变的器件

Fig. 2. (a) The schematic of an inverter circuit; (b) change device of doping drain; (c) change device of doping source.

侧可以看出,pMOSFET掺杂型硬件木马源极接触到V_{dd}的连线直接接触及到了n阱区域, 这相当于从n阱直接到了V_{dd}. 漏极接触也连接到了n阱和V_{dd}. 因此, 从V_{dd}到漏极形成了直通线. 从图1可以看出, 无论输入引脚是否有输入, 带有掺杂型硬件木马的反相器总是输出V_{dd}[9].

以两个nMOSFET组成的反相器作为验证的逻辑电路进行仿真, 电路原理图如图2(a)所示, 改变其中一个nMOSFET的掺杂离子杂质并进行ATLAS器件仿真. 图2(b)是改变nMOSFET漏极的ATLAS器件截面图, 图2(c)是改变nMOSFET源极的ATLAS器件截面图.

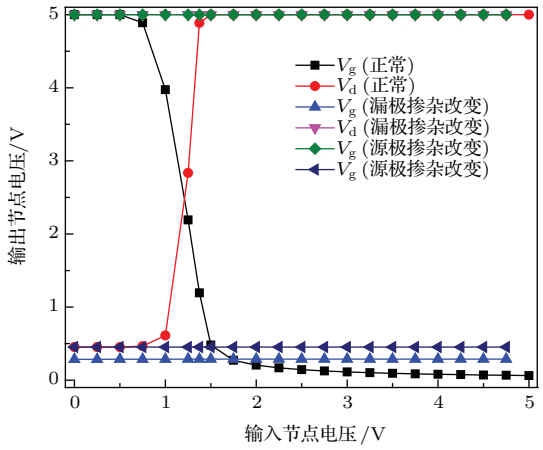

图3 反相器DC直流传输特性

Fig. 3. DC transmission characteristics of inverter.

攻击者改变nMOSFET (pMOSFET)源极或漏极的掺杂离子杂质后, 反相器的输出节点始终保持一个状态, 对正常反相器与被攻击的反相器的逻辑输出节点(V_{out}, V_g)和(V_{out}, V_d)的输出特性进行仿真. nMOSFET器件的宽长比为: $W/L = 5\ \mu m : 2\ \mu m$, 在改变掺杂杂质后, 进行DC直流和AC瞬态传输特性的仿真. DC直流输出特性如图3所示, AC瞬态传输特性如图4所示. 从图3中可以看出, 在反相器逻辑电路中带有受到攻击的MOSFET的输出节点无论是DC直流特性还是AC瞬态传输特性都始终保持一个状态. 输出逻辑不会随着输入节点的逻辑变化而发生变化, 输出的V_g, V_d与输入节点没有相关性. 对于安全数据密钥产生模块, 如果产生的随机数中有比特位是固定值, 无疑降低了密钥破解的难度. 从图4中看出, 对于掺杂型硬件木马无论是漏极掺杂改变还是源极掺杂改变, 进行AC瞬态传输特性测试时, 节点(V_{out}, V_g)的电压扰动较为明显. 这种扰动受掺杂浓度、杂质分布的影响, 而检测输出节点与输入节点的逻辑相关性则可直接检测到掺杂型硬件木马是否存在.

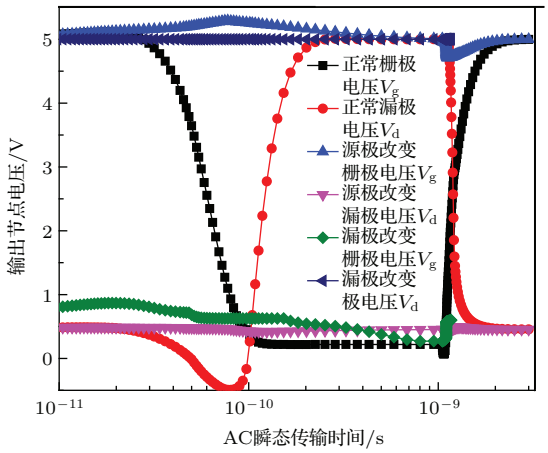

图4 反相器AC瞬态传输特性

Fig. 4. AC transient time of inverter.

2.2 热载流子注入型硬件木马

热载流子注入型木马是热载流子注入到MOSFET器件栅极氧化层中, 产生界面态、氧化层陷阱引起MOSFET器件的退化或失效. 当热载流子的能量高于Si-SiO_2的界面势垒时, 将会注入到氧化层中(对于电子注入的能量是3.2 eV, 而空穴的注入能量是4.5 eV, 因此热载流子注入型木马更容易出现在nMOSFET中)[10]. 随着MOSFET器件特征尺寸不断缩小, 栅极氧化层的厚度也不断地变薄, 栅氧化层中的电场不断增强, 尤其是靠近漏极区的电场迅速增加, 使得热载流子注入引起器件退化或失效的可靠性问题日益突出[11]. 热载流子有四个来源分别是: 沟道热电子(channel hot electron, CHE), 漏极雪崩热载流子(drain avalanche hot carrier, DAHC), 衬底热电子(substrate hot electron, SHE), 二次产生的热电子(SSHE). 本文只讨论起主要作用的CHE和DAHC过程.

1) 沟道热电子(CHE)

当漏极电压V_d等于栅极电压V_g时, 且它们都高于源极电压, 部分电子在MOSFET器件的漏极区被电场加速成为热电子, 当能量高于Si-SiO_2的界面势垒时, 便注入到栅氧化层中形成栅电流.

2) 漏极雪崩热载流子(DAHC)

当漏源电压V_{ds}至少2倍于V_{gs}时, 在MOSFET器件的漏极区附近会产生很高的电场加速

电子, 热电子的注入量受控于漏源电压V_{ds}. 高速的载流子又会与Si晶格发生碰撞, 再次产生电子-空穴对, 由于其雪崩机理造成大量热电子注入栅极氧化层, 使得器件严重退化或失效. 薄栅器件学研究已表明, 热电子注入造成的器件退化主要可以归结于三个因素: 氧化层的电荷注入和俘获; 由于电荷的俘获引起的界面态; Si—H键断裂引起的界面态. 由于目前微纳电子结构的器件偏压都很低, 不会产生明显的电荷俘获效应. 另外, 空穴的注入量远比电子注入量要小得多, 因此复合界面态也不可以忽略. 一般认为硅片经SC-1和SC-2清洗剂后表面带有很多的Si—H的悬挂键. Si—H悬挂键强度很弱, 注入的热电子打断Si—H键后造成氢释放, 形成的界面态是薄栅器件退化和失效的主要原因[10,11].

当界面态平衡时, 界面态的产生速率等于H的释放速率, 即Si和H键的复合速率为: $\beta_{\rm p}N_{\rm it}n_{\rm H}(0)$, 其中$N_{\rm it}$为界面态密度, $n_{\rm H}(0)$为界面处H的浓度. 则产生速率等于逃离速率方程为

$$\frac{{\rm d}N_{\rm it}}{{\rm d}t} = k\frac{I_{\rm ds}}{W}\exp\left(-\frac{\varphi_{\rm it}}{q\lambda E_{\rm m}}\right) - \beta_{\rm p}N_{\rm it}n_{\rm H}(0) = \frac{D_{\rm H}n_{\rm H}(0)}{L_{\rm H}}, \tag{1}$$

(1)式中, $D_{\rm H}$和$L_{\rm H}$分别是H的有效扩散系数和有效扩散距离, 并假设$N_{\rm it}|_0 = 0$, 则有

$$\frac{\beta_{\rm p}L_{\rm H}}{2D_{\rm H}}N_{\rm it}^2 + N_{\rm it} = tk\frac{I_{\rm ds}}{W}\exp\left(-\frac{\varphi_{\rm it}}{q\lambda E_{\rm m}}\right), \tag{2}$$

(2)式为静态应力的MOSFET在热载流子注入下的界面态产生过程[10]. 因此, 通过使用基于受主表面陷阱密度函数的热载流子退化(hot carrier degradation, HCD)模型仿真对单个nMOSFET进行退化压力测试. 如图5(a)所示, 在栅极氧化层厚度分别为1 nm和50 nm条件下, 器件退化条件为$V_{\rm g} = 1.5$ V, $V_{\rm d} = 3.3$ V, $T = 300$ K, 压力测试后在$V_{\rm d} = 0.1$ V下进行测量. MOSFET的阈值电压为$V_{\rm th}$, 在理想情况下漏极电流与漏源电压无关可表示为

$$I_{\rm D} = K_{\rm n}(V_{\rm gs} - V_{\rm th})^2, \tag{3}$$

(3)式中$K_{\rm n}$是电子迁移率, 栅极氧化层电容和沟道宽长比的函数. 器件压力测试结果是基于Newton方法给出. 从图5(a)和图5(b)中可以看出nMOSFET器件的阈值电压随压力测试时间的增长而迅速增加, nMOSFET的阈值电压随着HCD退化压力测试温度的降低有明显的线性增加趋势. 在同样的退化压力条件下增加栅极氧化层厚度(相对于改变了$K_{\rm n}$), 阈值电压虽然有所增加, 但可以有效地改善热载流子造成的器件退化问题.

一般情况下, 可靠性试验环境温度越高, 器件退化的速度就越快. 而热载流子注入型木马在常温或高温下致使芯片失效或退化并不明显, 而在低温下会被激活造成芯片退化或失效, 这是因为高能量热电子经过硅层时, 如果环境温度越高, 引起的Si晶格振动就越剧烈, 与热电子碰撞的概率就增大, 热电子与晶格碰撞后能量会损耗, 能量低于3.2 eV时将不能越过Si-SiO_2的界面势垒, 无法注入到氧化层中. 通过分析被热载流子注入的器件特性[12,13], 可以得出结构参数和工艺参数的物理型硬件木马对芯片功能的影响, 从而提出检测物理型硬件木马的方法.

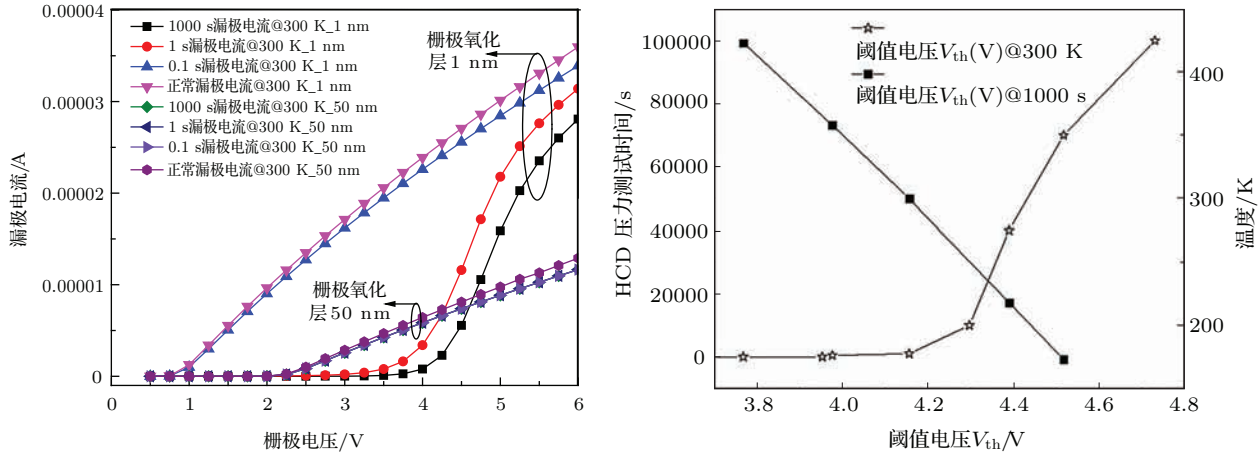

图5 (a) 300 K下MOSFET在不同氧化层厚度和不同时长HCD压力测试下的漏电流; (b) MOSFET在不同温度, 不同时长HCD压力测试下阈值电压的变化

Fig. 5. (a) The drain current of MOSFET in different oxide thicknesses and times of HCD stress at 300 K; (b) the variation of threshold voltage of MOSFET at under different temperatures and HCD stress times.

由图5可以看出, HCD压力测试的时间在1 s之后器件的阈值电压退化明显. 为了在不同温度下进行HCD压力测试时得出更明显的结论, 选取1 s和1000 s时间长度, T在173, 218, 300, 358, 423 K温度下进行相同的HCD压力测试. 1 s时间内的HCD压力测试结果如图6 (a)所示, 图6 (b)所示为1000 s时间内的HCD压力测试结果. 对比图5和图6的结果, 可以得出这样的结论: 为了更容易地检测出热载流子注入型硬件木马的存在, 需对芯片进行更长时间的HCD压力测试, 但随着压力测试时间的增长, 必须在更低的温度下进行功能测试才能区分出芯片中隐藏的热载流子型硬件木马. 因此, 在实际测试过程中应选取芯片器件能工作的最低温度进行检测.

单个nMOSFET器件的宽长比为W/L = 5 μm : 2 μm, 循环进行1000 s的HCD压力测试后接入反相器逻辑电路中, 进行DC直流、AC瞬态输出特性仿真. DC直流输出特性如图7 (a)所示, AC瞬态输出特性如图7 (b)所示. 从图7中可以看出, 带有退化器件的逻辑功能模块的DC直流传输特性与压力测试前相比变化明显, 而高频传输特性与压力测试前相比变化不明显.

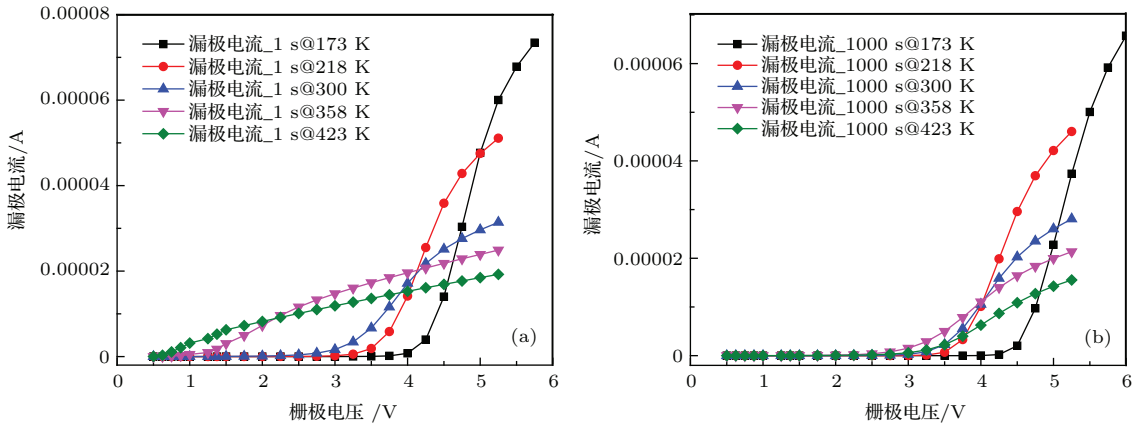

图6 (a) MOSFET在不同温度下, 1 s时长的HCD压力测试的栅-漏电流; (b) MOSFET在不同温度下, 1000 s时长的HCD压力测试的栅-漏电流

Fig. 6. (a) The gate-drain current of MOSFET in different temperatures and 1 s HCD stress time; (b) the gate-drain current of MOSFET in different temperatures and 1000 s HCD stress time.

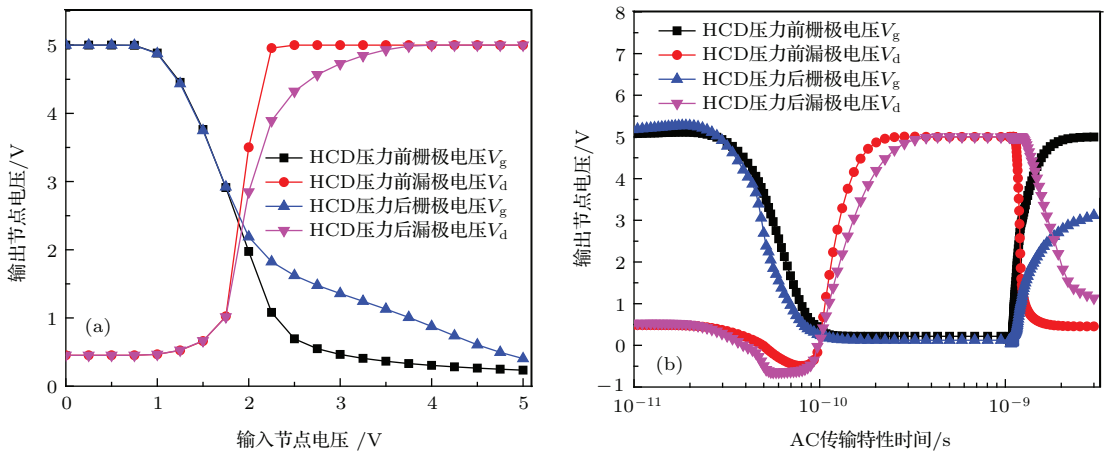

图7 (a) HCD压力测试前后反相器的DC直流输出特性; (b) HCD压力测试前后反相器的AC瞬态输出特性

Fig. 7. (a) The comparison DC transient characteristics of inverter image before and after HCD stress test; (b) the comparison AC transient characteristics of inverter image before and after HCD stress test.

在电流-电压分析中, MOSFET的漏电流可以表示为

$$I_{\rm D} = \frac{W}{2L}\mu_{\rm n}C_{\rm ox}[2(V_{\rm gs}-V_{\rm th})V_{\rm ds}-V_{\rm ds}^2], \quad (4)$$

将$W\mu_{\rm n}C_{\rm ox}/2L$定义为工艺电导参数, 因此, W/L作为电流-电压特性的设计参量. 为了验证热载流子注入对工艺电导参数W/L的影响, 对相同的器件结构、不同宽长比W/L的器件接入逻辑电路进

行功能测试. 将不同宽长比的nMOSFET器件在218 K下、1000 s的HCD压力测试后再接入反相器中进行逻辑功能测试. DC直流、AC瞬态传输特性结果如图8(a)和图8(b)所示. 从图8中得出相同的结论: 带有退化器件的逻辑功能模块的DC直流传输特性变化明显, 而瞬态传输特性没有明显变化. 这是因为随着器件宽度W和沟道长度L的不断缩小, 其物理特性更适合于高频瞬态信号的传输, 器件尺寸的缩小带来高频响应特性的提升, 弥补了器件退化造成的响应特性下降的影响. 由于在漏极区附近会形成较高的电场, 因此漏极端器件退化比其他区域更加明显, 所以在DC直流特性测量时, 只需测量图2中$V_{\rm out}$, $V_{\rm d}$节点即可明显发现热载流子注入的迹象.

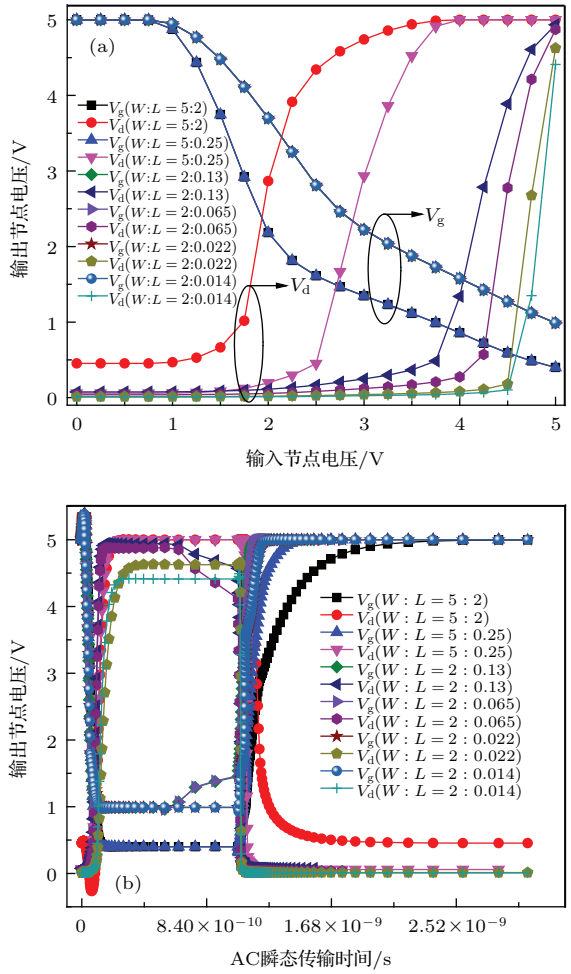

图8 (a) 由不同宽长比退化nMOSFET器件组成的反相器DC直流输出特性; (b) 由不同宽长比退化nMOSFET器件组成的反相器AC瞬态输出特性

Fig. 8. (a) DC transient characteristics of inverter circuit which consist of a normal nmos and a degradation nmos in different ratio of width and length; (b) AC transient characteristics of inverter circuit which consist of a normal nmos and a degradation nmos in different ratio of width and length.

从功率定律中可以得到$\Delta V_{\rm th} \propto (1/W)^a$, $\Delta V_{\rm th} \propto (1/L)^b$. 参数$a$和$b$都是可以从功率定律中得出的斜率, $a \approx 0.31$, $b \approx 3.51$, 斜率值b明显比a大很多, 表明器件沟道长度L比宽度W更具有决定性, 同时对HCD压力测试更敏感. 考虑多个参数的影响, HCD压力测试对阈值电压漂移的模型可以表示为[14]

$$\Delta V_{\rm th} = Ct^n (1/W)^a (1/L)^b \exp(c/V_{\rm d}). \quad (5)$$

另外, MOSFET的频率响应随着栅极长度的减小而增大. 对于单边pn结而言, 漏极的最大耗尽层的宽度为

$$x_{\rm d} = \sqrt{\frac{2\varepsilon(V_{\rm bi} + V_{\rm d})}{eN_a}}, \quad (6)$$

可以看出当栅极长度从L缩小到κL时, 为了能保持恒定的水平电场, 漏极电压必须从$V_{\rm d}$缩小到$\kappa V_{\rm d}$, 最大栅极电压也必须从$V_{\rm gs}$缩小到$\kappa V_{\rm gs}$, 氧化层的厚度需从$t_{\rm ox}$缩减到$\kappa t_{\rm ox}$. 随着氧化层的厚度缩减, 当栅-源电压产生的电场足够大时(电场强度大约为6×10^6 V/cm)将导致器件的失效. 通常不会考虑氧化层击穿的问题, 但随着热电子的涌入, 穿过氧化层的电子被俘获, 在氧化层内产生净负电荷密度, 热电子诱导的栅极电流能在很长时间内存在, 负电荷陷阱会造成阈值电压的正向漂移, 严重时则造成氧化层的击穿[15].

3 物理型硬件木马的检测

对于物理型硬件木马的检测, 首先要判断的是掺杂型硬件木马. 对功能模块进行测试时, 如果发现DC直流功能特性与AC瞬态传输特性都没有预期的输出, 则考虑是功能模块损坏或注入了掺杂型硬件木马. 而对于热载流子注入型硬件木马的检测, 目前已知的方法有以下两种: 1) 基于器件延时的监测技术[16−19], 该技术是通过一个额外的电路对晶体管的传输时延进行监测, 从而实现对热载流子注入型硬件木马的检测目的, 但由于路径延时需要高精度的计时工具, 且需要统计分析, 因此对测试人员专业素养要求过高; 2) 基于环路振荡器发生频率对实际物理参数的影响[20−22], 环路振荡器产生的频率也取决于电源电压$V_{\rm dd}$的值, 如果$V_{\rm dd}$下降则会增加门电路的延迟, 因此, 其周期时间的延迟增加, 相当于振荡频率的下降. 从本文的仿真结果看出, 无论是掺杂型硬件木马还是热载流子注

入型硬件木马, 其 AC 瞬态传输特性的变化都不如 DC 直流传输特性变化显著. 从实际检测物理型硬件木马的流程出发, 首先要确定芯片或器件的制线工艺; 其次通过测定芯片功能模块的 DC 直流传输特性, 确定芯片的功能是否完整, 并可以排除是否注入掺杂型硬件木马; 如果功能特性都正常或存在参数漂移的现象时, 考虑可能存在热载流子注入型硬件木马. 改变物理环境或进行器件寿命、压力测试, 使得快速地暴露出注入的物理型硬件木马. 因此, 我们提出检测热载流子注入型硬件木马的流程如下:

1) 在室温下, 测量功能模块的 DC 直流传输特性参数, 确保要测试的所有功能模块工作正常, 以检测可能存在的掺杂型硬件木马;

2) 在保证器件能正常工作的情况下, 选取最低温度, 在漏极上施加电压 $V_{\rm ds}$ 至少 2—5 倍于栅极电压 $V_{\rm gs}$, 施加高场压力 16 h 后, 测量功能模块的 DC 直流传输特性参数;

3) 取出芯片恢复到室温后, 标准供电下, 测量功能模块的 DC 直流传输特性参数;

4) 对比过程 1 和过程 2 的测量结果, 查看是否存在参数漂移现象;

5) 如果将步骤 3 中结果与步骤 1 的结果对比, 基本不存在漂移现象, 则重复上述 1—3 的过程若干次 (制线工艺越小, 晶体管尺度越小, 次数越多), 时间每次增长一倍;

6) 如果经过步骤 5 后出现了 DC 直流传输特性漂移的现象, 则将芯片置于 250 °C 的恒温烘干箱中 160 h;

7) 取出芯片后恢复到室温, 再次在标准供电下测量功能模块的 DC 直流传输特性参数;

8) 从步骤 7 中取出的结果与步骤 1 中的结果进行对比, 如果两次结果的 DC 直流传输特性参数基本一致, 则认定芯片中存在热载流子注入型硬件木马.

由于热载流子注入具有可恢复的物理特性, 在低温和高电场压力测试下使其暴露出明显的器件失效特性. 本文提出的这种流程提供了一个没有定量化的测试指导参考. 虽然物理型硬件木马是在晶圆或流片是注入进去, 而并非只影响注入的器件或所在的功能模块, 文献 [23] 中指出硬件木马在内存阵列控制器模块中具有“感染”的连锁反应特性, 因此可以在芯片关键模块中注入几个物理型硬件木马, 依靠其扩散感染作用引起全模块失效. 而上述检测过程仅对一直处于开启的并含有硬件木马的功能模块有用. 一个特殊不常用的模块为了能尽可能地暴露物理木马的存在, 需使用微探针侵入芯片后进行片上模块化测试.

4 结 论

本文介绍了两种物理型硬件木马的形成原理, 通过 ATLAS 器件仿真工具结合 SmartSpice 对由 2 个 nMOSFET 组成的反相器逻辑模块进行电路仿真, 对反相器逻辑模块的 DC 直流传输特性、AC 瞬态传输特性进行了输出仿真对比. 针对热载流子注入型硬件木马, 使用 1000 s 热载流子 HCD 器件退化压力测试, 在不同温度下和不同器件宽长比 W/L 下进行了电路逻辑输出分析. 仿真结果揭示了在低温条件下对输出漏极节点上进行 DC 直流传输特性监测, 更容易检测出硬件木马的存在. 对于多金属层芯片底层逻辑电路模块的检测, 需使用聚焦离子束 (focused ion beam, FIB) 等芯片侵入式分析工具. FIB 配合微探针 (micro-probe) 使用, 检测 MOSFET 电路中 $V_{\rm d}$ 漏极节点输出特性参数, 逐步缩小检测区域范围最终能够确认被恶意修改的器件. 总结仿真结果在一定基础上提出一个具体且针对物理型硬件木马可操作的检测方法和操作流程. 如果物理型与逻辑型硬件木马混合使用, 只有在特定条件下通过逻辑才触发物理型木马, 并利用物理型硬件木马的器件“感染”特性逐渐扩大器件失效范围, 可以实现长期深层次的隐蔽性. 进一步的工作是通过使用 FIB、芯片微探针等侵入式分析工具对功能模块进行检测, 探索对非一直开启的逻辑功能模块中物理型硬件木马检测技术.

本文作者特别感谢北京航空航天大学朱艳菊博士的理论模型分析与讨论.

参考文献

[1] Tehranipoor M, Koushanfar F 2010 *IEEE Design & Test of Computers* **27** 10

[2] Alkabani Y, Koushanfar F 2009 *Proceedings of Computer-Aided Design-Digest of Technical Papers* San Jose, CA Nov. 2–5, 2009 p123

[3] Banga M, Hsiao M S 2009 *Proceedings of Hardware Oriented Security and Trust* Francisco, CA July 27–27, 2009 p104

[4] Koushanfar F, Mirhoseini A 2011 *IEEE Trans. Inform. Forensics and Security* **6** 162

[5] Koushanfar F, Mirhoseini A, Alkabani Y 2010 *Proceedings of the Information Hiding* Calgary, AB June 28–30, 2010 p17

[6] Koushanfar F, Potkonjak M 2007 *Proceedings of Design Automation Conference* San Diego, CA June 4–8, 2007 p268

[7] Wei S, Potkonjak M 2011 *Proceedings of the Network and System Security* Milan Sept. 6–8, 2011 p176

[8] Wei S, Li K, Farina, Koushanfar, Miodrag Potkonjak 2012 *Proceedings of Design Automation Conference* San Francisco, CA June 3–7, 2012 p90

[9] Becker G T, Regazzoni F, Paar C, Burleson W P 2013 *Cryptographic Hardware and Embedded Systems* (California: Santa Barbara) pp197–214

[10] Zhang X W, En Y F 2015 *The Reliability Evaluation Method of Semiconductor Integrated Circuit* (Beijing: Electronic Industry Press) p142 (in Chinese) [章晓文, 恩云飞 2015 半导体集成电路的可靠性及评价方法 (北京: 电子工业出版社) 第 142 页]

[11] Liu H X, Zheng X F, Hao Y 2005 *Acta Phys. Sin.* **54** 1373 (in Chinese) [刘红侠, 郑雪峰, 郝跃 2005 物理学报 **54** 1373]

[12] Li Z H, Liu H X, Hao Y 2006 *Acta Phys. Sin.* **55** 820 (in Chinese) [李忠贺, 刘红侠, 郝跃 2006 物理学报 **55** 820]

[13] Xu J P, Li C X, Wu H P 2005 *Acta Phys. Sin.* **54** 2918 (in Chinese) [徐静平, 李春霞, 吴海平 2005 物理学报 **54** 2918]

[14] Lei X Y, Liu H X, Zhang K, Zhang Y, Zheng X F, Ma X H, Hao Y 2013 *Chin. Phys. B* **22** 047304

[15] Donald A N (translated by Xie S) 2015 *An Introduction to Semiconductor Devices* (Beijing: Electronic Industry Press) pp224–245 (in Chinese) [唐纳德 A N 著 (谢生 译) 2015 半导体导论 (北京: 电子工业出版社) 第 224—245 页]

[16] Austin T, Blaauw D, Mudge T, Flautner K 2004 *Computer* **37** 57

[17] Ahmad I, Kornain Z, Idros M F M 2006 *Proceedings of Optoelectronic and Microelectronic Materials and Devices* Perth, WA Dec. 6–8, 2006 p298

[18] Sato T, Kunitake Y 2007 *Proceedings of the Quality Electronic Design* San Jose, CA March 26–28, 2007 p539

[19] Agarwal M, Paul B C, Zhang M, Mitra S 2007 *Proceedings of the VLSI Test Symmposium* Berkeley, CA May 6–10, 2007 p277

[20] Quader K, Ko P, Hu C, Fang P, Yue J 1992 *Proceedings of the Reliability Physics Symposium* San Diego, CA March 31–April 2, 1992 p16

[21] Zhang J, Chu S F S 2002 *IEEE Trans. Electron. Dev.* **49** 1672

[22] Zhang X H, Tehranipoor M 2011 *Proceedings of the Design, Automation & Test in Europe Conference & Exhibition* Grenoble March 14–18, 2011 p1

[23] Shiyanovskii Y, Wolff F, Rajendran A, Papachristou C, Weyer D, Clay W 2010 *Proceedings of the Adaptive Hardware and System* Anaheim June 15–18, 2010 p215

Physical hardware trojan failure analysis and detection method*

Luo Yang† Wang Ya-Nan

(*China Information Security Evaluation Center, Beijing 100876, China*)

(Received 16 February 2016; revised manuscript received 8 March 2016)

Abstract

The semiconductor industry is rapidly developing in the global market, and chip design companies usually purchase the third-party EDA tools in order to shorten the design cycle of IC and reduce manufacturing cost. Therefore, in the IC chip production procedure there exist a lot of insecurity factors, and the hardware security of IC chips becomes the most important issue of the national security defense. Physical hardware trojan will modify the value of register, leak sensitive data and cause device degradation failure. Furthermore, the physical hardware trojans only modify the physical properties of the circuit chip rather than injects the malicious functional circuit. They are hidden more deeply than logical hardware trojans. Therefore, it is far-reaching significance issues for the hardware trojan detection methods and national security to study logic circuit transmission characteristics and the chip degradation failure physical mechanism which are caused by injection physical hardware trojans. In this paper, a metal-oxide-semiconductor field-effect transistor (MOSFET) device with injection dopant hardware trojan is realized by using ATHENA process simulation system to achieve the ion implantation process. The ATLAS simulation devices are tested using hot carrier injection degradation (hot carrier degradation is denoted by HCD) stress model for the degradation failure process which is caused by injecting the hot carrier injection hardware trojan (HCHT) into the MOSFET device. Another normal MOSFET combines with dopant hardware trojan MOSFET or hot carrier injection hardware trojan MOSFET to comprise the same inverter logic circuit by using the ATLAS two-dimensional (2D) device simulation system with SmartSpice instructions mode. The effect on logic circuit output characteristics caused by physical hardware trojan is studied by using Spice simulation to output the DC and AC transient time characteristics. It is also studied how the W/L value of a hardware trojan transistor influences the output characteristics of the logic circuit. We design an experiment to study transient characteristics of the same inverter logic module which consists of different W/L values of a transistor at different temperatures. The experiment is realized by Spice circuit simulation. In this paper, the effects of the variations of the HCD stress intensity and temperature on output characteristic are analyzed for hot carrier injection hardware trojan. The results indicate that the negative effect of hardware trojan on logic circuit DC current output characteristic is more obvious than AC transient time characteristic. Thus, we propose an effective method and a convenient procedure to detect the injection physical hardware trojan in packaged chips. Furthermore, the test process is a feasible operation method of detecting physical hardware trojan.

Keywords: hardware trojan, hot carrier injection, device degradation, failure analysis

PACS: 06.60.Mr, 06.90.+v, 07.05.Fb **DOI:** 10.7498/aps.65.110602

* Project supported by the National Natural Science Foundation of China (Grant No. 61402536).

† Corresponding author. E-mail: mddr@163.com