软件定义主动屏蔽层生成及防护技术研究

赵毅强[1],高 雅[1],马浩诚[1],张启智[1],叶 茂[1],夏显召[1,2],何家骥[1]
(1. 天津大学微电子学院,天津 300072; 2. 中国汽车技术研究中心,天津 300000)

摘 要: 由于安全芯片信息泄露事件的频发,提高安全芯片的防护能力刻不容缓. 本文提出了一种软件定义主动屏蔽层生成及防护系统构建的方法,无需具有安全背景知识即可在短时间内生成高熵值的顶层金属布线防护网络,有效遮蔽芯片加密模块等关键组件,同时满足合规的相关要求. 本文所提出的方法可由软件定义布线的类型、线宽、线间距等参数,能够适用于不同的工艺节点,且相关技术已经在华虹130 nm的工艺下进行了仿真验证,实现了主动屏蔽层与2种屏蔽层完整性检测电路的结合,验证了屏蔽层对聚焦离子束和微探针攻击的检测效果,实现了对侵入式物理攻击的有效感知与防护.

关键词: 集成电路安全; 主动屏蔽层; 哈密顿结构; 检测电路; 抗物理攻击
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112(2022)06-1381-08
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210957

Research on Software-Defined Active Shield Protection Technology

ZHAO Yi-qiang[1], GAO Ya[1], MA Hao-cheng[1], ZHANG Qi-zhi[1], YE Mao[1], XIA Xian-zhao[1,2], HE Jia-ji[1]
(1. *Institute of Microelectronics, Tianjin University, Tianjin* 300072, *China*;
2. *China Automotive Technology and Research Center, Tianjin* 300000, *China*)

Abstract: With the frequent occurrence of security chip information leakage incidents, it is imperative to improve the protection capabilities of security chips. This paper proposes a method of software-defined active shield generation and protection system construction, which can generate a high-entropy top-level metal protection network in a short time without the need for security background knowledge. The active shield can effectively shield key components such as chip encryption modules, and at the same time meet the regulatory requirements. The method proposed in this paper can define wiring type, line width, line space, and other parameters through the software, and can be applied to different process nodes. Relevant technologies have been simulated, and verified under the Hua Hong 130 nm process, realizing the combination of the active shield and two kinds of integrity detection circuits, verifying the detection effect of active shield against focused ion beam and microprobe attacks, and realizing effective perception and protection against intrusive physical attacks.

Key words: integrated circuit safety; active shield; Hamiltonian structure; detection circuit; resistance to physical attack

1 引言

近年来,随着信息安全领域日新月异的发展,安全芯片作为信息安全领域的底层基础和硬件保障,被广泛应用于涉及敏感信息场景下的许多关键基础设施中. 与此同时,随着攻击技术的不断进步,越来越多的针对安全芯片的攻击手段和案例被报道出来,如前美国军事安全专家Christopher Tarnovsky对英飞凌的SLE66 CLPE安全芯片实施微探针攻击获取关键数据[1],引起人们对芯片安全的高度重视.

随着物理攻击技术的发展,安全芯片面临的物理攻击威胁可分为3种:侵入式攻击、非侵入式攻击[2]和半侵入式攻击[3]. 其中,侵入式攻击以聚焦离子束(Focused Ion Beam,FIB)攻击[4]和微探针攻击为代表,这两类攻击通常进行组合,通过破坏芯片封装、反向工程来获得芯片版图,修改内部走线,读取存储数据[5]. 侵入式攻击是现有物理攻击中最有效、最直接的手段,为此,我国针对密码模块和安全芯片于2012年、2014年和2015年先后制订了《安全芯片密码检测准则》[6]《密码

收稿日期:2021-07-23;修回日期:2022-01-05;责任编辑:孙瑶
基金项目:国家自然科学基金重点基金(No.61832018);国家自然科学基金青年基金(No.62004112)

模块安全技术要求》[7]和《密码模块安全检测要求》[8]行业标准,其中明确规定了安全类芯片必须具有抗物理侵入攻击和非侵入攻击的能力.主动屏蔽层因其良好的抗侵入式物理攻击能力,成为保障硬件安全的主流手段.

主动屏蔽层的防护水平与屏蔽线网络的复杂程度密切相关,一些商用微处理器、智能卡等,采用了平行等势线、蛇形走线、螺旋线、希尔伯特曲线、摩尔曲线等拓扑结构[9,10].这些布线结构的信息熵值大多在0.6~0.8 bit之间,具有较明显的规律性,易于被分析破解;此外,大部分屏蔽层缺少完整性检测电路,因此防护效果难以保障.为了进一步提高芯片的安全性,本文基于哈密顿随机回路的拓扑结构进行优化,针对不同的应用场景和工艺条件,提出了一系列灵活易用的软件定义主动屏蔽层布线生成算法,不仅兼容多种节点的工艺,而且能够高效生成复杂无序的主动屏蔽层,其信息熵值高达0.95 bit,结合自研的屏蔽层完整性检测电路,能够极大地提高芯片的安全水平,最终形成了具备较高自动化程度的布线生成软件,具有较高的应用价值.

2 软件定义主动屏蔽层防护技术

主动屏蔽层的整体架构如图1所示,由屏蔽层、完整性检测电路以及被保护区域3部分组成.由于微探针和FIB攻击的方式是直接接触芯片,因此通常选用顶层或次顶层金属通过一层或多层金属的走线组成复杂的屏蔽层网络.屏蔽层不仅可以有效遮蔽金属层下方的加密模块、存储器模块等关键组件[11],而且还可以在通入检测信号后与完整性检测电路相结合,将参考检测信号与经过屏蔽层的待检测信号进行比对,监控屏蔽层的完整性状态,有效识别对屏蔽层的攻击行为[12],一旦识别到芯片受到攻击,立即产生报警信号通知主控单元,由主控单元进一步采取其他的防护手段.

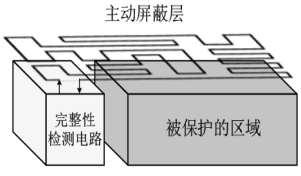


图1 软件定义主动屏蔽层系统整体架构

2.1 主动屏蔽层生成算法

应用于安全芯片的主动屏蔽层需要在完整覆盖芯片待保护区域的基础上,具备高随机性、高复杂度的特点.目前已知的基于哈密顿随机路径拓扑结构的生成算法主要为循环合并算法(Cycle Merging Algorithm,CMA)[13],但是其生成速率极大地受到布线面积的限制,即布线面积增大后,生成效率迅速降低.为了提高屏蔽层的生成效率,本文采用预先分类的思想,将回路按照能否合并进行分类,每次合并过程只在可以合并的回路中进行随机选择,避免了无效合并对时间的消耗,提升了布线效率.

依据预先分类的思想,基于改进人工鱼群算法[14,15]的随机哈密顿路径生成算法(Artificial Fish-Swarm Random-Hamiltonian Algorithm,AFSRHA)[16]被提出来.将人工鱼群算法与随机哈密顿路径的生成特点相结合,通过概念以及行为特征定义的改进,实现了一种高效的大面积随机哈密顿路径自动生成算法.

人工鱼群算法即通过模拟鱼类群体社会行为的智能寻优算法.现有的AFSRHA算法只能生成线宽线间距相等的哈密顿回路,即布线的宽度变大后,线间距也随之变大.不同集成电路工艺,对于最小线宽线间距会有不同的要求,并不全都是相等的,可调的线宽线间距会提升算法的灵活性,满足不同的布线需求.此外,较宽的线间距会导致攻击者不必切割金属布线层,探针即可从布线间距中扎入底层待保护电路并获取关键信息.

为了实现线宽与线间距均可根据需求进行调节的功能,在算法上将原本代表线宽线间距的参数一分为二,分别对线宽和线间距进行量化,且在最初的格点划分步骤中,将线宽和线间距2个参数进行归一化处理,在回路合并完成后会形成1个封闭图形,借助语言脚本对线宽线间距分别定义,将归一化的格点坐标转换为物理连线实际坐标,随后组合线宽线间距作为一个整体沿着封闭图形的边缘进行描绘,实现对线宽和线间距的区分处理,从而实现对算法的改进和优化.

AFSRHA算法的流程图和执行图分别如图2、图3所示.实现过程首先将布线面积的长和宽用线宽线间距归一后的参数进行划分,等效为图3(a)所示的格点.在算法的初始化阶段,将相邻的4个格点构成1个如图3(b)所示的正方形并标号,代表1条人工鱼,本文以25条人工鱼为例.每条人工鱼都标记有活跃度属性以及觅食、追尾、群聚3种行为.活跃度与鱼群和食物的距离成反比.活跃度为0的人工鱼为自由鱼群,是算法初始化后的初始鱼群;活跃度为1的人工鱼是比自由鱼群靠近食物的活跃鱼群,自由鱼群通过追尾行为可以加入活跃鱼群;活跃度为2的人工鱼则是正在进食的中心鱼群.随机选择1条人工鱼的位置投放食物,通过觅食行为,它的活跃度将变成2,活跃鱼群通过群聚行为可以加入中心鱼群.中心鱼群中的人工鱼数目被记录在公告板上,算法执行过程中公告板数据会一直更新,直到公告板上的数据达到规定数值.图3(c)中随机选择了18号鱼投食,18号鱼通过觅食行为形成的回路C即中心鱼群的初始回路.公告板更新为1,剩下的自由鱼数目为24.在追尾行为中,图3(c)中18号鱼周围的

17号、19号、3号、23号4条自由鱼活跃度提升为1,在其中随机选择1条19号活跃鱼通过群聚行为加入中心鱼群,回路C扩大如图3(*d*)所示,公告板更新为2,24号、14号、20号鱼通过追尾行为加入到活跃鱼群.接下来在17号、23号、13号、24号、20号5条鱼中随机选择1条通过群聚行为加入中心鱼群,回路C扩大如图3(*e*)所示,公告板更新为3,以此类推直到所有人工鱼被合并形成图3(*f*)所示的哈密顿回路.

总而言之,AFSRHA算法的执行过程就是通过随机选择的方式遍历待保护区域的格点,且每个格点只访问1次,最终形成1条封闭的随机哈密顿路径.由于鱼群具有追尾行为,每次随机选择的格点都会产生有效合并,故而提升了算法的效率.

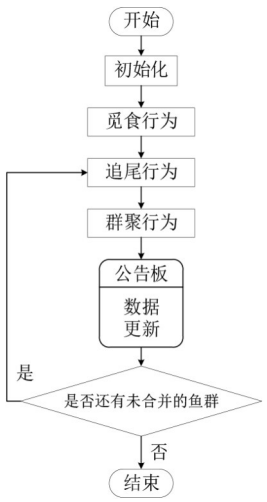


图2　AFSRHA算法流程图

2.2　熵值计算与效率评估

针对主动屏蔽层算法的评价指标主要是熵值和执行时间.熵值代表了算法生成的随机哈密顿路径的复杂度,是最首要的指标,只有保证了复杂度的屏蔽层才能具有良好的防护效果.其次是衡量算法效率的指标,即执行时间.随着集成电路规模的指数型增长,如何在短时间内生成大面积的屏蔽层布线也是算法需要重点考虑的一个方面.

区分屏蔽层布线的随机性和非随机性的一个明显特征是布线的平均各向同性.根据这个标准,当布线在所有方向上的分布几乎相等的时候,屏蔽效果更好;反之,当布线方向都趋同于一个方向时,布线的规律性较为明显,屏蔽效果不佳.根据这一思想,算法采用文献[17]中提出的熵值作为评价回路质量的指标.对于一个二维布线回路,熵值计算式为 $E(d)=\sum_{d\in\{x,y\}}-P(d)\times\log_2 P(d)$,上限值为1.0 bit,其中 $P(d)$ 是布线路径沿 d 方向的概率.将该计算式添加到布线算法中,可以计算任意布线回路的熵值,合理评价其复杂度指标.

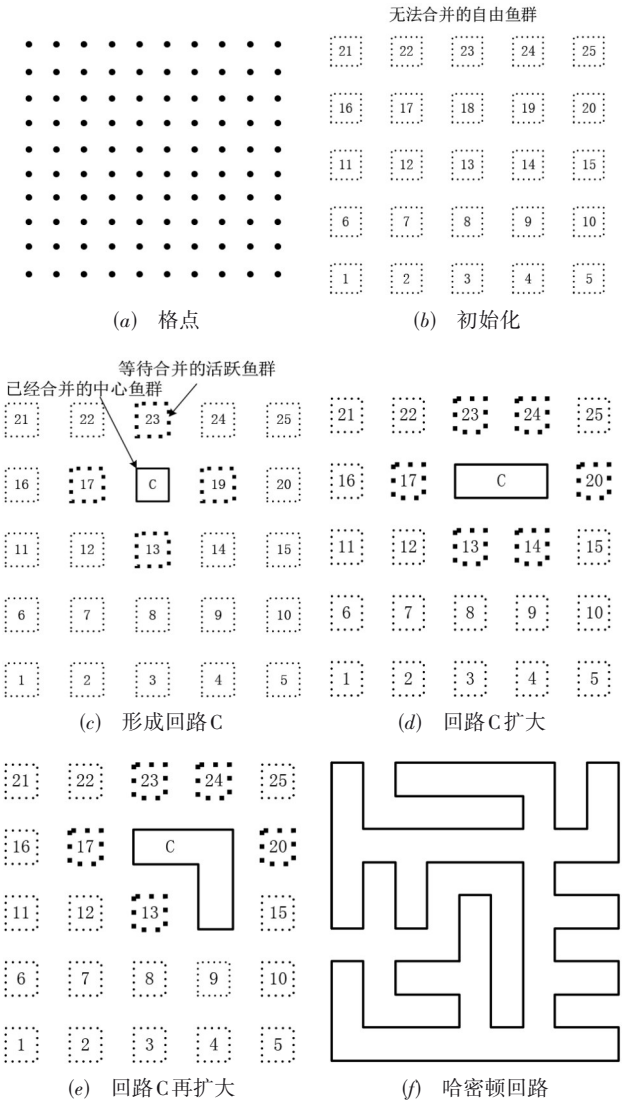


图3　AFSRHA算法步骤图

为了比较随机哈密顿布线与其他商用布线的复杂度,设计了随机蛇形走线算法,将其熵值与AFSRHA算法熵值进行比较,结果如表1所示.

表1　随机蛇形走线与AFSRHA算法熵值比较

面积大小/μm²	随机蛇形线	AFSRHA
	熵值/bit	熵值/bit
6 400	0.625	0.997
10 000	0.736	0.992
22 500	0.682	0.998
40 000	0.643	0.993

主动屏蔽层算法的生成时间计算通过MATLAB2016的算法执行时间(Execution Time,ET)来衡量,基于MATLAB2016平台,利用CMA算法与AFSRHA算法对同样面积的区域进行布线,比较它们的生成时间,

结果如表2所示.

表2 CMA与AFSRHA算法运行时间及熵值比较

面积大小/μm²	CMA		AFSRHA	
	生成时间/s	熵值/bit	生成时间/s	熵值/bit
400	12.2	0.965	0.9	0.992
900	129.4	0.991	1.3	0.997
1600	697.9	0.988	1.5	0.997
2500	2454.4	0.997	2.1	0.996
3600	7620.3	0.995	2.7	0.995

可以看出,基于同样的面积和平台,熵值指标方面AFSRHA算法生成的布线复杂度明显高于随机蛇形走线算法;时间效率方面AFSRHA算法明显高于CMA算法.

2.3 完整性检测电路设计原理

虽然屏蔽层的设计极其精密,但是依然存在被切割攻击的可能,需要更加主动地进行安全监测. 因此,高复杂度的主动屏蔽网络需要与完整性检测电路相配合,才能实现抵抗FIB以及微探针攻击的效果. 针对直接切割屏蔽层的FIB攻击,设计了通断检测电路;针对更高级的FIB和微探针攻击,设计了随机码流型检测电路,防止攻击者在切割屏蔽层后,通过主动打入码流使检测电路失效.

2.3.1 通断检测电路设计

通断检测电路模块如图4所示,其时序图如图5所示. 利用2个触发沿相异的D触发器D3和D4(其中D3为上升沿触发,D4为下降沿触发)对输入CLK和NET端口的信号分别进行分频,分频结果为图5中的VCLK信号和VNET信号. 在主动屏蔽层的起点注入CLK信号,在主动屏蔽层终点接受到的信号为NET信号,检测电路将CLK信号和NET信号进行比对. D1和D2这2个触发沿相异的D触发器对主动屏蔽层通断情况进行检测,采集时钟VCLK信号上升沿和下降沿时刻的VNET信号值,输出如图4中的D1_Q和D2_Q信号,经过异或门Y、反相器I得到最终的报警信号alarm_2. 一旦攻击者利用FIB切割金属线,NET信号将消失,该检测电路可以立即识别到攻击,图5所示的alarm_2信号翻转为高电平.

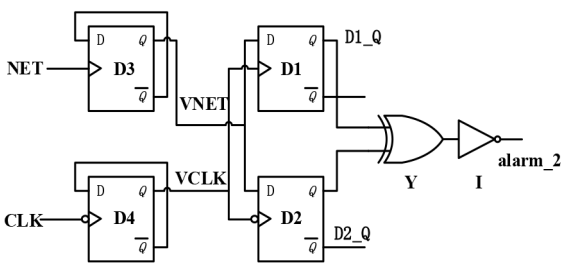


图4 通断检测电路模块

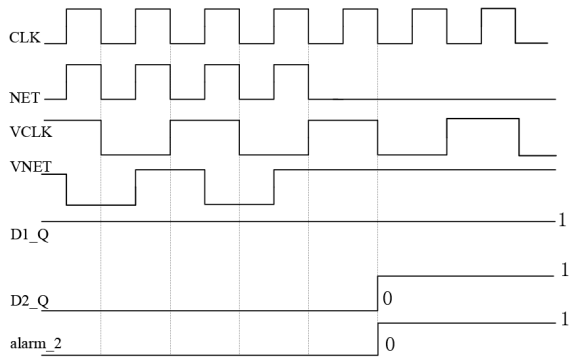


图5 通断检测电路时序图

2.3.2 随机码流型检测电路设计

主动型的通断检测在更加复杂的分析和攻击场景下,因为码流相对简单,依然有被复制破解的可能. 因此,随机码流型检测电路由随机信号产生电路向屏蔽层起点注入随机码流,在终点处将流过屏蔽层的码流与输入屏蔽层的码流进行比对,通过对码流的一致性分析来判断布线层是否受到物理攻击.

目前主流的随机信号产生电路均采用线性反馈移位寄存器(Linear Feedback Shift Register,LFSR)来生成随机码流[12]. 针对单通道的顶层金属布线层,通常会选择64 bit的LFSR中的1 bit为布线层提供随机码流,电路设计完成后,通入布线层的码流也随之固定. 一旦攻击者获取到随机发生器的种子,并注入相同的随机码流,现有的完整性检测电路将失效. 为了增加攻击难度,本文提出了新型的电路将在每个时钟周期随机切换输入到布线层的码流,进一步提高了电路的安全性.

此外,覆盖于芯片顶层的主动屏蔽层具有较长的金属走线,极易受到强烈变化的空间电磁场的干扰. 如果采用传统的单比特主动式码流检测技术,容易出现将异常干扰判定为攻击,从而出现误报警的现象. 本设计中的比对模块,使用累加器记录一定周期内的比对结果,将累加器结果与设定的安全阈值比较,当其超过阈值时,报警信号被触发,提升了报警的准确度.

比对电路的工作过程如图6所示. 为尽可能减少磁场等外部因素对检测结果的影响,信号比对过程将每8 bit视为1个比对周期,连续3个比对周期视为1个检测周期. 针对每个比对周期,将8 bit的LFSR产生的随机码流信号A1通入屏蔽层,将其与流经屏蔽层的输出信号B1进行单比特的逐一比对,0和1分别代表比对结果的成功和失败. 累加器将比对结果从0开始累加,若累加值超过2,则判断为受到攻击,输出高电平表示情况异常;若累加值等于1或2,则认为检测信号受到了外界干扰,输出低电平表示情况正常;若累加值等于0,则认为没有受到攻击,输出低电平正常信号. 针对每个检测周期内,如果其中3个比对周期都输出高电平异常

信号,则认为受到了攻击,最终报警信号 alarm_1 输出高电平,否则输出低电平正常信号.

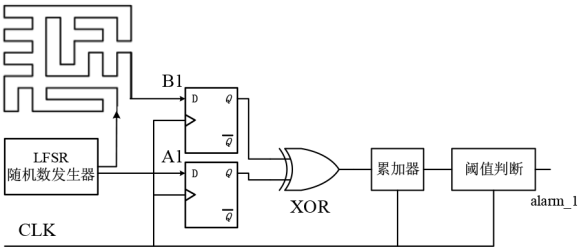


图6　比对电路模块图

3　实验结果与分析

3.1　实验设置

针对前文提出的通断和随机码流型2种检测电路架构,通过对主动屏蔽层模拟的FIB攻击,对能否检测出布线完整性被破坏攻击进行了验证. 实验选用华虹130 nm工艺库来实现检测电路的数字流程. 在10 MHz的时钟频率下,完成了从DC综合、Encounter布局布线、PrimeTime静态时序分析、VCS平台后仿以及PrimeTime-PX中平均功耗分析和基于时序的功耗分析等全部流程.

对于通断检测电路,给流过屏蔽层的时钟信号NET赋值与时钟信号CLK同周期的方波信号,在一段时间后将NET的赋值直接置0,来模拟FIB切断屏蔽线的攻击场景,并观察报警信号是否置1.

对于随机码流型检测电路,给流过屏蔽层的码流信号B1赋值与时钟信号CLK同周期的方波信号,来模拟FIB与微探针攻击切断屏蔽线后,向屏蔽线中注入码流的攻击场景,并观察一段时间后报警信号是否置1.

3.2　通断检测电路实验结果

对于通断检测电路,后端实现过程采用了M1至M5层金属进行布线,数字版图如图7所示.

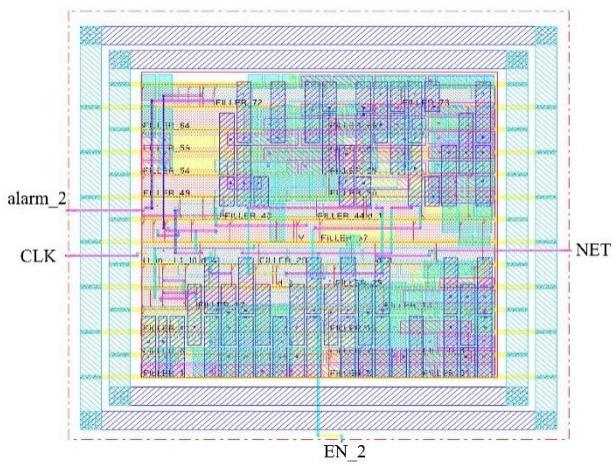


图7　通断检测电路数字版图

在测试文件中将通断检测电路的NET信号赋值为与时钟同频的方波信号,当FIB切断屏蔽线的攻击发生时,NET信号置0. 从图8的仿真结果可以看出,一旦屏蔽层被切割发生断路,仅仅需要1个时钟周期检测电路即可识别到攻击,报警信号 alarm_2 被触发,电路响应迅速且功能正确.

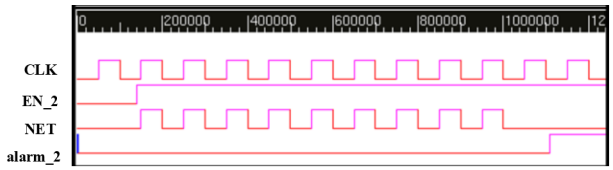


图8　通断检测电路仿真波形

3.3　随机码流型检测电路实验结果

对于随机码流型检测电路,后端实现过程采用M1至M5层金属进行布线,数字版图如图9所示.

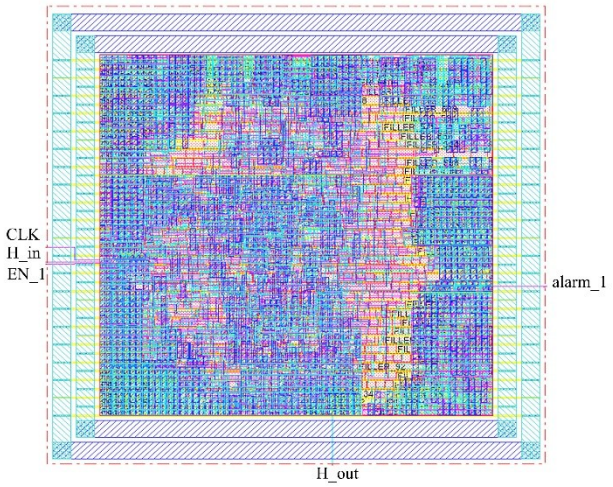


图9　随机码流型检测电路数字版图

当FIB与微探针攻击切断屏蔽线并注入码流进行攻击时,在电路的测试文件将B1信号赋值为与时钟同频的方波信号. 对于通入主动屏蔽层的随机码流信号A1,采用“双重随机”的方式生成. 利用6位LFSR的输出在每个时钟周期为变量m赋值一次,同时,选取LFSR输出的第m位赋值给A1信号,保证了随机码流信号的双重随机性.

图10为仿真电路. 从仿真结果可以看出,累加信号 cnt_total 通过累加的方式来记录比对周期内比对失败的情况,第1个比对周期中超过2 bit比对失败,因此在下一个比对周期中累加信号计数加1;第2个比对周期中同样超过2 bit比对失败,因此第3个比对周期中累加信号计数再加1. 当识别到连续3个比对周期都存在超过2 bit的比对错误后,仅仅需要2个时钟周期检测电路即可识别到攻击,触发报警信号 alarm_1,电路响应迅速且功能正确.

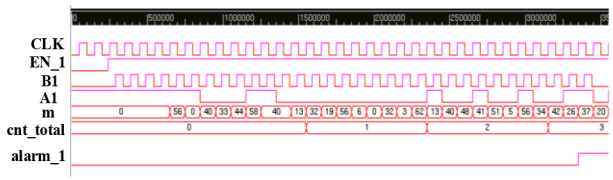
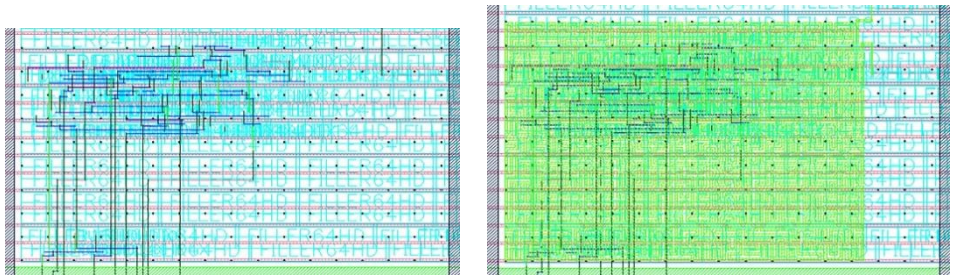


图 10 随机码流型检测电路仿真波形

3.4 不良效应评估

较长的主动屏蔽层布线可能会造成电路的天线效应,同时码流信号的通入导致了信号线之间的寄生电阻、寄生电容,这些不良效应可能会影响到待保护电路的功能,因此在布线阶段采用跳线、添加常闭传输门(NC)或反偏二极管(diode cell)等方式来消除天线效应.

为了测试寄生电阻和电容的影响,选择在 1 个 8 位伪随机数发生电路模块上覆盖主动屏蔽层布线,并打入码流信号,测试其 8 位输出信号值是否受到影响. 实验采用 virtuoso 平台实现主动屏蔽层与电路版图的连接,如图 11 所示,抽取网表文件与寄生参数文件进行 20 000 ns 的 hspice 仿真,比较结果如图 12、图 13 所示. 可以看出主动屏蔽层产生的寄生电阻和电容参数对底层电路的扰动十分微小,时间精度在 0.1 ns 左右.



(a) 未覆盖屏蔽层的电路 (b) 覆盖屏蔽层的电路

图 11 主动屏蔽层与电路版图的连接

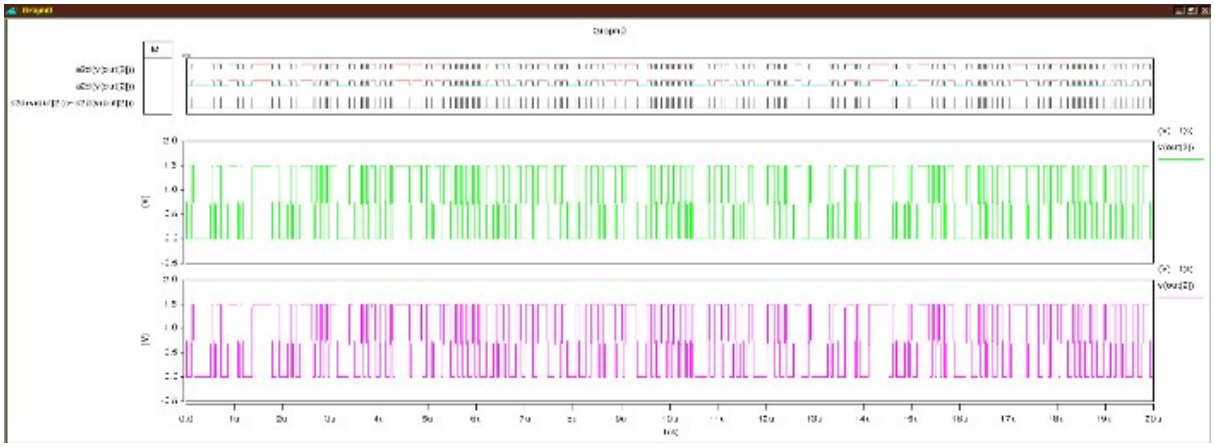


图 12 有覆盖(上)和无覆盖(下)主动屏蔽层的电路 out[2]信号输出的仿真波形比较

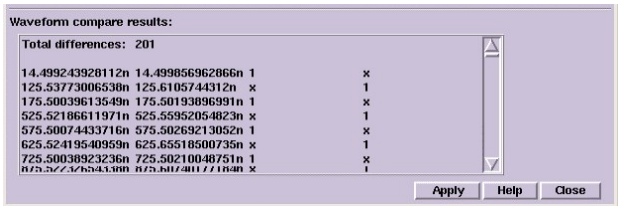


图 13 有无覆盖主动屏蔽层的电路 out[2]信号输出的仿真波形比较结果

3.5 开销分析

实验在不同工艺的情况下分析了通断检测电路和随机码流型检测电路基于时间的功耗信息以及平均功耗信息. 表 3 从面积、主电路中的检测电路面积占比、端口、单元数、功耗 5 个方面总结了 2 个检测电路的测试信息. 实验结果显示,2 种检测电路可全部由数字流程实现,工艺兼容性强,鲁棒性高,功耗、面积开销也相对较小. 此外,2 种检测电路可直接作为 IP 连同主动屏蔽层灵活植入到待保护电路的数字版图中,极大地节约了设计的时间成本,整套流程可以将安全芯片的防护等级提升至国家二级标准[6].

4 结论

本文提出了一种软件定义主动屏蔽层防护技术,基于随机哈密顿拓扑结构生成布线网络,结合主动屏

表3　检测电路测试结果表

	通断检测电路	随机码流型检测电路
面积	$70\times70\ \mu m^2$	$180\times180\ \mu m^2$
面积占比	0.16%	10.5%
端口	NET, CLK, EN_2, alarm_2	A1, B1, CLK, EN_1, alarm_1
单元数	91	1455
功耗	6.26×10^{-6}~9.63×10^{-6} W	1.28×10^{-4}~1.98×10^{-4} W

蔽层完整性检测电路,形成一套与集成电路设计流程相匹配的芯片防护系统. 作为有效抵御FIB和微探针攻击的主流防护手段,主动屏蔽层已经成为高安全等级芯片必备的安全保障结构. 未来可能会在利用主动屏蔽层主动对抗热故障注入、光故障注入、电磁故障注入等非侵入式攻击方面进行深入研究,同时会对本文设计芯片的流片结果进行基于实际芯片的验证. 随着人们对集成电路信息安全重视程度的提高,主动屏蔽层防护技术必将拥有广阔的应用前景.

参考文献

[1] TARNOVSKY C. Security Failures In Secure Devices[R]. Las Vegas: Black Hat DC Presentation, 2008.

[2] DAS D, MAITY S, NASIR S B, et al. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain[C]//2017 IEEE International Symposium on Hardware Oriented Security and Trust. New York: IEEE, 2017: 62-67.

[3] SKOROBOGATOV S P, ANDERSON R J. Optical fault induction attacks[J]. Lecture Notes in Computer Science, 2002, 2523: 2-12.

[4] 马向国, 顾文琪. 聚焦离子束加工技术及其应用[J]. 微纳电子技术, 2005, 42(12): 575-577, 582.
Ma X G, Gu W Q. Nanofabrication and applications of focused ion beam technology[J]. Micronanoelectronic Technology, 2005, 42(12): 575-577, 582. (in Chinese)

[5] TILBORG V H, JAJODIA S. Encyclopedia of Cryptography & Security[M]. Boston：Springer, 2011: 301-307.

[6] 国家密码管理局. 安全芯片密码检测准则: GM/T 0008—2012[S].

[7] 国家密码管理局. 密码模块安全技术要求: GM/T 0028—2014[S].

[8] 国家密码管理局. 密码模块安全检测要求: GM/T 0039—2015[S].

[9] SKOROBOGATOV S P. Semi-Invasive Attacks: A New Approach to Hardware Security Analysis[D]. Cambridge: University of Cambridge, 2005.

[10] 叶世芬. 安全芯片物理防护研究[D]. 杭州: 浙江大学, 2005.
YE S F. A Study of Security Chip Physical Protection[D]. Hangzhou: Zhejiang University, 2005. (in Chinese)

[11] 张赟. 抗物理攻击安全芯片关键技术研究[D]. 天津: 天津大学, 2016.
ZHANG Y. Study on Key Technique of Anti-Physical-Attack Security Chip[D]. Tianjin: Tianjin University, 2016. (in Chinese)

[12] 赵毅强, 辛睿山, 甄帅, 等. 顶层金属防护层研究综述[J]. 微电子学, 2019, 49(4): 558-562, 573.
ZHAO Y Q, XIN R S, ZHEN S, et al. Research review on top-metal active shield[J]. Microelectronics, 2019, 49(4): 558-562, 573. (in Chinese)

[13] BRIAIS S, CARON S, CIORANESCO J M, et al. 3D hardware canaries[C]//Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2012: 1-22.

[14] 李晓磊, 钱积新. 人工鱼群算法: 自下而上的寻优模式[C]//中国系统工程学会2001过程系统工程年会论文集. 北京: 中国石化出版社, 2001: 76-82.
LI X L, QIAN J X. Artificial fish school algorithm: Bottom-up optimization model[C]//Proceedings of the 2001 Process Systems Engineering Conference of the Chinese Society of Systems Engineering. Beijing: China Petrochemical Press, 2001: 76-82. (in Chinese)

[15] 李晓磊, 邵之江, 钱积新. 一种基于动物自治体的寻优模式: 鱼群算法[J]. 系统工程理论与实践, 2002, 22(11): 32-38.
LI X L, SHAO Z J, QIAN J X. An optimizing method based on autonomous animats: Fish-swarm algorithm[J]. Systems Engineering-Theory & Practice, 2002, 22(11): 32-38. (in Chinese)

[16] 赵毅强, 辛睿山, 王佳, 等. 基于人工鱼群算法的随机哈密顿回路生成方法: CN107688848B[P]. 2020-07-21.
ZHAO Y Q, XIN R S, WANG J, et al. Artificial Fish School Algorithm Based Random Hamiltonian Hoop Generation Method: CN107688848B[P]. 2020-07-21. (in Chinese)

[17] BRIAIS S, CIORANESCO J M, DANGER J L, et al. Random active shield[C]//2012 Workshop on Fault Diag-

nosis and Tolerance in Cryptography. Piscataway: IEEE, 2012: 103-113.

作者简介

赵毅强 男,1964年12月出生,河北辛集人. 现为天津大学教授,博士生导师,国家重点学科负责人,天津市电子科学与技术示范实验中心主任,天津市成像与传感微电子技术重点实验室副主任,天津市红外成像技术工程中心副主任,科技部、军科委项目、天津市科技项目评审专家. 主要研究方向为智能传感处理电路与系统设计、集成电路安全检测、抗物理攻击、侧信道评测与防护等.

E-mail: yq_zhao@tju.edu.cn

高 雅 女,1998年8月出生,辽宁东港人. 2020年6月毕业于天津大学微电子学院,获得工学学士学位. 2020年9月就读于天津大学微电子学院,现为硕博连读生. 主要研究方向为数字电路安全.

E-mail: gaoyaya@tju.edu.cn

夏显召(通讯作者) 男,1988年10月出生,安徽淮北人. 2019年毕业于天津大学微电子学院. 现为中国汽车技术研究中心与天津大学联合培养博士后. 主要研究方向为汽车芯片测评技术.

E-mail: xiaxianzhao@catarc.ac.cn

何家骥 男,1990年9月出生,河北衡水人. 博士,天津大学特聘副研究员,IEEE会员. 主要研究方向为数字集成电路(全流程)设计、集成电路硬件安全、硬件形式化验证、密码芯片设计与安全分析.

E-mail: dochejj@tju.edu.cn