基于线性无关矩阵的按需解锁硬件混淆方法

汪鹏君[1,2],叶顺心[2],张跃军[2],张会红[2]
(1. 温州大学电气与电子工程学院,浙江温州 325035; 2. 宁波大学信息科学与工程学院,浙江宁波 315211)

摘 要: 硬件混淆是一种通过定向修改软核、固核或硬核的芯片保护方法,已成为当前芯片安全领域的研究热点.本文针对多个硬件IP(Intellectual Property)核按需解锁安全保护,提出一种基于线性无关矩阵的按需解锁硬件混淆方案.该方案首先利用线性无关矩阵算法,生成可隔离外部输入密钥与内部解锁信号的随机矩阵;然后采用冗余和黑洞状态组合混淆技术,对IP核进行加密;最后根据用户需求,通过矩阵乘运算实现按需解锁.在SMIC 65 nm CMOS(Complementary Metal Oxide Semiconductor)工艺下,采用ITC(International Test Conference)基准电路和密码算法IP核实现硬件混淆.实验结果表明,所设计电路具有多IP核按需解锁功能,额外的面积和功耗开销均小于8%,且能有效防御寄存器翻转攻击、代码覆盖率攻击以及成员泄密攻击.

关键词: 线性无关矩阵; 冗余和黑洞状态; 按需解锁; 硬件安全
中图分类号: TP331 **文献标识码:** A **文章编号:** 0372-2112(2022)03-0703-07
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210061

Method of Unlock-on-Demand Hardware Obfuscation Based on Linear Independent Matrix

WANG Peng-jun[1,2], YE Shun-xin[2], ZHANG Yue-jun[2], ZHANG Hui-hong[2]
(1. *College of Electrical and Electronic Engineering, Wenzhou University, Wenzhou, Zhejiang* 325035, *China*;
2. *Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo, Zhejiang* 315211, *China*)

Abstract: Hardware obfuscation is a method of chip protection through targeted modification of soft core, solid core or hard core. It has become a research hotspot in the field of chip security. In order to unlock multiple hardware IP cores on demand and improve their security, an unlock-on-demand hardware obfuscation scheme based on the linear independent matrix is proposed in this paper. Firstly, by using the linear independent matrix algorithm, the scheme generates a randomized matrix to isolate the external input key and internal unlock signal. Secondly, it encrypts multiple IP cores based on a combination of redundant and black-hole states obfuscation technologies. Finally, according to users' needs, it unlocks chip on demand through matrix multiplication. By using the SMIC 65 nm CMOS(Complementary Metal Oxide Semiconductor) process, the ITC(International Test Conference) reference circuit and encryption algorithm IP core are implemented for the proposed hardware obfuscation design. The experimental results have shown that the designed circuit has the advantages of unlock-on-demand, low additional area and power consumption (both less than 8%), and effective defenses against code coverage attacks, register flip attacks and member leakage attacks.

Key words: linear independent matrix; redundant and black-hole states; unlock-on-demand; hardware security

1 引言

随着集成电路规模不断扩大,单块芯片上集成的IP核数量日益增多.例如人工智能芯片已集成多个IP(Intellectual Property)核:中央处理器、图像处理器、神经网络处理器、专用集成电路、现场可编程门阵列、神经元进程处理器等[1].为缩短研发周期,芯片设计方通常直接购买商业IP核实现部分模块功能.但随之而来的问题是芯片安全在全球供应链中频繁受到各种威胁.此外,由于商业IP核的盗版现象,合法的集成电路公司每年亏损约数亿美金的全球利润.因此保护芯片制造供应链中IP核的安全已经越来越受到集成电路领域的重视[2].同时由于芯片设计中IP核数量的增多与

收稿日期:2021-01-04;修回日期:2021-03-22;责任编辑:梅志强
基金项目:国家自然科学基金(No.61874078, No.61871244);国家重点研发计划项目(No.2018YFB2202100);宁波市公益性计划项目(No.202002N3134)

模块的细分,产生了按需解锁的市场需求.

现存硬件IP保护方法主要分为两大类,即基于认证的保护方法和基于混淆的保护方法. Sarkar等[3]提出在数字信号处理器(Digital Signal Processor, DSP)中植入难以擦除的"数字水印"或者认证签名以辨别真伪. 这种水印是一个或多个输入输出激励对,在正常工作情况下难以被发现,只有当输入特定序列时才会被激活,且仅在IP设计者利益受到侵害时才判定IP所有权,不能主动防御硬件IP的盗版攻击或逆向工程. 基于混淆的IP保护方法中,Yousra等[4]提出用远程激活的方式管理IP核,利用有限状态机的单个状态复制和物理不可克隆模块实现硬件加密. Chakraborty等[5]提出一种网表级混淆技术,可同时实现混淆和验证. Bhunia等[6]提出基于密钥混淆控制和数据流低开销的寄存器传输级硬件IP保护技术,将RTL(Register Transfer Level)代码转换成状态控制和数据流图,实现有限状态机的硬件混淆. Zhang等[7]提出基于物理不可克隆函数-有限状态机(Physical Unclonable Function- Finite State Machine, PUF-FSM)的硬件混淆,对FPGA(Field Programmable Gate Array)的IP核进行保护,并实现Pay-Per-Device的强制付费许可机制. 之后,Zhang等[8]又提出实用的逻辑混淆(Practical Logic Obfuscation, PLO)技术,以低开销实现电路网表级保护. 以上硬件混淆方法都是通过在状态机中加入冗余状态,防止电路初始化后直接进入正常工作模式,但是当电路进入正常工作模式便失去保护. Dofe等[9]提出一种基于黑洞状态的状态机混淆方法,在电路复位后直接进入正常初始状态,而没有考虑初始化信息泄露的问题. 以上基于冗余或者黑洞状态混淆的加密方法忽略了团队成员泄密的威胁. 张等[10]提出利用矩阵正交的方法加密多个硬件IP核,以降低团队成员泄密的威胁. 但是利用控制模块的正交运算所得密钥不具有唯一性. Sun等[11]提出一种按需解锁FPGA硬件IP的方法,能够有效防御恶意攻击,但不能直接应用于专用集成电路.

鉴此,本文提出一种基于线性无关矩阵的按需解锁硬件混淆方法. 该方法既能隐藏电路初始化信息,又能提高状态机正常工作模式的安全性. 在实现多硬件IP核按需解锁功能时,能以较小的硬件开销达到防御多种攻击的目的.

2 线性无关矩阵与信号折叠分组

2.1 线性无关矩阵

在线性代数中,若向量组的任意一个向量都不能由其他几个向量线性表示,则称这组向量线性无关[10]. 如式(1)所示,有m个n维向量,若只能找到唯一常量组$k_1=k_2=\cdots=k_{m-1}=k_m=0$使式(2)成立,则向量$\boldsymbol{\alpha}_1$, $\boldsymbol{\alpha}_2$, $\cdots$, $\boldsymbol{\alpha}_m$之间线性无关.

$$\begin{cases}\boldsymbol{\alpha}_1=[a_{11}\ a_{12}\ \cdots\ a_{1n}]^{\mathrm{T}}\\ \boldsymbol{\alpha}_2=[a_{21}\ a_{22}\ \cdots\ a_{2n}]^{\mathrm{T}}\\ \vdots\\ \boldsymbol{\alpha}_m=[a_{m1}\ a_{m2}\ \cdots\ a_{mn}]^{\mathrm{T}}\end{cases}\tag{1}$$

$$0=k_1\boldsymbol{\alpha}_1+k_2\boldsymbol{\alpha}_2+\cdots+k_{m-1}\boldsymbol{\alpha}_{m-1}+k_m\boldsymbol{\alpha}_m\tag{2}$$

将式(1)的向量组合成矩阵$\boldsymbol{A}_{m\times n}=[\boldsymbol{\alpha}_1,\ \boldsymbol{\alpha}_2,\ \cdots,\ \boldsymbol{\alpha}_m]^{\mathrm{T}}$,称该矩阵为线性无关矩阵. 矩阵$\boldsymbol{A}_{m\times n}$与另一向量$\boldsymbol{B}_{n\times 1}$相乘得内积$\boldsymbol{C}_{n\times 1}$,称该运算为矩阵乘运算. 若已知矩阵$\boldsymbol{A}$与内积$\boldsymbol{C}$求解向量$\boldsymbol{B}$,则当矩阵$\boldsymbol{A}_{m\times n}$的秩(矩阵中线性无关行向量的极大数目)大于$n$时$\boldsymbol{B}$不存在;当秩等于$n$时可得唯一向量$\boldsymbol{B}$;当秩小于$n$时可得无数个向量$\boldsymbol{B}$. 未知向量$\boldsymbol{B}$的求解数量$R$如式(3)所示,rank表示矩阵的秩.

$$R=\begin{cases}0 & ,\mathrm{rank}>n\\ 1 & ,\mathrm{rank}=n\\ +\infty & ,\mathrm{rank}<n\end{cases}\tag{3}$$

由此得到式(4)所示的基于线性无关矩阵的解锁方法. 该方法将线性无关的n阶矩阵$\boldsymbol{A}$植入芯片,与用户输入密钥序列$\boldsymbol{K}$相乘,得到向量$\boldsymbol{O}$,然后经信号折叠分组解锁IP核,故外部输入密钥并不是解锁IP核的直接匹配对象,即线性无关矩阵有效阻隔外部输入密钥和解锁信号.

$$\boldsymbol{O}_{n\times 1}=\boldsymbol{A}_{n\times n}\cdot\boldsymbol{K}_{n\times 1}\tag{4}$$

2.2 线性无关矩阵算法

随机线性无关矩阵能防御芯片的非法复制,因此可利用单位矩阵的逆向初等行变换,得算法1所示的线性无关矩阵算法. 该算法首先生成n阶单位矩阵$\boldsymbol{H}_{n\times n}$,然后循环$D$次如下步骤:(1)随机生成两个常量$t$和$s$;(2)随机选取$\boldsymbol{H}$中一行向量$\boldsymbol{\alpha}$,将其所有元素乘以$t$;(3)随机选取$\boldsymbol{H}$中两行向量$\boldsymbol{\beta}$和$\boldsymbol{\gamma}$,将$\boldsymbol{\beta}$乘以$s$并与$\boldsymbol{\gamma}$相加取代$\boldsymbol{\gamma}$向量;(4)随机互换$\boldsymbol{H}$中两行向量. 最后输出线性无关矩阵$\boldsymbol{A}$.

算法1 线性无关矩阵算法

generate diagonal matrix $\boldsymbol{H}_{n\times n}=\begin{pmatrix}1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & 1\end{pmatrix}$

for (i=0; i<D; i++){

random generate constant t and s

random select a vector $\boldsymbol{\alpha}$ in $\boldsymbol{H}$

$\boldsymbol{\alpha}\leftarrow t\boldsymbol{\alpha}$

random select two vectors $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ in $\boldsymbol{H}$

$\boldsymbol{\gamma}\leftarrow\boldsymbol{\gamma}+s\boldsymbol{\beta}$

random select two vectors $\boldsymbol{\delta}$ and $\boldsymbol{\theta}$ in $\boldsymbol{I}$

$\boldsymbol{\delta}\leftrightarrow\boldsymbol{\theta}$

}

$\boldsymbol{A}\leftarrow\boldsymbol{H}$

2.3 信号折叠分组

因为矩阵元素在芯片设计中以二进制表示,所以矩阵乘运算结果非常冗长. 为缩短解锁信号位数,可将式(4)中 $\boldsymbol{O}_{n\times1}$ 向量的元素折叠分组. 图1给出了利用异或门对向量单个元素 a_2 进行折叠分组的方法. 由于元素 a_2 的高位为0,有效信息集中于低位,所以可按顺时针将源信号折叠成短位数信号. 折叠后的信号被分为校验信号 Q 与冗余跳转密钥 P. 校验信号为解锁对应IP核的使能信号,冗余跳转密钥能使状态机经过冗余状态进入正常状态. 为使外部输入密钥具有唯一性,通过校验模块输出黑洞密钥 C_i. 该模块首先判定 Q 的正确性,正确则继续判定冗余跳转密钥 P 的正确性;否则跳过本次判定. 所有判定都正确则输出黑洞密钥 C_i 冗余跳转密钥和黑洞密钥共同组成IP核的解锁信号.

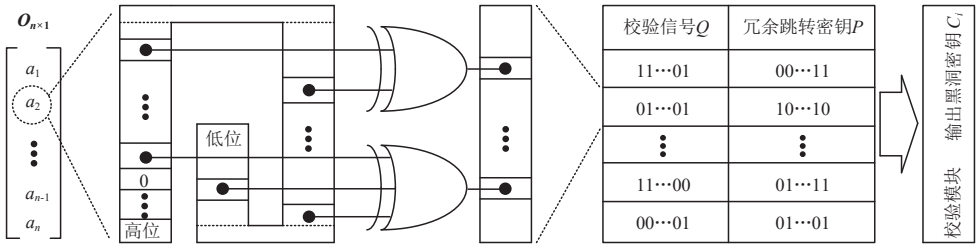

图1　信号折叠分组

3 按需解锁硬件混淆设计

芯片设计中IP核数量增多与模块细分,为按需解锁提供应用背景[12]. 根据市场或不同客户的需求,芯片设计方可设计多个混淆功能模块并购买一定数量混淆后的IP核实现不同需求的芯片. 设计方在售卖芯片给终端用户时,可以按需解锁相对应的IP核或功能模块.

3.1 冗余-黑洞状态混淆方法

为防御IP供应链中的状态机破解,提出图2所示的结合冗余状态和黑洞状态的硬件混淆方法. 冗余状态为添加到原始状态机初始状态前的多个状态,在电路进入正常状态前起保护作用;黑洞状态为添加到原始状态机周围的多个单向跳转状态,在电路进入正常状态后发挥防护效果. 当上电或者复位后,电路初始化状态为冗余状态 RS_0. 读取冗余跳转密钥后,状态机判定密钥是否与 P_0、P_1、P_2 对应,是则跳转到正常初始状态 S_0,否则进入冗余状态跳转循环. 冗余状态能防止攻击者不断复位以获得正确状态机的运行信息. 为防止攻击者通过置位状态机寄存器使电路跳过冗余状态直接工作于正常状态,故在正常状态周围设计单方向跳转的黑洞状态 B_i、B_i' 或 B_i''. 当状态机进入正常工作模式,在每个时钟上升沿采样黑洞密钥 C_1,若 C_1 不正确则状态机跳转到环绕于正常状态周围的黑洞状态. 根据 C_1 不同错误情况,状态机跳转进入 B_i、B_i' 或 B_i'',一旦跳转进入黑洞状态将不可逆,即电路只会在多个黑洞状态间跳转而不能重新进入正常状态. 为实现冗余-黑洞状态混淆,可针对RTL代码进行修改. 首先在代码端口声明处添加冗余跳转密钥 P 和黑洞密钥 C_i,并声明利用格雷码编码的冗余状态和黑洞状态;然后修改电路初始化状态为冗余状态 RS_0;最后将密钥信号设置为状态机跳转判定条件.

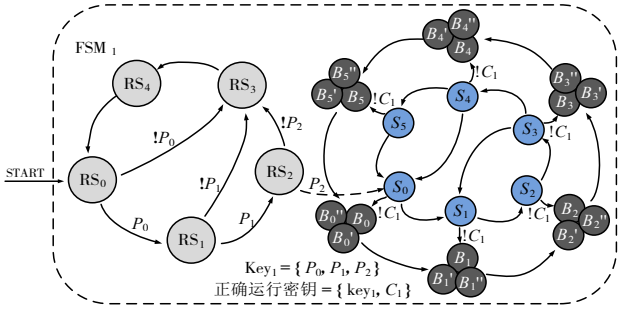

图2　冗余-黑洞状态混淆

3.2 按需解锁硬件结构

具有按需解锁功能的硬件结构包括密钥向量输入端口、线性无关矩阵存储模块、矩阵乘模块、信号折叠分组模块、解锁信号寄存器组和IP核. 图3为按需解锁多IP结构. 随机生成的线性无关矩阵与外部输入密钥向量在矩阵乘模块中进行运算. 所得二进制信号进入信号折叠分组模块进行压缩,并且生成冗余跳转密钥与黑洞密钥. IP核读取密钥,使状态机进入冗余循环、

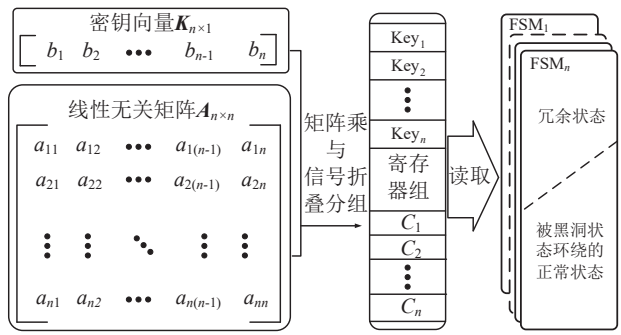

图3　多IP核按需解锁结构

黑洞循环或者正常工作模式,实现按需解锁功能.

3.3 按需解锁交互协议

交互协议表示设计团队、晶圆厂以及用户之间的芯片与密钥传递方案. 严格遵守交互协议可有效减少不必要的商业损失. 图4为按需解锁交互协议. 设计方(Design House, DH)将设计分成N个模块交由N个设计者完成或从第三方IP发布者购买商业IP. 设计者或IP发布者向原始状态机添加随机数量冗余状态和黑洞状态,同时生成对应的冗余跳转密钥以及黑洞密钥作为单个IP核的解锁信号投入到密钥数据库. 设计方利用算法生成随机的线性无关矩阵,将N个模块设计成整体,经由前端和后端各流程产生GDSII(Geometry Data Standard II)文件交由晶圆厂代工并封装. 用户根据设计方发布的功能清单选择所需要的功能模块,并将勾选清单和购买资金交给设计方. 设计方依据清单,从密钥数据库中计算按需解锁的密钥数据包,并生成芯片正确工作的状态信息交由用户. 用户将密钥数据包输入芯片后,获取稳定的芯片工作数据信息. 工作数据信息并没有明确的对应关系,且无法由此推算到具体内部情况. 用户将读取到的芯片工作数据信息和设计方所提供正确信息对比,判定是否成功解锁.

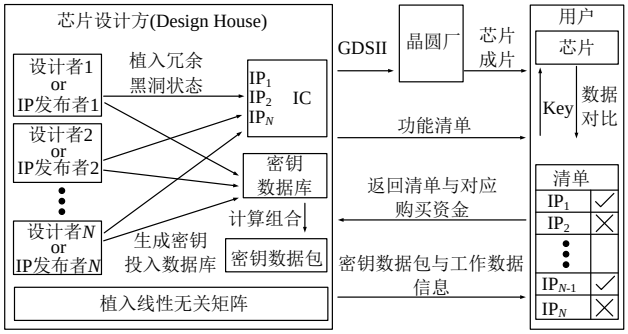

图4 按需解锁交互协议

4 实验结果与分析

在SMIC 65nm CMOS(Complementary Metal Oxide Semiconductor)工艺下,利用线性无关矩阵和冗余-黑洞状态混淆方法,对多硬件IP核进行加密并增加按需解锁功能,同时利用VCS、Design Compiler、TetraMAX等EDA(Electronic Design Automation)工具进行开销与安全性数据分析. 图5给出了64位密钥按需解锁4个IP核的仿真波形图. 为方便观测,在电路设计中引出IP_{1234}信号判定是否解锁成功. 在经过初始化、矩阵乘运算等步骤后,电路根据外部输入的密钥Key按需解锁对应的IP核,其中"1111"表示四个IP核全部解锁成功.

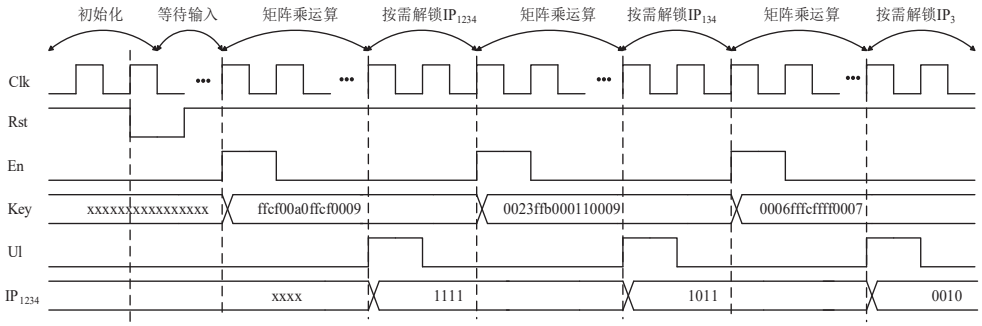

图5 按需解锁仿真波形

4.1 开销分析

使用ITC(International Test Conference)系列基准电路与密码算法IP核设计电路,并统计面积与功耗开销. 为模拟按需解锁功能的多IP核环境,将ITC系列基准电路进行组合. 例如CB0表示按需解锁ITC系列b01到b09的9个基准电路,CB1表示b01到b10的10个基准电路,以此类推,CB13即为按需解锁ITC系列b01到b22的22个基准电路. 图6为所设计电路的面积开销,以256位密钥为例,随着IP核数量由9个增加到22个,其总面积由19768.28 μm^2增大到191166.80 μm^2,但是其额外面积开销占比却从72.79%减小到7.53%. 同理32位、64位和128位密钥情况下,额外面积开销占比都随IP核数量增加而降低. 由于相同IP核数量下,更长

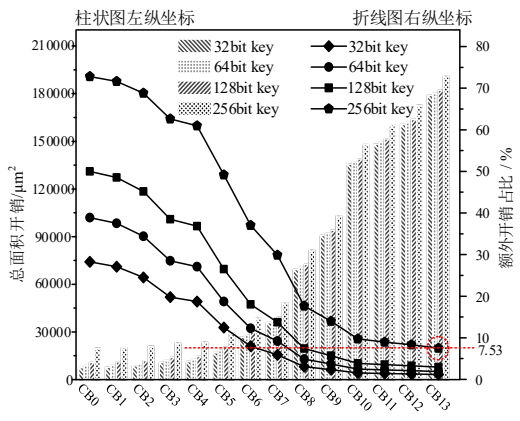

图6 面积开销

密钥需要更大线性无关矩阵,所以密钥由32位增加到256位,额外面积开销由1.59%增大到7.53%. 图7为所设计电路的功耗开销,同样以256位密钥为例,随着IP核数量由9个增加到22个,其总功耗由1.2738 mW增大到11.2463 mW,但是额外的功耗开销占比从68.61%减小到7.77%. 同理在相同位密钥情况下,额外功耗开销随密钥位数增加而增大. 表1给出了按需解锁加密算法IP核所测得开销,以Camellia、MISTY1_1clk、SEED_3clk、TDEA和SHA256加密算法(分别以E1~E5表示)的递增组合作为基准电路实现按需解锁. 表中EA(Encryption Algorithm)表示加密算法IP核,RBA(Redundant and Black- Hole States Area)表示添加冗余与黑洞状态所增加的面积,LIMA(Linear Independent Matrix Area)表示植入线性无关矩阵所增加面积,TA(Total Area)表示总面积,PA(Percent Area)表示额外面积占比,RBP(Redundant and Black-hole states Power)表示添加冗余与黑洞状态后所增加的功耗,LIMP(Linear Independent Matrix Power)表示植入线性无关矩阵所增加功耗,TP(Total Power)表示总功耗,PP(Percent Power)表示额外功耗占比. 额外面积与功耗开销主要由黑洞与冗余状态、线性无关矩阵存储模块和矩阵乘模块组成. 对于大规模加密算法,这三部分开销相对变化较小. 所以随着IP核数量和规模的增大,额外面积和功耗开销占比呈减小趋势. 总之,当芯片规模足够大时,实现按需解锁功能造成的额外开销占比可以忽略.

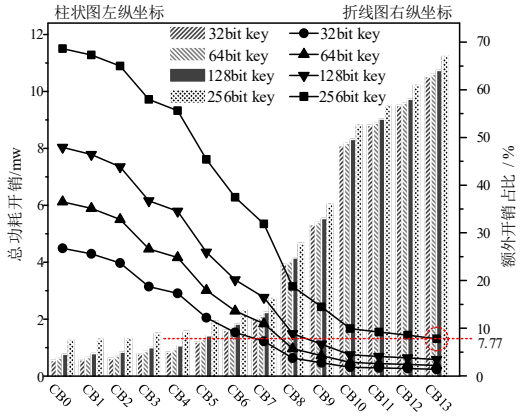

图7　功耗开销

表1　按需解锁加密算法IP核所测得开销

EA	RBA	LIMA	TA	PA	RBP	LIMP	TP	PP
E1+E2	140.96	2117.16	32122.28	7.02%	0.018	0.203	1.406	15.72%
E1+E2+E3	282.64	2355.04	45863.44	5.75%	0.021	0.233	2.0321	12.50%
E1+E2+E3+E4	312.56	2477.60	52990.84	5.27%	0.026	0.286	2.6521	11.76%
E1+E2+E3+E4+E5	340.35	2589.80	133890.23	2.19%	0.033	0.308	5.7541	5.93%

4.2　安全性分析

集成电路产业在全球化供应链中不断受到各种攻击威胁[13,14],本文将根据抗寄存器翻转攻击,抗代码覆盖率攻击和抗成员泄密攻击等指标阐述其安全性.

4.2.1　抗寄存器翻转攻击

攻击者可利用EDA工具观察电路内部线网或寄存器的翻转情况以辨别当前状态是否有效,因此可以使用寄存器状态翻转差异作为抗寄存器翻转攻击的评价指标. 若输入正确与错误密钥时,寄存器状态翻转差异较大,则攻击者可多次输入激励观察响应并总结寄存器状态翻转规律,最终破获芯片密钥. 基于线性无关矩阵的按需解锁硬件混淆设计在输入错误密钥时,状态机并未固定在某个冗余或黑洞状态. 当冗余跳转密钥错误时,状态机在多个冗余状态间跳转. 当正常工作模式时黑洞密钥错误,状态机在多个黑洞状态间跳转. 故输入正确与错误密钥时寄存器状态翻转情况接近. 实验中利用自动测试激励生成工具TetraMax产生激励信号,统计寄存器状态翻转情况,结果如图8所示,状态翻转差异为3%,表明所提方法能够有效抵御以观察寄存器状态翻转为基础的硬件密钥攻击.

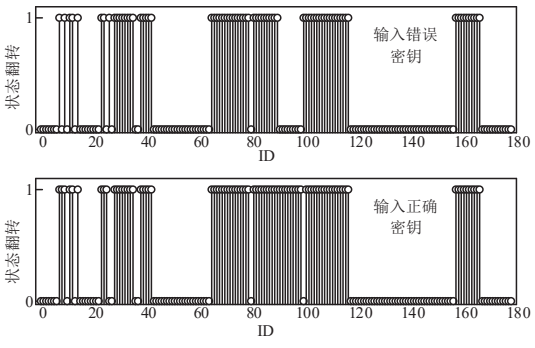

图8　正确/错误密钥下的状态翻转

4.2.2　抗代码覆盖率攻击

代码覆盖率为仿真过程中,RTL代码经过一定数量的激励输入所能达到的状态机覆盖率、状态跳转覆盖率、行覆盖率、条件分支覆盖率等的总和. 在RTL代码作为软核交易时,若状态机始终保持在某个状态,无法过渡到其他状态,则代码覆盖率低,攻击者可通过比较不同密钥输入下的代码覆盖率识别真正的功能模块电路. 图9给出了混淆前后代码覆盖率,其中DC1为ITC系列b01~b09基准电路组合成按需解锁电路,DC2为ITC系列b01~b10基准电路,以此类推,DC13为ITC系列b01~b22基准电路.

基于线性无关矩阵的按需解锁电路与原始电路代码覆盖率差异随着密钥长度增加而增大,但在256位密钥长度下,平均差异性仍然小于5%,所以所提方法能有效避免混淆状态跳转不均导致的信息泄漏.

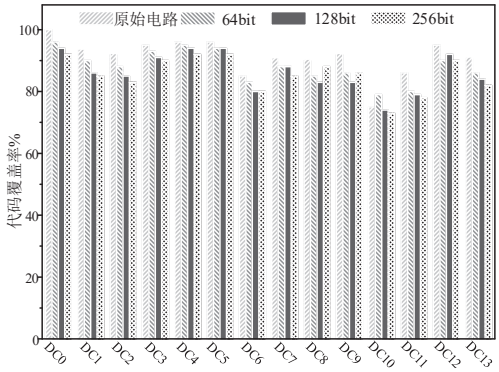

图9 代码覆盖率

4.2.3 抗成员泄密攻击

芯片规模的扩大使单人或单一团队完成芯片设计变得非常困难. 芯片设计方在制定方案时通常会将芯片切分成几个大模块交由不同团队设计,而团队内部又把大模块切分成小模块交由小团队设计. 分工协作使设计效率上升,但同时也会产生成员泄密的威胁. 因为常规加密方法是将密钥长度为M的设计划分为I个模块交由不同团队设计,每个团队平均分配M/I位密钥长度. 若I个团队中有x个成员泄露密钥,则剩余密钥被破解时间Y可由式(5)表示,其中T为尝试破解一次密钥的时间.

$$Y=2^{\frac{M}{I}(I-x)}\cdot T \tag{5}$$

以256位密钥加密为例,平均分配给16个设计团队,其破解时间与泄密团队成员数的关系如图10三角形线所示. 破解时间按式(6)进行归一化处理,在团队中出现成员泄密时,归一化的破解时间趋向于零,对成员泄密攻击没有抵抗力. 若根据式(4),利用线性无关矩阵将外部输入密钥与内部解锁信号隔离,则当有成员泄露自己团队设置的解锁信号时,攻击者很难由已泄露的解锁信号反推外部输入密钥,在应对暴力破解时几乎不会受到成员密钥泄露的影响,如图10矩形线所示. 因此利用线性无关矩阵的加密方法能够有效抵抗成员泄密攻击.

$$Y=\frac{\log_{10}(2^{\frac{M}{I}(I-x)}\cdot T)}{\log_{10}(2^{M}\cdot T)} \tag{6}$$

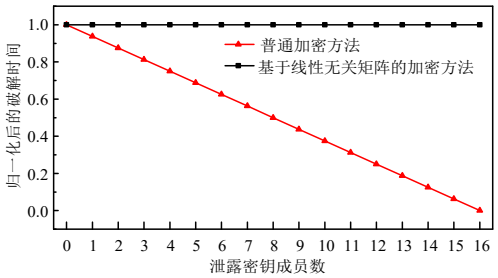

图10 成员泄密后被破解时间

4.3 与相关文献对比

表2为基于线性无关矩阵的按需解锁硬件混淆方法(Method of Unlock-on-Demand Hardware Obfuscation Based on Linear Independent Matrix, UDLIM)与其他硬件IP核保护技术在面积、功耗和安全性等方面的比较结果. UDLIM方法的额外面积开销占比和额外功耗开销占比仅为7.53%和7.77%,且增加了按需解锁(Unlock-on-Demand, UoD)多个硬件IP核功能,并能有效抵抗代码覆盖率攻击(Code Coverage Attack, CCA)、成员泄密攻击(Member Information Leakage Attack, MILA)、以及寄存器翻转攻击(Register Toggle Attack, RTA).

表2 与相关文献对比结果

文献	方法	保护IP数量	面积	功耗	UoD	CCA	MILA	RTA
文献[4]	DUP	1	13.6%	8.6%	-	-	–	-
文献[5]	HARPOON	1	19.4%	5.5%	-	√	-	-
文献[6]	ISO	1	13.3%	10.5%	-	-	-	√
文献[8]	PLO	1	0.56%	4.57%	-	-	-	√
文献[9]	DSD	1	15.2%	2.7%	-	√	-	-
文献[15]	HFO	1	8.2%	12.3%	-	-	-	√
文献[16]	HO	1	17.2%	5.17%	-	√	-	–
本文	UDLIM	N	7.53%	7.77%	√	√	√	√

5 结论

本文提出了一种利用线性无关矩阵、冗余和黑洞状态混淆的多IP核按需解锁方案,有效隔离了解锁信号和外部输入密钥的关联,克服了状态机初始化信息泄露以及正常工作模式下无保护的问题. 与多种混淆方法对比,所设计的电路不仅具有按需解锁的功能,且额外的面积和功耗开销均小于8%;在不同长度密钥输入情况下,寄存器翻转差异为3.65%,混淆前后RTL代

码的覆盖率平均差异小于5%,可同时防御寄存器翻转攻击,代码覆盖率攻击和成员泄密攻击. 为多IP核按需解锁的市场需求提供解决途径,具有广阔应用前景.

参考文献

[1] CHI M, XIAO D, CHANG R. Fast development of IC technologies in AI and IoT Era[C]// IEEE International Conference on Solid-State and Integrated Circuit Technology. Qingdao: IEEE, 2018: 1-4.

[2] 白创, 唐立军. 一种可靠的芯片指纹PUF电路[J]. 电子学报, 2019, 47(10): 2116-2125.
BAI Chuang, TANG Li-jun. A reliable physical unclonable function for chip fingerprint[J]. Acta Electronica Sinica, 2019, 47(10): 2116-2125. (in Chinese)

[3] SARKAR P, ROY D, SENGUPTA A, et al. Signature-free watermark for protecting digital signal processing cores used in CE devices[J]. IEEE Consumer Electronics Magazine, 2019, 8(1): 92-94.

[4] YOUSRA A, FARINAZ K, MIODRAG P. Remote activation of ICs for piracy prevention and digital right management[C]// IEEE/ACM International Conference on Computer-Aided Design. San Jose CA: IEEE, 2007: 674-677.

[5] CHAKRABORTY R S, BHUNIA S. HARPOON: An obfuscation-based SoC design methodology for hardware protection[J]. IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems, 2009, 28(10): 1493-1502.

[6] CHAKRABORTY R S, BHUNIA S. RTL hardware IP protection using key-based control and data flow obfuscation [C]// International Conference on VLSI Design. Bangalore: IEEE, 2010: 405-410.

[7] ZHANG J, LIN Y, LYU Y, et al. A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1137-1150.

[8] ZHANG J. A practical logic obfuscation technique for hardware security [J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2016, 24(3): 1193-1197.

[9] DOFE J, YU Q. Novel dynamic state-deflection method for gate-level design obfuscation[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37(2): 273-285.

[10] 张跃军, 王佳伟, 潘钊, 等. 基于正交混淆的多硬件IP核安全防护设计[J]. 电子与信息学报, 2019, 41(8): 1847-1854.
ZHANG Yue-jun, WANG Jia-wei, PAN Zhao, et al. Hardware security for multi IPs protection based on orthogonal obfuscation[J]. Journal of Electronics and Information Technology, 2019, 41(8): 1847-1854. (in Chinese)

[11] SUN P, CUI A. A new pay-per-use scheme for the protection of FPGA IP[C]// IEEE International Symposium on Circuits and Systems. Sapporo: IEEE, 2019: 1-5.

[12] GUHA K, SAHA D, CHAKRABARTI A. Blockchain technology enabled pay per use licensing approach for hardware IPs[C]// Design, Automation and Test in Europe Conference and Exhibition. Grenoble: DATE, 2020: 1618-1621.

[13] LI G, WANG P, QIAN H. Highly reliable multiport PUF circuit based on MOSFET zero temperature coefficient point[J]. Chinese Journal of Electronics, 2018, 27(4): 211-216.

[14] 杨轩, 叶文强, 崔小乐. 基于RRAM延时单元的PUF设计[J]. 电子学报, 2020, 48(8): 1565-1571.
YANG Xuan, YE Wen-qiang, CUI Xiao-le. PUF design based on RRAM delay unit[J]. Acta Electronica Sinica, 2020, 48(8): 1565-1571. (in Chinese)

[15] KOTESHWARA S, KIM C, PARHI K. Hierarchical functional obfuscation of integrated circuits using a mode-based approach[C]//IEEE International Symposium on Circuits and Systems. Baltimore: ISCAS, 2017: 1-4.

[16] KOTESHWARA S, KIM C, PARHI K. Key-based dynamic functional obfuscation of integrated circuits using sequentially triggered mode-based design[J]. IEEE Transactions on Information Forensics and Security, 2018, 13 (1): 79-93.

作者简介

汪鹏君　男,1966年生,浙江宁波人. 博士,教授,博士生导师,中国电子学会电路与系统委员会委员,中国人工智能学会理事,目前主要研究方向为集成电路设计、信息安全等技术及其相关理论.
E-mail: wangpengjun@wzu.edu.cn

叶顺心　男,1995年生,浙江衢州人. 宁波大学信息科学与工程学院硕士研究生,主要研究方向为硬件混淆安全设计.
E-mail: 502940763@qq.com