基于正交混淆的多硬件IP核安全防护设计

张跃军 王佳伟 潘 钊 张晓伟 汪鹏君*
(宁波大学信息科学与工程学院 宁波 315211)

摘 要：为了解决集成电路设计中多方合作的成员信息泄漏问题，该文提出一种基于正交混淆的多硬件IP核安全防护方案。该方案首先利用正交混淆矩阵产生正交密钥数据，结合硬件特征的物理不可克隆函数(PUF)电路，产生多硬件IP核的混淆密钥；然后，在正交混淆状态机的基础上，实现多硬件IP核的正交混淆安全防护算法；最后，利用ISCAS-85基准电路和密码算法，验证正交混淆方法的有效性。在台湾积体电路制造股份有限公司(TSMC) 65 nm工艺下测试正交混淆的多硬件IP核方案，正确密钥和错误密钥下的Toggle翻转率小于5%，在较大规模的测试电路中面积和功耗开销占比小于2%。实验结果表明，采用正交混淆的方式能够提高多硬件IP核的安全性，可以有效防御成员信息泄漏、状态翻转率分析等攻击。

关键词：正交混淆；合伙人组织；物理不可克隆函数；硬件IP安全性
中图分类号：TP331 **文献标识码**：A **文章编号**：1009-5896(2019)08-1847-08
DOI: 10.11999/JEIT180898

Hardware Security for Multi IPs Protection Based on Orthogonal Obfuscation

ZHANG Yuejun WANG Jiawei PAN Zhao ZHANG Xiaowei WANG Pengjun
(*Faculty of Electrical Engineering and Computer Science*, *Ningbo University*, *Ningbo* 315211, *China*)

Abstract: In order to solve the problem of member information leakage in multi-party cooperative design of integrated circuits, a orthogonal obfuscation scheme of multi-hardware IPs core security protection is proposed. Firstly, the orthogonal obfuscation matrix generates orthogonal key data, and the obfuscated key of the hardware IP core is designed with the physical feature of the Physical Unclonable Function (PUF) circuit. Then the security of multiple hardware IP cores is realized by the orthogonal obfuscation state machine. Finally, the validity of orthogonal aliasing is verified using the ISCAS-85 circuit and cryptographic algorithm. The multi-hardware IP core orthogonal obfuscation scheme is tested under Taiwan Semiconductor Manufacturing Company (TSMC) 65 nm process, the difference of Toggle flip rate between the correct key and the wrong key is less than 5%, and the area and power consumption of the larger test circuit are less than 2%. The experimental results show that orthogonal obfuscation can improve the security of multi-hardware IP cores, and can effectively defend against member information leakage and state flip rate analysis attacks.

Key words: Orthogonal obfuscation; PartnerShip Organization(PSO); Physical Unclonable Function(PUF); Hardware IPs security

收稿日期：2018-09-18；改回日期：2019-03-14；网络出版：2019-04-13
*通信作者： 汪鹏君 wangpengjun@nbu.edu.cn
基金项目：国家自然科学基金(61871244, 61874078, 61704094)，浙江省自然科学基金(LY18F040002)，浙江省科技厅公益技术应用研究(2016C31078)，亿像素视频加密与IP加密算法与硬件开发横向项目(HK2017000135)，浙江省大学生新苗人才计划(2018R405071)，宁波大学王宽诚幸福基金
Foundation Items: The National Natural Science Foundation of China (61871244, 61874078, 61704094),The Natural Science Foundation of Zhejiang Provincial (LY18F040002), The S&T Plan of Zhejiang Provincial Science and Technology Department (2016C31078), Algorithms and Hardware Development of Billion Pixels Video Encryption and IP Encryption (HK2017000135), Fresh Student Talents Program of Zhejiang Province (2018R405071), The K.C. Wong Magna Fund in Ningbo University

1 引言

随着芯片集成度上升，电路规模不断扩大，单个公司或设计团队完成复杂片上系统(System on Chip, SoC)的所有功能变得越来越困难[1]。例如人工智能芯片[2]产品由多个模块组成，包括：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、精简指令集计算器(Reduced Instruction Set Computer, RISC)处理器[3]、神经元进程处理器(Tensor Processing Unit, TPU)等。为避免芯片研发时间过长，寻求多方合作、共同完成芯片设计、权益共享已经成为集成电路发展的必然趋势[4]。目前，谷歌、三星和高通等约80家公司联合开发新型RISC-V芯片应用于人工智能芯片和汽车无人驾驶领域，引起广泛关注[5]。同时，地平线机器人和英特尔也合作推出基于高斯架构的先进驾驶辅助系统(Advanced Driver Assistance System, ADAS)系统[6]。上述的合作案例，均实现产品竞争力的极大提升，但合作的过程必须解决利益共享等问题。合作方要防止自身IP信息泄露、专利技术被其他团队窃取等，同时希望能够在合作中保持自有知识产权、防止恶意竞争以及恶意收购。

复杂SoC芯片的开发主要包括设计、制造、封装和测试等环节，在全球化的供应链中存在诸多安全威胁[7]。为了解决上述安全问题，越来越多的研究人员提出采用硬件混淆的方式来提高硬件IP核的安全性。文献[8]利用冗余和黑洞状态相结合的映射方式，实现有限状态机的混淆；文献[9]提出一种硬件集成电路(Integrated Circuit, IC)计量方法，通过物理不可克隆函数(Physical Unclonable Function, PUF)产生的唯一标识符来锁定IC设计；文献[10]基于密钥控制流方法，提出寄存器传输级(Register Transfer Level, RTL)的硬件IP混淆；文献[11]在预先综合的网表上进行修改并重新综合，实现功能和结构上的混淆；文献[12]提出一种动态的状态映射混淆方法，将原始数据通路映射到黑洞群。上述方法在一定程度上保护了硬件IP的安全，但这些方法仅针对单个IP核的安全问题展开研究，且局限于抵御逆向工程、侧信道攻击等外部攻击形式。因此，在多方合作的多硬件IP核中，内部成员信息泄漏等问题依然比较严峻。

随着供应链的全球化发展趋势，越来越多的IC公司希望或已经建立合伙人组织来完成项目研究。IC设计过程中通常有两种组织模式，即领导-成员组织(Leader Ship-member Organization, LSO)模式和合伙人组织(Partner Ship Organization, PSO)模式[13]。LSO模式由领导和成员两部分组成，在LSO中权力分配决定领导者与成员之间的关系。成员负责研究开发不同IP核的功能，而领导者需要将多个IP核整合为完整的功能芯片并完成销售。权力分配的不同决定了领导者与成员之间的内部利益分成，难以避免领导者的主观意愿，容易引发团队内部矛盾。同时，整体SoC芯片的密钥信息由领导者掌控，一旦领导者的信息遭到泄漏，将直接损害所有成员的利益。PSO模式是由两个及以上的合伙人共享利润的设计模式。设计者处于同等地位，分别设计IP核，并在各IP核中预留特征信息。PSO模式的优势主要体现在以下几个方面：(1)合伙人共同参与芯片设计，分享经营成果；(2)未经全体合伙人同意，所有设计者无法私自代表合伙团队出售设计成果。合伙人之间发生分歧时，可依内部进行协商，有利于调动成员的积极性和团队的和谐发展。鉴此，本文提出一种基于正交混淆的PSO实现方案，达到复杂SoC系统防御成员信息泄漏攻击的目的。

2 正交混淆方法

SoC用户设定密钥数据，每个合伙人设计的硬件IP核内含密钥数据。因此，正交混淆需要解决正交密钥产生和硬件IP核识别等问题。本文将采用正交混淆矩阵的方式产生正交密钥，PUF作为合伙人的硬件IP核标识[14]。正交混淆控制的子模块数量根据实际合伙人数量灵活变动，正交混淆矩阵在判定用户的密钥和IP核特征数据后，生成状态机的控制信号。正交混淆方法的结构框图如图1所示。

2.1 正交混淆的交互协议

交互协议定义了IC设计团队、芯片公司以及用户之间的密钥传递关系。首先芯片公司根据用户的需求，向IC设计团队提出具体的设计指标；然后由IC设计团队分工完成不同硬件IP核设计，芯片公司对所设计的芯片进行制造、封装和测试；最后，由芯片公司将产品售卖给用户。正交混淆的交互协议是一种高保密性的合伙人交互机制，如图2所示。与传统的LSO协议相比[15]，设计者处于同等地位，整体项目分成N组来完成不同IP核设计，同时需要在IP核中预留密钥信息$\boldsymbol{K}_{\mathrm{IP}}$，$\boldsymbol{K}_{\mathrm{IP}}$为32位二进制数。根据IP核在项目中的重要性来分配权重，权重越大优先级越高。结合N组密钥信息和权重数据，可构

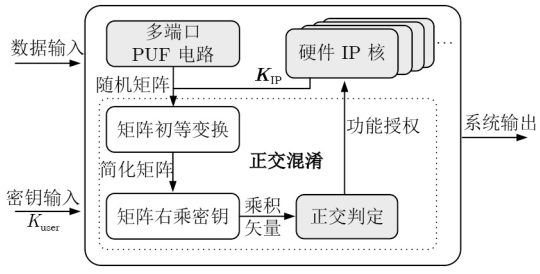


图 1 正交混淆方法结构框图

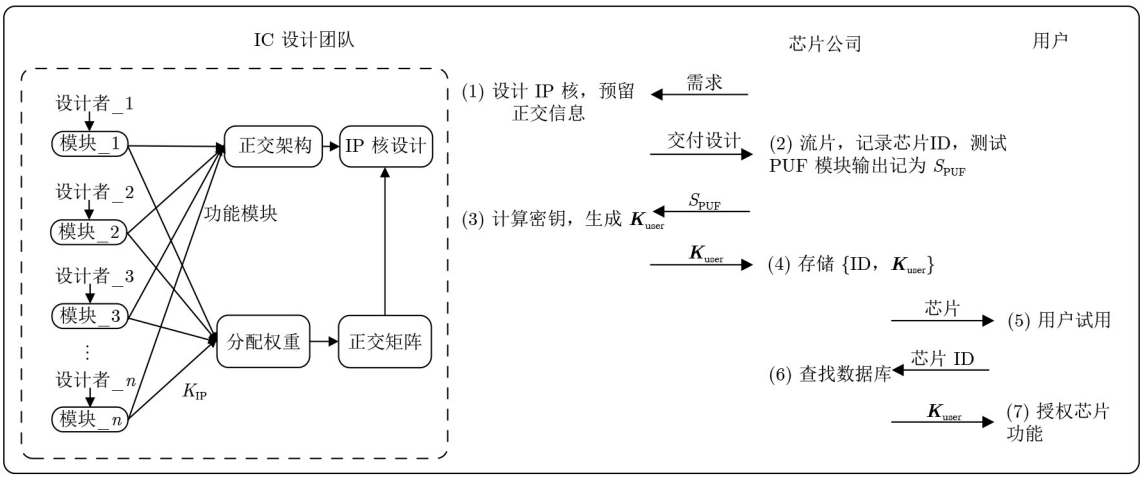


图 2 IC设计团队、芯片公司以及用户的正交混淆交互协议

建正交混淆矩阵。正交混淆矩阵经过初等变换后可获得用户许可密钥$\boldsymbol{K}_{\text{user}}$。设计团队将多个硬件IP核交付给芯片公司，但设计者持有自己IP核的密钥信息$\boldsymbol{K}_{\text{IP}}$，且对设计团队的不同成员之间保密。芯片公司将所设计的产品进行制造、封装和测试，并为每块芯片创建身份标识码(IDentification, ID)以及记录每块芯片的特征数据S_{PUF}。芯片公司将S_{PUF}发送回IC设计团队，S_{PUF}用于配合正交矩阵确定芯片的许可密钥$\boldsymbol{K}_{\text{user}}$。芯片公司获得密钥$\boldsymbol{K}_{\text{user}}$后将其与芯片ID存储到数据库。若客户要购买芯片，则需将芯片ID发送至芯片公司，芯片公司通过ID查找数据库中对应密钥完成芯片交易。正交混淆协议为芯片设计、制造和销售过程提供高安全性的密钥隔离技术。设计者持有密钥信息$\boldsymbol{K}_{\text{IP}}$，芯片公司持有芯片的特征数据$S_{\text{PUF}}$，用户购买到许可密钥$\boldsymbol{K}_{\text{user}}$，达到保护芯片供应链中不同成员的各自权益。

2.2 正交混淆的数学模型

数学上，定义了内积为0的两个向量为正交向量。为了实现正交混淆功能，本文采用数学矩阵和代数解空间相结合的方式来构建混淆信号处理的数学模型。在每个IP核中，通过复用模块内部的寄存器组预留特征向量$\boldsymbol{K}_{\text{IP}}$，所有特征向量在顶层构成正交混淆矩阵，每个向量作为矩阵的一行。n维矩阵表示n个IP核。同时，密钥$\boldsymbol{K}_{\text{user}}$以向量形式作为外部输入，通过矩阵各向量和密钥的内积来判定密钥的正确性。

由n个$\boldsymbol{K}_{\text{IP}}$组成的$n$维正交混淆矩阵$\boldsymbol{O}$，可以表示为$[\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n]^{\text{T}}$。由于每个$\boldsymbol{K}_{\text{IP}}$都与IP核设计者设定的密钥信息一一对应，需要$n$个$\boldsymbol{K}_{\text{IP}}$满足线性无关。如果$n$个$\boldsymbol{K}_{\text{IP}}$线性相关，则存在部分$\boldsymbol{K}_{\text{IP}}$可以被其它$\boldsymbol{K}_{\text{IP}}$线性表示，意味着采用剩余$\boldsymbol{K}_{\text{IP}}$亦能构成等价矩阵，被线性表示的部分$\boldsymbol{K}_{\text{IP}}$失去加密意义。所以$n$个$\boldsymbol{K}_{\text{IP}}$需为线性无关组，正交混淆矩阵$\boldsymbol{O}$为$n$行满秩矩阵[16]。多方设计者在设定$\boldsymbol{K}_{\text{IP}}$之前需先通过线性无关检测程序的验证，进而确保所有$\boldsymbol{K}_{\text{IP}}$之间线性无关，该线性无关检测程序采用C语言或其它编程语言较容易实现。此外，还需保证在检测过程中各自输入特征向量$\boldsymbol{K}_{\text{IP}}$不能被其他设计者获知。在此基础上，定义$n+m$列的混淆矩阵，其中$n$列为IP核特征矢量，$m$列为每块芯片的特征数据$S_{\text{PUF}}$，如式(1)所示

$$\begin{aligned}\boldsymbol{O}&=[\,\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n\,]^{\text{T}}\\&=\begin{bmatrix}\alpha_{11}&\alpha_{12}&\cdots&\alpha_{1n}&\alpha_{1(n+1)}&\cdots&\alpha_{1(n+m)}\\\alpha_{21}&\alpha_{22}&\cdots&\alpha_{2n}&\alpha_{2(n+1)}&\cdots&\alpha_{2(n+m)}\\\vdots&\vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\\alpha_{n1}&\alpha_{n2}&\cdots&\alpha_{nn}&\alpha_{n(n+1)}&\cdots&\alpha_{n(n+m)}\end{bmatrix}\end{aligned}\tag{1}$$

为判定输入密钥是否正交，假定外部输入为$n+m$位的密钥序列，采用矩阵右乘的方式与式(1)进行运算，可得n位正交判定信号$[p_1, p_2,\cdots,p_n]$，如式(2)所示。若p_i为0，则说明输入密钥正交于第i行向量，授权解锁对应的第i个IP核；若正交判定信号$[p_1, p_2,\cdots,p_n]$均为0，则说明输入密钥正确。

$$\begin{aligned}\begin{bmatrix}p_1\\p_2\\\vdots\\p_n\end{bmatrix}&=\begin{bmatrix}\varepsilon_1\\\varepsilon_2\\\vdots\\\varepsilon_n\end{bmatrix}\times\boldsymbol{K}_{\text{user}}\\&=\begin{bmatrix}\alpha_{11}&\alpha_{12}&\cdots&\alpha_{1n}&\alpha_{1(n+1)}&\cdots&\alpha_{1(n+m)}\\\alpha_{21}&\alpha_{22}&\cdots&\alpha_{2n}&\alpha_{2(n+1)}&\cdots&\alpha_{2(n+m)}\\\vdots&\vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\\alpha_{n1}&\alpha_{n2}&\cdots&\alpha_{nn}&\alpha_{n(n+1)}&\cdots&\alpha_{n(n+m)}\end{bmatrix}\\&\cdot\begin{bmatrix}k_1\\k_2\\\vdots\\k_{1(n+m)}\end{bmatrix}\end{aligned}\tag{2}$$

2.3 正交混淆的算法设计

为了确保正交混淆与原有IP核的兼容性，采用

正交算法顶层覆盖的方式，实现与多硬件IP核的融合设计，正交混淆算法的伪代码如表1所示。正交顶层覆盖原设计的IP核，IP核作为子模块可以嵌套与扩展。正交混淆算法模块初重置顶层信号，读取子模块的特征向量$\boldsymbol{K}_{\mathrm{IP}}$和外部输入密钥序列$\boldsymbol{K}_{\mathrm{user}}$，根据权重不同分配给每个IP核，最后通过有限状态机自动构造混淆矩阵$\boldsymbol{O}$。将混淆矩阵与输入密钥进行右乘运算，得到可用于控制多硬件IP核的正交判定信号$[p_1, p_2,\cdots,p_n]$。设计底层由可嵌套的IP核组成，不同IP核作为子模块保留了设计者预设的唯一正交矢量$\boldsymbol{K}_{\mathrm{IP}}$，接收来自顶层的使能信号$p_i$，当$p_i$为0时IP核正常工作。

表 1 正交混淆算法伪代码

正交混淆算法

输入： $\boldsymbol{K}_{\mathrm{user}}$

输出： $\{p_1,p_2,\cdots,p_n\}$

(1) 初始化正交模块

(2) 重置功能IP核

(3) 对各功能IP核分配权重

(4) **for** i←0 to N-1

　　for j←i+1 to N-1 {

　　do vector_j←vector_j-(vector_j[i]/vector_i[i])×vector_i

　　}

(5) **for** i←0 to N-1

　　for j←i+1 to N-1 {

　　do vector_i←vector_i-(vector_i[N-i]/vector_j[N-i])×vector_j

　　}

(6) 矩阵$\boldsymbol{O}$←{vector_1,vector_2,⋯,vector_N}$^{\mathrm{T}}$

(7) 向量$\boldsymbol{p}$←$\boldsymbol{O}$×$\boldsymbol{K}_{\mathrm{user}}$

2.4 正交混淆的电路实现

正交混淆的电路实现包括组合逻辑的混淆、状态机混淆和产生正交判定信号3部分，如图3所示。在组合逻辑中，通过修改逻辑电路的信号传输单元实现正交混淆功能。在状态混淆设计中，在原有状态机S_6～S_{10}的基础上增加了冗余状态机S_1～S_5，实现状态混淆的功能。此外，正交加密模块利用IP核的特征向量$\boldsymbol{K}_{\mathrm{IP}}$和芯片特征数据$S_{\mathrm{PUF}}$重构正交矩阵，将输入密钥$\boldsymbol{K}_{\mathrm{user}}$用于乘法运算。正交判定信号被用作混淆状态机的跳转条件，用于授权部分或全部IP核。

密钥和公钥分别是用于解锁具体某块芯片的许可序列和解锁所有芯片的通用序列。为了达到每块芯片有且只有一个密钥的目的，PUF电路被用于在芯片公钥中确定每块芯片的唯一序列，实现密钥唯一性[17]。由PUF电路产生随机的n–1维子空间，与之正交的密钥唯一，且子空间的数据互相独立、无法逆推。以此设计正交混淆，采用合伙人协同管理IP硬核的方式，可以极大地提高安全性。假定每个合伙人为子空间ε_i，也就是说每个合伙人仅能控制自己所设计的IP核，杜绝合伙人之间损害彼此利益的可能性。同时，正交算法允许IP硬核使用者购买IP硬核的部分功能，更加方便灵活。合伙人协同管理IP硬核的核心是构建正交混淆有限状态机，与领导者管理密钥方式的最大区别是正交混淆实现合伙人共同管理密钥。原有的混淆方法采用输入密钥$\boldsymbol{K}_{\mathrm{user}}$和预留序列KS是否相等的方式验证，识别和判定的方式简单，存在安全隐患。正交混淆方法用于集群成员硬件安全的复杂代数函数，采用正交的方式隐藏状态和PUF电路，并识别多个成员。当输

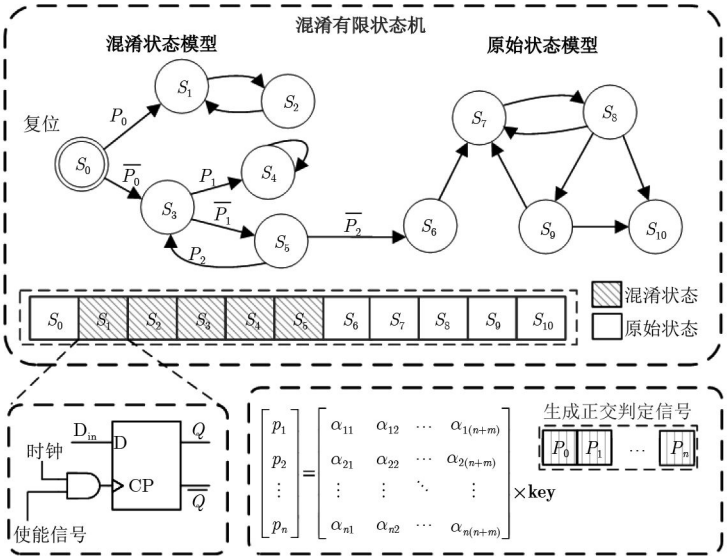


图 3 正交混淆的电路实现

入错误密钥时，混淆状态机将跳转到某些死循环$\{S_1, S_2\}$或黑洞状态S_4，只有当输入正确密钥时，混淆状态机才能正常运行。

3　实验结果与分析

在65 nm互补金属氧化物半导体(Complementary Metal Oxide Semiconductor, CMOS)工艺下，设计多硬件IP核的正交混淆算法并评估在不同IP核中的硬件开销，主要包括以下两部分：正交混淆算法的硬件设计与验证，基于ISCAS-85基准电路和密码算法的正交混淆设计与评估。实验过程涉及的工具软件为：电路综合采用Synopsys公司的Design Compiler, Verilog仿真和Toggle分析采用Cadence的NClaunch等工具软件。

3.1　混淆功能仿真结果

在ISCAS-85基准电路和密码算法等测试电路的基础上，本文验证了正交混淆功能的有效性。正交混淆的硬件仿真结果如图4所示。正交模块接收时钟、复位信号和密钥输入，内部寄存器复位发生在正常操作之前，在1个时钟周期内完成。密钥输入后通过计算产生正交判定信号，正交判定信号作为跳转条件，引导正交混淆有限状态机跳转，由状态机控制解锁不同IP核。

3.2　混淆开销分析

除了验证正交模块的功能外，实验对基于正交混淆的基准电路面积、功耗和延迟开销进行测试。开销测试实验根据基准电路规模大小将ISCAS-85模块和密码算法分成3组测试。混淆测试模块A采用ISCAS-85模块中的c1355, c1908, c2670, c3540电路；混淆测试模块B采用ISCAS-85模块中的c5315, c5315a, c6288, c7552电路；混淆测试模块C采用密码算法TDEA, SEED_3clk, MISTY1_3clk和AES中的EncCore部分。在不改变外在约束条件的前提下，3组混淆测试模块在台湾积体电路制造股份有限公司(Taiwan Semiconductor Manufacturing Company, TSMC) 65 nm和中芯国际集成电路制造有限公司(Semiconductor Manufacturing International Corporation, SMIC) 65 nm两种工艺下完成逻辑综合。通过和原始基准电路硬件开销对比，得到图5和图6的混淆设计开销测试结果。

从各模块和多电路混淆的开销比较可知，在相同工艺下，不同基准电路中正交混淆增加的额外面积开销基本保持稳定。将多个基准电路组合为多硬件IP核的正交结构增加了几乎恒定的面积和功耗开销。多硬件IP核混淆模块的额外开销不依赖于基准电路的大小，而是取决于正交混淆方法本身。表2为多硬件IP核的基本开销情况，作为子模块的基准电路增加时，正交混淆带来的具体额外开销存在微小增长，整体来看正交结构的基准电路开销越大，正交混淆的额外开销比例越小。

3.3　安全性分析

在LSO模式的加密设计中，领导负责设定整个密钥序列。如果在这种设计中出现成员信息泄漏问题，密码将完全泄露，攻击者可以在没有任何进一

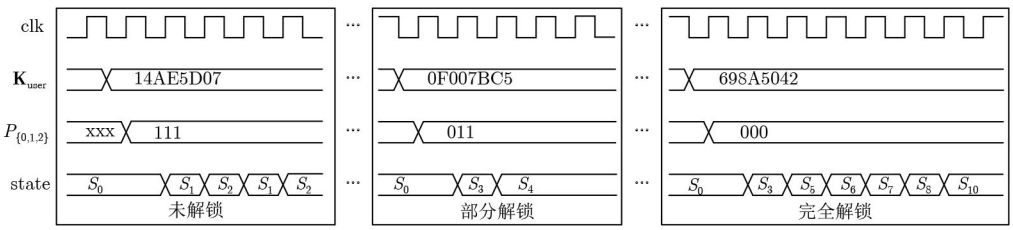


图 4 正交混淆功能仿真图

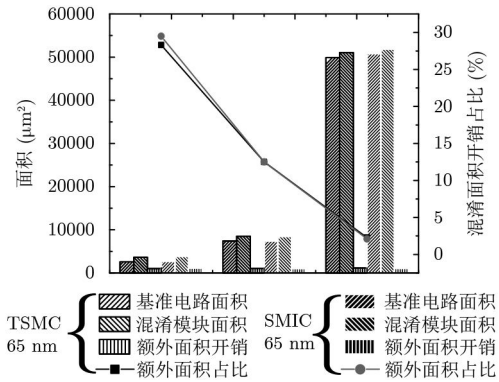


图 5 正交混淆的面积开销

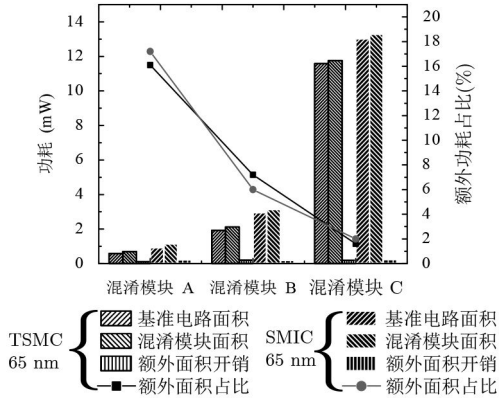


图 6 正交混淆的功耗开销

表 2 基准电路中硬件开销情况

	基准电路面积(μm^2)	测试模块面积(μm^2)	混淆面积开销(μm^2)	面积开销占比(%)	基准电路功耗(mW)	测试模块功耗(mW)	混淆功耗开销(mW)	功耗开销占比(%)	混淆模块延时(ns)
A1	6457.68	7391.68	934.00	12.60	0.3129	0.4392	0.1263	28.80	1.12
A1+A2	16851.96	17866.12	1014.16	5.70	3.3928	3.5517	0.1589	4.50	1.12
A1+A2+A3	32561.64	33618.80	1057.16	3.10	7.5221	7.7017	0.1796	2.30	1.15
A1+A2+A3+A4	49888.08	51038.76	1150.68	2.30	11.5796	11.7626	0.1830	1.60	1.20

注：表中A1, A2, A3和A4分别表示密码算法TDEA, SEED_3clk, MISTY1_3clk和AES中的EncCore部分。

步攻击的情况下用密码窃取芯片技术。使用Y_1表示有领导组织中成员信息泄漏下的攻击时间，则可以表示为

$$Y_1 = \begin{cases} 2^N \cdot T & , x = 0 \\ 0 & , x \neq 0 \end{cases} \tag{3}$$

其中，N是密钥位数[18]，T是攻击者的单次攻击周期，x是泄露密钥的成员的数量。在一般PSO模式的加密设计中，为了保证每一个设计者对他们设计的模块的控制，每个设计者都会掌握一部分密钥。在每个设计模块的贡献值不确定的前提下，假设每个模块的重要性是相同的，即设计者所掌握的密钥位数是相同的。以N位密钥为例，每个设计者将分别由n个设计者掌握N/n位密钥。如果在这种设计中发生成员信息泄漏问题，密钥的泄露位数与泄露密钥的成员数量相关。使用Y_2表示一般无领导组织中成员信息泄漏下的攻击时间，则可表示为

$$Y_2 = 2^{\frac{N}{n}\cdot(n-x)} \cdot T,\ x \le n \tag{4}$$

在基于正交混淆方法的PSO模式加密设计方案中，每个设计者都对其设计的IP核进行控制。由设计者掌握的特征向量构造的正交矩阵将直接确定密钥的正确性，因此由一组线性无关的特征向量间接确定密钥。使用Y_3表示基于正交混淆合伙人机制中成员信息泄漏下的攻击时间，可以表示为

$$\begin{aligned} &Y_3 = 2^{k\cdot\frac{N}{n}\cdot(n-x)} \cdot 2^{(1-k)\cdot N} \cdot (P \cdot T), \\ &P = 2^{\log_2 x} \end{aligned} \tag{5}$$

其中，k是衰减因子，引入k是为了实现归一化，满足3条曲线初始值为1，方便比较不同加密设计在成员信息泄露下的安全性衰减速度。乘积项$2^{(1-k)\times N}$为正交混淆设计中芯片电路矩阵运算所需的时间，有领导组织和一般无领导组织设计为密钥直接匹配，硬件计算时间为一机器周期，故在式(3)和式(4)中省去。P为当前矩阵解空间的计算复杂度，乘积项$(P\times T)$是获知当前成员泄露信息条件下获得正交矩阵解集的平均运算时间开销。与有领导组织和一般的无领导组织加密方法相比，基于正交混淆方法的合伙人机制更有效地防止了成员信息泄漏引起的芯片安全问题。3种加密方法的成员信息泄漏情况下的设计稳定性衰减情况如图7所示。其中γ为混淆设计在当前泄漏信息成员数量下芯片攻击者遍历密钥破解芯片所需的归一化时间单位，泄漏信息的成员越多，攻击者所需的时间越短，归一化时间γ可表示为

$$\gamma = 2^N \cdot T \tag{6}$$

在电路分析中，攻击者可以利用状态是否翻转来区分有效状态和混淆状态，状态翻转率Toggle可以用来作为混淆指标[14]。例如输入正确密钥时寄存器组翻转，输入错误密钥时寄存器组不翻转，则攻击者可以经过多次激励观察响应总结寄存器翻转规律，破获芯片密码。正交混淆方法当输入错误密钥时并非简单的将状态机锁死在某一个状态，而是根据密钥与正交混淆矩阵的计算情况进行不同的状态跳转，故输入正确或错误密钥时状态寄存器组翻转情况较接近。在正交混淆后c1355网表级电路中，借助TetraMax软件产生激励信号，然后利用NClaunch仿真随机记录内部200位寄存器的数据，根据记录的中间数据产生如图8所示的不同激励下c1355模块Toggle统计结果，在输入正确和错误密钥时，基于正交混淆的多硬件IP核寄存器翻转差异小于5%，可以防御寄存器翻转率分析攻击。

基于正交混淆的多硬件IP核设计与文献对比结果如表3所示。与基于SEED_3clk电路的ISO混淆方法相比，正交混淆面积开销减小1.9%；与基于

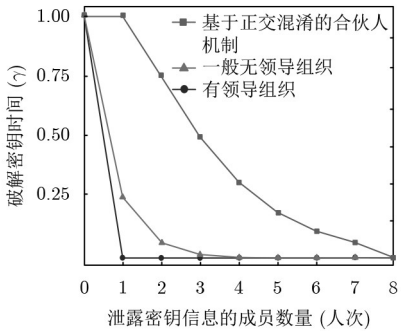
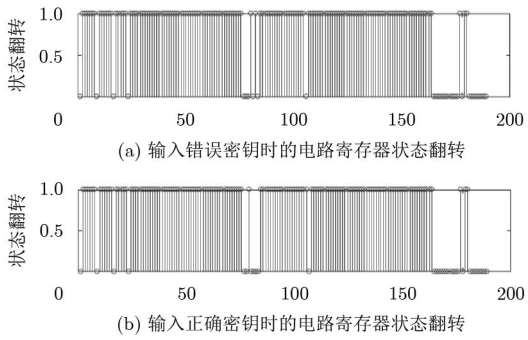


图 7 不同加密方法在成员泄密时的安全性曲线



(a) 输入错误密钥时的电路寄存器状态翻转

(b) 输入正确密钥时的电路寄存器状态翻转

图 8 Toggle仿真结果

ISCAS-85基准电路S38584模块的Dynamic State-Deflection相比，功耗开销降低2.6%。与此同时，与传统混淆方法相比，基于正交混淆的多硬件IP核支持多IP核混淆，且能够防御成员信息泄漏攻击(Member Information Leakage Attack, MILA)。

4　结论

本文提出一种基于正交混淆的多硬件IP核安全防护方法。该方法用于集群成员硬件安全的复杂代数函数，采用正交的方式隐藏状态和PUF电路，并识别多个成员。正交混淆过程覆盖IC设计、芯片测试与验证和后期销售阶段，在确保芯片原有功能正确性的前提下为各阶段提供严密的信息保护，保障PSO模式下的硬件安全。在65 nm CMOS工艺下，ISCAS-85基准电路和密码算法验证正交混淆的有效性。实验结果表明本文方案可以有效防御成员信息泄漏攻击，正确密钥和错误密钥下的Toggle翻转率接近，且在较大规模的测试电路中面积和功耗开销占比可小于2%。此外正交混淆设计为每个IP核向客户单独提供激活密钥，可以进一步增强芯片设计流程的安全性，保障复杂SoC的团队合作。

表 3　本文设计与文献[8–12]对比情况

文献	混淆方法	工艺(mm)	基准电路	面积(μm²)	功耗(mW)	速度(GHz)	混淆IP核数量	MILA
文献[8]	状态映射混淆	65	AES-ENC	25983.00	0.7558	–	单个	是
文献[9]	DUP	65	SEED_3clk	17506.08	3.2171	1.38	单个	是
文献[10]	ISO	65	SEED_3clk	17450.64	3.2830	1.72	单个	是
文献[11]	HARPOON	65	S38584	22995.40	6.3883	1.14	单个	是
文献[12]	Dynamic State-Deflection	65	S38584	21835.00	6.9262	0.86	单个	是
本文	正交混淆	65	SEED_3clk	17114.60	3.2815	0.98	多个	否
			AES-ENC	17326.44	4.0575	0.95		否
			s38584	20159.00	6.7456	0.83		否

参 考 文 献

[1] FYRBIAK M, ROKICKI S, BISSANTZ N, *et al*. Hybrid obfuscation to protect against disclosure attacks on embedded microprocessors[J]. *IEEE Transactions on Computers*, 2018, 67(3): 307–321. doi: 10.1109/TC.2017.2649520.

[2] JAEHA K and PARK K T. EE6: Can artificial intelligence replace my job? The dawn of a new IC industry with AI[C]. 2018 IEEE International Solid-State Circuits Conference, San Francisco, USA, 2018: 531–533.

[3] WERNER M, UNTERLUGGAUER T, SCHAFFENRATH D, *et al*. Sponge-based control-flow protection for IoT devices[C]. 2018 IEEE European Symposium on Security and Privacy, London, UK, 2018: 214–226.

[4] 许天燊. 万物互联驱动IC产业创新与合作[J]. 软件和集成电路, 2015(6): 16–20.
XU Tianshen. All things interconnection drives innovation and cooperation in IC industry[J]. *Software and Integrated Circuits*, 2015(6): 16–20.

[5] HONG C, KIM S H, KIM J H, *et al*. A linear-mode LiDAR sensor using a multi-channel CMOS transimpedance amplifier array[J]. *IEEE Sensors Journal*, 2018, 18(17): 7032–7040. doi: 10.1109/JSEN.2018.2852794.

[6] BUSE D S, SOMMER C, and DRESSLER F. Demo abstract: Integrating a driving simulator with city-scale VANET simulation for the development of next generation ADAS systems[C]. The IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops, Honolulu, USA, 2018: 1–2.

[7] VIJAYAKUMAR A, PATIL V C, HOLCOMB D E, *et al*. Physical design obfuscation of hardware: A comprehensive Investigation of device and logic-level techniques[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(1): 64–77. doi: 10.1109/TIFS.2016.2601067.

[8] 张跃军, 潘钊, 汪鹏君, 等. 基于状态映射的AES算法硬件混淆设计[J]. 电子与信息学报, 2018, 40(3): 750–757. doi: 10.11999/JEIT170556.
ZHANG Yuejun, PAN Zhao, WANG Pengjun, *et al*. Design of hardware obfuscation AES based on state deflection strategy[J]. *Journal of Electronics & Information Technology*, 2018, 40(3): 750–757. doi: 10.11999/

JEIT170556.

[9] KOUSHANFAR F. Provably secure active IC metering techniques for piracy avoidance and digital rights management[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(1): 51–63. doi: 10.1109/TIFS.2011.2163307.

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

[11] CHAKRABORTY R S and 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. doi: 10.1109/TCAD.2009.2028166.

[12] DOFE J and YU Qiaoyan. 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. doi: 10.1109/TCAD.2017.2697960.

[13] CANETTI R, ROTHBLUM G N, and VARIA M. Theory of Cryptography[M]. Berlin, Heidelberg: Springer, 2010: 72–89.

[14] CAO Yuan, ZHANG Le, CHANG C H, *et al*. A low-power hybrid RO PUF with improved thermal stability for lightweight applications[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2015, 34(7): 1143–1147. doi: 10.1109/TCAD.2015.2424955.

[15] ZHANG Jiliang, LIN Yaping, LYU Yongqiang, *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. doi: 10.1109/TIFS.2015.2400413.

[16] 张元达. 有限群构造[M]. 北京: 科学出版社, 1982: 203–206.
ZHANG Yuanda. Finite Group Construction[M]. Beijing: Science Press, 1982: 203–206.

[17] LAO Yingjie and PARHI K K. Statistical analysis of MUX-based physical unclonable functions[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2014, 33(5): 649–662. doi: 10.1109/TCAD.2013.2296525.

[18] BOŠNJAK L, SREŠ J, and BRUMEN B. Brute-force and dictionary attack on hashed real-world passwords[C]. The 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 2018: 1161–1166.

张跃军：男，1982年生，副教授，研究方向为信息安全芯片理论和设计.

王佳伟：男，1994年生，硕士生，研究方向为硬件安全和混淆设计.

潘 钊：男，1993年生，硕士生，研究方向为混淆状态机的设计与实现.

张晓伟：男，1987年生，讲师，研究方向为稀土掺杂硅基薄膜发光材料与光电子器件研究.

汪鹏君：男，1966年生，教授，研究方向为低功耗、高信息密度集成电路理论和设计、安全芯片理论和设计、多媒体技术及相关理论.