基于局部逻辑伪装的IC保护方法

杨 然[①] 高文超*[②]

[①](中国矿业大学数学学院 徐州 221116)

[②](中国矿业大学(北京)机电与信息工程学院 北京 100083)

摘 要：集成电路(IC)设计面临逆向工程的攻击，核心专利(IP)和算法被盗用，硬件安全受到威胁。该文提出一种电路伪装方法LPerturb，通过对其局部电路逻辑的扰动，实现IC电路的保护。对电路进行最大独立锥划分(MFFCs)，选取被伪装的最大子电路，确保输出逻辑扰动的局部性。针对要扰动锥结点逻辑，从锥中选择被替换的逻辑单元，以最小化代价对进行局部电路逻辑扰动。用多值伪装电路对扰动的逻辑值进行混淆保护，恢复相应的电路逻辑。实验结果表明，该方法能够稳定生成保护电路，具有较好的输出扰动性，能有效抵御SAT去伪装攻击，面积额外开销较小，时延影响可以忽略。

关键词：硬件安全；IC电路保护；IC伪装；逻辑混淆；最小项扰动

中图分类号：TP331 **文献标识码**：A **文章编号**：1009-5896(2021)09-2466-08

DOI: 10.11999/JEIT210577

Local Logic Camouflaging Based IC Circuit Protection Method

YANG Ran[①] GAO Wenchao[②]

[①](*School of Mathematics, China University of Mining and Technology, Xuzhou* 221116, *China*)

[②](*College of Mechanical Electronic & Information Engineering, China University of Mining & Technology* (*Beijing*), *Beijing* 100083, *China*)

Abstract: With illegal hardware reverse engineering attacks, the Integrated Circuit (IC) design suffers from the key Intellectual Property (IP)/algorithm piracy and hardware Trojan insertion. An IC camouflaging method, LPerturb, is proposed in this paper by local circuit logic perturbation for IP Protection. The circuit is partitioned into some Maximum Fanout-Free Cones (MFFCs), namely multiple functionally independent sub-circuits to be camouflaged, for output logic perturbation locally. A logic cell is selected in the MFFC sub-circuit. The cell is replaced to perturb the logic functionality of the MFFC minimally. A multi-logic camouflaged block is used to protect and restore the perturbed logic secret. Experimental results show that LPerturb can produce the camouflaged circuits steadily, which has good output corruptibility and effectively resists SAT based attack. The overhead in area and timing is also in low level.

Key words: Hardware security; IC protection; IC camouflaging; Logic obfuscation; Minterm perturbation

1 引言

集成电路(Integrated Circuit, IC)的重要性逐渐提高，IC盗版使得硬件安全受到严重威胁。借助非法的逆向工程手段，攻击者通过静态图像分析和动态匹配的方式，获取IC设计网表和核心算法。防止IC逆向工程攻击，保护其知识产权(Intellectual Property, IP)和硬件安全成为一个重要问题。电路混淆技术是一种抵抗IC剽窃的重要手段，通过增大攻击者理解电路设计的难度，阻止IC电路知识产权剽窃和硬件木马植入。电路混淆是一种主动保护技术，防止芯片IP被非法剽窃和篡改[1]，主要形式有逻辑加密[2]和IC伪装[3]。

在IC硬件安全领域，一直存在攻击方和防御方两者的对抗[4]，在这种对抗中硬件安全技术得到极大的提高。通过非法逆向工程手段，得到的IC逻辑网表中存在一些被混淆保护的逻辑单元，需要通过其它手段去还原这些逻辑单元的真实逻辑功能，这个过程称为去混淆攻击(de-obfuscation attack)。去混淆攻击的目标是用尽可能低的攻击复杂度高效

收稿日期：2021-06-15；改回日期：2021-08-12；网络出版：2021-08-23
*通信作者： 高文超 gaowc@cumtb.edu.cn
基金项目：国家自然科学基金(61834002)，北京信息科学与技术国家研究中心(BNR2019ZS01001)

Foundation Items: The National Natural Science Foundation of China (61834002), Beijing National Research Center for Information Science and Technology (BNR2019ZS01001)

地还原出混淆单元的功能，攻击复杂度越低，去混淆攻击越有效[5]。

去混淆攻击主要包括暴力枚举攻击、基于IC测试技术的攻击、基于划分的攻击、基于剥离手段的攻击和基于可满足性(SATisfiability, SAT)技术的攻击等。暴力枚举攻击[6]穷尽混淆单元所有可能的逻辑组合，破解单元的真实逻辑。基于IC 测试技术的攻击[6,7]利用控制和敏化等手段，观察主输入端-主输出端逻辑行为，还原混淆单元真实逻辑。基于划分的攻击[8]采取分而治之策略，将混淆电路分割成一些功能独立的子电路，降低攻击的复杂度。基于剥离手段的攻击策略DeCamo [9]针对最小项伪装方法，发现其伪装电路，分离出扰动电路，依据单个最小项保护原理，从扰动电路中找到替换的门和正确逻辑进行还原。基于SAT技术的攻击[10,11]是目前最有效的攻击技术，用SAT技术排除混淆单元错误的逻辑功能组合，得到正确的功能组合。

在去混淆攻击技术的促进下，一些新的混淆方法被提出。针对基于IC测试技术和暴力枚举的攻击，通过关联型电路混淆[6,12]的手段提高抵抗能力。针对基于SAT攻击，与树(And-Tree)混淆[13]和CamoPerturb[14] 等方法，降低排除功能组合的能力，使其攻击复杂度呈现指数级增长。

从IC保护的对象上来说，一般的IC伪装保护对象是整个电路，也就是说是面向IC电路的所有的逻辑(最小项)。文献[14]的CamoPerturb方法则是保护电路的其中一个最小项逻辑。在实际电路设计中，存在一些重要的逻辑功能点，担负着电路重要的功能。例如，在控制器上会有若干特定的关键编码，用于激活特定的控制信号。在访问控制机制中，需要对密码进行检查，启动有效信号。在中断控制器设计中，请求信号会启动中断处理。对这些特定的“编码”(即最小项)进行保护，也就是对整个电路实施了必要的保护。本文深入研究基于最小项保护策略，提出更加实用、稳定性更强、额外开销低的IC伪装方法LPerturb。

2　IC伪装技术

业界提出了一些IC电路伪装技术，在一定程度上抵抗了IC逆向工程的攻击。在IC布图层面，通过伪装逻辑门版图，使得逆向工程无法直接通过图像识别提取逻辑网表。这些经过特殊伪装技术设计的伪装单元，被用来替换电路中特殊选择的逻辑单元。目前常用的伪装技术包括真实/虚假连接伪装单元、基于新器件的伪装单元、基于SRAM的伪装单元等，其中最常用的手段是用真实/虚假连接方法构建伪装单元。

2.1　反向器/缓冲器伪装单元

反向器/缓冲器(INVerter/BUFfer, INV/BUF)伪装单元是一个由真实/虚假连接构成的伪装逻辑单元，广泛用于抵抗SAT攻击方法[13]中。如图1所示，当触点1为真，触点2为假时，伪装单元为反向器，反之则为缓冲器。本文采用文献[14]的方法，用这种INV/BUF伪装单元来构建输入映射和硬编码密钥生成，具有一定的伪装性。

2.2　基于最小项保护的伪装技术

针对基于SAT技术的攻击，文献[14]提出了一种基于最小项保护的伪装方法CamoPerturb。与传统IC伪装技术试图保护整个设计策略[15]不同，CamoPerturb试图保护设计中选定的最小项。通过改动电路初始结构，添加或删除主输出的一个逻辑最小项。同时，使用特殊设计的伪装电路恢复被扰动的最小项，该伪装电路具有抗SAT攻击的能力。CamoPerturb主要结构如图2所示，扰动电路C_{pert}为与原电路有一个最小项不同的改动后电路，伪装模块CamoFix负责保护和还原扰动的最小项。

伪装模块CamoFix由INV/BUF伪装单元组成，其输入为初始电路的主输入，每个输入均与伪装单元相连接；其输出与C_{pert}输出相异或，从而恢复主输出的正确功能。通过此结构，使得每一组输入向量每次仅能排除一个可能的逻辑门功能组合。在性能开销仅线性增长的情况下，基于SAT的去伪装技术的复杂性呈指数式增长，因而能够有效抵御基于SAT的去伪装技术攻击。

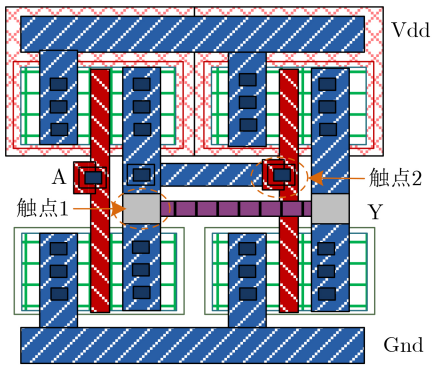

图 1 INV/BUF伪装单元结构[14]

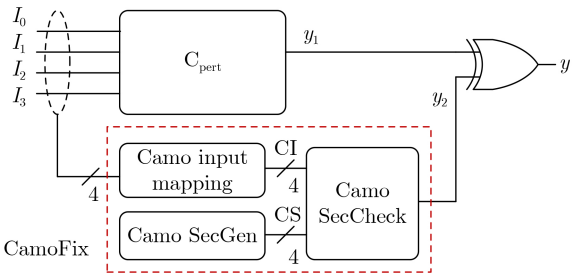

图 2 CamoPerturb结构[14]

3 局部电路逻辑扰动方法LPerturb

文献[14]只给出了最小项扰动思想，没有给出具体的最小项扰动方法，在一定程度上限制了CamoPerturb方法的应用。文献[9]和文献[16]给出了通过通路敏化与静态逻辑蕴涵技术，查找影响单个最小项的逻辑单元的方法。这些方法只关注逻辑单元对最小项的影响，没有考虑这个逻辑单元的替换可能会影响多个主输出。这个逻辑单元替换后只对一个主输出逻辑的单个最小项产生影响，但对其它主输出可能会带来多个逻辑功能的影响。

在对选择的逻辑单元进行逻辑替换时，有时候找不到只影响单个逻辑最小项的逻辑单元的输入逻辑向量。这种情况下，将会出现扰动多个最小项的状况。为了确保逻辑扰动的进行，需要处理多个逻辑最小项值扰动保护和重置的情况。以上情况，直接影响最小项扰动方法的稳定性。

另外，文献[9,14,16]针对的是整个电路主输出逻辑的保护，在对最小项进行伪装和逻辑功能恢复时，面对的是整个电路的主输入向量。这种策略带来的伪装代价是与输入向量位数呈正比关系，势必增加电路伪装的额外开销。

针对以上问题，尤其是最小项扰动方法的稳定性问题，本文提出一种局部电路的混淆方法LPerturb。在基于最小项保护的伪装技术思想基础上，通过对其局部子电路逻辑的扰动，实现对整个IC电路的保护。本文逻辑伪装方法伪代码见表1。步骤(1)利用3.1节介绍的最大独立锥划分方法，将整个电路切分成一些逻辑独立性子电路。步骤(2)对这些逻辑独立的最大子电路进行伪装，确保输出逻辑扰动的局部性。采用3.2节的方法，选择被替换的逻辑单元和替换的逻辑功能向量，确定逻辑门替换逻辑及相应的电路，进行局部电路逻辑扰动。然后，用3.3节的多值伪装电路对扰动的逻辑值进行混淆保护，恢复相应的子电路逻辑。最后，合并所有子电路产生伪装电路。

表 1 逻辑伪装方法LPerturb伪代码

输入：原始网表C_{orig}；

输出：伪装网表C_{camo}；

(1)利用最大独立锥划分方法，提取最大独立扰动子电路集$\{C_{\text{MMFCi}}\}$；

(2)for 最大独立扰动子电路C_{MMFCi} {

计算逻辑门的扰动最小项集合；

选择替换逻辑单元和扰动最小项集合；

确定逻辑门替换逻辑及电路；

生成子电路扰动电路C^{i}_{pert}和伪装模块C^{i}_{CamoFix}子电路；

生成伪装子电路C^{i}_{camo} }

(3)生成伪装电路C_{camo}

3.1 最大独立扰动电路提取

在进行扰动电路生成时，为了不影响多个输出函数的逻辑值，避免对其它输出函数带来不希望的扰动，借鉴FPGA工艺映射中的最大独立锥(Maxium Fanout-Free Cone, MFFC)划分方法[17]，对电路进行独立子电路提取，使得提取的子电路中的逻辑单元只对选定的输出端信号产生影响。

最大独立锥划分技术最初用于求解FPGA电路中无复制单元和面积最佳的LUT工艺映射，能够保证划分的子电路中信号传递方向和逻辑门的独立性。最大独立锥MFFC为电路中的一个子电路，其满足以下性质：(1)子电路只有一个最终的根结点作为输出结点；(2)所有子电路中的结点，除了根结点以外，其他结点的所有输出结点也均在子电路中；(3)在子电路中加入任意一个新结点后，第2条不能被满足。显而易见，在一个MFFC中的逻辑结点只直接影响该MFFC子电路根结点的逻辑。如图3所示，虚线框里的电路表示用MFFC划分后所得到的子电路。

在最大独立锥划分过程中，存在着最大独立锥包含的情况[18]，如图3中虚线框的MFFC被整个电路表示的MFFC所包含。在最大独立扰动电路提取过程中，需要综合考虑所提取出的输入信号端口数、子电路逻辑层级以及所包含的逻辑单元数。这些因素将会影响整个电路伪装带来的成本和性能上的增加，如输入信号端口数直接影响后续伪装电路模块的规模。输入端口多，所需要的INV/BUF伪装单元数目就会相应增多，带来面积成本的增加。一般来说，最大独立锥的输入端口控制在4～6个，逻辑层级在4～8层。

与传统的面向整个IC电路进行伪装的策略不同，采用最大独立扰动子电路保护策略可以提升伪装的保护能力。试图保护整个设计的IC伪装技术，容易遭受传统去伪装攻击。基于最小项保护的伪装策略，改变一项输出逻辑，输出扰动较小，也不能够

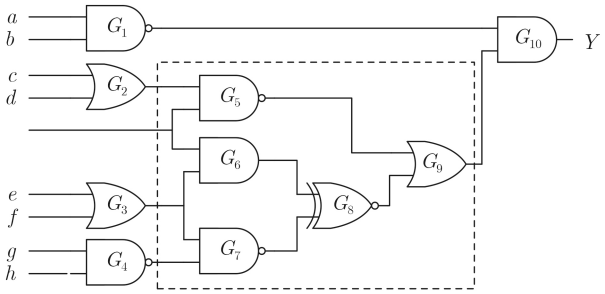

图 3 最大独立锥电路划分示例

很好地保护电路安全。将面向整个电路的最小项保护改变成面向局部子电路，能够获得较高的整体电路输出的扰动数量。局部子电路中扰动的逻辑，随着子电路输出信号向整体电路输出主端口的传播，整个电路的主输出数据被扰动数量，将会随着电路层级结构而增多，也将可能波及多个主输出端口。

相对于对整个电路扰动最小项策略，对最大独立扰动电路提取的子电路进行逻辑扰动策略，需要的额外电路单元要少。对整个电路扰动情况下，每一个CamoFix模块要面对整个电路的主输入向量。而对子电路进行扰动时，CamoFix模块只是面对子电路的输入向量。由于CamoFix模块的单元数与扰动最小项个数和输入向量大小呈现线性增长，在同样数量最小项扰动的情况下，对子电路扰动的方法将会产生较小的额外面积开销。

3.2 最小项扰动计算方法

文献[14]采用逻辑单元的替换方式，实现电路输出逻辑最小项扰动。在数字电路中，单元的逻辑功能会影响一部分逻辑最小项。借助通路敏化与静态逻辑蕴涵的手段[9,16]，可以得到一个电路中的逻辑单元输入向量$\boldsymbol{G}_i$影响该电路最小项的子集SMA($\boldsymbol{G}_i$)，从而获得逻辑单元G对电路最小项影响子集SMA$\{G\}$。对比原始逻辑单元G_{orig}与替换后逻辑单元G_{trans}真值表，可以得到相同输入而不同输出时所对应的输入向量的集合N'，从而可以得到逻辑门替换引起的最小项扰动的集合SMA$\{G_{\text{orig}} \to G_{\text{trans}}\} = \bigcup_{n\in\mathbf{N}'} \text{SMA}(\boldsymbol{G}_{i_n})$[9,16]。

如图4电路所示，采用通路敏化和向后直接蕴涵的手段，可以得到逻辑单元G_4的每一个输入向量能够影响的最小项，如表2所示。

从表2可以得到，逻辑单元G_4的输入$\{e,f\}$的向量**00**没有影响任何最小项，**01**向量影响了2个最小项m_{12}和m_{13}，**10**向量影响了1个最小项m_{15}，**11**向量影响了1个最小项m_{14}。如果用与门AND逻辑单元替换G_4，对Y输出没有任何最小项被扰动，替换后的电路与初始电路功能完全相同。若将G_4替换为或非门NOR，则一项最小项m_{14}被扰动，电路仅在主输入(a, b, c, d)=(1, 1, 1, 0)时，功能与初始电路不同，其余功能完全相同。同样，用Fun1逻辑进行替换可以扰动2个最小项m_{12}和m_{13}，用Fun2逻辑进行替换可以扰动1个最小项m_{15}。

基于子电路中逻辑单元各个输入向量对子电路输出最小项逻辑影响的分析，从中选出最终要进行扰动的最小项，将影响该最小项的逻辑单元替换成对应逻辑功能的逻辑单元，或者按照真值表产生相应逻辑功能的替换电路。

在进行逻辑单元选择时，可以遵循最小扰动优先的原则，选择最小项影响小的输入向量对应的逻辑单元进行替换。可以参考关联型电路混淆[12]选择方法，提升抵抗基于IC 测试技术攻击和暴力枚举攻击的能力。也可以采用等价类引导的选择方法[19]，提升抵抗划分攻击的能力，增强基于SAT攻击的抵抗力。

3.3 多值伪装模块

在文献[14]中，伪装模块CamoFix是由硬编码INV/BUF伪装门组成的，用来隐藏扰动最小项的特别电路。如图2所示，CamoFix由输入映射(Camo Input Mapping)、密钥生成(Camo SecGen)、密钥确认(Camo SecCheck)3个子模块组成。输入映射模块通过INV/BUF伪装门对输入向量进行加密编码，产生与输入向量不同的输入编码**CI**向量；密钥生成模块用INV/BUF伪装门电路产生硬编码密钥**CS**向量；密钥确认模块则比较检查**CI**向量和**CS**向量，只有当接收到扰动的最小项作为CamoFix的输入时，**CI**向量和**CS**向量的匹配才会一致，产生输出1。

在CamoPerturb中，只对单个最小项进行保护。CamoFix输入映射模块是单个最小项映射函数，只有当受保护的那个最小项出现在输入端口时，输入映射模块才能产生出正确的输入编码**CI**向量。

从3.2节最小项扰动计算中可以看出，逻辑单元各个输入向量影响的电路输出最小项逻辑的数量是不可控制的，可能是空集，也可能是多个最小项的集合。对于复杂的电路来说，尤其是经过逻辑综合优化后的电路，每个逻辑单元将会影响多个逻辑最小项。因此，CamoPerturb方法只针对1个最小

表 2　逻辑单元G_4影响最小项

输入向量		影响最小项SMA(i_1,i_2)	G_{orig}	G_{trans}			
e	f		XNOR	AND	NOR	Fun1	Fun2
0	0	{ }	1	0	1	1	1
0	1	$\{m_{12}(abc'd'),m_{13}(abc'd)\}$	0	0	0	1	0
1	0	$\{m_{15}(abcd)\}$	0	0	0	0	1
1	1	$\{m_{14}(abcd')\}$	1	1	0	1	1

项扰动的策略存在着局限性，极有可能找不到单个替换门只影响1个最小项，必须支持多个最小项逻辑的扰动保护。

为了能够在单个保护子电路中对多个最小项值进行保护，需要对CamoFix电路进行改造。构建多值伪装模块，支持多个最小项逻辑值的伪装保护。在保持CamoFix电路密钥生成模块和密钥确认模块功能不变的情况下，对输入映射模块进行重新设计。使其对多个最小项输入向量进行编码映射时，产生相同的输入编码**CI**向量。为此，按照CamoFix的输入向量编码规则，对多个最小项输入向量分别用INV/BUF伪装门建立各自的加密编码电路，以产生相同的输入编码**CI**向量。然后，对这些最小项输入向量加密编码电路，按位进行同或运算，产生出最后的总的**CI**向量。如对图4电路的2个最小项m_{12}和m_{13}同时实施扰动保护，需要分别建立(INV, BUF, INV, BUF)和(INV, BUF, INV, INV)两个输入向量加密编码电路(如图5所示)，以便产生共同的**CI**向量(0110)。与(INV, BUF, BUF, INV)硬编码密钥生成模块(如图6所示)产生的**CS**向量(0110)，在密钥确认模块(如图7所示)中进行匹配。这样就能够对多个最小项进行保护，在相应的最小项输入向量处产生输出1。

在基于SAT技术的攻击中，用一些能鉴别错误功能组合的输入向量(Discriminating Inputs, **DI**)排除不正确伪装单元的功能组合，最终识别出逻辑单元的真实功能。这些**DI**的集合称为鉴别输入向量集合(Set of Discriminating Inputs, **SDI**)，**SDI**集合中**DI**的数量|**SDI**|表示基于SAT攻击的时间复杂性。LPerturb方法在保护的安全性上，与CamoFix的安全性保持一致，使每个**DI**除了扰动的最小项向量外，都只消除对硬编码密钥**CS**的一个不正确的分配。攻击需要的**DI**数量与错误分配的数量一样多，是伪装门数量的指数。对于k个伪装门，l个扰动最小项数量，$|\mathbf{SDI}|=2^k-l$。对于一般电路，l的取值在1～3。

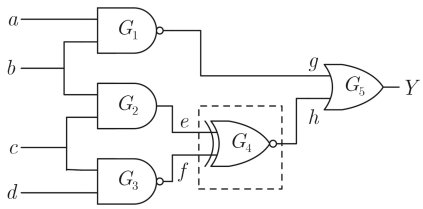

图 4 逻辑单元G_4最小项扰动计算

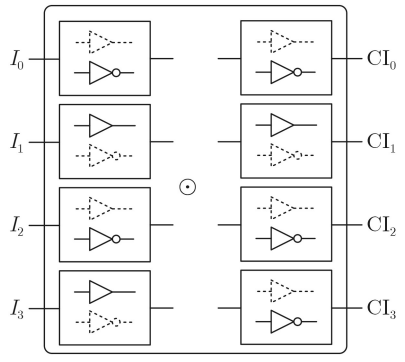

图 5 输入映射模块(产生m_{12}和m_{13}的**CI**编码)

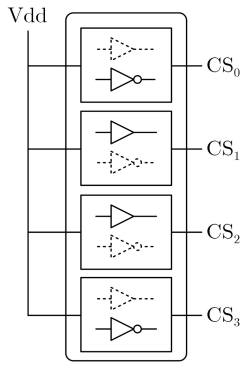

图 6 (INV, BUF, BUF, INV)硬编码密钥生成模块[14]

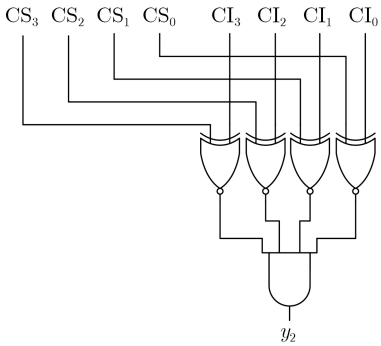

图 7 密钥确认模块[14]

4 实验与分析

通过实验对LPerturb方法的有效性进行评估，实验测试案例来自ISACS'89基准电路[20]和OpenSPARC微处理器的控制器电路[21]，选取与文献[14]中CamoPerturb相近的基准电路，实验测试电路基本信息参见文献[19]的表5.3。采用ABC综合工具[22]进行电路综合和预处理，通路敏化和逻辑蕴涵等计算选用Atalanta项目[23]的自动测试向量生成FAN算法。实验环境为Intel Core i5 CPU 2.7 GHz处理器，16 GB RAM，Linux系统。

4.1 抵御SAT攻击

为了测试LPerturb抵御SAT技术的攻击情况，采用文献[24]提出的基于SAT的增量算法，对LPerturb的伪装电路进行攻击破解实验。实验的伪装电路采用与文献[14]中CamoPerturb相同的伪装门个数，即替换的逻辑门个数为8～13。

图8给出实验数据，可以看出SAT攻击技术的运行时间与伪装门个数呈现出指数级关系。与文献[14]的实验结果对比，能够发现LPerturb基本保持了CamoPerturb的防御SAT攻击的特点，鉴别输入向量集合**SDI**中DI的数量|SDI|呈现出指数级增长，有效地抵御基于SAT技术的攻击。

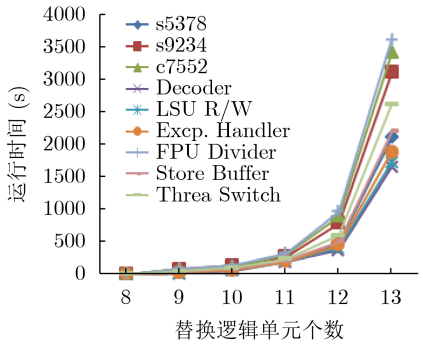

图 8 使用SAT攻击伪装技术的时间开销

同时，还针对文献[9]最小项保护伪装电路攻击技术DeCamo进行了攻击测试，在同样的测试案例和伪装门个数的情况下，DeCamo攻击的时间仅比SAT攻击技术的运行时间略长0.2～67.4 s。由于两个攻击技术的运行时间具有高度的相似度，在折线图上体现不出来，在此就不再列出。

从DeCamo攻击的实验结果来看，LPerturb方法能够防御DeCamo攻击。追其原因，LPerturb方法对局部电路的输出端信号进行保护，而非电路的主输出端信号，在一定程度上扰乱伪装电路的剥离；同时，对多个最小项值进行扰动的策略和逻辑单元的替换电路方法，可能使得DeCamo无法找到单个替换门进行还原。

4.2 输出扰动性

对于硬件保护技术来说，电路的输出扰动数量(output corruptibility)是IC伪装效果的一个评判标准。电路原始设计与伪装后的电路设计差别越大，即输出更改的数量越多，说明电路的伪装越成功。

通常，可以通过计算两者输出的汉明距离，评估输出扰动数量。电路的汉明距离，则由电路对应位置所产生的不同输出个数进行评估。不同输出逻辑个数占总输出逻辑个数比例越高，说明对该输出逻辑的扰动就越大。文献[14]的基于最小项伪装技术，保护主输出的一项最小项，输出逻辑的不同仅为1个。这种方法的伪装策略的汉明距离小，输出扰动性小。

本实验对LPerturb的输出扰动性进行了测量，与当前主流的伪装策略，如随机选择策略(Random Selection, RS)、基于集群的选择(Clique Based Selection, CBS)和基于输出扰动数量的选择策略(Output Corruptibility based Selection, OCS)[15]进行对比。

实验采用自动测试向量生成攻击工具HOPE，用1000个随机输入向量，计算原始电路与伪装电路输出的汉明距离。在同样的伪装门个数(8～13个)的情况下，测量计算LPerturb电路与原始电路的汉明距离。图9给出了本文LPerturb的汉明距离测量数据，并与当前主流的伪装策略RS, CBS和OCS方法[15]进行了对比。从图9可以看出，基于输出扰动数量的选择策略OCS具有较强的输出扰动性。本文LPerturb方法与随机选择策略RS接近，接近4种伪装技术的平均值附近。测量实验表明，文中方法可以提升伪装电路的输出数据扰动性。

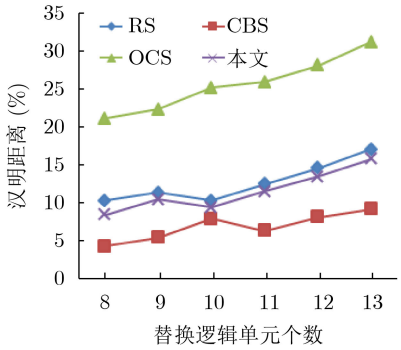

图 9 输出数据扰动性汉明距离比较

4.3 额外开销分析

硬件混淆技术采用一定的伪装技术，替换原有的逻辑单元，会带来面积成本和性能上的代价。LPerturb方法也会带来这种额外开销，主要是扰动原始电路、伪装模块和子电路输出的异或门等3个方面的额外开销。扰动原始电路的开销主要是替换逻辑单元带来的差异变化，与替换的逻辑差异有关，不好量化。一般来说，在逻辑门级替换的成本变化不会太大。伪装模块带来的成本变化容易计算，带来的额外开销与子电路扰动的最小项数目和输入端口数成正比。

采用TSMC 0.35 μm PDK 的俄克拉何马州立大学标准单元库和开源的ABC 综合工具[22]，对LPerturb方法进行额外开销估测。以文献[14]表4中给出的Inverter和Buffer数据为依据，对伪装模块中的INV/BUF单元选用Buffer单元进行替代估算。估算结果显示，伪装电路面积额外增加12.4%～27.6%，延迟增加不到1%。相对于文献[14]中的数据，面积和性能的额外开销有所降低。其主要原因是文中方法采用局部子电路扰动的策略，减少了伪装电路模块的规模。从时延分析的角度看，局部电路最小项

扰动稳定性提高了，替换后的逻辑单元带来的延时变化不大。

5 结束语

本文对基于CamouPertb最小项保护策略的IC伪装技术进行了分析，结合逻辑最小项扰动方法的局限性和稳定性，以及CamouPertb方法的实用性，提出了一种局部电路逻辑扰动的IC保护方法LPerturb。针对替换单元对多个输出函数的影响问题，采用最大独立锥的划分方法，获取具有最大逻辑独立性的扰动子电路。针对逻辑替换带来的多个最小项逻辑的扰动问题，采用多值逻辑保护方法，确保逻辑替换的可靠性。针对电路扰动对主输入和主输出依赖带来的额外开销大和输出扰动小的问题，采用局部子电路扰动的策略，提高了伪装的输出扰动性，在一定程度上降低了伪装的额外开销。此方法还存在一些优化的地方，如进一步研究最大独立锥划分对扰动稳定性和额外开销的影响，寻找较佳的独立锥的逻辑层次和输入端口数，提高基于最小项保护伪装策略的有效性和实用性。

参 考 文 献

[1] ZHANG Jiliang. A practical logic obfuscation technique for hardware security[J]. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2016, 24(3): 1193–1197. doi: 10.1109/TVLSI.2015.2437996.

[2] 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. doi: 10.11999/JEIT180898.
ZHANG Yuejun, WANG Jiawei, PAN Zhao, *et al*. Hardware security for multi IPs protection based on orthogonal obfuscation[J]. *Journal of Electronics & Information Technology*, 2019, 41(8): 1847–1854. doi: 10.11999/JEIT180898.

[3] 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.

[4] WANG Xueyan, ZHOU Qiang, CAI Yici, *et al*. Spear and shield: Evolution of integrated circuit camouflaging[J]. *Journal of Computer Science and Technology*, 2018, 33(1): 42–57. doi: 10.1007/s11390-018-1807-6.

[5] ROSTAMI M, KOUSHANFAR F, RAJENDRAN J, *et al*. Hardware security: Threat models and metrics[C]. 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, USA, 2013: 819–823.

[6] RAJENDRAN J, PINO Y, SINANOGLU O, *et al*. Security analysis of logic obfuscation[C]. The 49th Annual Design Automation Conference, San Francisco, USA, 2012: 83–89.

[7] YASIN M, SENGUPTA A, NABEEL M T, *et al*. Provably-secure logic locking: From theory to practice[C]. The 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA, 2017: 1601–1618.

[8] WANG Xueyan, ZHOU Qiang, CAI Yici, *et al*. An empirical study on gate camouflaging methods against circuit partition attack[C]. The on Great Lakes Symposium on VLSI, Banff, Canada, 2017: 345–350.

[9] JIANG Shan, XU Ning, WANG Xueyan, *et al*. An efficient technique to reverse engineer minterm protection based camouflaged circuit[J]. *Journal of Computer Science and Technology*, 2018, 33(5): 998–1006. doi: 10.1007/s11390-018-1870-z.

[10] YU Cunxi, ZHANG Xiangyu, LIU Duo, *et al*. Incremental SAT-based reverse engineering of camouflaged logic circuits[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2017, 36(10): 1647–1659. doi: 10.1109/TCAD.2017.2652220.

[11] SHAMSI K, LI Meng, MEADE T, *et al*. Circuit obfuscation and oracle-guided attacks: Who can prevail?[C]. Proceedings of the on Great Lakes Symposium on VLSI 2017, Banff, Canada, 2017: 357–362.

[12] YASIN M, SINANOGLU O, and RAJENDRAN J. Testing the trustworthiness of IC testing: An oracle-less attack on IC camouflaging[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(11): 2668–2682. doi: 10.1109/TIFS.2017.2710954.

[13] LI Meng, SHAMSI K, MEADE T, *et al*. Provably secure camouflaging strategy for IC protection[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2019, 38(8): 1399–1412. doi: 10.1109/TCAD.2017.2750088.

[14] YASIN M, MAZUMDAR B, SINANOGLU O, *et al*. CamoPerturb: Secure IC camouflaging for minterm protection[C]. 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, USA, 2016: 1–8.

[15] RAJENDRAN J, SAM M, SINANOGLU O, *et al*. Security analysis of integrated circuit camouflaging[C]. Proceedings of the 2013 ACM SIGSAC Conference on COMPUTER & Communications Security, Berlin, Germany, 2013: 709–720.

[16] 高文超, 罗世玲, 周强. 指定逻辑的电路最小项扰动算法[J]. 计算机辅助设计与图形学学报, 2020, 32(6): 1009–1016. doi: 10.3724/SP.J.1089.2020.17961.
GAO Wenchao, LUO Shiling, and ZHOU Qiang. A stable perturbation circuit minterm generation algorithm with

specific logic[J]. *Journal of Computer-Aided Design & Computer Graphics*, 2020, 32(6): 1009–1016. doi: 10.3724/SP.J.1089.2020.17961.

[17] CONG J and DING Yuzheng. On area/depth trade-off in LUT-based FPGA technology mapping[J]. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 1994, 2(2): 137–148. doi: 10.1109/92.285741.

[18] BEAMER S and DONOFRIO D. Efficiently exploiting low activity factors to accelerate RTL simulation[C]. 2020 57th ACM/IEEE Design Automation Conference (DAC), San Francisco, USA, 2020: 1–6.

[19] WANG Xueyan, ZHOU Qiang, CAI Yici, *et al*. Toward a formal and quantitative evaluation framework for circuit obfuscation methods[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2019, 38(10): 1844–1857. doi: 10.1109/TCAD.2018.2864220.

[20] BRGLEZ F, BRYAN D, and KOZMINSKI K. Combinational profiles of sequential benchmark circuits[C]. IEEE International Symposium on Circuits and Systems, Portland, USA, 1989: 1929–1934.

[21] Sun Microsystems. OpenSPARC™ T1 microarchitecture specification[EB/OL]. http://www.oracle.com/technetwork/systems/opensparc/t1-01-opensparct1-micro-arch-1538959.html, 2008.

[22] BRAYTON R and MISHCHENKO A. ABC: An academic industrial-strength verification tool[C]. Proceedings of the 22nd International Conference, Edinburgh, UK, 2010: 24–40.

[23] LEE H K and HA D S. Atalanta: An efficient ATPG for combinational circuits[R]. Technical Report, 93–12, 1993.

[24] LIU Duo, YU Cunxi, ZHANG Xiangyu, *et al*. Oracle-guided incremental SAT solving to reverse engineer camouflaged logic circuits[C]. 2016 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 2016: 433–438.

杨　然：女，1973年生，工程师，研究方向为大规模数值计算、组合优化算法.

高文超：女，1986年生，副教授，研究方向为时空大数据、计算机辅助设计.

责任编辑：马秀强