

基于 TVD 的逻辑混淆电路设计及其性能分析

李立威¹, 汪鹏君^{1,2*}, 张跃军^{1,3}

(1. 宁波大学 电路与系统研究所, 浙江 宁波 315211; 2. 温州大学 数理与电子信息工程学院, 浙江 温州 325035;
3. 密码科学技术国家重点实验室, 北京 100878)

摘要: 逆向工程和差分功耗分析(Differential Power Analysis, DPA)是盗取知识产权(Intellectual Property, IP)核信息的重要手段. 通过对逻辑混淆电路和数据功耗间关系的研究, 采用三相双轨预充逻辑(Three-phase Dual-rail Pre-charge Logic, TDPL), 利用定义的阈值电压(Threshold Voltage Defined, TVD)特性, 提出一种能防御逆向工程和 DPA 攻击的逻辑混淆电路方案. 该方案利用对称的差分下拉网络和灵敏放大器, 采用相同的电路结构, 通过阈值电压的配置实现不同的逻辑功能. Spectre 仿真验证表明, 基于 TVD 的逻辑混淆电路逻辑功能正确, 在多种 PVT(Process, Voltage, Temperature)下获得的归一化能量偏差和归一化标准差最高分别为 0.107 2% 和 0.045 3%, 与普通静态 CMOS 电路相比, 能耗独立性能提升 21.79%, 能够有效防御逆向工程和 DPA 攻击.

关键词: 逻辑混淆; 定义的阈值电压; 逆向工程; 差分功耗分析

中图分类号: TN79

文献标志码: A

文章编号: 1001-5132 (2019) 03-0040-05

随着超大规模集成电路和信息安全技术的发展, 知识产权(Intellectual Property, IP)的保护受到越来越多的关注. 然而, 对 IP 核展开的攻击方式层出不穷, 逆向工程是快速获取设计者核心技术的途径^[1]. 攻击者通过逆向工程剖析芯片的内部结构, 提取电路网表, 掌握芯片的实际功能, 影响设计者的合法利益, 芯片克隆等行为更是严重侵犯设计者的知识产权. 为保护 IC 设计中的关键技术不被轻易盗取, 近年来, 学者们提出逻辑混淆来保护电路. 版图级混淆通过虚拟孔来阻断金属之间的电气连接^[2-3], 在芯片自顶向下逐层剥离时极易与真实孔相混, 以此保护 IP 核. 然而, 基于虚拟孔的电路混淆技术需要在安全性和可靠性之间权衡. 调整金属层之间的间隙可防止攻击者通过磨片拍照提取电路关键信息, 但间隙过小, 在生产过程中由于刻蚀难度大等原因极易引起短路, 影响整个芯片的功能; 若金属间隙过大, 虽然可靠性较好, 但容易被逆向工程识别. 行为级混淆通过对电路中有限状态机的修改, 使得修改后的状态机在 IC 设

计者未授权的情况下, 不能直接跳转到原始有限状态机, 从而保护硬件 IP 核^[4]. 但冗余状态和黑洞状态的插入, 导致芯片面积和功耗开销过大, 而且容易遭到旁道攻击找出有效状态.

此外, 攻击者针对加密芯片可绕过密码算法本身, 采集不同轮函数加密过程中泄漏出来的物理信息如功耗、电磁辐射等, 并使用统计学方法推测出密钥, 即旁道攻击(Side Channel Attack, SCA)^[5]. 其中, 差分功耗分析(Differential Power Analysis, DPA)是 SCA 中最常见且最高效的一种攻击方式^[6]. 防御 DPA 攻击已成为当下研究的热点, 主要技术包括: 绝热动态差分逻辑(Adiabatic Dynamic Differential Logic, ADDL)^[7]、基于查找表的差分逻辑(LUT Based Differential Logic, LBDL)^[8]和灵敏放大逻辑(Sense Amplifier Based Logic, SABL)^[9-10]等, 但这些逻辑在输出负载电容不完全一致时, 仍有可能作为 DPA 攻击的突破点. 新近出现的三相双轨预充逻辑(Three-Phase Dual-Rail Pre-charge Logic, TDPL)引入了额外的放电阶段,

收稿日期: 2018-10-23.

宁波大学学报(理工版)网址: <http://journalg.nbu.edu.cn/>

基金项目: 国家自然科学基金(61874078, 61871244); 浙江省自然科学基金(LY18F040002); 浙江省公益项目(2016C31078).

第一作者: 李立威(1994-), 男, 浙江宁波人, 在读硕士研究生, 主要研究方向: 信息安全芯片理论和设计. E-mail: 794456736@qq.com

*通信作者: 汪鹏君(1966-), 男, 浙江奉化人, 博导/教授, 主要研究方向: 逻辑电路和低功耗集成电路. E-mail: wangpengjun@nbu.edu.cn

因此具有良好的恒定功耗特性, 使其在抗 DPA 攻击中具有明显的优势.

鉴此, 本文利用 TDPL 功耗与输入数据相互独立的特征, 结合注入离子掺杂浓度不同定义的不同阈值电压特性, 提出一种既能防御逆向工程又可防御 DPA 攻击的逻辑混淆电路. 所提方案采用 TSMC 65 nm CMOS 工艺实现, 并通过 Spectre 验证其功能和性能.

1 基于 TVD 的逻辑混淆电路设计

基于 TVD 的逻辑混淆电路由灵敏放大器、差分下拉网络、预充管、求值管和放电管构成. 当输入信号有效时, 下拉网络中的分支导通, 经过灵敏放大器比较 2 条分支的电压, 得到互补的输出信号. 具体电路如图 1 所示, 电路的工作时序图如图 2 所示, 工作过程分为预充电、求值和放电 3 个阶段. 当输入信号 $\overline{charge}$ 、 $\overline{discharge}$ 、 $\overline{eval}$ 为低电平时, 电路进入预充电阶段, P1、P2、P5 管导通, 输出 $\overline{out}$ 、 $\overline{out}$ 预充电至 V_{DD} ; 随着 $\overline{eval}$ 、 $\overline{charge}$ 变为高电平, MOS 管 P2、P5 截止, 电路预充电结束. 同时求值管 N21 导通, 电路进入求值阶段, 此时 $A=1$, $B=1$, 下拉网络中 N5、N6、N19、N20 导通, N2、N3 的栅极电压之前已预充至高电平, 因而有电流 I_1 、 I_2 流过. 由于 N5、N6 为低阈值管, 由 2 个交叉耦合反相器构成的灵敏放大器将电流差放大, $\overline{out}$ 率先放电至低电平, P4 导通, $\overline{out}$ 仍然保持高电平; 当 $\overline{eval}$ 为低电平, $\overline{discharge}$ 变为高电平时, N21 截止, 求值结束. 同时 N1、N4 导通, 电路进入放电阶段, $\overline{out}$ 、 $\overline{out}$ 放电至低电平, 一个工作周期结束, 实现异或逻辑功能. 基于 TVD 的与非门电路如图 3 所示, 在输入 0/0、0/1、1/0 时, $\overline{out}$ 放电至低电平, $\overline{out}$ 为高电平, 输入 1/1 时, $\overline{out}$ 放电至低电平. 基于 TVD 的或非门电路如图 4 所示, 输入 0/0 时, $\overline{out}$ 放电至低电平, $\overline{out}$ 为高电平, 输入 0/1、1/0、1/1 时, $\overline{out}$ 放电至低电平.

综上, 基于 TVD 的二输入异或门、与非门、或非门具有相同的电路结构, 仅通过配置阈值电压实现不同的逻辑功能, 而且在每个工作周期内的输出都从预充电 V_{DD} 开始放电至 V_{SS} , 消耗能量恒定, 与输入数据相互独立, 在防御逆向工程攻击的同时, 具有抗 DPA 攻击的特性.

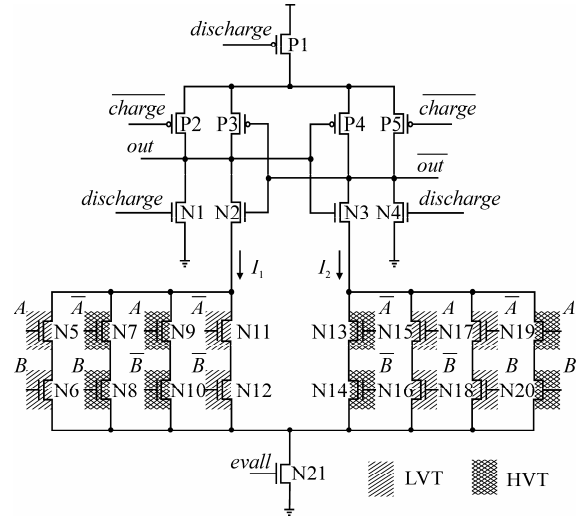


图 1 基于 TVD 的异或门电路

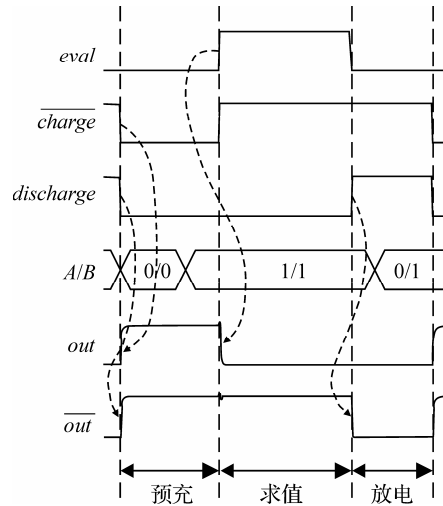


图 2 基于 TVD 的异或门电路工作时序图

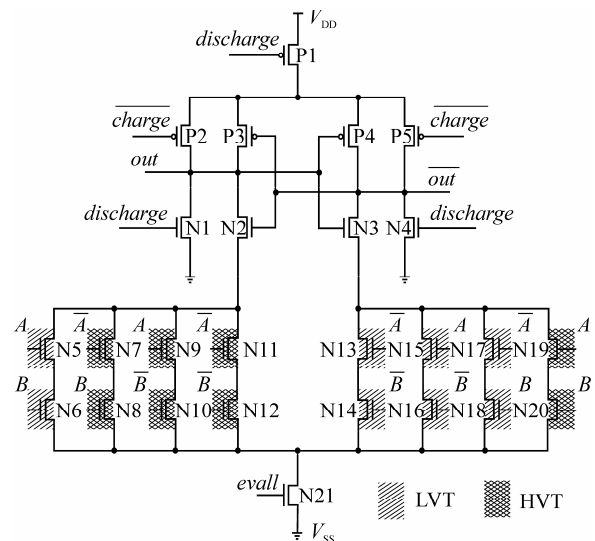


图 3 基于 TVD 的与非门电路

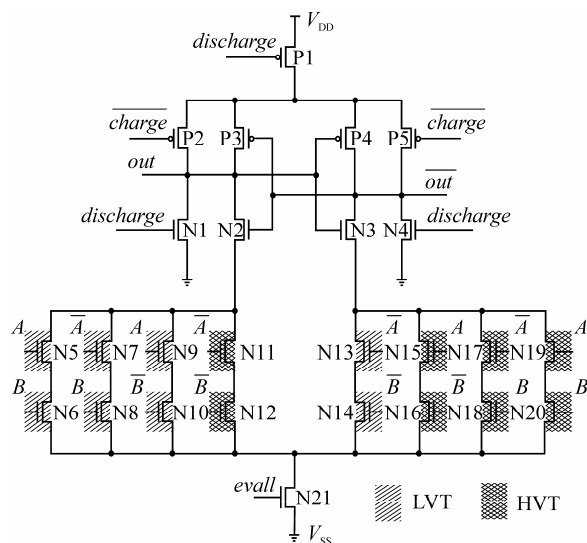


图4 基于TVD的或非门电路

2 实验结果与分析

设计基于TVD的逻辑混淆电路采用TSMC 65 nm CMOS工艺, 由Cadence spectre工具进行瞬态仿真, 并遍历所有激励。仿真波形如图5所示, 结果表明该电路逻辑功能正确。对单周期内电源电流曲线仿真分析(图6), 在3个工作阶段分别产生3个尖峰脉冲, 其中, 预充阶段产生的电流最大, 其产生的功耗也最大, 求值最小。将所设计的基于TVD的逻辑混淆电路与静态门电路进行比较, 以

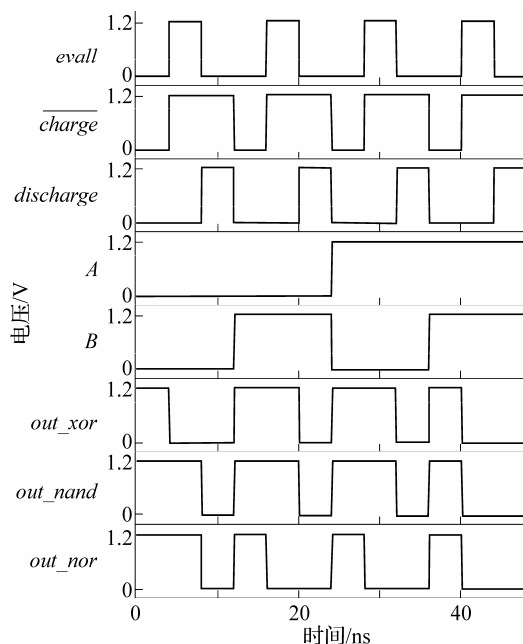


图5 基于TVD的逻辑混淆电路仿真波形

多个时钟周期内电路功耗的差异来表征电路的抗DPA攻击性能。以异或门电路为例, 从图7和图8可知, 静态异或门的功耗依赖输入信号, 输入信号不同会产生不同的功耗。而本文设计的基于TVD的逻辑混淆电路无论输入信号如何, 在多个时钟周期内, 功耗曲线近乎完全一致, 功耗与输入数据无必然联系, 能够有效抵御DPA攻击。

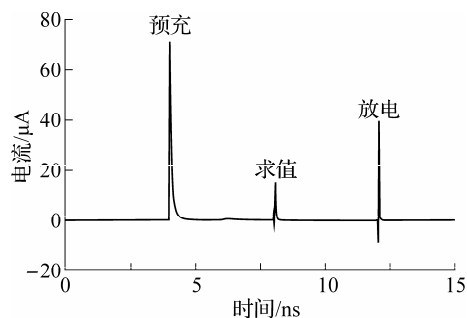


图6 基于TVD的异或逻辑混淆电路电流曲线

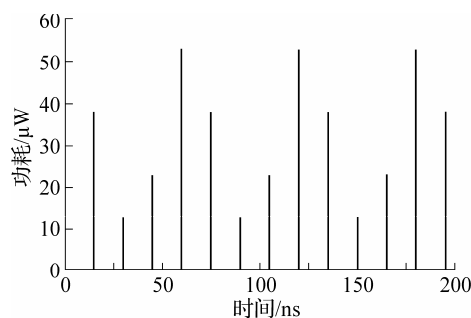


图7 静态异或逻辑电路功耗曲线

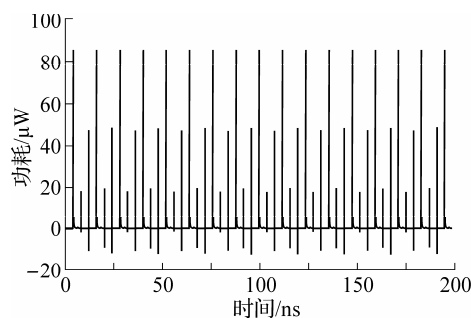


图8 基于TVD的异或逻辑混淆电路功耗曲线

采用全定制方式设计基于TVD的逻辑混淆电路, 异或电路版图如图9所示, 整个版图总共用到

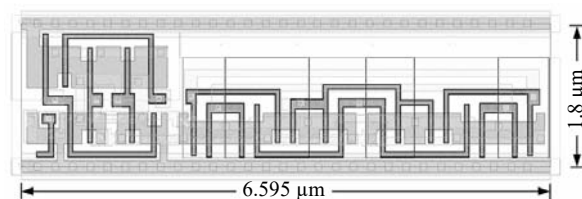


图9 基于TVD的异或逻辑混淆电路版图

表1 基于 TVD 的异或门电路能耗独立性能对比

组别	组合条件	$E_{\max}/\text{fJ}$	$E_{\min}/\text{fJ}$	$\Delta E/\text{fJ}$	$\bar{E}/\text{fJ}$	σ_E/fJ	NED/%	NSD/%
本文	TYP	10.631 4	10.627 7	0.003 7	10.629 6	0.001 3	0.034 8	0.012 4
	BCF	12.861 9	12.858 1	0.003 8	12.860 3	0.001 4	0.029 5	0.010 7
	WCS	8.858 6	8.849 1	0.009 5	8.856 0	0.004 0	0.107 2	0.045 3
	TL	11.648 2	11.645 3	0.002 9	11.646 5	0.001 1	0.024 9	0.009 4
	ML	15.941 8	15.936 1	0.005 7	15.939 6	0.002 1	0.035 8	0.013 4
DDPL ^[12]	TYP	4.007 0	3.986 0	0.021 0	3.996 0	0.008 0	0.500 0	0.200 0
SDML ^[13]	TYP	0.442 8	0.297 8	0.144 9	0.413 3	0.083 1	32.740 0	20.120 0
ST	TYP	0.001 9	0.001 0	0.000 9	0.001 6	0.000 4	47.108 6	21.804 6

2 层金属(M1 和 M2)布线. 通过最小化尺寸、版图对称性、源漏共用和电源共享等技术实现版图面积最小化. 最终, 所设计的基于 TVD 的逻辑混淆电路版图面积为 $6.595 \mu\text{m} \times 1.8 \mu\text{m}$.

通常采用归一化能量偏差(Normalized Energy Deviation, NED)和归一化标准差(Normalized Standard Deviation, NSD)来衡量评估数据与能耗间的依赖性^[11], 其定义为如下(1)式和(2)式:

$$N_{\text{NED}} = \frac{E_{\max} - E_{\min}}{E_{\max}}, \quad (1)$$

$$N_{\text{NSD}} = \frac{\sigma_E}{E}, \quad (2)$$

其中, E 为电路在 1 个时钟周期内消耗的能量, 定义如下:

$$E = V_{\text{DD}} \int_0^T I_{\text{DD}}(t) dt, \quad (3)$$

$E_{\max}$ 和 $E_{\min}$ 分别为多个时钟周期内电路能耗的最大值及最小值; $\bar{E}$ 为多个时钟周期电路的平均能耗, 定义如下:

$$\bar{E} = \left(\sum_{i=E_1}^{E_n} E_i \right) / n, \quad (4)$$

其中, σ_E 为多个时钟周期电路能耗之间的标准方差, 定义如下:

$$\sigma_E = \sqrt{\sum_{i=E_1}^{E_n} (E_i - \bar{E})^2 / n}. \quad (5)$$

表 1 给出了基于 TVD 的异或门电路与其他电路结构的异或门能耗独立性能对比. 为使仿真分析结果更接近芯片实际的工作环境, 需要考虑工艺偏差、电压波动及温度变化对电路性能的影响, 测试 5 种典型 PVT(Process, Voltage, Temperature)组合条件, 仿真环境如下: (1) TYP(Typical): TT 工

艺角, 工作电压与标准电压一致, 设置为 1.2 V, 环境温度 25 °C; (2) BCF(Best Case Fast): FF 工艺角, 工作电压比标准电压高 10%, 环境温度 -40 °C; (3) WCS(Worst Case Slow): SS 工艺角, 工作电压比标准电压低 10%, 环境温度 125 °C; (4) TL(Typical Leakage): TT 工艺角, 标准电压, 环境温度 125 °C; (5) ML(Maximal Leakage): FF 工艺角, 工作电压比标准电压高 10%, 环境温度 125 °C. 从表 1 中可知, 在不同 PVT 下, 本文所提出的基于 TVD 的异或逻辑混淆电路的归一化能量偏差均低于 0.107 2%, 归一化标准差均低于 0.045 3%, 相比静态(ST)电路仿真得到的结果, 在归一化能量偏差、归一化标准差分别降低了 47.07%和 21.79%, 具有显著的抗 DPA 攻击性能.

3 结论

逆向工程通过解剖产品还原设计及差分功耗分析采集功耗泄漏信息推测数据信息, 对芯片安全构成了严重的威胁. 本文采用 TDPL 逻辑, 利用阈值电压特性, 提出一种能有效防御逆向工程和 DPA 攻击的逻辑混淆电路设计方案, 使用相同的电路结构实现不同的逻辑功能. 实验结果表明, 基于 TVD 的逻辑混淆电路功能正确, 相比普通静态电路, 能耗独立性能提升了 21.79%, 能防御逆向工程和差分功耗分析的联合攻击. 但逻辑混淆电路通常是以牺牲面积换取其安全性能, 所以在实际应用中必需考虑安全性能与面积的折中以及合适的应用场景, 也将是今后深入研究的重要内容.

参考文献:

- [1] Hector G, Ckristian D, Elkim R. Standard cell camouflage

- method to counter silicon reverse engineering[C]. IEEE International Conference on Consumer Electronics, 2018: 1-4.
- [2] Muhammad Y, Ozgur S, Jeyavijayan R. 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.
- [3] Arunkumar V, Vinay C P, Daniel E H, 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.
- [4] Dofe J, Yu Q Y. 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.
- [5] Qu M, Chang Y C. Irradiation side-channel attack on cryptographic chip[C]. International Conference on Integrated Circuits and Microsystems, 2016:41-45.
- [6] Xie J, Sun W, Gu D, et al. Research on differential power analysis of HMAC-SM3[C]. International Conference on Computer Science and Intelligent Communication, 2015: 103-106.
- [7] Morrison M A, Ranganathan N, Ligatti J. Design of adiabatic dynamic differential logic for DPA-Resistant secure integrated circuits[J]. IEEE Transactions on Very Large Scale Integration Systems, 2015, 23(8):1381-1389.
- [8] 夏璐. 基于 LBDL 逻辑的抗 DPA 攻击安全芯片的设计与实现[D]. 长沙: 国防科学技术大学, 2012.
- [9] 钱浩宇, 汪鹏君, 张跃军, 等. 基于 SABL 的抗 DPA 攻击可重构加法器设计[J]. 华东理工大学学报(自然科学版), 2017, 43(1):97-104.
- [10] Nail E C A, Burak E, Ken M. A secure camouflaged logic family using post-manufacturing programming with a 3.6 GHz adder prototype in 65 nm CMOS at 1 V nominal VDD[C]. IEEE International Solid-State Circuits Conference, 2018:128-130.
- [11] Abdi O, Jahanian A. A new nano-scale differential logic style for power analysis attack[C]. IEEE Conference on Electrical Engineering, 2015:584-588.
- [12] Marco B, Luca G, Raimondo L, et al. Delay-based dual-rail precharge logic[J]. IEEE Transactions on Very Large Scale Integration Systems, 2011, 19(7):1147-1153.
- [13] Bharath L N, Kumar G. A novel countermeasure for power attacks[C]. IEEE Engineering and Systems, 2013: 1-4.

Design and performance analysis of logic obfuscation circuit based on TVD

LI Li-wei¹, WANG Peng-jun^{1,2*}, ZHANG Yue-jun^{1,3}

(1.Institute of Circuits and Systems, Ningbo University, Ningbo 315211, China;

2.College of Mathematics, Physics and Electronic Information Engineering, Wenzhou University, Wenzhou 325035, China;

3.State Key Laboratory of Cryptology, Beijing 100878, China)

Abstract: Reverse engineering and DPA (Differential Power Analysis) are the common techniques for stealing IP (Intellectual Property) information. By investigating the logic obfuscation circuit and the relationship between data and power, a scheme of the logic obfuscation circuit is proposed using TDPL (Three-phase Dual-rail Pre-charge Logic) and TVD (Threshold Voltage Defined) characteristics, which can prevent reverse engineering and DPA attacks. This scheme utilizes a symmetric differential pull-down network and a sense amplifier, the same circuit structure is used to achieve different logic functions through the configuration of threshold voltages. Spectra simulation results show that the logic obfuscation circuit based on TVD is designed with the correct logic function. Under various PVT tests, the normalized energy deviation and standard deviation are lower than 0.107 2% and 0.045 3%, respectively. Compared with the common static circuits, the proposed design achieves 21.79% higher in power independent performance, which is capable of defending against reverse engineering and DPA.

Key words: logic obfuscation; threshold voltage defined; reverse engineering; differential power analysis

(责任编辑 章踐立)