

一种抗物理攻击防篡改检测技术

张 赞¹, 赵毅强¹, 刘军伟^{1,2}, 李雪民¹, 杨 松¹

(1 天津大学 电子信息工程学院, 天津 300072;

2 信息工程大学 密码工程学院, 河南 郑州 450002)

摘 要: 提出一种应用于高安全芯片的抗侵入式物理攻击防篡改检测技术, 利用芯片顶层金属对侵入式攻击进行主动实时监测, 可有效地防止侵入式攻击对电路存储关键信息的提取. 提出了针对大规模电路的随机哈密顿回路版图优化加速生成算法, 能够在较短时间内生成高无序、大格点量的拓扑结构. 本方法可增加攻击者实施侵入式攻击所需的时间与成本, 提升大尺寸高安全芯片的物理防护能力.

关键词: 信息安全; 物理攻击; 屏蔽探测层; 随机哈密顿回路; 信息熵

中图分类号: TN492

文献标识码: A

文章编号: 1000-7180(2016)04-0121-04

A Temper-Resistant Detecting Technique Against Physical Attack

ZHANG Yun¹, ZHAO Yi-qiang¹, LIU Jun-wei^{1,2}, LI Xue-min¹, YANG Song¹

(1 School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China;

2 School of Cryptography Engineering, Information Engineering University, Zhengzhou 452400, China)

Abstract: A temper resistant detecting technique applied in high security chips is proposed in this paper. The method utilize the topmost layer to monitor attack behaviors in real time, which prevents the key information stored in circuits from being stolen. An optimized algorithm for generating a random hamilton path of the layout in VLSI circuits is proposed. Using this algorithm, a highly disordered topology with a large area can be generated in a short time. The proposed method can increase the time and cost for the invasive attacks and improve the physical defense ability.

Key words: information security; physical attack; shield; random hamilton path; entrop

1 引言

近年来, 超大规模集成电路(VLSI)、片上系统(SoC)及专用芯片(ASIC)在国民经济各领域得到了广泛的应用. 在医疗信息、生物识别等民用领域, 以及金融、军事等关键领域, 对高可靠数据安全芯片的需求在快速增长. 基于芯片级的硬件防护技术因具有可抗底层物理攻击等高安全优势, 与传统的软件加密防护技术互为补充, 正成为信息安全市场发展的主流趋势^[1].

专用集成电路中多包含有 EEPROM、FLASH 等非易失性存储单元, 用于存储程序、数据等关键信息. 目前, 针对系统芯片内存储数据, 已有微探针、聚

焦离子束(FIB)等多种侵入式、半侵入式的攻击方式被公开^[2]. 利用这些技术, 攻击者对电路结构进行修改, 进而探测、反向提取芯片内存储模块内的关键信息.

本文提出了一种应用于高安全芯片的防篡改屏蔽探测层及对应的版图生成算法, 其版图拓扑结构具有高复杂度的特点. 本方法适用于 SoC 等大规模专用芯片, 能够大幅地增加实施物理攻击所需的时间与成本, 有效地保护存储模块内的数据.

2 防篡改顶层金属防护技术

针对微探针、FIB 等侵入式物理攻击, 使用金属屏蔽探测层是芯片级物理防护主要的方式之一. 其

主要目的有以下两点:(1)通过使用一层或多层顶层金属布线,遮蔽芯片下方的物理架构,隐藏存储器模块等关键组件.同时,采用非常复杂的图形拓扑结构,极大的增加反向编译的时间与成本,起到版图迷惑的作用.(2)利用顶层金属屏蔽层作为传感网络层,通过判定传感层的异常态来检测物理攻击,当物理攻击被确定后,触发数据的积极式销毁,保证系统内存数据的安全.

传统的屏蔽探测防护技术可分为被动式和主动式两类^[3].如文献[4],被动式指的是通过使用信号放大调理电路来被动探测内嵌特定结构的电容值等电学参数的变化,进而判定物理攻击.然而,被动式防护判定电路结构复杂、成本较高,同时容易受到制造工艺偏差和使用环境的影响.更为重要的是,检测面积小、技术的通用性较低,并不适合超大规模电路的物理防护.针对此问题,主动式防护使用芯片顶层金属作为防护层,采用向传感网络层注入流密码的方式进行防护,通过信号的等效性检查来判定防护层的开路、断路进而检测物理攻击,如图1所示.检测电路可由全数字实现,技术的可移植性强,噪声容限与鲁棒性高,拓扑结构不受限,因而适用于 SoC 等大规模系统级芯片的物理防护.

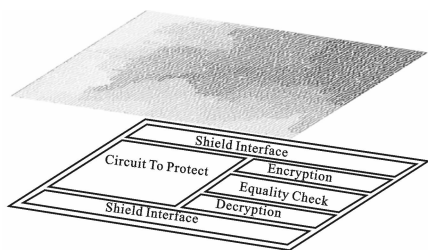


图1 防篡改顶层金属防护系统架构

文献[5-6]提出了采用随机哈密顿回路作为顶层金属防护层的思想,增加了反向编译的难度.由于生成哈密顿回路的过程是完全随机的,即使攻击者完全知晓版图生成的过程,依然无法获取任何的版图信息,具有很高的安全性.最后,相同规格的防护层有数量庞大的拓扑同构与变体,芯片的不同加工批次可使用完全不同的防护层结构,可进一步提高安全性,降低信息泄露的风险.

根据以上分析,本文所提出的顶层金属防护层具有以下特征:

(1)屏蔽层具有较大尺寸,能够遮蔽下方系统全部组件,防止对如总线扩展区域的微探针攻击;

(2)传感检测网络的版图拓扑结构具有很高的复杂度,对其进行反向编译十分困难;

(3)检测电路全数字化,具有较高容限,不受加工工艺偏差、使用环境和拓扑结构变化带来的影响;

(4)探测层传输的探测信号采用多通道,时序复杂,重复率低;

(5)使用最顶层金属,占用较少的布线资源,与标准加工工艺相兼容,能够通过金属密度检查和天线效应检查等制造工艺限制.

3 实现方法

3.1 算法复杂度分析

通过使用合适的算法,在较短的时间内求解出具有较高无序度、同时满足芯片面积要求的随机哈密顿回路拓扑结构是超大规模电路应用本技术的关键.文献[5-6]提出了一种有效的循环合并算法(Cycle Merging, CM),能够求解矩形格点的哈密顿回路生成问题.虽然本问题拓扑结构的生成求解过程实际并不需要解出最短路径,得到任意一条可行路径即可,但是由于求解任意无向图的旅行商问题(Traveling Salesman Problem, TSP)已被证明为 NP 完备问题,这意味着不能用任何已知的多项式算法对其求解,随着求解规模的不断增大,必定会遇到组合型爆炸问题.

对 CM 算法分析可知,由于需要合并的哈密顿图形数量、决断次数均随图形尺寸呈指数型增长,合并操作命中概率将大幅降低,并会造成大量的无效寻址与失败决断.其算法复杂度可由算法主体合并行为的执行量来评价.对于一个边长为 n 的正方形求解,最高算法复杂度为:

$$T_{CM}(n) = \frac{1}{2}n^4 + \frac{3}{2}n^2, O(n^4) \quad (1)$$

文献[5]在 4 h 的时间内,能成功求解约 3×10^5 格点数的哈密顿回路生成问题.但是,对于 VLSI,这样的求解速率不能满足芯片整体全遮蔽的需要.以 Chrt0.18 μm 工艺为例,其顶层金属为 MET-AL6,其设计规则检查(Design rules check, DRC)规定最小线宽、线间距均为 1.5 μm .若要实现单掩膜版(3 cm $\times$ 3 cm)芯片的全保护,其总格点数达到了 10^8 数量级.因此,针对超大规模电路的屏蔽层生成算法必须进行针对性的优化.

针对此问题,有多种优化思想可用来提升求解速度.首先是动态规划算法(Dynamic programming, DP),将问题剥离为若干个相互不独立的子问题,以上次求解的结果作为下次问题的输入,由内向外逐次求解,以实现一定的聚类效果,在一定程度上

降低了算法的复杂度. 同样对于边长为 n 的正方形, 其算法复杂度为:

$$T_{DP}(n) = \frac{2}{3}n^3 - \frac{1}{2}n^2 + \frac{5}{6}n - 1, O(n^3) \quad (2)$$

其次, 当版图规模十分庞大时, 可利用分治算法对求解过程进行优化. 将待求解问题逐级分割为若干个相互独立、规模较小的子问题, 直至问题可被直接求解. 其中, 均分切割的计算量下降最快, 聚类效果明显. 对矩形进行四等分切割, 其算法复杂度为:

$$T_{D\&C}(n) = \frac{4}{5}n^{\log_2 5}, O(n^{2.32}) \quad (3)$$

最后, 考虑到随着图形规模的增长, 版图结构的无序度呈对数型增加. 当拓扑结构的无序度达到安全芯片物理防护的要求后, 为了求解极大规模的防护层版图生成问题, 可利用随机重复单元的嵌套进一步加快求解速度. 其算法复杂度为:

$$T_{D\&C_rep}(n) = 4 \cdot \log_2 n - 4, O(\log_2 n) \quad (4)$$

在 LinuxTM 4.1.2、XeonTM X5690 的环境下对上述优化方式进行了实现与仿真, 其仿真结果如图2所示. 结果显示, 优化算法实现了聚类效果, 可明显加快版图生成速度.

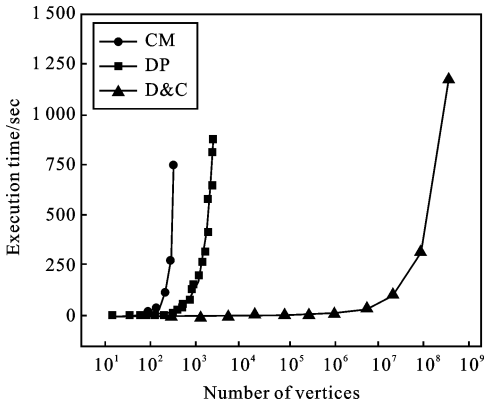


图2 优化算法执行时间

3.2 算法实现

根据以上分析, 提出的优化版图生成算法如下:
输入: 边长格点数最小值 L_c 、期望的无序度信息熵最小值 η ($0 \leq \eta \leq 1$)

输出: 哈密顿回路拓扑结构

步骤1: 格点初始化 $L_0 \times L_0$ ($4 \leq L_0 \leq L_c, L_0 \in \mathbb{Z}$)

步骤2: 哈密顿回路初始化

$$\text{Ham} = \left[\begin{pmatrix} 2i & 2i+1 & 2i+1 & 2i \\ 2j & 2j & 2j+1 & 2j+1 \end{pmatrix} \dots \right]$$

$$(0 \leq i, j < L_0/2)$$

步骤3: 判定单元初始化

$$\text{Filler} = \text{Filler}_1 \cup \text{Filler}_2$$

$$\text{Filler}_1 = \left[\begin{pmatrix} 2i-1 & 2i-1 & 2i & 2i \\ 2j-2 & 2j-1 & 2j-1 & 2j-2 \end{pmatrix} \dots \right]$$

$$(0 \leq i < L_0/2, 0 \leq j \leq L_0/2)$$

$$\text{Filler}_2 = \left[\begin{pmatrix} i-1 & i-1 & i & i \\ 2j-1 & 2j & 2j & 2j-1 \end{pmatrix} \dots \right]$$

$$(0 \leq i < L_0, 0 \leq j < L_0/2)$$

步骤4: 检查当前图形哈密顿回路条数, 条数唯一则迭代终止执行步骤9; 不唯一执行步骤5

步骤5: 从地址池随机挑选两条不同的哈密顿回路, 执行步骤6

$$\text{Ham}_1 = \text{rand}(\text{Ham}), \text{Ham}_2 = \text{rand}(\text{Ham}),$$

$$\text{Ham}_1 \neq \text{Ham}_2$$

步骤6: 判定单元随机排序, 取随机排序后的第 k 个判定单元

$$\text{Filler_rand} = \text{rand}(\text{Filler}),$$

$$[A, B, C, D] = \text{Filler_rand}_k$$

步骤7: 判定第 k 个判定单元与两条哈密顿回路关系

$$\text{Judge} = [A, B, C, D] \text{ismember}[\text{Ham}_1, \text{Ham}_2]$$

如果判定单元4顶点 A, B, C, D 分属两回路

$$\text{Judge} = [1100, 0011] \mid [0110, 1001] \mid$$

$$[0011, 1100] \mid [1001, 0110]$$

且 A, B, C, D 在两回路上分别两两相邻

$$\text{addr}[A-B] = \pm 1 \& \text{addr}[C-D] = \pm 1 \mid$$

$$\text{addr}[B-C] = \pm 1 \& \text{addr}[D-A] = \pm 1$$

则执行步骤8; 若未判定成功 $k = k+1$, 执行步骤6; 若所有判定单元遍历完成, 执行步骤5

步骤8: 以判定成功单元为合并节点将两回路合并为一条哈密顿回路, 执行步骤4

步骤9: 检查拓扑结构无序度信息熵值, $H(C)$

$$= \sum_{d \in \{x, y\}} -P(d) \cdot \log_2 P(d),$$

若 $H(c) < \eta$, 执行步骤11; $H(c) > \eta$, 执行步骤10

步骤10: 检查拓扑结构的格点数,

$L = \text{Length}(c) < L_c$, 执行步骤12, $L > L_c$, 算法结束, 输出图形

步骤11: 重复执行算法开始到当前为止的操作, 得到四条哈密顿回路, 执行步骤13

步骤12: 利用当前哈密顿回路作为重复单元, 得到四条哈密顿回路, 执行步骤13

步骤13: 平移坐标

$$\text{Ham}_2 = \text{Ham}_2 + L \begin{bmatrix} 1 & \dots & 1 \\ 0 & \dots & 0 \end{bmatrix},$$

$$\text{Ham}_3 = \text{Ham}_3 + L \begin{bmatrix} 0 & \cdots & 0 \\ 1 & \cdots & 1 \end{bmatrix},$$

$$\text{Ham}_4 = \text{Ham}_4 + L \begin{bmatrix} 1 & \cdots & 1 \\ 1 & \cdots & 1 \end{bmatrix}$$

步骤 14:定义判定单元,执行步骤 5

$$\text{Filler} = \text{Filler}_3 \cup \text{Filler}_4$$

$$\text{Filler}_3 = \left[\begin{pmatrix} l & l+1 & l+1 & l \\ L & L & L+1 & L+1 \end{pmatrix} \cdots \right]$$

$$(0 \leq l < L, l \in \mathbb{Z})$$

$$\text{Filler}_4 = \text{adiag}(1,1)\text{Filler}_3$$

利用上述算法生成的拓扑结构,在 Cadence™ Virtuoso™视角下最终版图如图 3 所示.

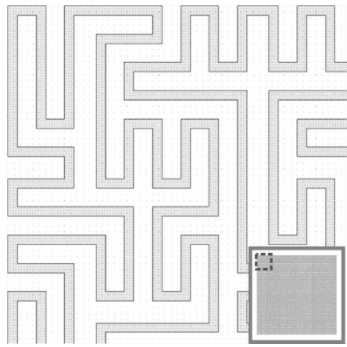


图 3 Cadence™ Virtuoso™下生成的版图

4 结束语

本文介绍了一种应用于大尺寸高安全芯片的抗物理攻击防篡改检测技术.通过优化的版图生成算法,在较短时间内生成高无序、大格点量(10⁹)的随机哈密顿回路结构作为芯片顶层金属屏蔽探测防护层,能够显著提升芯片针对侵入式物理攻击的防护能力.

参考文献:

[1] 冉彤,白国强.基于系统级封装(SiP)的信息安全芯片

集成设计[J].微电子学与计算机,2012,29(1):10-14.

[2] Torrance R, James D. The state-of-the-Art in IC reverse engineering[C]// Cryptographic Hardware and Embedded Systems - CHES9. Berlin Heidelberg, Springer, 2009.

[3] Cioranescu J M, Danger J L, Graba T, et al. Cryptographically secure shields[C]// 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). Arlington, VA, USA: IEEE Computer Society, 2014:25-31.

[4] Shahrjerdi D, Rajendran J, Garg S, et al. Shielding and securing integrated circuits with sensors[C]// Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference on. San Jose, CA, USA: IEEE, 2014:170-174.

[5] Briais, S, Cioranescu, J.-M, Danger, J.-L, et al. Random Active Shield[C]// Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on. Leuven, Belgium;IEEE, 2012: 103-113.

[6] Briais S, Caron S, Cioranescu J M, et al. 3D hardware canaries[C]//Cryptographic Hardware and Embedded Systems - CHES 2012. Berlin Heidelberg, Springer, 2012: 1-22.

作者简介:

张 赟 男,(1991-),硕士研究生.研究方向为集成电路设计.

赵毅强(通讯作者) 男,(1964-),博士,教授,博士生导师.研究方向为集成电路设计. E-mail: yq_zhao@tju.edu.cn

刘军伟 男,(1977-),博士研究生.研究方向为集成电路设计.

李雪民 男,(1990-),硕士研究生.研究方向为集成电路设计.

杨 松 男,(1990-),硕士研究生.研究方向为数字集成电路设计、算法设计.

(上接第 120 页)

[3] 彭石.基于用户兴趣和项目特征的协同过滤推荐算法研究[D].长沙:中南大学,2012:14-18.

[4] 邓爱林,朱扬勇,施伯乐.基于项目评分预测的协同过滤推荐算法[J].软件学报,2003,14(9):1621-1628.

[5] 曾赛.基于社交网络信任模型的项目推荐系统[D].广州:华南理工大学,2012:33-39.

[6] 曹建新,杨宁,夏培勇.一种基于改进信息熵的协同过滤算法[J].微计算机信息,2012,40(10):181-183.

[7] Shapley L S. On market games[J]. Journal of Economic Theory,1969,16(1):9-25.

[8] Roth A E, Sonmez T, Utuuer M. Pairwise kidney exchange[J]. Journal of Economics Theory, 2005, 152 (5):127-132.

作者简介:

顾 凯 男,(1988-),硕士研究生.研究方向为推荐系统. E-mail:gukainjut@126.com.

刘建明 男,(1975-),博士后,教授,博士研究生导师.研究方向为计算机及通信网络组网工程.