DOI:10.3876/j.issn.1000-1980.2019.06.011

故障攻击硬件仿真中低成本电路状态控制方法

刘 强[1,2], 李博超[1,2]

(1.天津大学微电子学院,天津 300072; 2.天津市成像与感知微电子技术重点实验室,天津 300072)

摘要:为了解决基于FPGA的故障注入攻击仿真中,由于使用全扫描方法处理待测电路造成的逻辑资源消耗大的问题,提出一种用部分扫描电路实现电路状态完全可控的方法,即在任何时刻都可以改变电路中所有触发器的值,模拟故障注入攻击,进而在设计阶段对集成电路的安全性进行早期评估。将电路抽象为图,扩展平衡结构部分扫描测试方法,通过扫描触发器选择和触发器使能添加实现对所有触发器的同时控制。采用SAT可满足性算法,基于电路逻辑产生故障测试矢量集,实现故障注入仿真。结果表明,相较于全扫描电路,部分扫描方法以新增少量输入端口为代价,平均减少28.04%的扫描触发器,进而降低故障注入攻击硬件仿真的逻辑资源消耗。

关键词:计算机辅助技术;部分扫描;故障注入攻击;硬件仿真;状态控制;可满足性问题

中图分类号:TP391.7 **文献标志码**:A **文章编号**:1000-1980(2019)06-0555-05

Low-cost state control method for hardware emulation of fault attack

LIU Qiang[1,2], **LI Bochao**[1,2]

(1. *School of Microelectronics*, *Tianjin University*, *Tianjin* 300072, *China*;
2. *Tianjin Key Laboratory of Imaging and Sensing Microelectronic Technology*, *Tianjin University*, *Tianjin* 300072, *China*)

Abstract: In order to reduce the logic overhead caused by the full scan method in the FPGA-based fault injection attack emulation, this study proposes a partial scan based method for the simultaneous control of circuit states, i.e., setting the values of all flip-flops in the circuit at any time, to emulate the fault injection attack. This emulation allows the early security assessment of integrated circuits during the design phase. Meanwhile, the method abstracts the circuit as a graph, extends the balanced-structure based partial scan method to select flip-flops, and then adds enable signals to achieve simultaneous control of all flip-flops. In addition, based on circuit logic, the SAT satisfiability algorithm is used to generate fault test vectors to be injected. The experimental results show that compared with the full scan, the proposed method reduces the number of scanning flip-flops by 28.04% on average, which reduces the logic overhead in the hardware emulation of fault injection attack at the cost of adding a small number of input ports.

Key words: computer aided technology; partial scan; fault injection attack; hardware emulation; state control; satisfiability problem

故障注入攻击已经成为攻击芯片的一种有效方法[1]。因此,在设计阶段评估芯片的抗故障注入攻击能力是十分必要的。现有的抗故障注入攻击评估方法主要包括芯片测试[2-3]、硬件模拟[4-6]和软件仿真[7-8]。Hayashi等[2]使用电磁脉冲、Sondon等[3]使用聚焦离子束投射来诱导芯片内部故障;Evangline等[4]添加多路分配器并使用故障注入信号(FIS)注入故障;Ebrahimi等[5]利用扫描链对触发器注入故障;徐松等[6]使用全扫描方法在FPGA上进行故障注入攻击模拟;He等[7]提出动态软件故障注入模型和方法; Luo等[8]提出了

基金项目:国家自然科学基金(61574099)

作者简介:刘强(1978—),男,副教授,博士,主要从事集成电路抗故障注入攻击研究。E-mail: qiangliu@tju.edu.cn

引用本文:刘强, 李博超. 故障攻击硬件仿真中低成本电路状态控制方法[J]. 河海大学学报(自然科学版),2019,47(6):555-559.
LIU Qiang, LI Bochao. Low-cost state control method for hardware emulation of fault attack[J]. Journal of Hohai University(Natural Sciences),2019,47(6):555-559.

基于程序变异的故障注入思想的软件故障注入模型。在上述方法中,芯片测试发现安全隐患再修改的周期长、成本高,而软件仿真的运算时间长。硬件模拟则可以提供高效且趋近于实际芯片测试的模拟。其中,资源消耗是硬件模拟的关键问题。文献[9]使用全扫描链故障注入,资源消耗平均增比为89.09%。大的硬件消耗会限制待测电路的规模,或者需要使用更大的FPGA芯片,增加仿真成本。

为此,本文提出部分扫描方法实现故障注入,有效减少资源消耗[10-12]。故障注入攻击模拟要求在指定时刻、指定位置注入故障,同时保持其余电路的正常工作状态。部分扫描测试方法[10-11]的目的则是检验电路运行过程中某一点是否存在故障,而不考虑其余电路的正常工作状态问题。因此,已有的部分扫描测试方法无法应用于故障注入估计模拟中。

通过扩展部分扫描测试方法[11],本文提出用于故障注入攻击模拟的电路状态控制方法。该方法通过插入部分扫描链以及D触发器分组使能信号,实现对待测电路状态的控制。扫描触发器的选取由平衡结构[11]和限制因素决定;分组使能通过D触发器分组,并使用可满足性(Satisfiablity,SAT)检测工具求解组内全部状态,确保组内D触发器的同时可控制。

1 基于部分扫描的故障注入流程

基于FPGA的故障注入攻击硬件平台,允许设计者在设计阶段对电路的抗故障注入攻击能力进行早期评估[8,13-14]。通过插入扫描链及控制模块实现故障注入。该方法将电路中部分D触发器变为扫描触发器,实现电路状态完全的可控性,在任意时刻向电路中任意寄存器注入故障。控制模块处理测试向量,控制电路的运行过程。

故障注入仿真流程如下:(a)综合待测电路生成网表文件;(b)对待控制D触发器分组,每组添加共用使能端,并将部分D触发器变为扫描触发器,完成待测电路扫描链的插入;(c)生成测试向量,并利用使能端分别对各组进行分时控制,实现故障注入。

2 基于部分扫描的电路状态控制方法

基于部分扫描的电路状态控制方法是在保证对电路内触发器实现同时控制的情况下,减少扫描触发器的数量。该方法主要包括以下3个步骤:

a. 将待测电路的网表转换为S图[11]。选择部分触发器变为扫描触发器,使电路转化为平衡结构。然后,选择部分扫描触发器,使得每个D触发器(DFF)的前一级为基本输入(PI)或扫描触发器(SFF)。

b. 将具有相同输入的DFF定义为关联触发器。获取S图中所有关联触发器,生成具有DFF节点关联信息的触发器关联图。由关联图,将触发器进行分组,每组触发器共用使能端。根据DFF的关联性,组内分割为子图。

c. 对组内每个子图的逻辑进行可满足性(SAT)检测,确保该子图的节点同时可控,生成测试向量集。若不满足,则重新分组。

2.1 部分扫描触发器选择

部分扫描触发器选择通过以下2个步骤完成。

a. 预处理网表中DFF,选取扇入较大的DFF变为SFF。预处理有两个目的。第一,大幅度降低后续SAT检测中布尔表达式生成的时间。在SAT测试文件生成过程中,随着DFF扇入的增加,布尔表达式项数将呈指数型增长。第二,在应用于大电路时,降低生成平衡结构电路算法运算时间。在平衡电路的过程中,寻找电路环路和寻找不相等路径算法的复杂度与DFF个数成平方关系[10]。预处理后,基于文献[11]的方法,将待测电路的部分DFF变为SFF,使电路变为平衡结构。图1是一个时序电路。其中,PI表示电路的基本输入,PO表示电路的基本输出,A、B、C、D、E、F表示DFF。平衡过程将D触发器E变为SFF,平衡后电路的S图如图2所示。

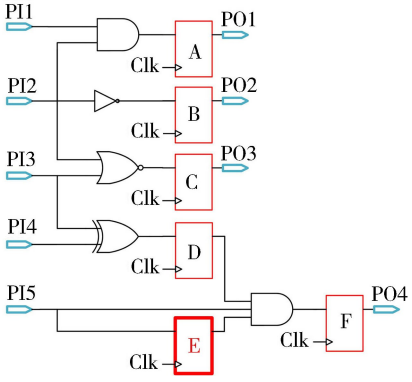

图1 时序电路

Fig. 1 Sequential circuit

b. 为了简化故障注入攻击模拟，要求 S 图中每个 DFF 的前一节点必定是可以控制的 PI 或者 SFF。首先，对 DFF 定级。将 S 图中零扇入的节点定为 0 级，其余节点根据其输入节点中的最大级数递增。其次，将偶数级节点对应的 DFF 变为 SFF，与前级节点断开。对处理后的电路 S 图进行判断，是否存在 DFF 节点的前级仍为 DFF 节点。若是，则进行迭代，重新定级；否则处理结束，返回 DFF 列表与控制节点列表。根据上述定级方法，图 2 中，PI1、PI2、PI3、PI4、PI5、SFF 定级为 0，A、B、C、D 定级为 1，F 定级为 2。故选择 D 触发器 F 变为 SFF。

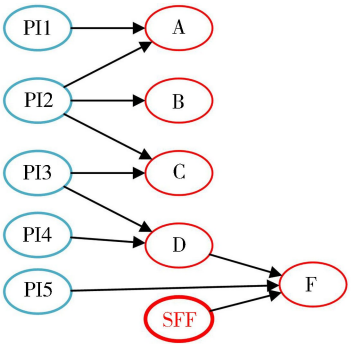

图 2　电路平衡结构 S 图

Fig. 2　Sequential graph of the circuit balanced structure

由于多个 DFF 节点会有相同的前级控制节点（PI 或 SFF），导致这些 DFF 的状态无法同时控制。所以，本文将 DFF 分组并添加使能端，实现分时控制。

2.2　使能添加

在添加使能之前，提取 DFF 节点的关联图。首先将 DFF 列表中每个 DFF 节点及其前级节点存入字典 X。图 2（触发器 F 已变为 SFF）中得到的字典 X 为｛A：［PI1，PI2］，B：［PI2］，C：［PI2，PI3］，D：［PI3，PI4］｝。然后，在字典 X 中对比每个 DFF 的前级节点列表。如果出现相同前级节点，则在节点关联图中添加连接关系。由图 2 得到的关联图为｛A：［B，C］，B：［A，C］，C：［A，B，D］，D：［C］｝，如图 3 所示，节点表示 DFF，边表示 DFF 之间具有共同输入。

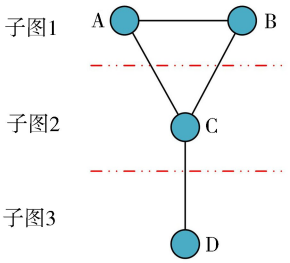

图 3　节点关联图

Fig. 3　Node correlation graph

在极端情况下，关联的每个 DFF 添加一个使能端，实现分时控制。但是，这会增加过多的使能信号，增加布线的难度。为了减少使能端，本文采取了 DFF 分组的方法。首先，对于与其他 DFF 均无关联的触发器节点，分组处理过程中无需考虑。分组完成后将该类触发器节点归于任意组内。其次，对触发器关联图中一组具有相同输入的 DFF 集合（在关联图中由边连接在一起的 DFF 集合），即初始子图，进行 SAT 检测，如果不满足，则分割子图生成新的分组。最后，对新生成分组和子图再次进行 SAT 检测，迭代上述过程，直到全部子图满足 SAT 检测。

子图分割流程如图 4 所示。第一步，先对子图内节点的两两关联性进行判断。选取子图内关联节点最多的节点，以该节点为起点继续迭代，在其关联节点列表中选取关联节点最多的节点。获取两两关联 DFF 节点列表 L_r。如果列表 L_r 长度达到既定阈值（原子图内节点数量的 50%），则将 L_r 列表中的触发器均分为 2 个子图。其余节点放入第 3 个子图，并将生成的 3 个子图分别置于 3 个组中。对于子图内有两两关联的情况，均分置于两组是最优解，可以快速将两两关联的 DFF 节点集划分为较小的子图。

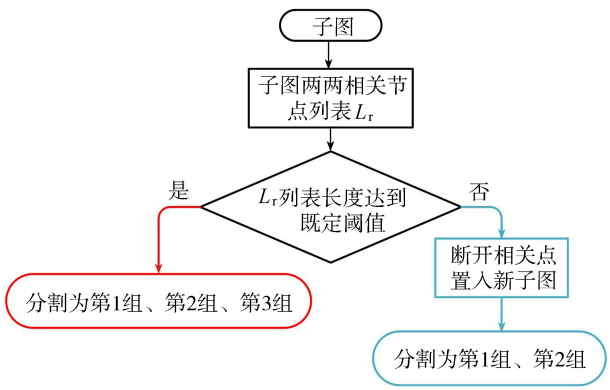

图 4　子图分割流程

Fig. 4　Subgraph segmentation process

第二步，如果不存在上述情况，则在子图内选取关联节点最少的 DFF 节点。将该点作为第一个子图，以该点为起点，找出下一组关联点集合，作为下一个子图。迭代求解直到原子图内的所有 DFF 节点划分完成。将得到的子图按照顺序间隔地放入 3 个组。这种方法保证了组内的子图中各个节点是不关联的，可以共用使能信号进行控制。通过组内分隔多个子图，减少分组数量，意味着使用更少的使能端。同时，通过限制子图内 DFF 节点数量，有利于实现对这些节点的可控性。将图 2 的 S 图根据本节中介绍的方法，提取为触发器关联图，如图 3 所示，并使用本节方法对该子图进行分割。根据本节方法，该子图被分为 3 个子图并置于 2 个组内，分组为［子图 1，子图 3］，［子图 2］。图 1 电路中的 DFF，E、F 已被归入扫描链，A、B、D 共用使能端，C 用一个使能端。通过扫描链及基本输入，分别控制分组［A、B、D］以及分组［C］的触发器状态，实现对

两组的分时控制。

2.4 子图状态可控性检测方法

通过获取子图的每个节点的布尔表达式,组成布尔表达式检测集,并用合取范式(CNF)文件描述,最后使用SAT求解器[15]求解CNF文件。如果解存在,则说明该子图中所有DFF可以同时控制。(a)对于电路S图中的每个待控制触发器节点,以及该节点前级控制节点,根据网表信息获得之间的组合逻辑关系。(b)对于所有控制节点的状态组合,调用逻辑分析函数,得到对应控制节点状态组合的该节点值。逻辑分析函数可处理的器件单元包括DFF,LUT,MUX,INV。该函数对不同的器件单元分类处理:若单元类型为DFF,则将输入直接赋给输出端口;若单元类型为LUT,则根据输入在初始化值init中寻到对应位的值赋给输出端口;若单元为MUX,则通过输入端口S选择输入端口赋值给输出端口;若单元为INV,则将输入端口值取反赋给输出端口。(c)根据输入节点的一种状态组合生成布尔表达式的一项。由于SAT求解器只能求解状态1的布尔表达式。因此,对于每个节点需要生成状态0和状态1的2个布尔表达式。由该节点得到的节点值判断,将该布尔表达式项归入其中一个布尔表达式。(d)在输入节点的全部状态组合都生成布尔表达式项后,获得两个完整的布尔表达式,分别存入状态0和状态1的布尔表达式集合中。子图内所有节点的布尔表达式生成后,获得两个完整的布尔表达式集合。(e)对子图内的所有节点,选定状态组合在布尔表达式集合中取出对应值,生成CNF文件。通过排列组合得到子图内节点的所有状态组合,验证子图内节点的全部状态的同时控制性。

3 实验及结果

本文采用ISCAS基准电路[16]进行实验。使用Synplify Pro工具在Virtex7系列下生成原始网表文件。实验在配有Intel i5-4590 CPU的计算机上运行。

实验中为避免过多分组,在分组-SAT检测迭代过程中,可通过选取未通过SAT的子图中的少量触发器,将其转变为SFF,使得子图通过SAT检测。表1统计了全扫描方法和平衡结构过程的SFF数量,并与本文提出的方法进行对比。结果发现,与全扫描电路相比,本文方法平均节省28.04%的SFF;使能端平均增加6.83个;与文献[11]提出的部分扫描测试方法相比,本文方法平均增加20.17%的SFF。同时,不同的电路结构,SFF数量相较于全扫描降幅与相较于平衡结构增幅各异。其中,电路S5378原始平衡结构SFF较少,本文方法SFF的降幅与增幅都较大;电路S9234的降幅较大,增幅较小,是理想的插入结果;电路S15850较为复杂,平衡结构归入较多SFF,使得本文方法相较全扫描方法降幅减小,同时,SFF相较平衡结构略微下降,表明预先扇入大的触发器简化了电路结构。

表1 扫描触发器插入结果比较

Table 1 Comparison of partial scan results between full scan, BALLAST, and proposed method

电路	全扫描方法SFF数量/个	平衡结构方法SFF数量/个	本文方法			
			SFF数量/个	较全扫描方法节约比/%	较平衡结构方法新增比/%	增加的使能端/组
S1196	18	4	6	66.67	50.00	3
S1238	18	4	7	61.11	75.00	3
S5378	179	84	104	41.90	23.81	4
S9234	211	162	170	19.43	4.94	2
S9234a	211	162	170	19.43	4.94	2
S13207	638	338	420	34.17	24.26	12
S13207a	638	338	420	34.17	24.26	12
S15850	534	468	467	12.55	0	3
S15850a	534	468	467	12.55	0	3
S38417	1 636	1 152	1 396	14.67	21.18	4
S38584	1 426	1 203	1 285	9.89	6.82	17
S38584a	1 426	1 203	1 285	9.89	6.82	17

4 结 语

本文提出了一种使用部分扫描链实现电路状态同时可控的方法,并将其应用于基于FPGA的电路故障注入攻击模拟中。通过选择部分扫描触发器,解决了由于插入扫描链造成的逻辑资源消耗过大的问题,并通

过对 D 触发器节点分组，实现对其完全可控。结果表明，该方法平均减少 28.04% 的扫描触发器，降低了故障注入攻击硬件仿真的逻辑资源消耗，有利于实现更大规模电路的故障注入攻击模拟。

参考文献：

[1] GHALATY N F, YUCE B, TAHA M, et al. Differential fault intensity analysis[C]//Randall Bilof. 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography. Busan: IEEE Computer Society, 2014: 49-58.

[2] HAYASHI Y, HOMMA N, MIZUKI T, et al. Transient IEMI threats for cryptographic devices[J]. IEEE Transactions on Electromagnetic Compatibility, 2013, 55(1): 140-148.

[3] SONDON S, MANDOLESI P, JULIAN P, et al. Heavy-ion micro-beam use for transient fault injection in VLSI circuits[C]// SHIFFLER D, WEBER B. 2014 IEEE 41st International Conference on Plasma Sciences (ICOPS) held with 2014 IEEE International Conference on High-Power Particle Beams (BEAMS). Washington, D. C.: IEEE, 2014: 1-1.

[4] EVANGELINE C, SIVAMANGAI N M. Evaluation of testability of digital circuits by fault injection technique[C]// KARTHIGAIKUMAR P. 2015 2nd International Conference on Electronics and Communication Systems (ICECS). Coimbatore: IEEE, 2015: 92-96.

[5] EBRAHIMI M, MOHAMMADI A, EJLALI A, et al. A fast, flexible, and easy-to-develop FPGA-based fault injection technique [J]. Microelectronics Reliability, 2014, 54(5): 1000-1008.

[6] 徐松, 刘强. 集成电路故障注入攻击仿真方法[J]. 计算机辅助设计与图形学学报, 2017, 29(8): 1563-1569. (XU Song, LIU Qiang. Simulation method for IC fault injection attacks[J]. Journal of Computer-Aided Design & Computer Graphics, 2017, 29(8):1563-1569. (in Chinese))

[7] HE Renya, TANG Longli, WANG Shihai, et al. Software dynamic fault model and injection method[C]//CHEN Wenhua. International Conference on Reliability, Maintainability and Safety(ICRMS). Hangzhou: IEEE, 2016:1-7.

[8] LUO Yin, YAO Rihuang, BIN Jianwei, et al. Research on a software fault Injection model based on program mutation[C]//LI Shaozi, DAI Ying, CHENG Yun. 2015 2nd International Conference on Information Science and Control Engineering. Shanghai: IEEE Computer Society, 2015: 419-423.

[9] 李涛, 刘强. 用于硬件模拟平台调试的低资源消耗扫描链插入方法[J]. 计算机辅助设计与图形学学报, 2016, 28(6): 1008-1015. (LI Tao, LIU Qiang. Resource efficient scan-chain insertion approach for debugging in hardware emulation systems [J]. Journal of Computer-Aided Design & Computer Graphics, 2016, 28(6): 1008-1015. (in Chinese))

[10] WOHL P, WAICUKAUSKI J A, COLBURN J E. Enhancing testability by structured partial scan[C]//Linda Milor. 2012 IEEE 30th VLSI Test Symposium (VTS). Hawaii: IEEE, 2012: 152-157.

[11] LI Tao, LIU Qiang. A low cost partial scan approach based on balanced sequential graph transformation[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37(5): 1109-1113.

[12] LI Tao, LIU Qiang. Cost effective partial scan for hardware emulation[C]//RANDLLl Bilof. 2016 IEEE 24th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM). Washington, D. C.: IEEE Computer Society, 2016: 131-134.

[13] JANNING A, HEYSZL J, STUMPF F, et al. A cost-effective FPGA-based fault simulation environment[C]//LUCA B, SYLVAIN G, ISRAEL K, et al. Workshop on Fault Diagnosis and Tolerance in Cryptography. Tokyo: IEEE, 2011: 21-31.

[14] MOGOLLON J M, GUZMAN-MIRANDA H, NAPOLES J, et al. FTUNSHADES2: a novel platform for early evaluation of robustness against SEE[C]//CUETO Juan. European Conference on Radiation and ITS Effects on Components and Systems. Sevilla: IEEE, 2012: 169-174.

[15] MSOOS. Wonderings of a SAT geek[EB/OL]. [2018-07-11]. https://www.msoos.org/cryptominisat5/.

[16] MICHAEL H. ISCAS89 sequential benchmark circuits[EB/OL]. [2016-04-16]. https://filebox.ece.vt.edu/mhsiao/iscas89.html.

(收稿日期:2018-12-10　编辑:张志琴)