doi:10.3772/j.issn.1002-0470.2020.09.001

基于授权机制的抗扫描旁路攻击方法研究①

卢新元②[*,**,***] 陈华军[****] 许 超[**] 王 剑[***]

([*]计算机体系结构国家重点实验室(中国科学院计算技术研究所) 北京 100190)

([**]中国科学院计算技术研究所 北京 100190)

([***]中国科学院大学 北京 100049)

([****]龙芯中科技术有限公司 北京 100190)

摘 要 研究了针对加密电路的扫描旁路攻击方法和安全扫描设计技术,考虑到现有的安全扫描设计存在故障覆盖率损失或者抵抗攻击性不足的问题,提出一种新的基于授权机制的抗扫描旁路攻击方法。该方法充分利用功能指令序列多样性和高复杂度的特点,通过功能指令序列对测试模式进行授权,将测试模式分为非安全测试模式和安全测试模式。非安全测试模式下,加密电路的密钥被屏蔽,无法通过扫描测试获取。安全测试模式下,加密电路可以进行正常的扫描测试。实验结果表明,采用上述基于授权机制的抗扫描旁路攻击方法的电路后,不仅可以保证安全测试模式下扫描测试故障覆盖率不变,而且非安全测试模式下攻击者无法通过现有的攻击方式获取密钥。同原始电路相比,该方法只需要添加极少的硬件电路,面积开销仅为0.3%。

关键词 扫描旁路攻击;密钥;功能指令;安全测试模式;扫描设计

0 引 言

伴随着现代通信以及网络技术的快速发展,信息安全问题变得尤为重要,通过加密算法加密传输或存储数据成为保证信息安全的重要手段。加密方式通常分为软件加密和硬件加密2种,通常软件加密的方式加密效率较低,因此基于硬件加密的芯片设计成为近些年信息安全领域研究和应用的热点。为有效地检测加密芯片的可靠性,可测试性设计必不可少。扫描设计作为广泛应用的可测性设计方法之一,能够有效提高电路的可控制性和可观测性,保证测试覆盖率。扫描设计能够有效地提高加密芯片可测试能力,但也降低了其安全性。有研究表明,采用数据加密标准(data encryption standard,DES)或改进加密标准(advanced encryption standard,AES)且带有扫描设计的加密芯片都可以被扫描旁路攻击方式[1]获取加密信息。

为保护密码芯片免于扫描旁路攻击,文献[2]提出了基于模式切换复位的保护策略,但在文献[3,4]中该策略被证明对只基于测试模式的攻击方法无效。文献[5]提出了基于线性反馈移位寄存器(linear feedback shift register, LFSR)结构的内建自测试方法,可以有效保障密码芯片的安全,但该方案不利于故障诊断。文献[6]提出了将保存密钥信息的触发器不放在扫描链上的部分扫描设计方法,能有效地防止密钥信息泄露,但会降低加密电路部分的可测试性。文献[7]提出了增加镜像密钥寄存器的方法,测试模式下可以用镜像密钥寄存器将密钥同加密模块隔离,但该方法需要在模式切换时进行系统复位,无法支持在线测试。文献[8]中的安全扫描测试结构为保证测试模式下密钥被屏蔽,只能有一拍捕获时钟,虽然可以支持在线测试,但无法支

① 国家自然科学基金(61521092)和中国科学院重点部署项目(ZDRW-XH-2017-1)资助。

② 男,1994年生,博士生;研究方向:计算机系统结构,芯片验证与测试;联系人,E-mail:luxinyuan@ict.ac.cn

(收稿日期:2019-09-17)

持延迟故障测试。文献[9]中提出了可以支持延迟故障测试的结构设计,但由于测试模式下密钥会被屏蔽,依然存在测试模式下密钥故障无法检测的问题。

不同于上述屏蔽密钥的方法,文献[10-16]提出了另一种保障密码芯片安全的方法,即混淆观测数据。文献[10]通过动态打乱子扫描链顺序的方法实现观测数据混淆,但已被证明可以用签名攻击破解。文献[11,12]提出了在扫描链中添加反相器或异或门的方法,但也被证明可以通过复位攻击等方法破解。文献[13]选择通过添加 LFSR 结构动态改变异或门在扫描链上的位置,该方法可以抵抗现有的扫描旁路攻击方法,但会带来较大的面积开销。文献[14]提出扫描数据加解密的方法,未授权的使用者移出的扫描数据将会被加密,但该方法会增加测试时间。文献[15]提出了静态混淆观测数据的方法,通过添加控制器和一组移位寄存器(shift register,SR)对扫描链上部分触发器的扫描使能进行控制,只有当 SR 中移入正确的测试密钥才能保证被控制的扫描触发器进行正确的移位操作,但该方法可以用测试模式下签名攻击破解。文献[16]提出了动态混淆观测数据的方法,动态改变被选择的扫描触发器,很大程度上增加了攻击的难度,但也无法证明这种动态混淆观测数据的方法是不可逆的。

针对以上方法存在的问题,本文提出一种基于授权机制的抗扫描旁路攻击方法,使用者需要在功能模式下输入预设的功能指令序列进行安全测试权限认证,在获取安全测试授权后,才能在安全测试模式下进行扫描测试。该方法不需要添加用来保存测试密钥的触发器,因此只需要很少量的面积开销,并且不会带来额外的测试时间开销。本文所提出的基于授权机制的抗扫描旁路攻击方法既能够保证无法被现有攻击方法所破解,又可以检测到密钥故障,在保证安全性的同时,不会损失故障覆盖率。

1　背景介绍

1.1　扫描测试原理

基于扫描链的扫描测试是可测试性设计中的一种关键测试方法,能够为芯片提供良好的可控制性和可观测性。扫描链结构如图 1 所示,通过在普通触发器前增加一个选择器的方式,将其串联成一条由多个触发器组成的长链。选择器的 2 个输入,分别来自于扫描输入(scan in,SI)和功能逻辑,并由测试控制(test control,TC)信号控制选择器选择数据输入来源。在测试模式下,首先将 TC 置 1,此时芯片处于移位模式,多拍时钟后将扫描输入值移入链上触发器中。然后将 TC 置 0,芯片从移位模式切换到捕获模式,经过一拍或多拍时钟将功能逻辑值捕获到触发器中。最后再次将 TC 置 1,将链上触发器中的值移出观测[17]。功能模式下,TC 值保持为 0,扫描链上触发器的数据输入来源于功能逻辑。

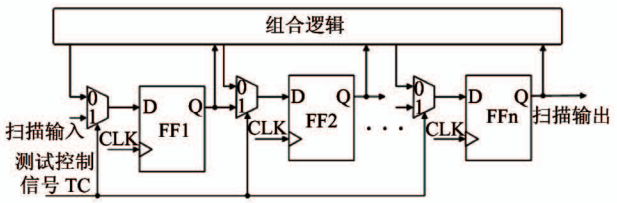


图 1　扫描链结构图

1.2　AES 加密结构

相比于 DES 加密算法,AES 加密算法因安全性较高、迭代对称而被广泛应用。以 AES 加密芯片为例,其加密模块结构如图 2 所示。加密过程中,首先将初始密钥和明文数据送入加密结构中进行第一次的异或操作,再将异或结果送入轮加密逻辑中。轮加密逻辑是 AES 加密结构的核心部件,轮加密逻辑中主要包括 3 个顺序完成的操作,分别是 S 盒、行移位和列混合。列混合完成的数据会同密钥生成器中产生的密钥再进行一次异或操作,并将结果存放在轮触发器中,这个过程称之为一次完整的轮加密操作。之后轮加密逻辑会多次重复上述的轮操作,直至最终加密完成。每一轮的数据都来源于上一轮操作中轮触发器保存的值,每一次轮加密操作中的密钥都由密钥生成器重新产生,并保存在密钥触发器中。根据密钥的长度不同,轮加密的次数也会不同,一般 128 位的密钥设计需要 10 次的轮加密操作,能够抵抗已知所有的数学攻击方法。

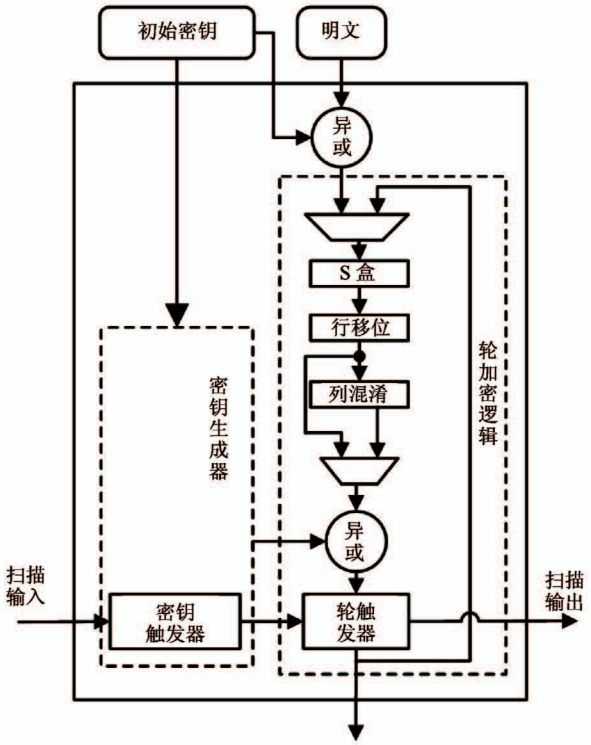


图2　具有扫描链的AES加密模块结构

在AES加密芯片的可测试性设计中为了满足覆盖率的需求,通常需要将存放加密中间状态值的密钥触发器和轮触发器放在扫描链中,本文将密钥触发器和轮触发器统称为加密相关触发器。在功能模式下,芯片可以进行正常的加密操作,加密的中间状态值保存在加密相关触发器中。当由功能模式切换到测试模式后,可以通过扫描链将加密相关触发器的值移出观测。攻击者利用该特性,在功能模式下输入一些特殊的明文,然后在第一次的轮操作完成后切换到测试模式下,将加密相关触发器的中间状态值移出观测,这样攻击者可以很容易获取密钥。

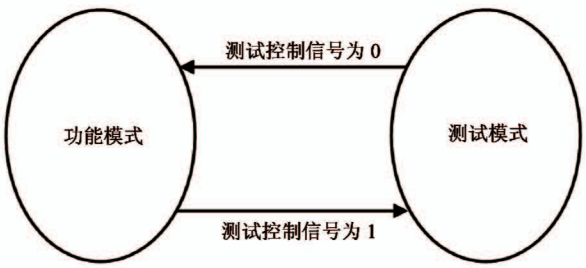
2　基于授权机制的安全扫描设计

2.1　模式切换机制

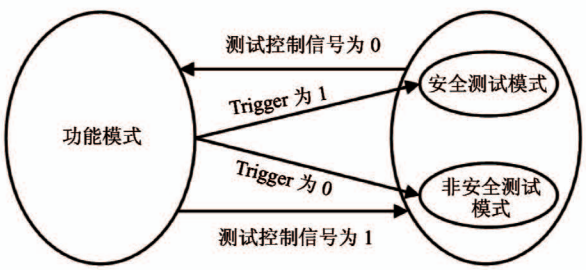
传统的无安全设计的芯片模式切换关系如图3(a)所示。

当系统复位完成后,由测试控制信号TC控制芯片的模式切换。TC为0时,芯片进入功能模式,可以进行正常的加密运算,但无法进行扫描链移位操作。TC为1时,芯片由功能模式切换到测试模式,扫描链可以进行正常的移位和捕获操作,攻击者可通过扫描链将加密相关触发器值直接移出观测,此时芯片处于一种容易被攻击的状态,无法保障密码芯片的安全。

本文提出的改进方法如图3(b)所示,将测试模式分为安全测试模式和非安全测试模式,并增加了一个模式切换信号Trigger。当TC由0跳变到1时,芯片由功能模式切换到测试模式,此时如果Trigger信号为1,则进入安全测试模式;如果Trigger信号为0,则进入非安全测试模式。当TC信号由1跳变为0时,芯片由测试模式回归到正常的功能模式。



(a) 无安全设计的模式切换



(b) 改进的后模式切换

图3　模式切换图

非安全测试模式下,密钥以及加密相关触发器值被屏蔽,测试者只能对其他触发器所在的扫描链进行正常的扫描测试。安全测试模式下,密钥不被屏蔽,加密相关触发器置在扫描链上可以进行正常扫描测试。

2.2　安全扫描设计的结构实现

本文的安全扫描结构设计主要包括测试权限分析模块、测试控制模块以及屏蔽模块,如图4所示。

测试权限分析模块负责在功能模式下对测试权限进行认证,并产生Trigger信号送入测试控制模块中。测试控制模块接收测试控制信号TC以及来自

于测试权限分析模块的 Trigger 信号，控制和实现模式切换，并产生安全测试信号 Secure _ test 送入屏蔽模块中。最终屏蔽模块根据 Secure _ test 的值决定是否对密钥和加密相关触发器进行屏蔽。

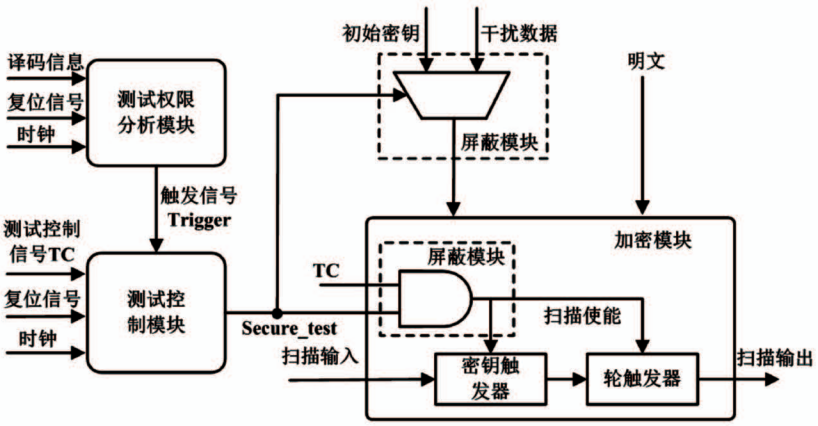


图 4　安全扫描设计结构图

2.2.1　测试权限分析模块

测试权限分析模块主要包括控制器以及测试权限生成模块，其结构如图 5 所示。控制器接收并处理来自于中央处理器（central processing unit，CPU）[18] 的译码信息，该译码信息为使用者输入正确的功能指令序列后 CPU 译码产生特定的信息，随后发出控制信号并送入测试权限生成模块中。测试权限生成模块包括一个有限状态机和一个信号生成器，由控制信号驱动有限状态机工作，当有限状态机到达特定的状态后，触发生成器负责将触发信号 Trigger 置 1，并送入测试控制模块中。每次对系统进行复位后，触发信号 Trigger 会重新置 0。

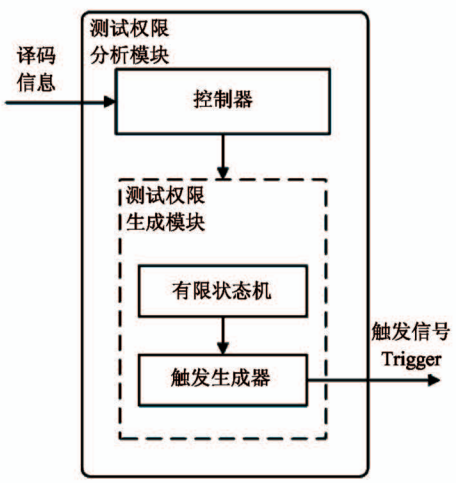


图 5　测试权限分析模块

2.2.2　测试控制模块

测试控制模块在整个过程中起着核心枢纽作用，负责接收 Trigger 信号完成模式切换，并产生 Secure _ test 信号实现对屏蔽模块的控制。测试控制模块由 1 个触发器 FF1、1 个时钟门控 CG、1 个异或门 A1 以及 1 个反相器 I1 组成，其结构如图 6 所示。触发器 FF1 为异步触发器，由复位信号 reset 进行复位。触发器的时钟端连接时钟门控 CG 的输出，CG 的使能端 EN 连接测试控制信号 TC。TC 和触发信号 Trigger 连接异或门 A1 的两输入端，A1 的输出端同触发器 FF1 的 D 端连接。触发器 FF1 的 Q 端与反相器 I1 输入相连，反相器输出安全测试信号 Secure _ test。该测试控制模块如何完成模式切换以及控制屏蔽模块将在下文 3.1 和 3.2 节中进行详细说明。

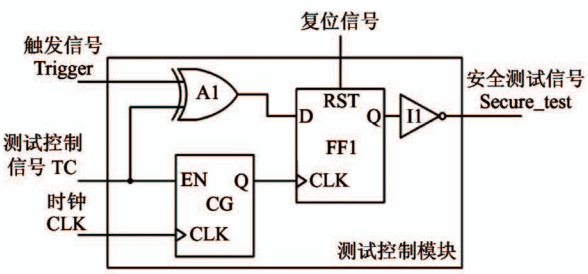


图 6　测试控制模块

2.2.3　屏蔽模块

屏蔽模块包括 2 个部分：密钥屏蔽模块和加密

相关触发器屏蔽模块,其结构如图 4 中虚线框内所示。密钥屏蔽模块中主要由二选一多路选择器构成。干扰数据(干扰数据位宽和密钥位宽一致)和密钥作为选择器的 2 个输入,安全测试信号 Secure _ test 作为选择器的选择信号。当攻击者无法获取安全测试权限时,干扰数据会被送入加密模块中,密钥被屏蔽。

加密相关触发器屏蔽模块主要由一个与门构成,与门的其中一个输入端同安全测试信号 Secure _ test 相连,另一个输入端则连接测试控制信号 TC,并将输出结果作为加密相关触发器的扫描使能信号。该模块可以根据 Secure _ test 的值,选择是否对加密相关触发器扫描链移出值进行屏蔽,因此当使用者没有通过测试权限分析模块的测试权限认证时,无法根据扫描链的观测值恢复密钥。

3 安全扫描设计操作流程

通过实现基于授权机制的安全扫描设计,得到安全扫描操作流程图如图 7 所示。

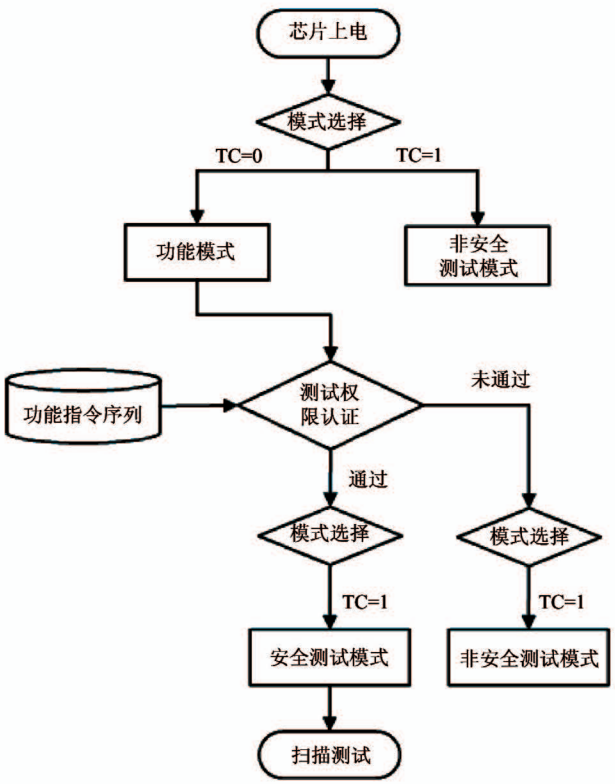


图 7 安全扫描操作流程图

3.1 功能模式操作

芯片完成上电操作进入工作模式后,将 TC 信号置为 0,芯片会进入正常的功能模式。根据图 6 中测试控制模块结构可知,此时测试控制模块中时钟门控 CG 使能 EN 无效,时钟无法通过 CG,触发器 FF1 不能完成时钟沿触发而发生跳变,因此触发器 Q 端输出值保持复位后的值 0,经过反相器 I1 取反后,Secure _ test 值为 1,测试控制模块输出安全测试信号。当屏蔽模块接收到为 1 的 Secure _ test 信号后,密钥屏蔽模块选择将密钥输出并送入到加密模块中。加密相关触发器屏蔽模块输出的扫描使能信号保持不变,加密相关触发器的输入来自于功能逻辑,加密模块可以进行正常的加密运算,并输出密文。注意到当 TC 为 0 时,Secure _ test 的值不受触发信号 Trigger 影响,因此无论是否在功能模式下对安全测试权限认证,功能操作都不受影响。

3.2 测试模式操作

芯片上电后,如果不预先进入功能模式下通过测试权限认证,而将 TC 直接置为 1,则芯片会进入非安全测试模式。或者当芯片在功能模式下,使用者没有进行测试权限认证或认证未通过,则安全测试权限分析模块输出 Trigger 信号为 0。此时,将 TC 信号由 0 置 1,芯片同样会切换到非安全测试模式。非安全测试模式下,TC 为 1,Trigger 为 0,测试控制模块内异或门 A1 输出为 1,并送到触发器 FF1 的 D 端。由于 TC 为 1,则时钟信号可以通过 CG 传递到触发器 FF1 上,当时钟上升沿到来时,触发器 FF1 捕获到值 1,并由 Q 端输出。经过反相器 I1 后,测试控制模块输出安全测试信号 Secure _ test 值为 0。当屏蔽模块接收到为 0 的 Secure _ test 信号,密钥屏蔽模块会将干扰数据作为密钥送入加密模块中。加密相关触发器屏蔽模块输出的扫描使能信号为 0,加密相关触发器无法进行正确的移位操作。因此,攻击者无法通过扫描移出值恢复密钥。

若想进入安全测试模式,需要在功能模式下进行测试权限认证。使用者输入正确的功能指令序列到 CPU 中,安全测试权限分析模块接收到译码信息后,将触发信号 Trigger 置为 1。此时,将 TC 信号由 0 置 1,芯片切换到安全测试模式。安全测试模式

下，TC 为 1，Trigger 也为 1，异或门 A1 输出 0 并送到触发器 FF1 的 D 端。由时钟上升沿触发，触发器捕获 0 值并由 Q 端送入反相器 I1 中，最终测试控制模块输出值为 1 的 Secure _ test 信号。密钥屏蔽模块选择密钥直接送入加密模块中。加密相关触发器屏蔽模块中输出的扫描使能信号与 TC 保持一致。在扫描测试过程中，需要由移位模式切换到捕获模式，TC 信号由 1 置为 0，此时 Secure _ test 值会保持不变。因此，安全测试模式下可以支持正常的扫描测试过程，密钥和加密模块中的故障均可以被检测到。

4　实验结果及分析

本文选取密钥位宽为 128 位的 AES 电路[19]以及龙芯某款 CPU 核作为实验对象进行仿真认证。实验选取的仿真工具为 VCS，综合工具为设计编译器（design compiler，DC）。上述的电子设计自动化（electronics design automation，EDA）工具都在 Linux 环境下运行，服务器的 CPU 主频为2.2 GHz，内存容量为64 GB。实验选择连续 3 条位宽为 32 位的移位指令作为正确的指令序列，输入正确的指令序列后，仿真结果如图 8 所示。图中虚线处为 TC 信号跳变的时刻，跳变前电路处于功能模式，跳变后切换到测试模式。功能模式下，CPU 根据指令 valid 信号接收并处理连续 3 条有效的移位指令，控制译码信号 signa、signb 以及 signc 的值连续发生跳变。信号 state 的值对应测试权限分析模块中状态机的不同状态，其中“0”代表初始状态，“1”代表接收到第 1 条正确的指令，“2”代表接收到前 2 条连续正确的指令，“3”代表接收到完整的指令序列。当状态机达到状态“3”后，在下一拍时钟的上升沿 Trigger 信号跳变为 1，电路由功能模式切换到安全测试模式，Secure _ test 信号保持为 1 不变。

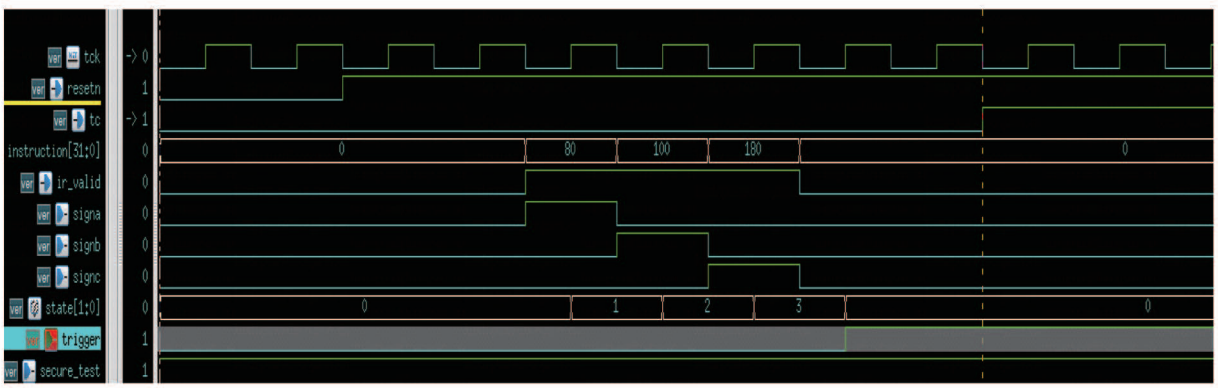


图 8　输入正确功能指令序列的仿真结果

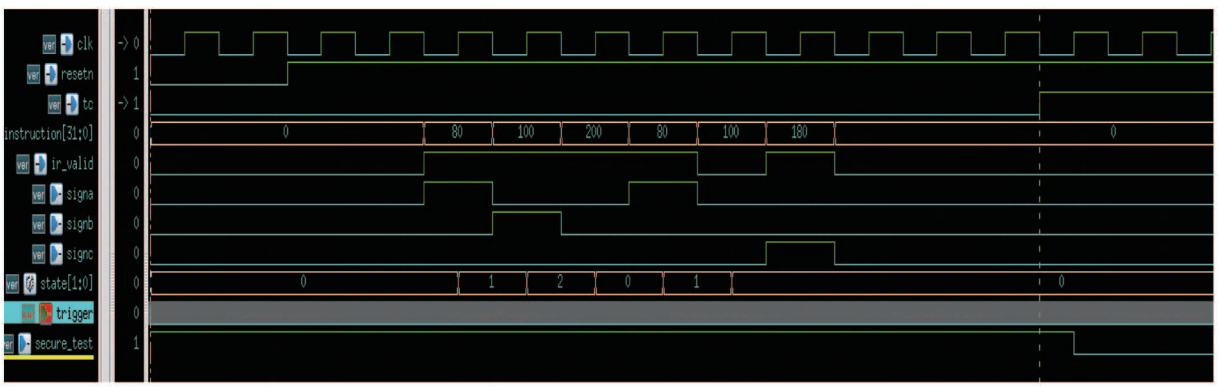


图 9　输入错误功能指令序列的仿真结果

若输入错误的功能指令序列后,其仿真结果如图9所示。指令序列中错误或无效的指令会导致译码信号 signb 和 signc 无法正确跳变。当状态机处于状态“1”或状态“2”时,接收到不正确的指令后均会重新跳转到初始状态“0”,信号 Trigger 保持为0,电路由功能模式只能切换到非安全测试模式,Secure _ test 信号由1跳变为0。

4.1 安全性分析

通常攻击者无法得知在进行密钥获取前,需要进入安全测试模式或如何进入安全测试模式。极端情况下,即便攻击者知道需要在功能模式下输入指令序列来触发安全测试权限分析模块生成 Trigger 信号,攻击者输入一段完全正确的功能指令序列的可能性也几乎为0。当安全测试权限分析模块没有将触发信号 Trigger 信号置为1时,攻击者永远只能由功能模式切换到非安全测试模式。此时,密钥以及加密相关触发器都被屏蔽,攻击者无法根据扫描链移出观测值恢复密钥,因此所有的已知攻击方式都无效。本文所提出的方法同引言中提到的几种经典安全扫描测试方法相比,安全性分析结果如表1所示。其中 k 和 j 分别表示添加反相器[9]方法中扫描触发器以及反相器的个数,L 表示静态混淆数据[12]方法中新增移位触发器的个数,m 表示功能指令序列中指令的个数,n 表示指令的位宽。

表1 不同安全扫描设计的安全性和可测试性对比

安全扫描设计	安全性分析		可测试性分析	
	可攻击方法	暴力攻击复杂度	测试向量及覆盖率影响	测试时间开销
模式切换复位[2]	测试模式攻击	无法暴力攻击	无影响	增加一个时钟周期
镜像密钥寄存器[7]	暂无	无法暴力攻击	无法检测密钥故障	无法在线测试
扫描链顺序扰乱[10]	差分攻击	2^{64}	无影响	增加多个时钟周期
反相器[11]	复位攻击	C_k^j	无影响	无开销
LFSR 混淆[13]	暂无	不确定	无影响	无开销
扫描数据加解密[14]	暂无	不确定	无影响	增加多个时钟周期
静态混淆数据[15]	签名攻击	2^L	无影响	增加 L 个时钟周期
动态混淆数据[16]	暂无	不确定	无影响	增加 L 个时钟周期
本文方法	暂无	$2^{m\times n}$	无影响	无开销

4.2 可测试性分析

当测试工程师可以进入安全测试模式下进行扫描测试时,密钥的值不会被屏蔽,加密相关触发器所在扫描链也可以进行正常移位和捕获操作,密钥以及加密模块的故障均可以被检测到,因此同未进行安全扫描设计的初始芯片相比,并没有故障覆盖率的损失。

由移位模式切换捕获状态时,一拍或者多拍的捕获时钟都不会影响测试控制模块输出的 Secure _ test 值,因此该安全扫描设计方法既支持固定性故障测试,又支持延迟故障测试,而且由于不需要修改扫描链的结构,传统的扫描链设计以及自动测试向量生成流程完全适用,生成的测试向量也不需要进行调整。本文采用的安全扫描设计同其他经典的方法相比,可测试性分析结果如表1所示。除添加反相器[9]和 LFSR 混淆[13]的方法,其他安全扫描设计都需要增加额外的测试时钟周期,但本文所提出的方法无需额外的测试时间开销。

4.3 面积开销分析

本文实验使用 DC 工具基于 130 nm 工艺进行综合和 DFT 设计,生成最终的网表。面积开销、组合单元以及时序单元个数统计如表2所示。其中初始设计是指未进行安全设计的 DFT 后的电路。

实验结果表明,新增的安全扫描结构面积仅约为初始设计面积的0.3%。同初始设计相比,组合单元和时序单元个数分别增加了333个和5个,占比仅为0.18%和0.9%。

表 2 面积开销统计

AES 电路	初始设计面积(nm^2)	改进后面积(nm^2)	新增面积占比	新增组合单元个数	新增组合单元个数占比	新增时序单元个数	新增时序单元个数占比
本文结构	2 264 089	2 271 067	0.3%	349	0.18%	5	0.9%

5 结 论

本文提出的基于授权机制的抗扫描旁路攻击方法,在功能模式下通过功能指令序列完成安全测试授权,并根据授权认证结果选择进入非安全测试模式或安全测试模式。非安全测试模式下,密钥被屏蔽,同时加密相关触发器所在扫描链的移出观测值被混淆,因此攻击者无法恢复密钥,保证了密钥的安全性。安全测试模式下,密钥不被屏蔽,密钥从存储器读出到送入加密模块的路径上故障都可以被扫描测试检测到。同时加密模块中的触发器以及组合逻辑故障也均可以被检测到,保证了加密相关模块的故障覆盖率。另外,通过功能指令序列触发的安全测试权限认证方式,安全性高且不失灵活性。一方面,攻击者在不知道正确功能指令序列的前提下,几乎不可能通过安全测试权限认证。另一方面,设计者可以根据芯片的安全等级,改变指令序列中功能指令的种类以及个数。本方法结构实现简单,并且几乎没有面积开销,可以适用于任何带有扫描设计的密码芯片中。

参考文献

[1] Zhou W, Cui A, Li H, et al. How to secure scan design against scan-based side-channel attacks[C]//Proceedings of the 2017 IEEE Asian Test Symposium, Taibei, China, 2017: 116-121

[2] Hely D, Bancel F, Flottes M L, et al. Test control for secure scan designs[C]//Proceedings of the 2005 IEEE European Test Symposium, Tallinn, Estonia, 2005:190-195

[3] Ali S S, Sinanoglu O, Karri R, et al. Test-mode-only scan attack using the boundary scan chain[C]//Proceedings of the 2014 IEEE European Test Symposium, Paderborn, Germany, 2014: 1-6

[4] Ali S S, Saeed S M, Sinanoglu O, et al. New scan-based attack using only the test mode and an input corruption countermeasure[J]. *IFIP Advances in Information and Communication Technology*, 2015, 461(1):48-68

[5] Mehta A, Saif D, Rashidzadeh R. A hardware security solution against scan-based attacks[C]//Proceedings of the 2016 IEEE International Symposium on Circuits and System, Montreal, Canada, 2016: 1698-1701

[6] Inoue M, Yoneda T, Hasegawa M, et al. Partial scan approach for secret information protection[C]//Proceedings of the 14th IEEE European Test Symposium, Seville, Spain, 2009: 143-148

[7] Yang B, Wu K, Karri R. Secure scan: a design-for-test architecture for crypto chips[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2006,25(10):2287-2293

[8] Cui A, Luo Y, Li H, et al. Why current secure scan designs fail and how to fix them? [J]. *Integration, the VLSI Journal*, 2017, 56:105-114

[9] Ahlawat S, Vaghani D, Singh V. Preventing scan-based side-channel attacks through key masking[C]//Proceedings of the 2017 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Cambridge, UK, 2017: 1-4

[10] Lee J, Tehranipoor M, Patel C, et al. Securing designs against scan-based side-channel attacks[J]. *IEEE Transactions on Dependable and Secure Computing*, 2007, 4(4):325-336

[11] Sengar G, Mukhopadhyay D, Chowdhury D R. Secured flipped scan-chain model for crypto-architecture[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2007, 26(11):2080-2084

[12] Agrawal M, Karmakar S, Saha D, et al. Scan based side channel attacks on stream ciphers and their counter-measures[C]//Proceedings of the 2008 International Conference on Cryptology in India: Progress in Cryptology, Kharagpur, India, 2008: 226-238

[13] Zhang D,He M, Wang X, et al. Dynamically obfuscated scan for protecting IPs against scan-based attacks through-

out supply chain[C]//Proceedings of the 2017 IEEE VLSI Test Symposium, Las Vegas, USA, 2017: 1-6

[14] Silva M D, Flottes M L, Natale G D, et al. Preventing scan attacks on secure circuits through scan chain encryption[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2019, 38(3):538-550

[15] Luo Y, Cui A, Qu G, et al. A new countermeasure against scan-based side-channel attacks[C]//Proceedings of the 2016 IEEE International Symposium on Circuits and Systems, Montreal, Canada, 2016: 1722-1725

[16] Cui A, Luo Y, Chang C H. Static and dynamic obfuscations of scan data against scan-based side-channel attacks [J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(2):363-376

[17] 许超, 陈华军, 郝守青, 等. 基于电路结构的测试捕获功耗优化方法[J]. 高技术通讯, 2019, 29(5):413-422

[18] 胡伟武. 自主 CPU 发展道路及在航天领域应用[J]. 上海航天, 2019, 36(1):5-13

[19] OpenCores. AES: Overview [EB/OL]. http://opencores.org/project, tiny_aes: OpenCores.org, 2014

Research on authorization mechanism against scan-based side-channel attacks

Lu Xinyuan[*,**,***], Chen Huajun[****], Xu Chao[**], Wang Jian[***]

([*]State Key Laboratory of Computer Architecture, Institute of Computer Technology, Chinese Academy of Sciences, Beijing 100190)

([**]Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190)

([***]University of Chinese Academy of Sciences, Beijing 100049)

([****]Loongson Technology Corporation Limited, Beijing 100190)

Abstract

The scan-based attacks and secure scan design are studied, and a new method based on authorization mechanism against scan-based side-channel attacks is proposed to avoid the loss in the fault coverage and being vulnerable to attack existing in current methods. The new method makes full use of the diversity and high complexity of the functional instruction sequence, and authorizes the test mode triggered by the functional instruction sequence. The test mode is divided into non-secure mode and secure mode. In the non-secure mode, the key of the encryption circuit is masked and can not be obtained through the scan test. In the secure mode, the encryption circuit can be scan tested normally. The experimental results show that the fault coverage of the circuits with the proposed method based on authorization mechanism against scan-based side-channel attacks remains unchanged in the secure mode and attackers can not decipher the cipher key through the known scan-based attacks in the non-secure mode. The area increases by only 0.3% compared with the original circuits with adding a few hardware circuits.

Key words: scan-based attack, cipher key, functional instruction, secure mode, scan design