

引用格式:景凤池,张金艺. 抗内存攻击的加密芯片双重动态混淆策略[J]. 微电子学与计算机,2020,37(5):75-81. [JING F C,ZHANG J Y. Anti-memory attack encryption chip dual dynamic obfuscation strategy [J]. Microelectronics & Computer, 2020,37(5):75-81.]

抗内存攻击的加密芯片双重动态混淆策略

景凤池¹,张金艺^{1,2}

(1 上海大学 微电子研究与开发中心,上海 200444;

2 上海大学 特种光纤与光接入网重点实验室,上海 200444)

摘 要: 目前,基于线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)的动态混淆策略和测试授权策略是保护加密芯片免受扫描旁路攻击威胁的主流方法,然而存储在内存中的 LFSR 种子或测试授权密钥极易受到针对内存的攻击。针对此问题,从应对扫描旁路攻击和应对内存攻击两个角度出发,设计双重动态混淆架构并基于此架构构建双重动态混淆策略。其中,构建基于 LFSR 自更新模块的扫描链数据动态混淆策略以应对扫描旁路攻击;构建 LFSR 输出序列动态混淆策略以应对内存攻击。实验表明,相较于目前主流的安全扫描策略,双重动态混淆策略在不影响芯片可测试性的同时,可以使加密芯片免受扫描旁路攻击和内存攻击的威胁;在 LFSR 自更新模块位数为 64 位、插入混淆逻辑门中异或门和同或门数量各为 8 位的情况下,面积开销为 0.31%,攻击人员暴力破解双重动态混淆策略所需应用的测试向量至少为 6.29×10^{18} 个。

关键词: 加密芯片;扫描旁路攻击;内存攻击;动态混淆

中图分类号: TN407

文献标识码: A

文章编号: 1000-7180(2020)05-0075-07

Anti-memory attack encryption chip dual dynamic obfuscation strategy

JING Feng-chi¹,ZHANG Jin-yi^{1,2}

(1 Microelectronic Research and Development Center, Shanghai University, Shanghai 200444, China;

2 Key Laboratory of Special Fiber Optics and Optical Access Networks,

Shanghai University, Shanghai 200444, China)

Abstract: At present, the dynamic obfuscation strategy based on the Linear Feedback Shift Register (LFSR) and the test authorization strategy are the mainstream methods to protect the encryption chip from the threat of side scan-based attack. However, the LFSR seed or test authorization key stored in memory is extremely vulnerable to the attack on memory. To solve this problem, a dual dynamic obfuscation architecture is designed and a dual dynamic obfuscation strategy is constructed based on the two perspectives of side scan-based attack and memory attack. Among them, a dynamic obfuscation strategy of scan chain data based on LFSR self-update module is constructed to deal with side scan-based attack. Build an LFSR output sequence dynamic obfuscation strategy against memory attack. Experiments show that compared with the current secure scan strategy, the dual dynamic obfuscation strategy can protect the encryption chip from side scan-based attack and memory attack without affecting the testability of the chip. The area overhead is 0.31% when the LFSR self-update module number is 64 bits, and the number of XOR and XNOR gates in obviating logic gates are 8 bits each, it would need applied at least 6.29×10^{18} test vectors for the attacker to brute force the dual dynamic obfuscation strategy.

Key words: encryption chip; side scan-based attack; memory attack; dynamic obfuscation

1 引言

基于扫描链的可测试性设计技术因其具有可控制性和可观察性的特点,便于对集成电路进行测试和调试,因此在集成电路测试领域应用广泛.然而,对于应用于硬件加密的加密芯片来说,扫描链的可控制性和可观察性特点是一把双刃剑.

一方面,采用基于扫描链的可测试性技术可以使测试人员访问加密芯片的内部节点,提高加密芯片的测试覆盖率;另一方面,攻击人员可以利用扫描链的两个特点,绕开复杂的加密算法对加密芯片实施扫描旁路攻击,并完成对加密芯片密钥的破解^[1-2].因此,寻找一种可以抵抗扫描旁路攻击的加密芯片安全扫描策略成为加密芯片领域研究的重点.

为提高加密芯片应对扫描旁路攻击威胁的能力,解决当前安全扫描策略应对内存攻击威胁的不足^[3-7].本文以 AES 加密芯片为例,对 AES 加密算法、扫描旁路攻击及内存攻击两类攻击进行剖析,并基于动态混淆策略设计双重动态混淆架构、构建双重动态混淆策略.

2 AES 加密算法及两类攻击剖析

2.1 AES 加密算法剖析

AES 加密算法是采用分组密码体制、可以加解密 128 位数据的对称加密算法.加解密过程需要使用相同的加密密钥,密钥长度可为 128 位、192 位或 256 位,对应加密轮次为 10 轮、12 轮或 14 轮.本文以加密密钥长度为 128 位、加密轮次为 10 次为例进行讨论,如图 1 所示. AES 加密算法以字节为基本处理单位,算法中的明文、密文和轮密钥都以 4×4 字节的状态矩阵表示.

AES 加密算法运行时,首先将初始密钥通过密钥扩展生成轮密钥.128 位密钥长度的 AES 算法包括 1 个初始轮、9 个重复轮及一个最终轮.明文首先与初始轮密钥进行异或操作,然后进行 9 个重复轮的轮变换操作及最终轮变换操作,最终生成加密后的密文.其中与前 9 轮重复轮操作不同,最终轮变换操作不包括列变换操作.轮变换操作包含以下四个步骤:

(1)字节代换(Sub Bytes):利用查表操作实现字节的非线性变化;

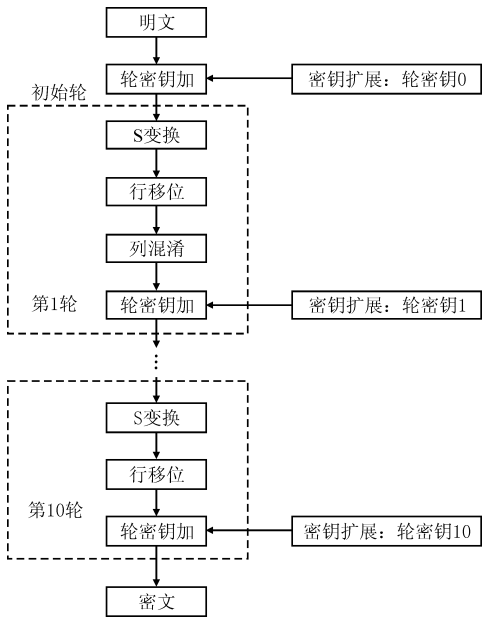


图 1 AES 加密算法工作流程

(2)行移位(Shift Rows):将状态矩阵中的每一行进行循环式移位操作;

(3)列混合(Mix Columns):利用固定矩阵对状态矩阵进行线性混淆;

(4)轮密钥加(Add Round Key):将轮密钥与状态矩阵中的数据进行异或操作.

AES 加密芯片中,每一轮加密所使用的轮密钥会存储在轮寄存器中.因为轮密钥包含与加密密钥相关的信息,相比于最终的密文具有较低的复杂度,因此是攻击人员实施扫描旁路攻击的攻击目标.

2.2 扫描旁路攻击剖析

2.2.1 模式切换攻击剖析

模式切换攻击是最早提出的扫描旁路攻击方法,仅需通过切换加密芯片的工作模式即可完成对加密芯片的攻击.模式切换攻击流程如下:

(1)明文输入:攻击人员控制加密芯片工作在功能模式并输入选定的明文,执行第一轮的加密操作后完成此步骤;

(2)扫描移出:攻击人员将加密芯片切换到测试模式,利用扫描链移位将加密结果移出;

(3)数据分析:攻击人员根据输入的选定明文对移出的扫描链数据进行分析,识别出扫描链中的轮寄存器并完成加密密钥的破解.

实施模式切换攻击需要两个条件:①攻击人员可以自由切换加密芯片工作模式,②攻击人员可以

窃取正确的扫描链数据. 因此可以从限制攻击人员切换加密芯片工作模式和限制攻击人员窃取正确的扫描链数据两个角度应对模式切换攻击.

2.2.2 仅测试模式攻击剖析

模式切换攻击可以完成对加密芯片的破解,但是模式重置对策可以应对模式切换攻击的威胁,因此仅测试模式攻击方法被提出,该方法只需要在测试模式下即可完成对加密芯片的攻击,成为目前扫描旁路攻击的主流攻击方法. 仅测试模式攻击流程如下:

- (1)扫描输入:攻击人员将选定测试向量串行移入扫描链中作为测试向量;
- (2)响应捕获:攻击人员执行捕获操作并将响应数据捕获到扫描链中;
- (3)扫描移出:攻击人员执行移位操作,将相应的测试响应移出扫描链;
- (4)数据分析:攻击人员对测试图形进行分析,根据 AES 加密算法特征识别出扫描链中的轮寄存器,并进一步完成加密密钥的破解.

仅测试模式攻击仅需在测试模式下即可实施攻击,可以绕过模式重置对策. 但是,实施该攻击同样需要①攻击人员可以应用选定的测试向量②攻击人员可以窃取到扫描链上正确的测试响应两个条件. 因此,设计人员可以从限制攻击人员应用选定的测试向量及窃取正确的测试响应两个角度展开研究.

2.3 内存攻击剖析

动态混淆策略和测试授权策略可以提高加密芯片应对扫描旁路攻击威胁的能力,然而这两种策略需要将 LFSR 种子或测试密钥存储在内存中. 攻击人员可以通过内存攻击窃取到 LFSR 种子或测试密钥,并利用窃取到的数据完成扫描链数据恢复工作或模式切换操作,以继续执行扫描旁路攻击.

利用内存攻击破解加密芯片需要满足如下条件:攻击人员窃取的 LFSR 种子或测试密钥可以直接用来进行扫描链数据恢复等工作,即加密芯片工作过程中不会对种子或测试密钥进行二次处理. 因此可以从此角度出发应对内存攻击威胁.

3 双重动态混淆策略构建

扫描旁路攻击要求攻击人员可以窃取正确的扫描链数据,内存攻击则需要攻击人员可以使用窃取到的 LFSR 种子或测试密钥进行扫描链数据恢复工作. 因此,从这两个角度出发,本文设计双重动态混淆架构,并基于此架构构建双重动态混淆策略,以解

决扫描旁路攻击和内存攻击对加密芯片威胁的问题. 其中,构建扫描链数据动态混淆策略限制攻击人员应用选定的测试向量及窃取正确的扫描链数据;构建 LFSR 输出序列动态混淆策略阻止攻击人员利用内存攻击窃取到的 LFSR 种子直接进行扫描链数据的恢复.

3.1 双重动态混淆架构设计

本文设计的双重动态混淆架构包括控制模块、LFSR 自更新模块、扫描链中插入的混淆逻辑门及扫描链中选定的扫描触发器,如图 2 所示. 其中, LFSR 自更新模块及扫描链中插入的混淆逻辑门构成扫描链数据动态混淆架构,用来构建扫描链数据动态混淆策略;扫描链中选定的扫描触发器及 LFSR 自更新模块构成 LFSR 输出序列动态混淆架构,用来构建 LFSR 输出序列动态混淆策略.

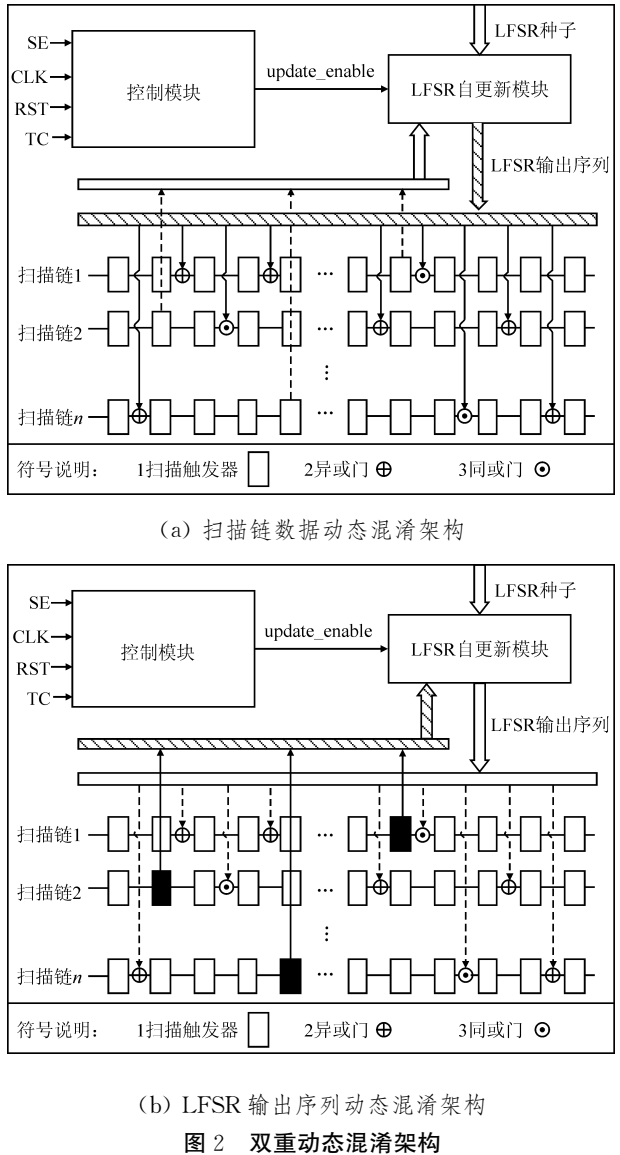


图2 双重动态混淆架构

①控制模块

控制模块的功能是控制 LFSR 输出序列混淆操作,模块中包含一个 N 位计数器、三个 1 位计数器、六个或门、三个与门、一个与非门及一个异或门。该模块由系统复位信号 RST、测试时钟 CLK、扫描使能信号 (Scan Enable, SE) 及测试控制信号 (Test Control, TC) 进行控制,用来为 LFSR 自更新模块提供自更新使能信号 update_enable 信号,控制模块电路图和时序图如图 3 和图 4 所示,其中 SE_count 信号为 N 位计数器的输出信号。

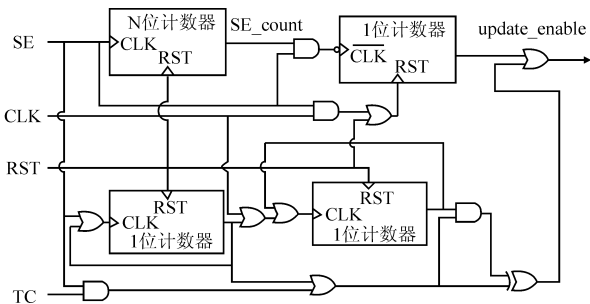


图 3 控制模块

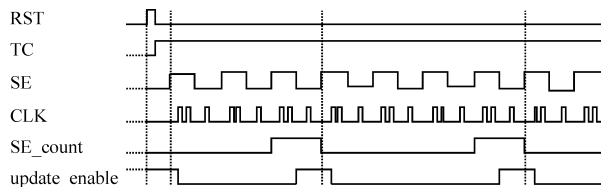


图 4 控制模块工作时序

②LFSR 自更新模块

LFSR 自更新模块具有两个作用,第一个作用是利用 LFSR 产生用于混淆扫描链数据的输出序列,第二个作用是利用扫描链中选定的扫描触发器混淆 LFSR 的输出序列。该模块由控制模块产生的 update_enable 信号及扫描使能信号 SE 控制。其中, update_enable 信号为 LFSR 自更新信号,SE 信号为 LFSR 的使能时钟信号。

LFSR 自更新模块通过在 LFSR 的基础上添加二选一选择器、异或门及同或门结构实现 LFSR 的自更新功能。其中,二选一选择器的一个输入信号为扫描链中选中的扫描触发器信号,另一个输入信号根据插入逻辑门类型的不同分别连接 GND 或 VDD 信号。选择器的选择信号为 update_enable 信号,当 update_enable 信号为低电平时,二选一选择器的输出信号不会对 LFSR 的输出序列产生影响,LFSR 按照已有输出序列继续运行;当 update_enable 信号为高电平时,利用选定的扫描触发器混淆 D 触发器

数据端的数据,LFSR 的输出序列被混淆,此后,LFSR 自更新模块将在更新后的输出序列基础上继续进行扫描链数据的动态混淆。

3.2 扫描链数据动态混淆策略

扫描链数据动态混淆策略基于扫描链数据动态混淆架构构建,该策略利用 LFSR 自更新模块的输出序列及扫描链中插入的混淆逻辑门对扫描链中的数据进行动态混淆,攻击人员在未获知 LFSR 自更新模块输出序列及混淆逻辑门插入的位置的情况下,无法将选定的测试向量应用到扫描链中,也无法窃取到正确的扫描链输出数据,因此无法实施扫描旁路攻击,如图 5 所示。测试人员在获取 LFSR 自更新模块输出函数及扫描链中混淆逻辑门插入位置等信息的情况下,可以根据扫描链数据动态混淆算法进行测试图形的处理和恢复,算法伪代码如下:

算法 1:扫描链数据动态混淆算法

输入:扫描链数据 $SC = \{SC_1 \cdots SC_L\}$, LFSR 自更新模块输出函数 function_update_LFSR

输出:混淆扫描链数据 $OSC = \{OSC_1 \cdots OSC_L\}$

变量: L 为扫描链的长度, M 为 LFSR 自更新模块位数, m 为中间变量, $m \leq M$

1. obfuscation $K = \text{function_update_LFSR}$, $m = 0$
2. for $i = 1; i \leq L; i++$ do
3. for $j = 1; j \leq L + 1 - i; j++$ do
4. if the j_{th} scan cell have insert logic gate
5. $m = m + 1$
6. if the insert logic gate is XOR gate
7. $OSC_i = SC_i \oplus K_m$
8. $SC_i = OSC_i$
9. else
10. $OSC_i = SC_i \odot K_m$
11. $SC_i = OSC_i$
12. End if
13. End if
14. End for
15. $m = 0$
16. End for

在加密芯片中应用扫描链数据动态混淆策略后,可以有效的限制攻击人员利用扫描链实施扫描旁路攻击,具体如下:

(1)模式切换攻击

在存在扫描链数据动态混淆策略的情况下,攻击人员每次控制 SE 信号进行模式切换时,扫描链中的数据都会受到 LFSR 自更新模块输出序列的混淆,从而使攻击人员无法窃取到正确的扫描链输出数据,无法满足攻击人员实施模式切换攻击所需要的第二个条件。因此模式切换攻击对双重动态混淆策略无效。

(2)仅测试模式攻击

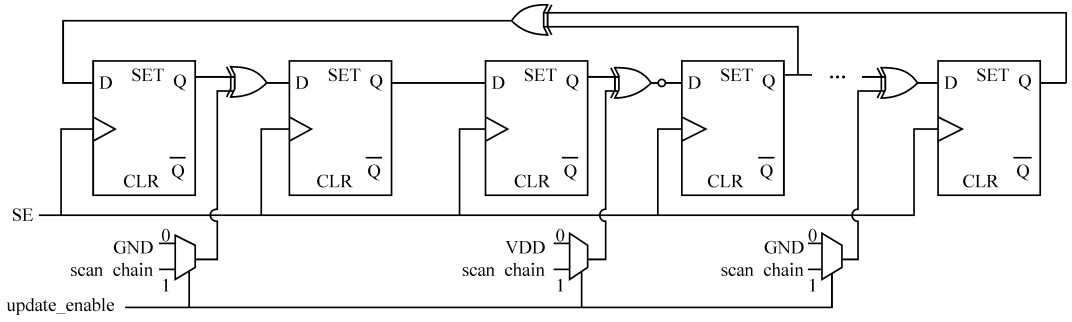


图 5 LFSR 自更新模块

在存在扫描链数据动态混淆策略的情况下,攻击人员实施仅测试模式攻击的两个攻击条件都无法满足,测试向量移入和测试响应移出时都会受到扫描链数据动态混淆策略的影响,从而使得攻击人员无法应用选定的测试向量并窃取正确的测试响应。因此,仅测试模式攻击对加密芯片无效。

攻击人员若想使用暴力方式破解扫描链数据动态混淆策略以继续进行扫描旁路攻击,则需要完成对 LFSR 的破解。暴力破解 LFSR 的次数与其长度有关,在攻击人员无法窃取 LFSR 种子的情况下,实现 M 位 LFSR 的破解需要尝试的次数 A 为:

$$A = 2^M \quad (1)$$

3.3 LFSR 输出序列动态混淆策略

扫描链数据动态混淆策略可以提高加密芯片抗扫描旁路攻击的能力,但是如果攻击人员通过内存攻击窃取到 LFSR 的种子,则可以轻松进行扫描链数据的恢复工作并继续完成扫描旁路攻击。针对此问题,本文基于 LFSR 输出序列动态混淆架构构建 LFSR 输出序列动态混淆策略。该策略利用扫描链中选定的扫描触发器和设计的 LFSR 自更新模块动态混淆 LFSR 的输出序列, LFSR 的种子加载到 D 触发器后,需要和扫描链中选取的扫描触发器进行异或或同或操作,因此,即使攻击人员通过内存攻击窃取到 LFSR 的种子,仍然无法直接破解 LFSR 自更新模块的输出序列。测试人员获知控制模块的工作时序和 LFSR 自更新模块结构的情况下,可以通过 LFSR 输出序列动态混淆算法计算正确的 LFSR 自更新模块输出序列,算法伪代码如下:

算法 2 LFSR 输出序列动态混淆算法

输入: LFSR 自更新模块种子 $seed = \{S_1 \cdots S_M\}$ 选中扫描触发器数据 $C = \{C_1 \cdots C_H\}$

LFSR 功能函数 $LFSR_function()$

输出: LFSR 自更新模块输出序列 $D = \{D_1 \cdots D_M\}$

变量: T 为更新周期, M 为 LFSR 自更新模块位数 H 为插入逻辑门个数, h 为中间变量, $h \leq H$

1. function_update_LFSR;

```

2.  D=LFSR_obfuscation(D=seed), h=0
3.  if SE_count == T
4.      D= LFSR_obfuscation(D={D_1...D_M}), h=0
5.      D= LFSR_function(D={D_1...D_M})
6.      SE_count = 0
7.  else
8.      D= LFSR_function(D={D_1...D_M})
9.  SE_count = SE_count + 1
10. End if
11. LFSR_obfuscation:
12. for i=1; i≤M; i++
13.     If the ith D flip-flop have insert logic gate
14.         h=h+1
15.         if is XOR and update_enable is 1
16.             Di=Di⊕Ch
17.         else if is XNOR and update_enable is 1
18.             Di=Di⊙Ch
19.         else Di=Di
20.         End if
21.     End if
22. End for
23. End LFSR_obfuscation
24. End function_update_LFSR

```

在加密芯片中应用 LFSR 输出序列动态混淆策略后,攻击人员无法通过内存攻击直接完成扫描链数据的恢复工作。若想完成扫描链数据的恢复并继续实施扫描旁路攻击,攻击人员需要解决以下两个问题:①确定 LFSR 自更新模块中插入混淆逻辑门的个数及位置②确定 LFSR 自更新模块中混淆逻辑门各类型的数量,即异或门和同或门分别插入的数量。假设 LFSR 自更新模块的位数为 M 位,插入的逻辑门的个数为 H ,其中异或门和同或门得个数分别为 X 和 Y , $H=X+Y$;则攻击人员至少需要尝试的次数 S 为:

$$S = C_H^M \times C_H^X \quad (2)$$

此外,在本文所提双重动态混淆策略中,测试人员或者攻击人员可以自由的切换加密芯片的工作模式,在测试模式下也可以自由切换移位操作和捕获操作。因此,测试人员可以对加密芯片进行正常的在

线测试、发射-捕获(Launch-Off-Capture, LOC)测试和发射-移位(Launch-Off-Shift, LOS)测试,从而可以对加密芯片进行更完整的扫描测试. 虽然本文所提策略会对测试流程造成一些影响,但是测试人员只需根据本文给出的扫描链数据动态混淆算法及LFSR 输出序列动态混淆算法即可完成扫描链数据的恢复及加密芯片的扫描测试.

4 实验结果与分析

为评估双重动态混淆策略给加密芯片原始电路

造成的面积开销,本文以 opencores 上 AES—128^[8]加密芯片为实验电路,利用 Design Compiler 及 DFT Compiler 等工具,计算因双重动态混淆策略引入的逻辑电路相比于原始电路的面积开销. 其中,综合考虑面积开销、安全性和便于不同安全扫描策略对比等因素,实验中将 LFSR 自更新模块的位数和 SOSD—64、DOSD—64 及 FTSL—64 策略中密码长度取为一致,为 64 位,LFSR 自更新模块中插入异或门和同或门的个数各 8 位. 不同安全扫描策略对比及实验分析如表 1.

表 1 安全扫描策略对比

策略	面积开销/%	安全漏洞	暴力破解次数	可测试性影响
SOSD—64	0. 18	仅测试模式特征攻击	264	LOC 不能正常进行
DOSD—64	0. 25	无	264	LOC 不能正常进行
FTSL—64	3. 09	无	264	无
Wang scheme	0. 11	无	—	不能进行在线测试
Proposed	0. 31	无	$6. 29\times10^{18}$	无

从实验结果可以看出,与本文提出的双重动态混淆策略相比,文献[9]中提出的 SOSD—64 策略虽然可以抵抗内存攻击的威胁且在面积开销这一指标上优于本文策略,但是该策略无法抵抗仅测试模式特征攻击[10]的威胁. 可测试性方面,由于应用了 SOSD—64 策略的 AES 加密芯片无法进行 LOC 测试操作,因此原始加密电路的可测试性会受到影响;文献[10]中提出的 DOSD—64 策略解决了 SOSD—64 策略应对仅测试模式特征攻击的不足,但是其仍然存在可测试性的不足;文献[6]中提出的 FTSL—64 策略虽然不存在可测试性方面的不足且可以为每个加密芯片提供单独密钥,但是该策略造成了较大的面积开销;文献[7]中 Wang 等人提出的策略相比于原始电路仅增加了 0. 11%的面积开销,由于该方案不存在种子或测试密钥,因此不会受到内存攻击的威胁,也不存在暴力破解种子和测试密钥的选项. 但是与本文策略相比,该策略不允许加密芯片进行在线测试,因此对加密芯片的可测试性会造成较大的影响.

此外,需要指出表 1 中双重动态混淆策略的暴力破解次数是考虑了存在内存攻击情况的结果,即由公式(2)得. 若不考虑存在内存攻击的情况,因为 LFSR 输出序列动态混淆策略的存在,攻击人员无法通过暴力尝试完成对 LFSR 种子的破解. 在 1GHz 频率下,以本文加密电路中扫描链长度 6720 为例,攻击人员想要应用 $6. 29\times10^{18}$ 个测试向量完

成暴力破解至少需要 $1. 33\times10^6$ 年,设计人员可根据公式(2)调整插入混淆逻辑门的数量和种类,以获得安全性和面积开销的平衡. 结合攻击人员实施内存攻击的难度,本文所提的双重动态混淆策略在不影响加密芯片可测试性的情况下可有效保护加密芯片免受扫描旁路攻击及内存攻击的威胁.

5 结束语

本文针对当前加密芯片安全扫描策略不能有效应对内存攻击威胁、未能全面考虑安全扫描策略对加密芯片影响的问题,提出抗内存攻击的加密芯片双重动态混淆策略. 实验分析表明,本文所提策略在不影响加密芯片可测试性的同时,提高了加密芯片应对扫描旁路攻击和内存攻击的能力. 但是由于在加密芯片原始电路中引入了 LFSR 自更新模块和控制模块,因此如何测试额外引入的电路是下一步研究的重点.

参考文献:

[1] 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.

[2] ALI S S, SINANOGLU O, KARRI R. Test-mode-only scan attack using the boundary scan chain[C] // IEEE European Test Symposium. Paderborn, Germany, 2014:1-6.

- [3] ZHANG D R, HE M, WANG X X, et al. Tehranipoor. Dynamically obfuscated scan for protecting IPs against scan-based attacks throughout supply chain[C] // VLSI Test Symposium. Las Vegas, America. 2017: 1-6.
- [4] WANG X, ZHANG D, MIAO H, et al. Secure Scan and Test Using Obfuscation Throughout Supply Chain [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, 37 (9): 1867-1880.
- [5] WU C C, KUO M H, LEE K J. A Dynamic-Key Secure Scan Structure Against Scan-Based Side Channel and Memory Cold Boot Attacks [C] // Asian Test Symposium. Hefei, China, 2018:48-53.
- [6] CUI A, CHANG C H, ZHOU W, et al. A New PUF Based Lock and Key Solution for Secure In-field Testing of Cryptographic Chips [J]. IEEE Transactions on Emerging Topics in Computing, DOI: 10.1109 /TETC.2019.2903387.
- [7] WANG W, WANG J, WANG W, et al. A Secure DFT Architecture Protecting Crypto Chips Against Scan-Based Attacks [J]. IEEE Access, 2019 (7): 22206-22213.
- [8] Hsing. Homer. AES: Overview [CP/OL]. (2012-10-13). [2020-03-31]. http://opencores.org/project,tiny_aes.
- [9] LUO Y, CUI A, GANG Q, et al. A new countermeasure against scan-based side-channel attacks [C] // IEEE International Symposium on Circuits & Systems. Montreal, Canada. 2016:1722-1725.
- [10] 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 & Security, 2017, 12(2):363-376.

作者简介:

景凤池 男,(1994-),硕士.研究方向为集成电路可测试性设计.

张金艺(通讯作者) 男,(1965-),研究员,博士生导师.研究方向 SOC/NOC 可靠性设计、无线通信类 ASIC 设计.

E-mail: zhangjinyi@shu.edu.cn.