

基于可满足性无关项的硬件木马设计与检测

武玲娟^{1,2}, 朱嘉诚¹, 唐时博¹, 谭静¹, 胡伟¹

(1. 西北工业大学网络空间安全学院, 陕西 西安 710072;

2. 华中农业大学信息学院, 湖北 武汉 430070)

摘要: 硬件木马是集成电路中隐含的恶意设计修改, 被激活后可用于发起高效的底层攻击。由此, 展示了一种新的利用可满足性无关项的轻量级高隐蔽性硬件木马安全威胁。该木马设计方法将轻量级木马设计隐藏于电路正常工作条件下无法覆盖到的可满足性无关项中, 使插入木马后的电路设计与原始设计完全功能等价。攻击者只需利用简单的故障注入攻击手段即可激活木马。基于 1024 位 RSA 密码核的实验结果显示, 所给出的木马设计能够逃避逻辑综合优化, 通过故障注入攻击能够有效恢复 RSA 密码核的私钥。在此基础上, 提出了一种能够有效检测该高隐蔽性木马设计的防御手段。

关键词: 硬件安全; 硬件木马; 可满足性无关项; 故障注入; 木马检测

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021025

Design and detection of hardware Trojan based on satisfiability don't cares

WU Lingjuan^{1,2}, ZHU Jiacheng¹, TANG Shibo¹, TAN Jing¹, HU Wei¹

1. School of Cyber Security, Northwestern Polytechnical University, Xi'an 710072, China

2. College of Informatics, Huazhong Agricultural University, Wuhan 430070, China

Abstract: Hardware Trojans are intended malicious design modifications to integrated circuits, which can be used to launch powerful low-level attacks after being activated. A new security threat of lightweight stealthy hardware Trojans leveraging discrete satisfiability don't care signals was demonstrated. These don't care could not be satisfied under normal operation and thus the circuit design with Trojan is functionally equivalent to the Trojan-free baseline. The attacker could activate the Trojan through simple yet effective fault injection. Experimental results on a 1024-bit RSA cryptographic core show that the proposed hardware Trojan can escape from logic synthesis optimization, and that the RSA private key can be retrieved by simply over-clocking the design. A defense technique that can effec-

收稿日期: 2020-11-14; 修回日期: 2020-12-24

通信作者: 胡伟, weihu@nwpu.edu.cn

基金项目: 国家自然科学基金(62074131); 湖北省自然科学基金(2020CFB190)

Foundation Items: The National Natural Science Foundation of China (62074131), The Natural Science Foundation of Hubei Province (2020CFB190)

论文引用格式: 武玲娟, 朱嘉诚, 唐时博, 等. 基于可满足性无关项的硬件木马设计与检测[J]. 网络与信息安全学报, 2021, 7(2): 35-42.

WU L J, ZHU J C, TANG S B, et al. Design and detection of hardware Trojans based on satisfiability don't cares[J]. Chinese Journal of Network and Information Security, 2021, 7(2): 35-42.

tively detect such stealthy Trojan design was provided.

Keywords: hardware security, hardware Trojan, satisfiability don't care, fault injection, Trojan detection

1 引言

随着集成电路产业链的全球化, 集成电路设计中通常会大量使用来自不可信第三方的知识产权 (IP, intellectual property) 核。这些 IP 中可能隐含设计规范之外的未公开恶意代码和后门。此外, 由于成本限制, 集成电路设计完成之后往往交由芯片制造商进行加工, 此过程中不可信制造商也可能插入未声明恶意设计修改。上述由不可信第三方引入的恶意设计修改, 称为硬件木马^[1], 硬件木马通常只有在特定的条件下才会激活, 现有的集成电路测试方法难以实现木马检测。攻击者可通过特定输入、侧信道、故障注入等方式激活木马, 从而造成敏感信息泄露、设计性能降低甚至系统失效, 造成极大的安全威胁^[2]。

Karri 等^[3]根据插入阶段、激活机制、负载特性等对硬件木马进行了系统分类。根据这一分类系统, Trust-HUB.org 平台上发布了一系列硬件木马设计。这些木马设计使用计时器或特定输入向量作为木马的激活条件^[4], 产生一个单一信号用于触发木马, 使这些木马很容易被翻转概率分析方法检测到^[5-6]。为了抵御基于翻转概率分析的木马检测方法, 研究者提出使用多个分离的信号作为木马触发信号的设计方法^[7-8], 由于采用基于木马在特定条件下触发的方式, 基于标签传播的翻转概率分析方法和基于无关项分析的方法仍能够将木马识别为恶意或冗余逻辑^[9-10]。可见, 现有硬件木马设计方法通常需引入低活度的触发信号、改变设计功能或存在显著的负载指纹, 上述特征使检测此类木马较为简单。

为了提高硬件木马的隐蔽性, 防止木马在设计阶段被检测到, 近年来, 研究者提出了基于无关项的木马设计方法, 利用集成电路设计空间中的外部无关项, 包括未声明的功能、有限状态机中未占用的编码、X 状态^[11-14]进行木马设计。插入木马的电路是原始电路设计空间的超集, 在正常工作情况下, 电路并不会进入木马所在的设计空间, 因此, 包含外部无关项木马的电路完全符合设计规范要求, 基于设计规范验证的方法难

以实现木马检测。但是, 该方法并不适用于设计空间被完全声明的集成电路。

文献[15]提出了一种利用可满足性无关项的硬件木马设计方法, 利用集成电路内部扇出重汇聚引入的可满足性无关项, 作为木马的触发信号, 控制木马泄露 AES 算法的密钥。相对于基于外部无关项的木马设计方法^[11-14], 上述工作适用于功能被完全声明的电路设计。同时, 由于木马设计隐藏在电路正常工作条件下无法满足的可满足性无关项中, 插入木马之后的电路设计与原始设计完全功能等价, 功能等价性验证并不能检测到木马, 该木马设计引入了 256 个二输入选择器, 负载指纹较为显著。

本文展示了一种新的利用可满足性无关项的轻量级高隐蔽性硬件木马安全威胁, 利用可满足性无关项, 设计了针对公钥密码系统的轻量级硬件木马, 揭示了公钥密码系统所面临的一种新的硬件木马安全威胁, 并通过实验验证其隐蔽性和可利用性。在此基础上, 提出了一种能够有效检测该高隐蔽性木马设计的防御手段。本文主要工作及贡献如下:

- 1) 展示了一种新的利用可满足性无关项的轻量级高隐蔽性硬件木马安全威胁;
- 2) 通过实验结果验证了该硬件木马设计的高隐蔽性和可利用性;
- 3) 提出了一种能够有效应对该高隐蔽性木马安全威胁的防御手段。

2 相关工作

本节介绍与本文工作密切相关的无关性木马设计。无关性木马利用集成电路设计空间的外部或内部无关项进行木马设计, 相比传统基于计数器或特定输入向量触发的木马设计方法, 具有更高的隐蔽性。

Fern 等^[11-12]利用集成电路设计中未声明功能引入的外部无关项进行木马设计, 选取电路中具有未声明行为的信号, 对其功能进行修改以添加恶意逻辑, 由于插入木马之后的设计空间是原始设计的超集, 使用者根据原始设计规范进行功能及形式化等价性验证并不能发现所插入的木马。

Nahiyen 等^[13]提出利用有限状态机中未声明状态进行木马设计的方法，基于集成电路设计或综合优化中引入的无关状态，插入恶意木马逻辑，在正常工作下，有限状态机不会切换到包含木马逻辑的状态，而攻击者可通过故障攻击使有限状态机进入恶意状态以激活木马。Krieg 等^[14]提出利用 X 无关项作为触发信号的木马设计方法，利用 X 无关项信号在仿真中为逻辑 0，而在实现电路中为逻辑 1 的特点，使设计阶段形式化等价性验证并不能检测到木马。以上方法^[11-14]可以提高木马的隐蔽性，但是，当电路功能被完全声明时，基于外部无关项的木马设计方法并不适用。

近年来，Hu 等^[15]提出利用集成电路内部无关项的木马设计方法，木马隐藏在电路正常工作条件下无法满足的可满足性或可观测性无关项中，攻击者通过故障注入攻击可以激活木马。基于内部无关项的木马设计方法在多用户 FPGA 平台上进一步完成了验证，攻击者通过部署能量损耗电路引入故障攻击可以远程激活木马，窃取其他用户的密钥信息^[16]。研究者提出利用混淆电路中未声明功能的木马设计方法^[17]，逻辑混淆是为了防止集成电路 IP 被盗窃、仿造，在原始电路中加入的设计，当混淆密钥被正确加载时电路实现设计规范中声明的正确功能，但是为了保护混淆密钥，当密钥不正确时，电路功能并不会被明确声明，因此，攻击者可以利用混淆密钥不正确时引入的未声明状态空间插入木马。

上述方法中研究者分别利用集成电路设计外部或内部无关项进行硬件木马设计。本文展示了一种新的硬件木马安全威胁，木马隐藏于电路正常工作条件下无法覆盖到的可满足性无关项中，设计了针对 RSA 公钥密码系统的轻量级硬件木马，通过故障注入攻击，能够有效激活木马恢复公钥密码系统的私钥。在此基础上，本文提出了一种可有效检测该新型硬件木马的防御措施。

3 威胁模型

利用可满足性无关项设计的硬件木马可在集成电路设计的不同阶段由不可信第三方电路设计者、EDA 工具或芯片制造厂家插入原始设计中。本文假设硬件木马由不可信第三方电路设计者插

入原始设计中，插入木马后的设计以寄存器传输级代码、门级网表、物理芯片或 FPGA 实现的形式提供给用户。

本文假设用户可以获得原始设计的规范，可依据设计规范对插入木马后的电路进行全面的功能验证，用户同样可以基于现有的木马检测方法对其进行分析。本文假设攻击者能够获得插入木马后的电路设计的细节信息，同时，假设攻击者可以控制电路模块的外部输入信号、观测公开的状态输出信号（如芯片忙信号 BSY），但无法观测私钥和解密结果等内部敏感信息。

4 基于无关项的硬件木马安全威胁

本节介绍公钥密码系统所面临的一种基于集成电路内部无关项的硬件木马安全威胁。该木马隐藏在电路正常工作条件下无法满足的可满足性无关项中，插入木马后的电路设计和原始设计完全功能等价。可通过提高时钟频率发起故障注入攻击来激活木马。

4.1 利用可满足性无关项的木马设计

可满足性无关项是集成电路设计内部由于扇出重汇聚引入的无关状态^[18]，在电路正常工作条件下，可满足性无关项无法被满足。如图 1 所示的电路，其布尔函数表达式为

$$O = A \cdot B + \bar{B} \cdot C + \bar{C} \cdot D \quad (1)$$

其中，内部信号(n1, n4)组成可满足性无关项，逻辑状态(1, 1)是(n1, n4)在正常工作条件下无法满足的状态，n1 和 n4 连接到逻辑门 g6。进一步可以把可满足性无关项扩展到全局的概念，即没有连接到同一个逻辑门的可满足性无关项，如图 1 中的内部信号(n5, n4)。(1, 1)是(n5, n4)在正常工作条件下无法满足的状态。通过布尔可满足性分析可以搜索到集成电路设计中的可满足性无关项。

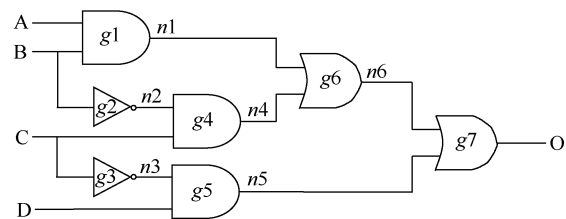


图1 可满足性无关项示例
Figure 1 Example of satisfiability don't cares

文献[15]提出了利用可满足性无关项的木马设计方法。如图 2 所示,可满足性无关项 $n5$ 、 $n4$ 作为木马的触发信号,分别通过寄存器后作为两个选择器的选择信号,输出信号逻辑表达式为

$$O_tj = n5 \cdot n4 \cdot f + \overline{n5 \cdot n4} \cdot O \quad (2)$$

在正常工作条件下, $n5 = n4 = 1$ 的逻辑状态无法满足,式(2)等价于

$$O_tj = O \quad (3)$$

即插入木马后的设计和原始设计完全功能等价,因此,功能等价性验证不能检测到木马。当攻击者通过故障注入攻击使可满足性无关项条件满足时,木马被激活,信号 f 被选择输出到 O_tj ,此时可通过观测公开输出信号 O_tj 获取敏感信息 f 。

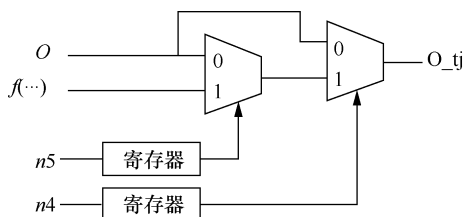


图 2 利用可满足性无关项的木马设计
Figure 2 Hardware Trojan leveraging satisfiability don't care

虽然式(2)可以仅由一个选择器实现,选择信号为 $n5 \cdot n4$,但是在正常工作条件下, $n5 \cdot n4$ 为逻辑 0,基于翻转概率分析的木马检测方法能够检测到木马。本文设计的木马设计使用了两个选择器,木马触发信号 $n5$ 、 $n4$ 分别作为两个选择器的选择信号, $n5$ 、 $n4$ 在电路工作中都会翻转,因此,可以逃避基于翻转概率分析的木马检测方法。同时,为了防止木马在电路逻辑综合中被优化,本文介绍的木马设计引入了两个寄存器,木马触发信号 $n5$ 、 $n4$ 分别通过寄存器后输入选择器。加入寄存器后,电路的设计功能仍然完全符合设计功能规范。

与不完全功能声明引入的集成电路设计外部无关项相比,可满足性无关项由电路内部扇出重汇聚引入,当电路功能被完全声明时,可满足性无关项仍然存在。因此,利用可满足性无关项

的木马设计方法适用于功能被完全声明的集成电路设计。

4.2 攻击模型

本文的攻击模型利用可满足性无关项信号的路径时延差引入故障攻击。正常工作条件下,可满足性无关项无法满足,木马不会被激活。由于两个木马触发信号路径存在差异,当提高输入时钟频率时,一个木马触发信号到寄存器的时序得不到满足,而另一个木马触发信号的时序仍然满足时,两个触发信号的逻辑关系将间歇性满足木马触发的条件,如同时为逻辑 1,此时木马被激活。

首先,插入木马之后的电路在正常时钟频率下,完成电路的初始化。然后,逐步提高时钟频率发起故障注入攻击。当木马触发信号中仅一个信号的时序失效时,木马触发条件将间歇性满足从而激活木马,此时,攻击者可以通过观测电路的公开状态输出信号,获取敏感信息。之后,继续提高时钟频率,两个木马触发信号时序均得不到满足,此时电路输出处于随机错误状态,不能根据输出信号获取有用信息。

5 实验结果与分析

本节以 RSA 密码核为例介绍本文基于可满足性无关项的硬件木马设计与攻击方法。

5.1 RSA 密码核木马设计和测试流程

利用集成电路设计内部可满足性无关项的木马设计、测试与攻击流程如图 3 所示。

1) 使用 Synopsys Design Compiler 对原始设计进行综合与映射,生成门级网表;然后,使用布尔可满足性分析工具在网表中搜索可满足性无关项。

2) 使用 4.1 节中介绍的木马设计方法在原始设计中插入木马;插入木马后的设计使用 Vivado 进行综合,检测木马是否能够逃避逻辑综合优化。

3) 在正常工作条件下,对插入木马的设计和原始设计进行随机仿真功能测试和功能一致性检查。

4) 基于攻击模型对通过测试的插入木马的设计发起故障注入攻击。

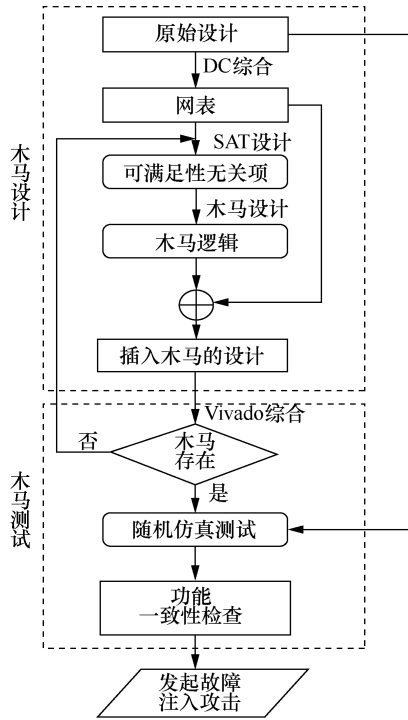


图3 硬件木马设计、测试与攻击流程
Figure 3 Hardware Trojan design, testing and attack flow

根据以上木马设计及测试流程，本文选取了日本东北大学 Aoki 实验室发布的开源 1 024 位 RSA 密码核作为设计基准，插入木马的 RSA 密码核结构如图 4 所示，主要包括状态控制单元、模乘计算单元及存储单元。RSA 密码核中包含一个密钥移位寄存器，在状态控制单元产生的使能信号控制下，移位输出密钥的最高位比特，RSA 算法根据最高位比特控制加/解密运算。本文选取模乘运算单元中的一对可满足性无相关项信号作为木马的触发信号，这两个信号在正常工作条件下不能同时为逻辑 1。触发信号分别经过寄存器后，作为多选器的选择信号。当两个触发信号同时为逻辑 1 时，木马被激活，密钥移位寄存器的最高位泄露至 BSY 信号。

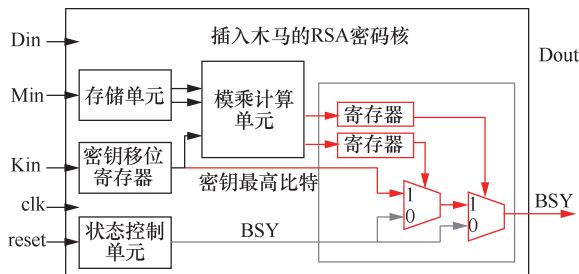


图4 包含无关项木马的 RSA 设计
Figure 4 RSA design with SDC Trojan

插入木马后的 RSA 密码核使用 Vivado 进行逻辑综合与实现，综合结果表明，本文介绍的木马设计能够逃避逻辑综合优化，综合后仍存在电路中。在相同的约束条件下，插入木马后的 RSA 密码核及原始设计综合结果如表 1 所示，插入木马后 LUT 资源减小 0.16%，FF 资源增加 0.15%，功耗降低了 0.57%。进一步地，通过线性移位寄存器产生随机输入，进行随机仿真功能测试。测试结果表明，正常工作条件下，木马没有被激活，插入木马后的 RSA 密码核与原始设计输出完全一致，功能等价。

RSA 密码核加/解密过程执行模幂运算，当密钥为 0 时，执行一次蒙哥马利模平方运算，当密钥为 1 时，执行一次蒙哥马利模乘和一次蒙哥马利模平方运算，其中，1 比特密钥 1 的运算时间为 1 比特密钥 0 运算时间的两倍。

木马激活，当前密钥位为 1 时，BSY 信号输出逻辑固定为 1；当前密钥位为 0 时，木马将 X 态输出到 BSY 信号，因此，可通过观测 BSY 信号是否有 X 态来确定当前密钥为 1 还是 0。然后，通过测量 BSY 信号被拉低段持续的最短时间，即为 1 比特密钥 0 的运算时间 Δt ，进而 1 比特密钥 1 的运算时间为 $2 \cdot \Delta t$ 。最后，运算时长除以单比特运算时间即可确定密钥长度，实现密钥的解码。

表 1 RSA 密码核对木马设计的影响
Table 1 Effects of SDC Trojan in RSA cryptographic core

RSA 密码核	参数				
	LUT	LUTRAM	FF	BUFG	总功耗
原始 RSA 密码核	3627	128	1343	1	0.701W
木马 RSA 密码核	3621	128	1345	1	0.697W
木马设计影响	-0.16%	0	+0.15%	0	-0.57%

5.2 故障注入攻击

本文选取 Xilinx XCZU9EG FPGA 芯片进行木马实现和布局布线后时序仿真。根据布局布线后时序分析报告，得到插入木马的 RSA 密码核的最高时钟工作频率为 129.31 MHz。

根据本文的攻击模型，首先，在 100 MHz 时钟频率下，对插入木马后的 RSA 密码核和原始设计分别进行布局布线后时序仿真，以保证密码核

正常初始化和密钥正常加载。100 MHz 下, RSA 密码核处于正常工作状态, 木马没有被激活, 插入木马后的 RSA 密码核和原始设计输出完全一致, 仿真波形如图 5(a)所示。然后, 逐步提高插入木马后的 RSA 密码核的输入时钟频率, 发起故障注入攻击。实验发现, 当时钟频率为 151.51 MHz 时, Dvld 信号产生了逻辑高电平, BSY 信号出现了不确定 X 态, 信号值在 X 和逻辑 1 之间切换, 此时木马被激活, 32 位密钥下仿真波形如图 5(b)所示。

根据本文介绍的木马设计方案, 当木马被激活且当前密钥位为逻辑 1 时, BSY 信号为逻辑 1; 而当前密钥位为逻辑 0 时, BSY 信号出现 X 态。因此, 可通过观测 BSY 信号是否有 X 态确定密钥为 1 还是 0。进一步地, 确定 1 比特密钥 0 的加密时长, 通过加密时长比较确定密钥为 1 和 0 的比特个数, 进而恢复出密钥。根据以上分析得到图 5(b)中 32 位密钥为 0x00903AD9, 与测试向量中设定的密钥一致, 即通过故障注入攻击, 观测状态输出信号 BSY 能够有效恢复出密钥。

151.51 MHz 输入时钟频率下, 本文进一步完成了 256 位、512 位、1024 位密钥的布局布线后时序仿真, 其中 1024 位密钥下仿真波形如图 5(c)所示, 木马激活下, BSY 信号波形在 X 和逻辑 1 之间切换, 基于上述分析方法, 同样可以恢复出

1024 位密钥。

继续提高输入时钟频率, 在 166.67 MHz 输入时钟频率下, 足够长的仿真时间内 BSY 信号一直为逻辑 1。此时, RSA 密码算法核有过多路径发生时序错误, 完全失效, 密钥移位寄存器也没有进行移位操作。166.67 MHz 时钟频率下 32 位密钥的仿真波形如图 5(d)所示, 此时, 不能根据 BSY 信号获取密钥信息。进一步地, 分别对多个不同的 32 位、256 位、1024 位密钥, 在 151.51 MHz 输入时钟频率下对插入木马的 RSA 密码核进行布局布线后时序仿真, 实验结果表明, 本文给出的攻击方法与密钥长度无关, 木马被激活后基于上述分析方法可以分别恢复出 32 位、256 位和 1024 位密钥。

6 无关项木马防御手段

本文展示了一种基于集成电路内部可满足性无关项的硬件木马安全威胁。由于木马隐藏在电路正常工作条件下无法满足的可满足性无关项之中, 插入木马后的电路设计与原始设计完全功能等价。本文介绍的硬件木马采用了两个木马触发信号和两级木马负载结构, 由于在正常工作条件下每个触发信号都会翻转, 基于逻辑功能测试和翻转概率分析的传统木马检测方法难以实现这种新型硬件木马检测。此外, 这种新型木马设计仅包含两个寄存器和两个选择器, 木马逻辑简单负

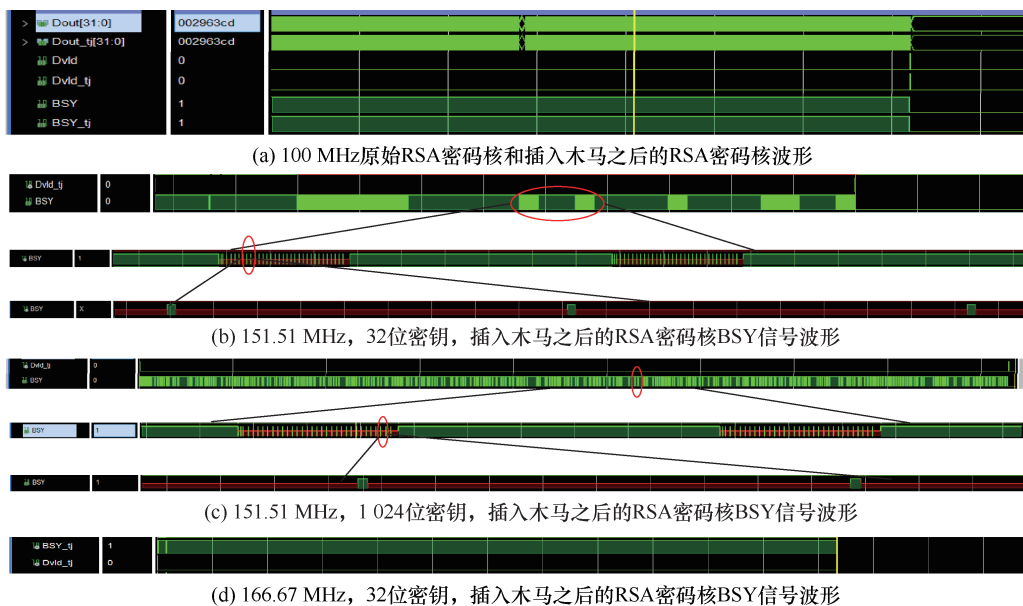


图5 100 MHz、151.51 MHz、166.67 MHz 时钟下布局布线后时序仿真结果

Figure 5 Post-implementation timing simulation results under 100MHz, 151.51MHz, 166.67MHz

载指纹小, 由于缺乏黄金芯片比对, 基于侧信道分析^[19-20]的方法也难以实现木马检测。因此, 针对这种新型硬件木马安全威胁需要提出新的防御手段。

近年来, 研究者提出属性驱动的硬件安全验证方法^[21-23], 通过在门级或者寄存器传输级基于信息流分析方法建立硬件安全模型, 实现对集成电路硬件安全属性的验证。本文介绍的硬件木马设计中存在密钥敏感信息到公开状态输出 BSY 信号的信息流传播路径, 基于上述硬件安全验证方法建立插入木马后 RSA 密码核的硬件安全模型, 对电路的保密性进行验证, 能够检测到从密钥到 BSY 信号的违反保密性安全属性的不安全路径。因此, 这种新型的硬件安全验证方法能够有效检测基于无关项的硬件木马安全威胁。此外, 基于频率扫描的木马检测方法, 通过采集不同时钟频率下电路时延信息进行木马检测, 由于与本文给出的通过提高时钟频率发起故障注入攻击的方法类似, 在特定的频率下有可能会激活木马从而实现木马检测。

7 结束语

本文的研究工作展示了一种新的利用可满足性无关项的硬件木马安全威胁及其防御手段。本文介绍了针对公钥密码系统 RSA 的硬件木马设计与实现, 实验结果表明这种新型硬件木马能够逃避逻辑综合优化; 在正常工作条件下, 木马不会被激活, 插入木马后的 RSA 密码核与原始设计完全功能等价; 通过故障注入攻击能够恢复出 1024 位 RSA 密码核的私钥。同时, 本文提出一种针对该高隐蔽性硬件木马的防御措施, 通过基于信息流分析的硬件安全验证方法, 能够有效检测到这种新型硬件木马引发的不安全路径。本文的研究工作有助于硬件设计者关注隐藏在集成电路内部无关项中的硬件木马安全威胁, 在设计阶段采取有效的防御手段解决潜在的安全隐患。

参考文献:

- [1] TEHRANIPOOR M, KOUSHANFAR F. A survey of hardware Trojan taxonomy and detection[J]. IEEE Design & Test of Computers, 2010, 27(1): 10-25.
- [2] LI H, LIU Q, ZHANG J. A survey of hardware Trojan threat and defense[J]. Integration, 2016, 55: 426-437.
- [3] KARRI R, RAJENDRAN J, ROSENFELD K, et al. Trustworthy hardware: identifying and classifying hardware Trojans[J]. Computer, 2010, 43(10): 39-46.
- [4] BAUMGARTEN A, STEFFEN M, CLAUSMAN M, et al. A case study in hardware Trojan design and implementation[J]. International Journal of Information Security, 2011, 10(1): 1-14.
- [5] WAKSMAN A, SUOZZO M, SETHUMANDHAVAN S. FANCI: identification of stealthy malicious logic using Boolean functional analysis[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. 2013: 697-708.
- [6] HICKS M, FINNICUM M, KING S T, et al. Overcoming an untrusted computing base: detecting and removing malicious hardware automatically[C]//2010 IEEE Symposium on Security and Privacy. 2010: 159-172.
- [7] STURTON C, HICKS M, WAGNER D, et al. Defeating UCI: building stealthy and malicious hardware[C]//2011 IEEE Symposium on Security and Privacy. 2011: 64-77.
- [8] ZHANG J, YUAN F, XU Q. Detrust: defeating hardware trust verification with stealthy implicitly-triggered hardware Trojans[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014: 153-166.
- [9] ZHANG J, YUAN F, WEI L, et al. VeriTrust: verification for hardware trust[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34(7): 1148-1161.
- [10] HAIDER S K, JIN C, AHMAD M, et al. Advancing the state-of-the-art in hardware Trojans detection[R]. Cryptology ePrint Archive, Report.
- [11] FERN N, KULKARNI S, CHENG K T T. Hardware Trojans hidden in RTL don't cares-automated insertion and prevention methodologies[C]//2015 IEEE International Test Conference (ITC). 2015: 1-8.
- [12] FERN N, CHENG K T. Detecting hardware Trojans in unspecified functionality using mutation testing[C]//2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). 2015: 560-566.
- [13] NAHIYAN A, XIAO K, YANG K, et al. AVFSM: a framework for identifying and mitigating vulnerabilities in FSMs[C]//Proceedings of the 53rd Annual Design Automation Conference. 2016: 1-6.
- [14] KRIEG C, WOLF C, JANTSCH A, et al. Toggle MUX: how X-optimism can lead to malicious hardware[C]//2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC). 2017: 1-6.
- [15] HU W, ZHANG L, ARDESHIRICHAM A, et al. Why you should care about don't cares: exploiting internal don't care conditions for hardware Trojans[C]//2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). 2017: 707-713.
- [16] MAHMOUD D G, HU W, STOJILJOVIC M. X-attack: remote activation of satisfiability don't-care hardware Trojans on shared FPGAs[C]//2020 30th International Conference on Field Programmable Logic and Applications (FPL). 2020: 185-192.
- [17] HU W, MA Y, WANG X, et al. Leveraging unspecified functionality in obfuscated hardware for Trojan and fault attacks[C]//2019

Asian Hardware Oriented Security and Trust Symposium (Asian-HOST). 2019: 1-6.

- [18] DUBBAR C, QU G. Satisfiability don't care condition based circuit fingerprinting techniques[C]//The 20th Asia and South Pacific Design Automation Conference. 2015: 815-820.
- [19] MAO B, HU W, ALTHOFF A, et al. Quantitative analysis of timing channel security in cryptographic hardware design[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, 37(9): 1719-1732.
- [20] NARASIMHAN S, DU D, CHAKRABORTY R S, et al. Hardware Trojan detection by multiple-parameter side-channel analysis[J]. IEEE Transactions on Computers, 2012, 62(11): 2183-2195.
- [21] HU W, ARDESHIRICHAM A, GOBULUKOGLU M S, et al. Property specific information flow analysis for hardware security verification[C]//Proceedings of the International Conference on Computer-Aided Design. 2018: 1-8.
- [22] HU W, MAO B, OBERG J, et al. Detecting hardware Trojans with gate-level information-flow tracking[J]. Computer, 2016, 49(8): 44-52.
- [23] ARDESHIRICHAM A, TAKASHIMA Y, GAO S, et al. Verisketch: Synthesizing secure hardware designs with timing-sensitive information flow properties[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS). 2019: 1623-1638.

[作者简介]



武玲娟（1984-），女，河北邢台人，博士，西北工业大学研究员，主要研究方向为硬件安全与形式化安全验证。



朱嘉诚（1996-），男，江苏常州人，西北工业大学硕士生，主要研究方向为硬件安全。



唐时博（1994-），男，陕西西安人，西北工业大学博士生，主要研究方向为硬件安全。



谭静（1997-），女，安徽合肥人，西北工业大学硕士生，主要研究方向为硬件安全。



胡伟（1982-），男，湖北孝感人，博士，西北工业大学副教授，主要研究方向为硬件安全、形式化安全验证与密码学。