·动态综述·

硬件木马综述

刘华锋[1,2]，罗宏伟[2]，王力纬[2]
（1. 华南理工大学 电子与信息学院，广州 510640；
2. 工业和信息化部 电子第五研究所 电子元器件可靠性物理及其应用技术国家级重点实验室，广州 510640）

摘　要： 集成电路在设计或制造过程中会受到硬件木马的攻击，使芯片与硬件的安全性受到威胁。硬件木马技术逐渐受到重视，已成为当今一个新的研究热点。文章介绍了硬件木马的概念，对三种主要的硬件木马分类方法进行了分析；着重探讨了硬件木马的检测方法。对检测方法存在的问题与面临的挑战进行了分析，指出基于旁路信号分析的硬件木马检测方法是当前最主要的一种检测方法。

关键词： 硬件木马；集成电路；芯片安全；检测方法
中图分类号： TN406　　**文献标识码：** A　　**文章编号：** 1004-3365(2011)05-0709-05

Survey on Hardware Trojan Horse

LIU Huafeng[1,2], LUO Hongwei[2], WANG Liwei[2]
(1. *School of Electronic and Information Engineering, South China University of Technology, Guangzhou* 510640, *P. R. China*;
2. *National Key Lab. of Sci. and Technol. on Reliab. Phys. and Appl. of Elec. Compon., CEPREI, Guangzhou* 510640, *P. R. China*)

Abstract: Integrated circuits are vulnerable to hardware Trojan horse either in design or during fabrication, which threatens security of chips and hardware. The hardware Trojan horse technology has raised serious concerns and become a new research focus. The concept of hardware Trojan horse was described, and three main classifications of hardware Trojan horses were analyzed. The state-of-the-art of hardware Trojan horse detection techniques were reviewed, and problems with detection methods and major challenges to be addressed in future researches were discussed. It has been pointed out that side channel signal analysis is the most important hardware Trojan horse detection method.

Key words: Hardware Trojan horse; Integrated circuit; Chip security; Detection method
EEACC: 0170N

1　引 言

近几年来，集成电路迅速发展，半导体的制造过程逐步全球化。为了缩短集成电路的设计周期，降低制造成本，许多芯片公司采用第三方 EDA 工具，引用第三方 IP 核，并将一些芯片的制造过程转移给成本更低的第三方公司或制造厂。但是这些“第三方”并不是都能完全信任的，可能存在人为的不安全因素，甚至是竞争对手的恶意攻击与破坏。因此，怎样保证这样生产出来的芯片的可靠性和安全性变得越来越重要。并且，现在芯片的应用十分广泛，芯片的功能更强大，设计更复杂，面积更细小，工艺更先进。因此，如何高效地认证芯片，并保证芯片和硬件的可靠性与安全性，变得尤为重要。

2　硬件木马简介

硬件木马（Hardware Trojan Horse）是指插入原始电路的微小的恶意电路。这种电路潜伏在原始电路之中，在电路运行到某些特定的值或条件时，使原始电路发生本不该有的情况[1-3, 7]。这种恶意电

收稿日期：2011-01-11；定稿日期：2011-03-30

路可对原始电路进行有目的性的修改，如泄露信息给攻击者，使电路功能发生改变，甚至直接损坏电路。硬件木马能够实现对专用集成电路(ASIC)、微处理器、微控制器、网络处理器、数字信号处理器(DSP)等硬件的修改，也能实现对 FPGA 比特流等固件的修改[4, 5]。

图 1 所示是一个简单的时序同步硬件木马，也称为“时间炸弹”。木马电路由一个 k 位计数器和异或门组成，每当计数器计数到特定值(一般由攻击者预设，如 2^{K-1})时，木马就会激活，并且把原始电路中的输出 ER 修改为 ER*，从而使电路发生改变。

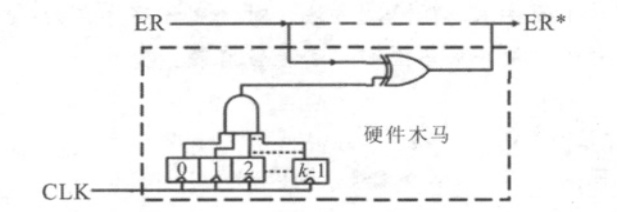

图 1 一个简单的硬件木马模型

Fig. 1 A simple model of hardware Trojan horse

在集成电路的设计和制造过程中，攻击者可采用很多方式，并且有很多机会在原始电路中植入硬件木马[5-7]。硬件木马一旦被人为隐蔽地插入一个复杂的芯片中，要检测出来是十分困难的[7-13]。第一，硬件木马通常只在非常特殊的值或条件下才能被激活并且发生作用，其他时候对原始电路的功能并无影响，它能躲过传统的结构测试和功能测试；第二，随着 IP 核重用技术的发展，系统芯片(SoC)上使用 IP 软核、IP 固核和 IP 硬核的数量增加，检测一个很小的恶意改动是极其困难的；第三，纳米级集成电路与复杂的系统很难通过物理性检测和破坏性反向工程检测出硬件木马，并且成本很高，耗时巨大，特别是当木马被选择性地插入到整体芯片中的一部分时，破坏性反向工程也不能保证剩余的集成电路没有木马；第四，由于硬件木马相对目标电路很小，工艺噪声与环境噪声使检测变得十分困难。

3 硬件木马的分类

硬件木马技术是一个相当新的研究领域，最近几年受到很大的关注。根据硬件木马的不同特性，从不同的角度将其分类，其中最为常见的分类方式有三种。

第一种分类方式比较简单，将硬件木马划分为组合型木马和时序型木马[3, 7, 13, 14]。组合型木马是指当电路的某个内部信号或节点出现特殊条件时才激活的组合电路；时序型木马是指当有限状态机(FMS)检测到某些内部电路信号状态出现特殊的序列时才激活的时序电路，如图 2 所示[14]。

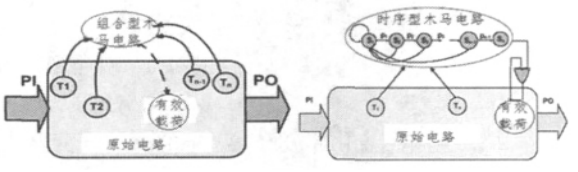

图 2 组合型木马电路(左)与时序型木马电路(右)

Fig. 2 Combinational (left) and sequential (right) Trojan horse circuits

第二种分类是将木马分为触发(也叫木马触发)和有效载荷(也叫木马有效载荷)两个主要的部分[2, 7]。触发部分就是激活木马的机制，有效载荷部分就是触发后木马发挥功能的电路。木马一触发，就会发送一个或多个信号给木马有效载荷部分，木马有效载荷部分就会工作，发生作用，从而破坏芯片或改变其功能。其中，木马触发部分可分为数字型和模拟型，数字型木马触发又可以分为组合型和时序型。同样，木马的有效载荷部分也可以分为数字型和模拟型。数字型的木马有效载荷可对电路节点的逻辑值产生影响，或改变存储单元的值。模拟型木马有效载荷一方面能影响电路的参数，如功率、噪声容限、延时；另一方面，它能在电路中产生一些多余的活动，虽然不会改变 IC 的功能特性，但是会使芯片加速老化[7]。

第三种分类是根据硬件木马的物理特性、激活特性和活动特性，将木马划分为三个主要类别[4, 5, 15]。其中，物理特性指木马在电路布局中的各种物理特征；激活特性指攻击者可能采用激活木马使其执行恶意行为的手段和策略；活动特性指木马植入电路之中可能发生的作用。因此，这种分类对定义和评估各种硬件木马的检测方法和防御策略的能力是很有用的。

物理特性分为类型、尺寸、分布、结构四个子类。其中，类型又分为功能型和参数型，功能型指那些通过增加或删减晶体管或门在物理上实现的木马；参数型是那些修改电路中已存在的线和逻辑而实现的木马。尺寸是根据木马在电路中添加、删除、或损坏芯片中的元件数量来划分的。分布是指木马在芯片的物理布局的位置。结构是指攻击者强行再生成布局，以插入木马，这会导致芯片的规格发生变化。这些变化会改变部分或所有的设计元件布局，而任何

对物理布局的恶意修改都会改变芯片的延时和功率特性，这会有利于木马的检测。

激活特性分成两类：外部激活，如通过天线或传感器与外面相互影响；内部激活，它又可以分为永久型激活和条件型激活。“永久”的意思指木马是一直都处于激活状态，可以在任何时候破坏芯片。条件型激活木马是指只有符合特定的条件时才被激活的木马。这种条件型激活木马都是通过增加芯片的逻辑门和/或触发器运行的，因此，它往往是一个组合电路或时序电路。

活动特性是根据硬件木马的破坏行为进行分类。木马的行为分为三类：修改功能、修改规格、发送信息。修改功能型是指通过增加逻辑，或删除或绕过现有的逻辑来改变芯片功能的木马。修改规格型是指以修改芯片的性能参数作为攻击重点的木马，如攻击者修改设计中的线和晶体管的几何布局而改变延迟。发送信息型是指发送关键信息给攻击者的木马。

4　硬件木马检测技术

硬件木马种类繁多，功能各异，并且植入方式也不尽相同，有的是在设计的 RTL 层插入[8]，有的是修改设计中的 IP 核[16]，有的是修改电路的 HDL 源代码[17]，风格迥异，涉及各个层次，这更加增大了检测硬件木马的难度。在过去几年中，硬件木马检测技术发展迅速，包括基于失效分析、逻辑测试以及旁路信号分析等检测方法。

最早的硬件木马检测方法是基于失效分析的方法，主要是应用成熟的失效分析技术，在所要验证的芯片中选取一部分，然后使用精密的仪器设备，如光学显微镜（SOM）、电子显微镜（SEM）、电压对比成像（VCI）、电荷诱发电压调整（CIVA）等进行失效分析[4]。然后，由扫描结果重构原始的电路设计，将反向工程设计与原始设计进行比较来判断芯片是否存在硬件木马[18]。这种方法对结构较简单的芯片的检测效果不错，但这种检测方法十分耗时，而且费用不菲，并且随着芯片的集成度越来越高，结构越来越复杂，特别是纳米技术的应用，这种检测方法往往变得无能为力[1, 4, 8, 18]。

基于逻辑测试的硬件木马检测方法需要产生测试激励，激活电路中活性很低的值和事件，特别是那些不易控制、不易察觉的节点与逻辑[14]，以便以最大的概率激活可能存在的硬件木马。这种方法是在用于 VLSI 故障测试的 ATPG 测试技术的基础上发展起来的。由于这种逻辑测试不受工艺变量和测试噪声的影响，所以能很好地检测出电路中各种小的硬件木马[7, 19]。但是，因为硬件木马的活性很低，因此穷举测试十分耗时，并且测试向量的生成比较复杂，特别是对诸如系统芯片（SoC）等大的 IC 检测是很困难的[20]。

基于旁路信号分析的硬件木马检测方法是目前使用最多、最有效的检测方法，主要是通过检测分析电路中的旁路信号，如时序、功率、电磁、热等，判断电路中是否含有木马。其中，IC 指纹法是其他基于旁路信号分析方法的基础。

4.1　基于功率信号的 IC 指纹法分析检测

基于功率信号的检测方法包括 IC 指纹法、基于局部电路的功耗分析、电流积分法以及基于电源瞬态功率的检测方法等。

IC 指纹法通过测试 IC 的功耗得到一个“指纹”，即原始 IC 的功耗特征曲线。然后，用这个 IC 指纹认证其他需要测试的芯片[1]。这种方法分为三步：1）得到原始 IC 的指纹，对原始 IC 输入高效的激励信号并进行多次测试，最大程度地运行电路，并且测量收集输出数据，分析它的功率和功能特性，并用测量的数据生成 IC 指纹；2）测试需要检测认证的怀疑含木马的同类 IC，获得此类 IC 的指纹（功耗特征曲线）；3）将原始指纹与第二步得到的指纹进行比较分析，判断它们是否有木马。

在电路功耗的测量过程中，需要考虑测量噪声、环境噪声功耗和工艺噪声的影响。虽然采取多次测量求平均可以移除测量噪声，但工艺噪声不能随机地被移除。在比较认证过程中，当木马相对芯片很小，而工艺噪声比较大时，木马功耗很容易被工艺噪声掩盖。这时，一般采用 Karhunen-Loeve 分析或功率轨迹投影法分析工艺噪声的特征向量来认证芯片是否植有木马。

如果木马较大，则认证过程相对简单。芯片的总功率等于动态功率与泄露功率之和：

$$P=\underbrace{\left(\frac{1}{2}\cdot C\cdot V_{DD}^{2}+Q_{se}\cdot V_{DD}\right)\cdot f\cdot N}_{\text{动态功率}}+\underbrace{I_{leak}\cdot V_{DD}}_{\text{泄露功率}}$$

式中，C、V_{DD}、Q_{se}是工艺参数，f 是时钟频率，N 为转换活动次数，I_{leak}为泄露电流。时钟频率 f 与动态功率呈线性关系，如果减低动态功率，并且木马较大，就可以区分原始电路与植有木马的电路的功率轨迹，从而检测出电路中是否植有木马。图 3 所示为原始的 AES 和植有木马的 AES 分别在时钟为

100 MHz（左）与 500 kHz（右）时的仿真结果。仿真显示，在工艺变量为±7%的情况下，IC 指纹法能检测出相对主电路 10%～0.01%大小的不同类型的硬件木马。

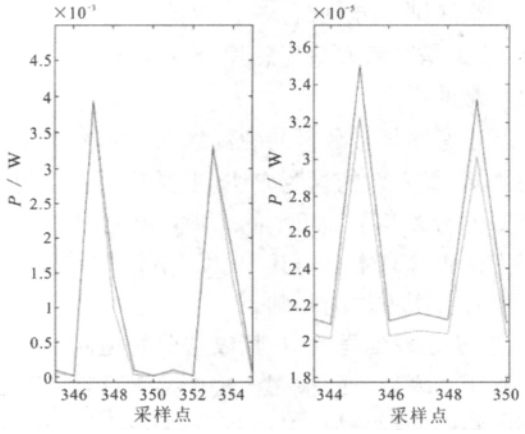

图 3 原始 AES（数值小）与植有木马的 AES（数值大）在 100 MHz（左）与 500 kHz（右）时的仿真结果

Fig. 3 Genuine (small value) and Trojan horse (large value) AES signals at 100 MHz (left) and 500 kHz (right)

4.2 基于时序信号的 IC 指纹法分析检测

基于时序信号的分析检测主要包括基于路径延迟的指纹法和基于高速延时特性的检测法。

基于路径延迟的指纹检测方法与基于功耗的 IC 指纹检测方法类似，检测方法的基本过程也相似，只是效果更好一些[9]。一个芯片会有很多延迟路径，每一个路径都代表芯片一部分的特性。所以，芯片的时序特性能生成一系列路径延迟指纹。不管木马相对整个电路来说是多么的小，它都能在路径视图里产生影响，从而可能被检测出来。完整的检测过程包括以下几个步骤：1）收集原始芯片的路径延迟；2）根据路径延迟生成指纹；3）木马检测。用相同高覆盖率的测试向量多次检测其他所有的芯片，将测试结果进行降维等相应的数据处理分析，再与原始电路的指纹比较，结果相同则认为被测试的芯片没有木马，否则就认为被测试的芯片有木马。

基于路径延迟的指纹检测方法运用统计特性分析处理工艺变量，能有效地检测出那种具有明确的有效载荷的硬件木马。但是，对隐藏着有效载荷的硬件木马的检测效果不好，并且当今的集成电路包含上百万个路径，想要测量所有的路径，特别是短路径，是不实际的。基于高速延时特性的检测法，其检测效果虽然有所改进，但是，IC 设计中有上百万的路径，这种方法要消耗很大的面积。总体来说，基于时序分析的检测效果要好于基于功率分析的检测效果，但是检测过程更加复杂。

现在，硬件木马检测技术的发展趋向于多样性和多重性。例如，采用多重激励作测试向量，以触发电路逻辑[19]，采用多重参数的旁路信号进行分析检测[20]，采用多重的稳态电流进行分析检测[22]，等等，检测效果都有改善。但是，硬件木马检测技术的难点仍然是[10, 21]：攻击者能在 IC 芯片中植入硬件木马的机会太多，对工艺变量的干扰不能有效地处理，不能全面地检测出不同芯片中的不同类型与不同大小的硬件木马，对 SoC 等复杂 IC 的检测效果不好，认证时间太长，成本太高。

除了上述基于检测方法的硬件木马检测技术外，还有一类基于硬件木马的防御策略的方法，主要是在电路中增加一些对原始设计没有影响的额外电路，甚至改变电路的设计结构，以预防和监控硬件木马，或便于硬件木马的检测。

5 结 论

近年来，硬件木马检测技术已成为一个新的研究领域，其中，基于旁路信号分析的硬件木马检测方法是当前发展最迅速，也是最重要的一种检测方法。但是，各种检测技术还不成熟，仍然存在各种不同的局限性，并且很多方法还只是停留在仿真阶段和实验阶段，并没有真正应用于实际工程之中。虽然基于旁路信号分析的方法是目前发展最好的硬件木马检测方法，能有效地检测出各种大的木马，但其容易受到工艺变量和测试噪声的影响，对小的木马的检测效果不理想；而逻辑检测方法不受工艺噪声的影响，能有效地检测出各种小的木马，但是测试向量生成很复杂，对大的木马的检测效果不够理想。所以，两种方法具有互补作用。同时，由于硬件木马植入方式的灵活性和自身的隐蔽性，很难通过单一的检测方法检测出各种未知的恶意电路。随着半导体芯片设计与制造的全球化，以及集成电路在军用和民用领域的广泛使用，保证芯片的安全性和可靠性变得举足轻重。开发新的硬件木马检测技术，或融合各种检测方法的优点，研究出像杀毒软件一样的通用而有效的检测方法或工具，仍是一个充满挑战的艰辛过程，但值得期待。

参 考 文 献：

[1] AGRAWAL D, BAKTIR S, KARAKOYUNLU D, et

al. Trojan detection using IC fingerprinting [C] // 2007 IEEE Symp Security and Privacy. Oakland, CA, USA. 2007: 296-310.

[2] WOLFF F, PAPACHRISTOU C, BHUNIA S, et al. Towards Trojan-free trusted ICs: problem analysis and detection scheme [C] // Automation and Test in Europe Conf. Munich, Germany. 2008: 1362-1365.

[3] BANGA M, HSIAO M. A novel sustained vector technique for the detection of hardware Trojans [C] // Int Conf VLSI Design. New Delhi, India. 2009: 327-332.

[4] WANG X, TEHRANIPOOR M, PLUSQUELLIC J. Detecting malicious inclusions in secure hardware: challenges and solutions [C] // IEEE Int Workshop HOST. Anaheim, CA, USA. 2008: 15-19.

[5] TEHRANIPOOR M, KOUSHANFAR F. A survey of hardware Trojan taxonomy and detection [J]. IEEE Design & Test of Computers. 2010, 27(1): 10-25.

[6] DARPA. Trust in integrated circuits (TIC) -proposer information pamp [EB/OL]. http://www.darpa.mil/MTO/ solicitations/baa07-24/index.html, 2008.

[7] RAJAT S C, SEETHARAM N, SWARUP B. Hardware Trojan: threats and emerging solutions [R]. 2009: 166-171.

[8] JIN Y, KUPP N, MAKRIS Y. Experiences in hardware Trojan design and implementation [C] // IEEE Int Workshop HOST. San Francisco, CA, USA. 2009: 50-57.

[9] JIN Y, MAKRIS Y. Hardware Trojan detection using path delay fingerprint [C] // IEEE Int Workshop HOST. Anaheim, CA, USA. 2008: 51-57.

[10] ALKABANI Y, KOUSHANFAR F. Consistency-based characterization for IC Trojan detection [C] // IEEE/ACM Int Conf Comp Aid Des. San Jose, CA, USA. 2009: 123-127.

[11] TEHRANIPOOR M, SUNAR B. Hardware Trojan horses [EB/OL]. http://www.springerlink.com/content/r1h6518 t98x10411, 2010.

[12] SALMANI H, TEHRANIPOOR M, PLUSQUELLIC J. New design strategy for improving hardware Trojan detection and reducing Trojan activation time [C] // IEEE Int Workshop HOST. San Francisco, CA, USA. 2009: 66-73.

[13] BANGA M, MICHAEL S H. A region based approach for the identification of hardware Trojans [C] // IEEE Int Workshop HOST. Anaheim, CA, USA. 2008: 40-47.

[14] CHAKRABORTY R S, PAUL S, BHUNIA S. On-demand transparency for improving hardware Trojan detectability [C] // IEEE Int Workshop HOST. Cleveland, OH, USA. 2008: 48-50.

[15] RAD R M, WANG X X, MOHAMMAD T, et al. Power supply signal calibration techniques for improving detection resolution to hardware Trojans [C] // Int Conf Comp Aid Des. San Jose, NJ, USA. 2008: 632-639.

[16] KING S T, TUCEK J, COZZIE A, et al. Designing and implementing malicious hardware [C] // Proc 1st Usenix Workshop Large-Scale Exploits and Emergent Threats. San Francisco, CA, USA. 2008: 1-8.

[17] ALKABANI Y, KOUSHANFAR F. Active hardware metering for intellectual property protection and security [C] // Proc 16th Usenix Security Symp. Berkeley, CA, USA. 2007: 291-306.

[18] SANNO B. Detecting hardware Trojans [EB/OL]. http://www.crypto.rub.de/imperia/md/content/seminare/itsss09/benjamin_sanno.semembsec_termpaper_20090723_final.pdf, 2009.

[19] CHAKRABORTY R S, WOL F, PAUL S, et al. MERO: a statistical approach for hardware Trojan detection [C] // CHES Workshop. Lausanne, Switzerland. 2009: 396-410.

[20] LI J, LACH J. At-speed delay characterization for IC authentication and Trojan horse detection [C] // IEEE Int Workshop HOST. Anaheim, CA, USA. 2008: 8-14.

[21] NARASIMHAN S, DU D D, WOLFF F, et al. Multiple-parameter side-channel analysis: a non-invasive hardware Trojan detection approach [C] // IEEE Int Symp HOST. San Diego, CA, USA. 2010: 13-18.

[22] AARESTAD J, ACHARYYA D, RED R, et al. Detecting Trojans through leakage current analysis using multiple supply pad IDDQs [C] // IEEE Symp Security and Privacy. Oakland, CA, USA. 2010: 159-172.

作者简介：

刘华锋(1986—)，男(汉族)，湖南株洲人，硕士研究生，目前主要从事硬件木马电路的设计与检测研究。

罗宏伟(1968—)，男(汉族)，湖南长沙人，研究员高级工程师，目前主要从事微电子和半导体器件的可靠性研究。

王力纬(1982—)，男(汉族)，湖南冷水江人，高级工程师，目前主要从事微电子和半导体器件的可靠性研究。