

用于硬件木马检测的电磁辐射分析方法研究

唐永康, 胡星, 苏颀, 李少青

(国防科技大学计算机学院, 湖南 长沙 410073)

摘要: 随着集成电路产业全球化的发展, 硬件木马已成为集成电路的主要安全威胁之一。目前能较好权衡检测成本与检测能力的侧信道分析方法越来越受到研究人员的关注, 其中, 电磁辐射分析方法是研究热点之一。重点分析并验证电磁辐射分析方法对硬件木马的检测能力, 并探究限制其检测性能的原因。在现场可编程逻辑门阵列(FPGA)上进行验证实验, 实验结果表明, 电磁辐射分析方法可以很好地检测电磁辐射频率分布独特的硬件木马电路, 但无法适用于电磁辐射频率分布复杂的硬件木马。

关键词: 检测能力评估; 电磁辐射; 硬件木马检测; 侧信道分析

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021030

Research on electromagnetic radiation based side-channel analysis method for hardware Trojan detection

TANG Yongkang, HU Xing, SU Ting, LI Shaoqing

College of Computer, National University of Defense Technology, Changsha 410073, China

Abstract: With the globalization of the integrated circuit industry, hardware Trojan is becoming the main threat to integrated circuits. At present, the side-channel analysis which can make a good trade-off between detection ability and cost, has attracted more attention from the academia. The side-channel analysis method based on electromagnetic radiation is one of the hotspots in hardware security field. The ability evaluation of electromagnetic radiation analysis method to detect hardware Trojan was focused, and the factor that limited their detection performance was explored. The experimental results on FPGA show that the electromagnetic radiation analysis method can effectively detect hardware Trojan whose electromagnetic radiation distribution is significantly different from surrounding circuits, but it cannot be applied to hardware Trojan with complex frequency distribution of electromagnetic radiation.

Keywords: detection ability evaluation, electromagnetic radiation, hardware Trojan detection, side-channel analysis

收稿日期: 2020-11-16; 修回日期: 2021-03-01

通信作者: 苏颀, suting@nudt.edu.cn

基金项目: 国家自然科学基金重点项目(61832018)

Foundation Item: The Key Program of National Natural Science Foundation of China (61832018)

论文引用格式: 唐永康, 胡星, 苏颀, 等. 用于硬件木马检测的电磁辐射分析方法研究[J]. 网络与信息安全学报, 2021, 7(2): 43-56.

TANG Y K, HU X, SU T, et al. Research on electromagnetic radiation based side-channel analysis method for hardware Trojan detection[J]. Chinese Journal of Network and Information Security, 2021, 7(2): 43-56.

1 引言

集成电路(IC, integrated circuit)已成为金融、通信与军事等信息领域的重要硬件支撑,但其也面临着诸多硬件安全威胁。硬件木马^[1]是为实现对IC关键信息的修改与监控而对IC原始电路进行的恶意篡改,其已成为多方关注的焦点。而随着IC设计复杂度的日益增长,IC设计者们不得不使用第三方知识产权核缓解设计压力;同时由于经济、技术能力的限制,大部分设计团队只能将设计好的IC数据交由第三方代工厂生产。因此,一些恶意的知识产权核供应商与代工厂可以很轻易地将硬件木马电路植入IC中。不同于传统安全威胁,硬件木马直接以硬件的形式实现,一旦植入IC中就无法移除,被感染的IC必须被弃用。因此硬件木马的隐蔽性与威胁程度极高,必须对其进行防护。

学术界为应对硬件木马威胁进行了大量的研究,包括逆向工程^[2]、功能测试^[3]以及侧信道分析^[1,4-14]等。其中,侧信道分析方法已被证明可以通过采集、分析IC工作时产生的功耗、电磁辐射以及红外图像等信息有效地实现硬件木马检测。

Agrawal等^[1]在2007年提出将侧信道分析应用到硬件木马检测中。随后,电磁辐射分析方法被提出并逐渐成熟,侧信道分析也成为最热门的硬件木马检测方法之一。电磁辐射分析方法通过比较目标IC与可信参考(纯净母本IC^[1]或寄存器传输级设计数据^[8]等)的电磁辐射差异以实现硬件木马检测。文献[4, 9-10]直接在时域上分析被测IC与母本IC电磁辐射强度曲线的绝对差异来识别被感染的IC。Chen等^[6]将二维主成分分析应用于电磁辐射强度数据分析,并使用反向传播神经网络实现硬件木马检测。该方法可以检测占宿主电路0.31%以上规模的硬件木马。He等^[7]提出在频域上比较电磁辐射分布仿真曲线与实际电磁辐射曲线的特定频率点可以实现硬件木马检测,基于该方法其成功检测了Trust-Hub中11种不同的硬件木马。文献[8]使用神经网络进一步提升了此方法的检测能力。现有研究已证明电磁辐射分析方法可以用于硬件木马检测,但它们没有探究

具有何种特征的硬件木马可以被电磁辐射分析检测,且并未讨论该类方法的局限性。

研究局限性就必须分析限制侧信道分析检测性能的主要因素:噪声。微弱的硬件木马信号极易被各种类型的噪声(测量噪声、环境噪声、工艺偏差和其他随机噪声)所掩盖^[1]。分析电磁辐射分析实现硬件木马检测过程中的噪声对研究该类方法的局限性具有重要意义。但是,现有文献对电磁辐射分析时的噪声模型考虑并不完整,并且其对噪声的分类未考虑电磁辐射的特性。

本文将针对电磁辐射分析方法,研究其用于硬件木马检测的有效性与局限性,分析其可以有效检测具有何种特征的硬件木马以及不适用于何种场景下的硬件木马检测。本文将首先介绍电磁辐射分析方法实现硬件木马检测的物理机理;然后,分析电磁辐射分析过程中所有可能的噪声源,完善噪声模型,并结合各噪声的异同点与电磁辐射分析的特点提出专用噪声模型;接着,在分析模型中各类噪声对检测的影响形式与程度的基础上讨论电磁辐射分析方法的有效性 with 局限性;最后,将在现场可编程逻辑门阵列(FPGA, field programmable gate array)中验证评估电磁辐射分析方法的有效性 with 局限性。目前还未有相关工作研究电磁辐射分析的专用噪声模型,并系统地分析评估该类方法的检测能力。本文的贡献如下。

(1) 基于电磁辐射分析方法检测硬件木马的物理机理,提出专用于电磁辐射分析的噪声模型。

(2) 分析噪声模型中各类噪声的干扰形式与影响程度,并讨论电磁辐射分析可以有效检测的硬件木马的特征以及电磁辐射分析方法的局限性。

(3) 在FPGA上验证了电磁辐射分析方法的检测有效性和局限性。实验结果表明,电磁辐射侧信道分析方法可以很好地检测电磁辐射频率分布独特的硬件木马,但无法适用于电磁辐射频率分布复杂的硬件木马。

2 研究背景

本节主要介绍电磁辐射分析方法检测硬件木马的物理机理,并回顾现有的电磁辐射分析方法。

2.1 检测物理机理

电磁辐射分析的基本理论是麦克斯韦方程^[15]，其中描述电磁转换和磁电转换过程的部分方程如下：

$$\oint_L \mathbf{E} \cdot d\mathbf{l} = - \iint_S \frac{\partial \mathbf{B}}{\partial t} \cdot d\mathbf{S} \quad (1)$$

$$\oint_L \mathbf{H} \cdot d\mathbf{l} = \iint_S \frac{\partial \mathbf{D}}{\partial t} \cdot d\mathbf{S} \quad (2)$$

其中， $\mathbf{B}$ 和 $\mathbf{H}$ 是磁通密度和磁场强度， $\mathbf{E}$ 和 $\mathbf{D}$ 是电场强度和电位移。

根据电位移的定义和 Biot-Savart 定律， $\mathbf{B}$ 和 $\mathbf{D}$ 分别由式(3)、式(4)给出。

$$\mathbf{B} = \frac{\mu_0}{4\pi} \int_L \frac{Id\mathbf{l} \cdot \mathbf{r}}{r^3} \quad (3)$$

$$\mathbf{D} = \varepsilon_r \varepsilon_0 \mathbf{E} \quad (4)$$

可以看到，电磁辐射是电流 (I) 的结果，并且与其频率有关。电磁辐射有两个重要特征：辐射强度和频率分布。因此，有两种不同的硬件木马检测思路，即在时域上分析待测 IC 的电磁辐射强度或在频域上分析其电磁辐射频率分布。同时，IC 中每个电路块的电流强度和工作频率不尽相同，这就导致整个 IC 的电磁辐射信息量巨大^[16]。因此，大部分方法会对 IC 进行分块，并在不同区域分别进行电磁辐射采集与分析^[10]。

从本质上来说硬件木马也是电路，其工作时同样会产生相应的电磁辐射强度和频率分布。在第三方代工厂或不可信知识产权核供应商向 IC 中植入硬件木马后，被感染区域内部电路工作时，电流特征将被改变，进而改变该区域的电磁辐射信息。这种变化可以被近场电探针^[16]或磁探针^[17]捕捉到。通常，硬件木马由触发逻辑和工作逻辑两部分组成，而只有触发逻辑会始终工作以判断触发信号是否出现并触发工作电路。因此，本文主要关注触发逻辑所产生的电磁辐射信息。

2.2 现有研究

Soll 等^[10]提出了一种基于待测 IC 的电磁辐射检测硬件木马的技术，将 IC 划分为多个区域，并成功地检测到了占 128 位 AES (advanced encryption standard) 电路规模 0.68% 的硬件木马。但是，该检测方法仅关注每个区域的电磁辐射强度，检测容易受到工艺偏差和电磁辐射干扰

(EMI, electromagnetic interference) 的影响。当硬件木马位于不同区域时 EMI 可能导致检测性能的差异。

随后 Balasch 等^[4]也参考上述方法实现了硬件木马检测。证明了该方法能够检测到占 AES 面积 1.3% 的硬件木马，但当木马的占比从 1.3% 降低到 0.1% 时，该方法就将无法实现检测。Ngo 等^[9]的研究表明，使用电磁辐射分析方法，检测到占原始电路面积 0.5%、1% 和 1.7% 的硬件木马的成功率分别为 74%、83% 和 95%。Chen 等^[6]进一步提出，二维主成分分析可以抑制电磁辐射强度曲线比较过程中噪声的影响，并提升检测的精度。该方法检测到占宿主电路规模 1.38% 以上的时序型硬件木马的成功率大于 88%，检测占比大于 0.31% 的组合格硬件木马的成功率大于 78%。王品等^[18]提出以高斯滤波的方式抑制木马芯片和非木马芯片差分电磁辐射信号中的噪声部分，并使用 K 最邻近算法对二者进行区分。该方法能以 90% 的准确率检测面积占宿主电路 0.76% 的硬件木马。

He 等^[7]应用空间投影变换的思想，将电磁辐射强度曲线从时域转换到频域，并比较特定频率点。该方法可以应对工艺偏差的影响，同时他们没有采用纯净母本芯片作为参考，而利用芯片设计数据进行电磁辐射的仿真作为硬件木马检测的纯净参考，成功地检测到了 Trust-Hub 中 11 种不同的硬件木马。为提高其方法的性能，将神经网络应用于被感染 IC 的识别^[8]，该方法的平均检测成功率高达 89.2%。但该方法关注的是待测 IC 的全局电磁辐射，并且这种仿真方法忽略了一些重要的噪声因素，如 EMI 噪声。

Supon 等^[19]与 He 等^[20]采用片上电磁传感器采集芯片的电磁辐射信息以实现硬件木马检测。该类方法已验证可以在 128 位 AES 中检测到 4 种不同类型的硬件木马^[20]，但他们同样没有将检测过程中的噪声模型考虑完全，并且添加电磁传感器可能会影响芯片性能。

综上所述，现有研究仅基于硬件木马的规模或触发逻辑类型来评估方法的检测能力，并未深入考虑其可检测的硬件木马的本质特性。并且现有方法进行检测时考虑的噪声模型并不完整，尤

其并未将周围电路对电磁辐射分析的影响考虑在内。而一些电磁辐射信息与周围普通电路类似的硬件木马很可能被隐藏在 EMI 噪声中,如果采取最高级的降噪方法消除 EMI 噪声,那么隐藏在其中的硬件木马信号也会随之被消减,这对分析评估电磁辐射分析方法的有效性和局限性是不利的。因此不同于现有的研究,本文将针对电磁辐射分析方法的特性建立专门的噪声模型,以全面分析影响硬件木马检测性能的潜在噪声因素。并通过分析不同噪声的干扰形式与影响程度研究电磁辐射分析方法的有效性与局限性。

3 噪声分析

本节首先分析硬件木马检测过程中的噪声源,并简单介绍这些噪声的特征;然后建立专用于电磁辐射分析的噪声模型;最后讨论这些噪声对硬件木马检测的影响。

3.1 噪声模型

由第 2 节的分析可知,电磁辐射分析可以用于检测硬件木马,但其检测性能容易受到各种类型噪声的影响。如图 1 所示,电磁辐射分析过程中噪声通常来自 3 个不同的阶段:电磁辐射采集阶段、IC 制造阶段以及 IC 工作阶段。

首先,在 IC 制造阶段,工艺偏差是主要噪声源。工艺偏差是 IC 制造时由于晶体管和金属线尺寸的细微不同而导致的制造偏差。文献[21]将工艺偏差分为片间偏差和片内偏差两类,分别代表两个同批次 IC 间的差异以及同一 IC 中两个晶体管间的差异。随着 MOS 晶体管的特征尺寸减小,越来越难以精确控制 IC 的制造过程[22]。而 MOS 管阈值电压和沟道长度的变化将影响电路的工作电流[23],从而影响其电磁辐射信息。因此在比较

待测 IC 与可信参考之间的电磁辐射时,硬件木马信号可能被工艺偏差造成的噪声所掩盖。

然后,采集 IC 电磁辐射时的噪声主要包括环境噪声和设备噪声。其中环境噪声主要来自宇宙噪声和大气噪声[24],它们服从正态分布,并且功率频谱密度在频谱中近似均匀分布;电磁辐射采集设备中的主要噪声源包括热噪声[25]、散粒噪声[26]、闪烁噪声和量化噪声。其中热噪声、散粒噪声以及闪烁噪声存在于所有电子设备中。由示波器中的模数转换电路(ADC)引起的一系列量化误差被称为量化噪声[27]。

最后,在 IC 工作时除了热噪声与闪烁噪声等随机噪声外,EMI 是最主要的噪声源[17]。这是因为 IC 中每个电路模块不仅会产生自己的电磁辐射,还会通过电路结构和耦合影响其他电路模块的辐射[8]。因此,IC 各区域的电磁辐射信息可能会受到周围电路的极大干扰。文献[4,10]中的实验结果表明,如果将硬件木马放置在某些大功率电路旁,那么该硬件木马的电磁辐射将会被掩盖。虽然一些规模庞大的硬件木马也可能影响周围电路的电磁辐射,从而更容易被检测到。但实际中,硬件木马的电磁辐射信号通常非常微弱,因此 EMI 是电磁辐射分析时最主要的噪声之一。

通过以上分析,首先可以将电磁辐射分析过程中的噪声分为:环境噪声($N_{\text{环境}}$)、设备噪声($N_{\text{设备}}$)、EMI 噪声(N_{EMI})、工艺偏差噪声($N_{\text{工艺}}$)以及一些其他随机噪声($N_{\text{其他}}$)。由于这些噪声是加性噪声[24],因此电磁辐射分析过程中的噪声模型可以表示为

$$N_{\text{total}} = N_{\text{环境}} + N_{\text{设备}} + N_{\text{EMI}} + N_{\text{工艺}} + N_{\text{其他}} \quad (5)$$

其中, N_{total} 代表电磁辐射分析过程中的所有噪声。

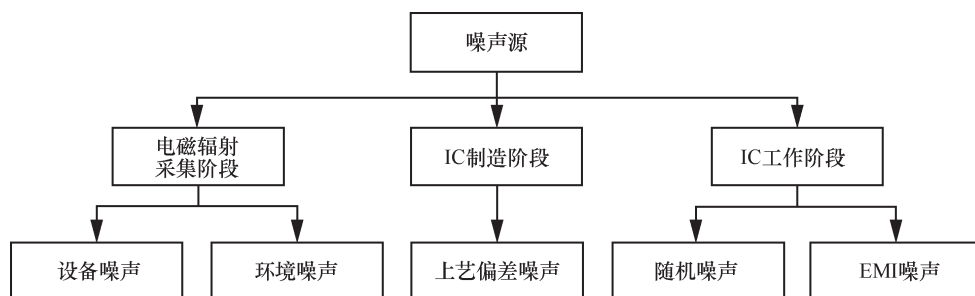


图 1 噪声源类型

Figure 1 Types of noise sources

然后，基于电磁辐射分析的特性对噪声进行分类、合并。本文将从时域上的电磁辐射强度和在频域上的频率分布来考虑这5种噪声的异同。

本文将环境噪声、设备噪声和一些随机噪声合并为底噪（ $N_{\text{底噪}}$ ）。因为它们在时域、频域中的分布明确，因此可以通过降噪算法将它们的影响控制在很小的范围内。由于EMI噪声和工艺偏差噪声在时域上对电磁辐射分析的影响很大，但在频域上的分布存在不同，因此本文将它们单独进行考虑。在频域上，EMI噪声的分布由于周围电路不同而发生变化。而IC生产后，其工艺偏差已经确定，由工艺偏差引起的电磁辐射变化将主要发生在0 Hz附近。因此噪声模型应修改为

$$N_{\text{total}} = N_{\text{底噪}} + N_{\text{EMI噪声}} + N_{\text{工艺偏差}} \quad (6)$$

对于电磁辐射分析来说，将待测IC的实际电磁辐射与可信参考进行比较是最关键的步骤之一。基于噪声模型可以给出正常情况下（ $S_{\text{正常}}$ ）和被硬件木马感染时（ $S_{\text{感染}}$ ），IC电磁辐射的信号-噪声模型，如下所示。

$$S_{\text{正常}} = S_{\text{电路}} + S_{\text{底噪}} + S_{\text{EMI噪声}} + S_{\text{工艺偏差}} \quad (7)$$

$$S_{\text{感染}} = S_{\text{电路}} + S_{\text{底噪}} + S_{\text{EMI噪声}} + S_{\text{工艺偏差}} + S_{\text{硬件木马}} \quad (8)$$

$S_{\text{电路}}$ 与 $S_{\text{硬件木马}}$ 分别是正常电路与硬件木马工作产生的电磁辐射。 $S_{\text{底噪}}$ 、 $S_{\text{EMI噪声}}$ 和 $S_{\text{工艺偏差}}$ 分别表示由底噪、EMI噪声和工艺偏差噪声造成的影响。

如前所述，由于噪声的随机性， $S_{\text{正常}}$ 和 $S_{\text{感染}}$ 进行比较时二者之间的差异可以表示为

$$\Delta S_{\text{差异}} = \Delta S_{\text{底噪}} + \Delta S_{\text{EMI噪声}} + \Delta S_{\text{工艺偏差}} + S_{\text{硬件木马}} \quad (9)$$

其中， $\Delta S_{\text{差异}}$ 表示两个信号之间的总体差异， $\Delta S_{\text{底噪}}$ 、 $\Delta S_{\text{EMI噪声}}$ 和 $S_{\text{工艺偏差}}$ 是各噪声引起的差异。

3.2 噪声影响分析

要实现硬件木马信号的检测，必须使其硬件木马的电磁辐射信号摆脱噪声的干扰。实现此目标的最有效方法是噪声抑制，这也是电磁辐射分析检测硬件木马的必要步骤。但实际上，硬件木马信号与某些噪声之间可能存在一定的联系，从而使在抑制噪声的同时，削弱硬件木马的电磁辐射。因此，需要分析模型中各类噪声对检测的影响形式与程度，并探究它们与硬件木马信号间是否可能存在联系。

(1) 底噪

由3.1节的分析可知，底噪的各组成部分在时域上都服从正态分布。本文对底噪的实际电磁辐射数据进行了采集验证。图2是采集到的数据（100组）中某一组的概率密度函数（PDF，probability density function）。红色曲线是由实际数据的均值和标准差建立的理想正态分布PDF，蓝色曲线是实际数据的PDF，两条曲线匹配度较高。同时，本文使用Jarque-Bera检验^[28]对正态分布进行了拟合优度检验，数据通过Jarque-Bera检验的概率为75%，因此可将底噪影响视为正态分布。

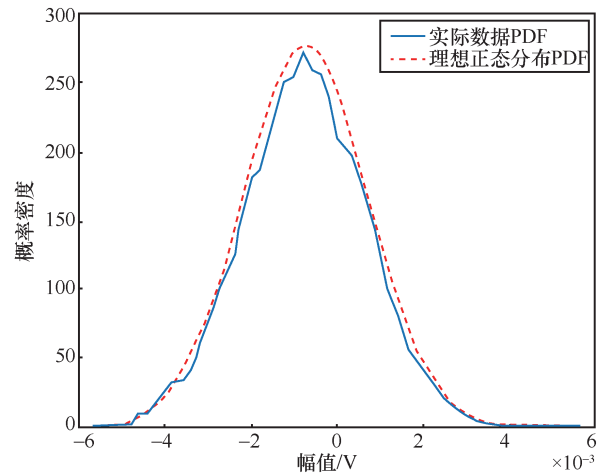


图2 底噪概率密度函数
Figure 2 Probability density function of background noise

根据以上特性，可以使用简单的均值滤波方法消除底噪的影响。即采用取多次连续采样后平均值的方法或者直接使用示波器内置的均值算法来实现降噪。降噪结果如图3所示，蓝色曲线代表底噪的原始数据，红色曲线是均值滤波降噪的结果。结果表明，即使采用最简单的降噪方法，也可以很好地抑制底噪。

虽然均值滤波是最简单有效的降噪方法，但该方法无法描述实际电磁辐射信号的非平稳特性，这意味着在其降噪电磁辐射时会丢失一些细节。因此，在验证评估电磁辐射分析方法的检测能力时，应使用更合适的降噪方法来更好地处理原始数据。此时，更青睐于使用在非平稳信号处理中应用广泛的小波滤波^[29]。小波滤波的基本理论是连续小波变换，表示如下：

$$W(a, \tau) = \int_{-\infty}^{+\infty} S(t) \psi_{a, \tau}(t) \cdot dt \quad (10)$$

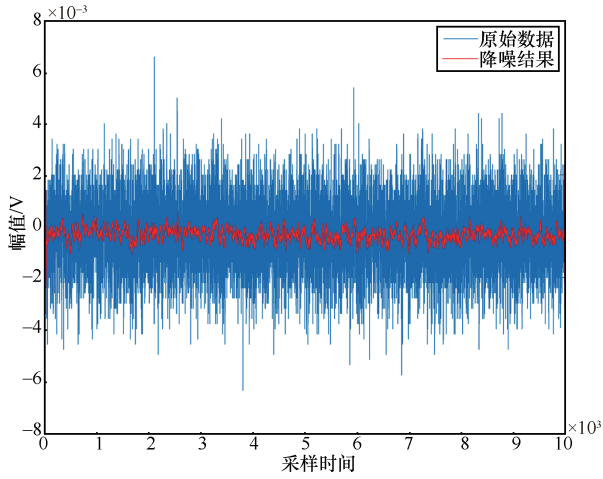


图 3 均值滤波降噪结果
Figure 3 The result of mean filtering

$$\psi_{a,\tau}(t) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-\tau}{a}\right) \quad (11)$$

其中, $S(t)$ 是待测信号, $\psi_{a,\tau}(t)$ 是具有出色的时频局部性的小波基函数。根据不同的待测信号调整参数 a 和 τ 可分析信号更多的细节。

使用小波函数的线性组合近似原始信号可以将该信号分解为多个频率段信号分量, 噪声通常存在高频分量中。根据阈值选择性处理高频分量后可以将信号重构为降噪信号^[26]。小波滤波可以根据信号的频率特性抑制噪声, 并保留目标信号的更多特征, 因此更适合电磁辐射信号分析。

(2) 工艺偏差噪声

电磁辐射分析方法对硬件木马的检测很容易受到工艺偏差的影响, 但受经济成本的限制, 无法通过实际实验检验工艺偏差对检测的影响。因此, 只能通过蒙特卡洛模型^[23,31]来进行工艺偏差的仿真实验。本文将 IC 分为 961 个电路块, 每个模块由相同的 AES 部分电路组成。在 Hspice 中, 仿真了工艺偏差噪声的影响。图 4 是 130 nm 工艺下的 IC 受工艺偏差噪声影响的电磁辐射仿真, 颜色深度代表电磁辐射的强度。同时, 随着制造工艺的提升, 工艺偏差噪声对电磁辐射强度的影响只会越来越大。因此, 对于时域上的电磁辐射强度分析, 工艺偏差噪声的影响将非常大。但理论上工艺偏差噪声几乎不会影响频域中的电磁辐射分析, 其原因如下。

IC 某电路模块的电磁辐射信号可由动态分

量 ($S_{\text{动态}}(t)$) 和静态分量 ($S_{\text{静态}}$) 的组合来描述:

$$S = S_{\text{动态}}(t) + S_{\text{静态}} \quad (12)$$

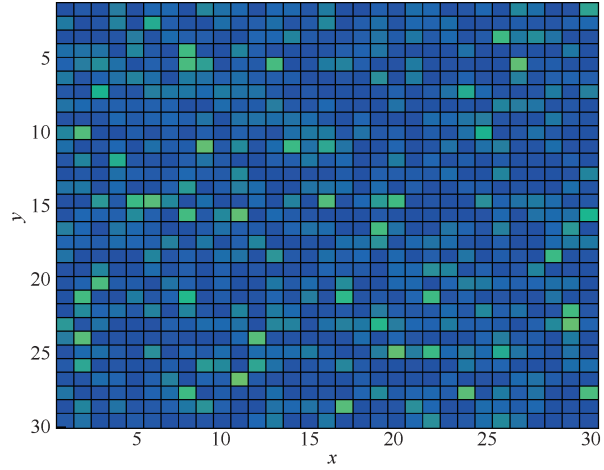


图 4 工艺偏差对电磁辐射强度的影响
Figure 4 The electromagnetic radiation intensity under process variation

在分析电路模块的电磁辐射强度时, 一般会在时域中对电磁辐射强度取均值, 此时主要关注静态分量部分。在对电磁辐射信号应用快速傅立叶变换 (FFT) 后可以将其变换到频域, 如式(13)所示。

$$F(S) = F(S_{\text{动态}}(t)) + F(S_{\text{静态}}) = \sum_{k=1}^n X_{\text{动态}}(f_k) + X_{\text{静态}}(f_0) \quad (13)$$

其中, $\sum_{k=1}^n X_{\text{动态}}(f_k)$ 和 $X_{\text{静态}}(f_0)$ 是 $S_{\text{动态}}(t)$ 和 $S_{\text{静态}}$ 在频域中的对应表达式。目标信号的频率分别为 $f_k, f_{k-1}, \dots, f_1$ 和 f_0 。显然静态分量的频率 (f_0) 为 0 Hz。

工艺偏差主要影响电磁辐射的强度, 并会引入一定的时延 (Δt)。二者将分别反映在信号的静态分量与动态分量中。工艺偏差噪声的电磁辐射信号 ($S_{\text{工艺偏差}}$) 可表示为

$$S_{\text{工艺偏差}} = \alpha S_{\text{动态}}(t + \Delta t) + \beta S_{\text{静态}} \quad (14)$$

$$F(S_{\text{工艺偏差}}) = F(\alpha S_{\text{动态}}(t + \Delta t)) + F(\beta S_{\text{静态}}) \quad (15)$$

其中, α 和 β 代表电磁辐射强度的影响因子。

根据傅立叶变换的性质有:

$$F(\alpha S_{\text{动态}}(t + \Delta t)) = \alpha \sum_{k=1}^n X_{\text{动态}}(f_k) e^{-j f_k \Delta t} \quad (16)$$

$$F(\beta S_{\text{静态}}) = \beta X_{\text{静态}}(f_0) \quad (17)$$

$$F(S_{\text{工艺偏差}}) = \alpha \sum_{k=1}^n X_{\text{动态}}(f_k) e^{-j f_k \Delta t} + \beta X_{\text{静态}}(f_0) \quad (18)$$

其中 $|e^{-j f_k \Delta t}| = 1$ ，这表明 Δt 不会影响实数域中的频率分析。

综上所述，工艺偏差噪声的影响主要发生在 0 Hz 附近，不会改变 IC 的电磁辐射特征频率分布，并且其对信号幅度改变很小，不会影响频域上的硬件木马检测。

(3) EMI 噪声

对 EMI 噪声的研究需要分析干扰的产生原理。由文献[8,10]可知，EMI 主要由待测区域附近其他电路模块的载流元件工作引起电磁辐射干扰。图 5 是 EMI 噪声产生原理，中心处的电路块代表待测区域，其周围其他电路块会产生相应的 EMI 噪声。

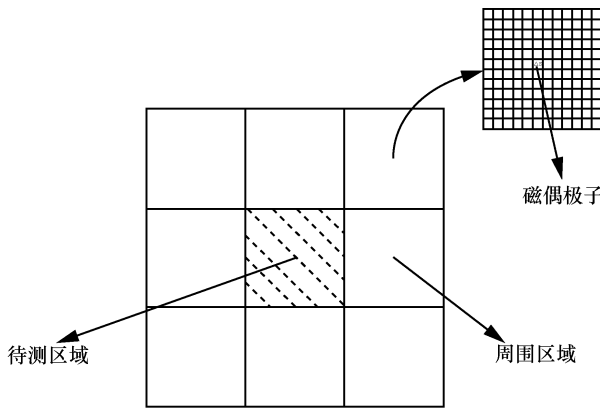


图5 EMI 噪声产生原理
Figure 5 Physical mechanism of EMI noise

分析 EMI 时最重要的概念是电偶极子和磁偶极子^[15]，可以认为 EMI 主要由它们产生。它们的分析方法相似，所以本文以磁偶极子为例进行分析。图 5 中待测区域周围的每个电路模块都由许多磁偶极子组成。磁偶极子影响空间中特定点 (P) 的原理如图 6 所示，其可表示为

$$\Delta B = \frac{\mu_0 m}{4\pi r^3} (2r \cos \theta + \theta \sin \theta) \quad (19)$$

其中， m 是磁偶极矩^[15]，可以由下式给出：

$$m = I \Delta S \quad (20)$$

然后，上述等式将转化为

$$\Delta B = \frac{\mu_0 I \Delta S}{4\pi r^3} (2r \cos \theta + \theta \sin \theta) \quad (21)$$

其中， ΔB 是由一个磁偶极子引起的磁通量。 r 和是基于球坐标的方向向量。 θ 是近场探头和磁偶极子之间的角度。因此 $2r \cos \theta + \theta \sin \theta$ 仅代表磁场的方向。 μ_0 是真空的磁导率。由此可得，决定磁偶极子 EMI 的主要参数是电流、电路面积以及磁探针与磁偶极子之间的距离。

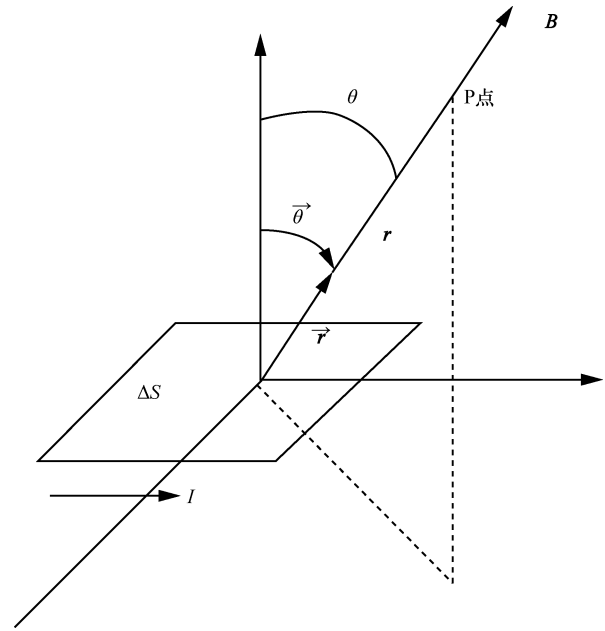


图6 磁偶极子对 P 点的影响
Figure 6 The effect on point P

因此，待测区域周围的总 EMI 噪声 (B) 可以由下式给出：

$$B = \sum \frac{\mu_0 I S}{4\pi r^3} (2r \cos \theta + \theta \sin \theta) \quad (22)$$

e 由待测区域周围的电路块数量决定， S 代表每个电路块的面积。

综上，EMI 噪声的主要由各电路块的电流和面积、磁探针和磁偶极子之间的距离以及电路块的数量所决定。EMI 噪声是不可避免的，而且很难消除，因此，本文将此噪声视为限制电磁辐射分析方法检测精度的最主要因素。

4 检测能力分析

上一节讨论了电磁辐射分析过程中主要的噪声以及它们的影响形式。由以上分析可知，在时

域上分析电磁辐射强度检测硬件木马的干扰因素远比频域上复杂,因此本节将主要讨论在频域上分析电磁辐射频率检测硬件木马的有效性与局限性。

4.1 有效性分析

如果要想实现硬件木马信号的检测,必须将硬件木马信号与噪声进行区分。在频域上则为:找出硬件木马信号与噪声的电磁辐射频率分布存在的差异。而在对电磁辐射信号进行降噪处理后,频域中的主要噪声为周围电路工作产生的 EMI 噪声。在决定 EMI 噪声的 4 个主要因素中,各电路块的面积对于同种 IC 来说是相同的,并且磁探针和待测 IC 之间的位置是相对固定的。而实际 IC 中不同电路块工作时电流变化频率不尽相同,因此随着电路块数量的增加,EMI 噪声的频率分布会越发复杂。但是,当电路正常工作时,它们的频率分布相对固定。因此,要在频域上有效地检测硬件木马至少需要满足以下两个条件之一:硬件木马的电磁辐射的频率分布与 EMI 噪声存在明显的不同;硬件木马的电磁辐射影响足够大。

由 3.2 节的分析可知,EMI 噪声是由周围普通电路工作产生的。因此,对于采用与普通电路有明显不同的特殊电路结构(如采用模拟电路设计等)或工作方式的硬件木马来说,其电磁辐射在频域中的分布将相对独特,且会区别于普通电路。这样可能造成待测区域的电磁辐射频谱中出现额外的特征频段。此时,被感染 IC 的电磁辐射分布与纯净参考进行差分将可以发现这些异常的特征频率段,并实现该类硬件木马的检测。当硬件木马的电磁辐射的特征频段与 EMI 噪声部分重合时,若硬件木马产生的电磁辐射影响足够大,那么在将其与纯净参考进行差分后,电磁辐射频谱中这些区域将仍然存在明显的特征频率,由此可以实现硬件木马检测。

4.2 局限性分析

电磁辐射分析方法实现硬件木马检测首先需要近场探针可以探测到由硬件木马引起的 IC 电磁辐射变化,因此电磁辐射分析必须进行底噪抑制。但是,即使用最高级的降噪方法,也会有一些噪声残留。因此,当硬件木马电路的活跃度极低时(最极端的情况下触发逻辑几乎不工作时),

其对 IC 的电磁辐射影响极小,将无法从残余的底噪中被区分出来,甚至探头无法获取硬件木马的电磁辐射信号,这也是电磁辐射分析方法研究所面临的重大难题之一。现有方法一般采用输入特定激励,尽可能提升触发逻辑的开关活跃度以实现硬件木马检测。

但是,即使硬件木马电路的活跃度增加,硬件木马的电磁辐射信号也可能无法与 EMI 噪声区分。现有研究大多是将硬件木马的电磁辐射与 EMI 噪声分离考虑的,并且大多数方法认为尽可能地抑制噪声就可以实现硬件木马检测,但实际上它们并不是完全独立的。实际中大部分硬件木马与普通电路的功能结构是类似的,因此其电磁辐射频率分布也十分复杂,其特征频率将散布在多个频率段内,并且产生的信号强度很弱。此时硬件木马的电磁辐射会隐藏在 EMI 噪声中,当尽可能抑制 EMI 噪声时,硬件木马的电磁辐射信号将受到影响而被削弱。

此外,根据 3.2 节的分析可知 EMI 噪声的频率分布相对固定但对检测的影响很大,并且因为周围电路也受到随机噪声的影响,因此 EMI 噪声具有一定的随机性。同时,探头重复定位存在随机偏差。而根据电磁辐射的原理可知,电磁辐射的总体强度与电路块的功率有关,当硬件木马的电磁辐射频率分布复杂时,本就微弱的硬件木马信号在各子区域的电磁辐射影响将变得更小。从而硬件木马信号会被 EMI 噪声所掩盖,电磁辐射分析方法将可能无法实现硬件木马检测。

4.3 验证评估方案

本小节评估验证电磁辐射分析方法的硬件木马检测能力,验证电磁辐射分析方法可适用于具有何种电磁辐射特征的硬件木马,以及该类方法在何种情况下可能失效。本文考虑了 3 种情况:硬件木马的电磁辐射特征独特与普通电路有明显差异的情况;硬件木马电路的活跃度极低的情况;硬件木马的电磁辐射频率分布复杂的情况(将硬件木马与 EMI 噪声联系起来)。

如图 7 所示,验证评估方案包括两部分:有效性和局限性评估验证。后者将进一步分为两种情况。因此,本文将分 3 步评估验证电磁辐射分

析方法的硬件木马检测能力。

首先，考虑硬件木马的电磁辐射特征独特的情况。在该场景下将使用单独的触发信号控制硬件木马电路的工作，然后遵循现有研究采用的策略尽可能提高硬件木马的活跃度。此时评估验证的是电磁辐射分析方法是否可以将电磁辐射特征独特的硬件木马从噪声中检测出来。

然后，考虑硬件木马电路的活跃度极低的情况。此时，评估验证的是当硬件木马的电磁辐射信号表现得像底噪一样时，电磁辐射分析方法是否可以成功实现检测，为此本文将尽可能降低硬件木马的活跃度。但需要说明的是，实现硬件木马检测具体需要多大的活跃度不在本文研究范围内。

最后，考虑硬件木马的电磁辐射频率分布复杂的情况。在该场景下，本文将继续尽可能提高硬件木马的活跃度，同时将周围电路的信号接入硬件木马的触发逻辑中，使其特征频率散布到 EMI 噪声中。此时评估验证电磁辐射分析方法对频率分布复杂的硬件木马是否会检测失败。

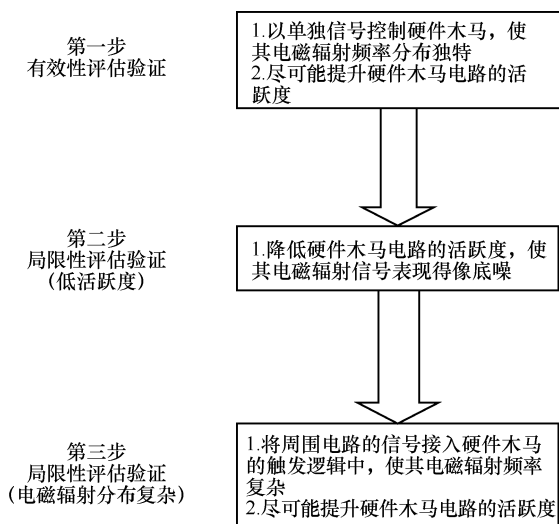


图7 验证评估方案
Figure 7 The validation scheme

5 实验与验证

本节在介绍实验环境后先验证 EMI 噪声的影响形式。然后，在 FPGA 上验证电磁辐射分析方法检测硬件木马的有效性。最后，在两种情况下验证该类方法的检测局限性。

5.1 实验环境

本文的实验平台包括 3 个主要部分：FPGA、近场探针和示波器。实验使用的是 Xilinx Spartan-3E XC3S50 FPGA。本文将 AES 电路作为测试基准电路，并使用 PlanAhead 软件的增量编译方式在不改变电路原始布局的条件下向其中植入硬件木马电路。本文将 NFP-3-P4 近场磁探针（频响范围为 30 MHz~3 GHz）放置在 FPGA 的上方，进行电磁辐射的采集。探针采集到的电磁辐射信息将被泰克 TDS3052C 示波器（采样频率为 500 MHz）捕获，并将其传输到上位计算机中进行进一步分析。整个实验包含 3 部分。

实验 1 EMI 影响验证实验：用于验证 EMI 噪声的影响形式。为了完全排除其他噪声的影响，该实验将在同一块 FPGA 上进行。实验中，待测区域包含硬件木马电路，AES 电路将围绕待测区域布置。

实验 2 有效性验证实验：用于验证电磁辐射分析方法的有效性。实验中，一块 FPGA 将配置为纯净的 AES 电路作为纯净参考。其他 3 块 FPGA 作为待测电路，其中包含相同的 AES 电路植入了不同的硬件木马。其中一块 FPGA 中的硬件木马电路如图 8 所示。该硬件木马将在“Enable”信号出现后几个周期触发（时延由 4 位信号“d”决定），并修改原始信号“p”。该硬件木马的功能由一个多路选择器（图 8 中的“MUX”）和一个减法计数器（图 8 中的“SUB_COUNTER”）实现。另外两块 FPGA 中的硬件木马分别是 Trust-Hub 中的 AES-T400（时序型硬件木马）和 AES-T700（组合型硬件木马）。

实验 3 局限性验证实验：用于验证电磁辐射分析方法的局限性。实验中，4 块 FPGA 中插入了 4 种不同的硬件木马。本实验基于实验 2 中硬件木马的电路结构对它们进行了一些修改，调整了它们监控的信号，因此其部分电路工作时的电流频率将会改变，进而改变其电磁辐射频率分布。

对于电磁辐射数据的预处理，利用均值滤波方法来抑制底噪的影响。为防止残留噪声的干扰，在验证评估电磁辐射分析方法的检测能力时，将使用小波降噪法进一步提高结果的可信度。降噪

通过信噪比 (SNR) 可以比较不同距离对硬件木马检测的影响。SNR 的计算如式(23)所示。

$$\text{SNR} = 10 \lg \frac{S_{\text{硬件木马}}^2}{S_{\text{噪声}}^2} \quad (23)$$

其中, $S_{\text{硬件木马}}$ 代表硬件木马的影响, $S_{\text{噪声}}$ 代表由噪声信号的影响。结果如表 1 所示, 其结果与图 10 的结论吻合。

表 1 信噪比
Table 1 Signal to noise ratio

实验条件	信噪比/dB	实验条件	信噪比/dB	实验条件	信噪比/dB
电路块 间距离远	-16.64	小波降噪	-14.34	HT IV	-10.70
		HT I	0.94	HT V	-11.06
电路块 间距离近	-17.19	HT II	2.19	HT VI	-9.47
		HT III	1.84	HT VII	-10.76

根据以上分析可知, 电路块的数量增加会影响待测区域电磁辐射频谱的复杂性; 电路块间的距离会影响各区域 EMI 噪声的幅度, 因而, EMI 噪声是限制电磁辐射分析方法在频域中实现硬件木马检测的主要因素。但 EMI 噪声的分布是相对确定的, 因此可以使用差分方法进行一定的抑制。

5.3 有效性验证实验

在硬件木马检测实验前, 先基于图 10(a)的实验条件, 使用小波降噪处理电磁辐射数据, 其结果如图 11 所示。比较图 10(a)与图 11 可以很明显看到, 与均值滤波相比, 小波滤波能更好地抑制噪声。在图 11 中出现噪声的频率段更少, 并且 EMI 噪声的幅值变小, 而电磁辐射信号的有效细节 (76.5 MHz 和 100 MHz 附近) 得以更完全地保留。比较表 1 中 SNR 也可得出类似结论。

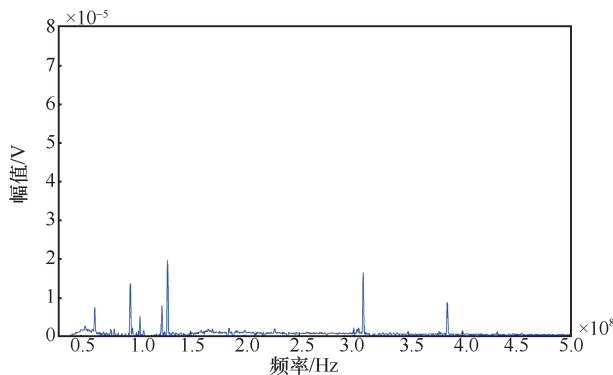


图 11 小波滤波降噪结果
Figure 11 The result of wavelet filtering

硬件木马的检测结果如图 12 所示, 其中红色圆圈内是硬件木马产生的电磁辐射。在图 12(a)中, HT I (电路结构如图 8 所示) 的电磁辐射主要分布在 76.5 MHz 和 100 MHz 附近。(105 MHz 和 310 MHz 附近的波峰是 EMI 噪声的频率偏差造成的异常波动)。HT II (AES-T400) 的检测结果如图 12(b)所示, 其电磁辐射分布在 184.5 MHz、227.5 MHz 和 256.5 MHz 附近。图 12(c)是 HT III (AES-T700) 的电磁辐射分布, 其主要出现在 95.5 MHz 和 172 MHz 附近。从表 1 中的 SNR 值 (明显的异常峰值已被去除) 可以看出, 本次实验中的各项 SNR 明显高于其他实验。实验结果证明, 电磁辐射分析可以有效地对电磁辐射频率分布独特的硬件木马进行检测。

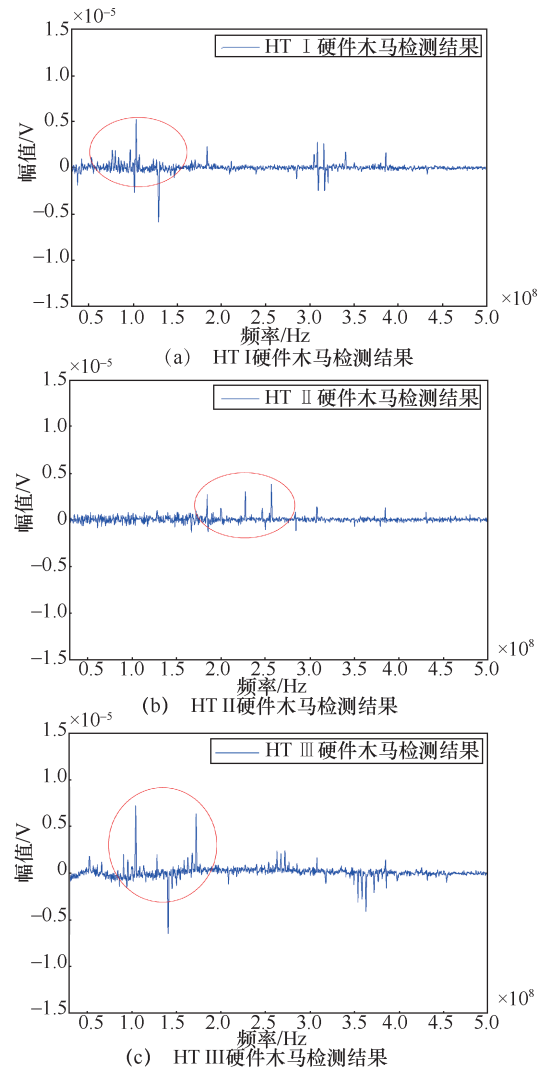


图 12 电磁辐射特征独特的硬件木马检测结果
Figure 12 Detection result for hardware Trojan with special features

5.4 局限性验证实验

本文的最后一个实验用于评估局限性。因为低活跃度硬件木马的检测结果相似，因此仅展示 HT I 硬件木马降低电路活跃度后 (HT IV) 的检测结果。在第二个场景中，本文根据评估验证方案修改了图 8 中的硬件木马 (HT V)，AES-T400 (HT VI) 和 AES-T700 (HT VII)。

场景 I

第一种情况是在硬件木马的电路活跃度很低的情况下进行硬件木马检测。图 13 给出了 HT IV 硬件木马的电磁辐射与底噪进行比较的结果。

在图 13 中几乎找不到硬件木马的特征频率。基于整个曲线来计算 SNR 得到如表 1 中所示的结果，由此可得电磁辐射分析方法未能检测该硬件木马。

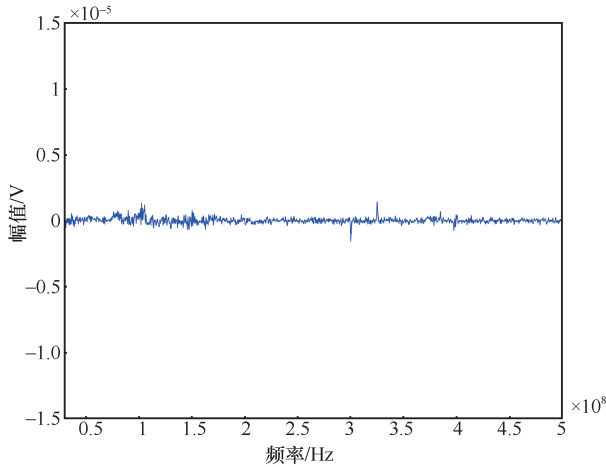


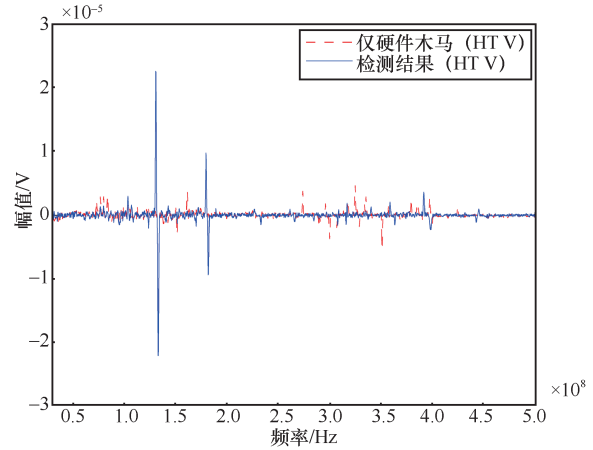
图 13 低活跃度硬件木马检测结果
Figure 13 Detection result for hardware Trojan with low activity

场景 II

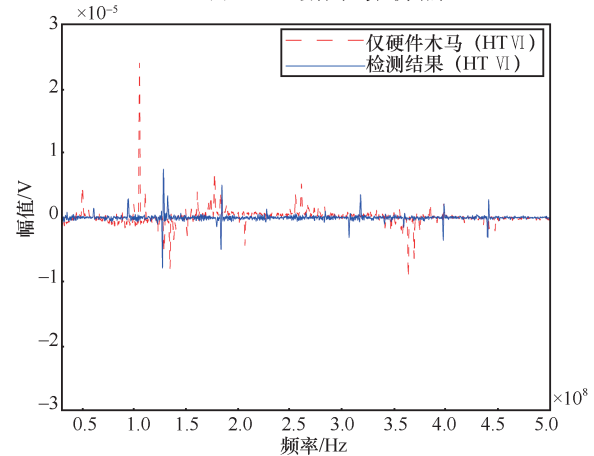
第二种情况是在硬件木马的电磁辐射频率分布复杂的情况下进行硬件木马检测。在尽可能增加硬件木马电路的活跃性后，图 14 中的红色曲线是待测区域仅硬件木马工作时的电磁辐射，蓝色曲线是硬件木马的检测结果。

比较图 14(a)中的红色和蓝色曲线，可以发现硬件木马电磁辐射的频率特征散布到 EMI 噪声中（即频率分布复杂）时，电磁辐射分析方法无法检测到 HT V 分布在 80 MHz、161 MHz 和 274 MHz 附近的电磁辐射特征。同样，HT VI (图 14(b)中 105 MHz、177.5 MHz 和 261 MHz 附近)和 HT VII(图 14(c)中 95.5 MHz、170 MHz

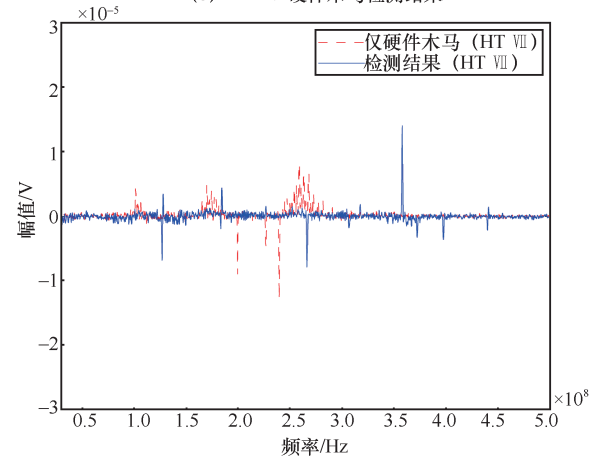
和 260 MHz 附近)的特征频率也无法从 EMI 噪声中检测出。因此可得当硬件木马的频率分布复杂度与普通电路类似时，即使硬件木马电路活跃度很高，电磁辐射分析也很难检测到该类硬件木马。



(a) HT V 硬件木马检测结果



(b) HT VI 硬件木马检测结果



(c) HT VII 硬件木马检测结果

图 14 电磁辐射分布复杂的硬件木马检测结果
Figure 14 Detection result for hardware Trojan with complex distribution

6 结束语

本文首先介绍了电磁辐射分析方法检测硬件木马的检测机理和噪声源。然后, 提出一个专用于电磁辐射分析的噪声模型, 并分析该模型中每种噪声的影响。在此基础上, 讨论了硬件木马电磁辐射信号和噪声之间的可能联系, 并提出了电磁辐射分析方法的有效性以及可能存在的局限性。在此基础上, 提出了相应的验证评估方案, 并在 FPGA 上进行了实验, 验证了其有效性和局限性。

基于实验结果可以得知, 对于采用与普通电路有明显不同的特殊电路结构(如采用模拟电路设计等)或工作方式的硬件木马, 其电磁辐射特征独特, 电磁辐射分析方法可以有效地对其实现检测。后续研究可以对这些为了规避常规检测方法而采用特殊设计的硬件木马建立电磁辐射特征库。此后可以通过直接识别待测 IC 电磁辐射数据中是否存在这些异常特征, 对库中硬件木马实现无纯净母本芯片检测。

同时, 由于实际中大多数硬件木马与普通电路的功能结构类似, 其电磁辐射频率分布复杂, 特征频率将分布在多个频率区域内, 并且产生的信号强度很弱。此时电磁辐射分析方法可能无法对该类硬件木马实现有效地检测, 因此电磁辐射分析方法通用性受限。后续可以研究克服该局限性的措施或寻找另一种在通用性上表现更好的方法(如红外图像侧信道分析方法)协同进行检测, 弥补电磁辐射分析的局限性。

电磁辐射分析方法的检测效率主要由电磁辐射采集效率与电磁辐射信号降噪算法效率决定。后续研究可以通过设计信号采集板卡将电磁辐射采集与噪声处理进行集成等方式, 以硬件降噪的形式提升电磁辐射分析方法的检测效率。

参考文献:

- [1] AGRAWAL D, BAKTIR S, KARAKOYUNLU D, et al. Trojan detection using IC fingerprinting[C]//2007 IEEE Symposium on Security and Privacy (SP'07). Berkeley, CA: IEEE, 2007: 296-310.
- [2] LIU C, CRONIN P, YANG C. A mutual auditing framework to protect IoT against hardware Trojans[C]//2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC). 2016.
- [3] CHAKRABORTY R S, WOLFF F, PAUL S, et al. MERO: a statistical approach for hardware Trojan detection[C]// Cryptographic Hardware and Embedded Systems - CHES 2009. Berlin, Heidelberg: Springer, 2009: 396-410.
- [4] BALASCH J, GIERLICH B, VERBAUWHEDE I. Electromagnetic circuit fingerprints for hardware trojan detection[C]//2015 IEEE International Symposium on Electromagnetic Compatibility (EMC). Dresden, Germany: IEEE, 2015: 246-251.
- [5] BANGA M, HSIAO M S. A region based approach for the identification of hardware Trojans[C]//2008 IEEE International Workshop on Hardware-Oriented Security and Trust. 2018.
- [6] CHEN Z, GUO S, WANG J, et al. Toward FPGA security in IoT: a new detection technique for hardware Trojans[J]. IEEE Internet of Things Journal, 2019, 6(4): 7061-7068.
- [7] HE J, ZHAO Y, GUO X, et al. Hardware Trojan detection through chip-free electromagnetic side-channel statistical analysis[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25(10): 2939-2948.
- [8] HE J, LIU Y, YUAN Y, et al. Golden chip free trojan detection leveraging electromagnetic side channel fingerprinting[J]. IEICE Electronics Express, 2019, 16(2): 20181065-20181065.
- [9] NGO X T, EXURVILLE I, BHASIN S, et al. Hardware Trojan detection by delay and electromagnetic measurements[C]//2015 Design, Automation Test in Europe Conference Exhibition (DATE). 2015.
- [10] SOLL O, KORAK T, MUEHLBERGHUBER M, et al. EM-based detection of hardware Trojans on FPGAs[C]//2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). Arlington, VA, USA: IEEE, 2014: 84-87.
- [11] TANG Y, FANG L, LI S. Activity factor based hardware Trojan detection and localization[J]. Journal of Electronic Testing, 2019, 35(3): 293-302.
- [12] TANG Y, LI S, FANG L, et al. Golden-chip-free hardware Trojan detection through quiescent thermal maps[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27(12): 2872-2883.
- [13] TANG Y, LI S, ZHANG F, et al. Thermal maps based HT detection using spatial projection transformation[J]. IET Information Security, 2018, 12(4): 356-361.
- [14] HAYASHI Y, KAWAMURA S. Survey of hardware trojan threats and detection[C]//2020 International Symposium on Electromagnetic Compatibility-EMC EUROPE. Rome, Italy: IEEE, 2020: 1-5.
- [15] NOTAROS B M. 电磁学[M]. 北京: 清华大学出版社, 2018.
- [16] NOTAROS B M. Electromagnetics[M]. Beijing: Tsinghua University Press, 2018.
- [17] BOSSUET L, FISCHER V, BAYON P. Contactless transmission of intellectual property data to protect FPGA designs[C]//2015 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC). 2015: 19-24.
- [18] QIU H, LUO C, FANG W, et al. Noncontact time-domain EMI measurement of two adjacent traces on a PCB[C]//2018 IEEE Symposium on Electromagnetic Compatibility, Signal Integrity and Power Integrity (EMC, SI & PI). Long Beach, CA: IEEE, 2018: 634-639.

- [18] 王品, 赵毅强, 刘燕江, 等. 基于高斯滤波和 K 最邻近算法融合的硬件木马电磁信息检测技术研究[J]. 南京大学学报(自然科学), 2020, 56(2): 264-269.
- WANG P, ZHAO Y Q, LIU Y J, et al. Hardware Trojan electromagnetic information detection based on fusion of Gaussian filter and K-nearest neighbour algorithm[J]. Journal of Nanjing University (Natural Science), 2020, 56(2): 264-269.
- [19] SUPON T M, RASHIDZADEH R. On-Chip magnetic probes for hardware Trojan prevention and detection[J]. IEEE Transactions on Electromagnetic Compatibility, 2020: 1-12.
- [20] HE J, GUO X, MA H, et al. Runtime trust evaluation and hardware trojan detection using on-chip EM sensors[C]//2020 57th ACM/IEEE Design Automation Conference (DAC). San Francisco, CA, USA: IEEE, 2020: 1-6.
- [21] MITTAL S. A Survey of architectural techniques for managing process variation[J]. ACM Computing Surveys, 2016, 48(4): 1-29.
- [22] RAI D, LACH J. Performance of delay-based trojan detection techniques under parameter variations[C]//2009 IEEE International Workshop on Hardware-Oriented Security and Trust. San Francisco, CA, USA: IEEE, 2009: 58-65.
- [23] HOU B, HE C, WANG L, et al. Hardware Trojan detection via current measurement: a method immune to process variation Effects[C]//2014 10th International Conference on Reliability, Maintainability and Safety (ICRMS). Guangzhou, China: IEEE, 2014: 1039-1042.
- [24] TUZLUKOV V P. Signal Processing Noise[M]. Boca Raton: CRC Press, 2002.
- [25] LEE E A, MESSERSCHMITT D G. Digital communication[M]. Boston, MA: Springer US, 1993.
- [26] BEENAKKER C W J, BÜTTIKER M. Suppression of shot noise in metallic diffusive conductors[J]. Physical Review B, Condensed Matter, 1992, 46(3): 1889-1892.
- [27] GRAY R M, NEUHOF D L. Quantization[J]. IEEE Transactions on Information Theory, 1998, 44(6): 2325-2383.
- [28] JARQUE C M, BERA A K. A test for normality of observations and regression residuals[J]. International Statistical Review / Revue Internationale de Statistique, 1987, 55(2): 163.
- [29] DAUBECHIES I, BATES B J. Ten lectures on wavelets[J]. The Journal of the Acoustical Society of America, 1993, 93(3): 1671.
- [30] DONOHO D L, JOHNSTONE I M. Ideal spatial adaptation by

wavelet shrinkage[J]. Biometrika, 1994, 81(3): 425-455.

- [31] CHA B, GUPTA S K. Efficient Trojan detection via calibration of process variations[C]//2012 IEEE 21st Asian Test Symposium. Niigata, Japan: IEEE, 2012: 355-361.

[作者简介]



唐永康(1992-), 男, 山东烟台人, 国防科技大学博士生, 主要研究方向为芯片与信息安全。



胡星(1989-), 女, 江西赣州人, 国防科技大学工程师, 主要研究方向为芯片与信息安全。



苏颀(1996-), 男, 湖南茶陵人, 国防科技大学硕士生, 主要研究方向为芯片与信息安全。



李少青(1963-), 男, 陕西西安人, 国防科技大学研究员, 主要研究方向为芯片与信息安全。