Chinese Journal of Electronics
vol. 33, no. 2, pp. 385–392, March 2024
https://doi.org/10.23919/cje.2022.00.310

RESEARCH ARTICLE

Analytical Models of on-Chip Hardware Trojan Detection Based on Radiated Emission Characteristics

Fan ZHANG[1], Dongrong ZHANG[2], Qiang REN[1], Aixin CHEN[1], and Donglin SU[1,3]

1. *School of Electronics and Information Engineering, Beihang University, Beijing 100191, China*
2. *Zhongguancun Laboratory, Beijing 100094, China*
3. *The Research Institute for Frontier Science, Beihang University, Beijing 100191, China*

Corresponding author: Donglin SU, Email: sdl@buaa.edu.cn
Manuscript Received September 14, 2022; Accepted October 20, 2022

Abstract — Since many third parties involved in integrated circuit (IC) manufacturing, hardware Trojans malicious implantation have become a threat to the IC industry. Therefore, varieties of reliable hardware Trojan detection methods are needed. Since electromagnetic radiation is an inherent phenomenon of electronic devices, there are significant differences in the electromagnetic radiated characteristics for circuits with different structures and operating states. In this paper, a novel hardware Trojan detection method is proposed, which considers the electromagnetic radiation differences caused by hardware Trojan implantation. Experiments of detecting hardware Trojan in field programmable gate arrays show that the proposed method can effectively distinguish the ICs with Trojan from the ones without Trojan by the radiated emission.
Keywords — Hardware Trojan, Radiated emission, Integrated circuit.
Citation — Fan ZHANG, Dongrong ZHANG, Qiang REN, *et al.*, "Analytical Models of on-Chip Hardware Trojan Detection Based on Radiated Emission Characteristics," *Chinese Journal of Electronics*, vol. 33, no. 2, pp. 385–392, 2024. doi: 10.23919/cje.2022.00.310.

I. Introduction

The current integrated circuit (IC) supply chain involves many untrustworthy participants, such as designers, manufacturers, and distributors. [1], [2], which are not entirely under the designer's control [3]. As a result, driven by illegitimate revenues, ICs are common targets for counterfeiting [4]–[6] and have become more vulnerable to be attacked or modified [7]–[9], such as hardware Trojan (HT) implantation.

It is evident that the system's quality cannot be guaranteed due to the unknown sources of the system components. Hardware Trojans can be implemented as hardware modifications to ICs, such as application specific ICs, commercial off-the-shelf components, microprocessors, and digital signal processors, or as firmware modifications to field programmable gate arrays (FPGA) bitstreams, by an untrusted third party, which poses a serious threat to the security of the system [10], [11].

However, hardware Trojan detection is a challenging work. On the one hand, Trojan circuits are difficult to activate and detect using random stimuli, since they can only be activated under extremely specific circumstances by design. On the other hand, physical inspection and destructive reverse engineering are challenging and expensive methods of detection, due to the complexity of the system and the nanometer IC feature sizes. Destructive reverse engineering also does not ensure that ICs that are not evaluated destructively are Trojan-free [12], [13].

Several novel Trojan detection schemes have been proposed recently, which can basically be divided into logic testing and side-channel analysis. Logic testing approaches, both functional and structural, attempt to develop directed test patterns to activate unknown Trojan instances and propagating their effects to output ports [9]. Although robust under process and measurement noise, these approaches are likely to fail to activate large Tro-

Associate Editor: Prof. Yikai CHEN, University of Electronic Science and Technology of China.

jans consisting of large numbers of trigger inputs. It means that most of the time, the hardware Trojan does not directly affect the output of IC. Since that, detecting abnormal signals from the side channel, such as supply current or path delay, which can be affected due to unintended design modifications, becomes an alternative method. The presence of a Trojan circuit will be reflected in the current drawn from the power supply, even if no switching occurs in the Trojan circuit. Any extra gate will consume extra leakage power, which is additive and can ideally be used to distinguish golden circuits from ones with Trojan [14]–[16]. Similarly, whether the hardware Trojan is implanted or not will also affect other physical characteristics of the ICs, thus being used as detection means, such as, timing [17], temperature [18], optics [19] or multiple characteristics [8] are used to distinguish a malicious design from a genuine one.

In this research, a novel electromagnetic radiation-based hardware Trojan detection technique is proposed. During operation, electromagnetic radiation leakage from ICs is unavoidable. The electromagnetic signals determined by the circuits' structure and the information that they process [20]. Their emission reflects the modes and states of the current circuit. Hence, through intercepting, processing and analysing these electromagnetic signals, the pertinent information can be reconstructed and recreated. This means that the electromagnetic signals emitted will differ depending on whether the circuits contain hardware Trojans or not. An innovative technique for hardware Trojan identification can be obtained by identifying differences in radiation emission signals. The proposed method has the following advantages:

- Without invasion of the IC, the proposed method employs electromagnetic radiation to detect hardware Trojans;
- The proposed method does not occupy the working port of the ICs, which makes it possible for real-time online testing;

The rest of this paper is organized as follows. In Section II, the theory and the proposed models for electromagnetic radiation of FPGA with or without hardware Trojans are presented in detail, which proves the theoretical feasibility of identifying hardware Trojan through radiation emission of FPGA. In Section III, a test scheme with the consideration of the propagation loss of electromagnetic radiation emission in space is designed. In Section IV, the radiation emission of Trojan chip and genuine chip are compared to validate the effectiveness of this method. Finally, some conclusions are drawn in Section V.

II. Radiation Model of Hardware Trojan Detection Method

FPGA is a common type of ICs. Because of its programmability, it is widely used in industry and IC preliminary design verification. In this paper, FPGA is also taken as an example to discuss the effectiveness of detecting hardware Trojan by radiation emission, and the relevant conclusions can be transferred to other types of ICs.

The basic structure of FPGA includes three parts: configurable logic block (CLB), input output block (IOB) and programmable interconnect (PI), as shown in Figure 1. The CLBs are composed of a large number of nonlinear logic switches. PI include wire segments and switch block (SB), through which signals of external devices can be connected to internal CLB through IOB, or interconnection between internal CLB of FPGA can be realized. For example, in Figure 1, the clock signal (orange thick solid line) generated by the external crystal oscillator of the FPGA enters the FPGA through IOB, and then is transmitted to each CLB requiring clock input via the PI [21].

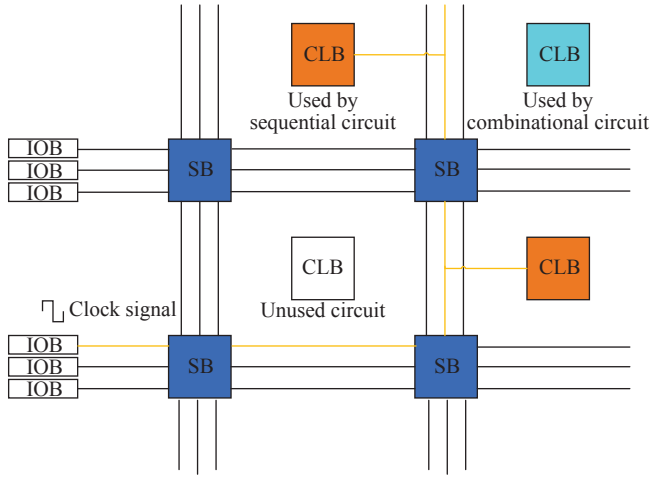


Figure 1 Basic structure of FPGA.

Since all components of the circuit are not ideal, there is always a small amount of electromagnetic radiation when the circuits are working. For FPGA, these electromagnetic radiation mainly includes two parts: 1) the leakage when high-speed electromagnetic signals are transmitted on the interconnection line of PI, and 2) the new frequency component generated by the nonlinear logic devices in CLB and PI when they are switching at high speed.

Almost all components and circuits are laid flat on the surface of the printed circuit board (PCB). Hence, for the two cases of unintentional electromagnetic leakage discussed above, it can be considered that the equivalent current source is parallel to the surface of the PCB. Of course, the more general discussion should include the weak leakage current perpendicular to the PCB, but even ignoring this part of current will not affect our general conclusion, so it is not considered in this paper.

Therefore, for an FPGA with or without hardware Trojan, its general radiation leakage model is shown in Figure 2. Considering that the hardware Trojan in FPGA often needs additional SLB and IP units to support its own functions, the circuit structure of the FPGA with and without the hardware Trojan is shown in Figures 2(a) and (b). On the one hand, the FPGA with the hardware

Trojan has the same circuits as the FPGA without the hardware Trojan in order to realize its required functions. On the other hand, compared with the FPGA without Trojan, the FPGAs with Trojan often have some redundant SLB and IP occupation to realize malicious functions.

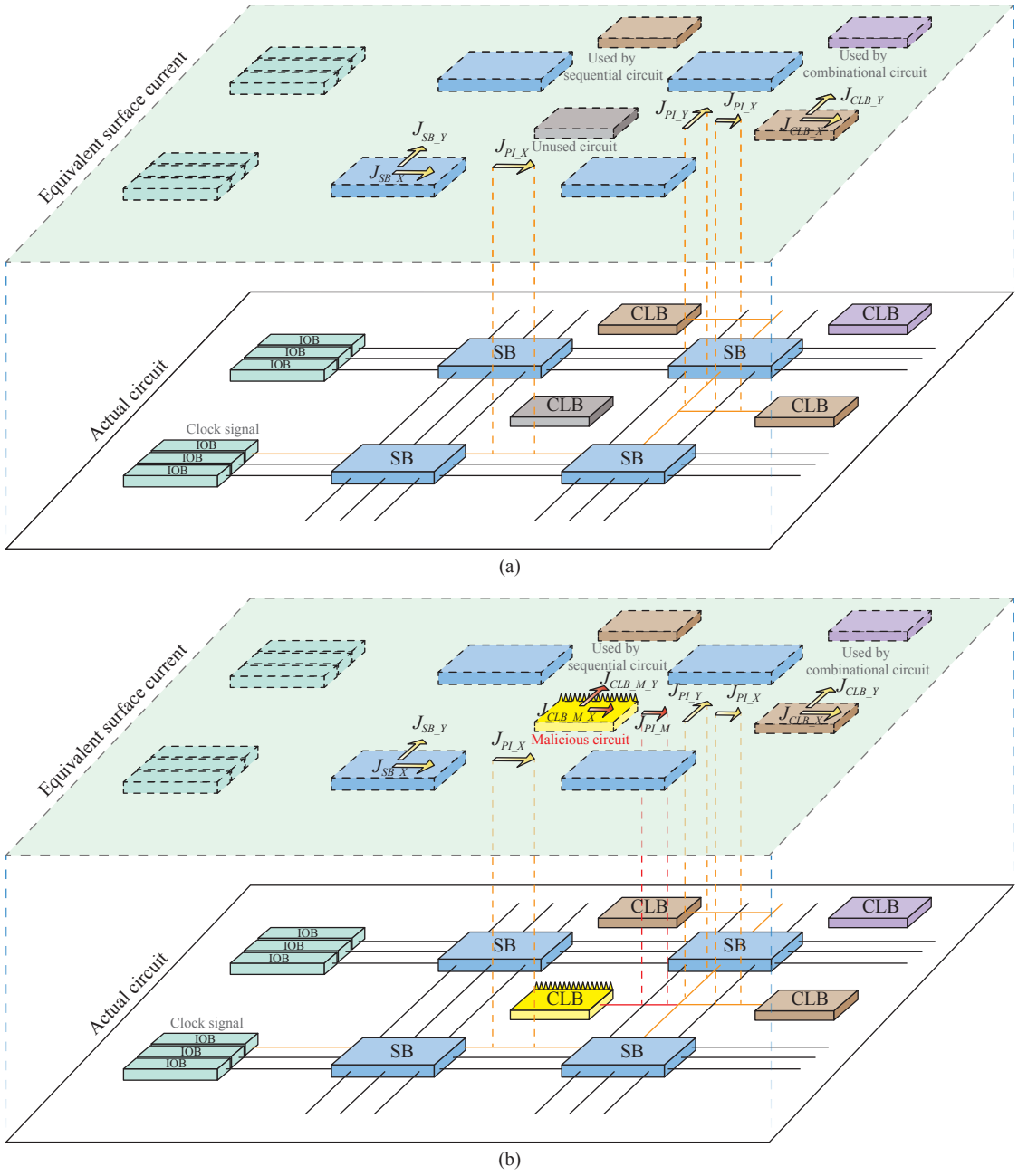


Figure 2 Equivalent current model of FPGA (a) without and (b) with Trojan.

We consider establishing a spherical coordinate system (r, θ, φ) with the center of FPGA as the origin. The coordinates of the source point are expressed as $\boldsymbol{r'}$, the field point are expressed as $\boldsymbol{r}$.

For FPGA without (wo) hardware Trojan, the surface current sources $\boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'})$ causing radiation emission mainly include the nonlinear devices in SB (J_{SB_X}, J_{SB_Y}) and CLB (J_{CLB_X},J_{CLB_Y}) and the interconnections (J_{PI_X},J_{PI_Y}) connecting these parts, as shown in Figure 2(a). For FPGA with hardware Trojan implanted, beside the above currents, as shown in Figure 2(b), some additional SB, CLB and interconnects need to be aroused to achieve malicious purposes. Therefore, the total current of a FPGA with (w) hardware Trojan ($J_{s\_\mathrm{wHT}}(\boldsymbol{r'})$) can be expressed as

$$\boldsymbol{J}_{s\_\mathrm{wHT}}(\boldsymbol{r'}) = \boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'}) + \boldsymbol{J}_{s\_m}(\boldsymbol{r'}) \tag{1}$$

where $\boldsymbol{J}_{s\_m}(\boldsymbol{r'})$ is the equivalent current sources of CLB, SB and interconnection lines used by the hard-

ware Trojan.

Taking FPGA without hardware Trojan as an example, the magnetic vector potential $\boldsymbol{A}_{\mathrm{woHT}}(\boldsymbol{r})$ can be expressed by surface current density $\boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'})$ as

$$\boldsymbol{A}_{\mathrm{woHT}}(\boldsymbol{r}) = \frac{\mu_0}{4\pi}\int_S \boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'})\frac{\mathrm{e}^{-\mathrm{j}k_0|\boldsymbol{r}-\boldsymbol{r'}|}}{|\boldsymbol{r}-\boldsymbol{r'}|}\mathrm{d}s' \tag{2}$$

If the field point is not too close to the source point, and the influence of $(r'/r)^2$ can be ignored. Under this assumption, $\mathrm{e}^{-\mathrm{j}k_0|\boldsymbol{r}-\boldsymbol{r'}|} \approx \mathrm{e}^{-\mathrm{j}k_0(r-\hat{\boldsymbol{a}}_r\cdot\boldsymbol{r'})}$ and $|\boldsymbol{r}-\boldsymbol{r'}| \approx r$, the integrand function in (2) can be approximated as follows:

$$\boldsymbol{A}_{\mathrm{woHT}}(\boldsymbol{r}) = \frac{\mu_0}{4\pi}\frac{\mathrm{e}^{-\mathrm{j}k_0 r}}{r}\int_S \boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'})\,\mathrm{e}^{-\mathrm{j}k_0\hat{\boldsymbol{a}}_r\cdot\boldsymbol{r'}}\mathrm{d}s' \tag{3}$$

Assuming that the current source is of small size, $k_0\boldsymbol{a}_{\boldsymbol{r}}\cdot\boldsymbol{r'} \approx 0$, then expand the exponential term of (3) and retain the first two terms to obtain

$$\begin{aligned}\boldsymbol{A}_{\mathrm{woHT}}(\boldsymbol{r}) &\approx \frac{\mu_0}{4\pi}\frac{\mathrm{e}^{-\mathrm{j}k_0 r}}{r}\int_S \boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'})\,(1+\mathrm{j}k_0\hat{\boldsymbol{a}}_r\cdot\boldsymbol{r'})\,\mathrm{d}s' \\ &= \frac{\mu_0}{4\pi}\frac{\mathrm{e}^{-\mathrm{j}k_0 r}}{r}\int_S \Big\{\boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'}) \\ &\quad +\frac{1}{2}\mathrm{j}k_0\left[\left(\boldsymbol{r'}\times\boldsymbol{J}_{s\_\mathrm{woHT}}\right)\times\hat{\boldsymbol{a}}_r\right. \\ &\quad \left.+(\hat{\boldsymbol{a}}_r\cdot\boldsymbol{r'})\,\boldsymbol{J}_{s\_\mathrm{woHT}}+\left(\hat{\boldsymbol{a}}_r\cdot\boldsymbol{J}_{s\_\mathrm{woHT}}\right)\boldsymbol{r'}\right]\Big\}\mathrm{d}s'\end{aligned} \tag{4}$$

The dipole moment of the electric dipole is defined as $\boldsymbol{P}_{\mathrm{woHT}}$, the dipole moment of the magnetic dipole is defined as $\boldsymbol{M}_{\mathrm{woHT}}$, and the polar moment of the electric quadrupole is defined as $\hat{\boldsymbol{Q}}_{\mathrm{woHT}}$.

$$\begin{cases}\boldsymbol{P}_{\mathrm{woHT}} = \displaystyle\int_S \boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'})\,\mathrm{d}s' \\ \boldsymbol{M}_{\mathrm{woHT}} = \displaystyle\int_S \left[\boldsymbol{r'}\times\boldsymbol{J}_{s\_\mathrm{woHT}}(\boldsymbol{r'})\right]\mathrm{d}s'/2 \\ \hat{\boldsymbol{Q}}_{\alpha\beta\_\mathrm{woHT}} = \displaystyle\int_S \left[\alpha'\boldsymbol{J}_\beta(\boldsymbol{r'})+\beta'\boldsymbol{J}_\alpha(\boldsymbol{r'})\right]\mathrm{d}s';\alpha,\beta=x,y\end{cases} \tag{5}$$

If we set $f(r) = \dfrac{\mathrm{e}^{-\mathrm{j}k_0 r}}{r}$. At the same time, it is considered that the radiation is dominated by the lower order term and the electric quadrupole term can be neglected, thus the (4) can be further simplified as

$$\boldsymbol{A}_{\mathrm{woHT}}(\boldsymbol{r}) \approx \frac{\mu_0}{4\pi}f(r)\left(\boldsymbol{P}_{\mathrm{woHT}} - \mathrm{j}k_0\hat{\boldsymbol{a}}_r\times\boldsymbol{M}_{\mathrm{woHT}}\right) \tag{6}$$

Furthermore, the electromagnetic field at any point above the FPGA without hardware Trojan can be obtained by magnetic vector potential $\boldsymbol{A}_{\mathrm{woHT}}$:

$$\begin{cases}\boldsymbol{H}_{\mathrm{woHT}}(\boldsymbol{r}) = \dfrac{\nabla\times\boldsymbol{A}_{\mathrm{woHT}}(\boldsymbol{r})}{\mu_0} \\ \boldsymbol{E}_{\mathrm{woHT}}(\boldsymbol{r}) = \dfrac{\nabla\times\nabla\times\boldsymbol{A}_{\mathrm{woHT}}(\boldsymbol{r})}{\mathrm{j}\omega\varepsilon_0\mu_0}\end{cases} \tag{7}$$

Similarly, the electromagnetic field at any point above the FPGA with Trojan can be expressed as

$$\begin{cases}\boldsymbol{H}_{\mathrm{wHT}}(\boldsymbol{r}) = \dfrac{\nabla\times\boldsymbol{A}_{\mathrm{wHT}}(\boldsymbol{r})}{\mu_0} \\ \boldsymbol{E}_{\mathrm{wHT}}(\boldsymbol{r}) = \dfrac{\nabla\times\nabla\times\boldsymbol{A}_{\mathrm{wHT}}(\boldsymbol{r})}{\mathrm{j}\omega\varepsilon_0\mu_0}\end{cases} \tag{8}$$

Then for the electric field at any point above the FPGA, the difference between the electric fields with or without hardware Trojan can be expressed as

$$\begin{aligned}\Delta E(r) &= \boldsymbol{E}_{\mathrm{wHT}}(r) - \boldsymbol{E}_{\mathrm{woHT}}(r) \\ &= \frac{\nabla\times\nabla\times\boldsymbol{A}_{\mathrm{wHT}}(r)}{\mathrm{j}\omega\varepsilon_0\mu_0} - \frac{\nabla\times\nabla\times A_{\mathrm{woHT}}(r)}{\mathrm{j}\omega\varepsilon_0\mu_0} \\ &= \frac{\mu_0}{4\pi}\frac{\mathrm{e}^{-\mathrm{j}k_0 r}}{r}\int_S J_{s-\mathrm{wHT}}(r')\,\mathrm{e}^{-\mathrm{j}k_0\hat{a}_r\cdot\boldsymbol{r'}}\mathrm{d}s' \\ &\quad -\frac{\mu_0}{4\pi}\frac{\mathrm{e}^{-\mathrm{j}k_0 r}}{r}\int_S J_{s-\mathrm{woHT}}(r')\,\mathrm{e}^{-\mathrm{j}k_0\hat{a}_r\cdot\boldsymbol{r'}}\mathrm{d}s' \\ &= \frac{\mu_0}{4\pi}\frac{\mathrm{e}^{-\mathrm{j}k_0 r}}{r}\int_S J_{s-m}(r')\,\mathrm{e}^{-\mathrm{j}k_0\hat{a}_r\cdot\boldsymbol{r'}}\mathrm{d}s'\end{aligned} \tag{9}$$

Obviously, the difference in electric field $\Delta\boldsymbol{E}$ is caused by the active hardware Trojan. As mentioned before, the current of the hardware Trojan $\boldsymbol{J}_{s\_m}$ is obviously not 0. At the same time, due to the complexity of the field and the arbitrariness of the test points, it is almost impossible to make the field generated by the hardware Trojan at any point above the FPGA be 0 through elaborate design. This provides a theoretical basis for us to monitor the hardware Trojan by radiation emission.

This problem is further elaborated from the perspective of simulation. According to (4)–(7), the electromagnetic field of the test point above the FPGA is determined by the equivalent electric dipole and the equivalent magnetic dipole on the FPGA surface. In order to simplify the discussion, the simulation only considers the equivalent electric dipoles on the surface of FPGAs as shown in Figure 3(a). In Figure 3(b), the electric dipoles in the blue frame are treated as the part of FPGA that completes basic functions, and the electric dipoles in the red frame are treated as the part of FPGA that is activated by hardware Trojan.

When the FPGA works and the hardware Trojan does not work, the electric field at 5 mm above the surface is shown in Figure 4(a). When the hardware Trojan works, the electric field at the same surface is shown in Figure 4(b). It can be seen that the work of the hardware Trojan affects the electric field distribution in space.

If (0 mm, 0 mm, 10 mm) is set as the observation point. The magnitude of electric field at this point is 0.8 dB less when there is a hardware Trojan working than when there is no hardware Trojan working. This conclusion is also applicable to the case where the electric dipoles and the magnetic dipoles coexist. Therefore, from the perspective of simulation, we can further confirm that

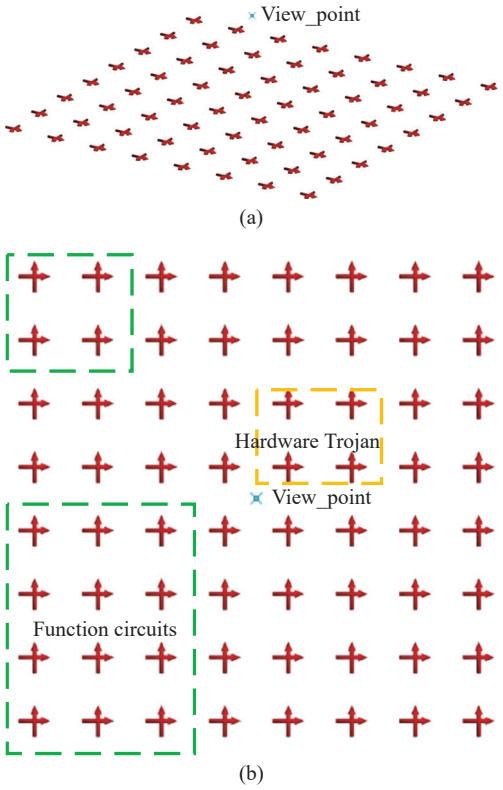


Figure 3 Hardware Trojan simulation based on equivalent electric dipoles. (a) The simulation of FPGA; (b) The equivalent circuit of FPGAs.

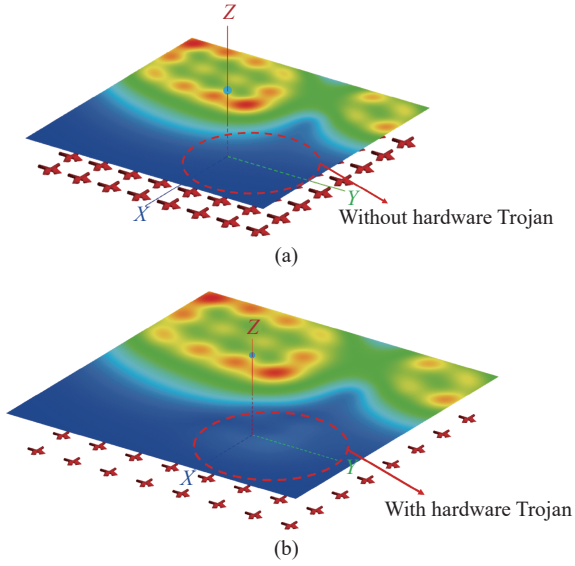


Figure 4 Hardware Trojan simulation based on equivalent electric dipoles. (a) The simulation of FPGA; (b) The equivalent circuit of FPGAs.

the difference between radiation emission with and without hardware Trojan can provide us with the possibility of detecting hardware Trojan from radiation emission.

III. Hardware Trojans Detection Method Based on Electromagnetic Radiation

In this section, the experimental setup is shown in Figure 5 to verify the hardware Trojan detection method based on radiation emission. The experiment system consists of a spectrometer, a near field probe, a probe support, and the integrated circuits with or without hardware Trojans (Target). Considering that electromagnetic radiation is easily susceptible to external interference, the whole experiment system is placed in an anechoic chamber.

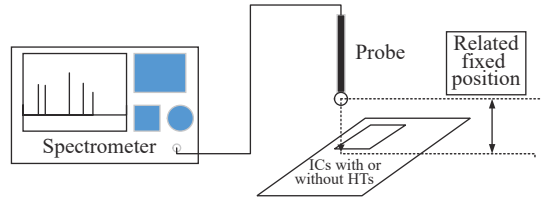
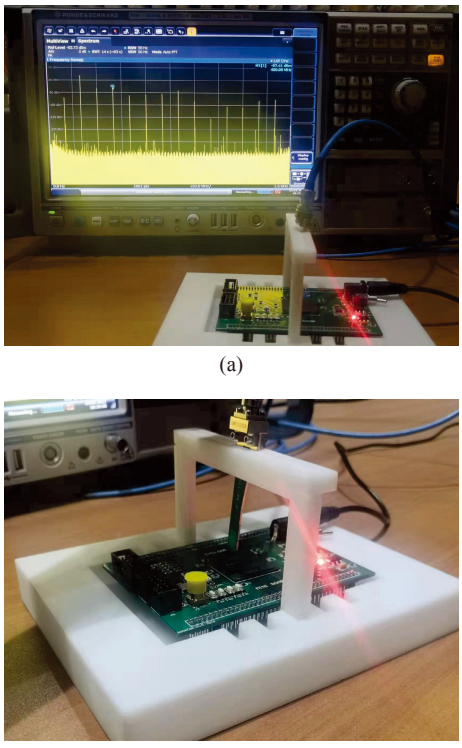


Figure 5 Schematic diagram of hardware Trojan detection based on radiation emission.

The spectrometer in this experiment system is R&S FSW26. Considering the main radiation emission frequency of IC, 0 to 1.5 GHz are chosen as the frequency span of the spectrometer. At the same time, in order to reduce unnecessary variables, RBW is set as 50 Hz in the test. The near field probe we used in this system is introduced in [21]. With the consideration of the propagation loss of electromagnetic radiated emission, the change of the relative position between the near field probe and IC will cause the data between each measurement to have no reference value. Therefore, the probe and ICs have to be kept with a relatively fixed position. A probe support is 3D printed to meet this fixed requirement, as shown in Figure 6(a). And the overall view of the system is shown in Figure 6(b).

Altera Cyclone 5CEFA4F23I7 is used as the FPGA platform. Using the above experiment system, the FPGA evaluation board (Altera Cyclone 5CEFA4F23I7) with different circuit firmware burned in were tested. There are different types of circuits under test, which are genuine circuits, circuits implanted with small Trojans (HT1) and circuits implanted with a novel large Trojans (HT2), as shown in Table 1. The circuit benchmark is Advanced Encryption Standard (AES) [22], and it is an implementation of 128-bit version of the AES block cipher. It should be noted that the proposed method is not limited to detecting hardware Trojans in cryptographic circuits. The input operands, namely, 128-bit plain text and 128-bit secret key, are provided by the controller FPGA to the main FPGA, with the on board 100-MHz oscillator. The Trojan circuits are a selection of HT benchmarks attacking an AES cryptographic circuit and these Trojans provide a wide variety of implementations. HT1 [23] is selected from a collection of well-known hardware Trojan testbench, which leaks key information through the power side channel. And HT2 is a novel hardware Trojan, which encrypts the key information obtained and transmits it through the data channel.

During the test, all three circuits executed the same



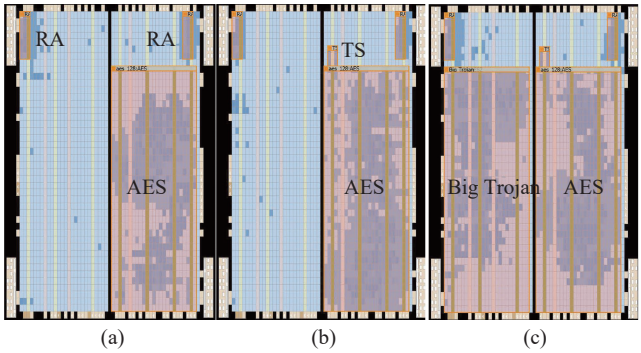
(a) (b)

Figure 6 Hardware Trojan detection platform based on radiation emission. (a) Probe support; (b) The overall view of the platform.

Table 1 The states of FPGAs under test

States of FPGAs	Kinds of HT inserted	No. register of HT
Genuine circuits	–	–
Circuits with HT1	AES-T100 [23]	64
Circuits with HT2	A novel HT	4425

instructions and the hardware Trojan is active. The FPGA resources activated by hardware Trojan is shown as Figures 7(a), (b) and (c), where the area named RA and AES is the resources to realise the basic function of circuit, meanwhile, the area named TS and Big Trojan stand for the resources occupied by HT1 and HT2.



(a) (b) (c)

Figure 7 FPGA resources activated by hardware Trojan of different scales. (a) Without HT; (b) With HT1; (b) With HT2.

What we can observe is a series of harmonic radiation caused by 100 MHz oscillator on the FPGAs. From the discussion in Section II, we can see that under different conditions of whether the FPGA has a hardware Trojan or not, due to the different structures of active circuits, the radiation emission strength of the FPGAs at the corresponding harmonic frequency under different conditions is also different. Hence, the amplitude of the harmonics of 100 MHz oscillator are used as an observation to monitor whether there is a hardware Trojan.

IV. Result and Analysis

One of the test data are shown in Figure 8. It can be seen that the viewed radiation emission of the FPGAs consists of two parts. One part is a harmonic with 100 MHz as the cycle, and the other part is the noise with amplitude lower than −120 dB. Considering that the noise amplitude lower than −120 dB is not high enough, it is very easy to be disturbed by the surrounding environment. Therefore, we focus on the harmonic part of radiation emission.

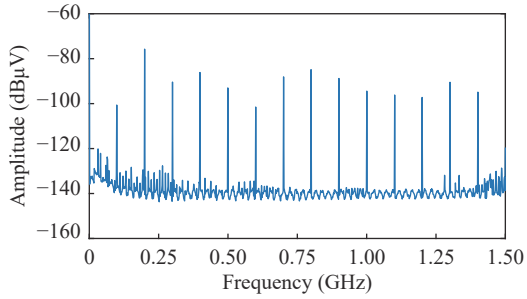


Figure 8 Single measured result of the spectrum with the hardware Trojan detection system.

Due to the strong aggregation of harmonic amplitude under different states, the box diagram is used to describe the test results which only focus on the peak value of the harmonics in Figure 9 using parts of test data of radiation emission results. Results shows that at each frequency point, the test results of each states have good aggregation and the results between each states are significantly different.

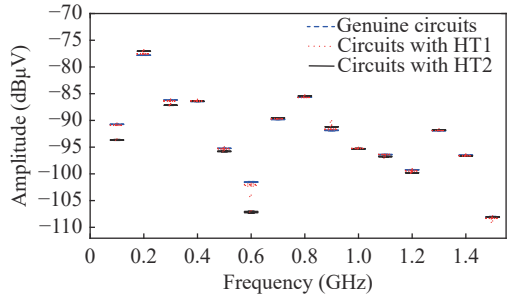


Figure 9 The test results of the FPGAs under three states.

In addition, to avoid the influence of random error, 5 FPGAs of the same type are used to verify the generality of the scheme in detecting hardware Trojans. From the conclusion summarized in the previous paragraph, we can define a series of new distances to predict whether

there is a hardware Trojan in the FPGAs. In the case of multiple tests in advance, the average result of the test of genuine circuit is Amp_{gi}, where Amp_i is the amplitude at the ith frequency point. If a circuit in an unknown state, and the test result is Amp_i. Distances can be defined as

$$d = \sqrt[p]{\sum_{i=1}^{14} \left|\mathrm{Amp}_{gi} - \mathrm{Amp}_i\right|^p} \tag{10}$$

In order to increase the richness of information contained in distance, a multi-dimensional distance space is constructed by using a variety of different distances in this paper, where $p = 2, 1, \infty$. The multi-dimensional distance space of the test results are shown in Figure 10. It can be seen that 44 groups of the distance data of all 50 groups of FPGAs without hardware Trojan is near the origin, and there is no test data of FPGA with hardware Trojan in the same area of the axis of $p = 1$ is less than 0.6 and the axis of $p = 2$ is less than 0.76. In this area, a high detection accuracy about 100% on picking out the FPGAs without hardware Trojans can be reached via the proposed method based on radiation emissions. It also shows that about 88% of the FPGAs without hardware Trojans is in the area that we picked out. In conclusion, via the proposed method based on radiation emissions, we can pick out most of the FPGAs without hardware Trojans ignoring the risk of picking FPGA implanted with hardware Trojan out.

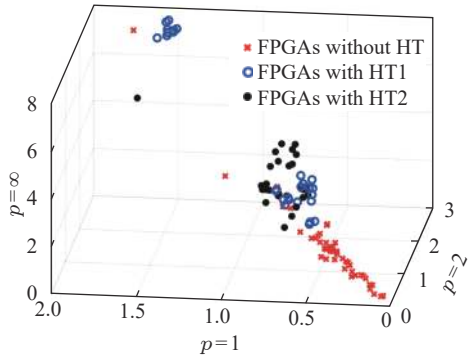


Figure 10 The test results of the FPGAs under three states.

V. Conclusion

In this paper, a novel hardware Trojan detection technique based on electromagnetic radiated emission of integrated circuits is proposed. A hardware Trojan detection system consideration of the propagation loss of electromagnetic radiated emission in space is built to validate the proposed method. In order to increase the richness of information contained in distance, a multi-dimensional distance space is constructed by using a variety of different distances in this paper. Experiment results shows that the proposed method has high detection accuracy in picking out the FPGAs without hardware Trojans and can distinguish FPGAs with small hardware Trojans (less than 100 registers) from the FPGA without hardware Trojans. The same testing method can be extended to hardware Trojan detection of other types of integrated circuits.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (Grant No. 61631002).

References

[1] X. X. Wang, D. R. Zhang, M. He, *et al.*, "Secure scan and test using obfuscation throughout supply Chain," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 9, pp. 1867–1880, 2018.

[2] D. Forte, S. Bhunia, and M. M. Tehranipoor, *Hardware Protection through Obfuscation*. Springer, Cham, Switzerland, pp.3-5, 2017.

[3] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10–25, 2010.

[4] M. M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the hardware snatchers," *IEEE Spectrum*, vol. 54, no. 5, pp. 36–41, 2017.

[5] S. Adee, "The hunt for the kill switch," *IEEE Spectrum*, vol. 45, no. 5, pp. 34–39, 2008.

[6] J. Kumagai, "Chip detectives [reverse engineering]," *IEEE Spectrum*, vol. 37, no. 11, pp. 43–48, 2000.

[7] S. Bhunia, M. S. Hsiao, M. Banga, *et al.*, "Hardware Trojan attacks: Threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[8] D. Agrawal, S. Baktir, D. Karakoyunlu, *et al.*, "Trojan detection using IC fingerprinting," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp.296–310, 2007.

[9] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," in *Proceedings of the 2009 IEEE International High Level Design Validation and Test Workshop*, San Francisco, CA, USA, pp.166–171, 2009.

[10] X. X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in *Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, Anaheim, CA, USA, pp.15–19, 2008.

[11] Y. Q. Lv, Q. Zhou, Y. C. Cai, *et al*, "Trusted Integrated Circuits: The Problem and Challenges.", *Journal of Computer Science and Technology,* vol. 29 , pp.918–928, 2014.

[12] R. Torrance and D. James, "Reverse engineering in the semiconductor industry," in *Proceedings of the 2007 IEEE Custom Integrated Circuits Conference*, San Jose, CA, USA, pp.429–436, 2007.

[13] J. A. Kash, J. C. Tsang, and D. R. Knebel, "Method and apparatus for reverse engineering integrated circuits by monitoring optical emission," US Patent US6496022B1, 2002-12-17.

[14] J. Aarestad, D. Acharyya, R. Rad, *et al.*, "Detecting trojans

through leakage current analysis using multiple supply pad I_{DDQ}s," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 893–904, 2010.

[15] Y. Alkabani and F. Koushanfar, "Consistency-based characterization for IC Trojan detection," in *Proceedings of the 2009 IEEE/ACM International Conference on Computer-Aided Design-Digest of Technical Papers*, San Jose, CA, USA, pp.123–127, 2009.

[16] M. Potkonjak, A. Nahapetian, M. Nelson, *et al.*, "Hardware Trojan horse detection using gate-level characterization," in *Proceedings of the 2009 46th ACM/IEEE Design Automation Conference*, San Francisco, CA, USA, pp.688–693, 2009.

[17] J. Li and J. Lach, "At-speed delay characterization for IC authentication and Trojan Horse detection," in *Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, Anaheim, CA, USA, pp.8–14, 2008.

[18] Y. K. Tang, S. Q. Li, L. Fang, *et al.*, "Golden-chip-free hardware trojan detection through quiescent thermal maps," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2872–2883, 2019.

[19] B. Y. Zhou, A. Aksoylar, K. Vigil, *et al.*, "Hardware Trojan detection using backside optical imaging," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 1, pp. 24–37, 2021.

[20] D. L. Su, S. G. Xie, A. X. Chen, *et al.*, "Basic emission waveform theory: A novel interpretation and source identification method for electromagnetic emission of complex systems," *IEEE Transactions on Electromagnetic Compatibility*, vol. 60, no. 5, pp. 1330–1339, 2018.

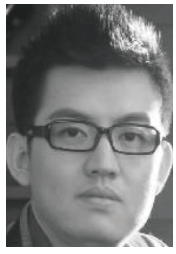
[21] J. W. Wang, Z. W. Yan, C. S. Fu, *et al.*, "Near-field precision measurement system of high-density integrated module," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, article no. 9509109, 2021.

[22] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*. Springer, Berlin, 2002.

[23] H. Salmani, M. Tehranipoor, and R. Karri, "On design vulnerability analysis and trust benchmarks development," in *Proceedings of the 2013 IEEE 31st International Conference on Computer Design (ICCD)*, Asheville, NC, USA, pp.471–474, 2013.

Fan ZHANG received the B.S. and M.S. degrees in electrical engineering from UESTC, Chengdu, China, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree at Beihang University, Beijing, China. His current research interests include antennas and radiation emission identification in EMC area. (Email: fanzhangee@buaa.edu.cn)

Dongrong ZHANG received the B.S. degree in electrical engineering from Beihang University, Beijing, China, in 2016, and the Ph.D. degree in electrical science and technology from Beihang University, Beijing, China, in 2022. In August 2022, he joined the Zhongguancun Laboratory as an Assistant Researcher. His current research field is hardware security and reliability, which include on-chip monitoring, physical design, on-chip dynamic adaptation methodologies, and counterfeit IC/PCB detection.
(Email: dongrongzhang@buaa.edu.cn)



Qiang REN received the B.S. degree in electrical engineering from Beihang University, Beijing, China, in 2008, and the M.S. degrees in electrical engineering from the Institute of Acoustics, Chinese Academy of Sciences, Beijing, in 2011, and the Ph.D. degree in electrical engineering from Duke University, Durham, NC, USA, in 2015. From 2016 to 2017, he was a Postdoctoral Researcher with the Computational Electromagnetics and Antennas Research Laboratory (CEARL), The Pennsylvania State University, University Park, PA, USA. In September 2017, he joined the School of Electronics and Information Engineering, Beihang University, Beijing, China, as an "Excellent Hundred" Associate Professor. His current research interests include numerical methods for multiscale and multiphysics modeling, metasurfaces, inverse scattering, and parallel computing.
(Email: qiangren@buaa.edu.cn)

Aixin CHEN received the Ph.D. degree in electromagnetic field and microwave technology from University of Electronic Science and Technology of China, Chengdu, China, in 1999. From 2000 to 2002, he was a Postdoctoral Fellow with the School of Electronic Information and Engineering, Beihang University, Beijing, China, where he is currently a Professor. His research interests mainly include antennas and electromagnetic compatibility. (Email: axchen@buaa.edu.cn)

Donglin SU received the B.S., M.S., and Ph.D. degrees in electrical engineering from Beihang University (BUAA), Beijing, China, in 1983, 1986, and 1999, respectively. In 1986, she joined the Faculty of School of Electronics and Information Engineering, BUAA, where she was first an Assistant, then a Lecturer, later on an Associate Professor, and is currently a Full Professor. Her research interests include the numerical methods for microwave and millimeter-wave integrated circuits and systematic electromagnetic compatibility design of various aircrafts.
(Email: sdl@buaa.edu.cn)