International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:11, No:5, 2017

Analysis of Lightweight Register Hardware Threat

Yang Luo, Beibei Wang

***Abstract*—**In this paper, we present a design methodology of lightweight register transfer level (RTL) hardware threat implemented based on a MAX II FPGA platform. The dynamic power consumed by the toggling of the various bit of registers as well as the dynamic power consumed per unit of logic circuits were analyzed. The hardware threat was designed taking advantage of the differences in dynamic power consumed per unit of logic circuits to hide the transfer information. The experiment result shows that the register hardware threat was successfully implemented by using different dynamic power consumed per unit of logic circuits to hide the key information of DES encryption module. It needs more than 100000 sample curves to reduce the background noise by comparing the sample space when it completely meets the time alignment requirement. In additional, an external trigger signal is playing a very important role to detect the hardware threat in this experiment.

***Keywords*—**Side-channel analysis, hardware threat, register transfer level, dynamic power.

I. Introduction

CURRENTLY, IC chip manufacture is showing an increasing trend of global cooperation, which shortens the development cycle, helps integrate various technologies, with the products manufactured in foundries at reduced costs. Therefore, the entire manufacturing process cannot be controlled by IC chip design companies. There are lots of security concerns in IC chip production process in terms of hardware Trojan injection and detection technology. We define the concept of hardware Trojan as a mechanism which changes the IC original circuit, inserts an additional malicious function in the original module, changing the device characteristics and behavior of the target device. In addition, the normal hardware functions were reassembled by trigger components, and this behavior was called the hardware threat. Generally, the hardware Trojan is composed of trigger and payload components. No standard procedure exists in the design of hardware Trojans or hardware threat; however, there does exist a wide variety of hardware Trojans posing threats to the transmission of information via hardware. Several hardware Trojan or hardware threat detection methods have been proposed in the past ten years. Simply put, there are three major categories: one is reverse engineering analysis technology using the tools like FIB (Focused Ion Beam), Nano-Probe, OBIC (Optical Beam Induced Current), EBT (Electron Beam Testing), LVP (Laser Voltage Probing), OBIRCH, VC (also called semi-invasive chip analysis techniques [1]-[3] or invasive chip analysis techniques [4]-[11]. But, they require extremely expensive instruments and time consuming operations. (It is almost an impossible mission to find the embedded tiny hardware Trojan due to the complexities of modern chip process technology). Because the payload of a hardware Trojan is triggered by waiting for the trigger condition from non-work state, the second category is trying to guess the activation conditions and inject rare events and vectors into the chip [12]-[16] in order to view the changes in the physical information of the chip. For example, information delay, thermal emission, echo response, and expected responses of information. But, this might not work in situations where the Trojan is activated under rare conditions. The third category is electrical information analysis by using side-channel sniff technology [17]-[19], e.g. electro-magnetic emission, photonics emission and power consumed, which belong to non-invasive chip analysis technique [20]-[24]. Nevertheless, these methods must be based on the availability of a golden chip sample. The analysis results of the DUT will be compared against the analysis results of the golden chip to tell whether a hardware Trojan or hardware threat exists. However, the effectiveness of side-channel analysis methods greatly depends on the sensitivity of the measuring equipment. Non-invasive chip analysis has two mainly methods including simple electromagnetic analysis (SEMA) and simple power analysis (SPA) of CMOS circuits. Wherein, the electromagnetic side-channel analysis is sensitive to background environmental, effective information is easily drowned in environmental noise. Nonetheless, circuit power consumed is easier to sample and analysis than SEMA technique [19].

In this paper, we present the design and implementation of a RTL flipped register hardware threat based on a FPGA development board. This register hardware threat leaked the first 16-bit (1010110100000000) of DES private key on the total power consumed by using various number of flipped registers. The design of register hardware threat is detailed in this paper. The hidden mode of leaked key information was analyzed in detail in the total power consumed based on the effective register flip power consumed. A lightweight detection method is proposed by comparing the three numbers of samples (n=100, n=1000, n=100000). We reach the conclusion that the hardware threat detection feature curves of power consumed should be more than 100 thousand samples. This work realized a lightweight approach and basic parameter to detect the power consumed by register hardware threat.

II. Preliminaries and Threat Set-Up

The power consumed of a CMOS circuit is mainly composed of static and dynamic power consumed. There is always some

Yang Luo is with the China Information Technology Security Evaluation Center, Researcher, China (phone: +86-18810529167, fax: +8610-82341195, e-mail: mddr@163.com).

Beibei Wang, was with the Department of Microelectronics and Nanoelectronics, Tsinghua University. She is currently with the China Information Technology Security Evaluation Center, China (e-mail: 18515523883@163. com).

leakage current in MOS circuits due to the principle of physical device, which is the static power consumed of CMOS device. Although it continually decreases due to the evolution of device process technology, it will always exist. Chip designs usually set the limit of maximum static power consumed. And dynamic power consumed is the sum of the current consumed by the chip capacitor and internal and external short circuit constituted when transistors change states. Therefore, the analysis process is a major step in the analysis of the dynamic power consumed to learn the internal status of the circuit and prepare for reverse engineering. Dynamic power consumed is generally composed of circuit register flip, short, competition and adventure. There are two factors to detect the hardware threat in chip circuit:

1) Average power consumed, the value is the average of the total power consumed in a period of time. It affects the physical characteristics in terms of thermal effects.
2) Instantaneous power consumed, which can be obtained by measuring at any time. It usually expresses the power consumed in a number of instruction execution cycles.

The total power consumed can be summarized as:

$$P = (\frac{1}{2} \cdot C \cdot V_{DD}^2 + Q_{se} \cdot V_{DD}) \cdot f \cdot N + I_{leak} \cdot V_{DD} \quad (1)$$

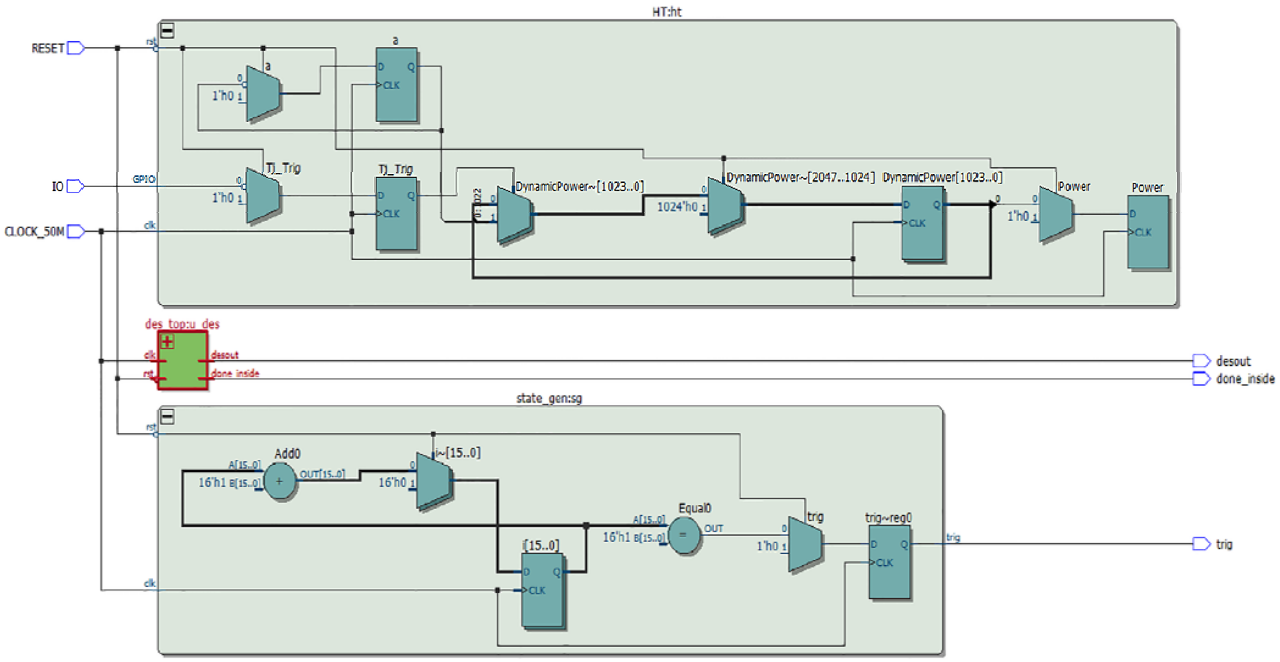

Fig. 1 The RTL view of entire circuit module

The term $(\frac{1}{2} \cdot C \cdot V_{DD}^2 + Q_{se} \cdot V_{DD}) \cdot f \cdot N$ in (1) is dynamic power, which is proportional to the operation frequency f of the switching device (Clock Frequency). In (1), C is switching capacitance, V_{DD} is the supply voltage, N is the switching activity, Q_{se} is technology dependent parameter. We can see from the formula that the overall power consumption is reduced if the circuit is operated at lower frequency. So, if there are different clock generator systems between security module and hardware threat circuit, we can reduce the clock frequency of a security module to increase the dynamic power of hardware threat accounting for the major set. The hardware threat could be more easily detected when the security module was operated at very low frequency, since the power consumed by hardware threat will make up a greater portion of the total power consumed [25].

The whole project was implemented on a FPGA chip, consisting of a register module as the hardware threat, a DES encryption module and a trigger module. All the modules share a common clock source so the frequency reduction technique cannot be used to detect hardware threat. The DES encryption module has been working as a power scramble. The purpose of this experiment is to find out the relationship between flip-power consumed by various numbers of registers and detection sensitivity. The aim which is joined a DES encryption module in the chip running time modules is to achieve the different proportion analysis of hardware threats in chip actual module. The RTL view of the entire circuit is shown in Fig. 1. The FPGA development board is shown in Fig. 2.

The numbers of registers module flipping are divided into: 32-bit, 128-bit, 512-bit, 1024-bit for dynamic power comparison and analysis. Although the hardware circuit always exists in the chip, there is only static power consumed because hardware threat is not activated when the registers are not flipped. In order to reveal the relationship of the blind flip chip register number and power consumed, LeCroy 104Xi-A 1GHz oscilloscope is used.

Fig. 2 The real FPGA experimental development board

Sample space data are very limited due to the limited storage capacity of the oscilloscope, and the monitor IO data collection program could not be completed align on the many sets of data, so we set hardware threat trigger condition as an external IO port. When IO port power is grounded, the hardware threat is not activated. When the IO port is set to V_{DD}, the hardware threat is activated. The average curve of 100000 sample curves was obtained by using Inspector security analysis software. The detailed comparison of the parameters of the experiment is shown in Table I. From Table I, it can be seen when the hardware threat registers flipped to 32bit and 128bit, the dynamic power consumed gap is minimum and the gap of dynamic power consumed per logic unit is the maximum. When the register flips to 32bit, it leaks information "0", and when the register flips 128bit it leaks information "1". Experimental results are shown in Fig. 3 in orange curve. When the register flips to 512bit, it leaks information "0", and when the register flips 1024bit it leaks information "1". Experimental results are shown in Fig. 3 in blue curve. The comparison experiment results show that it is possible to hide the key information by using nonlinear relationship of dynamic power consumed per logic unit. If the dynamic power consumed per logic unit is not in nonlinear relationship that will make it vulnerable to hardware threat through security analysis.

III. Detection Method of Register Hardware Threat

The register hardware threat mainly exists in scattered form to avoid the hot from the local focus and the regional magnetic anomaly detection. Meanwhile, there are four types of trigger conditions to leak information:

1) user input triggered;
2) always on;
3) physical parameter triggered;
4) time triggered.

TABLE I
Units for Logic and Dynamic Power Consumed Properties

Element \ Bit	32-bit	128-bit	512-bit	1024-bit
HT logic /n	71	263	1031	2055
Total logic /n	1214	1408	2180	3200
Scale /%	5.848%	18.6789%	47.2935%	64.2187%
Total Power without HT	40.3246	42.8479	42.4897	54.3692
Total Power with HT	41.3630	44.9980	47.6988	66.9047
Dynamic Power	1.0384	2.1501	5.2091	12.5355
Dynamic power per area	0.014625	0.0081752	0.0050524	0.0061

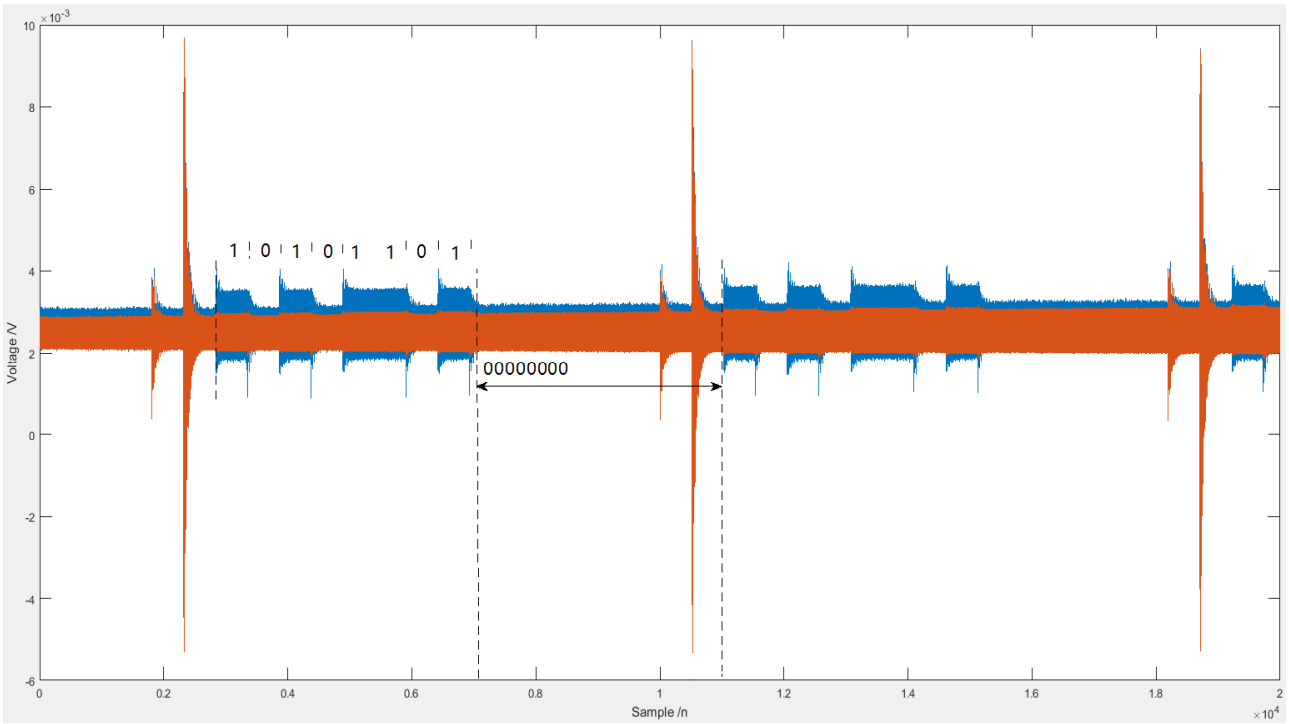

Fig. 3 Comparison view of leaking key in different numbers bit of register

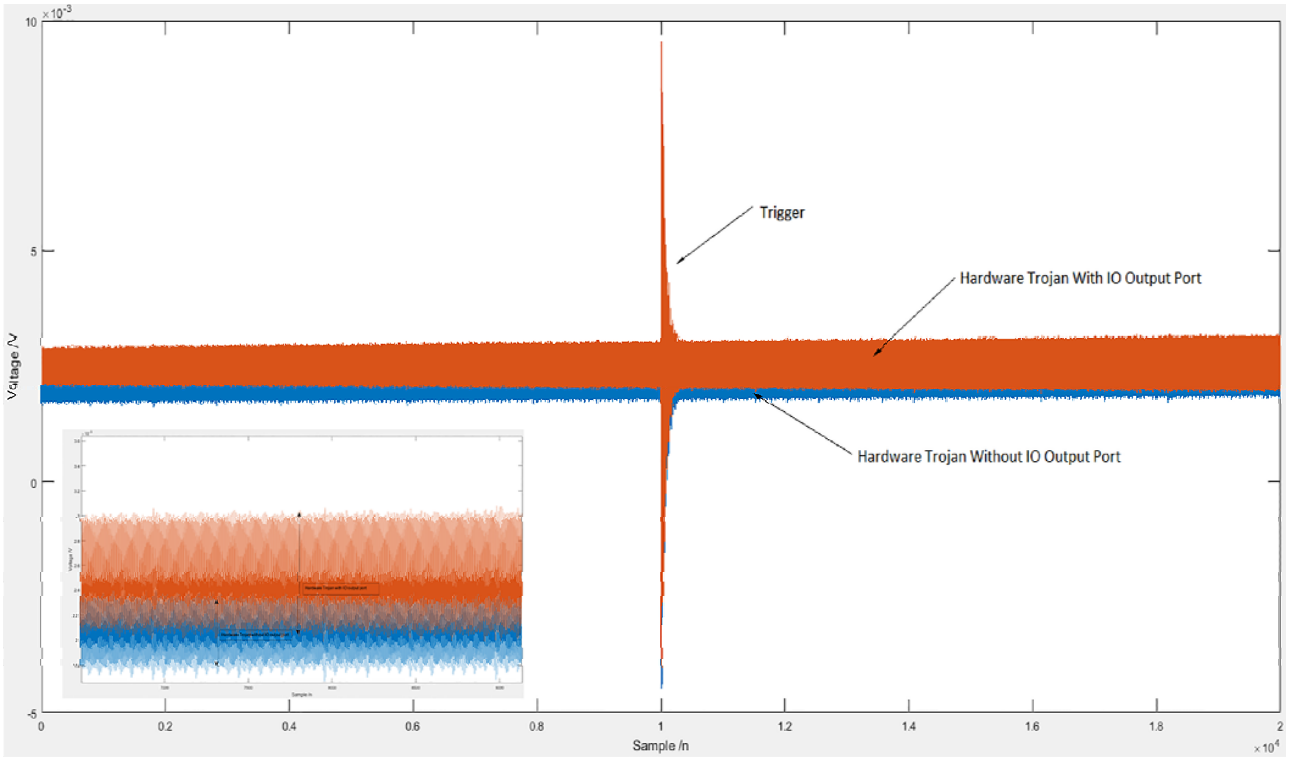

Fig. 4 The effect on dynamic power consumed by bounding output to GPIO ports

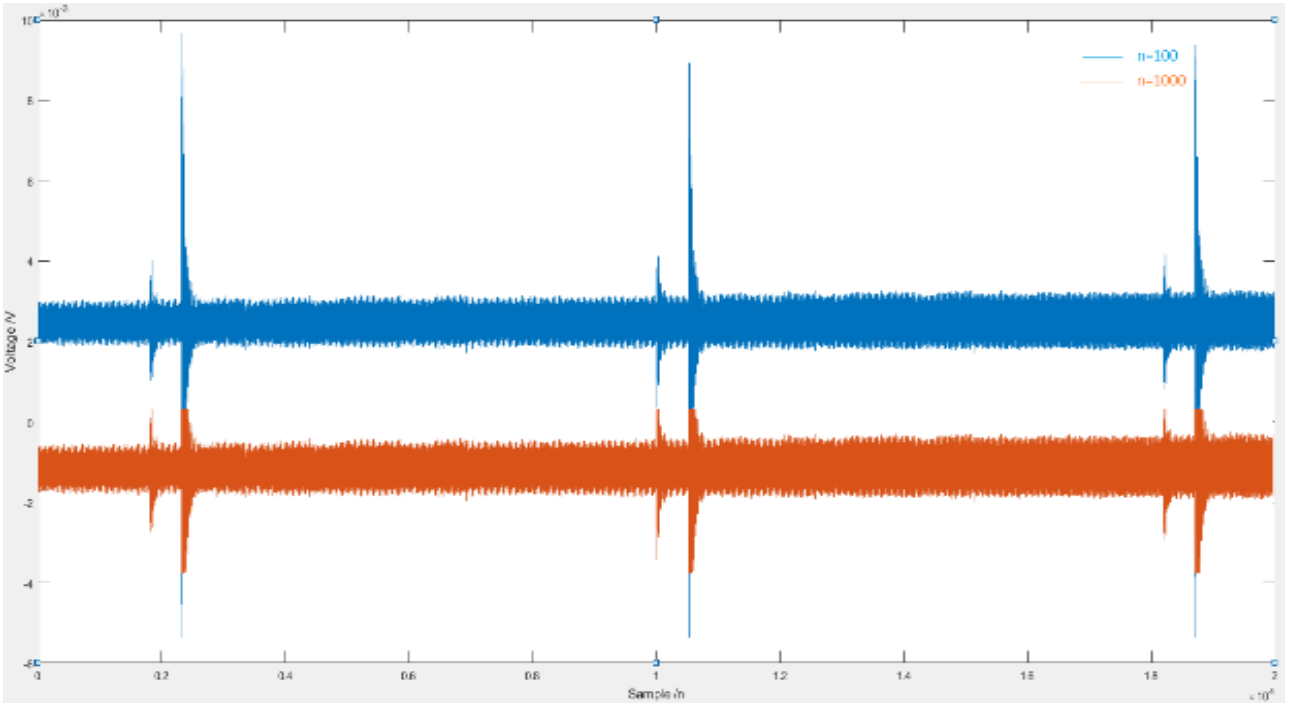

Fig. 5 The average feature curves of samples n=100 and n=1000

In our experiments, we found that hardware threat usually does not output bound to GPIO ports, because the registers flip to the IO output port will cause high dynamic power consumed due to charge and discharge of the capacitor. The effect on dynamic power consumed by bounding output to GPIO ports by hardware threat is shown in Fig. 4.

At present, we do not have a defined process to detect hardware threat for blind chip. The key is the alignment of the trigger time to analyze power leakage feature curves. In order to explain the problem, hardware threat registers set the triggering signal to the GPIO port when it returned. It is significant to analyze the curves in the same process after triggering the hardware threat.

1) Always on hardware threat detection, generally, the moment of power on is used as the trigger signal.
2) User input triggered hardware threat detection, it will imitate all sensitive information, vector, rare event.
3) Physical parameter triggered hardware threat detection, physical pressure test method is used to satisfy physical conditions to trigger hardware threat.
4) Time triggered hardware threat detection, from the point of view of the attacker, time triggered hardware threat usually leaked information in a short time. Its interval time is very accurate and short, then the power consumed increases transiently. That time can be seen on the oscilloscope trigger signal, then the curves could be captured.

There is an important problem to handle that is data sample space after time alignment trigger signals. In this experiment, the effect on the number of samples was analyzed by comparing various numbers of average samples feature curves. The number of samples n=100 and n=1000 is compared in Fig. 5, which shows that the leaked information is not easy to distinguish in precise time alignment of average of two curves. It could discern leaked key bits of DES encryption module basically when increased the number of samples of curves (n=100000) in Fig. 6.

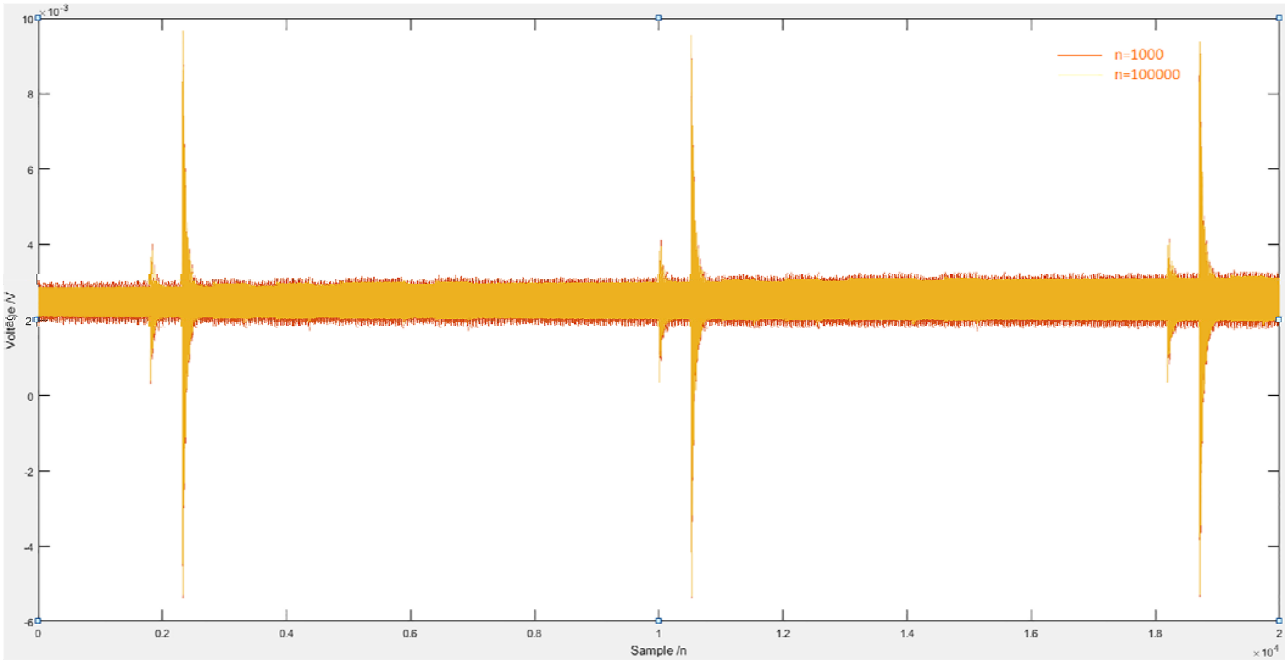

Fig. 6 The average feature curves of samples n=1000 and n=100000

IV. Conclusions

In this paper, we present implementation and analysis method of a lightweight register transit level (RTL) register hardware threat based on a MAX II FPGA. The dynamic power consumed by various numbers of flipping register was obtained and analyzed. The experiment result showed that it was successful to design the register hardware threat by using various dynamic power consumed per unit of logic circuits to hide the key information of the encryption module. Currently, more than 100 side-channel analysis methods of detection hardware threats had been proposed by researchers. Although none of them is considered the standard processes or authoritative guide to detect the hardware threats, side-channel information analysis is the trade-off at cost, time and accuracy.

Hiding the power consumption of flipping registers with different sizes in the total power consumption of the chip, which is way the register hardware threat works, is analyzed in this paper. An attacker not only extracts leaked information but also prevents the detection of hardware threat. Furthermore, this paper explains the importance of the presence or absence of external trigger signal to detect the presence of hardware threats. Thus, hidden prompt trigger information to attacker is the key to the successful design of a hardware threat. The average feature curve was obtained by selecting the prompt trigger as the alignment trigger signal. It needs to sample 100000 times at least to reduce the influence of background noise. We studied the hardware threat in order to detect whether it exist. Further work will be focused on intelligent hardware Trojans defined as the next generation of hardware Trojans compromise of firmware, the low level driver system, hardware circuit to extract core private keys of security chip.

ACKNOWLEDGMENT

The authors express their appreciations to Yanju Zhu, who is currently a Ph.D candidate at Beijing University of Aeronautics and Astronautics. This project is supported by the National Natural Science Foundation of China (Grant Nos. 61402536).

REFERENCES

[1] D. Nedospasov, J. P. Seifert, C. Helfmeier, C. Boit, "Invasive PUF Analysis," Proceedings of Fault Diagnosis and Tolerance in Cryptography Santa Barbara, CA Aug. 20, 2013, p30-41.

[2] M. Fyrbiak, C. Kison, W. Adi, "Construction of Software-Based Digital Physical Clone Resistant Functions," Proceedings of Emerging Security Technologies Cambridge Sept. 9-11, 2013, p109.

[3] D. G. Liu, Q. Dong, "Combating side-channel attacks using key management," Proceedings of IEEE International Symposium on Parallel & Distributed Processing Rome May 23-29, 2009, p1-8.

[4] P. Y. Chen, R. C. Fang, R. Liu, C. Chakrabarti, Y. Cao, S. M.Yu, "Exploiting resistive cross-point array for compact design of physical unclonable function," Proceedings of IEEE International Symposium on Hardware Oriented Security and Trust Washington, DC May 5-7, 2015, p26.

[5] S. Chen, J. L. Chen, D. Forte, J. Di, M. Tehranipoor, L. Wang, "Chip-level Anti-Reverse Engineering using Transformable Interconnects," Proceedings of IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems Amherst, MA Oct. 12-14, 2015, p109-115.

[6] M. L. Wan, Z. Q. He, S. Han, K. Dai, X. C. Zou, "An Invasive-Attack-Resistant PUF Based on Switched-Capacitor Circuit," IEEE Trans. On Circuits and Systems I: Regular Papers, vol. 62, p2024-2034.

[7] Y. F. Xie, X. Y. Xue, J. G. Yang, Y. Y. Lin, Q. T. Zou, R. Huang, J. G. Wu, "A Logic Resistive Memory Chip for Embedded Key Storage with Physical Security," IEEE Trans. On Circuits and Systems II: Express Briefs vol. 63 p336-340.

[8] C. Boit, C. Helfmeier, U. Kerst, "Security Risks Posed by Modern IC Debug and Diagnosis Tools," Proceedings of Fault Diagnosis and Tolerance in Cryptography Santa Barbara, CA Aug.20-20, 2013, p3-15.

[9] P. Choi, D. K. Kim, "Design of security enhanced TPM chip against invasive physical attacks," Proceedings of IEEE International Symposium on Circuits and Systems Seoul, Korea (South) May 20-23, 2012, p1787-1790.

[10] U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, G. Csaba, "Applications of High-Capacity Crossbar Memories in Cryptography," IEEE Trans. On Nanotechnology vol. 10, pp.489-498.

[11] K. Kursawe, A. R. Sadeghi, D. Schellekens, B. Skoric, P. Tuyls, "Reconfigurable Physical Unclonable Functions–Enabling Technology for Tamper- Resistant Storage," Proceedings of Hardware-Oriented Security and Trust Francisco, CA July 27-27, 2009, pp. 22-30.

[12] B. Mainak, S. H. Michael, "A Region Based Approach for the Identification of Hardware Trojans," Bradley Department of Electrical and Computer Engineering, Virginia Tech., Host'08, 2008.

[13] F. Wolff, C. Papachristou, S. Bhunia, R. S. Chakraborty, "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme," In Proceedings of the IEEE Design Automation and Test in Europe, Munich, Germany, 10-14 March 2008, pp.1362-1365.

[14] A. Waksman, M. Suozzo, S. Sethumadhavan, "FANCI: Identification of Stealthy Malicious Logic Using Boolean Functional Analysis," In Proceedings of the ACM SIGSAC Conference on Computer & Communications Security (CCS'13), Berlin, Germany, 4–8 November 2013, pp. 697–708.

[15] M. Hicks, M. Finnicum, S. T. King, M. M. K. Martin, J. M. Smith, "Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically," In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010, pp. 159–172.

[16] H. Salmani, M. Tehranipoor, J. Plusquellic, "New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time," In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust, Francisco, CA, USA, 27–27 July 2009, pp. 66–73.

[17] R. M. Rad, X. Wang, M. Tehranipoor, J. Plusquellic, "Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans," In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, San Jose, CA, USA, 10–13 November 2008, pp. 632–639.

[18] R. Rad, J. Plusquellic, M. Tehranipoor, "Sensitivity Analysis to Hardware Trojans Using Power Supply Transient Signals," In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust, Anaheim, CA, USA, 9 June 2008, pp. 3–7.

[19] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar, "Trojan Detection using IC Fingerprinting," In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 20–23 May 2007, pp. 296–310.

[20] T. Xu, J. B. Wendt, M. Potkonjak,"Matched Digital PUFs for Low Power Security in Implantable Medical Devices," Proceedings of Healthcare Informatics Verona, Sept.15-17, 2014,pp.33-38.

[21] L. Zhang, Z. H. Kong, C. H. Chang, "PCKGen: A Phase Change Memory based cryptographic key generator," Proceedings of IEEE International Symposium on Circuits and Systems Beijing, May 19-23, 2013, pp.1444-1447.

[22] Y-I. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, "Map-Based Analysis of IEMI Fault Injection into Cryptographic Devices," Proceedings of IEEE International Symposium on Electromagnetic Compatibility Denver, CO Aug. 5-9, 2013, pp.829-834.

[23] Y-I. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, H. Sone, "Precisely timed IEMI fault injection synchronized with EM information leakage," Proceedings of IEEE International Symposium on Electromagnetic Compatibility Long Beach, CA Aug. 14-19, 2011, pp.738-742.

[24] Pongaliur K, Abraham Z, Liu A X, Xiao L, Kempel L 2008 Proceedings of High Assurance Systems Engineering Symposium Nanjing Dec. 3-5 2008 p353.

[25] K. Nowaka, G. Carpenter, F. Gebara, J. Schaub, D. Agarwal, P. Rohatgi, W. E. Hall, S. Baktir, D. Karakoyunlu, B. Sunar, "IC Fingerprinting and Stable IS Sensors for Enhanced IC Trust," 2006.