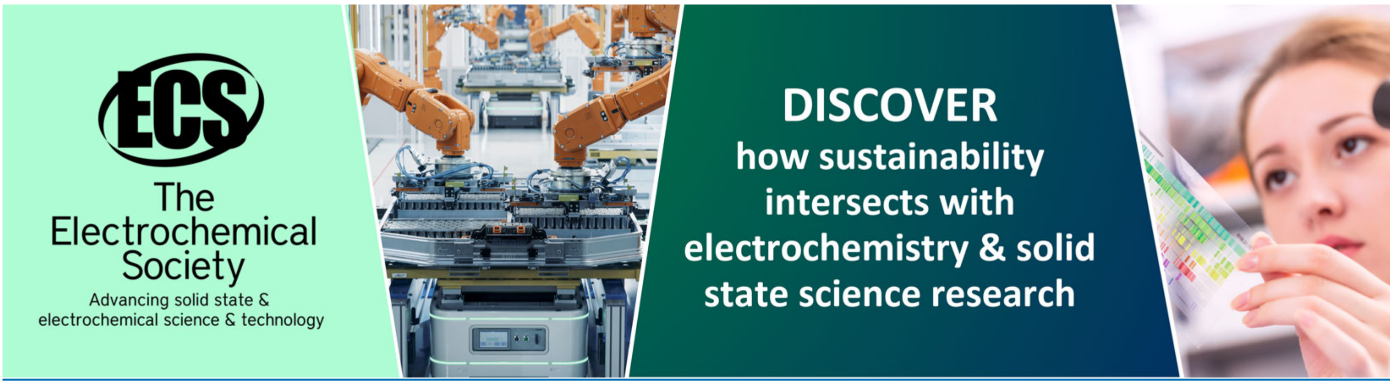
Journal of Physics: Conference Series

An EHW - based Anti - power Consumption Detection Hardware Trojan Implantation Method

To cite this article: Lijun Liu *et al* 2020 *J. Phys.: Conf. Ser.* **1684** 012084


ECS
The Electrochemical Society
Advancing solid state & electrochemical science & technology
DISCOVER
how sustainability intersects with electrochemistry & solid state science research

An EHW - based Anti - power Consumption Detection Hardware Trojan Implantation Method

Lijun Liu[1,a*], Qiao Ding[2,b], Tianyu He[3,c]

[1]Department of Equipment Simulation Training Center, Peoples Liberation Army Engineering University, Shijiazhuang, China

[2]Department of Equipment Simulation Training Center, Peoples Liberation Army Engineering University, Shijiazhuang, China

[3]Department of Basic course, NCO School of Artillery and Air Defense Academy, Shenyang, China

[a*]eyku12@ykzq-it.com

[a]1846554395@qq.com, [b]644097601@qq.com, [c]tianyu_he@126.com

Abstract—Hardware Trojan (HT) is developing towards miniaturization and concealment, but the detection of this kind of HT is still in the research state. The main reason is that the real HT has some problems such as difficult sampling and few kinds, so it is necessary to design the circuit with this kind of HT artificially. Therefore, the EHW technology is introduced to implant this kind of HT, and the original circuit is redesigned to make the power consumption change small and increase the HT function, so as to achieve the effect of concealment.

1. Introduction

With the rapid development of electronic technology, integrated circuit (IC) has been widely used in all aspects of life, from smart phones, computers to satellites, missiles and so on. Its security, reliability, stability are even more important. However, the production and manufacturing process of IC is not safe. For example, in order to speed up the design to buy the third-party IP core, and in order to reduce the cost to manufacture outsourcing and so on. There are potential security risks in the whole production process, which may be implanted Hardware Trojan (HT), resulting in abnormal circuit functions [1-3], seriously affecting people's normal production and life. Therefore, how to ensure the safety and reliability of IC has become an urgent task Hot issues.

In order to detect whether the IC is safe and reliable, many researchers have begun to study the HT detection technology. The main detection methods include side-channel analysis (power consumption [4-6], electromagnetic [7,8], temperature [9, 10], delay [11-13], etc) logic test [14-16], runtime detection, etc. Although these methods can detect some HT, they are not perfect and need further research, for example: 1) The side-channel signals released by small and medium-sized HT in large-scale circuits are not obvious, which makes it difficult to analyze and detect the side-channel analysis. 2) The logic test of the inert nodes can not be fully covered. It can miss the detection of small HT. 3) Runtime detection needs to use additional system resources, which is difficult to ensure the monitoring of all HT behaviors, and there are still loopholes. These problems are mainly related to the lack of research objects, because it is difficult to sample real HT, which makes researchers know too little about such hard to detect HT, how many kinds of HT are, what defects are, and how to detect them efficiently. Therefore, it is necessary to design such HT artificially to provide research objects for detection.

In recent years, the design of HT not only needs to achieve malicious purpose in function, but also needs to consider the problem of concealment. For example, Fern et al. [17] created a covert communication channel between system on chip (SOC)components, which is suitable for any topology and protocol. Sepulveda et al. [18] designed an improved "prime + probe" cache attack against 128 bit advanced encryption standard. For the first time, the design uses bus communication to improve its efficiency. Yang et al. [19] designed an ordinary HT, which can attack the key based on bit string technology with only one trigger.

Although the concealment problem is considered in the design of the above HT, the number of logic gates increases more and the power consumption changes obviously, which is easy to be detected by power consumption detection technology, and the concealment needs to be further improved. To solve this problem, this paper proposes to use EHW technology to implant hidden HT, redesign the original circuit, increase the HT function, and reduce the impact on power consumption as far as possible, so as to achieve the purpose of concealment.

2. Problem Analysis

2.1. Structural Analysis

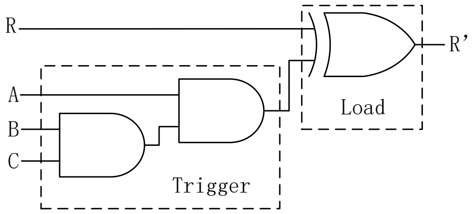


Fig. 1 HT in Combinational Circuit

HT is mainly composed of trigger part and load part. As shown in Fig. 1, implanting HT in the circuit will generally add a certain number of logic gates to realize the HT function, bringing changes in power consumption, electromagnetic and other side-channel signals. Therefore, HT with more logic gates have poor concealment, so it is necessary to reduce the number of logic gates and the impact on various side-channel signals as far as possible.

2.2. Power Consumption Analysis

The power consumption of CMOS logic gate circuit is mainly determined by charge discharge power consumption P_c [20]:

$$p_c = \frac{1}{2} C_L f V_{DD}^2 Z \qquad (1)$$

C_L is the load capacitance of the logic gate, f is the operating frequency, V_{DD} is the supply voltage, Z is the total number of logic gates flipped in the circuit. The first three parameters are fixed in the same circuit, so the power consumption of the circuit is mainly related to the flip of the logic gate.

2.3. EHW technology

The basic idea of EHW technology is the organic combination of evolutionary algorithm and programmable logic devices. Through coding, initial population, cross mutation selection and other operations, a variety of circuits that meet the requirements can be searched according to the truth table.

The EHW technology is used to redesign the circuit to increase the HT function and reduce the impact on the original circuit power consumption as far as possible, so as to improve its anti power detection ability.

3. Experiment and Analysis

3.1. Power Consumption and Logic Gate Change

From the analysis of power consumption, it can be seen that the change of power consumption is mainly related to the flip of logic gate. The changes of logic gate flip caused by the same HT implanted in different circuits are different, that is to say, the power consumption changes are also different.

In order to evaluate the influence of logic gate modification on power consumption variation, the types of logic gates are randomly changed in C6288, C1355, and C880 (ISCAS85 benchmark circuit) circuits to "XOR" logic gates (the flip of logic gates changes greatly). Then, HSPICE simulation software is used to test the average change rate of power consumption, as shown in Table 1. In order to more clearly compare logic gate change quantity influence on the average power consumption rate, get the curve in Fig. 2.

Table 1 Power Consumption Change and Logic Gate Modification

ΔG	$\overline{Q_P}$		
	C6288	C1355	C880
1	0.10	1.67	0.86
2	0.47	2.43	2.76
3	0.48	2.72	3.92
4	0.58	4.27	5.81
5	0.58	6.80	5.91
6	0.51	6.36	7.19
7	0.62	6.82	8.90
8	0.59	5.83	11.84

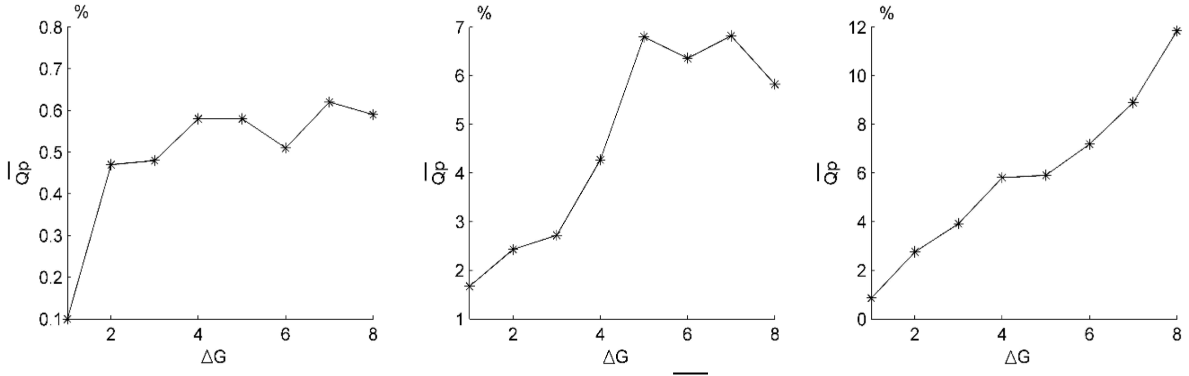


Fig. 2 Change Rate of Average Power Consumption $\overline{Q_P}$ with Modification of Logic Gate ΔG

It can be seen from Table 1 and Fig. 2 that with the increase of logic gate modification variables, the amount of power consumption change is also increasing, but not completely linear increase. It is possible that the logic gate changes more and the power consumption changes little. In this case, the concealment effect of HT is better. Therefore, the smaller the change of the original logic gate is, the better, but it is not absolute. It needs to be analyzed combined with power consumption experiment.

3.2. Implanting Bug-based HT

A sub circuit is intercepted from C1355 (as shown in Fig. 3), and the bug-based HT is implanted, and the comparison experiment is carried out with the direct implanting method.

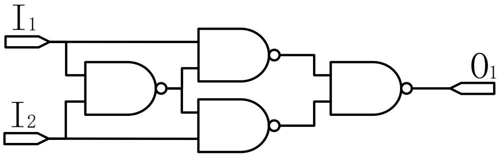


Fig. 3 Original Sub Circuit

According to the function of the original sub circuit, the truth table is obtained. By modifying some bits in the original truth table, the purpose of implanting bug-based HT is achieved, as shown in Table 2.

TABLE 2 TRUTH TABLE

In		Out	
I_1	I_2	Original	Bug-based
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	0

EHW technology is used to evolve the modified truth table. Parameter setting: evolution matrix is5×5, population size is 50, maximum genetic algebra is 1000, and there are 7 logic gates (NOT, AND, NAND, OR, NOR, XOR, XNOR) can be selected. The mutation rate is 0.1, and there is no crossover operation (which is not conducive to evolve). The termination condition is to generate 1000 kinds of circuits that meet the requirements, and select the circuit whose number of logic gates and flip of the logic gate are close to the original sub circuit, as shown in Fig. 4.

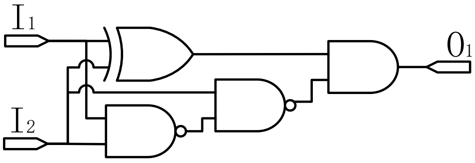


Fig. 4 HT Implanted in EHW Method

By using the direct implanting method, the bug-based HT is implanted, and a certain number of logic gates will be added, as shown in Fig. 5.

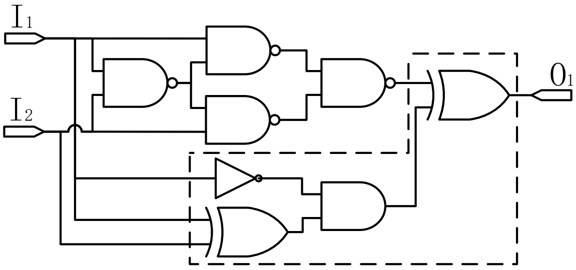


Fig. 5 HT Implanted in Direct Implanting Method

Finally, the HT circuits implanted in the two methods are replaced by the original sub circuits, and the power consumption is tested by HSPICE simulation software. The results are shown in Table 3.

TABLE 3 COMPARISON RESULTS OF THE TWO METHODS

Method	G	$\overline{Q_P}$
Direct	+4	3.76%
EHW	Δ4	2.79%

As can be seen from table 3, compared with the direct implanting method, the total number of logic gates of the HT implanted with EHW technology are not changed, and the power consumption change rate is also relatively low, which reduces by 25.8%. The anti power detection ability is improved and the concealment effect is better.

4. CONCLUSION

Using EHW technology to implant HT and redesign the part of the original circuit, it is possible that the changes of power consumption and logic gate number are relatively small. The ability of anti power detection is strong, and the concealment is good. It shows that the next step needs to focus on this kind of hidden HT.

REFERENCES

[1] S. Bhunia, M. S. Hsiao, M. Banga and S. Narasimhan, “Hardware Trojan Attacks: Threat Analysis and Countermeasures,” Proc. IEEE, vol. 102, no. 8, pp. 1229-1247, Aug. 2014.

[2] Y. Q. Lv, Q. Zhou, Y. C. Cai, and G. Qu, “Trusted integrated circuits: the problem and challenges,” J. Comput. Sci. Technol., vol. 29, no. 5, pp. 918-928, Sept. 2014.

[3] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, “Hardware Trojans: Lessons Learned after One Decade of Research,” ACM Trans. Des. Autom. Electron. Syst., vol. 22, no. 1, pp. 1-23, May 2016.

[4] Y. Jin and D. Sullivan, “Real-time trust evaluation in integrated circuits,” in Proc. Design Autom. Test Europe Conf. Exhibit. (DATE) Dresden, Germany, Mar. 2014, pp. 1-6.

[5] J. Li, L. Ni, J. H. Chen and E. Zhou, “A novel hardware Trojan detection based on BP neural network,” in Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC), Chengdu, China, Oct. 2016, pp. 2790-2794.

[6] L. Ni, J. Li, S. F. Lin and D. Xin, “A method of noise optimization for Hardware Trojans detection based on BP neural network,” in Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC), Chengdu, China, Oct. 2016, pp. 2800-2804.

[7] B. Y. Zhou R. Adato M. Zangeneh et al., “Detecting Hardware Trojans using backside optical imaging of embedded watermarks,” in Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC), San Francisco, CA, USA, Jun. 2015, pp. 1-6.

[8] J. He, Y. Zhao, X. Guo and Y. Jin, “Hardware Trojan Detection Through Chip-Free Electromagnetic Side-Channel Statistical Analysis,” in IEEE Trans. Very Large Scale Integr. VLSI Syst., vol. 25, no. 10, pp. 2939-2948, Oct. 2017.

[9] Nowroz A N, Hu K, Koushanfar F, et al. Novel Techniques for High-Sensitivity Hardware Trojan Detection Using Thermal and Power Maps[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014, 33(12): 1792–1805.

[10] X Zhong, J Wang, B Kan. Hardware Trojan Detection Through Temperature Characteristics Analysis[J]. Journal of Electronics and Information Technology, 2018，40(03)：743-749.

[11] Li J, Lach J. At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection[C]//Proceedings of 2008 IEEE International Workshop on Hardware-Oriented Security and Trust. Anaheim, CA, USA: IEEE, 2008: 8–14.

[12] Jin Y, Makris Y. Hardware Trojan Detection Using Path Delay Fingerprint[C]//Proceedings of 2008 IEEE International Workshop on Hardware-Oriented Security and Trust. Anaheim, CA, USA: IEEE, 2008: 51–57.

[13] Xiao K, Zhang X, Tehranipoor M, et al. A Clock Sweeping Technique for Detecting Hardware Trojans Impacting Circuits Delay[J]. IEEE Design & Test of Computers, 2013, 30(2): 26-34.

[14] A. G. Voyiatzis, K. G. Stefanidis and P. Kitsos, “Efficient triggering of Trojan hardware logic,” in Proc. IEEE 19th Int. Symp. Design Diagnostics Electron. Circuits Syst. (DDECS), Kosice, Slovakia, Apr. 2016, pp. 1-6.

[15] C. A. Kamhoua, H. Zhao, M. Rodriguez and K. A. Kwiat, “A Game-Theoretic Approach for Testing for Hardware Trojans,” IEEE Trans. Multi-Scale Comput. Syst., vol. 2, no. 3, pp. 199-210, July-Sept. 2016.

[16] W. Saad, A. Sanjab, Y. Wang, C. A. Kamhoua and K. A. Kwiat, “Hardware Trojan Detection Game: A Prospect-Theoretic Approach,” IEEE Trans. Veh. Technol., vol. 66, no. 9, pp. 7697-7710, Sept. 2017.

[17] N. Fern, I. San, Ç. K. Koç and K. T. Cheng, “Hiding Hardware Trojan Communication Channels in Partially Specified SoC Bus Functionality,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 36, no. 9, pp. 1435-1444, Sept. 2017.

[18] J. Sepulveda, M. Gross, A. Zankl and G. Sigl, “Exploiting Bus Communication to Improve Cache Attacks on Systems-on-Chips,” in Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI), Bochum, Germany, Jul, 2017, pp. 284-289.

[19] Y. Yang, L. Wu, Y. Yuan, and X. Zhang, “A General Hardware Trojan Technique Targeted on Lightweight Cryptography with Bit-Serial Structure,” in International Conference on Security and Privacy in New Computing Environments Cham, Switzerland: Springer, Apr. 2019, pp. 647-655.

[20] M. F. Xue, A. Q. Hu, J. WANG, “A Novel Hardware Trojan Detection Technique Using Heuristic Partition and Test Pattern Generation,” Chin. J. Electron., vol. 44, no. 5, pp. 1132-1138, May 2016.

[21] Zhang, Jun-Bin;Cai, Jin-Yan;Meng, Ya-Feng;Meng, Tian-Zhen.A novel self-adaptive Circuit design technique based on evolvable hardware[J].International Journal of Automation and Computing.2016：43473.