Reusing Logic Masking to Facilitate Hardware Trojan Detection

Arash Nejat, David Hely, Vincent Beroulle
Université Grenoble Alpes, LCIS: Laboratoire de Conception et d'Intégration des Systèmes, Valence, France
firstname.lastname@lcis.grenoble-inp.fr

Abstract - Hardware Trojan (HT) and Integrated Circuit (IC)/ Intellectual Property (IP) piracy are important threats which may happen in untrusted fabrication foundries. Modifying structurally the ICs/IPs design to counter the HT threats has been proposed, and it is known as Design-For-Hardware-Trust (DFHT). DFHT methods are used in order to facilitate HT detection methods. In addition, logic masking methods modify the IPs/ICs design to harden them against the IP/IC piracy. These methods modify a circuit such that it does not work correctly without applying the correct key. In this paper, we propose DFHT methods leveraging logic masking approach.

I. INTRODUCTION

Despite the fact, fabless semiconductor business model is cost-efficient, it induces security threats. Since the IC layout is available within fabrication foundries, ICs are exposed to the insertion of malicious functionalities during fabrication, the so-called Hardware Trojan (HT). They are also exposed to IP piracy or counterfeiting.

HTs are defined as any malicious alterations of the normal behavior of IC or IP. They may be inserted in ICs by untrusted foundries, or in IPs by IP-developers though the focus of the work is on the first issue. They can for instance either leak confidential information or cause unexpected faults and failures. Regarding the HTs diversity, an abstract model has been proposed which considers that any HT has two distinct parts: the trigger part and the payload part. The trigger part activates the HT while the payload part performs HT missions once it is activated. This model is used in the different HT detection methods. Many different HT detection methods have been presented. They are based on: (1) side-channel-analysis that tries to detect HTs by considering the HT effects on circuit parameters such as power consumption and paths delay, (2) conventional functional/structural tests which aim at triggering HTs by applying proper input patterns and then observing the HT effects on outputs [1].

Side channel analysis faces with two important challenges: Process Variations (PV) and Environment Variations (EV). PVs are variations in some transistor characteristics that happen during IC manufacturing. EVs happen due to changes in the operating environment of the circuit while the circuit is working. The HT side channel effects, especially when the HT is very small, may be undetectable among PV or EV.

The challenge of testing-based HT detection methods is to generate proper test vectors in order to activate hard-to-trig HTs and also to observe the effect of hard-to-observe HTs on outputs. HT designers can design various hard-to-test (hard-to-trig and to observe) HTs by combining many low controllable and observable signals in the circuit. Fortunately increasing the HT size enhances the chance of HT detection by side channel analysis. This is because even a non-triggered HT has effects on the circuit parameters [1]. On the other hand, for small HTs, e.g. HTs made of few gates, side-channel-based HT detection methods may be impotent while testing-based HT detection is more promising.

HT-detection-challenges encourage IP/IC designer to structurally modify the IC/IP design in order to facilitate HT detection methods. This approach is known as Design-For-Hardware-Trust (DFHT) [1]. Many DFHT methods at different abstraction level have been proposed.

In addition, logic masking methods, which have often been miscalled “obfuscation” or “logic encryption” in previous literatures [2], modify the IP/IC such that it does not correctly work without applying the correct key. The modifications can involve both the combinational and the sequential parts. The logic masking of combinational parts, which is the focus of this work, is performed by adding key-inputs and keygates (XOR and XNOR gates). They are added in order to provide two distinct modes: the masked mode and the normal mode. Key-inputs increase the truth table size of the circuit and keygates produce wrong outputs while key-inputs are not fed by the correct keys.

Logic masking has also been proposed as one HT-prevention approach. Indeed, logic masking makes the HT insertion complex. Since the HT attackers during the fabrication stage have a masked design, they may insert unskillful-designed HTs which will be activated while the IC is working in the masked mode [3].

This work focuses on how logic masking methods can be leveraged towards a DFHT method. In section II, we propose to leverage logic masking methods in order to facilitate HT detection methods based on testing approaches and side channel analysis. According to this general baseline, our contribution includes three logic masking methods with three different objectives:

1. To facilitate path delay based HT detection by generating shorter paths for nets which belong only to long paths
2. To facilitate power based HT detection by localizing switching activity.
3. To facilitate test based HT detection by removing rare signals which can be proper for the trigger part of HTs.

We also measure the masking quality for each proposed method. The masking quality can be measured according two main criterions: 1) the Hamming distance (HD) between the correct output and wrong outputs while the key-inputs have the correct value or wrong values [4], 2) the number of mismatch points between the original circuit and its peer masked circuit [5]. This can be reported by formal verification tools.

II. INCREASING THE HT DETECTION CAPABILITIES LEVERAGING LOGIC MASKING

A. Improving path-delay-based HT detection methods

Since short paths have low delay variability [6], the HT induced additional delay would be more detectable if the HT is inserted within a short path. Attackers thus try to avoid inserting HT within such paths. Vulnerable points are these nets that only belong to long paths; and a net is the most vulnerable net, if its including-shortest-path is longer than the including-shortest-path of other nets. We propose an iterative algorithm which generates short fake paths with one keygate for the most vulnerable net, in each iteration. Note that in order to hide the HT-delay-effect, the HT attacker can increase the drive strength and capacity load of the cells which are before and after the HT. Fortunately it increases the success of power based HT detection methods. In [7] we compared the results of this logic masking method with the proposed DFHT method in [6]. Their algorithm makes shorter path for vulnerable nets without any change in functionality and without performing logic masking. The results in [7] show that our masking method has almost the same results as [6] with the same area overhead. In addition in [8] we reported the HT detection improvement after performing technology mapping. Our method enhances the HT detection probability in masked circuits 25%-55%. In addition, the masking quality of our method is compared with [5] and also randomly keygate insertion. In all circuits our method is better than the randomly keygate insertion. And also by accepting more than 10% area overhead, we have almost the same results as [5]; however our method has HT detection improvement. –Our future work includes two measurements: 1) HT detection probability in layout level, 2) the masking quality according to the first explained criteria.

B. Improving power-based HT detection methods

The success of power based detection methods depends on the proportion of HT power consumption to the total power of the circuit (higher proportion, higher HT detection). In addition, both HT and IC power are related to their switching activity (SA). As a result, in order to improve these methods, the SA of HT must be increased while the total power of IC is decreased simultaneously. One solution is to localize SA. It means to increase the SA in one part of the IC, and to decrease it in other parts. As a result, while the IC power is decreased, the HT power is increased if the HT is trigged from the increased-SA (targeted) part. The main purpose here is then to insert the key gate so that they can be used to perform such SA isolation. First, we divide the circuit into different parts, equal to the number of keygate that we can use. Afterward, one keygate is assigned to each part. If one part in normal mode has high (low) SA ratio, a net in the part should be selected such that the part in masked mode has low (high) SA ratio. Our current experiments include 2 main steps: 1) using traditional partitioning algorithm, such as KL or FM algorithm, for the circuit division at gate level, 2) finding the threshold of SA ratio to call a partition has high (low) SA ratio. Our future experiments will target the circuit division and the keygate insertion post placement operations, according to the found threshold.

C. Improving testing-based HT detection methods

As mentioned, low-controllable signals are the best targets for HT attacker. One can combine them and make a very rare event for the HT activation. If a circuit has no low-controllable signal, attackers have to combine more signals to create a rare event condition to trigger the HT. This increases the chance of side-channel-analysis HT detection methods. As a result, we aim at removing low-controllable signals using keygates.

We also propose an iteratively-greedy algorithm which investigates all circuit signals to find the best signal for one keygate-insertion, in each iteration. The algorithm has two objectives: 1) to remove rare signals, and 2) to achieve 50% HD between the correct output and incorrect outputs. In [9], we reported results of the algorithm when it has just the second objective. The achieved average HD of our algorithm [9] and the proposed one in [4] are 49.90% and 48.9%, respectively.

III. CONCLUSION

In this work we have proposed DFHT approaches which leverage logic masking approaches in order to increase HT detection methods. Our approach targets three DFHT methods which increase the HT detectability based on path-delay, power, and testing. The future works will focus on measuring the masking quality of the previously proposed methods. Also, the first implementation has been realized at RT level, further implementations will be performed after post placement.

REFERENCES

[1] Bhunia, S., Hsiao, M. S., Banga, M., & Narasimhan, S. (2014). Hardware Trojan Attacks: Threat Analysis and Countermeasures. Proceedings of the IEEE, 102(8), 1229-1247.

[2] Colombier, B., Bossuet, L., & Hély, D. (2016). From secured logic to IP protection Microprocessors and Microsystems: Embedded Hardware Design (MICPRO), Elsevier, 2016

[3] Nejat, A., Hely, D., & Beroulle, V. (2015, December). Facilitating side channel analysis by obfuscation for Hardware Trojan detection. In 2015 10th International Design & Test Symposium (IDT) (pp. 129-134).

[4] Rajendran, J., Zhang, H., Zhang, C., Rose, G. S., Pino, Y., Sinanoglu, O., & Karri, R. (2015). Fault analysis-based logic encryption. IEEE Transactions on Computers, 64(2), 410-424.

[5] Chakraborty, R. S., & Bhunia, S. (2009). HARPOON: an Obfuscation-based SoC design methodology for hardware protection. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 28(10), 1493-1502.

[6] Shekarian, SMH, & Zamani, MS (2015). Improving hardware Trojan detection by retiming. Microprocessors and Microsystems , 39 (3), 145-156.

[7] Nejat, A., Hely, D., & Beroulle, V. "Reusing Logic Masking to Facilitate Path-Delay-Based Hardware Trojan Detection" in Proceedings of the 22nd IEEE International Symposium on On-Line Testing and Robust System Design(IOLTS), Sant Feliu de Guixols, Catalunya, Spain, 2016.

[8] Nejat, A., Hely, D., & Beroulle, V. "How Logic Masking Can Improve Path Delay Analysis for Hardware Trojan Detection" accepted in the 34nd IEEE International Conference on Computer Design (ICCD), Phoenix, USA, 2016.

[9] Samimi, S.M.S., Aerabi, E., Nejat, A., Fazeli, M.,, Hely, D., Beroulle, V. "High Output Hamming-Distance Achievement by a Greedy Logic Masking Approach" accepted in 14th IEEE East-West Design & Test Symposium (EWDTS), Yerevan, Armenia, 2016.