Microprocessors and Microsystems 38 (2014) 246–252

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

A study on the efficiency of hardware Trojan detection based on path-delay fingerprinting

Arash Nejat [1], Seyed Mohammd Hossein Shekarian [1], Morteza Saheb Zamani *

Department of Computer Engineering and Information Technology, Amirkabir University of Technology, Tehran, Iran

ARTICLE INFO

Article history:
Available online 31 January 2014

Keywords:
Hardware security
Hardware Trojan detection
Design for hardware trust
Analysis of hardware security

ABSTRACT

Hardware Trojan horses (HTHs) are among the most challenging treats to the security of integrated circuits. Path-delay fingerprinting has shown to be a promising HTH detection approach. However, previous work in this area incurs a large hardware cost or requires expensive testing techniques. Moreover, the relation between technology mapping and the efficiency of delay-based HTH detection have not yet been studied. In this paper, we present a HTH detection method which uses an effective test-vector selection scheme and a path-delay measurement structure. Furthermore, we demonstrate the large impact of technology mapping on the effectiveness of delay-based HTH detection. We also show that delay-based detection methods are highly scalable. In case of choosing an area-driven design strategy, the average HTH detection probability of our approach is about 63%, 78% and 90% if false alarm rate is 0%, 2% and 16%, respectively. However, with modifications in the technology mapping, the results show improvements to 85%, 94% and 99%, at the cost of about 20% area overhead. In addition, the efficiency of our method would not decrease for large benchmarks with thousands of gates.

1. Introduction

The high cost of silicon chip fabrication has caused most hardware manufacturers to outsource the fabrication of their integrated circuits (ICs) to the third party foundries [1]. These foundries can serve attackers by modifying the circuit's design or its physical parameters. These modifications, usually known as hardware Trojan horses (HTHs), may change the functionality or reliability of a chip in a disastrous way [1,2].

HTHs are classified into parametric and functional types. Parametric HTHs are modifications in the characteristics of existing wires and gates while functional HTHs are designed by adding or removing gates and transistors [1]. The focus of this paper is on the HTHs of the latter type which usually have more complicated and damaging behaviors. Moreover, this paper concentrates on the HTHs which are inserted into the design during the fabrication process.

HTHs must be triggered by some internal or external events or a sequence of such events, to become operative. A wisely designed HTH is triggered only under rare conditions. For example, the attacker usually uses a rarely-changed signal which already exists in the original circuit as an input of the HTH and designs the HTH in a way that it is triggered only if that signal changes. For this reason, HTHs are not usually detectable by conventional testing methods [1]. Parametric testing or side-channel analysis techniques are reported to be more effective for HTH detection. These techniques are based on the fact that even a non-triggered HTH may change the side-channel properties of the chip [3]. For example, the HTH may change the power consumed by the circuit, or it may alter the delay of some paths in the design [1]. The greatest challenge of these techniques is process variation which may cover the Trojan effects and limit the scalability of the techniques.

Techniques based on path-delay analysis are among the most promising side-channel analysis approaches for HTH detection [4–9]. However, previous efforts in this area are not without limitations. The approach presented in [4] seems to be powerful in detecting HTHs which contribute to the delay of critical paths. However, employing this technique to detect HTHs that only change non-critical path-delays requires a large number of test vectors. Other delay-based HTH detection techniques use delay measurement structures [5–9]. Some of these techniques can reduce the difficulties of detecting HTHs on non-critical paths [7–9] but they incur additional hardware cost and design complexities. Moreover, these techniques do not benefit from a proper design strategy and test vector generation.

* Corresponding author. Tel./fax: +98 2164542720.
E-mail addresses: a.nejat@aut.ac.ir (A. Nejat), shekarian@aut.ac.ir (S.M.H. Shekarian), szamani@aut.ac.ir (M. Saheb Zamani).
[1] Tel.: +98 2164545124.

http://dx.doi.org/10.1016/j.micpro.2014.01.003
0141-9331/

In this paper, we address the challenges of using path-delay measurement to detect HTHs. Our contributions are as follows:

1. A novel HTH detection approach is presented based on path delay fingerprinting. The essence of this technique is to test the delay characteristics at different frequencies. Varying the frequency can simplify delay measurement in non-critical paths. In addition, modified scan chain helps to measure the delay-paths. Our approach needs hardware redundancy in the structure of scan flip-flops (SFF) which are already widely used in ICs for testing various models of faults. An SFF is a flip-flop (FF) with extra scan logic, scan input and scan output which are used during the test mode to set or fetch the value of that FF.
2. Guidelines are presented for the efficient use of some other related ap-proaches in the literature.
3. HTH detection probabilities on paths are estimated based on path-delay characteristics. The detection probabilities are also valid for any HTH detection technique based on single path-delay fingerprinting if the proposed guidelines are followed.
4. The impact of technology mapping on the delay-based techniques is investigated, and design hints are provided to improve the probability of HTH detection.
5. The scalability of delay-based Trojan detection techniques is studied and shown as an important score of this methods compared to the power-based Trojan detection approaches.

Our experiments are conducted on various ISCAS'89 benchmarks. 90 nm process technology is used because there is close accurate information about timing variation in this technology [10]. In case of area-driven technology mapping, the average detection probability of our approach is 63%, 78% and 90% by accepting a zero, 2% and 16% false alarm rate, respectively. However, these detection probabilities correspondingly improve to 85%, 94% and 99% if it is tried to design the circuit with shorter paths due to the less background variation effects of paths with shorter delay. Our experimental results also show that contrary to the power-based HTH detection techniques, the delay-based approaches are intrinsically scalable.

The rest of this paper is organized as follows: Section 2 introduces the previous work. The basic idea of our approach is described in Section 3. The detailed approach is presented in Section 4. Section 5 presents the experimental setup and results. The method used to estimate HTH detection probability is also explained in these sections. Finally, Section 6 concludes the paper and purposes some future works.

2. Previous work

Attackers try to hinder the process of HTH detection by making the trigger conditions as rare as possible. Moreover, the HTHs which only produce analog outputs (e.g., power characteristics) would not be detected even by an exhaustive testing [11]. Hence, it is usually impractical to detect HTHs by using traditional testing methods. Post-design HTHs may not be detected by reverse engineering either, since they may exist only in a portion of fabricated chips [1]. It is noteworthy that reverse engineering is a destructive process, so it is helpful only when applied on a single chip or a small fraction of chips. Many efforts have been made in recent years to develop more convenient methods for HTH detection.

Some test pattern generating approaches are presented in [12–14] to adapt testing techniques for HTH detection. However, these techniques are of limited gain for large circuits. Authors in [3] demonstrated that side-channel analysis is a more efficient approach for detecting HTHs. This is because even non-triggered HTHs may change the side-effect characteristics of a chip recognizably. Two of such characteristics are widely used for the purpose of HTH detection, namely, power consumption [3,15] and path-delays [4–9,16,17]. As it is demonstrated in [8,18], analyzing both power and delay profiles of the circuit is needed to achieve better results. As the focus of this paper is on the path-delay analysis, related work in this area is discussed in the rest of this section.

The first systematic approach for path-delay fingerprinting was presented in [4]. This approach collects the overall delay characteristics of the whole design by analyzing some genuine chips. The genuine chips are assured to be Trojan-free by using invasive techniques. The data is used as a reference to verify the genuineness of other chips. However, HTHs that merely change non-critical path-delays can hardly be detected by this technique.

Shadow registers are used in [5,6] for HTH detection. Each shadow register is placed next to a register in the design, getting the same input as that of the original register. The shadow registers are triggered by a shadow clock signal with a controllable phase offset. Path-delays can be measured by changing the phase offset. Ring oscillators (ROs) are also employed for HTH detection [7,8,16,17]. ROs can be added to a design in a way that they can measure the delay characteristics. The large hardware cost is the main drawback of both structures.

Another delay-based HTH detection approach is introduced in [9], which creates a delay chain by bypassing some of the FFs in the design. Besides 10% area overhead, this technique suffers from leaning on the delay analysis of long paths. These long-delay paths are generated due to the FF bypassing process. As we demonstrate in Section 5, long-delay paths may not be qualified candidates for being tested for HTHs.

3. The basic idea

An intelligent attacker tries to avoid adding an HTH on critical paths (paths with the largest delay). Otherwise, changes in the timing characteristics of the circuit would be simply identifiable. However, changes in the delay of non-critical paths would be unrecognizable by using conventional timing test approaches.

The main idea of the proposed approach is to test the circuit at proper frequencies. Each path is tested at a clock cycle with a period equal to the delay of the path under test. We name this clock cycle as *zero-slack clock cycle*. The slack of a path becomes zero at its corresponding zero-slack clock cycle unless an HTH increases the path-delay. Consequently, the HTH is mapped into a path-delay fault, i.e. a fault that causes the propagation delay of a path to increase beyond its expected value [19]. Now, an SFF can be employed to monitor the path outputs. As in delay-fault test techniques [15], one pair of test vectors must be produced for path-delay fault as well as HTH testing in our approach. The two test vectors are chosen in a way that they cause two complementary values at the output of the path. As a result, these vectors can generate a desirable transition in the target path and propagate the transition to the SFFs. If the delay of a path increases due to the HTH, the correct value cannot pass the path during the zero-slack clock cycle and the SFF will have incorrect value. This issue is illustrated by an example in Fig. 1.

In this figure, it is assumed that all the gates have 1-unit delay and the delay of interconnects is negligible. The critical path has a 3-unit delay, so the minimum allowed clock period is 3 units. The attacker is assumed to connect an HTH (the colored gate) to the output of gate G3. The connections of the trigger circuit to the original circuit are neglected in this figure. The delay of the bold path is increased by 1 unit due to the existence of the HTH. This additional delay is not recognizable by at-speed testing unless a zero-slack clock cycle (here, a clock cycle with a period of 1 unit) makes the bold path sensitive as the critical path.

In summary, our approach maps the chip delay characteristics to observable functional behaviors. The Trojan detection technique