Microelectronics Journal 77 (2018) 16–25

Contents lists available at ScienceDirect

Microelectronics Journal

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

Hardware Trojan detection by timing measurement: Theory and implementation

Hao Xue *, Saiyu Ren

Electrical Engineering, Wright State University, Dayton, OH 45324, USA

ARTICLE INFO

Keywords:
CMOS
Hardware security
Hardware Trojan detection
Timing measurement

ABSTRACT

Due to outsourcing of chip product chain, hardware is vulnerable to be attacked. For example, an attacker who has access to hardware fabrication process can alter the genuine hardware with insertion of concealed hardware elements (Hardware Trojan). Microelectronic circuits are almost always a part of hardware devices, so microelectronic circuit Hardware Trojan (HT) detection becomes a key aspect in hardware security. A novel microelectronic HT detection circuit based on timing analysis is proposed in this paper. The detection circuit can be adopted in combinational and sequential microelectronic circuits. The proposed technique is implemented in IBM 90 nm CMOS process and Xilinx ISE FPGA. Based on experimental results, with one detection circuit embedded in testing-path, an HT with size that is 2.81% of host-circuit size is detectable at detection probability of 90% with a 10% probability of a false positives. Both detectable HT size and detection probability can be improved by adding more detection circuits to testing-path. The probability of false positives is controlled by the testing clock period.

1. Introduction

Microelectronic circuit is not only ubiquitous component of the hardware devices, but also is a key facilitator for devices communicating with other systems. The integrity of microelectronic circuit design and fabrication becomes a major concern for hardware security. Providing a secure environment for microelectronic circuit design does not ensure integrity of the hardware since fabrication is typically outsourced to dedicated integrated circuit (IC) foundries [1–3]. During fabrication process, the genuine IC is potential to be altered by inserting a Hardware Trojan (HT), which involves malicious and clandestine modifications to the fabricated microelectronic device that changes the functionality when compared to the original design [4,5]. An HT can tamper with the host-chip's function [6], modify parametric properties [7] or even have confidential information transmitted to the attacker.

To address the issue of providing robust and reliable IC products, a number of HT-resistant circuit design [8], and HT detection techniques have been developed in the past decade. Authors in Ref. [9] introduced a specific voting circuit to protect from hardware Trojans embedded in third party IP cores during regular operation. Gate-level information-flow tracking in Ref. [10] is effective in detecting HT that can cause undesirable information flow either through a maliciously modified datapath or a covert side channel. These two detection techniques are designed for detecting specific HT. However, general-purpose HT detection techniques are very needed in modern IC process because of its wide applicability. Most of the published general-purpose HT detection methods in post-silicon stage are categorized as HT activation and side-channel analysis. Normally HT circuits are designed stealthily to avoid detection. Activation techniques can wake up a dormant HT to augment the HT effect on the host chip parameters, resulting in enhancement of detection probability [11]. In Refs. [12,13], authors apply specific input patterns to lower host-chip activity while keeping HT active to maximize HT contribution on power consumption of host-chip, eventually increase the detection probability. In Ref. [14], authors use specific input patterns to magnify the timing impact of HT on host-chip.

Side-channel analysis consists of power and timing analysis. Embedded HT will add current paths and loads to the original circuit, that result in extra power consumption on wires and gates in HT affected area. HT can be revealed by measuring the differential power characteristics of the attacked circuit. A self-reference-based power-analysis HT detection methodology is proposed in Refs. [15,16]. IC is partitioned into segments. The differential power consumption in one segment is compared with others to ascertain HT's presence. Statistical analysis is proved to be effective in facilitating HT detection probabilities. In Ref. [17], singular value decomposition and linear programing processing are used to identify the power or delay difference caused by HT.

* Corresponding author.
E-mail address: xue.10@wight.edu (H. Xue).

https://doi.org/10.1016/j.mejo.2018.05.009
Received 29 August 2017; Received in revised form 12 February 2018; Accepted 14 May 2018

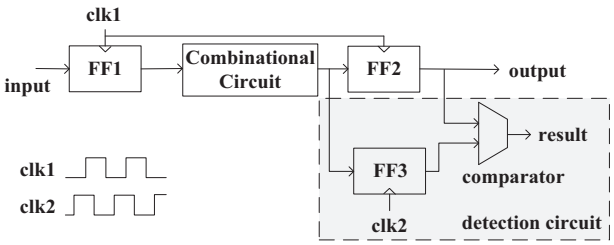

Fig. 1. Block diagram of HT detection circuit using PUF.

In this paper, a timing analysis-based HT detection circuit is proposed and implemented using CMOS 90 nm and Xilinx FPGA. A practical result is obtained in implementations. A HT with size of 2.81% of host-circuit is detectable at detection probability of 90%. Moreover, the detectable HT size and detection probability can be improved by adding more detection circuits in the testing-path. Compared to the state-of-the-art timing analysis-based HT detections, the proposed design incorporates low overhead and tunable detection probability to accommodate different security requirements of circuit designs.

This paper is organized as follows: Section 2 summarizes the existing research work on timing analysis-based HT detection techniques; Section 3 presents the proposed HT detection technique; the proposed HT detection technique is implemented on benchmarks in Section 4; conclusion is included in Section 5.

2. Previous work

Embedded HT will add extra capacitance, resulting in more charging and discharging delays to HT affected paths. HT can be revealed by measuring the differential timing characteristics of the attacked circuit.

Authors in Ref. [14] chose many clean (free of HTs) ICs and ran a variety of input patterns to record specific delays of paths to establish key delay fingerprints. Afterwards, circuits-under-test (CUT) are tested under the same input patterns and verified by comparing timing parameters with genuine fingerprint. Due to the complexity of millions of paths in a complicated chip and instability of golden standards caused by inter and intra-die variations, this method becomes infeasible for large circuit designs.

Instead of comparing with genuine fingerprint, authors in Ref. [18] compare the delay of testing-paths with a set of symmetric paths, which are other paths that have the same topology as the testing-paths. The delay of testing-paths and symmetric paths will be the same unless an inserted HT breaks symmetry. Symmetry can naturally exist in ICs or be artificially added. This method can avoid the difficulty and cost of finding a golden model for all ICs with variable parameters. However, the detection probability suffers from intra-die parameter variation, and the detection method is limited in that huge area-overhead may emerge due to a bulk of artificial symmetries are required. Also, massive effort is accumulated in finding existing symmetric paths and the specific test vectors to measure desired path delays.

Authors in Ref. [19] increase the system clock frequency to create clock glitches until resulting in faulty operation. Then the delay of IC critical paths for several bits are estimated with the faulted outputs and the corresponding clock frequency. The simulated path delays are compared to golden parameters to ascertain security reliability. Statistical analysis method is introduced in Ref. [20] to facilitate the identification of HT. A test-vector selection scheme and a novel timing measurement structure proposed in Ref. [21] are effective in accurate path-delay measurement.

In Ref. [22], a HT detection method based on a *physical unclonable function* (PUF) is proposed, as shown in Fig. 1. It is used to detect HT in register-to-register paths. The registers (*FF1*, *FF2*) in *main circuit* are triggered by the main system clock (*clk1*). Circuits inside the dotted box is HT detection circuitry, and the register in it (*FF3*) is triggered by a shadow clock (*clk2*), which has the same frequency with main system clock (*clk1*) and a controlled negative shift. The negative shift of shadow clock makes *FF3* to be triggered earlier than *FF2*, thereby output of *combinational circuit* arrives *comparator* through *FF3* ahead of it through *FF2*. The shadow clock negative shift is increased until the register outputs are unequal. That clock shift time is claimed to be the *combinational circuit* delay. The *combinational circuit* is suspicious of being HT-attacked if the measured delay is substantially different from the pre-determined designed timing. This technique is at-speed detection, which can be applied at both test-time and run-time, but it requires extra circuit with large over-head to control skewed clock (*clk2*). Moreover, it can only be used in sequential circuit register-to-register paths.

A modified timing analysis-based HT detection technique is proposed in this paper, in which the clock skew control circuit is eliminated to simplify the detection circuit. The experimental results show that the HT detection circuit overhead is competitive compared to state-of-the-art with similar detection probability. The main contributions of this technique are as follows:

- HT detection circuit area, timing, and power overhead on host-circuit are reduced. The proposed detection circuit operates with main system clock, so the specific clock skew control circuit (normally with thousands of gates) for HT detection is eliminated.
- The proposed HT detection technique is not restricted to be applications with register-to-register paths (e.g. [19,22]). This technique can be used on any circuit path by isolating the path with extra registers.
- Location of HT can be estimated. The detection signals of each HT testing-path are read out in series. The path of suspected HT can be determined by the location of abnormal detection signal.
- Tunable detection probability to accommodate different security requirements of circuit designs. HT detection probability can be increased by more detection circuits pairing with one testing-path, meanwhile detection circuit overhead is increased. The selection of testing-path paired with one detection circuit is determined by chip designer based on vulnerability of the path, desired HT resistance, and limitations on parameter overhead. For example, the security-sensitive portion of circuit (e.g., memory) is required to be covered by more detection circuits to achieve more accurate HT detection. Memory circuit is security-sensitive, because the key data stored in memory could be a target for attackers. While security-robust portion of circuit (e.g., critical path) can be covered by less (or even zero) detection circuits to reduce workload and circuit overhead. Critical path is security-robust, because any extra connection on critical path will slow chip operating frequency, that can be easily revealed in post-fab functional test.

3. Timing analysis-based HT detection

This section introduces the timing analysis-based HT detection algorithm, functional block diagram and a sub-circuit design. To simplify the introduction of detection algorithm, all cases in this section assume no manufacturing or environmental variations, and experimental results are based on schematic simulation with *tt* (typical-typical) corner. The effect of operating variations is considered in Section 4.

3.1. Timing analysis-based HT detection algorithm

In order to avoid detection, typically HTs are designed staying dormant until activation. The proposed detection technique algorithm and implementation are with premise that the HT remains dormant (sleeping mode) during detection process.

An HT circuit embedded in testing-path will add extra capacitance, resulting in more charging and discharging delays to the testing-path [23,24]. The delay time (time from applying an input pattern to signal arriving at output) will be increased for a HT-attacked CUT compared to HT-free CUT due to the additional delay caused by HT circuit. The