European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 4, 2020

LDPC BASED HARDWARE TROJAN DETECTION

Sathya Vignesh R*, Sivakumar A*, Shyam M*, Jagadeesh Babu S*, Yogapriya J**

** Assistant Professor, ECE, R.M.K. Engineering College,*

***Programmer Analyst, Cognizant, Chennai*

Abstract—Hardware Trojan (HT) can be introduced by an adversary at an untrusted design or fabrication house. Depending on the interests of the adversary the HT can cause change in functionality, denial-of-service, and information leakage or reliability reduction. In the existing system, a self-referencing based HT detection method using path delays which eliminates the requirement of golden ICs, is used. Further, we developed a procedure to select paths that minimizes the effect of both inter-die and intra-die PV. We have used topologically symmetric paths to mitigate inter-die variations and selected closer paths to exploit the spatial correlation to reduce the impact of intra-die variations. In the proposed system, Low density parity check with majority logic gate is used to predict the unknown post silicon errors occur in the integrated chips. Those small errors produce a large variation in the development of complex circuitry which utilizes maximum space of the FPGA. The proposed system uses Quartus II software and provides the simulation model showing the normal establishment of data transfer and Hardware Trojan affected system separately.

Keywords—Hardware Trojan, Activation time, Transition probability, Dummy flipflop, Low Density Parity Check

1. INTRODUCTION

Trusted microcircuit design may be a newly proposed topic thanks to the progress of globalization and therefore the fast-improving IC manufacturing technology. Because of global economic pressures, the event and fabrication of advanced ICs are migrating offshore so as to lower the value. As a result, the entire IC supply chain once located in one country are often spread globally now. To control these manufacturing facilities is nearly impossible while on the opposite hand, to compromise the IC supply chain for sensitive commercial and defense applications becomes easier. Also, under the pressure of market requirements, auto-placement and auto-routing tools are widely utilized in modern IC design to deal million-gate level circuits so as to scale back product developing cycle time. These tools, however, aren't optimal and leave many chip space unused. Based on the advanced IC manufacturing technology, it's much easier for attackers to embed some malicious circuits, so-called, Trojan circuits within the unused space, or other parameters without changing the area of the whole chip. Traditional function testing is a smaller amount effective in detecting Trojan circuit for the subsequent reasons, 1) the trigger condition of a Trojan rarely appears, 2) Trojan inputs might be any patterns within the gap between the vast amount of exhaustive input patterns and therefore the relatively bit of testing patterns actually used, 3) the harm of Trojan circuits may evolve after a long time after chips are implemented.

For example, the Trojan is often a series of XOR gates to match some inner signals with a preset value, a worth which will not appear under normal testing patterns. Only if the attacker loads a special test pattern could the Trojan be triggered to try to harm to the circuit. It is also very difficult to construct fault models as there are many types of Trojans and it is difficult and unnecessary to construct a faulty model for each type of Trojan. Without the fault model, it is not possible to develop Trojan detection methods systematically leveraging the powerful EDA tools. In our work, we develop models which may represent most of the Trojan circuits and help

us detect these Trojans and construct trusted ICs. Although the destructive reverse engineering to check the integrity and genuineness of manufactured chips is a useful method to deal with any types of Trojan circuits, it can't guarantee those untested to be Trojan free. Based on the explanations mentioned above, certain agencies have restricted circuit designs for military usage to the factories which have passed certain certifications. But not everyone can afford the high cost to put manufacturers under their control. Furthermore, because the trusted design idea emerges, vendors and consumers of economic grade cryptographic and security critical hardware have began to concentrate on this subject. For them, cost is that the most concerning aspect in order that they are going to be the most force to push for an inexpensive testing method in detecting Trojan circuits.

The manufacturing tests exist to detect defects as production of ICs is imperfect and subject to process variation. These detection methods can be useful to detect Trojans, but they are far from sufficient. In general, malicious Trojans attempt to bypass or disable the safety fence of a system. An adversary tries to cover the extra components; hence more advanced detection techniques are necessary. These techniques should be non-destructive and it should be possible to test large quantities of chips. A common Trojan is passive for the most time span an altered device is in Threat use, but the activation can cause a fatal damage. If a Trojan is activated the functionality are often changed, the device are often destroyed or disabled, it can leak tip or level the safety and safety. Trojans are stealthy; meaning the precondition for activation may be a very rare event. Traditional testing techniques are not sufficient. A manufacturing fault may happen at a random position while malicious changes are well placed to avoid detection. The threat can come from the foe that attacks the design of the genuine Integrated circuits. It is important to "know your enemies and know your-self", so the attacker role is as important. Because of globalization of the semiconductor design and fabrication process, ICs are becoming increasingly vulnerable to malicious activities and alterations. These vulnerabilities have raised serious concerns regarding possible threats to military systems, financial infrastructures, transportation security, and household appliances. The best way is to verify the trustworthiness of the manufactured chips upon return to the clients. This requires defining a post manufacturing step to validate the chip's conformance with the original functional and performance specifications. We call this new step silicon design authentication

2. BACKGROUND AND RELATED WORK

Trojan detection methodologies

Several Trojan detection methodologies are developed over the past few years. Without loss of generality, the methods employed are categorized as either side-channel analysis or Trojan activation, which are mainly chip-level solutions and architectural-level Trojan detection solutions. Trojan detection using side-channel signal analysis, Side-channel signals, including timing and power, are often used for Trojan detection. Trojans typically change a design's parametric characteristics for example, by degrading performance, changing power characteristics, or introducing reliability problems in the chip. This influences power and/or delay characteristics of wires and gates in the affected circuit. Power-based side-channel signals can provide visibility of the interior structure and activities within the IC, enabling detection of Trojans without fully activating them. Timing-based side channels can detect a Trojan's presence if the chip is tested using efficient delay tests that are sensitive to small changes in the circuit delay along the affected paths which can effectively differentiate Trojans from process variations.

Power-based analysis:

Agrawal et al. were the primary to use side-channel information to detect Trojan contributions to circuit power consumption. To obtain the facility signature of Trojan-free (i.e., genuine) ICs, random patterns are applied and power measurement is performed. The data belonging to each power measurement consists of

several elements, including power consumption of the circuit after applying inputs that are the same in all Trojan-free ICs; measurement noise, which may be removed by several measurements; process variations, which are random and can't be removed; and Trojan contributions to the measured power consumption. After patterns are applied, a limited number of ICs are reverse engineered to make sure they're Trojan free. Once the reference signature is obtained, the same random patterns are applied to the IC under authentication (IUA). If the IUA's power signature differs from the reference signature, the IUA is taken into account suspicious which it'd contain a Trojan. Trojans of various sizes under different process variations are detected by applying random patterns and observing the signatures. If the Trojan is comparable in size with the circuit, its impact on the circuit-transient current will be significant and could be measured easily. However, process variations will mask the impact of very small Trojans on circuit power consumption.

Timing-based analysis:

Li and Lach proposed a delay-based physical unclonable function (PUF) for hardware Trojan detection. This method uses a sweeping-clock-delay measurement technique to live selected register-to-register path delays. Trojans can be detected when one or a group of path delays are extended beyond the threshold determined by the process variations level. The following figure shows the path delay measurement architecture. The main circuit is the register-to-register combinational path that is to be characterized, and the registers on this path are triggered by the main system clock (CLK1). The components outside the box are part of the testing circuitry. The shadow register takes the same input as the destination register in the main circuit but is triggered by the shadow clock (CLK2), which runs at the same frequency as CLK1 but at a controlled phase offset. The results latched by the destination register and therefore the shadow register are compared during every clock period. If the comparison result is unequal, the path delay is characterized with a precision of the skew step size. This method employs an on-die temperature monitor to overcome the problem of temperature affecting path delay. This monitor uses a ring oscillator as the clock input of a counter to measure operating temperature. Because the oscillator is embedded within the main circuitry and its switching frequency is temperature dependent, the authenticator can calculate the effective response from the reported temperature and delay signature. Although effective, this technique suffers from considerable area overhead when targeting today's large designs with millions of paths. Jin and Makris proposed a new finger print generating method using path delay information of the entire chip. A chip has many delay paths, each representing one a part of the characteristic of the whole chip.

The timing features can generate a series of path delay fingerprints. Regardless of how small the Trojan is compared to the entire chip size, it can be significant in the path view and could be detected. The entire testing procedure includes three steps:

1. Path delay gathering of nominal chips.
Many chips are selected from a fabricated design High-coverage input patterns are run on the sample chips, and high-dimension path delay information is collected. Then, the sample chips are checked via reverse engineering to make sure they're genuine circuits.

2. Fingerprint generation. According to the trail delays, a series of delay fingerprints are generated and mapped to a lower-dimension space.

3. Trojan detection. All other chips are checked under the same test patterns. Their delay information is reduced to a low dimension and compared to the delay fingerprints. This method uses statistical analysis to

affect process variations. Because today's circuits can include millions of paths, measuring all paths especially the short ones is not practical.

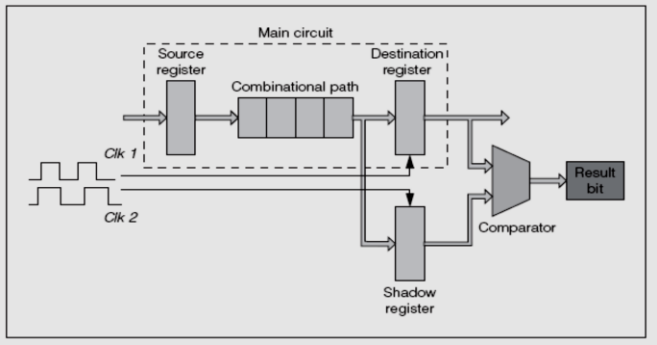

Fig. 1

DETECTION METHODOLOGY

In this system, Low density parity check with majority logic gate is used to predict the unknown post silicon errors occur in the integrated chips. Those small errors produce a large variation in the development of complex circuitry which utilizes maximum space of the FPGA. The proposed system used Quartus II software and provides the simulation model showing the normal establishment of data transfer and Hardware Trojan affected system separately.

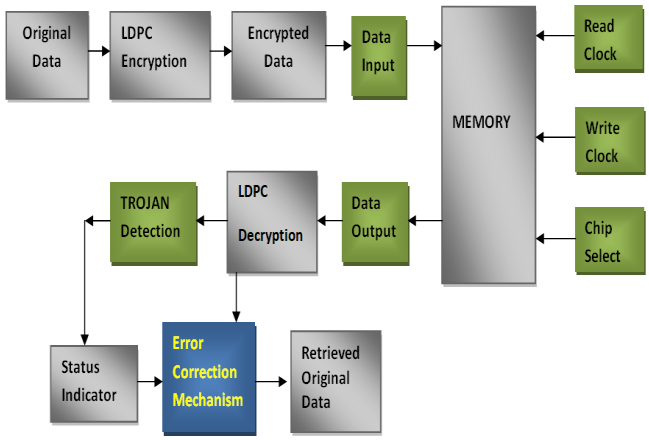

Fig. 2

3. RESULT

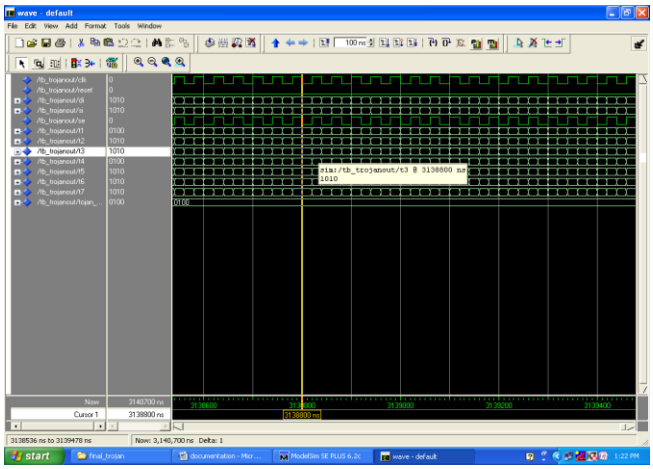

Fig. 3

4. CONCLUSIONS

In this paper, we demonstrate that the topology of a circuit and therefore the number of primary inputs and flip-flops determine switching activity of the circuit. Within the following, transitions are modeled using GD and therefore the number of clock cycles taking to get a transition is estimated on the average. Furthermore, it's shown that inserting dummy scan flip-flop can reduce transition generating time. This realization results in develop a dummy flip-flop insertion procedure aiming at augmenting transition probabilities of nets during a design, and increasing activity of hardware Trojans in Integrated Circuits. The simulation results for s38417 benchmark demonstrate that it's possible to significantly increase switching activity in Trojan circuits. Smaller Trojans could also be fully activated and cause functional failures. Larger Trojans might contribute more into side-channel signals and are detected as abnormality.

REFERENCES

1. U.S.D. Of Defense, “Defense science board task force on highperformance microchip supply,” Washington, D.C., 2005 [Online]. Available: http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf
2. S. Adee, “The hunt for the kill switch,” IEEE Spectrum, 2008 [Online]. Available: http://www.spectrum.ieee.org/print/6171
3. X.Wang, M. Tehranipoor, and J. Plusquellic, “Detecting malicious inclusions in secure hardware: Challenges and solutions,” in Proc. IEEEInt. Workshop Hardware-Oriented Security Trust (HOST), 2008, pp.15–19.
4. M. Banga and M. S. Hsiao, “A novel sustained vector technique for the detection of hardware Trojans,” in Proc. Int. Conf. VLSI Des., 2009, pp. 327–332.
5. R. S. Chakraborty and S. Bhunia, “Security against hardware Trojan through a novel application of design obfuscation,” in Proc. Int. Conf. Comput. -Aided Des. (ICCAD), 2009, pp. 113–116.
6. M. Banga and M. S. Hsiao, “A region-based approach for the identification of hardware Trojans,” in Proc. IEEE Int. Workshop Hardware-Oriented Security Trust (HOST), Jun. 2008, pp. 40–47.

7. M. Banga, M. Chandrasekar, L. Fang, and M. S. Hsiao, “Guided Test generation for isolation and detection of embedded Trojans in ICs,” inProc. IEEE/ACM Great Lakes Symp. VLSI, Apr. 2008, pp. 363–366.
8. D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, “Trojan detection using IC fingerprinting,” in Proc. Symp. Security Privacy, 2007, pp. 296–310.
9. R. Rad, X. Wang, J. Plusquellic, and M. Tehranipoor, “Power Supplysignal calibration techniques for improving detection resolution to hardware Trojans,” in Proc. Int. Conf. Comput.-Aided Des. (ICCAD),2008, pp. 632–639.
10. M. Tehranipoor and F. Koushanfar, “A survey of hardware Trojan taxonomy and detection,” IEEE Des. Test Comput., pp. 10–25, 2010.
11. J. Li and J. Lach, “At-speed delay characterization for IC authentication and Trojan horse detection,” in Proc. IEEE Int. Workshop Hardware-Oriented Security Trust (HOST), 2008, pp. 8–14.
12. Y. Jin and Y. Makris, “Hardware Trojan detection using path delay fingerprint,” in Proc. IEEE Int. Workshop Hardware-Oriented SecurityTrust (HOST), 2008, pp. 51–57.
13. D. D.Wackerly,W. Mendenhall, III, and R. L. Scheaffer Mathematical Statistics With Application, 7th ed. Belmont, CA:Thomson LearningInc, 2008.
14. X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, “HardwareTrojan detection and isolation using current integration and localizedcurrent analysis,” in Proc. Int. Symp. Fault Defect Tolerance VLSI Syst. (DFT), 2008, pp. 87–95.