International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 2, Issue 9, September 2015

Hardware Trojans, A State Of The Art

[1] Sudeendra kumar K, [2] K.K. Mahapatra
[1][2]Department of Electrical and Electronics Communication Engineering
National Institute of Technology, Rourkela

***Abstract:*— Time to market demand has forced integrated circuit design, manufacturing and testing to be done at different places across globe. This approach has led to numerous security concerns like overbuilding of chips from foundries, IP protection, counterfeiting and hardware Trojans. In this work, we focus on hardware Trojans in chips. In the process of finding the answer to above mentioned security issues, we present literature survey, interim results and a holistic view on possible future work. We also present the case study of hardware Trojans.**

I. INTRODUCTION

Currently electronics is used in every span of life from entertainment to military applications. We have entered an era where most systems are built through integrated circuits in order to reduce size of the system. The safe and effective operations from bank transactions to space missions will depend on security and reliability of electronic chips used in those systems. The globalization of electronic chip industry has led to the sourcing of components from untrusted sources that poses a security threat to the systems where cryptographic circuits are used and also in defense electronic systems. To mitigate this problem, exhaustive research in hardware security is conducted in recently. The well-known threats can be categorized as follows:

1. Counterfeit electronic components: The major sources of counterfeit parts are: -Extraction of electronic parts from obsolete PCB's and selling recycled parts as new components, unauthorized production of chips from foundries without the permission of IP owner or design house and failed parts or out of spec components coming out from the test centers into open market [1].
2. Hardware Trojans (HT): A malicious circuit inclusions into the design from an adversary with an intention to damage the functionality of the chip at a much later date or leaking confidential information like keys used in cryptography. The hardware Trojans are designed in such a way that they are triggered only after the occurrence of rare event in the design or by a very rare inputs. So it is challenge to find hardware Trojans either in pre-silicon or post silicon design verification and testing. [1][2] [6].
3. Side Channel Attacks (SCA): SCA is a well-known attack on cryptographic circuits to leak the key used in encryption of the secret data. The adversary can use power side channel, timing side channel to get the key. The recent literature reports attacks based on EM waves and LASERs. Another well-known SCA is based on test structures (Design for Testability circuits) inside the chip [4] [5].
4. Intellectual Property (IP) Protection: The original equipment manufacturers (OEM) will get support from both hardware and software vendors. The IP used in products and solutions from these vendors should be protected. The suitable measures along the supply chain to protect IP of different vendors, OEMs and individuals are necessary [1] [3].

II. MOTIVATION

From Nov-2007 through May 2010, U.S.Customs officials said they seized 5.6 million counterfeit chips. Two men indicted in Oct-2010 admitted importing 13,000 fake chips altered to resemble those from legitimate companies, including Intel, Atmel, Altera and National semiconductor, intended to be supplied to Department of Defence [2].

The above mentioned media reports confirms the serious threats in the field of hardware security. The defence sector is really paranoid about counterfeit parts and hardware Trojans. The electronic gadgets used in high value businesses, critical care medical equipment like pacemaker are vulnerable to SCA and HT [6]. There is urgent need to study, understand and take necessary steps to find the solutions to the hardware security problems. We have chosen the problem hardware trojans in this investigation.

III. HARDWARE TROJANS

We have developed a novel methodology within ASIC design flow for Trojan detection using standard tools within the framework. The proposed methodology is shown in fig.1 and fig.2.

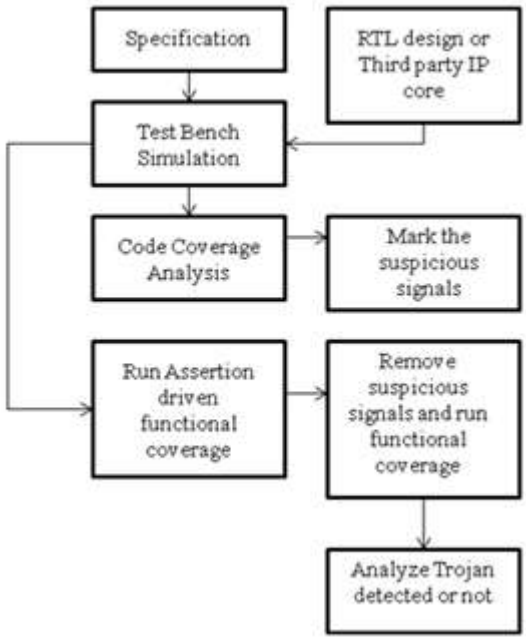

Fig.1 Verification flow at RTL lev

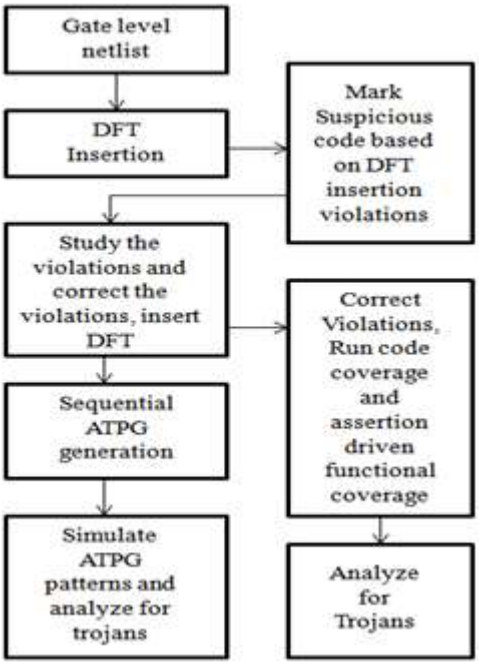

Fig. 2 DFT Insertion and ATPG simulation

The fig.1 shows the flowchart to detect the Trojans at RTL level. The standard verification procedures like code coverage, assertions and functional coverage can be used to recognize the suspicious signals inside the design. After removing the suspicious signals and circuits, if the design is completely functional, then we may conclude the removed redundant circuit as HT [6] [7].

The fig.2 shows the flowchart to detect the Trojans during Design for Testability (DFT) and Automatic Test Pattern Generation (ATPG). In few cases, adversary designs HT as asynchronously to hide the HT's from verification procedures which clock driven. DFT insertion tools will raise violations for asynchronous blocks, which makes them suspicious. The stuck at fault (SAF) and path delay fault (PDF) patterns can trigger hardware Trojans and can be observed during ATPG simulations [7] [10].

AES Case Study: Hardware Trojan detection techniques are generally validated against standard benchmark circuits. Trust-Hub provides benchmark circuits for variety of applications ranging from cryptographic circuits like AES, RSA and processors. The highly vulnerable designs for HTs are cryptographic cores and processors. In cryptographic cores, AES is most vulnerable and Trust-Hub provides 21 AES benchmarks. The proposed verification scheme and DFT insertion is verified on 21 AES benchmarks. Out of 21 benchmarks, 19 benchmarks will get detected in the proposed methodology. AES benchmarks and their weakness of detected. benchmarks are presented in Table 1. Except AES-T100 and AES-T200, other benchmarks are weak and Trojans are detected in straight forward verification techniques and DFT insertion procedures [8][9][10].

Based on the experience and weakness we have designed a novel HT benchmark is also proposed. The fig.3 shows weakness of existing HT benchmark. The HT block does not have output port, which is major weakness. In a modified novel HT benchmark is shown in fig.4 which overcomes the earlier weakness. In a novel HT benchmark, the shift register intermediate signals are taken out as 128-bit signal, fed into multiplexer input and select line of mux is also 128 bit width.

In the select line of multiplexer, all 128 bits should become zero to push the output of shift register as encrypted output. By the AES structure and operation, the probability of 128-bits getting zero value is very less in the shift register. So the result of AES block will get connected to output.

AES Benchmark (from Trust-Hub)	Type	Weakness
AES-T500, AES-T1800 and AES-T1900	Denial of Service (DoS)	Module without a output
AES-T600, AES-T2000 and AES-T2100	Leakage current based Trojans	Module without a output
AES-T400, AES-T1600 and AES-T1700	RF Signal based Trojans	Extra unused pin
AES-T700, AES-T800, AES-T900, AES-T1000, and AES-T1200	CDMA based power side-channel based Trojans	Asynchronous block (causes DFT insertion violations)
AES-T1300, AES-T1400 AEST1500	Dynamic power side-channel Trojans	Module without a output
AES-T100, AES-T200 and AES-T300	Always on Trojans	AES-T300 will get detected and others will go undetected

Table 1: AES Benchmarks and their weaknesses

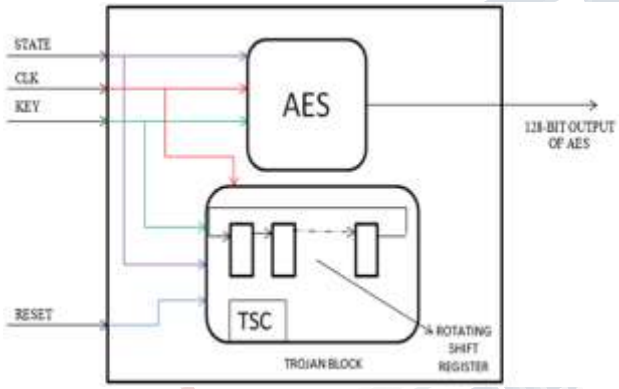

Fig.3: Block diagram showing Weakness of Trojan Benchmark

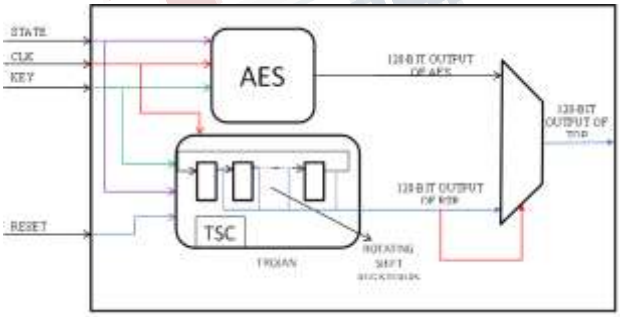

Fig 4:Novel AES Benchmark to overcome the weakess of existing Benchmarks

Processor Case Study: Trust-Hub also provides HT benchmark circuits for processors. Few Processor HT benchmarks will get detected in verification and DFT methodologies (fig.1 and fig.2) and few will escape. It is evident from literature survey and also from our interim results that, SCA based HT detection is not much useful in detecting Trojans, because rarely we find data leakage Trojans in processors. Pre-silicon verification techniques are basically intended to check for functionality and it is new for verification teams to check for unintended or malicious behavior. Table.2 shows the interim results of this case study [8] [9][12].

Based on the experiences of Trojan behavior and weakness of processors, secure properties, assertions can be developed to increase security assurance levels.

Benchmark	Malicious activity	Detection under proposed scheme	Model checking
MC8051-T200	The Trojan activates the internal timers of 8051 in the idle mode.	Detected (functional coverage)	Under progress
MC8051-T400	The Trojan is triggered when a specific sequence of commands is executed. The Trojan disables handling interrupt after activation.	Detected	Under progress
MC8051-T500	The Trojan replaces some data such that only an attacker can analyse the output. The Trojan trigger detects a specific command, and the Trojan payload replaces specific data after Trojan activation.	Undetected (both in functional and code coverage)	Under progress
MC8051-T600	The Trojan disables any jump in algorithms running by the micro-controller. The Trojan gets activated when an interrupt is detected on the pin INT0. The Trojan payload modifies the program counter to disable jumps.	Detected (functional coverage)	Under progress

Table 2: Processor Trojan Benchmarks and their detection under our framework

IV. CONCLUSIONS

A novel verification framework to suspect Hardware Trojans in IP cores, mainly in processors and cryptographic circuits.

A Novel HT Benchmark for validation of Trojan detection techniques.

REFERENCES

[1]. Rostami M, Koushanfar. F, Karri. R, "A Primer on Hardware Security: Models, Methods, and Metrics", *Proceedings of IEEE*, Vol. 102, Issue – 8, pp. 1283-1295, Aug 2014.

[2] "Defense Science Board (DSB) study on High Performance Microchip Supply," www.acq.osd.mil/dsb/reports/ADA435563.pdf, 2005.

[3] SEMI, "Innovation is at risk as semiconductor equipment and materials industry loses up to $4 billion annually due to IP infringement." www.semi.org/en/Press/P043775, 2008.

[4] Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Flottes, Rouzeyre and Verbauwhede, "Test versus Security: Past and Present", IEEE transactions on emerging computing-2013.

[5] Stephan Mangard et.al.,"Power Analysis Attacks:Revealing the secrets of smart cards" Springer Science-2007.

[6] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," IEEE Design & Test of Computers, vol. 27, no. 1, pp. 10–25, 2010.

[7]. DARPA, "Integrity and Reliability of Integrated Circuits (IRIS)," http://www.darpa.mil/Our_Work/MTO/Programs/Integrity_and_ReliabilityofIntegratedCircuits, 2012.

[8] https://www.trust-hub.org/resources

[9]. Xuehui Zhang and Mohammad Tehranipoor, Case Study: Detecting Hardware Trojans in Third-Party Digital IP Cores, IEEE International Symposium on HOST-2011.

[10]. Trey Reece, William H Robinson, "Analysis of data-leak hardware Trojans in AES cryptographic circuits" Technologies for Homeland Security (HST), 2013 IEEE International Conference on pp. 467-472

[11]. L. Lin, M. Kasper, T. Güneysu, C. Paar and W. Burleson, "Trojan Side-Channels: Lightweight Hardware Trojans through Side- Channel Engineering," 11th International Workshop Cryptographic Hardware and Embedded Systems (CHES), pp. 382-395, 2009.

[12]. Seetharaman Narasimahan, *et.al*, Hardware Trojan Detection by Multiple Parameter Side-Channel Analysis, IEEE Transactions on computers, vol.62, No.11, November-2013.

