A SOC BUS ARCHITECTURE FOR DETECTING AND THWARTING IC FUNCTIONAL VIRUSES WITH REDUCED ACTIVATION TIME

D.Gowri, A.Mohamed Abbas

ABSTRACT: While the issue of Trojan ICs has been receiving increasing amounts of attention, the overwhelming majority of anti-Trojan measures aim to address the problem during verification. While such methods are an important part of an overall anti-Trojan strategy, it is statistically inevitable that some Trojans will escape verification-stage detection, in particular in light of the increasing size and complexity of system-on-chip (SOC) solutions and the increasing use of third-party designs. In contrast with much of the previous work in this area, we specifically focus on run-time methods to identify the attacks of a Trojan and to adapt the system and respond accordingly. We describe a solution including a bus architecture in which the arbitration, address decoding, multiplexing, wrapping, and other components protect against malicious use of the bus.

***Index Terms*— Bus MUX, DSFF, Golden memory, Hardware Trojan, RSA Cryptography, Trojan activation time, Threshold, Wrapper.**

1. INTRODUCTION

Chip design and fabrication process has become a trend in integrated circuit (IC) market due to economical profit, with limiting the control of customer over IC supply chain. Motivated adversary takes advantage of such restriction to tamper IC supply chain by maliciously implanting extra logic as hardware Trojan circuitry into an IC . Consequently serious concerns rise about security and trustworthiness of electronic systems. An attacker can change a design net list or subvert the fabrication process by manipulating design mask, without affecting the main functionality of the design.

Hardware Trojan detection is an extremely challenging problem and traditional structural and functional tests cannot effectively address it. Trojan circuits have stealthy nature and are triggered in rare conditions. Trojans are designed such that they are silent most of their life time and may have very small size relative to their host design, with featuring limited contribution into design characteristics. These suggest that they most likely connect to nets with low controllability and/or observability. It is expected that Trojan inputs are supplied by nets with low transition probabilities to lessen its impact on circuit side-channel signals such as power and delay. Automatic test pattern generation (ATPG) methods used in manufacturing test for detecting defects do so by Operating on the net list of the Trojan-free circuit. Therefore, existing ATPG algorithms cannot target Trojans directly. Trojan detection makes efficient pattern generation necessary to disclose Trojan impact on design characteristics beyond process and environmental variations. Trojan detection methods using transient power analysis require patterns that increase Trojan activity whereas keep circuit activity low to magnify, Trojan contribution into the circuit power consumption. Methods that are based on delay analysis and require that generate transition on nets that supply Trojan inputs to reveal wiring and input gate resistance and capacitance impact of Trojan on the circuit delay characteristic. From authentication standpoint, it is critical to:

1) Analyze time to generate transition at Trojan input and in Trojan circuit

2) Reduce authentication time.

In this project, a methodology is developed to increase the probability of generating a transition in functional Trojan circuits and to analyze the transition generation time. Transition probability is modeled using geometric distribution (GD) [13] and issued to estimate number of clock cycles required to generate a transition on a net. An efficient dummy flip-flop insertion procedure is proposed to remove rare triggering condition of Trojans.

The procedure identifies nets with transition probability less than a specific transition probability and inserts dummy flip-flops such that the transition probabilities of all nets in the design are greater than a specific transition probability. It should note that dummy flip-flops are inserted in a way that will not change the functionality and timing of design.

The effectiveness of dummy flip-flop insertion is examined by evaluating different transition probability thresholds for various Trojan circuits. The relation between authentication time, the number of required transitions in Trojan circuit, and tester clock is studied. These parameters would help determine the transition probability threshold of a design.

The transition probability threshold, in turn, provides an estimation of area overhead induced by inserted dummy flip-flops. Our simulation results show

significant improvement in Trojan detection and reduction in Trojan activation time.

1.1 EXISTING SYSTEM:

Previous Work only focuses on handling and thwarting Trojan viruses with extensive algorithm and detection circuits.

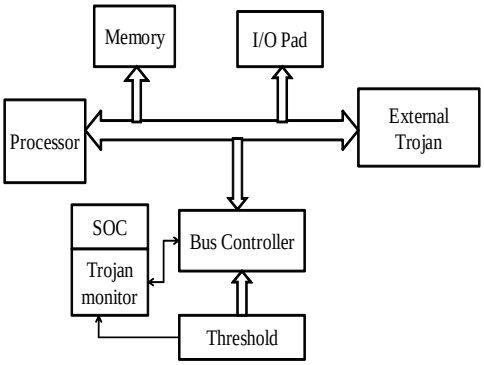

Fig 1.1 Existing System

A method of Dummy flip flop design is introduced to reduce the activation time of Trojan effectively.Transition is modeled by geometric distribution and the number of clock cycles required to generate a transition is estimated. Furthermore, a dummy scan flip-flop insertion procedure is proposed aiming at decreasing transition generation time. The procedure increases transition probabilities of nets beyond a specific threshold. The relation between circuit topology, authentication time, and the threshold is carefully studied.

Limitation:

- The detection techniques only applicable for Trojan viruses.
- Area overhead due to insertion Dummy Scan flip-flops.
- Non fixed net list.

1.2 PROPOSED SYSTEM:

Pipelining Techniques can be used to enhance the flow of detection and execution of Trojan. This paper can be extended to detect multiple types of Hardware viruses like Win. Salient, worm32 etc…

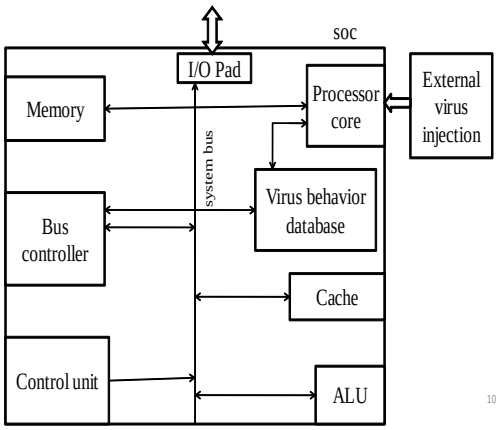

Fig 1.2 (a) Proposed Systems using SOC

To verify the functionality of Trojan activating mechanisms in much more complex circuit a novel Cryptographic architecture will be tested for various virus pattern presences including Trojan. A test vector based Trojan activating pattern will be tested in cryptographic structure for measuring its activating and deactivating time.

An Trojan injected RSA cryptography circuit will be used as test chip circuit.

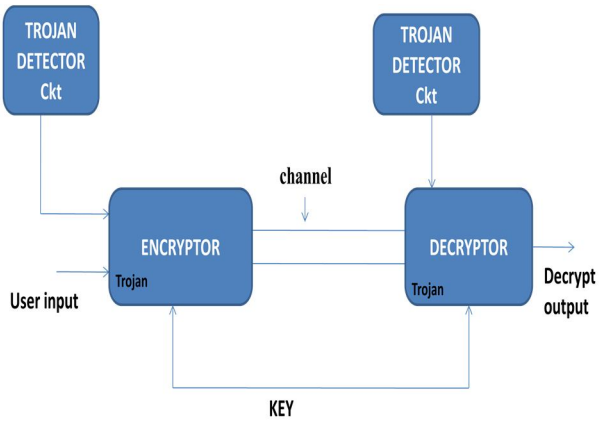

Fig 1.3 (b) Proposed System Using RSA Cryptography

2. DESIGN FLOW for SOC

Design flow is divided by the Structural RTL level into:

Front End: specify, explore, design, capture, synthesis - Structural RTL.

Back End: Structural RTL - place, route, mask making, fabrication.

3. MODIFIED BUS ARCHITECTURE

This section presents a description of a set of key designs that can be utilized to thwart virus attacks. These designs use an AMBA-based SOC.
This modified bus architecture includes.

- Secure address decoder
- Secure arbiter
- Secure bus multiplexer
- Wrappers for masters and slaves
- Bus Transactions data and functional block integrity checking

3.1 Secure address decoder

This contains conventional address decoder as well as additional designs to Detect an attempt by a malicious bus master to access a restricted address. Block normal bus masters from accessing malicious slaves.

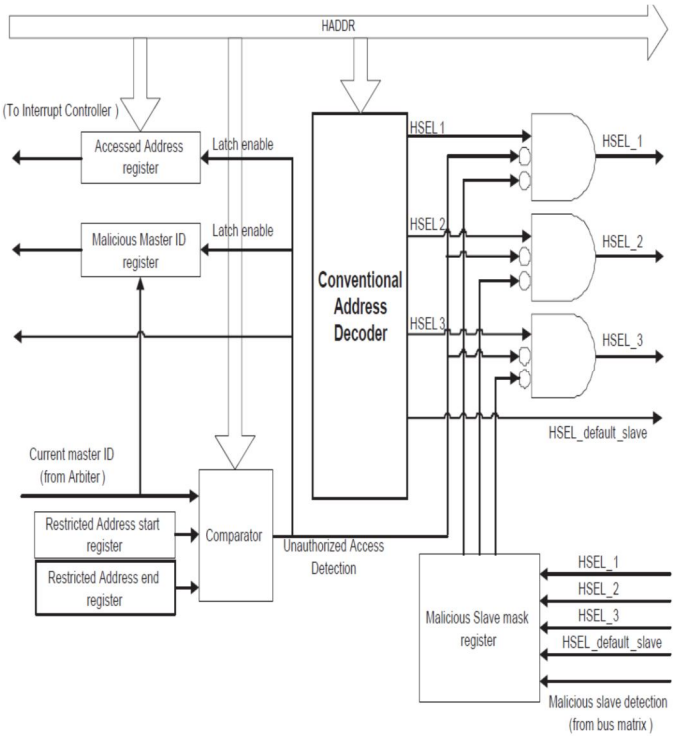

Fig. 3.1 Secure address decoder

3.2 Arbiter and multiplexer

This detects and nullifies malicious bus lock by intruders and avoids grants of bus master chip to unauthorized access.

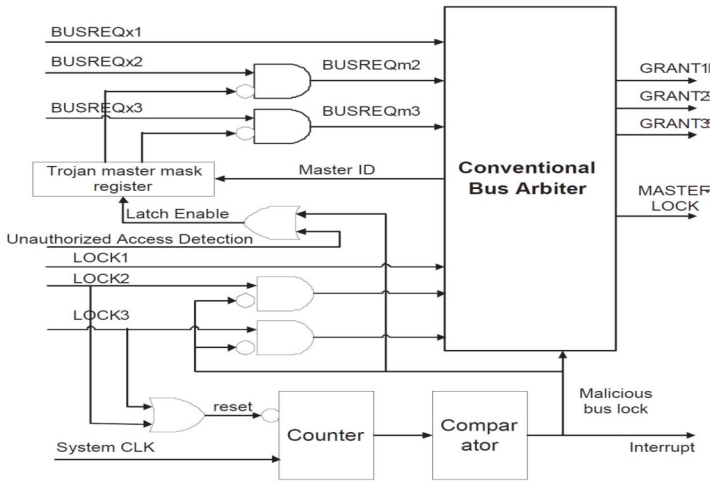

Fig 3.2 Arbiter.

3.3 Wrapper for Masters and slaves

Data transactions and bus control signals to, from on master is visible to other masters and slaves on the system. Malicious masters and slaves could hack this data and leak them to off chip destination. This wrapper especially prevents hacking.

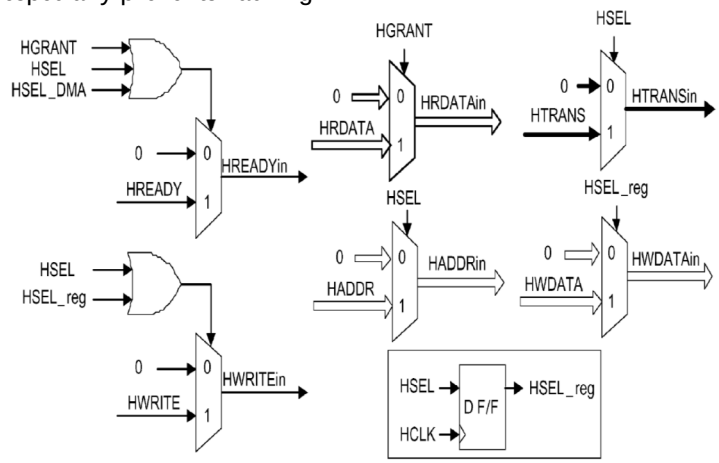

Fig 3.3 Wrapper for blocking and passing bus signals.

3.4 Bus transaction data and functional block integrity checking

This prevents the internal logic blocks from being corrupted by virus, for this built in self test (BIST) is utilized to assist the operation.

4. TROJAN DETECTION

4.1 System Using SOC techniques:

- Golden memory
- Wrapper
- MUX
- Dummy scan flip flop counter
- Specific threshold

4.2 System using RSA CRYPTOGRAPHY:

This Techniques used to identify the Trojan in complex circuit.

- Inserting Trojan with cryptography circuit.
- Detecting the virus in both encrypt circuit and decrypt circuit.
- Decrypted output is show in FPGA Kit.

4.2.1 RSA ASYMMENTRIC CRYPTOGRAPY:

Using this formula to identify the public and private key. Using this key to detect the viruses in complex circuit.

1)Prime key:

$$N = p * q$$

2) Public key:

Z / public key # 0

Here,

$$Z=(p-1)*(q-1)$$

3) Private key:

(private key*public key) – 1

divided by Z = 0

4.3 HARDWARE AND SOFTWARE SPECIFICATION

Tools Used:

- MODELSIM
- QUARTUS II

4.3.1 MODELSIM

ModelSim is a verification and simulation tool for VHDL, Verilog, SystemVerilog, and mixed language designs. the ModelSim simulation environment. It is divided into four topics, which you will learn more about in subsequent lessons.

- Basic simulation flow
- Project flow
- Multiple library flow
- Debugging tools

4.3.2 Quartus II

Quartus II software delivers superior synthesis and placement and routing, resulting in compilation time advantages. Compilation time reduction features include:

- Multiprocessor support
- Rapid Recompile
- Incremental compilation

4.4 SECURE ADDRESS DECODER

A secure memory can be named as golden memory in which our Trojan detection program will be stored and it cannot be reedited. With reference to the start and end register the golden memory address location can be reconfigured. A conventional address decoder will be modified as secure address decoder through which the gold memory location can be completely hidden.

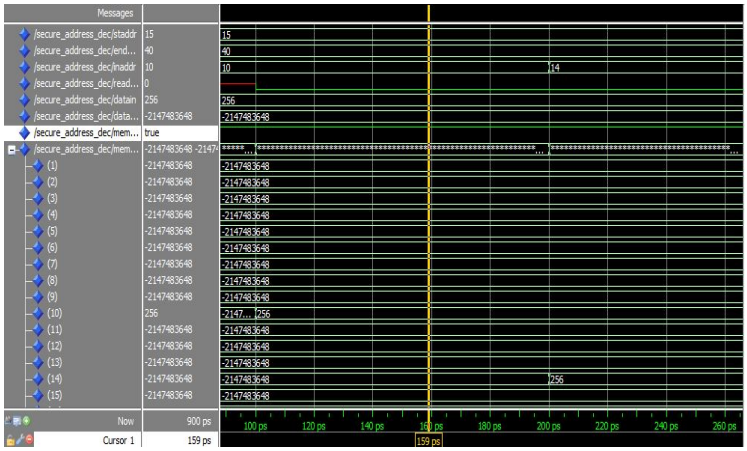

Fig 4.4 a) Golden memory true output

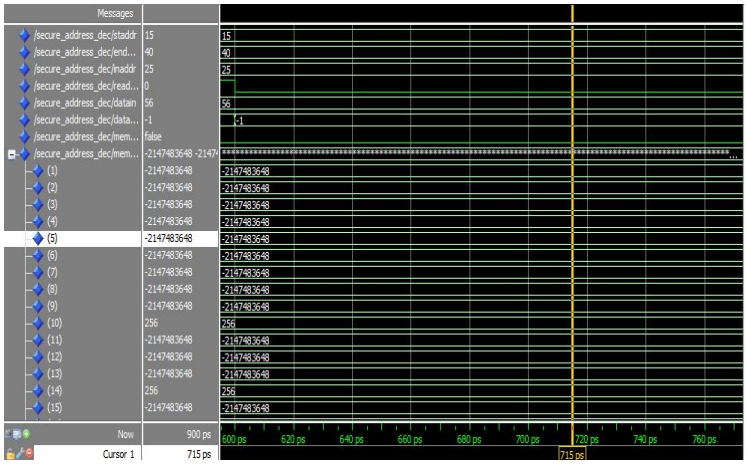

Fig 4.4 b) Golden memory false output

4.5 BUS MULTIPLEXER

Bus multiplexer consists of a Bus monitor with Threshold input.The Bus monitor continuously scan the Bus signal and compare it with the threshold count.If the Bus utilization(tclk) is activated more than the threshold time, then it is identified as a suspicious signal and immediately the granted permission will be revoked and Bus signal will be deactivated.

ALGORITHM

If (trojan count>threshold) then

trojan count:=0;

```
trojan clk<='deactivate';
elsif (clk count mod 10 =0) then
trojan clk<='activate';
```

Bus Output:

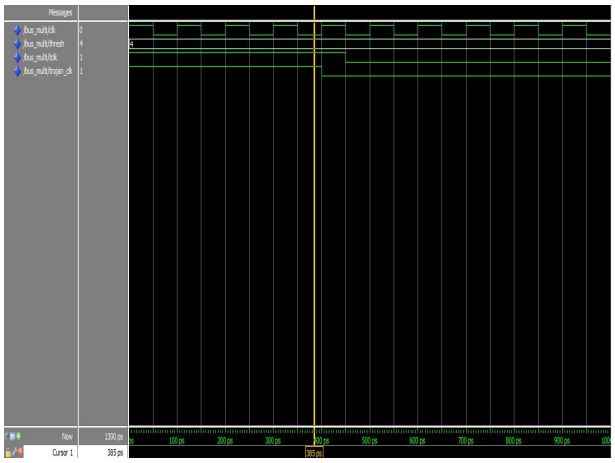

Fig 4.5 Bus multiplexer

4.6 WRAPPER:

Data transactions and bus control signals to, from on master is visible to other masters and slaves on the system. Malicious masters and slaves could hack this data and leak them to off chip destination. This wrapper especially prevents hacking.

Bus transaction data and functional block integrity checking:

1) loss of data integrity, either by direct manipulation of bus transaction data via the bus interface logic or through corruption of the internal operations of a functional block.

2) In a secure IC, built-in self test (BIST) can be utilized to assist detection of this form of Trojan.

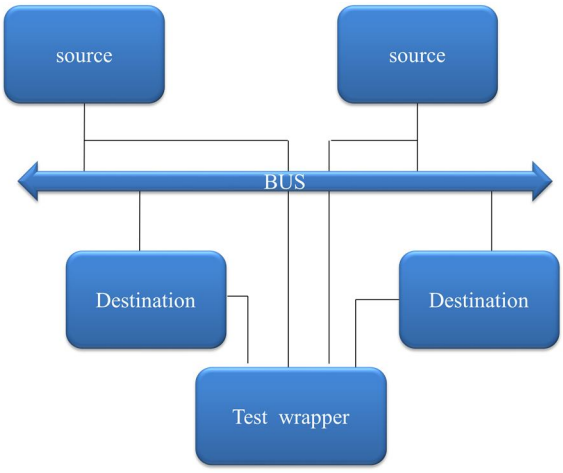

Fig 4.6 wrappers block diagram

Grants permission to the corresponding sources and destination continuously monitor the flow of BUS signals. When a pair of source and destination need to communicate over bus channel. Control over the selection of path capability to block the flow of clock to sub unit Wrapper ensures the protection of system from spying.

4.7 SPECIFIC THRESHOLD:

Increases transition probabilities of nets beyond a specific threshold. Threshold is a Limitation criterion to differentiate the bus signal as a secure or Trojan data. Threshold can be specifically assigned to circuit parameters for reducing activation time.

VIRUSES DETECTION OUTPUT

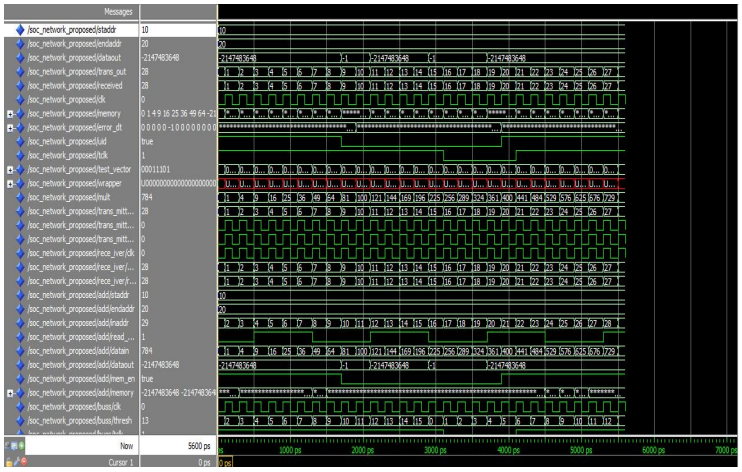

Fig 4.7 Viruses detection

4.8 DUMMY SCAN FLIP FLOP:

DSFF aim is decreasing the transition generation time. DSFF doesn't impact any changes in the operation but the flow. It will act as an scanning medium of pass through signals which helps for Trojan Activation.

4.9 RSA ASYMMETRIC CRYPTOGRAPHY OUTPUT:

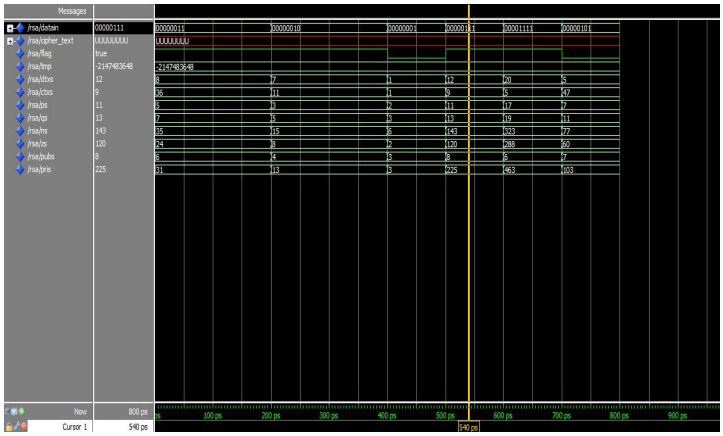

Fig 4.9 Cryptography output

6. FUTURE WORK:

A design methodology of inserting dummy scan flip flops for reducing the Trojan activation time in a VLSI hardware chip has been discussed. The detection of Trojan circuit becomes complex due to the nature of circuit under the test complexity. To evaluate the accuracy and speed of Trojan detection mechanism in complex VLSI circuitry, a cryptographic chip can be used as test chip and the Trojan activation time delay and power consumption can be measured and tabulated.

REFERENCE

[1] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar,"Trojan detection using IC fingerprinting," in *Proc. Symp. SecurityPrivacy*, 2007, pp. 296–310.

[2] H. Salmani, M. Tehranipoor, and J. Plusquellic, "New design strategyfor improving hardware Trojan detection and reducing Trojan activationtime," in *Proc. IEEE Symp. Hardware-Oriented Security Trust(HOST)*, 2009, pp. 66–73.

[3] Lok-Won Kim and John D. Villasenor,"A System-On-Chip Bus Architecture for Thwarting Integrated Circuit Trojan Horses".

[4] Mohammad Tehranipoor, Hassan Salmani, Xuehui Zhang, and Xiaoxiao Wang,"Hardware: Trojan Detection and Design-for-Trust Challenges".

[5] 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.

[6] M. Banga and M. S. Hsiao, "A region based approach for the identificationof hardware Trojans," in *Proc. IEEE Int.Workshop Hardware OrientedSecurity Trust (HOST)*, Jun. 2008, pp. 40–47.

[7] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomyand detection," *IEEE Des. Test Comput.*, pp. 10–25, 2010.

[8] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "HardwareTrojan horse detection using gate-level characterization," in *Proc. IEEEInt. Des. Autom. Conf. (DAC)*, 2009, pp. 688–693.

[9] MilicaMitic and Mile Stojcev,"An Overview of On-Chip Buses".

[10]Rajat Subhra Chakraborty, Seetharam Narasimhan and Swarup Bhunia, "Hardware Trojan: Threats and Emerging Solutions".

[11] S. Adee, "The hunt for the kill switch," *IEEE Spectrum*, 2008 [Online].
Available:http://www.spectrum.ieee.org/print/6171.

[12] 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.

[13] 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.

[14] Y. Alkabani and F. Koushanfar, "Consistency-based characterization for IC Trojan detection," in *Proc. Int. Conf. Comput.-Aided Des.(ICCAD)*, 2009, pp. 123–127.

[15] A Trojan-resistant System-On-Chip Bus Architecture.