IIPS: Infrastructure IP for Secure SoC Design

Mushfiq Mahmud

Term Paper based on the study of the paper by Xinmu Wang et al.: IIPS: Infrastructure IP for Secure SoC Design
IEEE Transactions On Computers, pp. 2226-2238, August 2015

1. Abstract

Infrastructure Internet Protocol for Security (IIPS) is an onboard solution for System on Chip security. It is meant to provide security from the time of manufacturing chips that is shown to be better than Design-for-security (DfS) features since it doesn't require much power costs or affect performance. The paper provides examples and simulations that show how IIPS can protect against scan chain based attack through low-overhead authentication using VIm-Scan, counterfeiting attacks using a Physical Unclonable Function (PUF) and hardware Trojan attacks through a test infrastructure for trust validation. IEEE 1500 Standard for Embedded Core Test (SECT) also makes the IIPS plug and play functional.

2. Introduction

Modern SoC chip design relies on infrastructure IP. In addition to the hardware or software based attacks after a chip has been deployed from manufacturing, there are a bunch of threats that need to be accounted for that may occur while the chip is being manufactured.

These may include:

- Design modifications by hardware Trojan attacks
- Hardware intellectual property (IP) theft
- Actual attacks on cryptographic systems before being distributed, e.g. side-channel attack, fault-based attack, and scan-based attack.

Although solutions to some of these threats exist via Design for Security (DfS) methods, DfS imposes some problems for heterogeneous SoC designs. There might be conflicting design and test requirements from separate DfS solutions as well as the need to adjust IP for each methods. All of this results in a considerable increase in overall design time as well power expenditures. Moreover, multi-core SoCs which are common nowadays make it really difficult to implement DfS measures.

Therefore, in this paper an onboard IIPS was proposed to solve these problems at once. IIPS can communicate directly with the multiple cores of an SoC using the IEEE 1500 Standard embedded Core Test (SECT). This is an integrated module that acts as a plug-and-play reusable core. It has the ability to stop attacks or help with detecting attacks during manufacturing tests thereby protecting from varied attacks.

List of
(a) Figures: 1
(b) Tables: 1, 2

Explanation of new terms

IP: Intellectual Property

DfS: Design for Security

IIPS: Infrastructure IP for Security

PUF: Physical Unclonable Function

Scan Chain (SC) : A method to make testing SoCs easier by scanning the state of all Flip-Flops on an SoC.

SFF: Scan Flip-Flop

SECT: (IEEE 1500) Standard for Embedded Core Test

The IIPS is separate from the cores and is only used when testing is being carried out during manufacturing. This results in the IIPS having very low power costs as well as performance drops. It is a first of its kind onboard SoC hardware protection solution. It works by interfacing with the functional cores of the SoC through standard boundary scan architecture.

This paper will explore how the IIPS can protect against three models of threats which include the threats that are the most prevailing:

- Scan based attacks that can infiltrate the scan chain and leak valuable information
- A Physical Unclonable Function (PUF) is implemented for device authentication
- An infrastructure for trust validation is implemented for hardware Trojans.

All of the above have their own sections in which the technicalities will be discussed.

3. Working Process

According to the IEEE SECT, the SoC has two ways of accessing the internal cores: Wrapper Serial Ports (WSP) or Wrapper Parallel Ports (WPP). The IIPS uses the WSP. It has a test data IO port called WSI/WSO as well as a test clock (WRCK) and control signals (WSC). Figure 1 shows a simplified block diagram which shows how the IIPS interacts with the cores. The IIPS has these parts:

- Master Finite State Machine (M-FSM) that controls the working mode of IIPS
- Scan Chain Enabling FSM (SE-FSM) that offers control over enabling the scan chains
- Clock control module to generate necessary clock and control signals

After being enabled, The test inputs are taken from WSP. Each cores receive a scan chain enable signal (SC_EN) and the original clock to each core is replaced with an internally produced test clock that can support ScanPUF authentication and Trojan detection. The test control inputs are also replaced with the IIPS's own control signals that can help capture the test responses. The original test signals are automatically preserved by IIPS. The process is as follows:

- From Idle mode, Scan Chain Enable (SC_EN) can be started by a specific vector sequence applied at WSP.
- Two states, ScanPUF or TrojDet state, can be set to perform ScanPUF authentication or hardware Trojan detection, respectively.
- Since both ScanPUF and Trojan detection chains need to have at least one active scan chain, SC_EN state leads the ScanPUF and TrojDet states.
- This acts as a verification tool since specific sequences of vectors are required for M-FSM to switch across different security functions. This also helps prevent unintentional trigger of a function.

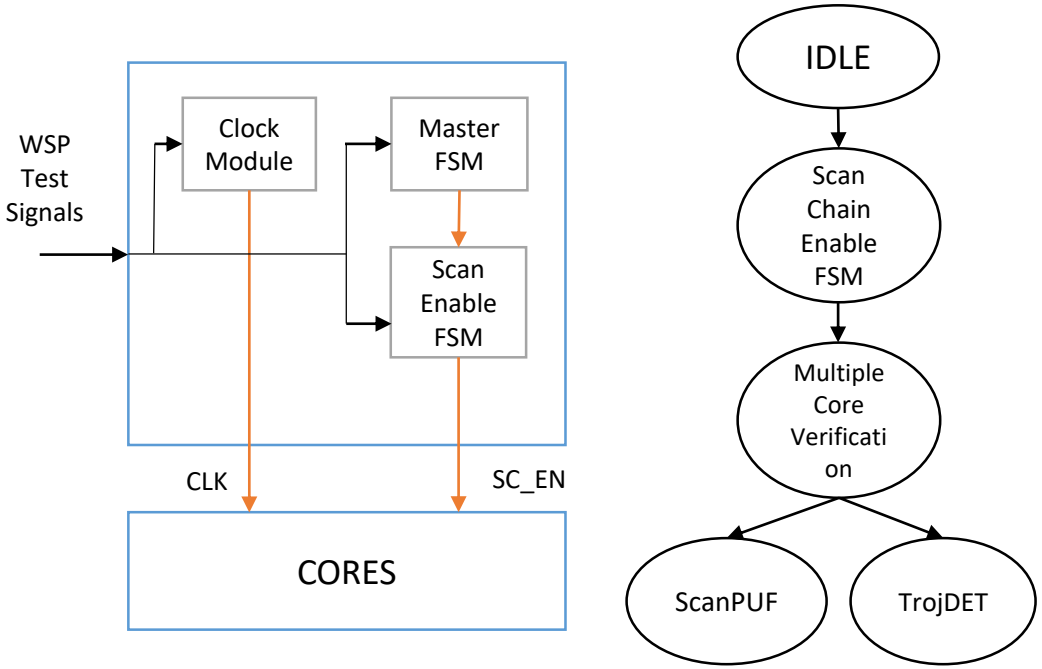

Figure 1: Simplified Block Diagram & State Diagram for the IIPS

4. Design, Security and Testing

The different design components and threat moderation strategies that are included in the IIPS are described in this section.

4.1. Scan Chain & VIm-Scan

Scan Chain is a method to make testing SoCs easier by scanning the state of all Flip-Flops. Although scan chain is very helpful in modern ICs, confidential data from the chip could be exposed. Some safe scan designs try to employ validation techniques to allow only safe scan accesses. One such technique is the Vim-Scan which has a low operating cost. It prevents the scanning of outputs until positive validation is made. This has been included in the IIPS since it allows to be setup with minimal changes in structure of the chip and therefore can be integrated into the SoC without an hassles in addition to having a low operation cost.

An external scan chain enable signal SC_EN for each of the functional cores is generated. When SC_EN is high, preventing both the scan input and output can lock the chain. Locking the external enable prevents interfering with the timing of the internal scan enable and SC_EN is defaulted to zero to disable all the scan chains when in non-testing mode. Furthermore, in order to start the two testing modes (ScanPUF and TrojDET), first all the cores have to be enabled using specific input vectors to each core.

4.2. Counterfeiting Attacks

In order to prevent counterfeiting or cloning of ICs, Physical Unclonable Functions (PUFs) can be employed to make unclonable IC fingerprints. PUF produces device signatures that are exclusive by taking advantage of path delay and other core procedures inside the circuit to ensure security. Therefore they can make very authentic ICs since they are supposed to be extremely detailed and sturdy. Therefore, the ScanPUF architecture has been integrated into the IIPS since they take up less space and don't mess up the SoC testing flow. Scan chain is used in the IP to fulfill ScanPUF. It also uses up low power and is very sustainable.

The delays that occur randomly in the scan paths are modelled and used as a signature that is unique. The scan chain is initialized in test mode and an array of ones and zeroes is generated and scanned. If old values are latched into the flip-flops still, that means that the signature was not generated.

Core designers can produce test sets for ScanPUF and Trojan detection at core level since they are core dependent. System incorporators can then make the test sets develop to SoC level. The core terminals have to be interpreted to the corresponding SoC pins, and also when the parallel test interface is being used, the paths between the Core Under Test (CUT) must be searched for test stimuli and response propagation. Both the ScanPUF and Trojan detection can use the same procedure for testing but care must be taken to terminate a test by leaving a gap via a clock cycle between tests.

4.3. Hardware Trojan Attack

To prevent hardware attacks such as malevolent alteration of the design, IIPS uses side-channel analysis based methods using a combinational path delay detection.

Similar to ScanPUF testing, the test sets have to produced by core designers and then later developed towards the SoC level for Trojans inside a core. Although, in order to tackle Trojans that affect communication between cores, the test sets should be produced at the SoC level.

Table 1: SoC configuration for Hardware Trojan Detection for trojans affecting inside and between cores. DMA is Direct Memory Access.

	Active	Bypass
Trojans inside Core	CPU	GPU, RAM, DMA
Trojans in system Bus (between cores)	CPU, RAM, GPU	DMA

5. Testing & Simulation Results

To illustrate how much silicon real estate was being used up, two example SoCs with full scan infrastructure were tested with different components. ‘Benchmark SoC 1’ had sequential circuits while ‘Benchmark SoC 2’ had a more realistic 32-bit processor. The results are shown in Table 1. We must note that the hardware overhead increases slowly with the number of scan chains (and therefore scan flip flops (SFFs)) since it is a logarithmic relation. Therefore, the hardware overhead actually decreased for ‘Benchmark SoC 2’ since it has more scan chains.

The result shows that for the realistic SoC, IIPS did not incur too much overhead. Furthermore, since IIPS is only enabled during testing and not normal operation, power overhead is also significantly reduced.

Table 2: Hardware Overhead Results

	Benchmark SoC 1	Benchmark SoC 2
# of SFFs	464	36,193
# of scan chains	3	146
Area (μm^2)	7,154	614,280
IIPS Area (μm^2)	546	4,978
Area increase (%)	7.6	0.8

The testing for Hardware Trojans & ScanPUF are beyond the scope of this paper since they involve FPGA development boards & inter-die calculation methods. However, in summary, it was proven that in 500 chips, 128 bit signatures for the path delay when doing ScanPUF yielded an average of around 64 bits in signatures that were exclusive. Also, for Hardware Trojan testing, different circuit paths that had differing amount of path delays were tested using modelled Trojans and there was an average accuracy of around 93.7%.

6. Conclusion

6.1. Flexibility

Even though, IIPS uses only certain pats of the IEEE 1500 infrastructure, it shows a lot of promise. If IIPS were to use more aspects of the infrastructure, such as using the parallel wrapper instead of serial, more testing time could be saved. Furthermore, since the IEEE infrastructure is a standard, even if the IIPS had to use another infrastructure, it would more or less would not need a lot of adjustment. This shows that the IIPS can be flexible for SoCs.

6.2. Scalability

IIPS shows good scalability. Since the test time does not increase that dramatically with size and also the protection against scan based attack is based on system-level authentication and scan chain activation logic is independent of the SoC size. Since the IEEE 1500 infrastructure is already there, the power and hardware overhead is not significant as shown by Table 1. Moreover, IIPS can be used with other infrastructure IPs as well which would diminish operating costs more due to resource sharing and a centralized control logic. With all the testing protocols already designed into the IIPS, it could be implemented both into hardware as well as controllers that are programmed by software (e.g. microcontroller).

6.3. Self-security

Although the IIPS can protect against hardware security onboard an SoC, the security of the IIPS itself also has to be maintained. The IIPS modules can be designed and produced by SoC manufacturers in a confidential situation t prevent fraud and cloning. Fortunately, the recreation of a state machine from layout alone, even if received from untrusted vendors, would be extremely hard and also integrating undiscoverable threats inside Finite State Machines is extremely difficult. This could be made harder by hardware obfuscation approaches to makes reverse engineering that much more challenging.

7. References

- Wang, Zheng, Basak, Bhunia, “IIPS: Infrastructure IP for Secure SoC Design”, in IEEE Transactions On Computers Vol. 64, No. 8, August 2015, pp. 2226–2238
- G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in Proc. 44th Annu. Des. Autom. Conf., 2007, pp. 9–14.
- S. Paul, R. S. Chakraborty, and S. Bhunia, “VIm-Scan: A low overhead scan design approach for protection of secret key in scan-based secure chips,” in Proc. IEEE VLSI Test Symp., 2007, pp. 455–460.
- B. Gassend, D. Clarke, M.V. Dijk, and S. Devadas, “Delay-based circuit authentication and applications,” in Proc. ACM Symp. Appl. Comput., 2003, pp. 294–301.

- F. DaSilva, et al., “Overview of the IEEE P1500 Standard,” in Proc. Int. Test Conf., 2003, pp. 988–997.
- IEEE 1500 Embedded Core Test [Online]. Available: http:// grouper.ieee.org/groups/1500/, 2014.
- E. J. Marinissen, “The role of test protocols in automated test generation for embedded-core-based system ICs,” J. Electron. Testing: Theory Appl., vol. 18, no. 4/5, pp. 435–454, Aug.–Oct., 2002.
- K. Xiao, X. Zhang, and M. Tehranipoor, “A clock sweepingtechnique for detecting hardware trojans impacting circuits delay,” IEEE Des. Test Comput., vol. 30, no. 2, pp. 26–34, Apr. 2013.
- S. Narasimhan, W. Yueh, X. Wang, S. Mukhopadhyay, and S. Bhunia, “Improving IC security against Trojan attacks through integration of security monitors,” IEEE Des. Test Comput. Special Issue Smart Silicon, vol. 29, no. 5, pp. 37–46, Oct. 2012.