STEP: A Unified Design Methodology for Secure Test and IP Core Protection

Pranav Yeolekar[1], **Rishad A. Shafik**[2], **Jimson Mathew**[3], **Dhiraj K. Pradhan**[4], **Saraju P. Mohanty**[5]
[1,2,3,4]Dept. of Computer Science, University of Bristol, Bristol, BS8 1UB, UK
[5]NanoSystem Design Laboratory (NSDL), University of North Texas, Denton, TX 76203, USA
E-mail: csras@bristol.ac.uk[2], jimson@cs.bris.ac.uk[3], pradhan@cs.bris.ac.uk[4], saraju.mohanty@unt.edu[5]

ABSTRACT

Intellectual property (IP) core based embedded systems design is a pervasive practice in the semiconductor industry due to shorter time-to-market and tougher cost competitions. Protecting the design information in these IP cores and securing test from various attacks are two emerging challenges in today's embedded systems design. Recently reported techniques address these challenges considering secure test and IP core protection separately. However, for ensuring high security during IP core functionality and also during test, joint consideration of secure test and IP core protection is much needed. In this paper, we propose a novel and unified design methodology, called STEP (**S**ecure **TE**st and IP core **P**rotection), which addresses the joint objective of secure test and IP core protection. The aim of STEP design methodology is to achieve high security at low system cost using the same key integrated hardware during test and IP core functionality. We evaluate the effectiveness of STEP design methodology considering advanced encryption standard (AES) system as a case study. We show that proposed design methodology benefits from high security and test accuracy, requiring up to 9% higher area and 20% power overheads.

Categories and Subject Descriptors

B.7 [**Hardware**]: Integrated Circuits; K.6.5 [**Computing Milieux**]: Security and Protection—*Physical Security*

General Terms

Design

Keywords

Security and protection, intellectual property core

1. INTRODUCTION

With continued technology scaling to unprecedented levels, embedded systems design is increasingly becoming complex. This is further exacerbated by the shorter time-to-market demands with design constraints related to power, performance and reliability. To address such design complexity, designers have resorted to highly modular, reusable and effective design approach using intellectual property (IP) cores. Although such design approach has proven to be effective to date, an emerging challenge for IP core based design approach is to securely protect the design information from design pirates or hackers. These design pirates or hackers intrude into the design information through various tampering or attack mechanisms, including reverse engineering techniques, power and timing analysis and fault injection or even through stealing fabrication masks, etc [1, 2, 3]. The design information can be then misused by them in the following two ways. Firstly, the design information can be used to build counterfeit and competitive products, causing direct financial losses [4]. Secondly, the design information can be altered deliberately, inflicting damage of reputation and more financial losses. Hence, protection of IP core design information and functionality is one of the major concerns for semiconductor industry [5, 6].

Traditional IP core design methodology integrates design for test (DfT) features in the hardware design. The premise of the DfT features is that the original and also the added hardware can be validated against various defects or faults to ensure correct functionality [7]. Scan chain based testing is considered as a *de facto* standard of DfT due to its simplicity of design and high fault coverage [8]. It is implemented through insertion of a chain of flip-flops between logic blocks for providing with a mechanism to observe responses of these logic blocks using different test patterns. However, since these scan chains directly reveal the internal state of the logic blocks and their circuits, extracting design information from them becomes easier for design pirates or hackers through response analysis or side channel attack during testing [9]. Hence, secure testing is a critical requirement for DfT [10, 11].

Over the years, researchers have proposed various techniques and methodologies to address IP core protection and secure test. For example, an IP core protection approach using locking of combinational logic circuits was proposed by Roy *et al* [12]. Their protection approach uses separate locking key for every single chip and enables a licensing technique allowing only approved users to be able to unlock the device. Chakraborty *et al* [13] proposed another protection approach using hardware obfuscation technique at netlist level. In this approach, every chip requires activation by a specific input sequence. When activation does not occur, response of the hardware changes randomly. Among others, IP core protection techniques using watermarking were proposed by Castillo *et al* [14] and Kahng *et al* [4]. The watermarking is incorporated by hosting the bits of a digital signature during design specification using combinational logic within the original design. To secure the design from various attack mechanisms during scan chain based testing, a number of different other techniques have been shown. For example, scan chain scrambling technique by Hely *et al* [15], scan chain randomization technique by Lee *et al* [9] and scan chain replacement approach with de Bruijin graph based shift register chains by Fujiwara *et al* [16] were proposed. The main idea in these works is to make side channel based attack difficult by dividing scan chains into sub-chains and making information in the scan chains unpredictable to the attacker. Another secure DfT approach using flipped scan chains was shown by Sengar *et al* [17]. In their approach, inverters are inserted randomly in the scan chains for protection.

The above works address IP protection and secure test separately [11, 12, 13, 17]. However, such consideration do not automatically complement security and protection during test and also during normal IP core functionality. For example, with an IP core protection technique alone, it is still exposed to security threats during testing as it is possible to reverse engineer the bitstream through side channel attacks [7]. Similarly, with a secure DfT alone, it is possible to carry out a response analysis during normal operation to extract design information [14]. To provide with security and protection at all times, it is important that secure DfT and IP core protection are considered as a joint objective, which is the main of this paper. However, system design with such joint objective is confronted with conflicting design requirements with the system cost. This is because, design for IP core protection introduces extra hardware resources. Due to addition of these hardware resources, either fault coverage obtained during testing will need to be compromised, or more scan chains and test patterns would be needed to ensure required fault and test coverage. Moreover, to ensure security during testing, further hardware resources and test patterns would be required, causing high system overhead. As a result of such design requirements with possible overheads involved, design for secure test and IP core protection is highly challenging [7].

In this paper, we propose a *novel* and *unified* STEP (**S**ecure **TE**st and IP **P**rotection) design methodology to address secure test and IP core protection as a joint objective. The aim is to use the same hardware resource for secure test and IP protection to achieve low system cost. We show that STEP is simple to implement and features high security and test accuracy at low system overheads. To the best of our knowledge, this is the first paper that addresses unified methodology with such joint design objectives. The rest of this paper is organized as follows. Section 2 presents the proposed unified design methodology, STEP, for secure test and intellectual property (IP) core protection, while Section 3 details the secure test and IP core protection architectures generated through STEP using an advanced encryption standard (AES) design as a case study. Section 4 presents the comparative system costs and security analysis of the secure AES systems generated using the STEP design methodology with the insecure AES systems designed using traditional methodology. Section 5 concludes the paper.

2. PROPOSED DESIGN METHODOLOGY

In this work, we propose a unified design methodology, STEP, for secure test and IP core protection. The STEP design methodology removes the need to add dedicated hardware separately for security and protection in the system and hence gives low area and power overheads (Section 4 details results of different systems overheads and security analysis). Figure 1 shows the STEP design methodology, highlighting the four major design phases. The first two design phases deal with traditional design methodology based on functional design and design for test (DfT) using scan chains. The other two phases integrate security features into scan chain based test and also incorporate IP core protection. The detailed descriptions of STEP design phases follow.

2.1 Phase I: *Functional Design*

This phase includes the design specification at register-transfer level (RTL). This is followed by simulation to validate functionality of the RTL design. Once validated, the design is then synthesized, which generates netlist of the design. Using this netlist, power and area analysis are carried out. To validate the functionality of the post synthesis design, gate-level simulation is also carried out.

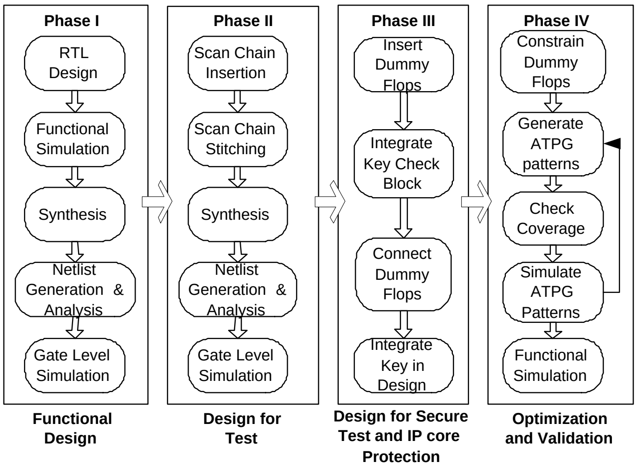

Figure 1: Proposed unified design methodology, STEP, for secure test and IP core protection

2.2 Phase II: *Design for Test*

This phase implements the design for test (DfT) strategy through insertion of scan chains and scan chain stitching in the netlist generated in Phase I. This is done through replacing the original flip-flops by the scan flip-flops and stitched together to form the scan chain. This is then followed by synthesis to generate the new netlist with DfT features. Using this netlist, area and power analyses are carried out to determine the overheads caused by introducing DfT in this design phase. Finally, gate level simulation is carried out to validate the functional behavior of the design (Figure 1).

2.3 Phase III: *Design for Secure Test and IP Core Protection*

This is the most crucial part of the design methodology as hardware changes are made to introduce security in the design. These hardware changes include insertion of dummy flip-flops in the design to form a shift register and integrating key checking hardware block to the design at the netlist level. Due to insertion of dummy flip-flops, the scan chains are broken in the design in Phase II (Figure 1). As a result, the complexity of determining secret information through scan-based side channel attacks increases substantially, making the scan chains secure. To provide further security and protection during test and also during normal operation in the IP core, random key generation and comparison hardware is integrated in the system. The random key generation is carried out through a pseudo-random bit-sequence (PRBS) generator. During testing operation, this PRBS key generator receives seed from scan chain data, while during normal operation the PRBS key generator receives pre-defined seed for generating a random sequence of numbers. Such key generation makes it very hard for a design hacker to extract bit-streams through reverse engineering. Further details of the key based mechanism for secure test and IP core protection are presented in Section 3.2 using a case study of an AES system.

2.4 Phase IV: *Optimization and Validation*

In this final phase, design optimization and validation is carried out to minimize system cost in terms of area and power. First, the the number and placements of the dummy flip-flops are constrained to minimize the system cost. Then the test patterns for scan chains are generated through automatic test pattern generation (ATPG). With the given test patterns, the effectiveness of the secure test (Phase III) is found out and fault coverage is analyzed through the covered and uncovered faults. Pattern generation and fault coverage analysis is continued until desired coverage is obtained. When desirable coverage is achieved, simulations are carried out to validate the effectiveness and functionality of the system with integrated secure test and IP core protection.

The unified design methodology outlined above can be used to generate a system with integrated secure test and IP core protection architectures. The secure test and IP core protection architectures implemented on an AES system are shown next.

3. SECURE TEST AND IP CORE PROTECTION ARCHITECTURES

In this section, the proposed unified design methodology, STEP (Section 2), is employed for secure test and IP core protection of an advanced encryption standard (AES) benchmark system [18]. The AES system has been chosen as a case study, as also used in [10, 17], since it is widely used in various critical cryptographic applications in finance, banking, security, etc. In the following, secure test and IP core protection architectures of an AES system, generated by proposed STEP design methodology, are presented in details.

3.1 Secure Test Architecture

Figure 2 shows secure test architecture of an AES system generated using STEP design methodology (Figure 1). For demonstration purposes, only two scan chains are shown. As can be seen, to incorporate secure test in the test architecture, dummy flip flops are inserted randomly in the design (Phase III, Section 2). The addition of these dummy flip-flops into the scan chains increase the complexity of determining secret information through scan-based side channel attacks and thus make scan chain based testing secure.

To incorporate further security in the test architecture, key integrated security hardware block is introduced. This hardware block consists of a key checker and a pseudo-random bit-sequence generator (PRBS) (Figure 2). The key checker holds hard-coded secret key, which is only available to a licensed or approved user. The key checker checks this key against the key input from all dummy flops that is N bits wide. The PRBS generator feeds pseudo-random sequences on every clock cycle using the seed from the scan chain inputs.

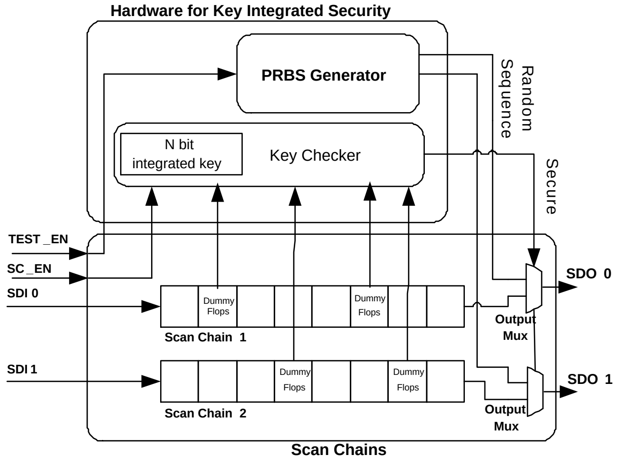

Figure 2: Secure test architecture generated by STEP design methodology for an AES system

With the added hardware resources, the operational sequence in the secure test architecture generated by STEP design methodology is given below:

(a) Enable Testing Mode: The secure testing is enabled by HIGH $TEST\_EN$ signal. This also enables key checking mechanism as SC_EN is set to LOW.

(b) Scan Cycles: When testing is enabled, the data is shifted into the scan chain through $SDI0$ and $SDI1$ and the response is checked at the output signals $SDO0$ and $SDO1$. During this time, LOW *SC_EN* acts as a select line for the scan multiplexers. The data shifting happens in *LOAD* and *SHIFT* cycles. During *LOAD* cycle, the internal data from the combinational logic are loaded into the scan chains and during *SHIFT* cycle, these data are shifted out.

(c) Key Checking: To enable these shifted data at the output multiplexer, the key checker must check the hard-coded key in it with the N bits key stored in N dummy flip-flops during every *LOAD* cycle. When a key match takes place, the key checker generates output as LOW *Secure* signal, which acts as the select line for enabling the shifted scan data at the output multiplexer (as $SDO0$ and $SDO1$). In case of mismatch, HIGH *Secure* output signal is generated, which acts as a select line for the output of PRBS generator. The random sequence generated by PRBS is enabled at the output multiplexer. Hence, unapproved users without the secure key fail to see any meaningful sequence at the output multiplexer.

Using the above secure test mechanism with key integrated security hardware, it becomes extremely hard for a design pirate or hacker to extract the design information. This is because, the design hacker will need access to the following three information to successfully extract design information: (a) the size of the random key, N, (b) the position of dummy flip-flops, and (c) the seed used in PRBS key generator. However, the addition of such hardware resources also add to the system overheads and costs. Section 4 presents the resulting system costs and security analysis for the secure test architecture.

3.2 IP Core Protection Architecture

The basic principle of IP core protection in STEP design methodology is to use variable keys during operation, which is an effective technique for protection against unsolicited design attacks and intrusion [7]. Figure 3 shows the block diagram of an IP core architecture incorporating variable key protection. Due to unified design methodology, the same hardware is used for IP core protection during normal operation. However, the following operational changes are incorporated for variable key based protection:

- The dummy flip-flops now forms an N bits shift register.
- The PRBS generator is now used as an internal variable key generator using pre-defined seed.
- The key checker now checks for variable key sequence in every iteration instead of the hard-coded key that was used during secure test operation.
- The first scan chain input ($SDI0$) is now used as the input for the N bits shift register formed by the dummy registers.

With the above changes, the operating sequence of the IP protection architecture generated by STEP design methodology is as follows:

(a) Enable Functional Mode: When the $TEST\_EN$ pin is LOW, the chip enters into functional mode. During functional mode, *SC_EN* is is set to HIGH. This enables the logic data input at the output of the scan multiplexers.

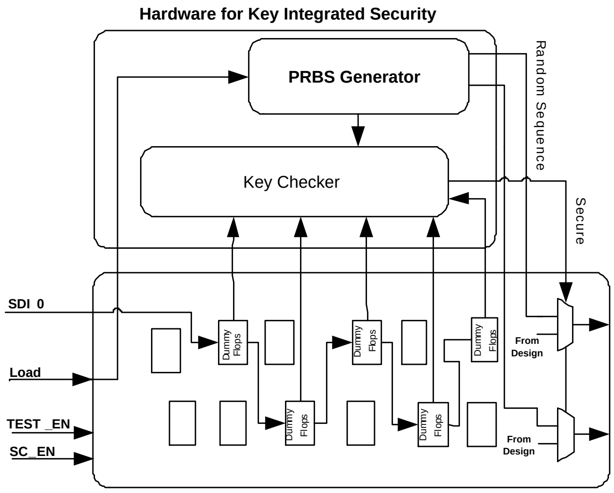

Figure 3: IP core protection architecture generated by STEP design methodology for an AES system

(b) Variable Key Generation: The PRBS generates a new key during every new iteration in the AES core with a given pre-defined seed. This forms a variable key generation scheme.

(c) Key Checking: The variable key from the PRBS is then compared within the key checker against the key stored in the N bits shift registers. These shift registers are formed through random inter-connection scheme among the dummy flip-flops within the scan chains (Figure 3). The key sequence is loaded into these shift registers through the scan input $SDI0$. When there is a key match, the key checker generates a HIGH *Secure* signal enabling the design logic data to be selected at the output. When there is no key match, the key checker generates a LOW *Secure* signal enabling the previously generated random sequence from PRBS to be selected at the output.

With the added key integrated security hardware through STEP design methodology, the AES system only works as expected for approved or licensed users, who have access to the given key sequence. Due to variable key integration in the IP core architecture, it provides with highly protected IP core against any security threats in terms of reverse engineering or even other response analyses techniques. This is because, for extracting actual design information, the hacker must decode the following three information: (a) the variable key sequence, (b) the interconnections of dummy flip-flops used to form a shift register to shift and hold a variable key sequence, and (c) the seed used for PRBS. The following section presents the details of the resulting system costs due to addition of the key integrated security hardware for IP core protection, emphasizing the achievable security level through STEP design methodology.

4. RESULTS AND ANALYSIS

To evaluate the effectiveness of the proposed design methodology, three secure AES systems with varied complexity (i.e. number of S-boxes) are designed with the proposed STEP design methodology (Section 2). These secure AES systems are then compared with insecure systems of the same generated using traditional design flow (Phases I and II in STEP, Section 2). The comparative evaluations are carried out through the following comparisons: area, power, testability and security. The comparative analyses follow.

4.1 Area Comparisons

Figure 4 shows the comparative areas (in μm^2) of the three secure and insecure AES systems found through post-synthesis evaluations in Synopsys Design Compiler^{TM}. From Figure 4 two observations can be made. The first observation is related to the fact that with higher complexity of the AES systems, the resulting area of AES systems increases as expected. For example, as complexity increases from 4 S-box to 16 S-box, the area increases by about 39% and 42% for the secure AES (through STEP) and for traditional insecure AES, respectively. The second observation is that the secure AES systems designed using the STEP design methodology (Section 2) gives higher area (in μm^2) than the insecure AES systems. The higher area for secure AES is expected due to addition of key integrated security hardware in secure test and IP core protection architectures (Section 3). However, due to unified design methodology in STEP using the same hardware for both secure test and IP core protection, the area overhead is kept low. From Figure 4 it can be seen that up to 9% area overhead is caused for incorporating security in the 8 S-box AES system, when compared with that of 8 S-box insecure AES system.

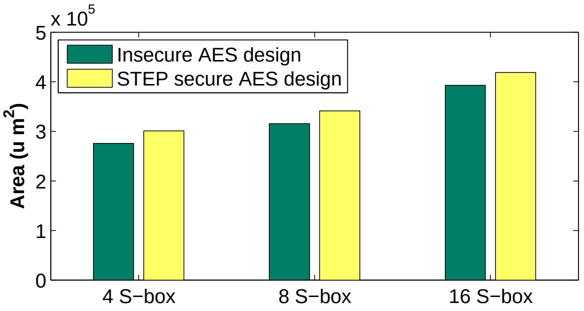

Figure 4: Area comparisons between secure AES systems using the proposed unified design methodology, STEP (Figure 1), and insecure AES systems

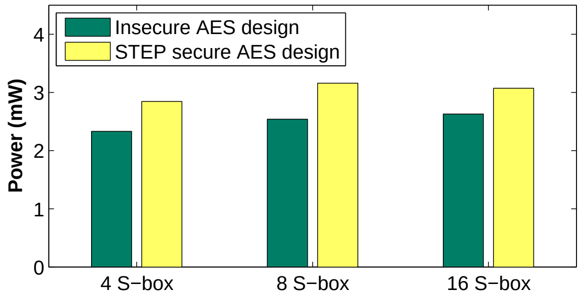

Figure 5: Power comparisons between secure AES systems using the proposed unified design methodology, STEP (Figure 1), and insecure AES systems

4.2 Power Comparisons

Figure 5 shows the comparative power consumptions (in mW) between three secure AES systems with proposed STEP design methodology (Section 2) and insecure AES systems using traditional design methodology (Phase I and Phase II, Figure 1). The power consumptions were evaluated using Synopsys Design Compiler^{TM}. As can be seen, with higher complexity of the AES, the power consumption increases. This is expected because with higher AES complexity (i.e. with higher S-box designs), the number of AES iterations and also the computations carried out over a given time increases [18]. For example, as AES complexity increases from 4 S-box to 16 S-box for the secure AES systems, the power consumption increases by about 13%. From Figure 5 it can also be seen that the power consumption is higher for secure AES systems when compared with that of similar insecure AES systems. For example, the power consumption increases by up to 20% for the proposed secure 8 S-box AES system, when compared with the same of an insecure 8 S-box AES system. The higher power consumptions in secure design is

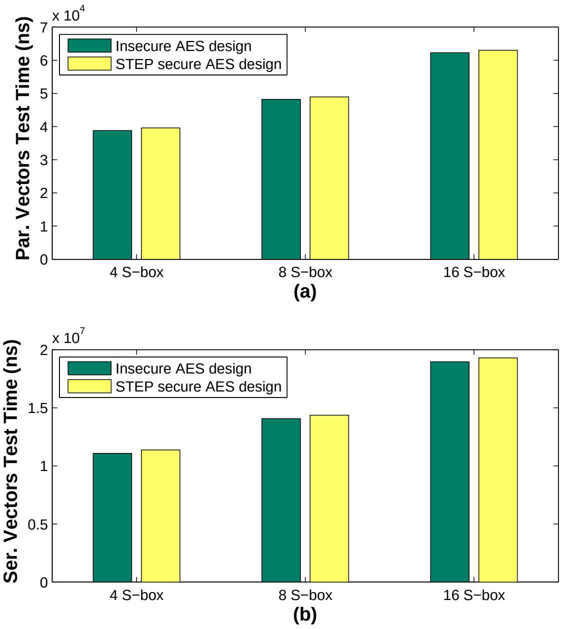

Figure 6: Comparative test times (in ns) for (a) parallel vectors, and (b) serial vectors using secure design methodology (Section 2) and insecure design methodology

due to addition of key integrated security hardware in unified design methodology in STEP (Section 3).

4.3 Test Time and Fault Coverage Analysis

Since the secure test and IP core protection architectures generated by proposed STEP design methodology integrates extra hardware (Section 3), it is important that the test capabilities are compared between the secure and insecure AES systems. To this end, Figures 6(a) and (b) show the comparative test times taken by different secure and insecure AES systems using the parallel and serial test vectors. These test vectors were input through Synopsys Tetra Max^{TM}. From these figures, two observation can be made. Firstly, as expected it can be seen that the test times are considerably lower for parallel vectors (Figure 6(a)) compared to the serial vectors (Figure 6(b)). This is because parallel test vectors significantly reduce the time required for the scan chain data to be loaded and shifted. Secondly, as can be seen, the secure AES systems generated using the proposed unified STEP design methodology takes more more test time for both parallel and serial test vectors. This is because secure AES systems use fixed (in testing mode) and variable (in functional mode) key based hardware to incorporate secure test and IP core protection (Section 3). The key generation, loading and checking mechanism within this integrated security hardware require extra test time (i.e. up to 2% extra delay for 4 S-box secure AES system) compared to the original test times in the insecure AES systems.

Table 1: Total faults injected, fault coverage and number of test patterns tested in different secure AES systems generated using the proposed STEP design methodology (Section 2)

AES System	no. of faults	Fault Coverage	Test Patterns
4 S-box	94316	99.04	775
8 S-box	116256	99.03	963
16 S-box	160412	99.02	1244

Test capabilities of the secure AES systems are further evaluated in terms of the required number of test patterns for achieving a specified fault coverage. Table 1 shows the number of inserted faults, corresponding fault coverage obtained and the number of test patterns used for testing in different secure AES systems. Columns 1 and 2 show the AES designs and number of faults injected, while columns 3 and 4 show the corresponding fault coverage and the number of test patterns used. As can be seen, with increased design complexity, higher number of faults need to be investigated and tested for due to increased number of iterations and area of the AES (Section 4.1). For these given number of faults, 99% fault coverage can be effectively achieved using the secure test architecture (Section 3.1). However, this fault coverage is achieved using various numbers of test patterns (column 5, Table 1). As expected, as the design complexity increase, the number of test patterns used also increases. For example, from 8 S-box secure AES design to 16 S-box secure AES design the number of test patterns increase by about 29%.

To compare the test capabilities between secure and insecure AES systems, Figure 7 shows the comparative number of test patterns used by the secure and insecure AES designs for a given fault coverage (i.e. 99% fault coverage). These test patterns were generated using special testbenches in Synopsys Tetra Max^{TM}tool. As can be seen, the secure test in AES system generated using STEP design methodology uses up to 2% higher number of test patterns for achieving similar test coverage as that of the test in insecure AES system. The extra test patterns in secure test can be explained as follows. The extra key integrated security hardware used in secure test architecture (Section 3.1) requires more scan chains and hence more test patterns are needed to achieve similar fault coverage.

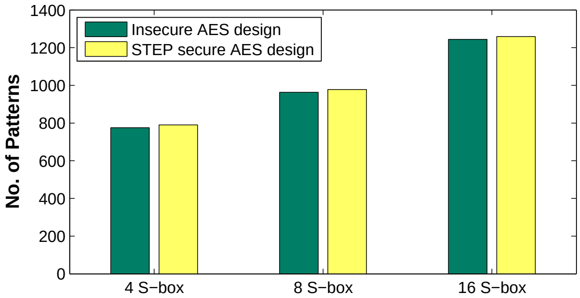

Figure 7: Comparative number of test patterns for similar test coverage between secure AES designs and insecure AES designs

4.4 Security Analysis

The proposed STEP design methodology gives high security advantage at the cost of up to 9% area, 20% power and 2% test overheads (Sections 4.1, 4.2 and 4.3). To understand the effective security advantage in the system, in the following hacking scenarios of secure test and IP core protection are briefly explained.

4.4.1 Test Security Analysis

To successfully hack into the secure test architecture, a hacker must extract the following information (Section 3.1): (a) the size of the random key, N, (b) the positions of N dummy flip-flops within S total flip-flops within scan chain, and (c) the seed used in PRBS key generator, R. Assuming that the hacker stores his guessed random key and PRBS seed in an M bits number and that $M \geq N$, the number of combinations hacker has to try for guessing N (C_N) and R (C_R) correctly are

$$C_N = 2^M \quad , \quad C_R = 2^M \quad . \tag{1}$$

Also, to guess the correct position information of the dummy flip-flops the hacker will have to try another C_{ff-pos} combinations, given by

$$C_{ff-pos} = G \binom{S}{N} \quad , \tag{2}$$

where S is the size of a scan chain with dummy flip-flops, N is the number of dummy flip-flops and G is the number of scan chains. Since for each N and R guess, the hacker will have to try to locate the dummy flip-flop positions, the total number of combinations the hacker would need to try for successfully breaking into the secure test system is given by number of combinations given in (1) and (2), i.e.

$$C_{test} = C_N \ C_R \ C_{ff-pos} = 2^{2M} \ G \ \binom{S}{N} \quad , \tag{3}$$

which is extremely challenging.

4.4.2 IP Core Protection Analysis

For a successful attack in the IP core architecture, a hacker must extract the following information: (a) the sequence of k variable keys, (b) the protocol to shift in the key, i.e. a given interconnection of N connections out of total S scan chain flip-flops, and (c) the seed used for PRBS key generator, $\mathcal{R}$ (Section 3.2).

Considering k keys in the sequence, the number of combinations the hacker have to try for getting the correct sequence (C_{seq}) and the seed ($C_{\mathcal{R}}$) in an M bits number are given as

$$C_{seq} = 2^{kM} \quad , \quad C_{\mathcal{R}} = 2^{M} \quad . \tag{4}$$

For correctly guessing the interconnection scheme among N dummy flip-flops and also to identify their positions within G number of scan chains of length S each, the hacker will have to try C^{ff-con}_{guess} combinations, given by

$$C_{ff-con} = G \ N! \ \binom{S}{N} \quad . \tag{5}$$

Since for each N and R guess, the hacker will have to try to locate the dummy flip-flop positions and connections at the same time, the total number of combinations the hacker would need to try for successfully breaking into the secure IP core proection is given by (4) and (5), i.e.

$$C_{IP} = C_{seq} C_{\mathcal{R}} C_{ff-con} = 2^{M(k+1)} \ G \ N! \ \binom{S}{N} \quad , \tag{6}$$

which is again extremely challenging.

As can be seen from (3) and (6), STEP design methodology provides high security advantage over insecure design methodologies requiring the hacker to generate large number of combinations to extract the design information. As an example, considering N=32, G=8, S=132 and k=4 for an 8 S-box AES system, a total of $C_{test} = 6.7 \times 10^{50}$ and $C_{IP} = 1.4 \times 10^{115}$ combinations are required for breaking into secure test and IP core protection, respectively. This can be further made more challenging by increasing the number of combinations through the use of more and longer scan chains (i.e. higher G and S) with higher number of dummy flip-flops (i.e. higher N). However, this will impose higher system costs in terms of area, power and test times or accuracy.

5. CONCLUSIONS

We have presented a novel design methodology for secure test and IP core protection. We have shown that the proposed unified design methodology, STEP (**S**ecure **TE**st and IP core **P**rotection), is simple to implement and employs the same key integrated security hardware for providing with security and protection during test and IP core functionality (Sections 2 and 3). Due to such use of unified security hardware, the STEP design methodology benefits from high security at low system costs. To evaluate the effectiveness of the proposed design methodology, different AES systems were designed and compared with similar insecure systems as case studies. The comparisons showed that our methodology offers significantly high security requiring high order of magnitude combinations required by the hacker to break into the security and protection of an 8 S-box AES system. This security advantage is achieved at the cost of 9% higher area, 20% higher power and 2% higher test times overheads (Section 4) without affecting the test capabilities.

6. REFERENCES

[1] L. Spitzner, "The Honeynet Project: trapping the hackers," IEEE Security & Privacy, vol.1, no.2, pp. 15- 23, 2003.

[2] E. Oswald, S. Mangard,ă"Counteracting Power Analysis Attacks by Masking," Chapter ină*Secure Integrated Circuits and Systems*. ISBN 978-0-387-71829-3, pp. 159 – 178. January 2010.

[3] D. Boneh, R. A. DeMillo, and R. J. Lipton. "On the importance of checking cryptographic protocols for faults," in *Lecture Notes in Computer Science*, 1233, pp. 37-Ű51, 1997.

[4] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, "Constraint-based watermarking techniques for design IP protection," *IEEE TCAD*, vol. 20, no. 10, pp. 1236–1252, Oct. 2001.

[5] Y. M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security" In *Proceedings of 16th USENIX Security Symposium*, pp. 291–306, Niels Provos (Ed.). Berkeley, CA, USA.

[6] D. C. Musker, "Protecting and exploiting intellectual property in electronics", in *Proc. IBC Conf.*, 1998.

[7] M.A. Razzaq, V. Singh, and A. Singh, "SSTKR: Secure and testable scan design through test key randomization", in *20th IEEE Asian Test Symposium (ATS)*, New Delhi, India, Nov. 2011.

[8] S. Wang, W. Wei, "A Technique to Reduce Peak Current and Average Power Dissipation in Scan Designs by Limited Capture," in *Proc. of Asia-Pacific Design Automation Conference, ASP-DAC*, pp.810–816, 23-26 Jan. 2007.

[9] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic, "Securing Designs against Scan-Based Side-Channel Attacks", *Dependable and Secure Computing, IEEE Transactions on*, vol.4, no.4, pp. 325-336, Oct.-Dec. 2007

[10] B. Yang; K. Wu; R. Karri, "Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard," in *Proc. International Test Conference*, pp 339-344, 2004.

[11] U. Chandran and D. Zhao, "SS-KTC: A High-Testability Low-Overhead Scan Architecture with Multi-Level Security Integration," in *Proc. of IEEE VLSI Test Symposium*, 2007.

[12] Jarrod A. Roy, Farinaz Koushanfar and Igor L. Marko, "EPIC: Ending Piracy of Integrated Circuits", in *Proc. of DATE*, 2008.

[13] R.S Chakraborty,S. Bhunia, "HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection", in *IEEE Trans. Computer Aided Design of Integrated Circuits and Systems*, vol. 28, no. 10, pp. 1493–1502, Oct. 2009.

[14] E. Castillo, U. Meyer-Baese, A. Garcia, L. Parilla, and A. Lloris, "IPP-HDL: Efficient intellectual property protection scheme for IP cores", *IEEE Trans. of Very Large Scale Integration (VLSI) Systems*, vol. 15, no. 5, pp. 578-590, May 2007.

[15] D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyre, and N. Berard. "Scan design and secure chip," in *Proc. 10th IEEE International On-Line Testing Symposium*, 2004.

[16] H. Fujiwara and M. E. J. Obien, "Secure and testable scan design using extended de Bruijn graph", in *Proc. 15th Asia and South Pacific Design Automation Conference*, 2010.

[17] G. Sengar, D. Mukhopadhyay, D. R. Chowdhury, "Secured Flipped Scan Chain Model for Crypto-Architecture," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 26,no.11, Nov. 2007.

[18] National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.