A Low-Cost Unified Design Methodology for Secure Test and Intellectual Property Core Protection

Rishad A. Shafik, *Member, IEEE,* Jimson Mathew, *Member, IEEE,* Dhiraj K. Pradhan *Fellow, IEEE,*

***Abstract*—On-chip security is an emerging challenge in the design of embedded systems with intellectual property (IP) cores. Traditionally this challenge is addressed using ad hoc design techniques with separate design objectives of secure design for testability (DfT), and IP core protection. However, in this paper, we will argue that such design approaches can incur high costs. Underpinning this argument, we propose a novel design methodology, called Secure TEst and IP core Protection (STEP), which aims to address the joint objective of IP core protection and secure testing. To ensure that this objective is achieved at a low cost, the STEP design methodology employs common key integrated hardware. This hardware is incorporated in the system through an automated design conversion technique, which can be easily merged into the electronic design automation (EDA) tool chain. We evaluate the effectiveness of our proposed design methodology considering various implementations of advanced encryption standard (AES) systems as case studies. We show that our proposed design methodology benefits from design automation with high security, and protection at the cost of low area, and power consumption overheads, when compared with traditional design methodologies.**

***Index Terms*—Secure test, intellectual property protection.**

ABBREVIATIONS

AES	Advanced Encryption Standard
ATPG	Automatic Test Pattern Generation
DfT	Design for Testability
EDA	Electronic Design Automation
EM	Electro-magnetic
IP	Intellectual Property
LFSR	Linear Feedback Shift Register
PRBS	Pseudo-random Bit Sequence
SoC	System-on-Chip

NOTATIONS

C_{IP}	Number of combinations for breaking IP security
C_{test}	Number of combinations for hacking during test
G	The number of scan chains
N	The size of the random key in the PRBS key generator
R	The seed used in the PRBS key generator
S	Total number of flip-flops in the design under test

I. INTRODUCTION

Continued technology scaling has enabled the fabrication of faster devices with smaller geometries. Examples of such devices include IBM's 22-nm [1], and Intel's emerging 16-nm [2]. These devices feature unprecedented integration capacity, and low power consumption. However, with these technological advances, design complexity is also increasing significantly, which is further exacerbated by shorter time-to-market demands coupled with design constraints related to application complexity, performance, and reliability. To address such design complexity, designers have traditionally resorted to a highly modular, reusable, effective design approach using intellectual property (IP) cores [3].

However, because similar IP cores are used in numerous system-on-chips (SoCs), an emerging challenge for such a design approach is to securely protect the design information and the underlying data from design hackers or pirates. Due to their modular, well-defined component based structure with known functionalities in them, IP cores can easily reveal design information, and data, when subjected to external tampering or intrusion based attacks [4], [5]. These tampering or attack mechanisms include reverse engineering techniques [6], [7], differential power and timing analysis [8], [9], and fault injection or stealing fabrication masks [10]. More recently, a silicon scanning based attack was demonstrated by [13] to reveal vulnerable design information in military systems. The design information, and data retrieved from these attacks, can then be misused by hackers in the following two ways. First, the design information can be used to build counterfeit competitive products, causing direct financial losses. Second, the design information can also be altered deliberately, inflicting damage to confidentiality and reputation [11]. Hence, protection of the IP core design information and the underlying data is a major design concern for embedded systems, particularly for those used in cryptographic systems [12].

To ensure correct functionality of these systems after manufacturing, traditional design methodology integrates design for testability (DfT) features into the hardware design. The main objective of introducing DfT features is that the original and added hardware can be validated against various defects or faults with different manifestations [14]. Scan chain based testing is considered as a *de facto* standard of DfT due to its simplicity of design, low cost, high controllability, and high fault coverage [16]. These scan chains are implemented through an insertion of interconnected flip-flops between the logic blocks. The aim is to provide a mechanism to observe the responses of these logic blocks using different test patterns. However, because these scan chains directly reveal the internal state of the logic blocks, and the underlying circuits, extracting the design information becomes easier for the design pirates or hackers through response analysis or side channel attacks [17]. Hence, secure testing is another critical requirement in cryp-

R. A. Shafik is affiliated with School of Electronics and Computer Science (ECS) in the University of Southampton, UK, while J. Mathew and D.K. Pradhan are affiliated with Microelectronics Research Group in the Department of Computer Science, University of Bristol, UK

Manuscript received in March 2014; first revision in June 2014, followed by second revision in May 2015, and accepted in June 2015.

tographic systems [18], [19].

To address the issues related to IP core protection, and secure test, researchers have proposed various techniques and methodologies over the years (Section II provides a detailed account of these techniques). These techniques address IP protection and secure test separately. For example, in [20], [21], IP core protection techniques have been proposed, while in [19], [26], scan chain based secure test methodologies have been shown. However, such considerations do not automatically complement security and protection during test, and during normal IP core functionality. Furthermore, to incorporate secure test and IP core functionality, separate considerations lead to very high overall system costs. To reduce the overall system cost, a unified design methodology with the joint design objective of IP core protection and secure testing is much needed.

To address secure test and IP core protection issues, this paper makes the following ***contributions***.

- We propose a *novel* and *unified* **S**ecure **TE**st and IP **P**rotection (STEP) design methodology using minimal hardware resources for securing designs during tests, and also for protecting IP cores during normal functionality.
- Fundamental to this methodology is an automated dummy flip-flop insertion and placement technique during the early design phase, which can be integrated into the Electronic Design Automation (EDA) tool chain.

To the best of our knowledge, this is the first paper that provides a unified, automated design methodology with such a joint design objective.

The rest of this paper is organized as follows. Section II presents some related works highlighting motivation towards a low cost, unified design methodology, while Section III outlines the proposed design methodology for secure test and intellectual property (IP) core protection. Section V details the secure test and IP core protection architectures generated through the proposed methodology using an advanced encryption standard (AES) system design as a case study. Section VI presents the comparative system costs, and security analysis of the secure AES systems generated using the STEP design methodology. Finally, Section VII concludes the paper.

II. Related Works and Motivation

Over the years, various approaches have been proposed by researchers to address the issue of IP core design and data protection. For example, an IP core design protection approach using combinational logic circuit locking was proposed by Roy *et al.* [20]. Their protection approach uses a 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.* [21] proposed another protection approach using a hardware obfuscation (i.e. deliberately confusing the internal information) technique implemented during the low-level circuit design. In this approach, every chip requires activation by a specific input sequence. When activation does not occur, the response of the hardware changes randomly. This effect makes hacking the design information and underlying data highly challenging. Among others, IP core protection techniques using watermarking were proposed by Castillo *et al.* [22], and Kahng *et al.* [11]. The watermarking is incorporated by hosting the bits of a digital signature during design specification using combinational logic within the original design. Solving the correct logic through watermarking is an NP-hard problem. Hence, to reduce the design complexity, Ni and Gao [23] proposed a low compexity detector-based watermarking technique for soft IP core protection.

To secure the design from various attack mechanisms during scan chain based testing, a number of different alternate techniques have been proposed. A scan chain scrambling technique dividing the original scan chain into sub-chains was proposed by Hely *et al.* [24]. Due to such scan chain scrambling, responses from side channel attacks become unpredictable, and hard for hackers to extract logic information from. A similar technique using a scan chain randomization technique was shown by Lee *et al.* [17]. This technique employs random interconnections between scan flip-flops to make responses non-deterministic for hackers. Similar principles with a scan chain replacement approach was presented by Fujiwara *et al.* [25]. The original scan chains were first divided into a number of sub-chains. These sub-chains are then replaced by shift register chains using de Bruijin graphs to obfuscate the responses and logic to hackers. Another secure DfT approach using flipped scan chains was shown by Sengar *et al.* [26]. In their approach, inverters are inserted randomly into the scan chains to obfuscate the internal logic, and ensure protection. A similar counter-measure to scan chain based threats have been shown in US Patent 7577886 [15]. The patent showed an effective technique to distribute the secure key within the scan chain. Such a key based test operation ensures that, to perform the test operations, a user must be authorized first, thus securing design information during test.

In the above works, secure test and IP core protection are considered as separate objectives [19], [20], [21], [26]. However, such considerations do not automatically provide security and protection during test, or duringnormal 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 [14]. Similarly, with a secure DfT alone, it is possible to carry out a response analysis during normal operation to extract the design information [22]. To ensure security and protection at all times, it is important that secure DfT and IP core protection are considered together. However, system design with such a consideration is confronted with design constraints related to the system cost because design for IP core protection introduces extra hardware resources. Due to the addition of these hardware resources, more scan chains and test patterns would be needed to guarantee high fault and test coverage. On the other hand, to ensure security during testing, further hardware resources and test patterns would be required, causing high system overhead. Due to such conflicting design requirements with overhead involved, design for secure test and IP core protection is highly challenging [14]. This work addresses the above challenges using a *novel* and *unified* STEP) design methodology, described next.

III. Proposed Design Methodology

The proposed STEP design methodology incorporates a unified key integrated hardware rather than separate hardware resources for security and IP protection as used in traditional design methodology. As a result, it benefits from high security at all times with low system overhead (Section VI details system overhead, and security analysis). Fig. 1 shows the STEP design methodology, highlighting three major design phases. The first design phase deals with traditional design methodology based on design for test (DfT) using scan chains, which is then followed by design for security and protection with integrated common key based hardware resources. The final phase incorporates test and system cost evaluation, and optimizes for high fault coverage at low-cost hardware overhead. In the following, each STEP design methodology phase is further detailed.

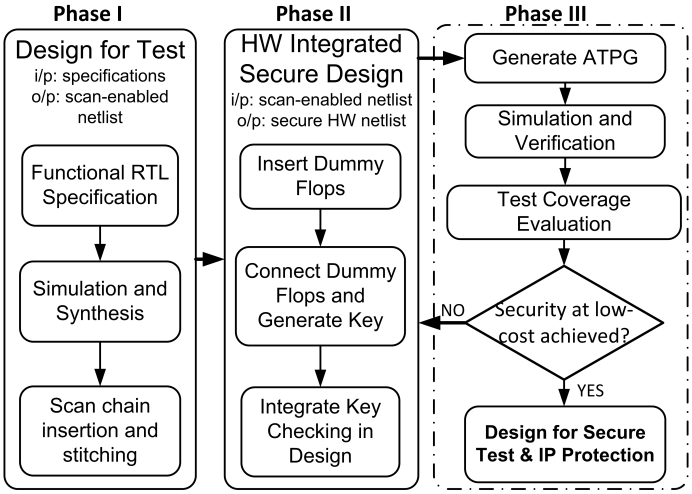


Fig. 1: Proposed unified design methodology, STEP, for secure test and IP core protection.

A. Phase I: Design for Test

This phase includes the RTL design specification, followed by simulations to validate the functionality of the design. Once validated, the design is then synthesized for generating the functional design netlist. It is then followed by introducing the DfT features through insertion of scan chains, and their stitching. The introduction of DfT features is done through replacing the original flip-flops by the scan flip-flops, and stitched together to form the scan chain. The scan chain based design is then synthesized to generate the netlist with DfT features. Using this netlist, area and power analyses are carried out to determine the overheads caused by introducing DfTs in this design phase. Finally, gate level simulation is carried out to validate the functional behavior of the design (Fig. 1).

B. Phase II: Design for Security

This phase is the most crucial part in the proposed design methodology as hardware changes are made to introduce security in the design. These hardware changes include two steps: cost-constrained dummy flip-flops insertion, and integration of key secured hardware, as shown in Fig. 1. In the following, these two steps are further detailed.

1) Insertion of Dummy Flip-flops: To initiate the design for security phase, first dummy flip-flops are inserted randomly into the original scan chains. These dummy flip-flops form a shift register, and break the original chains produced in Phase I by the scan flip-flops (Fig. 1). With such broken scan chains, the complexity of determining secret information through scan-based side channel attacks increases substantially, making the scan chains secure.

The dummy flip-flops insertion in this design phase is carried out in a systematic and automated way, described in Algorithm 1. The insertion is carried out by a separate HDL source-to-source parser and converter written in a high-level language, unlike manual insertion and stitching techniques previously used by [12], [21]. As can be seen, for a given scan chain array with S flip-flops, the parser initially determines the approximate number of flip-flops (N) that needs to be inserted per scan chain as the ratio of the total number of flip-flops to be inserted ($C \times G \times S$), to the number of scan chains G less the cost C (line 3). During this step, the maximum number between cost-constrained flip-flops and the minimum number of secure dummy-flops is selected as the target number of dummy flip-flops to be inserted in the design for security. Following this step, the location of each dummy flip-flop is determined randomly. For each new dummy flip-flop, its input is stitched with the previous flip-flop's output, and the output is stitched to the next flip-flop's input (lines 8-11). Such insertion and stitching are carried out until all scan chains have dummy flip-flops inserted in them (lines 4-8). Following the automated insertion, a new HDL file is generated that includes the dummy flip-flops with expected cost.

Algorithm 1 Automated dummy flip-flops insertion for a target security cost $\mathcal{C}$ (in %)

1: **Assume**: G scan chain arrays with S flip-flops each; $G \geq 1$
2: **Assume**: N' is the minimum number of secure dummy flip-flops
3: $N = \max\left(\frac{C \times G \times S}{G - C}, N'\right)$ // Number of dummy flip-flops
4: **for** g = 1:G **do**
5: **for** i = 1:N **do**
6: //Generate random number between 1 to (S+i)
7: x = RandomNumber(1, S+i)
8: //Stitch new dummy input to the random flop output
9: $g.i \rightarrow$input = $x \rightarrow$output
10: //Stitch new dummy output to the random flop input
11: $g.i \rightarrow$output = $(x+1) \rightarrow$input
12: **end for**
13: **end for**

The inserted dummy flip-flops are also connected as shift registers to allow key shifting during IP core protection (not shown in Algorithm 1). Additionally, N extra flip-flops are also inserted, and co-located with the dummy flip-flops using the same algorithm (Algorithm 1). These flip-flops are used to store the hardcoded key provided with a licensed user, and connected in random order to confuse the design hacker.

2) Key Checking Hardware: To provide security and protection during tests, and also during normal operation in the IP core, random key generation and comparison hardware are integrated into 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 a seed from the dummy flip-flops, while during normal operation the PRBS key generator receives a pre-defined seed for generating a random sequence of numbers. Such key generation makes it very hard for a design hacker to extract the design information or data through a side channel attack. Further details of the key based mechanism for secure test and IP core protection are presented in Section V-B using a case study of an AES system.

C. Phase III: Optimization and Validation

In this final phase, design optimization and validation is carried out to minimize the system cost in terms of area and power overhead, iteratively. First, the number and placements of the dummy flip-flops are constrained to minimize the system cost (through varying the C value in Algorithm 1). 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 evaluated, and the fault coverage is analyzed through the covered and uncovered faults. Pattern generation and fault coverage analysis is continued until the desired coverage is achieved. When the desirable coverage is achieved, functional 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 aim is to effectively reduce the overall system costs incurred due to additional security hardware compare to traditional ad hoc, and separate secure test, and IP core protection mechanisms. The secure test, and IP core protection architectures implemented on an AES system are shown next.

IV. Security Threat Model

Fig. 2 shows details of the threat models the proposed STEP design methodology is developed to protect against. Fig. 2(a) shows the security threat during test through side channel attacks, while Fig. 2(b) shows the envisioned design hacking mechanism during functionality of the IP core. Both security threat models are popular in secure test and IP core protection research [18], [19], [26], [21].

As can be seen, during tests, the scan chain outputs can be tapped through the side channel of the scan chains by the design hacker (Fig. 2(a)). The channel outputs can then be analysed for logic sequences, and their timings, to decode the logic design of the original design. Such side-channel attacks require the design hacker to carry out iterative analyses to decode the design information. Because scan chains are incorporated for almost all possible flip-flops in the combinational design for testability, and controllability considerations, design hackers can easily break into the design information if no security measures are incorporated.

Unlike side-channel attacks, design hacking during IP core functionality requires a much more rigorous set up. In this set up, the design hacker first feeds the design with some input data. The output data (output data 1) with such input data are then analyzed, and reverse engineering techniques are applied to generate similar outputs from the IP cores (output data 2). If both the outputs are matched, the design is then sequentially analysed, and the design hacker proceeds with further sets of input data. Similar to side-channel attacks, IP core attacks require the design hacker to carry out iterative input and output analyses to decode the design information (Fig. 2(b)).

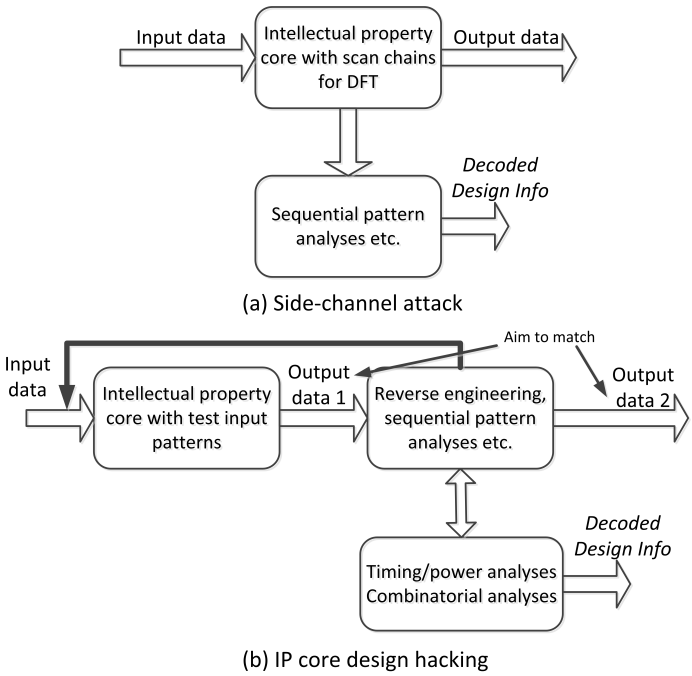


Fig. 2: Security threat model: (a) side-channel attack during test, (b) IP core design hacking using test inputs.

To address the security threats above, the proposed STEP design methodology incorporates unified key incorporated security measures. The secret keys are embedded in the chips, and the attacker has no access to the manufacturer's reference databases holding these keys. Attackers may do non-invasive attacks, such as collecting the EM emanations, or feeding the circuits with known inputs and observing the outputs. The PRBS is assumed to be of a good design (see Section VI), and it is assumed that the attacker cannot guess the PRBS output sequences. Both the chip designer and the manufacturer are trusted with the overall design layout.

V. Secure Test and IP Core Protection Architectures

In this section, the proposed unified design methodology STEP (Section III) is employed for secure test and IP core protection in an advanced encryption standard (AES) benchmark system [27]. The AES system has been chosen as a case study, as it was also used in [18], [26], because it is widely used in various critical cryptographic applications in finance, banking, security, etc. In the following, the secure test and IP core protection architectures of an AES system, generated by the proposed STEP design methodology, are described in details.

A. Secure Test Architecture

Fig. 3 shows a secure test architecture of an AES system generated using the STEP design methodology (Fig. 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 (Algorithm 1, Phase II, Section III). The addition of these dummy flip-flops into the scan chains increase the complexity of determining secret information through scan-based side channel attacks (Fig. 2(a)), and thus makes the scan chain based testing secure.

To incorporate security into the test architecture, a key integrated security hardware block is introduced. This hardware block consists of a key checker, and a PRBS generator (Fig. 3). The PRBS generator is essentially a set of LFSRs, which can generate a random sequence based on the scan chain inputs (details not shown for simplicity). The key checker holds a hard-coded secret key, which is only available to a licensed or an 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.

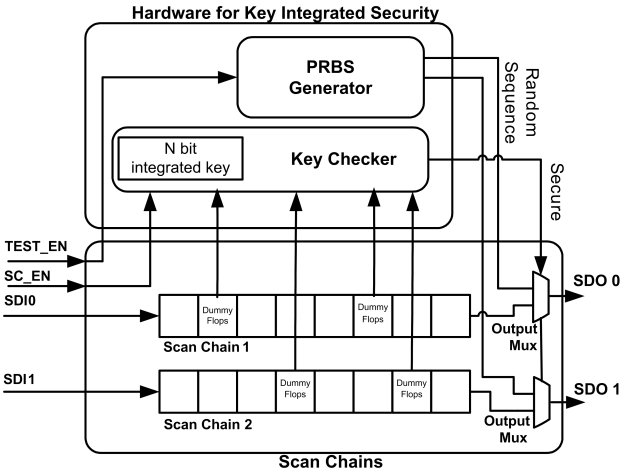


Fig. 3: Secure test architecture generated by STEP design methodology for an AES system.

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

1) *Enable Testing Mode:* The secure testing is enabled by a HIGH $TEST\_EN$ signal, which also enables key checking mechanism as SC_EN is set to LOW.
2) *Scan Cycles:* When testing is enabled, the data are shifted into the scan chain through $SDI0$, and $SDI1$; and the response is checked at the output signals $SDO0$, and $SDO1$. During this time, a LOW SC_EN generates a secure select line for the scan multiplexers for an authorized user. The data shifting happens in *LOAD*, and *SHIFT* cycles. During the *LOAD* cycle, the internal data from the combinational logic are loaded into the scan chains; and during the *SHIFT* cycle, these data are shifted out to the $SDO0$, and $SDO1$ signals. However, when the user is not authorized, the key checker generates select signals such that random sequences are shifted out to the output signals.
3) *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 bit key stored in N dummy flip-flops during every *LOAD* cycle. When a key match takes place, the key checker generates an output as a LOW *Secure* signal, which acts as the select line for enabling the shifted scan data at the output multiplexer (as $SDO0$, and $SDO1$). In the case of a mismatch, a HIGH *Secure* output signal is generated, which acts as a select line for the output of the PRBS generator. The random sequence generated by the PRBS is enabled at the output multiplexer. Hence, unapproved users without the secure key fail to see any meaningful sequence at the output multiplexer during test.

Using the above secure test mechanism with a key integrated security hardware, it becomes extremely difficult for a design hacker to extract the design information. The difficulty arises as the design hacker will need access to three pieces of information to successfully extract the design information through a side-channel attack (Fig. 2(a)): 1) the size of the random key N, 2) the position of dummy flip-flops, and 3) the seed used in the PRBS key generator. Section VI analyzes the resulting system security, and the associated costs for the secure test architecture (Fig. 3).

B. IP Core Protection Architecture

The novelty of IP core protection in the STEP design methodology is to use a similar hardware architecture with variable secure keys during operation. Such a security measure is effective for protection against unsolicited design attacks, and intrusion during IP core functionality [14]. Fig. 4 shows the block diagram of an IP core architecture incorporating variable key protection. Due to the 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 form an N bit shift register.
- The PRBS generator is now used as an internal variable key generator using a pre-defined seed.
- The key checker now checks for a 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 the STEP design methodology is as follows.

1) *Enable Functional Mode:* When the $TEST\_EN$ pin is LOW, the chip enters into the functional mode. During the functional mode, SC_EN is set to HIGH. This setting enables the logic data input at the output of the scan multiplexers.
2) *Variable Key Generation:* The PRBS generates a new key during every new iteration in the AES core with

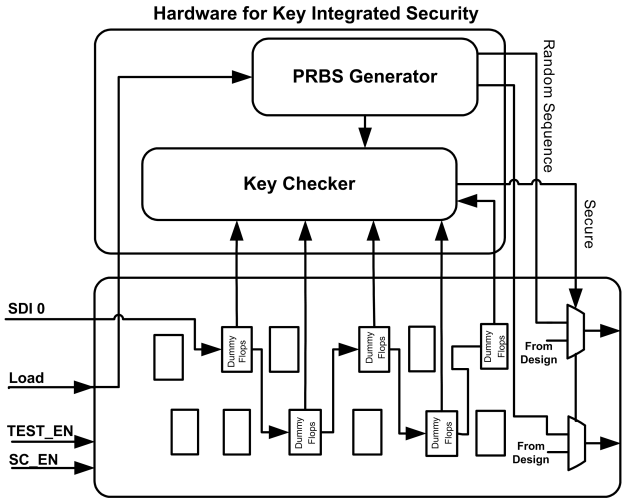


Fig. 4: IP core protection architecture generated by the STEP design methodology for an AES system.

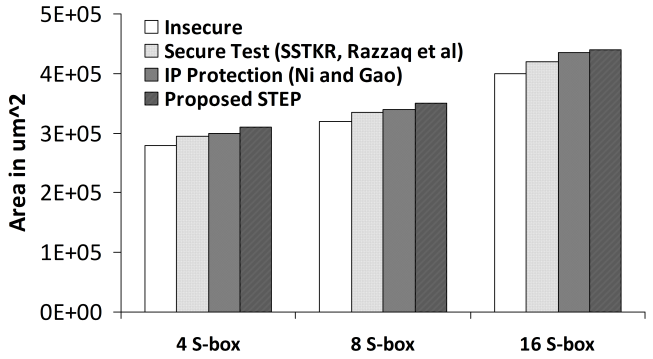


Fig. 5: Area comparisons between secure AES systems using the proposed unified design methodology, STEP (Fig. 1), separate secure test and IP core protection techniques, and also insecure AES systems.

a given pre-defined seed, resulting in a variable key generation scheme.

3) *Key Checking:* The variable key from the PRBS is then compared within the key checker against the key stored in the N bit shift registers (when IP core functionality is enabled, a select line loads the hard-coded keys). These shift registers are formed through a random interconnection scheme among the dummy flip-flops within the scan chains (Fig. 4). 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 due to unauthorized access, the key checker generates a LOW *Secure* signal, enabling the previously generated random sequence from the PRBS to be selected at the output.

With the added key integrated security hardware in the STEP design methodology, the AES system only works as expected for approved or licensed users. Due to variable key integration in the IP core architecture, it provides a high level of protection of the IP cores in the presence of any security threats in terms of reverse engineering or response analyses techniques. For extracting the actual design information, the hacker must decode three pieces of information: 1) the variable key sequence, 2) the interconnections of the dummy flip-flops used to form a shift register to shift and hold a variable key sequence, and 3) the seed used for the PRBS generator. The following section presents the details of the resulting system costs due to the addition of the key integrated security hardware for IP core protection. Section VI-D analyzes the achievable security through the STEP design methodology.

VI. Results and Analysis

To evaluate the effectiveness of the proposed design methodology, three secure AES systems with varied complexity (i.e. the number of transformation tables called S-boxes) are designed with the proposed STEP design methodology (Section III). These secure AES designs use 128 dummy flip-flops (i.e. N=128) to support 128-bit integrated key-supported secure test and IP core protection (Section V). The impact of cost directed dummy flip-flop insertion (Algorithm 1) will be investigated further in Section VI-A. The secure designs are then compared with insecure designs of the same, generated using a traditional design flow (Phases I in STEP, Section III), a design with secure test alone, and also a design with IP core protection alone. The secure testing design has been incorporated for the AES systems using dummy flip-flop insertion (as shown in Phase II, Section III-B) with a randomized test key approach, similar to [15], and [14], while IP core protection has been implemented by generating separate security codes (i.e. state control codes) using the key generating hardware (see Phase III, Section III-C) to compare against previously known watermark signature codes as shown by Ni and Gao in [23]. These comparative evaluations are carried out in terms of area and power overhead, performance and testability features, and security. The comparative analyses follow.

A. Area Comparisons

Fig. 5 shows the comparative areas (in μm^2) of the three AES systems found through post-synthesis evaluations in the Synopsys Design Compiler™. From Fig. 5 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 the AES systems increases, as expected. For example, as the complexity of the AES system 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 the traditional insecure AES, respectively. Such an increase in area is due to increased circuity with more S-boxes in the design. The second observation is that the secure AES systems designed using the STEP design methodology (Section III) give a higher area (in μm^2) than the other AES systems. The higher area for the STEP secure AES is expected due to the addition of key integrated security hardware in the secure test and IP core protection architectures (Section V). However, due to unified design methodology in the STEP using the same hardware for

both secure test and IP core protection, the area overhead is comparatively low when compared with secure test [14], and IP protection [23], alone. From Fig. 5, see that up to 9% area overhead is caused for incorporating security in the 8 S-box AES system, when compared with that of the 8 S-box insecure AES system. When compared with the separate designs for secure test [14], and IP core protection [23], the proposed STEP design has little area overhead (up to 3%), with the added advantage of joint secure test and IP core protection.

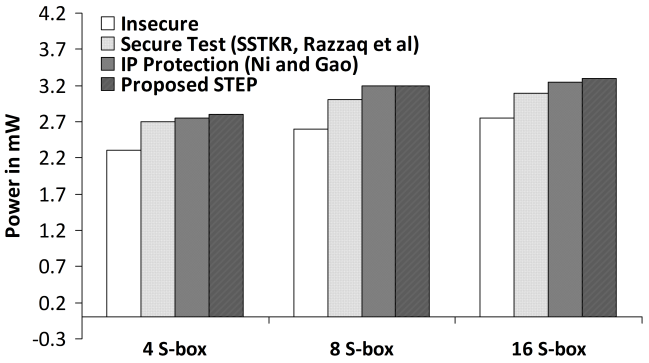


Fig. 6: Power comparisons between secure AES systems using the proposed unified design methodology, the STEP (Fig. 1), and the insecure AES systems.

B. Power and Performance Comparisons

Fig. 6 shows the comparative power consumptions (in mW) between secure AES systems designed with the proposed STEP methodology (Section III), secure test only, IP core protection only, and insecure design using the traditional design methodology (Phase I, Fig. 1). The power consumptions were evaluated during runtime using the Synopsys Design Compiler™. As can be seen, with the higher complexity of the AES, the power consumption increases. This outcome is expected because, with the 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 [27]. 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 Fig. 6, it can also be seen that the power consumption is higher for secure AES designs when compared with the other AES designs. 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. As expected, the power overhead in the STEP design methodology is higher than separate designs for secure test [14], and IP core protection [23], done separately. However, the power overhead is comparatively low when a combined secure test and IP core protection is taken into account. This outcome is primarily due to the common key integrated security hardware in a unified design methodology in STEP (Section V). Note that power consumptions incurred during secure tests are not compared in detail because the test power overhead is typically negligible as the number of original flip-flops is very high compared to the number of inserted dummy flip-flops. For example, if 128 dummy flip-flops are inserted into 2000 original scan flip-flops for storing the 128-bit dynamically generated key, the test power overheads ranges between 0.5% to 1%.

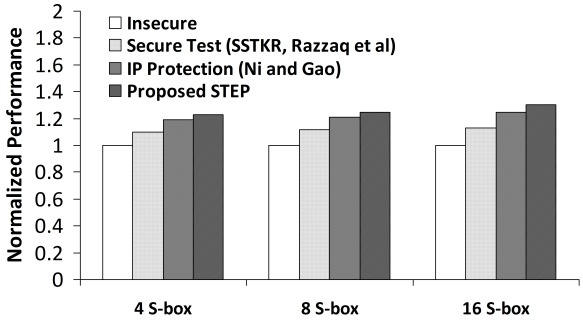
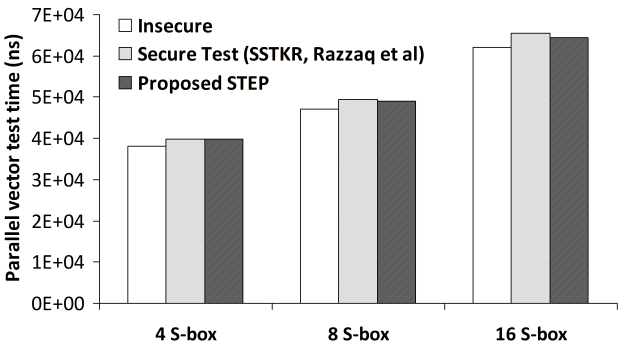


Fig. 7: Performance comparisons between secure AES systems using the proposed unified design methodology, the STEP (Fig. 1), and the insecure AES systems.

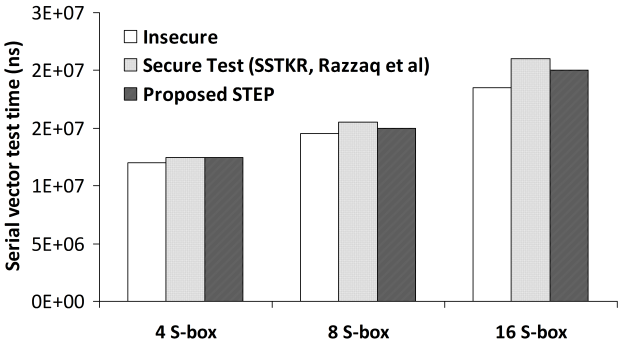
Fig. 7 shows the comparative normalized performances of three secure AES systems designed with the proposed STEP methodology (Section III), secure test only, IP core protection only, and insecure design using the traditional design methodology (Phase I, Fig. 1). The performances were evaluated as execution times for a given set of AES datasets in the Synopsys Design Compiler™environment, and were normalized with respect to the execution times of the insecure design. As expected, with additional security measures, the performance overhead increases. This result happens because, with security measures, the number of AES iterations increase both for secure design alone, and also for the IP core protection alone. Note that the design with IP core protection has more performance overhead than does the design with secure test alone, as the key integrated during runtime incurs higher computations per AES step. The STEP design methodology generates AES designs that incur similar performance overhead as does IP core protection alone [23], but show higher performance overhead than does secure test alone [14], as expected.

C. Test Time and Fault Coverage Analysis

Because the secure test and the IP core protection architectures generated by the proposed STEP design methodology integrate extra hardware (Section V), it is important that the test capabilities are compared between the secure and insecure AES systems. To this end, Fig. 8(a) and (b) show the comparative test times taken by different AES designs using the parallel and serial test vectors in the Synopsys TetraMax™simulation environment. For comparisons, the design with the secure test mechanism proposed by Razzaq *et al.* [14], and the design with no security enabled (using Phase I, Fig. 1), have been implemented for the test environment. From these figures, the following observations can be made. First, as expected, it can be seen that the test times are considerably lower for parallel vectors (Fig. 8(a)) compared to the serial vectors (Fig. 8(b)). This outcome is expected as parallel test vectors significantly



(a)



(b)

Fig. 8: Comparative test times (in ns) for (a) parallel vectors, and (b) serial vectors using secure design methodology (Section III), and insecure design methodology.

reduce the time required for the scan chain data to be loaded and shifted. Secondly, the secure AES design generated using the proposed unified STEP design methodology takes more test time for both parallel and serial test vectors. This outcome happens because secure AES designs use fixed (in testing mode) and variable (in functional mode) key based hardware to incorporate secure test and IP core protection (Section V). The key generation, loading, and checking mechanisms within this integrated security hardware require extra test time (i.e. up to 4% extra delay for the 4 S-box secure AES system) compared to the original test times in the insecure AES systems. When compared with the design with secure tests [14], it can be seen that the proposed STEP design takes up to 2% less time during the test as security checking only takes place during shifting out of multiplexor data in the STEP design as opposed to both during shifting in, and shifting out in [14].

To compare the test capabilities between secure and insecure AES systems, Fig. 9 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 test benches in the Synopsys Tetra Max^{TM}tool.

As can be seen, both secure designs of the AES system (the STEP design, and the design with secure test [14]) use up to 4% more test patterns for achieving similar test coverage as that of the test in the insecure AES system. This outcome is expected as the extra key integrated security hardware used

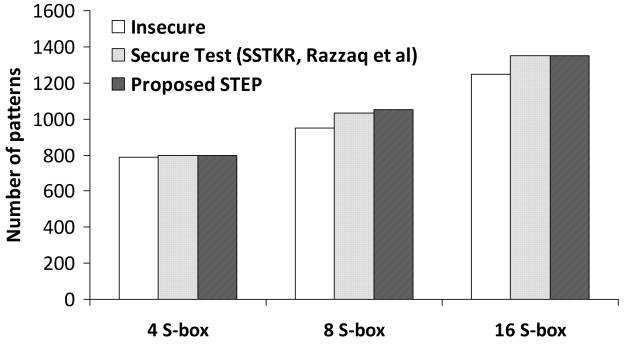


Fig. 9: Comparative number of test patterns for similar test coverage between secure AES designs and insecure AES designs.

in the secure test architecture in the STEP (Section V-A), and also in the secure design in [14], requires more scan chains, and hence more test patterns, to achieve similar fault coverage. Note that, due to the similar secure test approach in the STEP design, and the secure test design [14], a similar number of test patterns are required.

TABLE I: The total number of faults injected, and the corresponding fault coverage and the number of test patterns tested in different secure AES systems, generated using the proposed STEP design methodology (Section III)

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 I shows the number of inserted faults, the 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 the number of faults injected; columns 3, and 4 show the corresponding fault coverage, and the number of test patterns used. As can be seen, with increased design complexity, a higher number of faults need to be investigated and tested due to the increased number of iterations, and the area of the AES (Section VI-A). Despite such a high number of faults, up to 99% of these can be effectively detected using the secure test architecture (Section V-A). However, this fault coverage is achieved using various numbers of test patterns (column 5, Table I). As expected, as the design complexity increases, the number of test patterns used also increases. For example, from the 8 S-box secure AES design to the 16 S-box secure AES design, the number of test patterns increase by about 29%.

D. Security Analysis

The proposed STEP design methodology gives a high security advantage at the cost area, power, and test overhead (Sections VI-A, VI-B, and VI-C). To understand the effective security advantage in the system, in the following, hacking scenarios of the secure test and IP core protection are briefly

explained. Later, a case study of the authorized and unauthorized access using the secure AES design generated through the STEP design methodology is detailed.

1) Test Security Analysis: To successfully hack into the secure test architecture through a side-channel attack (Fig. 2(a)), a hacker must extract the following information (Section V-A).

- The size of the random key, N.
- The positions of N dummy flip-flops within S total flip-flops within the scan chain.
- The seed used in the PRBS key generator, R.

Assuming that the hacker stores his guessed random key and the PRBS seed in an M bit number, and that $M \geq N$, the numbers of combinations the hacker has to try for guessing N (C_N), and R (C_R) correctly are given as

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

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

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

Because 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 the 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.

2) IP Core Protection Analysis: For a successful attack in the IP core architecture through iterative sequential analyses and reverse engineering (Fig. 2(b)), a hacker must extract the following information (Section V-B).

- The sequence of k variable keys.
- The protocol to shift in the key, i.e. a given interconnection of N connections out of S scan chain flip-flops.
- The seed used for the PRBS key generator, $\mathcal{R}$.

Considering k keys in the sequence, the number of combinations the hacker has 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 scan chains of length S each, the hacker will have to try C_{guess}^{ff-con} combinations, given by

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

Because 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 protection 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), the STEP design methodology provides a high security advantage over insecure design methodologies, requiring the hacker to generate a large number of combinations to extract the design information. Fig. 10 shows the number of combinations required during test and IP functionality to hack into security in the STEP design methodology (obtained through (3, and (6))). As can be seen,

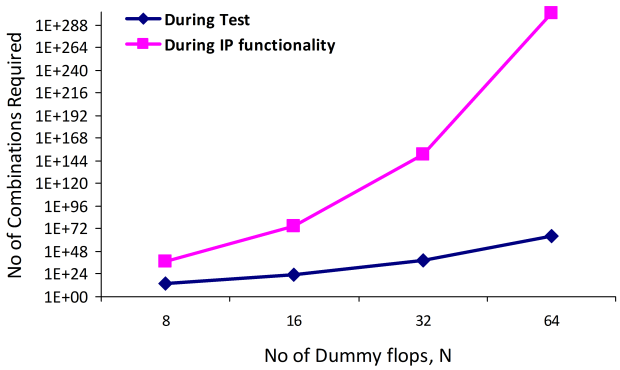


Fig. 10: The number of combinations required during testing, and also during IP functionality, to hack into the STEP design security with a varied number of dummy flip-flops.

with an increased number of dummy flip-flops (incorporated through automatic insertion demonstrated in Algorithm 1), the number of combinations required increases exponentially. As an example demonstration, considering N=32, G=8, S=128, and k=4 for an 8 S-box AES system (in reality S is much larger, eg. for an AES system it is 2000+), a total of $C_{test} = 2.7 \times 10^{38}$, and $C_{IP} = 8.2 \times 10^{150}$ combinations would be required for breaking into the secure test, and the IP core protection, respectively. This condition 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 a higher number of dummy flip-flops (i.e. higher N), which will impose higher system costs in terms of area, power, and test times or accuracy (see Sections VI-A, VI-B, and VI-C).

3) Other Security Concerns: The proposed design methodology makes the design hacking equally challenging, even for a legitimate user. A legitimate user will be given an approved key for the PRBS, which will reveal the size of the key, N. This key will be used to give him authorized access to the design, both during secure testing, and also during IP core functionality, through the key integrated secure hardware (see Section V). However, to hack into the design information, the user will require the positions of N dummy flip-flops within S total flip-flops in the scan chain, and the seed used in the PRBS key generator R during secure test. Moreover, the user will require the sequence of k variable keys generated through key shifting, the shifting protocol, and the PRBS seed R for design hacking during IP core functionality. Using (3), and (6), the numbers of combinations a legitimate user will need to

reveal design information are given by

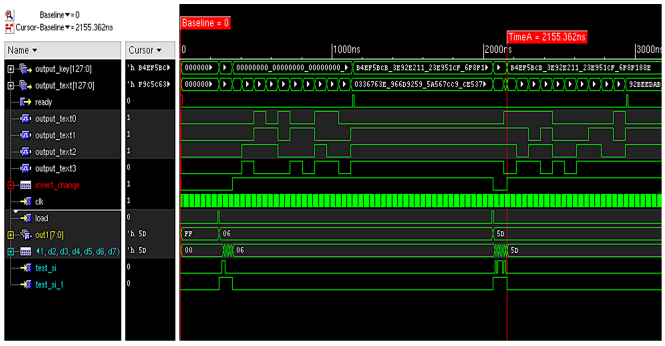
$$C_{test} = 2^{2N}\ G \binom{S}{N} \quad , \ and \tag{7}$$

$$C_{IP} = 2^{N(k+1)}\ G\ N! \binom{S}{N} \quad . \tag{8}$$

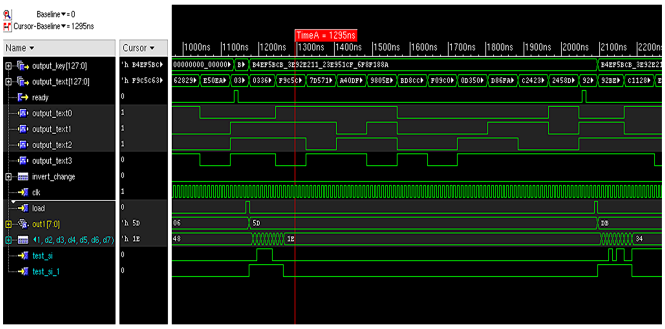
As can be seen, even for a legitimate user, the numbers of combinations are challenging.

The proposed methodology also provides effective protection against any side channel attack using the test access ports. These ports are usually laid out as standard chip interfaces, to be used during post-manufacturing tests. However, security can still be partly compromised through scan probing attacks. Scan probing attacks require the hacker to dissect the chip, bypassing the final mux, which is an extremely cumbersome process. Moreover, even if the hacker was successful with such probing, he would still have to identify the locations of the random placement of the dummy flip-flops, and the key used to protect the information during the secure test (Fig. 3).

4) Case Study: Secure and Insecure Access: Fig. 11 shows a simulation waveform of the 4 S-box AES system with a 128-bit key, highlighting the re-seeding during authorized and unauthorized access. The Cadence Incisive Enterprise Simulator (IES) has been used to design and validate the AES system design using the STEP design methodology, and obtain the simulation waveform for functional verification. As can



(a) Authorized access.



(b) Unauthorized access.

Fig. 11: Case study of authorized and unauthorized access with re-seeding during IP core functionality.

be seen, the $test\_si$ signal is used to drive the key into the AES scan chains; registers $d1$, $d2$, $d3$, $d4$, $d5$, $d6$, and $d7$ form the shift register in the key chain. The outputs from all registers are concatenated, and shown in the waveforms (the third last signal in both figures). The *out1* signal shows the variable key generated internally for the PRBS, the *load* signal indicates the start of a new iteration, and on every new load a new key is generated. During authorized access, this key is always matched by the newly generated key through shifting (Section V-B). When the key is matched during authorized access, it triggers the assertion through the *invert_change* signal. During such access, the output signals *text0*, *text1*, *text2*, and *text3* are enabled through the multiplexer, and the encryption takes place in usual order (Fig. 11(a)). However, when there is a mismatch during unauthorized access, the key is mismatched, and these outputs are driven randomly as the output of the PRBS sequence is enabled through the multiplexer (Fig. 11(b)). From the figures, it can also be seen that, during every *ready* signal, the PRBS generator is re-seeded using the currently generated key (Section V-B). The re-seeding process ensures a very high security in the proposed STEP design methodology. Note that, when the AES key is changed, the AES output (*output_text*) also changes depending on the individual scan chain outputs.

VII. Conclusions

A novel design methodology for secure test and IP core protection was proposed. It was shown that the proposed unified design methodology STEP achieves security and protection during test and IP core functionality through a unified key integrated security hardware (Sections III and V). The addition of such unified hardware was facilitated through an automated flip-flop insertion, which can be easily incorporated within an EDA tool chain. To evaluate the effectiveness of the proposed design methodology, different AES systems were designed and compared with the other secure and insecure systems as case studies. The comparisons showed that our methodology offers significantly high security, requiring a high order of magnitude of combinations for the hacker to break into the security and protection. We demonstrated that the secure test and IP core protection advantages are achieved at the cost of low area, power, and test overhead (Section VI).

References

[1] R.-han Kim, S. Homes, S. Halle, V. Dai, J. Meiring, A. Dave, M.E. Colburn, H.J. Levinson, "22 nm technology node active layer patterning for planar transistor devices," in *Proc. of XXII SPIE Optical Microlithography*, L. H. J. and M. V. Dusa, Eds., vol. 7274, 2009, pp. 72742X-1–72742X-6.

[2] S. R. Shenoy and A. Daniel, "Intel architecture and silicon cadence the catalyst for industry innovation," Intel Corp., Tech. Rep., April 17 2009.

[3] 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.), USA.

[4] 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. 37-51, 1997.

[5] L. Bossuet and D. Hely. "SALWARE: Salutary Hardware to design Trusted IC," in *Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, TRUDEVICE*, Avignon, France, 2013.

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

[7] A. Waksman, S. Sethumadhavan, and J. Eum. "Practical, Lightweight Secure Inclusion of Third-Party Intellectual Property," IEEE Design & Test, vol.30, no.2, pp.8-16, April 2013.

[8] P. C.Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," in *Lecture Notes in Computer Science: Proceedings of Crypto'99*, Springer-Verlag, pp. 388-397, 1999.

[9] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. of the 16th Annual Intl. Cryptology Conference on Advances in Cryptology*, pp.104-113, UK, 1996.

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

[11] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. of Computer Aided Design of Integrated Circuits and Systems (TCAD)*, vol. 20, no. 10, pp. 1236–1252, Oct. 2001.

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

[13] S. Skorobogatov *et al.*, "Breakthrough silicon scanning discovers backdoor in military chip," to appear in Proc. of *Intl. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Sept. 2012.

[14] 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.

[15] F. Bancel and D. Hely. "Method for testing an electronic circuit comprising a test mode secured by the use of a signature, and associated electronic circuit." U.S. Patent No. 7,577,886. 18 Aug. 2009.

[16] 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, ASPDAC*, pp.810–816, 23-26 Jan. 2007.

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

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

[19] 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.

[20] Jarrod A. Roy, Farinaz Koushanfar and Igor L. Marko, "EPIC: Ending Piracy of Integrated Circuits," in *Proc. of Intl. Conference on Design, Automation and Test in Europe (DATE)*, 2008.

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

[22] 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.

[23] M. Ni and Z. Gao, "Detector-based watermarking technique for soft IP core protection in high synthesis design level," in Proc. of Intl. Conference on Communications, Circuits and Systems, pp. 1348-1352, 2005.

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

[25] 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 (ASPDAC)*, 2010.

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

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

Rishad A. Shafik is a senior research fellow in the School of Electronics and Computer Science (ECS), University of Southampton, UK. Before joining this group, he worked as a post-doctoral research fellow in the University of Bristol, UK from 2011 to 2013. Prior to that, he also worked in the Islamic University of Technology (IUT, a subsidiary organ of the OIC) as an assistant professor from 2002 to 2006. Dr. Rishad received his Ph.D., and M.Sc. (with distinction) degrees from the University of Southampton in 2010, and 2005; and the B.Sc. in Electronic Engineering degree (with distinction) from the IUT, Bangladesh in 2001. He is one of the editors of the book "Energy-efficient Fault-tolerant Systems," published by Springer USA, and author of 65+ IEEE and ACM journal and conference research articles. He is generally interested in the energy-efficiency, reliability and security aspects of embedded computing systems.

Jimson Mathew is currently a research associate in the Department of Computer Science at the University of Bristol, UK. Prior to joining the University of Bristol, he held research positions in the Centre for Wireless Communications, National University of Singapore, Bell Laboratories Research (Lucent Technologies) North Ryde, Australia, and Royal Institute of Technology (KTH), Stockholm, Sweden. Since 2005, he has been with the Department of Computer Science, University of Bristol, UK. His research interest primarily focuses on low power design and testing, Sigma Delta Converters, Fault-tolerant Computing, and Galois field based arithmetic. Dr. Jimson has published 100+ research papers in reputed IEEE and ACM journals and conferences, and has edited or authored two books, published by Springer USA.

Dhiraj K. Pradhan currently holds a Chair in Computer Science at the University of Bristol (U.K.). Recently, he had been Professor of Electrical and Computer Engineering at Oregon State University, Corvallis. Previous to this, Dr. Pradhan had held the COE Endowed Chair Professorship in Computer Science at Texas A & M University, College Station, also serving as founder of the Laboratory of Computer Systems there. Prior to this, Professor Pradhan held a Professorship at the University of Massachusetts, Amherst, where he also served as Coordinator of Computer Engineering. Dr. Pradhan has also worked at IBM; University of California, Berkeley; Oakland University (Michigan); the University of Regina, in Saskatchewan, Canada; and as Visiting Professor at Stanford University (Calif.). Professor Pradhan is author and editor of numerous books on fault-tolerant, energy-efficient, and secure computing. A Fellow of ACM, IEEE, and Japan Society of Promotion of Science, Professor Pradhan is also the recipient of a Humboldt Prize, Germany. In 1997, Dr. Pradhan was also awarded the Fulbright-Flad Chair in Computer Science.