Defence Science Journal, Vol. 73, No. 6, November 2023, pp. 728-737, DOI : 10.14429/dsj.73.6.18879

Design of a Scan Chain for Side Channel Attacks on AES Cryptosystem for Improved Security

G. Sowmiya and S. Malarvizhi*

Department of Electronics and Communication Engineering, SRM IST, Kattankulathur, Chennai - 603203, India
**E-mail: malarvig@srmist.edu.in*

ABSTRACT

Scan chain-based attacks are side-channel attacks focusing on one of the most significant features of hardware test circuitry. A technique called Design for Testability (DfT) involves integrating certain testability components into a hardware design. However, this creates a side channel for cryptanalysis, providing crypto devices vulnerable to scan-based attacks. Advanced Encryption Standard (AES) has been proven as the most powerful and secure symmetric encryption algorithm announced by USA Government and it outperforms all other existing cryptographic algorithms. Furthermore, the on-chip implementation of private key algorithms like AES has faced scan-based side-channel attacks. With the aim of protecting the data for secure communication, a new hybrid pipelined AES algorithm with enhanced security features is implemented. This paper proposes testing an AES core with unpredictable response compaction and bit level-masking throughout the scan chain process. A bit-level scan flipflop focused on masking as a scan protection solution for secure testing. The experimental results show that the best security is provided by the randomized addition of masked scan flipflop through the scan chain and also provides minimal design difficulty and power expansion overhead with some negligible delay measures. Thus, the proposed technique outperforms the state-of-the-art LUT-based S-box and the composite sub-byte transformation model regarding throughput rate 2 times and 15 times respectively. And security measured in the avalanche effect for the sub-pipelined model has been increased up to 95 per cent with reduced computational complexity. Also, the proposed sub-pipelined S-box utilizing a composite field arithmetic scheme achieves 7 per cent area effectiveness and 2.5 times the hardware complexity compared to the LUT-based model.

Keywords: Advanced Encryption Standard (AES); Scan chain; Side channel attack; S-box; Scan Flip-Flop (SFF); Bit masking; Logic BIST (Built-in Self Test)

NOMENCLATURE

BIST	Built-in Self-Test
SFF	Scan Flip-Flop
MFF	Masked Flip-Flop
LUT	Look-Up Table
RNG	Random Number Generator
DfT	Design for Testability
TPG	Test Pattern Generator
ORA	Output Response Analyzer
SI	Scan In
SO	Scan Out
SE	Scan Enable
CUT	Circuit Under Test
LFSR	Linear Feedback Shift Register
AES	Advanced Encryption Standard
AE	Avalanche Effect
SPA	Simple Power Analysis Attack
DPA	Differential Power Analysis Attack
SAC	Strict Avalanche Criterion
FPGA	Field Programmable Gate Array
BER	Bit Error Rate
GF	Galois Field

Received : 16 February 2023, Revised : 20 June 2023
Accepted : 23 June 2023, Online published : 03 November 2023

1. INTRODUCTION

Increased advancements in electronic Integrated Circuit (IC) technology have resulted in billions of transistors per square inch of silicon. When such a complex design is tested for its functionality, the testing process becomes laborious and expensive. In particular, for IC circuits in high-speed applications, the conventional testing process becomes ineffective and requires sophisticated test equipment. The concept of "Built-in Self Test" (BIST) is the hardware or software to test the functionality of the circuit built inside the chip[1-2]. Hardware-based crypto-chip designs are more popular and have evolved a lot. Advanced Encryption Standard (AES) is the most frequently deployed method of security, and it finds use in many applications, namely communication, IoT, blockchain, etc. Hardware-based crypto chips (AES) are also attempted by VLSI design. For authenticated key production and memory staging, the hardware design of AES in[3-4] employs a Look-Up Table (LUT) and unique key-based countermeasures[5]. describes a LUT-based AES design that reduces computation time for a key generation while using less power. AES encryption algorithms need to be more consistent with high-end applications due to their highly complicated key generation process as well as susceptibility to side-channel attacks, resulting in poor performance and substantial

complexity overhead. The complex AES chip testability can be addressed using the mixed-mode BIST technique[6-7].

Side channel is one of the most prevalent attacks on crypto chip and it captures the physical effect while the chip is in function, making it easy to detect the information from it. A literature review[8] identifies the design aspect of AES crypto engines and provides a semiconductor mask for AES,[9] while identifying the design aspect of high-performance cryptographically secure processors. Pseudo-random number generators are created for high-performance Random Number Generator (RNG). Existing standards were used to create requirements for accelerator design, and a new digital technology accelerator for random numbers was created[10] to design an effective anomaly-based semi-supervised model to detect encryption at runtime. Testing is an additional critical feature for the security chip, since an undetected defect during the testing procedure may prompt an exploitable security blemish. Testing a high-speed crypto chip design for its function while protecting it from attacks is necessary. Therefore, if any appropriate consideration is taken to upgrade the testability, this will decrease the security[11-12].

One feasible and low-cost method of testing such a crypto chip is to include a unique piece of hardware to test its functionality and provide security. Such design for testability is referred to as Design for Testability (DfT)[13]. It is seen in the literature that most of the crypto chip design employs a scan to test for its functionality, which is otherwise known as "fault coverage." The scan test method provides high fault coverage[14-15]. In this method, while the chip runs in functional mode (logic is connected to the externally visible pins), it does not support mode-switching requests[16], which are nothing more than switching from test mode to functional mode. There is a possibility of retrieving the secret key in an existing scan attack in functional mode as well as in testing mode. When switching between modes, use the reset option to stop retrieving the secret key. The work[17] investigated the strength of a differential-based side channel to recover a secret key. The scan-oriented attack utilises the scan-based architecture as a doorway to permit attackers to decrypt a cryptographic core. The scan chain also promotes chip testing, allowing the test engineers to access the circuit design's internal state, leading to an attack on the cryptographic chip. In order to avoid this, a public partial scan design is implemented to provide both testability and security. A modified scan structure for a secure and scalable technique for all types of attacks were introduced[18-19].

Similarly, many researchers employed DfT techniques in the chip testing domain and were among its implementation. Scan chain-based techniques are the most popular. BIST also employs a scan chain-based design, as it is the simplest way to set every flip-flop and observe every flip-flop in the crypto chip. The literature[20] found that most crypto chip designs employ scan-based testing for cryptographic functionality. Test patterns are the unique input combinations that test the design for its functional verification. These test vectors should have good observability and controllability. Controllability refers to the ability to set a particular value at each node in a circuit by setting a value at the circuit input and observability is being able to detect the circuit's status at any time while undergoing testing. From the security point of view, an intruder can shuffle these test vectors, thereby altering the observability and controllability of the design. There have been few works published on hardware crypto core design methods, and the DfT method[21] exists, which offers reduced test cost and IC functionality.

This study relates the DfT scan design approach used for AES crypto-core design while testing in BIST. When it comes to crypto cores, the BIST can act as a loophole for attacks, so in order to overcome this, a scan chain design with enabled bit-level masking is proposed. An important measure for assessing the strength of the hard-core cryptographic design is the Avalanche Effect (AE). A good algorithm is one with a high AE value. AES is referred to as a property of an algorithm that allows a slight input change (for example, flipping a bit) to result in a significant change in output (more than half of the bit flip). In order to use the positive features of classical cryptography, like bit scrambling, which is combined with a modern cryptographic algorithm that uses keys[22], and to predict the level of encryption, the best S-box size can be predicted using the Avalanche Effect[23]. To improve the throughput of the AES encryption algorithm, a pipelining method is incorporated by dividing the blocks of the circuit[24-25].

A literature review suggests that two domains, security, and testing, can be integrated into the design. As a result, the effort is coordinated to bring novelty to the testing and a hardware resist design to reflect a security enhancement against hardware attacks, with simulation testing the circuit's functionality for its targeted functions. The salient contribution of this work is:

- S-box design ie., a byte substitution block in the AES method, and additional security is provided in the testing phase of the circuit.
- A simple scan architecture with randomized mask test pattern generation enhances the performance of the S-box architectural design for better acceleration and throughput.

The paper is organised as follows: Section 2 gives a brief theory of AES and BIST architecture design. Section 3 provides detailed information about the proposed scan-based testing methods and section 4 and 5 provides S-box implementation methods and AES security enhancements schemes. Experimental results and discussions in section 6 and section 7 conclude the work.

2. PRELIMINARY DETAILS

This section provides a brief review of the AES and structure testing methods. AES is the most likely and extensively used symmetric encryption method. It is a block cipher and encrypts the data in blocks of 128 bits with each key size of 128/192 or 256 bits as input called "plain text" and outputs 128 bits as encrypted data called "cipher text." AES's main operation is based on substitution and permutation, which means that output data is obtained through a series of linked operations of replacing and shuffling input data. The number of iterations/rounds required depends on the input length; for example, 128 bits require 10 rounds, 192 bits require 12 rounds, and 256 bits require 14 rounds to convert a plain text to

cipher text. Each cycle involves a number of processing stages, one of which is based on the encryption key itself. The sub-byte substitution is considered a prime part of the algorithm, where an enhancement in security is provided by our proposal, as indicated in Fig. 1.

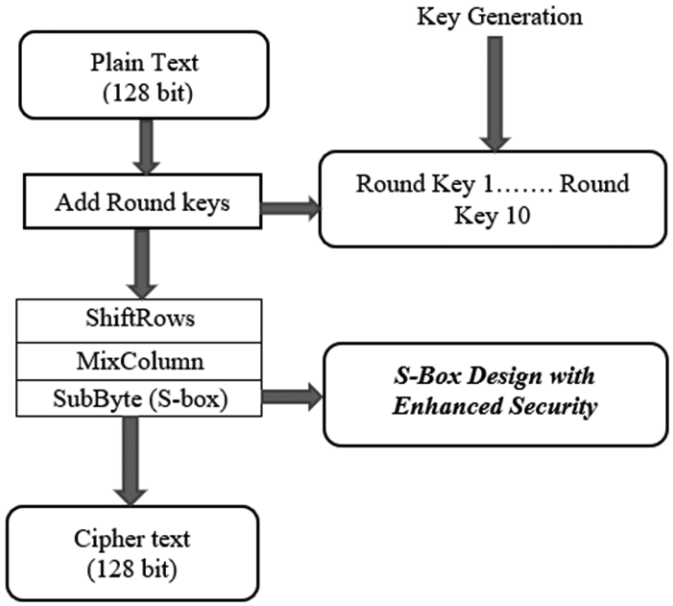

Figure 1: Proposal for enhanced S-box security.

testing, there is a possibility of a hardware attack. In IC testing, Built-in self test is an additional logic design that periodically tests the operation of the crypto chip. There are two types of BIST methods, one is based on memory and known as MBIST, which generates patterns in the memory and reads them to log any defects. The second one is Logic BIST (LBIST), which is based on the generation of pseudo-random patterns that are applied to the internal scan chains. Scan chain represents a Flip Flop (FF) arrangement known as Scan FF (SFF). Testing of an IC is done in an easier way by providing a test pattern that sets the FF in the scan chain and observes its output for functional verification. Three components make up the basic BIST architecture. Figure 2(a) depicts the on-chip BIST architecture, which has a (i) BIST (Built-in Self Test) controller (ii) Test Pattern Generator (TPG) and (iii) Output Response Analyser (ORA).

The test pattern generator generates the patterns required to check the faults in the Circuit Under Test (CUT) and propagate the results to ORA. The standard Linear Feedback Shift Register (LFSR) generates the pseudo-random patterns, which are test vectors. A Scan Flip Flop (SFF) is the fundamental component of the scan chain and the structure of the SFF is shown in Fig. 2(b).

A 2x1 multiplexer is added to the input of a D flip-flop to create a scan flip-flop. When SE equals zero, one of the MUX's inputs acts as the functional input D; when SE is equal to one, it

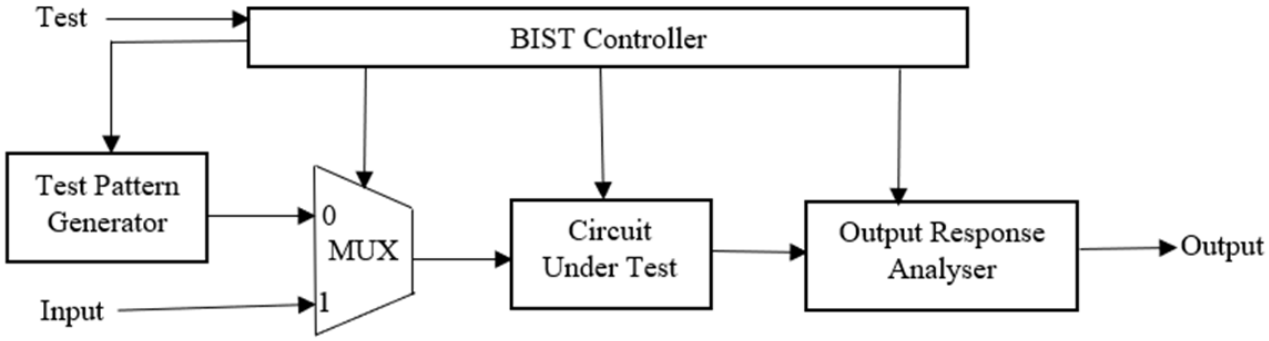

Figure 2(a). On-chip BIST architecture.

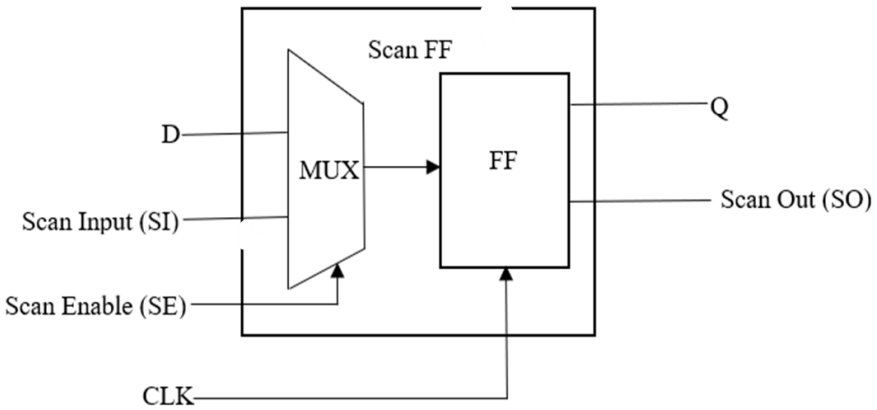

Figure 2(b). Single scan flip flop.

AES when implemented in hardware as a crypto chip, is vulnerable to attacks. During manufacturing, the crypto chip IC has to be tested for its correctness and functionality. During

serves as the Scan-In (SI) input. The MUX can be controlled by a selection bit named Scan Enable (SE). The Scan Enable (SE) decides whether D input or scan input from the Test Pattern

Generator (TPG) reaches the output of FF at the active clock edge. A scan chain was created by connecting the scan SFFs. The design, or CUT, is active while the SE signal is active; the scan chain functions as a shift register. The first FF serves as the link for the scan input, while the last SFF serves as the link for the scan output. There are three steps to how a CUT operates normally and during the testing phase is given as:

- Scan In(SI): To load the test pattern and the design in test timing mode
- Capture: The response of the CUT for the loaded test pattern will be captured as its response to the design is kept in timing mode.
- Scan Out(SO): The response captured is unloaded, and the design is returned to test timing mode.

As a result, all combinational logic in the FF is skipped when SI is fed into the SFF. The scan chain serves as the shift register since the test pattern flows from SI to SO and vice versa for the next FF. Test patterns are serially entered starting from the SI of the first FF in the scan chain, shifting to the next FF at the active clock edge. (n-1) clock cycles are required, where n is the total number of FF scans in the scan chain.

3. DESIGN PROPOSAL FOR IMPROVED SECURITY AND TESTING OF S-BOX

From Section 2, it is inferred that there is a hardware implementation of the S-box; during testing, the attackers can tap the secret information by targeting the scan out of the scan chain design. The proposal targets a simple scan chain design approach, of AES S-box system design imparting additional security and its performances are measured.

3.1 Substitution Bytes Transformation Model

The pre-calculated values create designs for LUT-based sub-byte conversion and its inverse. It maintains the values in a ROM-based lookup table, making it one of the most popular S-boxes for Sub byte operations. The 256 data are pre-calculated and stored in specific memory components within the Look Up Table-based S-box architecture, conveniently accessible across the address bus. This memory element-based method, however, has a large route delay overhead since read operations require time to reach. The cost of developing an S-box using memory elements is substantial, and it also uses much power. The limitations of LUT-based S-box

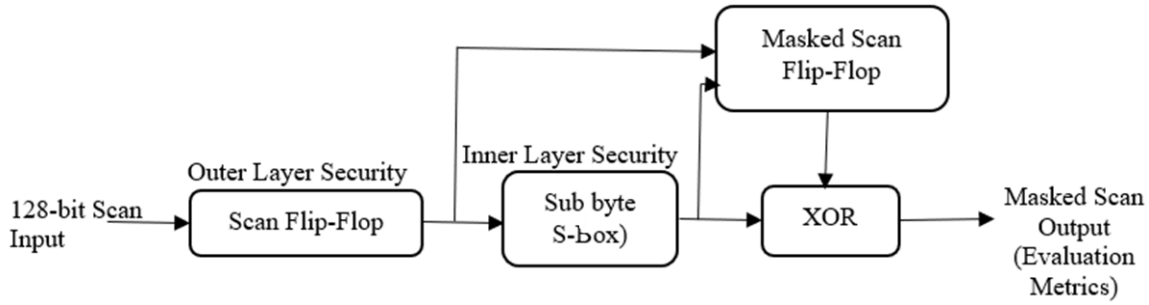

Figure 3. Proposed scan chain design for additional security.

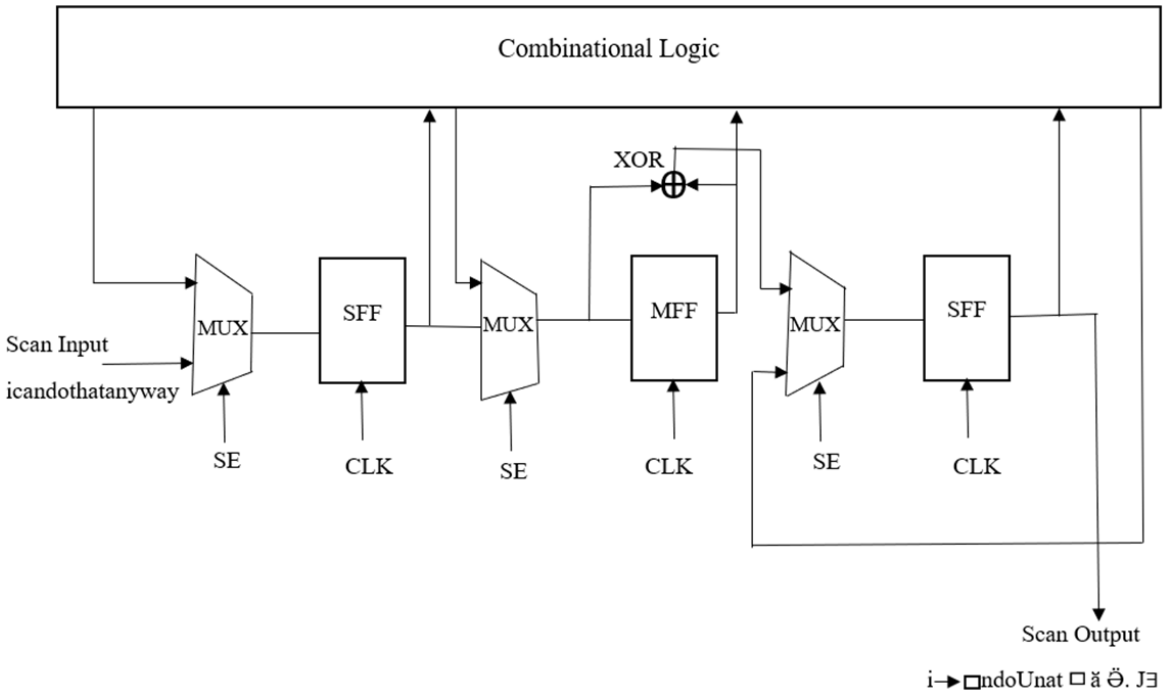

Figure 4. Architecture of proposed scan chain design.

implementations can be solved with combinational logic, considerably reducing complexity. To increase the operating frequency, a dynamic composite field-based strategy can also be pipelined. By computing the multiplicative inverse in the Galois field (2^8) and then executing an affine transformation, the S-box transformation is generated.

3.2 Methodology to Design a Scan Chain Cell

Conventional scan flip flips become a significant security risk once cryptographic digital systems are constructed utilising the BIST. Hence, the flip flops in the design are to be modified as SFF (Scan Flip Flop) in order to be put into a scan chain. AES is formed once BIST is triggered utilizing SFFs. To improve the secured scan FF design, in contrast to the SFF converter, comprises two operations: a bit inverter as well as an XOR gate. Bit masking is also done randomly, with no consideration for the AES core design. The scan input enters the scan flipflop for the outer layer, masking is done for all the 128 bits then only 100 per cent transformation of bits can be achieved for inner layer masking even if one-bit change can achieve maximum transformation at the output. Once the input enters the MFF (Masked Flip Flop) the bits are XOR-ed i.e., the bits are masked and then the masked bits enter the consecutive flipflop and finally, the scan out delivers the ciphered and masked output which is shown in Fig. 3. In order to enhance the security, the existing method used outer layer masking of the scan chain to achieve the bits transformation. However, the proposed method uses inner layer masking to achieve more transformation of bits to enhance security with reduced device utilisation and complexity. The evaluation metrics for the cipher output using the parameter avalanche effect, the number of bits transformed at the output after masking is calculated.

As mentioned, hardware crypto chips are prone to hardware attacks during testing. By noticing power dissipation for a period of time, it is possible to hack the information, which can be called a "power analysis attack." Therefore, the Circuit Under Test (CUT) is based on an estimate of power dissipation, so it is possible to get the information, i.e., the byte that is substituted for the 16-bit input, during testing. Figure 4 depicts the proposed scan chain design's detailed architectural view.

This proposed scan cell design modification provides test pattern randomization in the scan cell. In this case, the input text (icandothatanyway) is decomposed into 128-bit macroblocks as windowing lengths, and all four different AES transformations are applied in different orders to generate the final end-cipher text (i → ndoUnat □ ă Ӧ. J□).

Algorithm: Modified scan operation for data propagation to avoid scan-based attacks

Input – input text – T (message block with windowing length – 128 bit)
Output – cipher text

Step 1: Set AES transformation level, cipher key (K) and scan cell insertion//Initialization value
Step 2: Isolate scan FF inside S box transformation and replaced with secured mask FF
Step 3: Compute cipher key generation
CK={*sbox* (*K*[1]), *sbox* (*K*[2]), *sbox* (*K*[3]), *sbox* (*K*[4])}
Step 4: Divide input text into non-overlapping windows as follows:

```
for i=1: round
 for j=1:4
  E_s (j) = (T(j)<<j);                  // Shift rows
   E_mc (j)= Mix_Column (E_s (j)); //mix column
 E_sb (j)= S-box (E_mc(j));             // sub byte transformation
 E_out (i)= E_sb (j)xor E_sb(j);        // key based transformation
 end
 end
 Set scan mode for scan FF
 Set boundary cells for boundary
 preservations
 Set cipher key preservations
```

Step 5: Apply the test pattern generation model.

The proposed BIST crypto model consists of the following processes: cipher computation, fault modeling, and cipher modification. To quantify and explore the hiding properties of input text while retaining security during the data transformation process. However, the data transformation level and other performance metrics of the proposed cryptosystem do not differ significantly with respect to their normal functional mode. The sequence of testing is as follows:

- Keep the mode in the test and let the latches accept the data from scan-in input.
- Shift in and out of the test data to validate the scan path.
- Apply the test patterns to the primary input.
- After sufficient propagation, switch the mode to functional mode and look at the primary output of the circuit.
- Repeat the steps until all inputs are applied.

The scan design technique is a systematic method for designing sequential circuits for testability. Controllability and observability can be improved by giving more access to logical nodes with extra primary input lines and multiplexers. However, adding extra input pins might increase the cost of packaging and chip manufacturing. Scan registers with both shift and parallel load capabilities are used in the proposed design. When using a scan-based design, multiplexers and a mode (test or normal) control signal connects the storage elements to create a serial shift register or scan path. In test mode, the scan-in signal is clocked into the scan route while the output of the final stage latch is scanned out. As illustrated in Fig. 5, the circuit functions sequentially and consistently with the scan-in path.

4. IMPLEMENTATION OF S-BOX

The implementation of the S-box has two approaches one is LUT based S-box and another one is a Composite Field S-box. The LUT Based S-box needs more area and makes unbreakable delays. So, the composite field is implemented only by combinational logic. The multiplicative inverse value is calculated using Composite Field Arithmetic in the Composite field S-box.

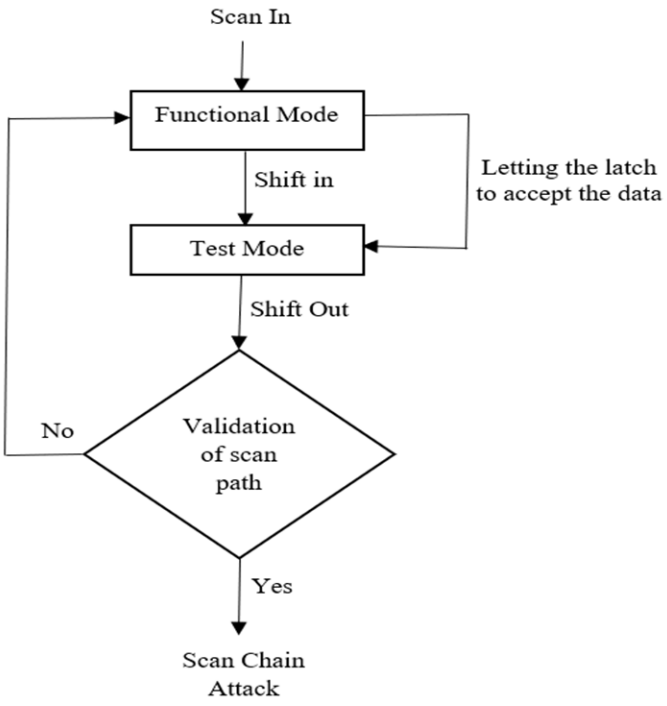

Figure 5. Process flow of scan chain for testability.

4.1 LUT-based S-box

The Look Up Table (LUT)-based realisation of the S-box needs a significant amount of ROM or EPROM memory. The values will be stored in memory, and to get the necessary value, rows and columns will be scanned. Bulk memory is needed for LUT-based S-box implementation, which is easy to do. Since LUT has a set access time, the LUT S-box has a fixed structure, resulting in an inevitable delay.

4.2 Composite Model S-box

A composite field approach that uses the affine transformation and two sub-module multiplicative inversions can be used to implement the S-box. Byte substitution begins by utilising isomorphic mapping to change the input into a composite field. The output of the isomorphic mapping is then applied to the multiplicative inverse of the Galois field, and the result is then remapped using an inverse isomorphic function and an affine transform. The costliest module is the multiplicative inverse, which has a number of hardware blocks significantly lower using GF (Galois field) arithmetic.

4.3 Sub-pipelined S-box

A composite field-based model can be pipelined to improve the operating frequency. Pipelining can be done by reducing the critical path. This has the advantage of increasing the throughput. The proposed method uses 6 stage pipelining to reduce the critical path. The performance comparisons among LUT, Composite and Sub-pipelined composite models will be discussed in Table 3.

5. SCAN-BASED ATTACKS AND SECURITY

A secure model for a system is to ensure a secure design by anticipating different types of risks and attempting to mitigate them. The security designer also adds layers of protection to isolate a danger before it impacts safe operations.

5.1 Cryptanalytic Interpolation Attacks

This work is mostly concerned with scan chain-based security. The use of scan tests, as mentioned earlier, allows the design for testability to convey all information about the chip successfully. It is difficult to uphold the level of controllability and observability so that the testability of the circuit strives to offer security, which is the purpose of chip design, because of the key leakages.

5.2 AES Square Attack

The AES square Attack obtains the encryption key to propagate groups from plain text to cipher. However, changing the real key regularly can raise the number of attempts required to pose key management issues. However, using the input biometric, we may create any number of key sequences, and the split keys can be used for each round operation. The attack needs 16 iterations to obtain a 128-bit key, and it could only probe the last byte of each key unit and change the actual key however, the square attack is also practically impossible.

5.3 Power Analysis Attack

There are two types of power analysis attacks exist (i) Simple Power Analysis Attacks (SPA) and (ii) Differential Power Analysis Attacks (DPA). SPA is a side-channel attack that involves examining the graph visually used by the devices. There will be variations in the power while the device performs different operations. DPA is also a side-channel attack that analyses the power consumption statistically and measures the power from the cryptosystem. Therefore, by varying the power consumption of the hardware during the operation using secret keys. Since masking is done at the initial stage, there will be differences in power during operation, so the proposed method is highly vulnerable to these kinds of attacks.

6. PERFORMANCE EVALUATION

The research presents a scan test approach that can alter the scan data in a simple and random manner while testing and analysing it based on discrimination capabilities. The randomised addition of revised scan FF through the scan chain provides the best security. Finally, the cryptographic model is generated using the QUARTUS II EDA tool design compiler and the CYCLONE III EP3C16F484C6 device.

6.1 Avalanche Effect

Avalanche Effect (AE) is a crucial parameter for evaluating the robustness of crypto algorithms, even a slight modification to the plain text input will have a significant impact on the result. Therefore, changing just 1 bit in the plain text can affect the property. In this situation, every updated result can be examined as at least a 50 per cent change of the bits in the output cipher text.

$$Avalanche\ Effect = \frac{No.\ of\ Bits\ Flipped\ in\ Cipher\ Text}{No.\ of\ Bits\ in\ Cipher\ Text}$$

Throughput: This parameter is used for checking the

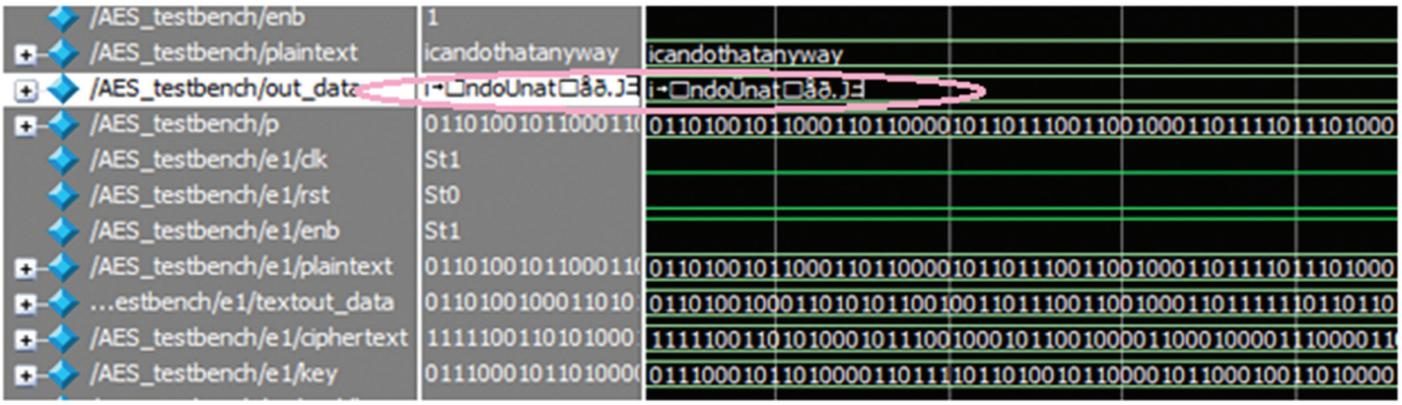

Figure 6. Outer layer masking bit transformation using proposed SFF.

Figure 7. One-bit inner layer masking selection transformation for proposed SFF.

algorithm's hardware implementation. Throughput, expressed in Gbps or Mbps, denotes the number of processed bits per unit of time. The formula to determine the throughput is given as follows:

$$Throughput = \frac{No.\ of\ Bits\ Processes \times Fmax}{Latency}$$

Figures 6 and 7 show that the proposed cipher transforms a 128-bit block plaintext and generates the same bit of cipher text using a 128-bit key retrieved from the scan input. The results show the outer layer masking which is the change in I/O layer or boundary scan (have to change many flip-flops). The inner layer masking shows that change in one flip-flop leads to maximum bit changes using the proposed SFF method. The encryption stage includes physical and key-based transformations, as well as several rounds of transformations permutation, cyclic shifts, bit-wise transformations, S-box and modulo computations and so on are only a few examples. The proposed cryptosystems security is assessed using criteria like key sensitivity, computation time and robustness against certain attacks.

6.2 Comparative Analysis of Proposed Scan Flip-Flop

Several FPGA implementations of AES cryptosystem bit masking techniques are also included in this part to demonstrate the performance measures of our AES cryptosystem. The suggested cryptosystem operation frequency and area overhead are significantly reduced. As a result, the cipher text should change with a probability of 50 per cent when one bit in the plaintext or key is supplemented and this phenomenon is known as the "Avalanche Effect" shown in Table 2. Additionally, the basic sequence used by each round can be altered to increase security.

Table 1 shows the performance of the outer layer and inner layer masking of the scan flip flop and its operating frequency. It is inferred that masking at the inner layer occupies less area with reduced frequency and also there is an increase in security. Since masking is done internally it is difficult to identify which flip-flop is masked. Based on the requirement, inner layer masking is preferred wherever there is a compromise in speed

Table 1. Analysis of proposed masked scan FF at outer and inner layers with FPGA hardware synthesis using CYCLONE-III EP3C16F484C6 device

Security methodology	Area			Max. frequency (MHz)
	Logic cell	Look up table	Logic registers	
Masking at the outer layer	5256	3384	1872	132.24
Masking one bit layer	5046	3188	1872	124.06

Table 2. Comparison table of a proposed scan AES with another state of art AES model

AES models	Block size of AES	Devices used	Avalanche effect (%)	Scan chain mode protection	Number of slices	Max. frequency (MHz)
S-box design based on LUT with improved Key Expansion (Zodpe, *et al.*, (2020))	128-bit	Xilinx-XC6VLX240T	52	No	4085	462.13
S-box Composite model with bit level masking- (Proposed model-ii)	128-bit	Xilinx-XC6VLX240T	93	Yes	5126	201.2

and outer layer is preferred wherever there is a compromise in area. Table 2 compares state-of-the-art methodologies of FPGA synthesis results for the architecture where the masking of bits is done at the inner layer of the scan flip-flop. Here the same block size of 128-bit is taken and the maximum bit transition is achieved ie., the avalanche effect achieved is a maximum of 93 per cent (for the composite model) which is approximately a 41 per cent increase in bit transition than the LUT-based method.

6.3 Performance Comparison

The Quartus II system, which offers complete support for all widely used techniques for describing the intended circuit into a CAD system, is utilized for the performance comparison. The user provides the required circuit in the Verilog hardware description language when using the Verilog design entry technique used in this lesson. Furthermore, by utilizing the prospective metrics of the dynamic computing side, the sub-pipelining model may be used to reduce memory and give path delay optimisation.

6.3.1 Hardware Complexity Report

Table 3 shows the experimental findings of the FPGA RTL synthesizer tool, which was designed to evaluate the hardware utilisation report. The proposed sub-pipelined S-box achieves 7 per cent area effectiveness compared to the composite model and 2.5 times the hardware complexity compared to the LUT-based model.

Table 3. Performance comparisons among LUT and sub-pipelined composite field sub-byte conversion models using CYCLONE-III EP3C16F484C6 device

Substitution box architecture	Area (Logical elements used)	LUT slices	Max. frequency MHz
Look-up table model	216	4085	1.21
Composite model	87	5126	1.2
Sub-pipelined model	80	4560	509.16

Compared to conventional architecture, the proposed optimized s-box model decreases the number of registers and logical blocks consumed. FPGA RTL synthesis findings have revealed that the effectiveness of LUT less optimised sub-byte conversion over standard sub-byte model is remarkable.

The suggested sub-byte model outperforms the conventional LUT in this graph. By examining the worst-case classpath during data propagation, the time-to-search timing analyzer tool was utilized to determine the highest frequency of the operation summary. The pipelined composite field s-box surpassed both the traditional direct LUT s-box and its composite model with a maximum running frequency of 509.16 MHz, according to the F_{max} values. GF composite field mathematical models also directly impact critical path delay due to their sequential operation.

6.4 Energy Efficiency Measures

The power report is created using the power analyzer tool, which examines both total power and dynamic power independently. Sub-pipelined optimal composite field computing, in contrast to the traditional LUT approach, uses less power.

The results show the comparison of dynamic power and total power. On comparison of dynamic power with composite model and sub-pipelined model the reduction is approximately 34 per cent and around 4 per cent reduction in total power consumption.

6.4.1 Signal Transition Reduction and Performance Analyses

Because of the large group of multiplication components and associated bit transitions, the computations in Galois Field (2^8) are exceedingly complex, resulting in greater signal transitions. Though some LUT models provide significant transition reduction, the issue occurs when it comes to signal transitions. Only a small number of transitions are used in each level of the composite fields in this framework, resulting in lower total transition rates, as given in Table 4.

Table 4. Comparison of transition control and power reduction using the CYCLONE- III EP3C16F484C6 device

Signal detector	Number of transitions (millions /sec)	Dynamic power dissipation (mW)	Total power consumption (mW)
Look-up table model	45.66	12.46	153.96
Composite model	45.90	9.45	151.37
Sub-pipelined S-box	47.48	7.02	147.90

As given in Table 5 it is well proved that the proposed crypto cores outperform other existing methods with superior improvements of 55 per cent to 95 per cent in avalanche effect when masking is done at the inner layer of the scan flip-flop. The avalanche effect in the Table 5 represents the sub-pipelined composite model for different iterations maximum range upto

Table 5. Avalanche effect and throughput comparison of different algorithms using the CYCLONE-III EP3C16F484C6 device

Algorithm	No. of bits	Throughput (Gbps)	Logic cells	LUT slices	Avalanche effect (%)	Pipelining
AES[4] Harshali Zodpe, Ashok Sapkal	128	3.45	5688	5688	52	Non-pipelined
Fast AES[5] Xin-qiang, L.U.O., *et al.*	128	30	3788	3788	51 to 63	6
Proposed algorithm (Sub-pipelined)	128	47.93	3178	4560	55 to 95	6

95 per cent since 6 stage pipelining is done over here. The proposed model outperformed other existing methods in terms of complexity, improved data rate and throughput. In order to reduce the overall computational delay and to increase the throughput pipelining was adopted and achieved 47.93 Gbps throughput than the existing method.

Table 6 is the level of information based on changes in data bit position. It is well proved that the sensitivity analysis carried out with the basis of one-bit change at the receiver side shows superior performance.

Table 6. Entropy value of different bit positions

Changes in data position bit (%)	Transformation level (%)	Entropy
5	99.8	0.2
10	99.75	0.4
25	99.8	0.45
50	99.8	0.34
75	99.8	0.39
100	99.8	0.40

7. CONCLUSIONS

Hardware encryption solutions are frequently used to protect data and to increase the throughput. In this paper, a technique to enhance the encryption quality of AES algorithm in scan-based testing to produce secure BIST is analyzed and a new hybrid pipelined AES algorithm with enhanced security features is proposed. A masked bit-level scan flipflop for a scan-protected solution is proposed for secure testing. Also, the work provides robustness to avoid information leakage about the physical implementation of cipher text from side-channel attacks. In order to increase the throughput a new hybrid pipelined AES algorithm with enhanced security feature is implemented. Thus, the proposed method outperforms with other methods in terms of improved data rate, Security and throughput. The avalanche effect for sub-pipelining method has been increased up to 95 per cent with reduced computational complexity. Also the proposed sub-pipelined S-box achieves 7 per cent area effectiveness compared to the composite model and 2.5 times the hardware complexity compared to the LUT-based model. Also, achieves a throughput of 47.93 Gbps when synthesized using the CYCLONE-III EP3C16F484C6 device.

REFERENCE

1. Menbari, A. & Jahanirad, H. A concurrent BIST architecture for combinational logic circuits. *In* 10th International Conference on Computer and Knowledge Engineering (ICCKE), IEEE, 262-267, 2020. doi: 10.1109/ICCKE50421.2020.9303669.
2. Rao, A.R. & Praveena, R. BIST architecture for secure testing VLSI circuits for security. ISSN-2339-2344. 2020, **7**(15), 2339-2344. doi: 10.31838/jcr.07.14.181.
3. Yutian, G.; Tamore, S.M. Siddiqui, A.S. & Saqib, F. Key update countermeasure for correlation-based side-channel attacks. *J. Hardware and Syst. Sec.*, 2020, **4**, 167-179. doi: 10.1007/s41635-020-00094-x.
4. Zodpe, H. & Sapkal, A. An efficient AES implementation using FPGA with enhanced security features. *J. King Saud Univ. - Eng. Sci.* 2020, **32**(2), 115-122. doi: 10.1016/j.jksues.2018.07.002.
5. Xin-qiang, L.U.O.; et al. Low-cost and fast AES encryption method for industrial wireless network. *J. Beijing Univ. Posts and Telecommun.,* 2015, **38**(1), 55.
6. Ali, Md Liakot; Rahman, Md Shazzatur & Hossain, F.S. Design of a BIST implemented AES crypto-processor ASIC. *Plos One,* 2021, **16**(11). doi: 10.1371/journal.pone.0259956.
7. Rahman, M.S. & Ali, M.L. Design of a built-in-self-test implemented AES crypto processor ASIC. *In* 11th International Conference on Electrical and Computer Engineering (ICECE), Dhaka, Bangladesh, pp. 347-350, 2020. doi: 0.1109/ICECE51571.2020.9393083.
8. Sasdrich, P.; Bilgin, B.; Hutter, M. & Marson, M.E. Low-latency hardware masking with application to AES. *IACR Transact. Cryptographic Hardware and Embedded Syst.*, 2020, 2, 300–326. doi: 10.13154/tches.v2020.i2.300-326.
9. Luca, B.; Crocetti, L.; Falaschi, F.; Bertolucci, M.; Jacopo, B.; Fanucci, L. & Saponar, S. Cryptographically secure pseudo-random number generator IP-core based on SHA2 algorithm. *Sensors*, 2020, **20**(7), 1869. doi: 10.3390/s20071869.
10. Yusuf, K.; Dincer, B.; Yilmaz C. & Savas, E. Spy detector: An approach for detecting side-channel attacks at runtime. *Int. J. Inf. Security*, 2019, **18**(4), 393-422. doi: 10.1007/s10207-018-0411-7.
11. Hely, K.R. & Karri, R. Security challenges during VLSI test. *In* IEEE 9th International New Circuits and systems conference, 2011, 486-489. doi: 10.1109/NEWCAS.2011.5981325.

12. Li, X.; Li, W.; Ye, J.; Li, H. & Hu, Y. Scan chain based attacks and countermeasures: A survey. *IEEE Access.* 2019, **7**, 85055-85065. doi: 10.1109/ACCESS.2019.2925237.
13. Shiny, M.I.; Devi, N. & Trustworthy, M. Scan design & testability using obfuscation and logic locking scheme for wireless network application. *Mobile Network Appl.,* 2022, **27**, 1000–1018. doi: 10.1007/s11036-021-01857-8.
14. Lee, J.; Tehranipoor, M.; Patel, C. & Plusquellic, J. Securing designs against scan-based side-channel attacks. *IEEE Transact. Dependable and Secure Comput.,* 2007, **4**(4), 325-336. doi: 10.1109/TDSC.2007.70215.
15. Aijiao, C.; Luo, Y. & Chang, Chip-Hong. Static and dynamic obfuscations of scan data against scan-based side-channel attacks. *IEEE Transact. Inf. Forensics and Security.,* 2016, **12**(2), 363-376. doi: 10.1109/TIFS.2016.2613847.
16. Ali, Sk Subidh; Saeed, S.M.; Sinanoglu, O. & Karri, R. Novel test-mode-only scan attack and countermeasure for compression-based scan architecture. *IEEE Transact. Comput.-Aided Design of Integrated Circuits and Syst.,* 2015, **34**(5), 808-821. doi: 10.1109/TCAD.2015.2398423
17. Yanhui, L.; Cui, A.; Qu, G. & Li, H. A new countermeasure against scan-based side-channel attack. IEEE International Symposium on Circuits and Systems (ISCAS)., 2016, 1722-1725. doi: 0.1109/ISCAS.2016.7538900.
18. Jayesh, P. & Mehta, U. A novel countermeasure against differential scans attack in AES algorithm. In International Symposium on VLSI Design and Test. Springer, Singapore. 2019, 297-309.
19. Chen, X.; Aramoon, O.; Qu, G. & Cui, A. Balancing testability and security by configurable partial scan design. *In* IEEE International Test Conference in Asia (ITC-Asia)*.,* 2018*,* 145-150. doi: 10.1109/ITC-Asia.2018.00035.
20. Rajasekar, P. & Mangalam, H. Design and implementation of power and area optimized AES architecture on FPGA for IoT application. Circuit World Emerald Publishing Limited., 2021, **47**(2), 153-163. doi: 10.1108/CW-04-2019-0039.
21. Wang, W.; Wang, J.; Wang, W.; Liu, P. & Cai, S. A secure DFT architecture protecting crypto chips against scan-based attacks. *IEEE Access*, 2019, **7**, 22206-22213. doi: 10.1109/ACCESS.2019.2898447.
22. Xu, Y.; Deng, F.; Xu, W.; Huo, G.; Yang, Y.; Jin, Y. & Cui, X. Unified coprocessor for high-speed AES-128 and SM4 encryption. *In* 2022 IEEE 6th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*,* 2022, 640-644. doi: 10.1109/IAEAC54830.2022.9929737
23. Muthavhine, K.D. & Sumbwanyambe, M. An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect. *In* International Conference on Information and Communications Technology (ICOIACT)*,* 2018, 114-119.
24. Kamsiah, M.; Nazran, M.; Pauzi, M.; Hani, F.; Ali, M. & Ariffin, S. Analyse on avalanche effect in cryptography algorithm. European Proceedings of Multidisciplinary Sciences, 2022. doi: 10.15405/epms.2022.10.57.
25. Taher, H.M.; Al-Rahman, S.A. & Shawkat, S.A. Best S-box amongst differently sized S-boxes based on the avalanche effect in the advance encryption standard algorithm. *Int. J. Electrical and Comput. Eng.,* 2022, **12**(6), 6535-6544. doi: 10.11591/ijece. v12i6.pp6535-6544.

CONTRIBUTORS

Ms G. Sowmiya obtained her MTech degree in VLSI Design under Advanced Computing and Information Processing department from SASTRA University, Thanjavur, India. Her current research interest include: VLSI testing, low power VLSI, cryptography, and network security.
In the current study she came up with the concept, carried out the literature survey, examined the work with simulation and analysis.

Dr S. Malarvizhi obtained her PhD degree in Wireless Communication from Anna University, Chennai, under Faculty of Information Communication Engineering in 2006 and working as a Professor in the Department of ECE, SRM Institute of Science and Technology, Kattankulathur, Chennai. Her areas of interest include: Single processing and machine learning in hardware through BRNS funds and deep learning for breast cancer diagnosis AMD Xilinx (WIT).
In the current study she has guided in simulation methodology, reviewed the progress of work and provide insights into formulation and results.