Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Design of Testability Structures With Security For Machine Intelligence Based Cryptosystem

G Sowmiya (sg8182@srmist.edu.in)
SRMIST: SRM Institute of Science and Technology
S. Malarvizhi
SRM University: SRM Institute of Science and Technology

Research Article

Keywords: Scan-based attacks, AES core, Controllability and Observability, Design-for-Testability, Crypto system, Side-channel attacks, Bit Masking

Posted Date: January 11th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1217671/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Abstract

During testing utmost all appropriate and suitable strategy needs to be established for consistent fault coverage, improved controllability and observability. The scan chains used in BIST allows some fine control over data propagations that is used as a backdoor to break the security over cryptographic cores. To alleviate these scan-based side-channel attacks, implementing a more inclusive security strategy is required to confuse the attacker and to ensure the key management process which is always a difficult task to task in cryptographic research. In this work for testing AES core Design-for-Testability (DfT) is considered with some random response compaction, bit masking during the scan process. In the proposed scan architecture, scan-based attack does not allow finding out actual computations which are related to the cipher transformations and key sequence. And observing the data through the scan structure is secured. The experimental results validate the potential metrics of the proposed scan model in terms of robustness to the scan attack and penalty gap that exists due to the inclusion of scan designs in AES core. Also investigate the selection of appropriate location points to implement the bit level modification to avoid attack for retrieving a key.

1. Introduction

In recent years cryptographic algorithms are implemented as digital systems to meet desired data rate and other energy requirements. But complex design translation during fabrication increases the probability of faults which need to be detected to ensure the reliability. Testing of modern digital systems is becoming a difficult task to accomplish especially when the system deals with SoC level implementation and allows only limited access to the design. To handle these issues testing has to be manageable and should allow more controllability and observability. Controllability helps to configure and generate essential input stimulus for most appropriate testing and observability enables to explore the most finite state of the design during testing.

Scan-based test is the most prominent method used widely in Design for Test (DfT) technique with improved testability. It also provides high fault coverage with appropriate test pattern generation and response analysis. However, for testing cryptographic algorithms it is also important that Scan-based tests be robust and

resistant against attacks. In most cases basic information can be leaked or explored by some side channels like states, timing etc. It is known as Side Channel Attacks (SCA). The most commonly used SCA is categorized into two types: Correlation Power Analysis (CPA) and Correlation Instantaneous Frequency Analysis (CIFA). Both the types escalate the vulnerability of the secured AES core. El-Moursy et al., (2020) investigates the chances of using chaotic clocking to secure the AES cores furthermore increase its resistance level against CPA and CIFA attacks. However, computing exact chaotic clocks to effectively protect the core and associated power envelope is a difficult task to accomplish. To mitigate this task chaotic clocks are statistically computed from two sets of chaotic systems.

Scan chain-based attack is one such attack which uses the scan-based design as a backdoor to decode the cipher key of a cryptographic core for attackers. Even for highly secured public cryptographic algorithms like AES, the attack is carried out by accessing intermediate states during testing, and its actual strength is compromised. Testing is an essential measure to ensure the quality while not compromising the security. However, using scan chains to carry side-channel based attacks to get secret information from cryptographic core is unavoidable; it requires unique solutions to defend. In general Design for Testing (DfT) methodology in scan design replaces the all D flip-flops with scan cells which are connected through scan chains. This scan chain model allows controllability and observability with reduced hardware complexity of BIST and testing time. However, the attacker can carry out iteration only on test-mode-only and countermeasures proposed for defending these attacks isolate the normal mode of cryptographic transformations. Apart from hiding the transformations involved inside cryptographic modules, cipher key protection is prioritized over being cracked.

This paper presents a novel scan chain architecture which used modified scan flip flop to generate the masked test patterns with least energy consumption and computational complexity overhead, without compromising the fault coverage. This is obtained by inserting modified SFF randomly and the transform computation associated with masking results in unpredicted ciphers. The paper is organized as follows. Section 2 presents some preliminaries on various scan architecture introduced for robust scan mode testing and BIST implementations. The proposed secured scan mode testing and its functionality is presented in section 3. Experimental results for performance validation are performed with the different combinations of SFF in section 4. Conclusion is given in section 5.

2. Related Work

The scan chains enabled Design for Testability (DfT) technology is prominently used in many digital systems to ensure the frequent testing of the design by achieving improved fault coverage and observability. But it leads some potential security threats by allowing the attackers to monitor the scan chains to attack a system. Many existing works introduced unique DfT solutions to secure the cryptographic systems against scan attacks. In [1] Nara et al., analyzed scan-based differential attack to explore key operation in Elliptic Curve Cryptography (ECC) and investigates the iterative execution in mode to get different transformation models used for generating the cipher. The intermediate results obtained from the scan chains offer useful information to carry out scan-based non-invasive attacks.

Ali et al., [2] carried out detailed analysis of all kind of test-mode-only scan attack on AES core and explored the demands of scan architecture modification in DfT infrastructure to defend attack results and reduce the vulnerability of AES core to test-mode-only attacks. It also investigates the process associated with retrieval of secret keys even with the presence of decompressor and compactors. Cui et al., [3] developed the key and lock method based on static obfuscation for securing the scan data. Here instead of shuffling the scan cells, some of the scan cells are altered to modify the scan data during testing. Though the static obfuscation is not sufficient for masking the scan data yet, it can resist the test-mode-

only signature-based attack. For all other attacks dynamic obfuscation of scan data is introduced by cyclically shifting the scan data based on key throughout the testing process.

Wang et al., proposed a new testing methodology to prevent scan-based attacks using the supply chain. Here Dynamically Obfuscated Scan (DOS) model is used for protecting scan data from attackers. Both test patterns and its signal responses are protected using obfuscation key to defend all kinds of non-invasive scan-based attacks without compromising the fault coverage. The BIST scheme developed by Luo et al., used a shift register to control the operations of scan cells. Using appropriate configuration set by designed the shift register is functions correctly and produces random results during the testing mode. These registers driven approaches offer improved testability with least complexity and they resist all known scan-based attacks.

Rahman et al., [6] explores the vulnerabilities of scan testing, it's increasing number of attacks over cryptosystem and associated security concerns. It also introduced logic obfuscation to defend all sorts of scan-based attacks and analyzed its influences in scan-based BIST structure. Popat et al., [9] investigates the process involved in Differential Scan Attack (DSA) over AES to retrieve the secret key information. It also proved that security measures through time compactor is not optimal for the AES system and introduced the novel Modular Exponentiation Secure Scheme (ME-SS) mechanism for defending the scan attack. Here by insulating the details of the cipher key and clearing the insecure states, improved security is provided to AES. Rajasekar et al., (2020) designed a low complexity energy efficient AES core using hierarchical optimization in each stage of AES. The optimization includes multiplicative inverse, affine transforms and X-time multipliers for area efficiency. Finally multistage pipeline and hardware resource sharing among S-Box and Mix column offers improved throughput rate during hardware implementation.

Nandan et al., (2020) invented an optimal substitution box model using enhanced Galois field-based transform for multiplication in AES algorithm. Here the AES core comprises simplified arithmetic components namely AND, XOR, XNOR for the complete designing process. By replacing AND gates by NAND gates, the transistor counts are significantly reduced. In addition to this, some logical re-sizing models are also incorporated for implementing 4-input XOR gate which narrow down the path delay overhead and energy consumption. The less delay can be obtained by architecture.

The secured scan architecture developed in Wang et al., enables fully automatic test control blocks which are loaded to protect the cipher key in BIST mode besides disable this source information during normal mode operations. Based on security measures analyzed test authorization is also incorporated for complete robustness to scan attacks using some authorization key for initializing the testing process. In (Lee et al.,) dynamic-key based secure scan architecture is proposed based on some intrinsic Physical Unclonable Function (PUF) to mitigate both scan and memory-based attacks without causing any significant measure in the testing scheme. Here while testing, a scan attack is defended by not shifting out the original responses into the scan chain, memory attacks are impossible since test key is not stored in memory.

Biclique Cryptanalysis widely used the hash function for cryptanalysis measures over block cipher algorithms. In this type cryptanalysis, the worst-case reference is used, which is formulated from brute force. It provides to new benchmark. In general, biclique is formulated by length and dimension. The metrics of biclique, over conventional brute force are as follows: computational cost for construction and number of matchings. In general, Advanced Encryption Standard (AES) is most widely used crypto core algorithm in much wireless communication, but due to the emergence and technical advancements of various attacks namely linear cryptanalysis, differential cryptanalysis, boomerang attack, related-key based discrimination attack, side channel attacks, etc. the demands for improved security are emerging steadily. Lavanya et al., (2020) introduced dynamic scale variations in the AES shift row stage and unique expansion unit in key generation stage of the AES core to improve its resistance towards all sorts of cipher attacks and the actual computations complexity of cryptanalysis has also increased considerably. This modified AES core includes both improved physical and key based transformations to incorporate both enhanced diffusion and confusion during cipher conversion. Sasdrich et al., (2020) developed novel hardware masking for AES crypto system that does not cause any notable latency problems. Here LUT-based Masked Dual-Rail is used with statistical Pre-charge Logic (LMDPL) for security. Cui et al., (2020) proposed novel key update-based countermeasure for power and electromagnetic analysis-driven side channel attacks on the crypto cores. The countermeasure incorporates a secure coprocessor to offer secure key generation and memory storage [3].

3. Recapitulation Of Advanced Encryption Standards

The further desired along with colossally adopted symmetric encryption algorithm expected occurs confront these days is the Advanced Encryption Standard (AES) algorithm. It is established at the minimum of six time's rapid than triple DES. Since its key size was insignificant a substitution for DES was needed. With escalating computing power, it was examined to be vulnerable against exhaustive key search attack. To overcome this drawback Triple DES was outlined but it was found slow. In order to make a cipher text the AES algorithm uses a substitution-permutation, or SP network, with multiple rounds.

- **Substitution of the bytes**: In the first step, the bytes of the block text are substituted based on rules dictated by seeded S-boxes (substitution boxes).
- **Shift rows**: In this step, except the first all rows are shifted by one.
- **Mix columns**: By mixing the block's columns the cipher is used to jumble up the message.

In current day cryptography, AES is acquired extensively which supports both hardware and software. There are no empirical cryptanalytic attacks against AES till date has been found. Built-in adjustability of key length is added additionally in AES, which allows enduring against the advancement in ability to perform comprehensive key searches. However, for DES, the security of AES is assured only if it is precisely implemented and good key management is earned. Certain advantage that AES possess such as swift, superficial to implement still more hard to attack, and it has been enormously used in secure

communication applications. Unlike the scan-based attack, which can leak information remotely through communication module, side-channel attackis hard to carry out in end-to-end communication.

The illustrative structure of AES is given below

3.1 Scan Design and Countermeasures:

An AES core is designed and inside which BIST is enabled using scan flip-flop SFF. A scan flip-flop (Fig. 2) multiplexer added with is a D flip-flop added with the input and one input of the Multiplexer acts as the functional input of D, and the others acts as the Scan-In (SI) input. The MUX selection bit can be controlled by the Scan/Test Enable (SE/TE) signal. Scan flip-flops are used extensively for device testing. Input is given to SFF, the data is shifted in and a random flip-flop is chosen and masking is done. So as a result, even the actual input is given the original output cannot be retrieved. During BIST implementation overall scan test is decomposed into four pages and scan FF in s-box unit is masked to avoid side channel information leakages.

3.1.1. Bit Level Scan Masking

Standard scan flip flops are a highly vulnerable threat to security during BIST implementation of cryptographic digital systems. Here initially, when it is switched from normal mode to test mode resetting the chip was done and exploited to safeguard. The proposed modified scan FF is encrypting the data propagated through scan chains using modulo operation during testing mode as shown in Figure 1, to narrow down the controllability and observability of AES core to attackers. During scan testing for each successive test pattern generated for fault detection, estimating or assuming the cipher differences between the pattern inputs is not possible and cipher key based transformed results also ends with another cipher with maximum data masking. As compared to the converter SFF, two operations are included with a simplified bit inverter and an XOR gate in proposed modified secured scan FF design. Moreover, bit masking is carried out in a completely random manner without considering the AES core design perspective.

3.2 Security vs. Resource Efficiency

AES core consists of group of hierarchical transformation modes which includes both physical and key based transformation that are randomly selected in each round of operations based on design constrained in terms of hardware resource and memory space. Therefore, it is essential to optimize the computational complexity without compromising security. Among all other blocks, s-box units require minimal resources and computational tasks since other computations like mix columns and shift rows need several multiplications and bit transitions. Additionally, it has been prominently used in several works as potential replacements to s-box encoding with unique characteristics that can be utilized for the key generation process as well.

3.2.1 Interpolation Attacks

By considering the cipher as a polynomial the coefficient values are predicted to extract the complex algebraic function used to generated S-box values. It doesn't require any prior knowledge about the cryptographic key. With completely randomized transformation level called diffusion in the cipher, along with the confusion layer provides by substitution makes this system robust against this type of attack. Moreover, there is no algebraic relationship between input text and generated cipher due to non -linear transformation that make this attack impractical.

3.2.2 SQUARE Attack

Square Attack is used to recover the cipher key used for propagation of sets from plaintext to cipher. Though this attack is independent of the number repetition in S-box and the key expansion unit one can increase the number of guesses required to carry out this kind of attack by changing the true key periodically but this will lead to key management problems. But here we can generate any number of key sequences from input biometric, in addition, the isolated keys can be used for each round of operations. This mode of attack required 16 repetitions to recover 128-bit true key and by changing the true key for every clock instant it can explore only last byte of each key units during the attack.

4. Experimental Results

Our proposed work presented a scan test methodology which can generate a simple and randomized modification of scan data during testing and evaluated it focusing on the discrimination capability. The random insertion of modified scan FF in the scan chain offers maximum security measures. AES core is grouped into four sections and test inputs are applied directly into the corresponding scan chains. Here by using page selection and row/column selection bits, the scanning operation can be changed dynamically. To avoid fault masking scan OUT is directly fed into response analyzer. And finally, the cryptographic model was described in Verilog HDL and synthesized using the QUARTUS II EDA design compiler tool.

4.1 Scan Mode AES Model

This section also includes various FPGA implementations of AES cryptosystem masking schemes to prove the performance metrics of our AES cryptosystem mode. Here both operating frequency and complexity overhead of the proposed cryptosystem is considerably reduced while the number of bits in the block cipher and the transformation rate are well matched with AES cryptosystem. In addition, the key sequence used for each round can also be changed to maximize the security level. The performance measure in terms of logical unit utilized and operating frequency are shown in Table 1. Table 2 provides FPGA synthesis results of the architecture in Altera and compared to its state-of-the- methods. Due to the unavailability of Xilinx- XC6VLX240T, the comparison is made using Altera- EP3C16F484C6.

Table 1
Hardware complexity and performance comparison of proposed robust scan framework with FPGA hardware synthesis.

Security mechanism	Area			F-max (MHz)
	Logic cell	LUTs	Logic registers	
Outer layer masking	5269	3396	1873	132.56 MHz
One bit masking	5064	3191	1873	125.13 MHz

Table 2
State-of-the-art comparison of proposed robust scan AES core with other FPGA models.

AES type	AES block size	Devices	Avalanche Effect (%)	Scan mode protection	Number of slices	F-max (MHz)
AES model – LUT S-box with improved Key expansion (Zodpe et al., (2020))	128-bit	Xilinx-XC6VLX240T	50%	No	4095	463.42
Proposed model-composite S box with bit level masking	128-bit	Altera-EP3C16F484C6	90-95%	Yes	4638	223.56 MHz

4.2 Security Analysis

The proposed cipher performs transformation on a 128-bit block of input plaintext and uses a 128-bit key extracted from scan input and generated 128-bit cipher text as shown in Figure 3 & 4. The encryption stage consists of physical as well as key based transformation, multiple rounds of transformations which comprise of permutation, cyclic shifting,

bitwise rotations S-box and modulo operations etc. The security evaluation of proposed cryptosystems is carried out using robustness over some attacks and parameters measures such as key sensitivity, computation time etc.

5. Conclusion

Here the implementation of secured BIST in AES cryptographic algorithms using scan-based testing is analysed. It has been previously signified that scan chains not only offer a backdoor to some attacks but also provides observability. Here, bit level scan FF based masking is proposed as a scan-protection scheme to carry out secured testing. As compared to other scan tests, this technique has no impact on the quality of the test or the model-based fault diagnosis. Here the modified scan FF in AES core causes least design complexity & power optimization overhead with insignificant delay measures. This SFF-based analysis for AES core is validated using different sets of multiple scan FF derived from the SFF which doesn't require any sort of masking parameters.

Declarations

Declaration of interests

We wish to confirm that there are no known conflicts of interest associated with this publication or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Ali A. El-Moursy; Abdollah M. Darya; Ahmed S. Elwakil; Abhinand Jha; Sohaib Majzoub.” Chaotic Clock Driven Cryptographic Chip: Towards a DPA Resistant AES Processor”, IEEE Transactions on Emerging Topics in Computing Dec. (2020). https://doi.org/0.1109/TETC.2020.3045802

[2] Nara, R.; Togawa, N.; Yanagisawa, M.; Ohtsuki, T. Scan-based attack against elliptic curve cryptosystems. In Proceedings of the Asia and South Pacific Design Automation Conference, Taipei, Taiwan, 18–21 January (2010); pp. 407–412. https:// doi.org/10.1109/ASPDAC.2010.5419848.

[3] Ali, Sk Subidh, Samah M. Saeed, Ozgur Sinanoglu, and Ramesh Karri. "Novel test-mode-only scan attack and countermeasure for compression-based scan architectures." IEEE transactions on computer-aided design of integrated circuits and systems 34, no. 5 (2015): 808-821.

[4] Cui, Aijiao, Yanhui Luo, and Chip-Hong Chang. "Static and dynamic obfuscations of scan data against scan-based side-channel attacks." IEEE Transactions on Information Forensics and Security 12, no. 2 (2016): 363-376.

[5] Wang, Xiaoxiao, Dongrong Zhang, Miao He, Donglin Su, and Mark Tehranipoor. "Secure scan and test using obfuscation throughout supply chain." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 37, no. 9 (2017): 1867-1880.

[6] Luo, Yanhui, Aijiao Cui, Gang Qu, and Huawei Li. "A new countermeasure against scan-based side-channel attacks." In 2016 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1722-1725. IEEE, (2016).

[7] Rahman, Md Tauhidur, Domenic Forte, and Mark M. Tehranipoor. "Protection of assets from scan chain vulnerabilities through obfuscation." In Hardware Protection through Obfuscation, pp. 135-158. Springer, Cham, (2017). https://doi.org/10.1007/978-3-319-49019-9_6.

[8] Popat, Jayesh, and Usha Mehta. "A novel countermeasure against differential scans attack in AES algorithm." In International Symposium on VLSI Design and Test, pp. 297-309. Springer, Singapore, (2018).

[9] Rajasekar P. And Mangalam H, “Design and implementation of power and area optimized AES architecture on FPGA for IoT application.” Circuit World Emerald Publishing Limited (2020).

https://doi.org/10.1108/CW-04-2019-0039.

[10] V. Nandan R. Gowri Shankar Rao “Low-power and area-efficient design of AES S-Box using enhanced transformation method for security application”. International Journal of Communication Systems (2020). https://doi.org/10.1002/dac.4308.

Figures

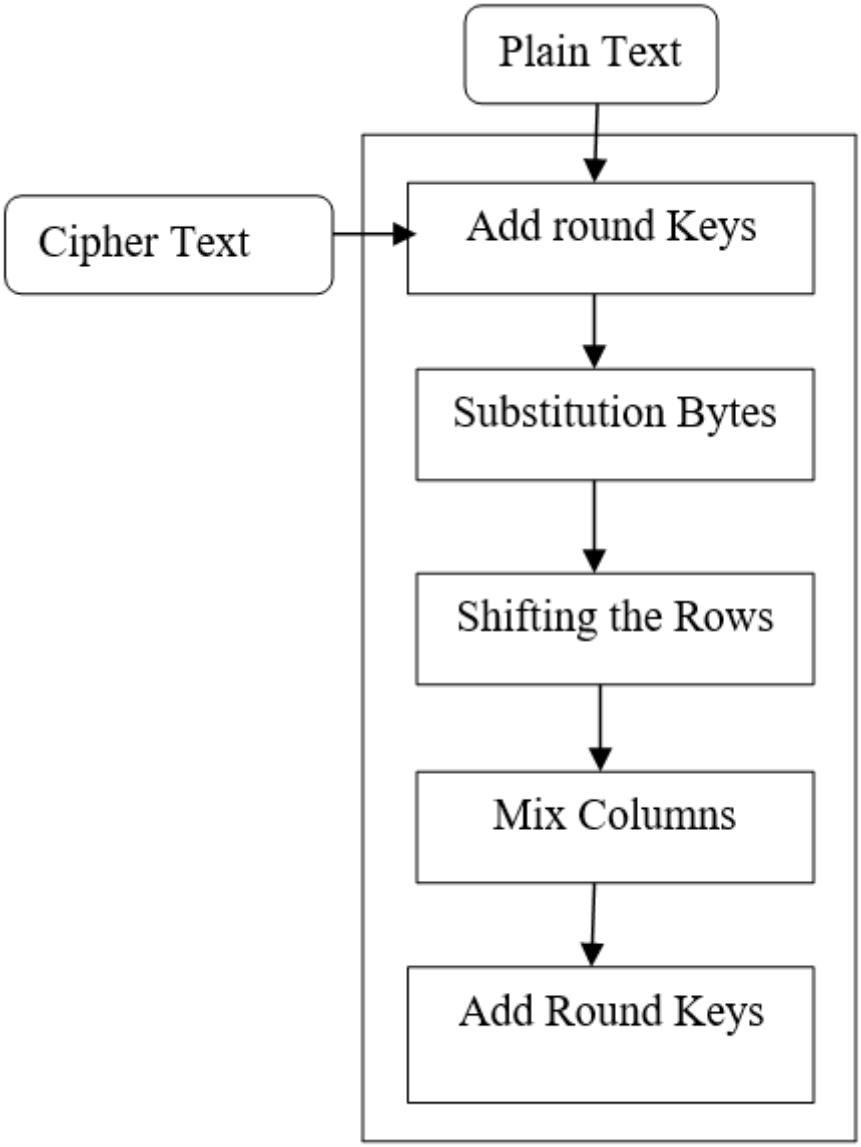

Figure 1

AES Encryption Processing Steps

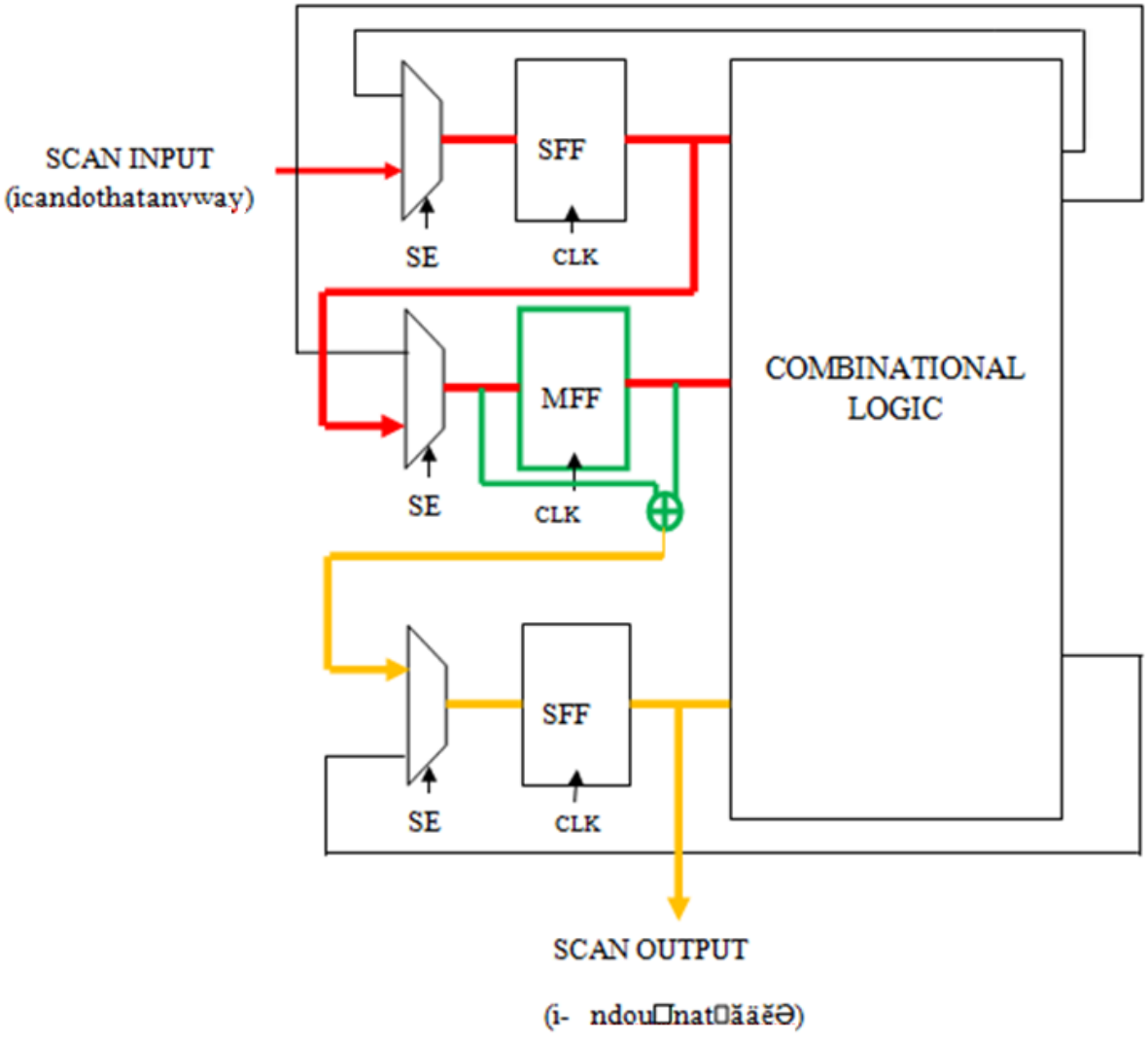

Figure 2

Architectural design for bit level masking scheme for AES BIST application

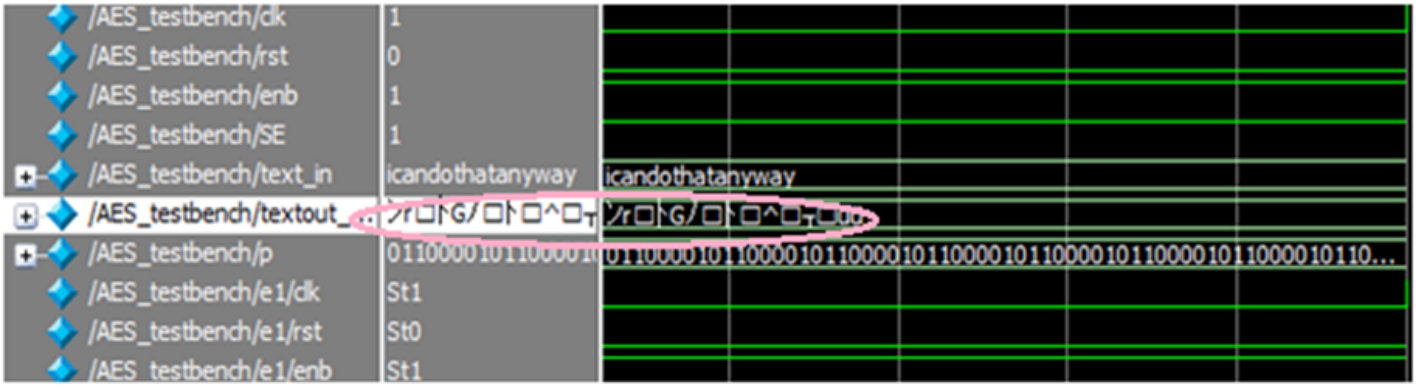

Figure 3

Masking selection with 128-bit outer layer transformation using proposed SFF.

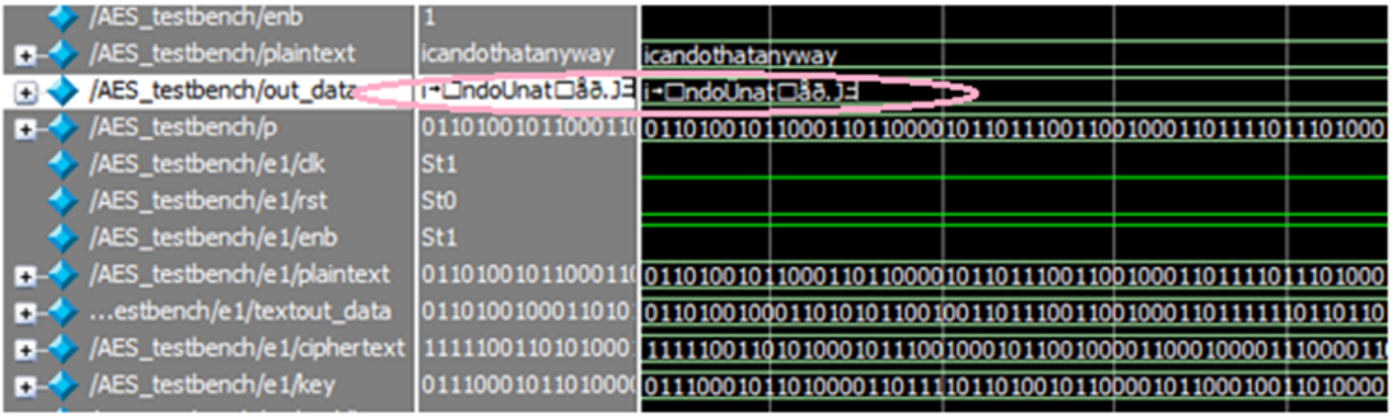

Figure 4

Masking selection with a one-bit inner layer transformation using proposed SFF