Differential Fault Analysis on High Throughput AES

T. Soundarya

M. Tech (VLSI Design) Department of Electronics and Communication Engineering, Kattankulathur Campus, SRM University, India

Abstract: ***Cryptography plays a key role in ensuring the privacy and integrity of data. Cryptanalysis is the study of how to crack encryption algorithms and their implementations. Differential cryptanalysis is a plain text attack which occurs in the cryptographic system. Testing can control and observe the internal states of the system. While testing in the cryptographic system, by observing the input and output bit changes, the third parties may shift out key. To reduce the observability and to increase the security, Robust Secure Scan design (RSS) is proposed. RSS design encrypts the content during scan chain operation. By adding pipelining process in the S Box and transforming the S Box transformation into combinational design, 50% high throughput is achieved over the standard Encryption algorithm. By this method the security is much improved as it incorporates RSS design, which involves double encryption process.***

Keywords: AES, S-box transformation, lookup table

1. Introduction

Cryptographic is an art of creating secret codes and Cryptanalysis is the science and art of breaking those codes. Encryption is a disintegrable part of all communication networks and information processing systems, for protecting both stored and in transmit data. Encryption is the transformation of plain data known as plaintext into unintelligible data known as ciphertext through an algorithm referred to as cipher. The Data Encryption Standard (DES) was considered as a standard for the symmetric key encryption. DES has a key length of 56 bits. However, this key length is currently considered small and can easily be broken. Scan chains are the most popular testing technique due to their high fault coverage and least hardware overhead. However, scan chains open side channels for cryptanalysis. Scan chains are used to access intermediate values stored in the flip-flops, thereby, ascertaining the secret information, often known as key. Conventional scan chains fail to solve the conflicting requirements of effective testing and security.

Rijndael can be specified with key and with multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. Therefore, the problem of breaking the key becomes more difficult [1]. In cryptography, the AES is also known as Rijndael [2]. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

The Advanced Encryption Standard (AES) is an encryption standard chosen by the National Institute of Standards and Technology (NIST) in 2001, which has its origin in the Rijndael block cipher. Several studies in the area had identified the nonlinear SubBytes transformation as the major problem in achieving both small area and high speed VLSI in AES implementations.

A. Side channel attacks

Scan test has been widely adopted as a testing technique among VLSI designs, including crypto cores. These scan chains might be used as a ―side channel‖ to recover the secret keys from the hardware implementations of cryptographic algorithms, for example scan-based attacks on Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Elliptic Curve Cryptography (ECC) have been illustrated in [1]–[3], respectively.

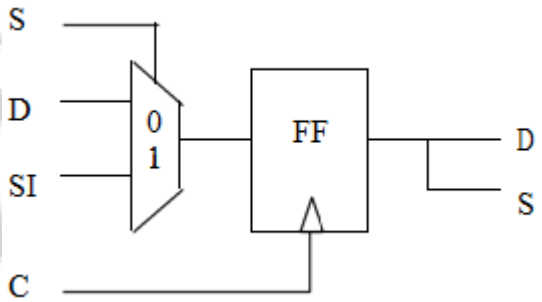

Figure 1: Normal scan FF

In general, the scan-based side channel attacks (SSCA) could be viewed as one kind of differential cryptanalysis by using scan chains of crypto cores chains of crypto cores. Unlike other known side channel attacks, SSCA is much easier. It is because that in SSCA, in addition to the primary outputs of the crypto cores, a hacker could use scan chain to shift out the intermediate contents during a cryptographic operation. Average overall only 544 plaintexts are required to discover the AES key by using SSCA, which clearly shows the great potential threat of scan-based side channel attack [5].

2. Description of AES Algorithm

The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. Encryption converts data to an unintelligible form called cipher-text. Decryption of the cipher-text converts the data back into its original form, which is called plain-text.

A. AES encryption

The AES algorithm operates on a 128-bit block of data and executed Nr - 1 loop times. A loop is called a round and the number of iterations of a loop, Nr, can be 10, 12, or 14 depending on the key length. The key length is 128, 192 or 256 bits in length respectively. The first and last rounds differ from other rounds in that there is an additional AddRoundKey

transformation at the beginning of the first round and no MixCoulmns transformation is performed in the last round [3]. In this paper, the key length of 128 bits (AES-128) is used as a model for general explanation.

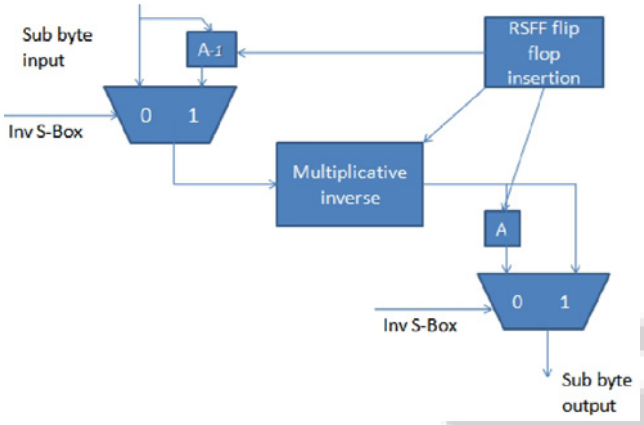

Figure 2: LUT less implementation of S-box and Inverse S-box with synchronous RSFF

B. SubBytes Transformation

The SubBytes transformation is a non-linear byte substitution, operating on each of the state bytes independently. In existing methods the SubBytes transformation is done using a once precalculated substitution table called S-box.But in this work the SubByte transformation is computed by taking the multiplicative inverse in GF(2^8) followed by an Affine transformation. For the InvSubByte transformation, the inverse affine transformation is applied first prior to computing the Multiplicative inverse.

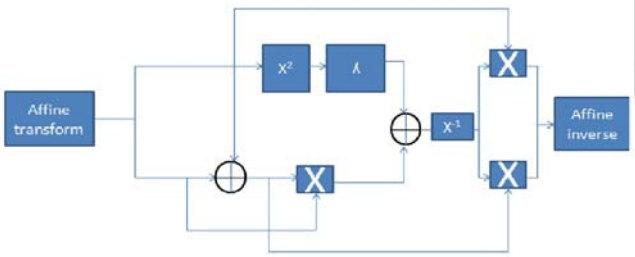

Figure 3: Multiplication inverses

C. ShiftRows Transformation

In ShiftRows transformation, the rows of the state are cyclically left shifted over different offsets. Row 0 is not shifted; row 1 is shifted one byte to the left; row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left.

D. MixColumns Transformation

In MixColumns transformation, the columns of the state are considered as polynomials over GF (28) and multiplied by modulo x4 + 1 with a fixed polynomial c(x), given by: $c(x)=\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.

E. AddRoundKey Transformation

In the Add Round Key transformation, a Round Key is added to the State - resulted from the operation of the MixColumns transformation - by a simple bitwise XOR operation.

3. Robust Secure Scan

To reduce the controllability and observability of unintended users a robust secure scan is designed.RSS design encrypt the content during scan chain operation. Encrypted content is given as the input to the Cryptographic algorithm [6].

For the security and testability requirements, a novel robust secure scan-based test approach is proposed as a countermeasure against scan-based differential cryptanalysis. Block diagram of the RSS design is shown in fig 4.

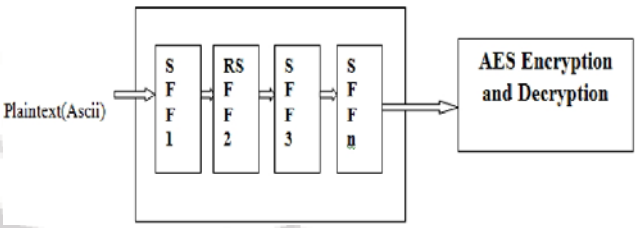

Figure 4: RSS Design

In a System there are two modes of operation functional mode and scanning mode. In the normal function mode (SE==0) SFF loads data from the logic through DI, and the output to logic is DO. In proposed RSFF (fig 4), an additional inverter and the XOR gate are inserted along the scan path. Thus in function mode, RSSF works like a traditional scan flip flop. In scan test mode, that during scan shift operation, the content of FF is XOR ed with SI to be shifted out to the next SFF and the inverted scan-in data (SI) will be loaded into FF. Thus for hackers, it becomes extremely complicated to identify the relationship between the input response and the scan-out response.

A. Proposed scheme- Robust secure scan design

The basic idea of the proposed RSS design is to encrypt the contents in scan chains during scan operation, so as to reduce the controllability and observability of unintended users. It becomes more complicated for hackers to identify the bit differences between pairs of related plaintexts when they are encrypted under the same key. One kind of the proposed RSS design is shown in Fig. 4, in which the contents of two neighboring SFFs are encoded during scan operation from a security aspect.

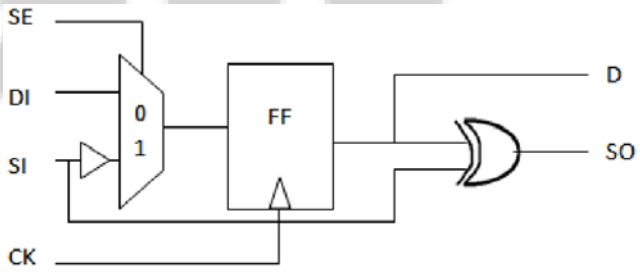

Figure 5: Proposed RSSF

When compared with the traditional SFF, an extra inverter and

an XOR gate are introduced in the RSS design. This simple logic could be used for encryption during scan operations and therefore fully compatible with industry standard design tools from a design perspective, when integrated into current design flows it only requires the RSSF added into the cell library [6].

4. Implementation and Result Discussions

In this section, security analysis and implementation overhead are discussed to show the advantages of the proposed secure test technique over existing methods.

A. Analysis of Scan based attack

Due to the avalanche effect of cryptographic algorithms, there exist two kinds of scan-based differential cryptanalysis, called as constant based (CBA) and fixed hamming-distance-based attack (FHDA). Here let us use AES as an example
B. Process against Scan based attack

When using the proposed RSS, it can be easily configured that once the data of SFFs passing the replaced RSSFs, they would be encrypted and this makes it extremely difficult to identify the positions of SFFs in the scan chain from external. In addition, because the proposed RSSFs deals with the scan-in and scan-out as well, it is also difficult for hackers to set the CFFs to desired states with no detailed knowledge of the scan structure implementation.

Replace the last SFF in the scan chain with RSSF, and then conduct FHDA .The response of two pairs of plaintexts do not belong to any of the original four pairs, which lead the hackers to get wrong keys.

C. Implementation

The scan flip flop is used to test the function and it shift between the functional mode and scanning mode using a multiplexer. When the SE=0(select enable) the function of the AES algorithm got processed and SE=1 the testing process undergoes.

Robust secure scan gives double encryption to the input of the AES algorithm during the scanning mode. During Encryption process text is converted to cipher text to make it unreadable to anyone except those possessing special knowledge using key. Using decryption the cipher text is converted to the original plaintext, it's the reverse process of Encryption.

RSS with AES algorithm is simulated using Modelsim 6.4a and synthesized using Quartus II 9.0

cryptographic algorithm to explain these two kinds of attacks. CBA takes advantages of the fact that in encryption process, the contents of some special registers are independent on the inputted plaintext. For example, the round registers in AES, without special protection, for each normal inputs, in the first cycle they would be 0001, and then 0010,……. 1010. By using several different plaintext inputs and scanning out the contents at different times of the cryptographic operation, these registers could be easily identified. Then by setting the registers as 1010 (i.e., to indicate the round cycle is 10, the last round for 128-bit AES), which is because in AES the mix-column operation is bypassed in the last round, it became much easier to discover the secret keys. Such a kind of attack is called constant-based attack. FHDA is another kind of scan-based attack by counting the number of bit changes on relevant plaintexts so as to discover the secret key, and refer to [2] for more details on FHDA.

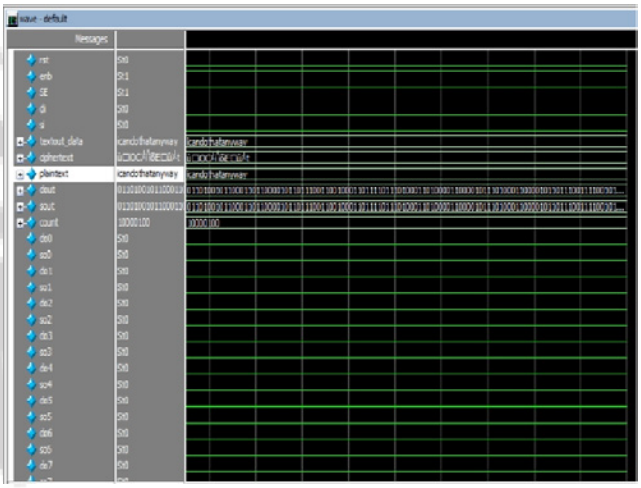

Figure 6: Simulated output of AES algorithm

In normal mode (SE=0) the input to the AES algorithm got processed remains constant and Scanning mode(SE=1) the input to the AES algorithm got double encrypted using RSSF and a scan control unit. Simulated output of AES is shown in fig 6 and flow summary is shown in fig 7.

Flow Status	Successful - Wed Dec 05 21:22:27 2012
Quartus II Version	9.0 Build 132 02/25/2009 SJ Web Edition
Revision Name	asddd
Top-level Entity Name	encrypt_decrypt_top
Family	Cyclone III
Device	EP3C16F484C6
Timing Models	Final
Met timing requirements	N/A
Total logic elements	9,009 / 15,408 (58 %)
Total combinational functions	8,718 / 15,408 (57 %)
Dedicated logic registers	1,037 / 15,408 (7 %)
Total registers	1037
Total pins	259 / 347 (75 %)
Total virtual pins	0
Total memory bits	0 / 516,096 (0 %)
Embedded Multiplier 9-bit elements	0 / 112 (0 %)
Total PLLs	0 / 4 (0 %)

Figure 7: Flow summary of AES with RSS

There are two modes of operation normal mode (SE=0) and scanning mode (SE=1).In SFF, during the functional mode the AES algorithm got processed and in scanning mode, all the input combination got tested. Simulated output of AES in scanning mode shown in figure 8.

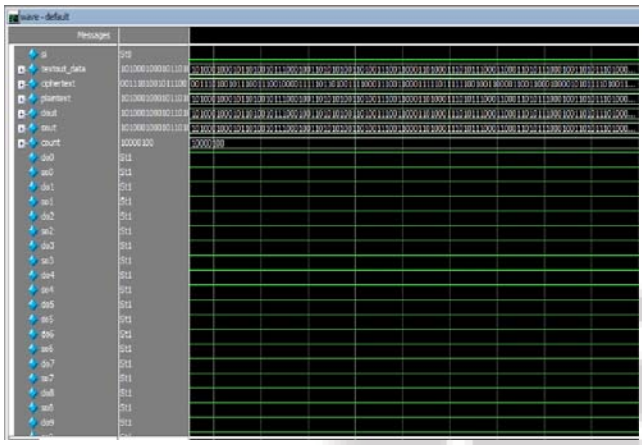

Figure 8: Simulated output of AES in Scanning mode-inserting RSS

S Box in AES algorithm is implemented is LUT-based S-box/Inverse S-box to show the efficiency. The design uses an iterative looping approach with block and key size of 128 bits, without using lookup table.

Flow Status	Successful - Sun Mar 17 19:54:06 2013
Quartus II Version	9.0 Build 132 02/25/2009 SJ Web Edition
Revision Name	aessss
Top-level Entity Name	encrypt_decrypt_top
Family	Cyclone III
Device	EP3C16F484C6
Timing Models	Final
Met timing requirements	N/A
Total logic elements	4,980 / 15,408 (32 %)
Total combinational functions	4,715 / 15,408 (31 %)
Dedicated logic registers	1,141 / 15,408 (7 %)
Total registers	1141
Total pins	259 / 347 (75 %)
Total virtual pins	0
Total memory bits	0 / 516,096 (0 %)
Embedded Multiplier 9-bit elements	0 / 112 (0 %)
Total PLLs	0 / 4 (0 %)

Figure 9: Flow summary of AES without LUT

This gives a way to add pipelining stages to increase the frequency of operation as well as high throughput.

Along with S-box transformation, pipelining in all other transformation is implemented to solve the longest critical path problem. The delay is reduced when implementing the S box without LUT. Comparison of delay is shown in Table 1 [6].

S Box Implementation in AES with LUT(ns)	S Box Implementation in AES without LUT(ns)
8.881	.108

RSS in AES With LUT(ns)	*RSS in AES Without* LUT(ns)
12.08	5.02

Table 1: Comparison of delays

5. Conclusion and Future Work

A Secured cryptographic system was designed, modeled and verified using the System Verilog hardware description language. It's a countermeasure against scan based differential cryptanalysis. Since RSS technique involves double encryption process the security of Cryptographic system is improved over the standard encryption algorithm. By inserting RSS design without LUT in the AES process the delay got reduced.

The security can be further increased by inserting robust secure scan design in the Shift rows transformation and in the mix column transformation of the AES algorithm.

References

[1] B. Yang, K.Wu, and R. Karri, Scan based side channel attack on dedicated hardware implementation of data encryption standard," in Proc.Int. Test Conf., 2004, pp. 339–344.

[2] B. Yang, K.Wu, and R. Karri, Secure scan: A design-for-test architecture for crypto chips," IEEE Trans. Computer Aided Des. Integr. Circuits Syst., vol. 25, no. 10, pp. 2287– 2293, Oct. 2006.

[3] R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, Scan-based attack against elliptic curve cryptosystems," in Proc. IEEE ASP-DAC,2010, pp. 407–412

[4] G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury, Secured flipped scan-chain model for crypto-architecture," IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., vol. 26, no. 11, pp. 2080–2084, Nov. 2007

[5] M. Agrawal, S. Karmakar, D. Saha, and D. Mukhopadhyay, ―Scan based side channel attacks on stream ciphers and their counter-measures," in Proc. Int. Conf. Cryptology India (INDOCRYPT), 2008, pp. 226–238

[6] Y. Shi, N. Togawa, M. Yanagisawa, and T. Ohtsuki, Design-for-secure-test for crypto cores," in Proc. IEEE Int. Test Conf., 2009, pp. 1–1, Poster-11

[7] D. Hely, M. Flottes, F. Bancel, B. Rouzeyre, and N. Bérard, ―Scan design and secure chip,‖ in Proc. Int. On-Line Test. Symp., 2004, pp. 219–224