ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

NCRICT-2017

Ahalia School of Engineering and Technology

Vol. 6, Special Issue 4, March 2017

Advanced Secure Scan Technique against Differential Cryptanalysis

Aagna K.[1], **Akshaya Gopinath**[2], **Chandni J**[3]

Student, Electronics and Communication Engg, Ahalia School of Engineering & Technology, Kerala, India[1,2,3]

Abstract: In our communication system, security is an important factor. Secured communication assists to protect the confidentiality of data. Secured communication can be obtained by encrypting the data. Cryptography is one method of encrypting our message or information. Fundamentally, the problem lies on the inherent contradiction between testability and security for digital circuits. Hence, there's a need for an efficient solution such that both testability and security are satisfied. Several secure scan techniques exist. Of which the modified scan design of Shatterproof secure scan makes it more difficult to discover the internal scan architecture. Thus a modified scan design which ensures higher level of security is explained in this paper.

Keywords: Cryptography, secure scan, testability.

I. INTRODUCTION

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography is the art of creating secret codes and Cryptanalysis is the science and art of breaking those codes. Cryptography includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit. Encryption is a disintegrable part of all communication networks and information processing systems. Encryption is the transformation of plain data known as plaintext into unintelligible data known as ciphertext through an algorithm referred to as cipher.Any system connected to the internet is bound to eventually be attacked by hackers, and it will be extremely difficult to create a system that is impregnable to outsiders. However, the mathematical formulas involved in encryption are complex enough that even if the hacker manages to steal an encrypted file, he may never be able to break through the code and access the content. Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols.[1]Encryption algorithm are broadly classified as Symmetric or Asymmetric algorithm based on the type of key used. One of the main subjects in cryptography is the symmetric key cryptography, where a shared key of a certain size will be used for the encryption and decryption processes. The encryption accomplished using above kind of cipher are also called as private key encryption and public key encryption respectively. Symmetric algorithm has one key. So the sender who encrypts the information and the receiver who decrypts the information needs to have the same key. Asymmetric algorithm have two keys. One is the public key and other is the private key.Private key is also called as symmetric key. In symmetric key scheme, the key used for encryption and decryption are same. Symmetric algorithm consists of various types of algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), TripleDES. Among this algorithms AES algorithm is very difficult to crack and is well suitable to security service applications.It is designed in a way that has better resistance against existing attacks.Scan based test is a double edged sword. On one hand, it is a powerful test technique. on the other hand, it is an equally powerfu1 attack tool. Scan-based tests are used to validate the function of a hardware system at fabrication time and in field. So several secure scan techniques were designed as a counter measure against scan based attacks.

II. SECURE SCAN TECHNIQUES

A flipped scan was introduced by adding inverters along the scan path so as to make it difficult for hackers to discover the internal scan structure at the cost of small hardware overhead; however it cannot protect the circuit under test from scan based attacks.The security threat of flipped scan was discussed by introducing a simple reset based SSCA and then developed a XOR chain structure for secure testing.

Later on RSSF design is introduced to encrypt the contents in scan chains during scan operation, so as to reduce the controllability and observability of unintended users. By doing this, it becomes more complicated for hackers to identify the bit differences between pairs of related plaintexts when they are encrypted under the same key. 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. The robust scan flip-flop (RSSF) has identical pinouts when compared with the traditional scan flip-flop,

DOI 10.17148/IJARCCE

and is 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.[2]

A novel SSSFis designed to encrypt the contents in scan chains during scan operation, so as to reduce the controllability and observability of unintended users. By doing this, it becomes more complicated for hackers to identify the bit differences between pairs of related plaintexts when they are encrypted under the same key. The SSS design is shown ,in which the contents of two neighbouring SFFs are encoded during scan operation from a security aspect. When compared with the traditional SFF, an extra inverter and an XOR gate are introduced in the SSS design. This simple logic could be used for encryption during scan operations. The additional inverter and the XOR gate are inserted along the scan path; they do not affect the timing of the design. Thus in function mode, SSSF works like a traditional scan flip-flop. We observe that the proposed shatterproof secure scan flip-flop (SSSF) has identical pin outs when compared with the traditional scan flip-flop as, and is therefore fully compatible with industry standard design tools from a design perspective.[5]

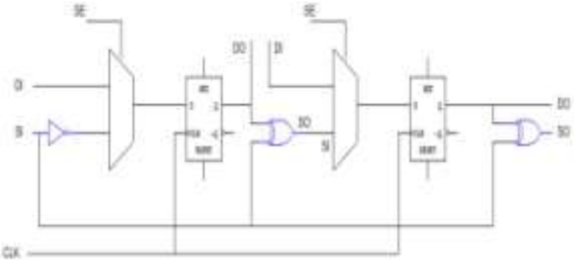


Fig 1: Shatterproof secure scan design

Therefore, in this paper we propose a secure scan architecture called Encipher Shatterproof Secure Scan design which is the modified version of SSS design.

III. ENCIPHER SSS DESIGN

Encipher SSS design is obtained by adding a multiplier circuit to SSS design. When in normal function mode (SE=0) SFF loads data from the logic through DI, and the output to logic is DO. Because of the inverter and the XOR gate that are inserted along the scan path, timing of the design is not affected. Thus in function mode, ESSSF works like a traditional scan flip-flop. When in scan test mode, during scan shift operation, the content of FF is XORed with SI to be shifted out to the next SFF and the inverted scan-in data (SI) will be loaded into FF. As a result, during scan in/out, the data that passes ESSSF would be encoded. A binary multiplier is an electronics circuit used in digital electronics to multiply two binary numbers thereby increasing the number of bits. In the security aspects as number of bits increases security level is improved . This is because as key size increases the number of permutations increases thereby making it more complex for the hackers to decipher the information. Multiplier circuit is found to be the best option to increase the key length. A two bit binary multiplier circuit is used in the proposed system.

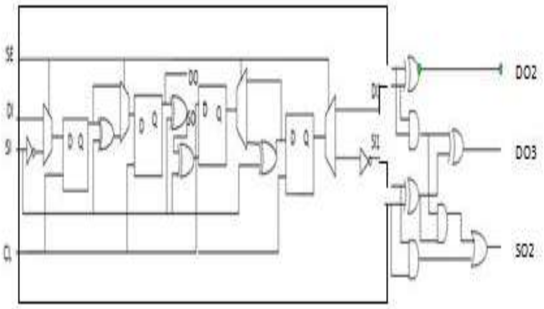
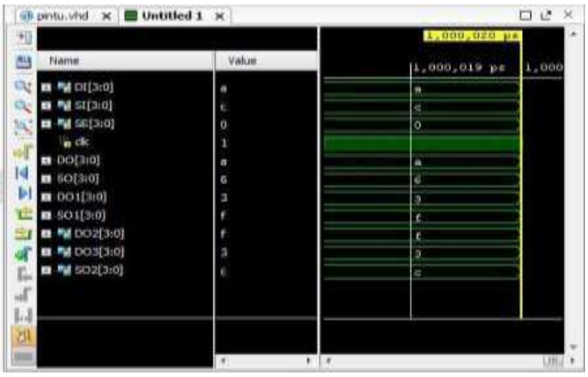


Fig 2: Encipher SSS Design

IV. SIMULATED OUTPUT OF VHDL CODING



```
Name        Value
DI[3:0]     a
SI[3:0]     c
SE[3:0]     0
clk         1
DO[3:0]     a
SO[3:0]     6
DO1[3:0]    3
SO1[3:0]    f
DO2[3:0]    f
DO3[3:0]    3
SO2[3:0]    c
```

V. RESULT AND DISCUSSION

The programs of traditional flip-flop, RSSF and shatter proof secure scan were simulated in Modelsim and Xilinx software. In traditional system, a scan flip-flop and multiplexer is used. So the input data which is given is outputted as such. In case of RSSF additional XOR and NOT gate provides more security to the data which is given as input. Shatter proof is an advanced version of RSSF. ESSSF is the advanced version of SSSF. By using ESSS design into the chip, testing and accessing scan chains are guaranteed to be allowed only by an authorized user. The proposed technique has a negligible area overhead, has no negative impact on chip performance and places several levels of security over the scan chain protecting it from potential attacks. In the system security increases as bit length increases.

VI. CONCLUSION

The simulation result of ESSS design is shown in Fig 3.It is simulated in model sim SE plus 6.2 c. Data input (DI), scan input(SI), scan enable(SE) and clock are inputs to the system. A three bit output is obtained for a two bit input which increases the complexity and thus the security. The encryption on data input depends upon the scan enable and clock.

In this paper, a new Encipher shatterproof secure scan technique is introduced as an effective countermeasure against scan-based differential cryptanalysis. Thus to develop secure test techniques for these crypto cores becomes an emergent task so as to guarantee the security as well as the quality. The proposed scheme can be used to protect the intellectual property of a chip, which is easily compromised using conventional scan chains. The security of the flipped scan chain against scan-based attacks depends on the fact that the attacker is unable to ascertain the structure of the scan chain due to the presence of inverters in the chain. All the advantages and simplicity of traditional scan test are preserved; therefore it is desirable in modern crypto designs as a secure test solution with ignorable design/test overhead.

REFERENCES

[1] Ms.G. Agalya and Mrs.S.Sudha,” VLSI Implementation of Robust Secure Scan based design for differential cryptanalysis” caes journals,vol. 3,Aug 2013.

[2] YouhuaShi,NozomuTogawa,Masao Yanagisawa and Tatsuo Ohtsuki “Robust secure scan design against scan-based differential cryptanalysis” IEEE Trans. on very large scale integration systems, vol. 20.no. 1,Jan 2012.

[3] NeleMenten, LejlaBatina, Bart Preneel, and Ingrid Verbauwhed “A Systematic Evaluation of Compact Hardware Implementatioms for the Rijndael S – box” Sprainger- Verlag Berlin Heidelberg, 2005

[4] Bo YangKaijie Wu and RamwshKarri,” Scan based side channel attack on Data Encryption Standard” Polytechnic University, Brooklyn, NY,11201, 2004.

[5] Basil Varghese and MeeraThamby,” Shatterproof secure scan design against scan-based side channel attacks”. International conference, ICMF 2013.

[6] AES page available via http://www.nist.gov/Crypto Toolkit

[7] Analysis of recent secure scan test technique available via http://dx.doi.org/10.4236/jsea.2016.93008,march 2016.