Indian Journal of Science and Technology, *Vol 7(4S), 28–33, April 2014*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Optimal Hamming Distance Model for Crypto Cores against Side Channel Threats

K. P. Sridhar* **and D. Muralidharan**

VLSI Design, School of Computing, SASTRA University, India; vkpsri@gmail.com, murali@core.sastra.edu

Abstract

Microelectronic crypto devices contain intellectual property like secret data to be protected against side channel attack. Scan chain based attacks come under the category of side channel attack where the hackers attack a scan path through observing and comparing the relationship between intermediate hamming distances values for different test vector patterns. Hence our novel hamming model should overcome the scan based attack and should not give any correlation relationship in hamming distance by providing the similar intermediate values for all test vector patterns which are obtained through an optimal way of inserting Optimal Scan Flip Flop (OSFF) randomly to the scan path chain. Implementation of our proposed integrated circuits is written in Verilog and synthesised with XILINX Spartan III FPGA. The report is compared with Robust Scan Flip Flop (RFSS) hamming model to estimate the overhead of component minimized in OSFF.

Keywords: Crypto Cores, Chip Security, FPGA, Verilog, VLSI Testing

1. Introduction

Hardware implementation of Crypto graphic devices undergoes Side channel attacks due to hackers by stealing the unauthorized content in Large Scale Integration (LSI) chip. Attackers themselves observe the scan data properties like hamming distance in between Scan In and Scan Out. Then manipulate the similarity in these properties for different test patterns. This complex observation leads to discover secret information from the cryptographic systems. There are few systems had been hacked already by attackers[1,2]. Retrieving a secret key in 128 bit AES[1], by focus on the round key element present in discriminator at scan out having only 2^8 possible input key values. The comparisons result of different discriminators help the attackers to hack a secret key even in advanced encryption standard. In elliptic curve cryptography system, finite field binary arithmetic is applied and it requires field point multiplication during decryption and encryption which leads to lot of research in point field multiplications area[1].

Hacking can be performed through ascertaining hamming values observed in elliptic curve cryptography which is done by watching scan chain sequences bit by bit in order to identify the memory element position which specifies the hamming value on it. Utilizing the several different intermediate hamming values, the secret key is determined from the scan path. The observation reports results that an unauthorized key on the elliptic curve cryptographic circuit is determined through 29 arithmetic points over the elliptic curve. Overall time taken to identify the key is just 40 seconds[2]. Hackers can able to use the secret key for different card by designing it similarly and rob the money through the newly designed smart card. Hacker may do an unknown access of internet mobile banking transaction. They can also make the very expensive transactions through the unauthorized key. It indicates that there is the threat in scan chain path leading to attack in cryptography Large Scale Integration (LSI) Chip. Thus it shows the security in crypto devices is needed to be enhanced. Few papers also proposed with secure design against side channel attack.

An inverter[3] is placed randomly to scan chain in order to change the scan out value of scan chain just not like to be a Linear Feedback Shift Register (LFSR). Use of NOT gates or Inverter in the scan chain data path should not

*Author for correspondence

destroy the general operation functionality of the crypto chip. The secure design for the scan path testing is obtained by placing a certain amount of logic inverters between the selected scan paths on flip flop cells. But it protects against the observation of scanned data which determine the intermediate hamming distance values contain in the memory element. This method leads to high timing overhead and NOT gate functionality is identified during Circuit Under Test (CUT).

To reduce the test timing and volume of test data we follow the circular scan method[4]. This method aggravates scan path design chain from the design circuit and it retains the normal scan input node pin for the chip circuit. So there is no need for Automatic Test Equipments (ATE). The output given to Multi Input Signature Register (MISR) is only the varied bits from the part of test vectors on the modified scan chains. But this method also cannot overcome CUT drawback.

Design for Secure Test for Crypto Cores[6] gives solution for crypto cores by appending a enable design flip flop into the conventional scan Flip-Flop. Scan data[7] is dynamically altered through appending the latches to particular flip flop on the scan path but all those above method dose not worried about Hamming distances.

The rest of the paper is arranged as follows. In Section 2, discuss about the drawback of existing system. In Section 3, presents the proposed optimal scan flip flop, implementation and its Hamming distance computation. Section 4, simulation and minimization comparison of optimal and robust model along with their synthesis report and level of security provided are given. Section 5 wrapped up the conclusion of this paper.

2. Existing System

In general scan chain, the Hamming distance is evaluated between scan in and scan out. Differences in Hamming distances for different pattern provide the register position. Hence there is a possibility to guess the secret key which shows that crypto system is attacked by the hacker. This is because of the avalanche effect in crypto graphic algorithm. The avalanche effect state that, when a scan in input is changed slightly, altering a single bit on input then their output needs to be changed significantly where half of the scan out output bits need to be varied. To overcome a Hamming distance based attack a side channel attack in scan chain, the Robust methodology of secured scan design against scan based differential cryptanalysis[5] is architected. In this method the hamming values are given between two scan in inputs which makes it more difficult for the attackers to identify the secret key. Instead of making comparison between scan in and scan out, Hamming distance is observed and compared between two responses. Scan in also called as response. In this method first response is input of scan chain and second response is all possibility combination of scan in pairs from input test pattern, otherwise vector pair from Vector pattern computed from input test pattern.

Testing in LSI circuit can be taken place by two types namely BIST (Built In Self Test) and DFT (Design For Testability). In case of BIST, Vector patterns are induced by automatic test pattern generation tool. But in DFT, we cannot able to generate this Vector patterns inside the circuits. Hence this robust method not suitable for DFT and also consume large time and require more component for computation and high cost. Our proposed Optimal Hamming model overcome this issues where the computation of hamming distance takes place within scan in and scan out providing same level of security which is more complicate for the hackers to guess intermediate values and does not require extra Vector pattern for hamming distance computation.

3. Proposed System

The proposed OSFF design is shown in Figure 1 which contains two modes, traditional mode and functional model. In traditional mode EN = 0, it behaves like a general scan flip flop scan in input is received from DI and scan out is delivered by DO. While in functional mode it act as Optimal Scan Flip Flop (OSFF) encrypt the scan in input SI plain text pattern to produce the cipher text Scan out SO. Before entering into functional mode we need to test the chip at normal mode itself. Once the testing is completed, Functional mode is activated and output SO is always high. OSFF contains extra inverter and XOR gate to the general traditional Scan Flip Flop.

Now OSFF is replaced for Scan Flip Flop (SFF) at randomly in the scan chain on multiples position. In default, we need to replace at first position SFF with OSFF. Then the output of scan chain is encoded. In attacker perspective, it becomes extremely difficult to determine the similarity between outputs. Assume that we want to apply a Test Pattern for Scan In (SI_n, SI_{n-1}, ...SI_2, SI_1, SI_0).

The output of Scan Chain by OSFF flip flop is Scan Output (O_n,O_{n-1},.....O_2,O_1,O_0). For RSFF flip flop the Scan

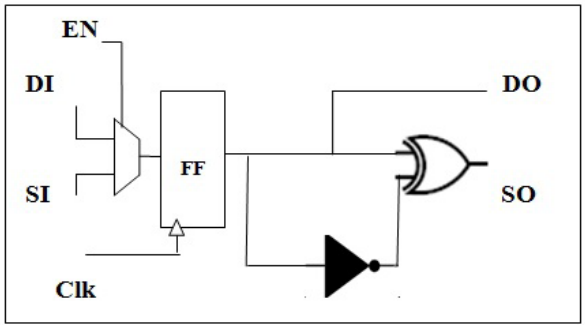

Figure 1. Optimal Scan Flip Flop (OSFF).

Output is $(S_n,S_{n-1},.....S_2,S_1,S_0)$ and additional Test Vector Pattern is given as $(V_n,V_{n-1},.....V_2,V_1,V_0)$. If i numbers of OSFFs flip flop replaced at random positions X of scan flip flop were the scan chain consisting j number of flip flop the scan out is given as,

$$On = (SIn)\ XOR\ (NOT\ SIn) \forall \begin{pmatrix} For\ X = i,\ were\ i = 0\ and\ 1\ or\ 2 & j, \\ Otherwise\ i = 0\ and\ 1\ and\ 2 & j \end{pmatrix}$$

3.1 Computation of Hamming Distance in Optimal

In RFSS, it requires an additional test vector emulated from scan input to provide the same hamming distance for all Scan in inputs. Method for calculating of scan out S_n and vector for RFSS method is presented in paper[5]. However, the result of Vector calculation is shown in Table 1, Hamming computation shown in Table 2 and Table 3 and scan out S_n result is shown at Table 4. But in Optimal method does not require an additional test vector to provide security. For example, we are going to calculate Hamming Distance (HD) for 4 bit pattern. The Test Pattern (TP) consists of 2^4 possibilities of scan in input ($RSI_{0,1..\ n}$) and each scan in input has 2^4 possibility hamming distance. Hence there is 16 x 16 = 256 hamming distances in the test pattern. Hamming distances is the numerical output value between two inputs, state that total number of 1's in output value when we XOR the two input. Let assume that the test pattern consists of Hamming Distance (HD 0, HD 1.... HD N) for each Scan in test vector pattern ($RSI_{0,1..\ n}$) and each Scan in input vector ($SI_{0,1....\ n}$) has a Hamming Distance HD $N_{(0,1..n).}$ Then hamming distance computation by optimal method and overall comparison between RFSS and OSFF is tabulated in Table 4 which shows both the method produce same hamming distances for different input patterns.

Table 1. Test vector computation in RSFF

Cyle	Response	Vector
1	0 0 0 0	0 0 0 1
	0 0 0 1	0 0 0 0
	0 0 1 0	0 0 1 1
	0 0 1 1	0 0 1 0
	0 1 0 0	0 1 0 1
	0 1 0 1	0 1 0 0
	0 1 1 0	0 1 1 1
	0 1 1 1	0 1 1 0
2	1 0 0 0	1 0 0 1
	1 0 0 1	1 0 0 0
	1 0 1 0	1 0 1 1
	1 0 1 1	1 0 1 0
	1 1 0 0	1 1 0 1
	1 1 0 1	1 1 0 0
	1 1 1 0	1 1 1 1
	1 1 1 1	1 1 1 0

Table 2. Flow of HD computation in RFSS

Input	Pair Selection	Direction Towards	Cycle
0 0 0 0	Response	Downwards	1
0 0 0 1	Vector	Downwards	1
0 0 1 0	Response	Upwards	1
0 0 1 1	Vector	Upwards	1
0 1 0 0	Vector	Upwards	1
0 1 0 1	Response	Upwards	1
0 1 1 0	Vector	Downwards	1
0 1 1 1	Response	Downwards	1
1 0 0 0	Response	Downwards	2
1 0 0 1	Vector	Downwards	2
1 0 1 0	Response	Upwards	2
1 0 1 1	Vector	Upwards	2
1 1 0 0	Vector	Upwards	2
1 1 0 1	Response	Upwards	2
1 1 1 0	Vector	Downwards	2
1 1 1 1	Response	Downwards	2

$\forall$ HD 0 to HD N - 2

$$HD\ N(0,1 \ldots n)\ for\ SIn = \begin{bmatrix} On\ XOR\ SIn\ if(SIn = RSIn) \\ SIn\ XOR\ SIn\ if(SIn = RSIn) \\ \forall\ HD\ Nn = SIn\ XOR\ RSIn - 1 \end{bmatrix}$$

$\forall$ HD 0 to HD N - 2

$$HD\ N(0,1 \ldots n)\ for\ SIn = \begin{bmatrix} On\ XOR\ SIn\ if(SIn = RSIn) \\ SIn\ XOR\ SIn\ if(SIn = RSIn) \\ \forall\ HD\ Nn = SIn\ XOR\ RSIn - 2 \end{bmatrix}$$

$\forall$ HD N

$HD\ N(0,1 \ldots n)\ for\ SIn = On\ XOR\ SIn$

Table 3. Sample computation hamming distance in RFSS for first three inputs

Input = 0 0 0 0, d = 0			Input = 0 0 0 1, d = 0			Input = 0 0 1 0, d = 0		
Response	Response Pair (down)	HD	Response	Vector Pair (down)	HD	Response	Response Pair (up)	HD
0 0 0 0	0 0 0 0	0	0 0 0 0	0 0 0 1	1	0 0 0 0	0 0 1 1	2
0 0 0 1	0 0 0 0	1	0 0 0 1	0 0 0 1	0	0 0 0 1	0 0 1 1	1
0 0 1 0	0 0 0 1	2	0 0 1 0	0 0 0 0	1	0 0 1 0	0 0 1 0	0
0 0 1 1	0 0 0 1	1	0 0 1 1	0 0 0 0	2	0 0 1 1	0 0 1 0	1
0 1 0 0	0 0 1 0	2	0 1 0 0	0 0 1 1	3	0 1 0 0	0 0 0 1	2
0 1 0 1	0 0 1 0	3	0 1 0 1	0 0 1 1	2	0 1 0 1	0 0 0 1	1
0 1 1 0	0 0 1 1	2	0 1 1 0	0 0 1 0	1	0 1 1 0	0 0 0 0	2
0 1 1 1	0 0 1 1	1	0 1 1 1	0 0 1 0	2	0 1 1 1	0 0 0 0	3
1 0 0 0	0 1 0 0	2	1 0 0 0	0 1 0 1	3	1 0 0 0	0 1 1 1	4
1 0 0 1	0 1 0 0	3	1 0 0 1	0 1 0 1	2	1 0 0 1	0 1 1 1	3
1 0 1 0	0 1 0 1	4	1 0 1 0	0 1 0 0	3	1 0 1 0	0 1 1 0	2
1 0 1 1	0 1 0 1	3	1 0 1 1	0 1 0 0	4	1 0 1 1	0 1 1 0	3
1 1 0 0	0 1 1 0	2	1 1 0 0	0 1 1 1	3	1 1 0 0	0 1 0 1	2
1 1 0 1	0 1 1 0	3	1 1 0 1	0 1 1 1	2	1 1 0 1	0 1 0 1	1
1 1 1 0	0 1 1 1	2	1 1 1 0	0 1 1 0	1	1 1 1 0	0 1 0 0	2
1 1 1 1	0 1 1 1	1	1 1 1 1	0 1 1 0	2	1 1 1 1	0 1 0 0	3

HD – HAMMING DISTANCE

Downwards (down), Upwards (up)

Table 4. Hamming distance for two different input d = 0 , d = 1

Response					Robust Scan-out				r3	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	Optimal Scan-out				r3	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
									r2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1					r2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
D	r3	r2	r1	r0	s3	s2	s1	s0	r1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	o3	o2	o1	o0	r1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
									r0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1					r0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	0	0	0	1	1	1	0		0	1	2	1	2	3	2	1	2	3	4	3	2	3	2	1	1	1	1	1		0	3	3	2	3	2	2	1	3	2	2	1	2	1	1	3
0	0	0	0	1	1	1	1	1		1	0	1	2	3	2	1	2	3	2	3	4	3	2	1	2	1	1	1	1		4	0	3	2	3	2	2	1	3	2	2	1	2	1	1	4
0	0	0	1	0	1	1	0	1		2	1	0	1	2	1	2	3	4	3	2	3	2	1	2	3	1	1	1	1		4	3	0	2	3	2	2	1	3	2	2	1	2	1	1	2
0	0	0	1	1	1	1	0	0		1	2	1	0	1	2	3	2	3	4	3	2	1	2	3	2	1	1	1	1		4	3	3	0	3	2	2	1	3	2	2	1	2	1	1	3
0	0	1	0	0	1	0	0	0		2	3	2	1	0	1	2	1	2	3	2	1	2	3	4	3	1	1	1	1		4	3	3	2	0	2	2	1	3	2	2	1	2	1	1	2
0	0	1	0	1	1	0	0	1		3	2	1	2	1	0	1	2	3	2	1	2	3	2	3	4	1	1	1	1		4	3	3	2	3	0	2	1	3	2	2	1	2	1	1	3
0	0	1	1	0	1	0	1	1		2	1	2	3	2	1	0	1	2	1	2	3	4	3	2	3	1	1	1	1		4	3	3	2	3	2	0	1	3	2	2	1	2	1	1	1
0	0	1	1	1	1	0	1	0		1	2	3	2	1	2	1	0	1	2	3	2	3	4	3	2	1	1	1	1		4	3	3	2	3	2	2	0	3	2	2	1	2	1	1	2
0	1	0	0	0	0	0	1	0		2	3	4	3	2	3	2	1	0	1	2	1	2	3	2	1	1	1	1	1		4	3	3	2	3	2	2	1	0	2	2	1	2	1	1	2
0	1	0	0	1	0	0	1	1		3	2	3	4	3	2	1	2	1	0	1	2	3	2	1	2	1	1	1	1		4	3	3	2	3	2	2	1	3	0	2	1	2	1	1	3
0	1	0	1	0	0	0	0	1		4	3	2	3	2	1	2	3	2	1	0	1	2	1	2	3	1	1	1	1		4	3	3	2	3	2	2	1	3	2	0	1	2	1	1	1
0	1	0	1	1	0	0	0	0		3	4	3	2	1	2	3	2	1	2	1	0	1	2	3	2	1	1	1	1		4	3	3	2	3	2	2	1	3	2	2	0	2	1	1	2
0	1	1	0	0	0	1	0	0		2	3	2	1	2	3	4	3	2	3	2	1	0	1	2	1	1	1	1	1		4	3	3	2	3	2	2	1	3	2	2	1	0	1	1	1
0	1	1	0	1	0	1	0	1		3	2	1	2	3	2	3	4	3	2	1	2	1	0	1	2	1	1	1	1		4	3	3	2	3	2	2	1	3	2	2	1	2	0	1	2
0	1	1	1	0	0	1	1	1		2	1	2	3	4	3	2	3	2	1	2	1	0	1	2	1	1	1	1	1		4	3	3	2	3	2	2	1	3	2	2	1	2	1	0	2
0	1	1	1	1	0	1	1	0		1	2	3	2	3	4	3	2	1	2	3	2	1	2	1	0	1	1	1	1		4	3	3	2	3	2	2	1	3	2	2	1	2	1	1	0
1	0	0	0	0	0	1	1	0		0	1	2	1	2	3	2	1	2	3	4	3	2	3	2	1	1	1	1	1		0	3	3	2	3	2	2	1	3	2	2	1	2	1	1	3

Hamming distance is same for different inputs d = 0, d = 1 in both the method, but in RFSS the scan out sn is varied for each input. Even if it is varied, output of the entire scan chain is always one this is due to scan control unit at the end of scan path. The control unit produces high value when the circuit is under test (CUT). Hence the job of control unit is obtained in optimal method by placing OSFF compulsory at the end of scan chain. We have already done this, which leads us to get output always high and it is shown in Table 4. Both this system has the demerits where the tested chip cannot perform CUT test again.

Our proposed system obtained high level of security which do not allow a hacker to attack system in case of intermediate hamming distance where it is same for all inputs. Hence it is becoming more complicate for hackers to evaluate the similarity between two computed Hamming distances between two scan input vectors. The advantage of proposed method is mainly focus on minimizing the electronic component overheads which is shown on Table 5. The OSFF model works similarly like conventional scan chains model and does not use any extra test key bits or clock cycles for providing security. Hence our proposed model is applicable for all crypto devices like Smartcard, Credit card, SIM card, TV Set up boxes, etc.

4. Performance Evaluation

The novel Hamming Distance model implemented through Hardware Description Language (HDL) Verilog. Figure 2 shows the Simulation Result of Optimal Method, first the system is runs as normal scan flip flop for input 00000, hamming distance is estimated and the system runs again for same input with optimal scan flip flop by

Table 5. Comparison of robust and optimal synthesis report

Statistics	ROBUST METHOD	OPTIMAL METHOD	Minimized [%]
4x32-bit ROM	1	1	0
Adders/ Subtractors	48	48	0
Registers	532	88	83.45
Comparators	16	0	100
Multiplexers	8	0	100
Number of bonded IOBs	38 out of 124 30%	31 out of 124 25%	16.66
Total REAL time completion	7.00 seconds for Robust Method and 5.00 seconds for Optimal Method		
Total CPU time completion:	7.48 seconds for Robust Method and 5.19 seconds for Optimal Method		

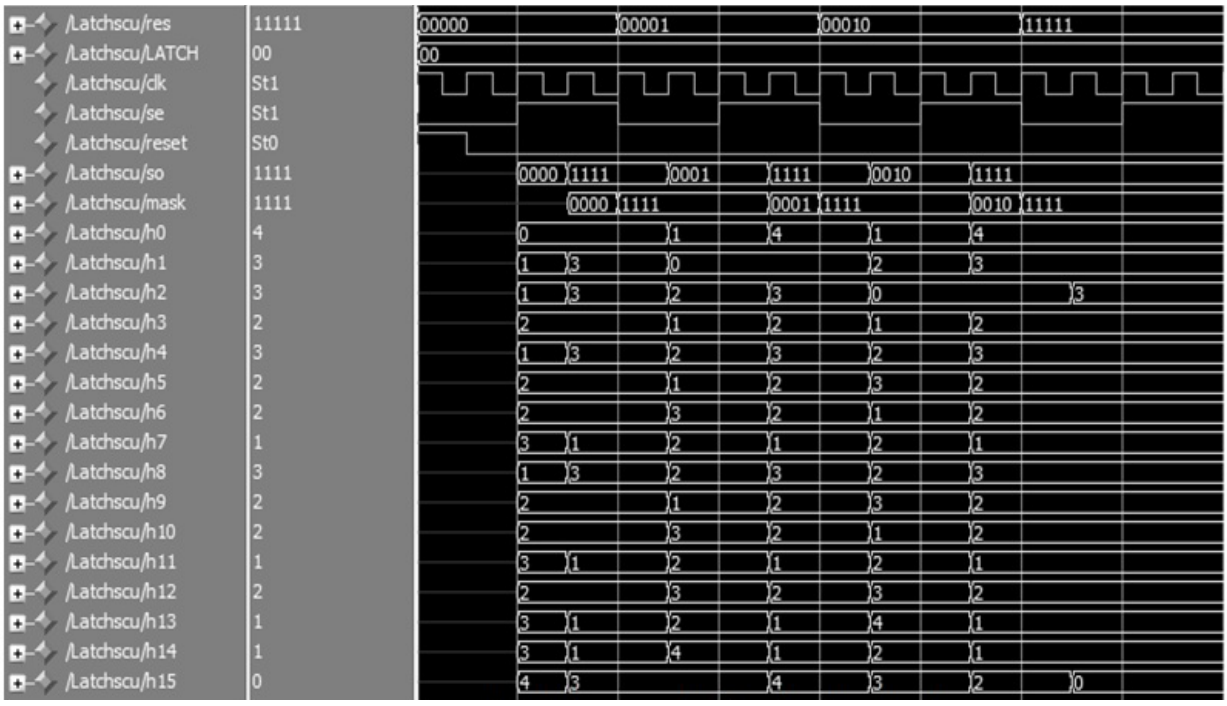

Figure 2. Simulation result of optimal method.

making the Enable EN = 1. The simulation wave form is generated for the four different inputs in both traditional and optimal scan flip flop modes.

The Simulated Verilog code is synthesised by ISE XILINX Design tool using SPARTAN III FPGA (Field Programmable Gated Array) Kit. The synthesis report is generated for both robust and optimal model consisting 256 Hamming distances in desired of showing the minimization of optimal system. Comparison of component utilizations and timing analysis of robust and optimal model is given in Table 5. Figure 3 shows the top level view of RTL Schematic logic of novel optimal hamming model.

4.1 Security Analysis

A scan path chain structure[4] having N registers flipped element and O = (N + 1)/2 Optimal Scan Flip Flop register, the chances to determine the default scan path by an attacker with the known values of N is approximately $1/2^N$. This optimal method providing high security authentication against the two different methods of scan based on differential cryptography attacks called as constant value based and fixed intermediate hamming values based attacks.

Security is provided by means of same intermediate hamming distance for all the Test Pattern. In this method, the finding similarity in the output for two different inputs with minimum 2 bit values is difficult. Hence we provided the security, protection against side channel attack. Binomial expression for the chances of hackers to successfully finding the path of the scan chain is approximately,

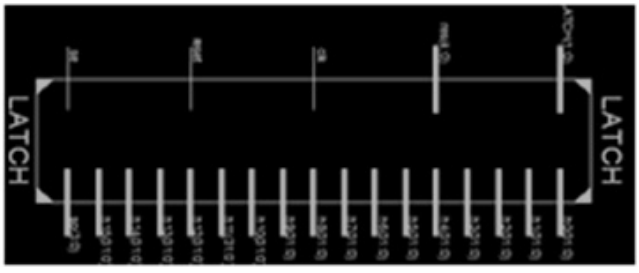

Figure 3. View of RTL schematic for optimal model.

N = Scan flip flops, O = Optimal Scan Flip Flop

Hence we can stores the valuable and sensitive binary data information on a chip with high level security.

5. Conclusion

In this paper, a novel optimal hamming distance model and secure scan method is applied which provides an effective countermeasure against scan based attacks in scan path. The probability of hackers to successfully guessing the scan chain structure is very difficult which shows the security level of the proposed system. It could be fully compatible with all cryptanalysis devices with less amount of component overhead along with the traditional general scan system.

6. References

1. Nara R. Scan-based attacks against cryptography lsis and their countermeasure; 2011.
2. Nara R, Togawa N, Yanagisawa M, Ohtsuki T. Scan-based attack against elliptic curve cryptosystems, design automation conference. 15th Asia and South Pacific Design Automation Conference (ASP-DAC); 2010 Jan 18–21; Taipei. IEEE. p. 407–12.
3. Sengar G, Mukhopadhyay D, Chowdhury DR. Secured flipped scan-chain model for crypto-architecture. IEEE Trans Comput Aided Des Integrated Circ Syst. 2007; 26(11):2080–84.
4. Arslan B, Orailoglu A. Circularscan: a scan architecture for test cost reduction. Proceedings Design, Automation and Test in Europe Conference and Exhibition; 2004 Feb 16–20. IEEE. 1290–95.
5. Shi Y, Togawa N, Yanagisawa M, Ohtsuki T. Robust secure scan design against scan-based differential cryptanalysis. IEEE Transactions on Very Large Scale Integration Systems. 2012; 20(1):176–81.
6. Shi Y, Togawa N, Yanagisawa M, Ohtsuki T. Design-for-secure-test for crypto cores. ITC 2009. International Test Conference; 2009 Nov 1–6; Austin, TX. IEEE. 1.
7. Atobet Y, Shi Y, Yanagisawa M, Togawat N. Dynamically changeable secure scan architecture against scan-based side channel attack. IEEE Soc Design Conference; 2012 Nov 4–7; Jeju Island. IEEE. p. 155–58.