Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip

Sivasankaran Saravanan[1(✉)], Mikias Hailu[2], G. Mohammed Gouse[3], Mohan Lavanya[4], and R. Vijaysai[4]

[1] College of Engineering, Debre Berhan University, Debre Berhan, Ethiopia
saran@dbu.edu.et
[2] Electrical and Computer Engineering Department, Debre Berhan University, Debre Berhan, Ethiopia
hailumikias@dbu.edu.et
[3] College of Computing, Debre Berhan University, Debre Berhan, Ethiopia
galety.143@dbu.edu.et
[4] School of Computing, SASTRA Deemed University, Thanjavur, Tamilnadu, India
m_lavanyass@ict.sastra.edu, vijaysai@it.sastra.edu

Abstract. Present crypto based smart systems very popular for secure application. But all this system was targeted by various threats, malfunctions, hacking and side channel attack. Cryptography algorithm will try to give secure in data encryption and decryption but failed in direct hardware implementation. This paper provides an optimized secure testing method against side channel attack in crypto chips. This proposed system reduces the switching activity in latches and also reduces the power consumption in architecture. It avoids unwanted latches to obtain optimization in area by random insertion of scan chain design. This optimized architecture was targeted to RSA crypto algorithm to show the effectiveness of the proposed method over various existing methods.

Keywords: Cryptography algorithms · Side channel attack · Secure testing · Crypto chips

1 Introduction

Crypto-devices like Smartcards, Credit cards, SIM cards had a rapid growth in usage [1], similarly threats on reliability of such devices has raised concern due to side channel attack. LSI (Large Scale Integration) in Crypto-devices exhibit a secure architecture to achieve a user-friendly communication. Hence security can be obtained by use of cryptography algorithm such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA, Elliptic Curve Cryptography (ECC) to encrypt/decrypt important data. AES and DES are Symmetric key crypto-systems which make use of the same secret key in encryption and decryption. However, it may be difficult to securely share the same secret key while in communication. RSA and ECC Public-key cryptosystem, on the other hand, make use of different keys to encrypt and decrypt so

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019
Published by Springer Nature Switzerland AG 2019. All Rights Reserved
F. A. Zimale et al. (Eds.): ICAST 2018, LNICST 274, pp. 410–417, 2019.
https://doi.org/10.1007/978-3-030-15357-1_34

that it solves the key sharing problem. Still we cannot able to implement cryptography technique directly onto an LSI itself.

It may be applicable along with memories, processors, I/O's, and control circuits. Then it's quite possible that a scan path includes random elements caused by memories, processors, I/O's, and control circuits other than registers of cryptography circuits storing the intermediate values. Although cryptographic algorithm is used, there is a threat on LSI chip to deciphered a secret key from crypto-devices. Scan-based attack is a method to retrieve a secret key from the scanned data obtained from the scan path in the cryptography LSI chip. Therefore, without any compromise in testing and security it is necessary to develop secure scan architecture against scan-based attack. Testing in LSI circuit can be take place by two types BIST (Built In Self-Test) and DFT (Design For Testability). BIST is more secure because it does not require visible scan chains, but BIST incurs more overhead and yields less fault coverage when compared to scan-based DFT. It has high fault coverage and least hardware overhead. However, scan chains are open and visible to use. Hence, this paper focuses on crypto-chip testing by DFT. Already crypto-chip have been hacked by Scan-based Attacks against Cryptography LSIs and their Counter-measure [2].

2 Existing System

Few papers had been proposed with secure design against side channel attack, in this some of the proposed methods make scan path unusable for attackers by limiting scan path control. Side Channel Attack on Dedicated Hardware Implementations of DES was discussed in paper [3], by loading pairs of known plaintexts with one-bit difference in the normal mode and then scanning out the internal state in the test mode, which determine the position of all scan elements in the scan chain. In paper [4], scan-based attack against ECC was elaborated. In paper [5], instead of secret key, test key is used in test mode to prevent scan-based attack. However, by doing this will limit the test application, which is because it doesn't support at-speed online testing. In paper [6], an inverter is placed randomly to scan chain and test controller limit the use of scan chain by comparing scan in with the pre-set value when the circuit is designed.

To reduce the test timing and volume of test data we follow the circular scan method [7]. This method increases scan chain count exponentially in the circuit while retaining the original scan input pin count. Hence no necessity for high cost Automatic Test Equipment (ATEs). Output is given to Multi-Input Signature Register (MISR) were only the varying bits of a test slice in the new scan chains is updated for each shift cycle. In paper [8], Secure Scan and Secure chip technique is introduced for DFT were the comparison scan chain cannot perform directly for retrieving the secret key but this method uses large amount of electronic component in terms of multipliers and flip flops. Robust Secure Scan Design Against Scan-Based Differential Cryptanalysis [9], efficient spatial dependency method but has a drawback in internal scan structure still able to hack by using reset-based scan or flush test. In paper [10], Design-for-Secure-Test for Crypto Cores by adding a stimulus launched flip-flop into the traditional scan flip-flop to maintain the high-test quality without compromising the security but result in hardware overhead. In paper [12, 14] discussed about side channel attack in SM9 method. Cache

based side channel attack was elaborated in paper [13]. In paper [18], bit level power consistency analysis in hardware Trojan was discussed. A hardware Trojan attack on FPGA based cryptographic key generation was explained in paper [19].

In paper [11], secure scan architecture against scan-based attack by using SDSFF (State Dependent Scan Flip-Flop) is proposed as in Fig. 1. In SDSFF, an XOR and a latch are integrated into a traditional scan FF to increase the security of scan chain. The latch memorizing a past state of the scan FF can change a scan FF output. According to the load signal, the value of the latch could be updated. By doing this, the structure of scan chain could be dynamically changed even after it is designed. Hacker cannot know the value updated in latch, so that the SDSFF can't be operated by attackers. Hence our proposed Optimized Scan Flip Flop (OSFF) will reduce the switching activity in latches which leads us to reduce the power consumption in architecture, by reducing the unwanted latches we can obtain optimization in area. Hence latches should insert randomly to scan chain design. The optimized architecture was emulated on RSA to show the effectiveness of the proposed method.

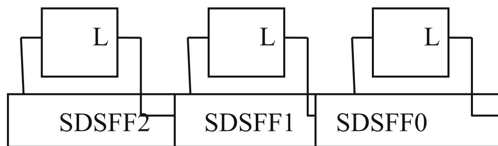

Fig. 1. Block diagram of existing system [11]

3 Proposed Architecture

Optimized architecture design is to encrypt and decrypt data in scan chain were hacker cannot able to observe the working functionality of flip flops. Hence its complicated for unintended user to find the difference between pair of plaintext. The proposed architecture OSFF design is shown in Fig. 2. Along with traditional flip flop, in addition it contains Single Latch and XOR Gate. As it contains two working mode, normal mode and test mode. In normal mode, its act like a general flip flop were the input and output value are same but differ in clock pulse. In test mode its act like OSFF flip flop output is depend upon latch value.

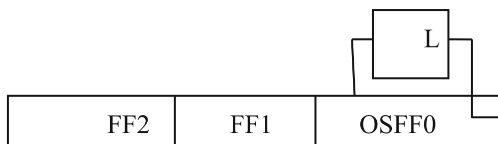

Fig. 2. Proposed block diagram

Example: Scan chain model which consists of OSFFs in the first position shown in Figs. 3 and 4. Table 1 shows the changes in scan output data where it depends upon

latches. Here test vector of Scan In data is taken as SI = S3, S2, S1, S0 and DI = D3, D2, D1, D0, all this four bit vector produce Scan Out depends upon Latch Enable. If EN is 0 then the scan chain performs as normal mode else its act in test mode.

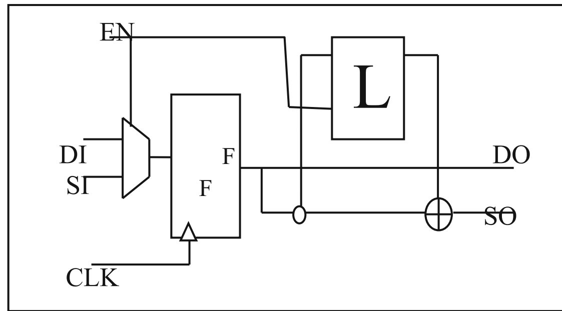

Fig. 3. Basic block of the proposed method

The latch (L) is always presented in the test-mode. The output in test-mode depends upon the number of latch presented in that scan chain. If total number of latches inserted to scan chain is even then input is equal to output otherwise output was inverted from the applied input. Selection between the mode is take place by Enable (En), which is also load signal for latch. By doing this we can able to operate the latch only at test-mode. Here, latch is inserted randomly to scan structure no need to replace a flip flop with OSFF. Assume that latch is attached in j^{th} flip flop of scan chain, then j^{th} flip flop is called as OSFF flip flop. All existing system, have need to replace the flip flop in scan chain but our proposed system not required the replacement which give us additional advantage. Now apply a test vector to the optimized architecture as,

Test Vector V = (V_{N-1}, V_{N-2}, …..V_2, V_1, V_0).
Response R = (R_{N-1}, R_{N-2}, ….R_2, R_1, R_0).
Scan In SI = (SI_{N-1}, SI_{N-2} …. SI_2, SI_1, SI_0).
Scan Out SO = (SO_{N-1}, SO_{N-2} …. SO_2, SO_1, SO_0).

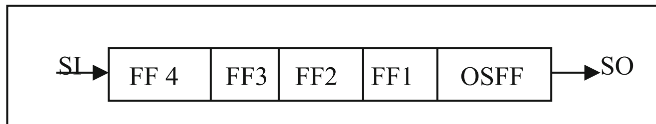

Fig. 4. Scan chain with OSFFs

Table 1. Changes in scan out

Scan in		Scan out	
		EN = 0	EN = 1
SI	DI	DO	SO
S3, S2, S1, S0	D3, D2, D1, D0	D3, D2, D1, D0	S3′, S2′, S1′, S0′
S3, S2, S1, S0	D3, D2′, D2, D1	D3, D2′, D2, D1	S3′, S2′, S1′, S0
0010	0001	0001	1101
1111	000	000	0000

Hence $SO_{[i]}$ will depends latch, if latch is enabled otherwise, latch is disabled.

Pseudo code:

```
If  ~ (EN)
{    DO [ i ] = DI [ i ] ;
     DO [ i + 1] = DI [ i+1]; ......
     DO [ i + (n-1)] = DI[i + ( n-1 )];  // i =  LSB
     DO [ i + n] = DI [ i + n];            //  n =  MSB
}   Else
{   N = 1                          //  i = Current Flip Flop Position
  For (i =0; i<j;i= i+1)               //  j=Total no of Flip Flop
     N = N+1;             //  N = Total number of  Latches
     If (N % 2 == 0) then {
     if (L == ‘ 0 ‘ and  i == ‘ 0 ‘ ) then  process State 1
     else if (L ==‘ 1 ‘ and  i == ‘ 0 ‘ )then process State2
     else if (L ==‘ 0 ‘ and  i == ‘ 1 ‘ )then process State1
     else (L ==‘ 1 ‘and  i == ‘ 1 ‘ )then process State2 }
    else  {
     if (L == ‘ 0 ‘ and  i == ‘ 0 ‘ ) then  process State 2
    else if ( L ==‘ 1 ‘ and  i == ‘ 0 ‘ )then process State1
    else if ( L ==‘ 0 ‘ and  i == ‘ 0 ‘ )then process State2
    else (L ==‘ 1 ‘ and  i == ‘ 1 ‘ )then process State1}
    Process (State 1) {SO [i] = ((SI [i]) ^ L);
    SO [ i + 1] = ((SI [i + 1]) ^ L);
    SO [ i + (n-1)] = (SI [i+( n-1)] ^ L);
    SO [ i + n] = (SI [i + n] ^ L);}
    Process (State 2) {SO [i] = ~ ((SI [i]) ^ L);
    SO [ i + 1] = ~ ((SI [ i + 1]) ^ L);
    SO [ i + (n-1)] = ~ (SI [i+( n-1)] ^ L);
    SO [ i + n] = ~ (SI [ i + n] ^ L);}
```

L = Value of Latch either 0 or 1,were Value of Latch L = SI [Previous Bit Value].

In SDSFF, Total number of Flip Flop is always equal to Total number of Latch. In SDSFF Scan Out SO[i] = SI[i] ^ L[i] ^ L[i − 1] ^ L [i − 2]…… (Untilli = 0). OSFF Scan Out: SO[i] = SI[i] ^ L[i]. To increase the security level we can increase the latch

randomly to the scan chain, but this would not affect the test time because in SDSFF we want add the N numbers of content in N latches to the value of flip flop, for finding the output of Nth flip flop which take large amount of time and operation [11]. But in our proposed method, were the scan chain containing N number of Latches for M numbers of flip flop (were N is always less than M), We count the total number of latches N, if N modulus of 2 is equal to 0 then output is equal to input else output is equal to inverse of input. In normal mode, DI is given as input and output DO is produced as same as input working like general flip flop.

In test mode, SI is given as input and output SO is produced based on value of Latch. Total number of latch is even then, SO = SI if its add SO = ∼SI were SI is XOR ed with LATCH L. The existing state dependent scan flip flop method uses N number of latch for N number of flip-flops. However, our proposed optimized method uses random number of latch for N number of flip flops were shown in Fig. 3. Hence total number of transaction to compute scan out in proposed method is very less when compared to state dependent flip flop. This help us to reduce the consumption of power. Total number of latches used to compute output in state dependent flip flop is high. Overall usage of number of latch in proposed system is less, hence total area is reduced in our LSI circuit.

4 Experimental Result

The optimized architecture was implemented on 512-bit RSA. It was simulated, synthesis using VHDL and targeted to SPARTAN 3 on Xilinx software. Result report was tabulated on Tables 2 and 3. RSA cryptographic processor architecture is based on Montgomery Algorithm. This architecture made the processing time faster and used for comparatively smaller amount of area space in the FPGA [15–17].

Table 2. Scan chain of single SDSFF and OSFF

Components utilization	Slices	Flip flops	4 input LUTs
Basic RSA (512-bit)	11090	8132	19748
SDSFF [11]	11170	8244	19860
Proposed OSFF	11170	8228	19844

Table 3. Scan chain of multiple SDSFF and OSFF

Scan-chain content	Total number of latches	Overhead [%]	Delay [%]
Proposed OSFF	4/16/32	0	4.83
SDSFF	4	0.135	4.83
SDSFF	16	0.274	4.83
SDSFF	32	0.551	4.83

Proposed method targets to optimized architecture design for both the functions of encrypt and decrypt data in scan chain. It promises to complicate the user to find the changes between pair of plaintext information. The proposed architecture OSFF, designed along with basic flip flop latch and xor logic. To implement our proposed method, inserting the latch at the fourth position was observed and synthesis report is generated. Similarly, now replace fourth position flip flop with SDSFF and report is taken which show the overhead of flip flop and LUTs in Table 2.

Table 3 show the result of SDSFF overhead comparison with OSFF when the scan chain containing 4, 16, 32 SDFF and OSFF. Overall critical path delay is same, hence the test time will remain same in both the method. Analyzing the security for OSFF based design were the possibility to discover a secret key through scan chains using known scan-based attack is to know the number of OSFFs. The random positions of inserted latch were the data in latches changes from time to time. However, all of these are not known to attackers which make impossible or at least very difficult for them to discover through scan operations.

5 Conclusion

Crypto-chips are very popular in secure applications but it also targeted for various attacks. Side channel attack is one of the attack which focuses in this paper. Proposed work provides an efficient secure to prevent side channel attack, which is caused by various parameters. This proposed system saves power by reduces unnecessary switching. Area optimization is also achieved in this method. Experimental results show that proposed method is very useful for reduced area optimization without compromising time. Thus, this method will be well fit to prevent side channel attack with efficient area. Using this method along with high speed design is recommended for future research work.

References

1. Thomasson, J.P., Baldi, L.: Smartcards: portable security. In: Innovative Systems in Silicon Conference, pp. 259–265. IEEE (1997)
2. Ryuta, N.: Scan-based attacks against cryptography LSIs and their countermeasure, ICSLABS (2011)
3. Yang, B., Wu, K., Karri, R.: Scan based side channel attack on dedicated hardware implementations of data encryption standard. In: ITC International Test Conference (2004)
4. Nara, R., Togawa, N., Yanagisawa, M., Ohtsuki, T.: Scan-Based Attack Against Elliptic Curve Cryptosystems, IEEE Conference (2010)
5. Yang, B., Wu, K., Karri, R.: Secure scan: a design-for-test architecture for crypto chips. IEEE Trans. Comput. Aided Des. Integr. Circ. Syst. **25**(10), 2287–2293 (2006)
6. Sengar, G., Mukhopadhyay, D., Chowdhury, D.R.: Secured flipped scan-chain model for crypto-architecture. IEEE Trans. Comput. Aided Des. Integr. Circ. Syst. **26**(11), 2080–2084 (2007)

7. Arslan, B., Orailoglu, A.: Circular scan: a scan architecture for test cost reduction. In: Proceedings of the Design, Automation and Test in Europe Conference and Exhibition. IEEE (2004)
8. Hely, D., Flottes, M.L., Bancel, F., Rouzeyre, B., Berard, N., Renovell, M.: Scan design and secure chip. In: Proceedings of the 10th IEEE International On-Line Testing Symposium (IOLTS 2004) (2004)
9. Shi, Y., Togawa, N., Yanagisawa, M., Ohtsuki, T.: Robust secure scan design against scan-based differential cryptanalysis. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **20**(1), 176–181 (2012)
10. Shi, Y., Togawa, N., Yanagisawa, M., Ohtsuki, T.: Design-For-Secure-Test for Crypto Cores, International Test Conference (2009)
11. Atobet, Y., Shi, Y., Yanagisawa, M., Togawat, N.: Dynamically Changeable Secure Scan Architecture Against Scan-Based Side Channel Attack, IEEE Conference (2012)
12. Zhang, Q., et al.: Side channel attacks and countermeasures for identity based cryptographic algorithm SM9, Security and communication networks (2018)
13. Yarom, Y., Falkner, K.: FLUSH + RELOAD: a high resolution, low noise, L3 cache side channel attack. In: USENIX Security Symposium (2014)
14. Yuan, F., Cheng, Z.: Overview on SM9 identity-based cryptographic algorithm. J. Inf. Secur. Res. **2**, 1008–1027 (2016)
15. Anand, A., Praveen, P.: Implementation of RSA algorithm on FPGA. Int. J. Eng. Res. Technol. (IJERT) **1**(5), 1–5 (2012)
16. Sahu, S.K., Pradhan, M.: FPGA implementation of RSA encryption system. Int. J. Comput. Appl. **19**(9), 10–12 (2011)
17. Ibrahimy, M.I., Reaz, M.B.I., Asaduzzaman, K., Hussain, S.: FPGA implementation of RSA encryption engine with flexible key size. Int. J. Commun. **3**(1), 107–113 (2007)
18. Zhang, Y., Quan, H., Li, X., Chen, K.: Golden free processor hardware Trojan detection using bit power consistency analysis. J. Electron. Test. **34**(3), 305–312 (2018)
19. Govindan, V., Chakraborty, R.S., Santikellur, P., Chandhary, A.K.: A hardware Trojan attack on FPGA based cryptographic key generation: impact and detection. J. Hardw. Syst. Secur. **2**, 225–239 (2018)