DPA Resistant AES Using a True Random Based LFSR Technique

Reenu Tomy[1], Vinoj P.G.[2]

[1]M.Tech Student, Department of Electronics and Communication Engineering, SCMS School of Engineering and Technology, Karukuuty, Cochin, Kerala, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, SCMS School of Engineering and Technology, Karukuuty, Cochin, Kerala, India

Abstract: ***Advanced Encryption Standard (AES) is an algorithm, which is used to protect data, which uses cipher key in order to protect the data block. However this is vulnerable to Differential Power Attack (DPA) . In order to protect AES from DPA attack we can use masked AES technique, which is implemented in this paper. In first order masked AES we are removing the correlation between the intermediate result and the secret key. One of the main drawback of this method is large area consumption. We can alleviate this problem by introducing randomness in to it by using LFSR. The comparison between both the architectures are made on the basis of the power rating estimated using Xilinx ISE tool.***

Keywords: Advanced Encryption Standard (AES), Differential Power Analysis (DPA), Masking

1. Introduction

One of the relatively recent and very powerful form of attack against cryptographic devices are physical attacks. Physical attacks are mainly side channel attacks, which exploits the side channel information mainly time, power consumption and electromagnetic emission. When the attack is based on the power consumption, it is mainly called Power Analysis Attack. It is very powerful which does not require the detailed knowledge of the implementation of the device. Differential Power Analysis has become a major threat to crypto chips since it can effectively extract the secret key. There are several methods to resist the DPA attack, but most of the techniques require large hardware and time consuming. DPA attack can extract the secret key using the power consumption information.

In order to prevent the attack of AES against DPA attack we can use the method of randomness, which randomizes all the intermediate results that occur during the computation of the algorithm. This can be done by adding random values to the intermediate results and this is often called masking. In this paper we are dealing with the first order masked AES its disadvantageous and further improvement that could be made in this masking. We must remove the correlation between the intermediate value and the secret key in order to resist the DPA attack. One of the disadvantage of the masked AES is the area required. It is more complicated due to the extra area required to perform the masking fuhnctions. In masking functions the intermediate value is concealed by XOR ing with mask which is random value.

It has been proposed that the first order masked AES has been successfully attacked by higher order attacks. They can successfully retrieve the private key using second order DPA attack. Refined DPA attack can secretly retrieve the secret key. Masking is a common method used to prevent differential power analysis (DPA) attack. However, first-order masking cannot prevent higher-order DPA attacks. Higher-order masking should be implemented. Hardware accelerator based higher-order masking has performance higher, but it uses large area. General purpose processor (GPP) based higher-order masking is efficient in area, but it is not able to meet performance requirements.

2. Literature Survey

The literature survey focuses its attention towards AES, to utilize under low power consumption, security enhancement, better performance and greater efficiency. Karri, Wu, K., Mishra, and Kim, (2002) found Error Detection Schemes for Fault-Based Side-Channel Cryptography of Block Ciphers which are symmetric in nature . They presented algorithm level, round level, and operation level CED (Concurrent Error Detection) architectures for block ciphers which are symmetric in nature. The algorithm was independent in nature and can be applied to almost any block cipher which are symmetric. The proposed scheme presents moderate area overhead and interconnects to produce permanent as well as transient fault tolerance. This technology assumes that the key RAM, comparator, or both encryption and decryption modules simultaneously are not under attack or faulty

The implementation capability in VLSI environment is also studied and analyzed in depth. Farhadian.A and Aref.M.R (2009) presented good method for simplifying and approximating the s-boxes based on power functions . This paper deals with cipher algorithms, power functions over finite fields and special inversion functions have a good role in the S-box design structure. A new systematic effective method is introduced to crypt analyze such S-boxes. This method is very simple and does not need any attempt and can be considered as a quick criterion to find some simple calculations. Using this new method, approximations can be obtained for advanced encryption standard (AES) like S-boxes, such as AES. Finally as an application of this method, a simple linear approximation for AES S-box is introduced.

Akashi Satoh, Sumio Morioka, and Seiji Munetoh (2011) introduced a Compact Rijndael Hardware Architecture with S-Box Optimization. Data paths are encrypted and decrypted and all arithmetic components are used again. A very small size of 5.4 K gates is resulted for a 128-bit key Rijndael circuit using a 0.11-µm CMOS standard. To reduce the hardware size, the order of the arithmetic functions were changed, and the encryption-decryption data paths are very well combined with respect to cell library. Logic optimization techniques were applied to the arithmetic components, and gate counts were reduced.

Ashkan Masoomi and Roozbeh (2012) presented a new approach for detecting and solving errors in satellite communications using Hamming Error Correcting Code . A premium model to detect and resolve Single Event Upsets in on-board implementations of the AES algorithm was depend on hamming error correcting code. Single Even Upset (SEU) faults occur in the on-board during encryption because of radiation. Some of the AES modes like ECB, CBC, OFB, CFB and CTR performances have been verified. From that, CTR mode has been recommended as the good choice for satellites

Ramesh Babu, George and Kiransinh (2012) presented a Securing Distributed Systems Using Symmetric Key Cryptography . It was used to find the privilege of Symmetric Key Cryptography for Security in Distributed Systems. The key cryptographic algorithms DES and AES were used commonly. The DES and AES algorithms were evaluated on the measures such as size of the key, size of the block, number of iterations etc. From the review of the literatures of various implementations and analysis of AES and DES, it can be concluded that AES algorithm has supreme qualities over the DES algorithm in many areas.

3. Architecture for First Order Masked AES

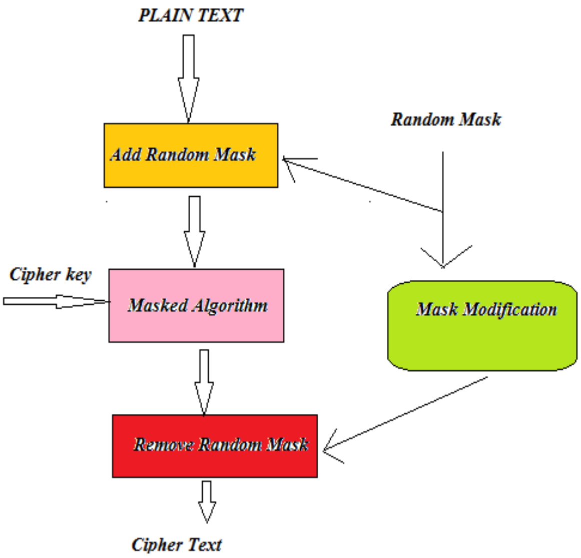


Figure 1: Architecture of First order masked AES

For removing the DPA attacks, we need to destroy the correlation between intermediate results and the secret key. The masked AES is more difficult due to extra area required to do the masking functions. In the masked implementation, the intermediate value is covered by exclusive-oring (XOR) it with the random mask m . In the round function of the AES design, linear transformations are ShiftRows, MixColumns, and AddRoundKey. while SubBytes is the only nonlinear transformation. Linear_Op is defined as the linear transformation, therefore, masking Linear_Op with m is shown as follows

Linear_Op(x xor m) = Linear_op(x) xor Oper (m)

The SubBytes which is non linear operation is defined as S-box, which should have the following character
S – box(x xor m) not equal to S – box(x) xor S – box(m)

The new S-box denoted as S – box' recomputed as follows
S – box' (x xor m) = S – box(x) xor m'

m' and m are the output and input masks bytes of the Subbytes. It holds

m' = S – box(m)

Generally, it needs 6 byte random values to mask a 128- bit AES . This masking method is known as first-order asking. It might be broken by higher-order DPA attacks.

Masked AES was simulated in MODELSIM SE 6.3f

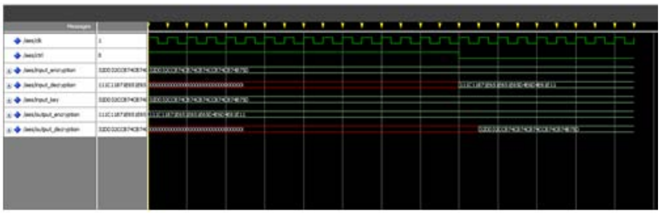


Figure 2: Simulation result of First order Masked AES

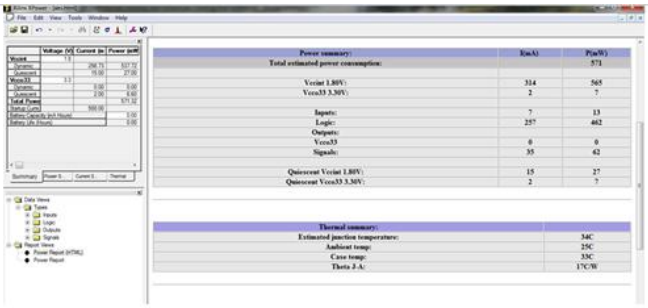
Fig 2 shows the simulated ouput of first order masked AES. The simulation results of AES steps including Add_round key, Matrix Multiplication, Shift row and substitution all are shown together . The power and area of the existing masked AES is calculated. . This can be calculated by Simulating in Xilinx ISE 8.1i. Design Summary of first order masked AES is shown below:

Total equivalent gate count for design: 20,230

Logic Distribution:
Number of occupied Slices: 1,217 out of 6,912 17%

Number of Slices containing only related logic: 1217 out of 1217 100%

Number of Slices containing unrelated logic: 0 out of 1217 0%



Power summary:	I(mA)	P(mW)
Total estimated power consumption:		571
Vccint 1.80V:	314	565
Vcco33 3.30V:	2	7
Inputs:	7	13
Logic:	257	462
Outputs:		
Vcco33	0	0
Signals:	35	62
Quiescent Vccint 1.80V:	15	27
Quiescent Vcco33 3.30V:	2	7

Thermal summary:	
Estimated junction temperature:	34C
Ambient temp:	25C
Case temp:	33C
Theta J-A:	17C/W

Figure 3: Power rating of First Order Masked AES

Fig 3 shows the power analysis in the case first order masked AES. The power rating has been estimated using Xilinx ISE 8.1 and the total estimated power consumption was found to be 571mw.The major drawback here in the existing method that is first order masked AES, we need 128 bit XOR gates so the total number of gates become more than 10,000 nearly 20,000

4. Architecture of Modified AES

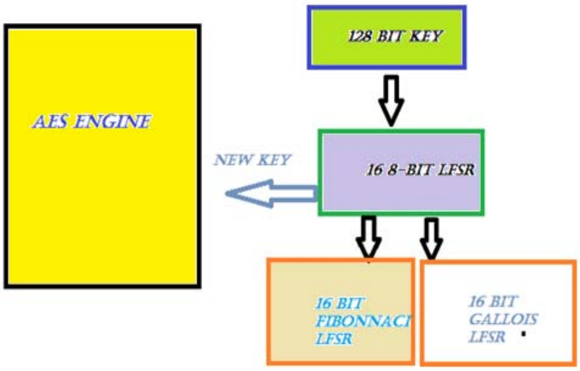
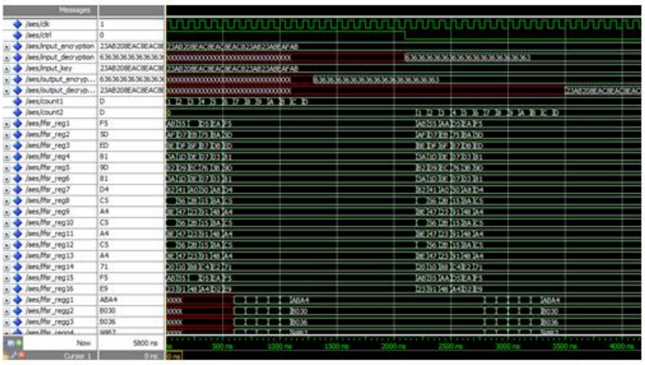


Figure 4: Architecture of Modified AES

Instead of using this XOR gate we will go for new method of randomness using LFSR ie Linear Feedback Shift Register. n. Linear feedback shift registers (LFSRs) provide an economical, fast, and efficient method for generating a wide variety of pseudorandom sequences. A different architecture that incorporates a true random number generator is proposed not only to counteract the DPA attack but also we can generate a true sequence which is random. With the proposed architecture, the AES engines security level can be further enhanced while the area overhead can be also reduced. The DPA attack correlation between the leaked power information can be calculated using the statistical analysis and the predicted power consumption. Noises can be removed by statistical analysis and therefore, the DPA attack can still be successfully do even in a noisy environment .The secret key of a cryptographic circuit can be is closed from the correlation index of the analysis result.

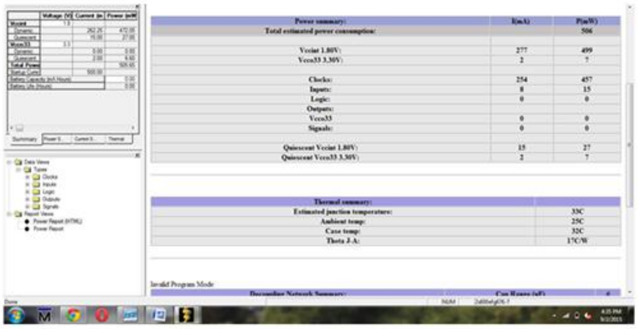
.



```
Messages
/aes/clk                  1
/aes/ctrl                 0
/aes/input_encryption     23AB208EAC8EAC8
/aes/input_decryption     636363636363636
/aes/input_key            23AB208EAC8EAC8
/aes/output_encryp...     636363636363636
/aes/output_decryp...     23AB208EAC8EAC8
/aes/count1               D
/aes/count2               D
/aes/lfsr_reg1            F5
/aes/lfsr_reg2            5D
/aes/lfsr_reg3            ED
/aes/lfsr_reg4            81
/aes/lfsr_reg5            9D
/aes/lfsr_reg6            81
/aes/lfsr_reg7            D4
/aes/lfsr_reg8            C5
/aes/lfsr_reg9            A4
/aes/lfsr_reg10           C5
/aes/lfsr_reg11           A4
/aes/lfsr_reg12           C5
/aes/lfsr_reg13           A4
/aes/lfsr_reg14           71
/aes/lfsr_reg15           F5
/aes/lfsr_reg16           E9
/aes/lfsr_regg1           ABA4
/aes/lfsr_regg2           B030
/aes/lfsr_regg3           B036
          Now             5800 ns
      Cursor 1            0 ns
```

Figure 5: Simulation result of modified AES

Fig 5 shows the 5-bit simulation result of modified AES. The simulation was performed using ModelSim 6.3f. The simulation shows that the number of gate count is drastically reduced and thus the area and power has been reduced.



Power summary:	I(mA)	P(mW)
Total estimated power consumption:		506
Vccint 1.80V:	277	499
Vcco33 3.30V:	2	7
Clocks:	254	457
Inputs:	8	15
Logic:	0	0
Outputs:		
Vcco33	0	0
Signals:	0	0
Quiescent Vccint 1.80V:	15	27
Quiescent Vcco33 3.30V:	2	7

Thermal summary:	
Estimated junction temperature:	33C
Ambient temp:	25C
Case temp:	32C
Theta J-A:	17C/W

Invalid Program Mode

Figure 6: Power rating of modified AES

Fig 6 shows the power analysis in the case of modified AES. The power rating has been estimated using Xilinx ISE 8.1 and the total estimated power consumption was found to be 506mw.

5. Inferences

Power is calculated in milli Watt (mW) and the comparison is calculated. The table 1 gives the power of both architectures. It shows that modified AES requires minimal power. Here power is reduced by several mW using proposed architecture when compared to existing architecture which is based on the LFSR based AES

Table 1: Power consumption

TYPE	POWER
MASKED AES	571
MODIFIED AES	506

Table 2 indicates the gate count comparison

Table 2: Gate Count Comparison

TYPE	GATE COUNT
MASKED AES	20,010
MODIFIED AES	10,000

This indicates that the modified AES in the proposed scheme performs faster than the first order masked AES based architecture. Even though, there is only slight reduction in area and delay in first order masked AES, this architecture provides a good amount of reduction in power consumption. This method is capable to bring down the power from 571mw to 506mW and moreover, it limits the use of the resources

6. Future Scope

This new encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century." It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques

7. Conclusion

The performance of DPA resistant AES is improved by using first order masked AES. The problem with the masked AES is the number of gates used is nearly 20,000 which is fairly large and thus increasing the area . The power consumption is also fairly large. The number of XOR gates used in masked AES is numerous .since the XOR gates have only two inputs, here in masked AES we are using 128 bits XOR gates. Thus the number of gates is large. In order to remove this difficulty we adopt a new method , we introduced randomness in to the AES engines by introducing LFSR's. The 128 bit key word is divided into 16 8-bit sub keys by using LFSR's. Thus the randomness is introduced in to the key. From here the 8-bit sub keys are grouped to form 16 bit and given to FIBONACCI LFSR and GALOIS LFSR in order to increase the randomness. Thus the key is shuffled properly. Since the number of gates is drastically reduced here there is sufficient improvement in reducing the area. The total number of gate used here is nearly 10,000 instead of 20,000 earlier and the power consumption drastically reduced which is proven by the simulation results.

References

[1] S. Tillich and J. Großschädl, "Power analysis resistant AES implementation with instruction set extensions," in CHES. NewYork:Springer, 2014, vol. 4727, LNCS, pp. 303–319
[2] Y.Wang and Y. Ha, "FPGA-based 40.9-gbits/s masked AES with area optimization for storage area network," IEEE Trans. Circuit Syst. II, vol. 60, no. 1, pp. 36–40, Jan. 2013.
[3] M. M. Mbaye, N. Bélanger, Y. Savaria, and S. Pierre, "Loop acceleration exploration for ASIP architecture," IEEE Trans. Very Large Scale (VLSI) Syst., vol. 20, no. 4, pp. 684–696, Mar. 2012
[4] T. Güneysu, "Utilizing hard cores of modern FPGA devices for high performance cryptography," J. Cryptograph. Eng., vol. 1, no. 1, pp. 37–55, Apr. 2011.
[5] D. A. Osvik, J. W. Bos, D. Stefan, and D. Canright, "Fast software AES encryption," in FSE 2010. NewYork: Springer, 2010, vol. 6147, LNCS, pp. 75–93
[6] M. Rivain and E. Prouff, "Provably secure higher-order masking of AES," in CHES. New York: Springer, 2010, vol. 6225, LNCS, pp. 413–427

Author Profile

Reenu Tomy received the B. Tech degree in Applied Electronics and Instrumentation Engineering from Mahatma Gandhi University, Kerala at Rajagiri College of Engineering And Technology 2011, after that two years of working experience as a project engineer in Wipro Technologies now she is pursuing her M. Tech degree in VLSI and Embedded systems under the same university in SCMS School of Engineering and Technology, Cochin.