AES design based on Secure Double Rate Registers (SDRR)

[1] P.D HARSHITHA, [2] ANURADHA J P

[1] M.Tech, BNMIT, [2] Assitant Professor, BNMIT

Abstract*— Power Analysis Attack (PAA) are a class of Side Channel Attacks (SCA) which is based on power consumption measurements whose major concern is the protection of secret data stored in cryptographic devices. In this paper, we introduce the concept of Secure Double Rate Registers (SDRR) as a Register Transfer Level (RTL) countermeasure in order to increase the security of cryptographic devices against PAA. SDRR is exploited in AES 128 bit architecture, the random data in the entire clock cycle is evaluated by the combinational path. One of the main advantage is that our technique does not require duplication of combinational path to process the random data thereby limiting area overhead unlike previous RTL countermeasures. This paper compares the implementation results for Rijndael algorithm, conventional AES algorithm with normal registers and AES algorithm with SDRR. It is found that with the use of SDRR the security, delay and power has been improved. Different approach is followed for S-box operation in AES algorithm which helps us to reduce the usage of memory. This proposed system is implemented, simulated using V9erilog HDL and synthesized by Xilinx tool.

***Keywords*— Hardware Description Language (HDL), Power Analysis Attack (PAA), Register Transfer Level (RTL), Secure Double Rate Register (SDRR), Side Channel Attacks (SCA)**

I. INTRODUCTION

Cryptography is the practice of creating a cryptosystem to prevent all the recipients except the intended ones from accessing the information that is being encrypted. The encryption process takes a plain text, a key and applies a mathematical algorithm to it in order to give out the cipher text. It consists of both encryption and decryption process and they can be classified as asymmetric or symmetric based upon the key used for encryption and decryption. National Security Agency (NSA) has selected AES algorithm to be used by Information Assurance Directorate to protect national security systems. Successful use by United States government led to wide spread use in private sector and hence became more popular algorithm used in symmetric key cryptography.

II. METHODOLOGIES

A. Rijndael algorithm

Rijndael algorithm is the block cipher chosen by the National Institute of Science Technology (NIST) as the Advanced Encryption Standard (AES). It is more advanced than DES and also it defines a method in which it generates a series of subkeys from the original key. It is a new generation symmetric block cipher that supports key sizes of 128 bit, 192 bit and 256 bits. Rijndael algorithm for 128 bit RTL schematic is as shown. It considers 128-bit plain text and key as input and gives out 128-bit plain text at the output after performing both encryption and decryption. It consists of two parts encryption and decryption. It consists of 10 rounds initiated with add round key. Key expansion unit also has been designed in this to generate different keys for various rounds. This block could have also been removed in which case the user will have to interfere and enter the keys as input.

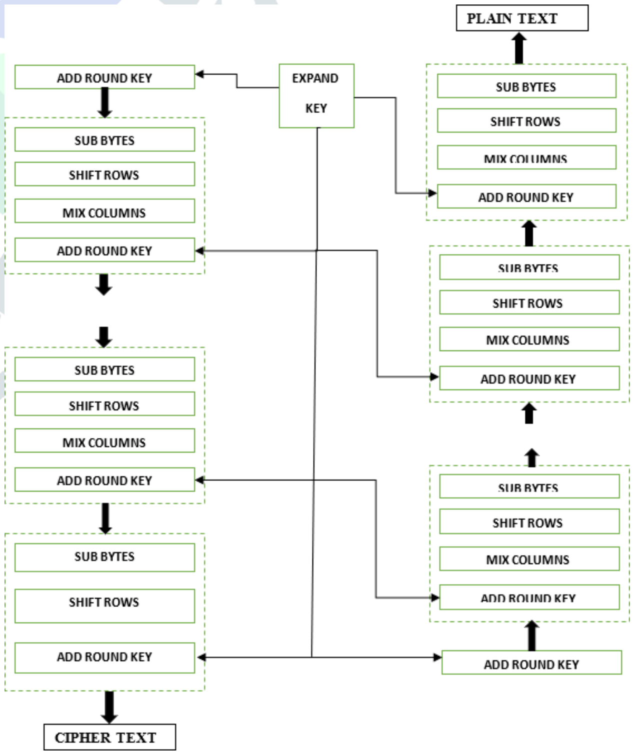


Figure 1: Rijndael algorithm for encryption and decryption

There are two separate key expansion blocks one for encryption and the other for decryption. There is clock signal in this module. According to AES algorithm, all the basic steps like sub bytes, shift rows, mixed columns and add round key will be performed along with key expansion. Figure 2 shows the RTL schematic of Rijndael algorithm.

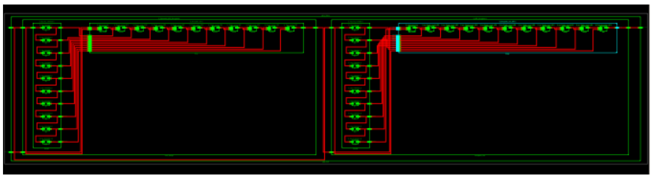


Figure 2: RTL schematic of Rijndael algorithm

The left part of the RTL schematic represents encryption block and key expansion for the same and similarly the right part of the schematic represents the decryption block and the key expansion of decryption. The simulated waveform for the same as shown in figure
3. Where in the inputs are the 128 bit plain text and 128 bit key and the obtained outputs are 128 bit cipher text after encryption and 128 bit plain text after decryption.

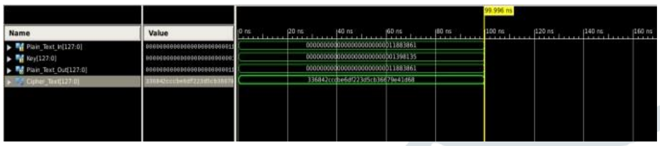


Figure 3: Simulated waveform for Rijndael algorithm

B. Conventional AES-128 bit

Conventional Advanced Encryption Standard Algorithm which takes 128-bit plain text and 128-bit key as the input along with the clock and gives 128-bit cipher text and 128-bit plain text as the output as shown in figure
6. Figure 4 shows the block diagram for conventional AES-128 bit.

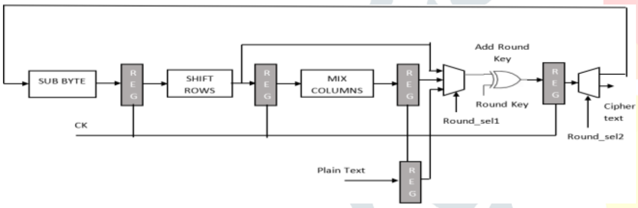


Figure 4: Block diagram of conventional AES-128 bit

It is intended to perform both encryption and decryption. It also includes key expansion technique also, this block can also be neglected in which case the different keys can be given as input by the user itself. Whereas this is not the case if we have key generation block which generates different keys for each and every round of encryption and decryption, in such a case there is no intervention of the user. The RTL schematic is as shown in figure 5.

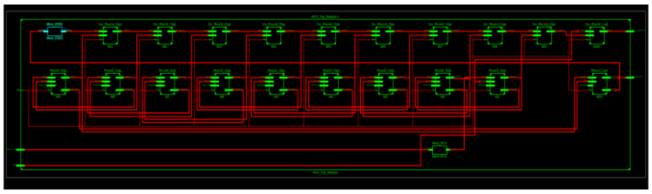


Figure 5: RTL schematic of conventional AES-128 bit

There are 10 rounds of operation in encryption, they are followed by add round key after which round 1 will begin. Round 1 operation consists of sub-bytes operation followed by shift rows and mix column and in the end add round key operation is performed. This operation is the same for all the rounds from round 1 to round 9. Final round is the round 10, this differs slightly from rest of the rounds. Round 10 consists of sub-bytes operation first which is then followed by shift rows and add round key to produce the 128-bit cipher text.
Similarly, there are 10 rounds of operation in decryption as well. For decryption block cipher text of 128-bit is the input and 128-bit plain text is the output. The first round is the add round key which consists of simple xor operation of the 128-bit cipher text and the key generated from the key expansion block during the 10th round that is the final round. This is the first round in decryption, the second consists of inverse shift rows, inverse sub bytes, add round key followed by inverse mixed columns. This is the same sequence for the rest of the rounds too till round 9. Final round consists of inverse shift rows, inverse sub bytes and add round key in the end to the 128-bit plain text.

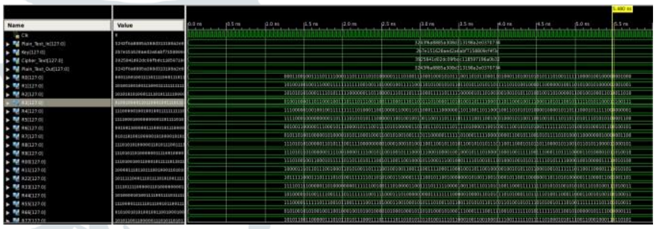


Figure 6: Simulated waveform of conventional AES-128 bit

C. AES with SDRR

This AES architecture involves a special type of registers knows as Secure Double Rate Registers (SDRR). The block diagram of the SDRR is as shown in figure 7. It internally consists of two cascaded registers and a multiplexor at the input side. This multiplexor is a two is to one multiplexor and the two inputs to it are plain text and the random data which is generated from the random number generator or otherwise may be given by the user also. The flipflops in the SDRR are clocked by the same clock signal CK. The multiplexor has a select signal SEL which is used to select between the input data or the plain text and the random data. Based upon the SEL signal, either input data or the random data will be sent to the flipflops. Basically, the SEL signal is mainly used to select between the input data and the random data.

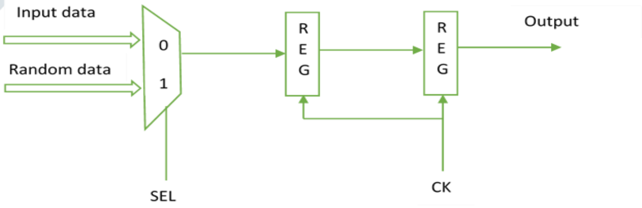


Figure 7: Block diagram of SDRR

Figure 8 represents the RTL schematic of the SDRR. The existing block diagram for AES 128-bit with SDRR is as shown in figure 9.

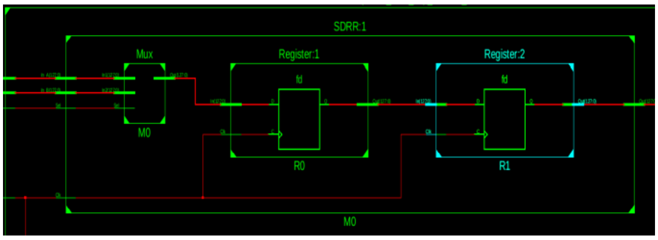


Figure 8: RTL schematic of SDRR

This architecture uses SDRR as a substitute for one of the register at the input side. SDRR can store the data on rising edge and falling edge of the SEL signal according to the CK signal. Hence, SDRR is used for having this advantage. The modified and proposed block diagram for AES-128 bit with SDRR is as shown in figure 10.

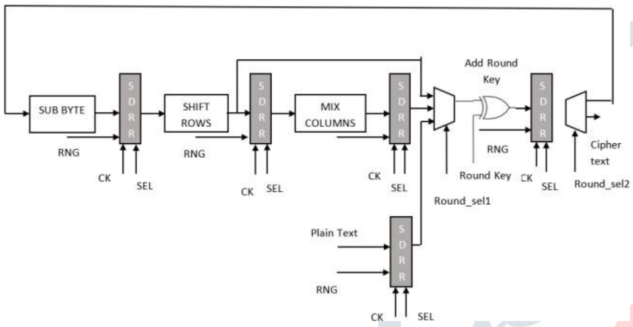


Figure 9: Existing block diagram of AES-128 bit with SDRR

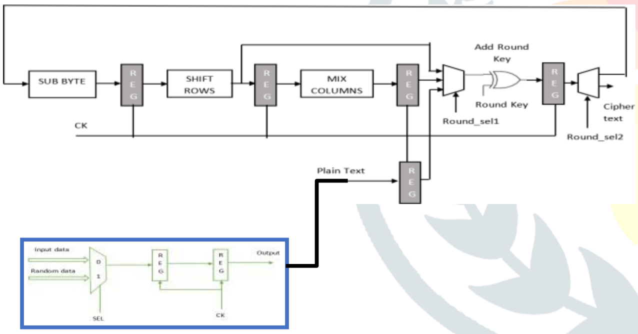


Figure 10: Proposed block diagram of AES-128 bit with SDRR

The RTL schematic of this proposed AES-128 bit with SDRR is as shown in figure 11. The left part represents the SDRR at the input side and the right portion represents the AES-128 bit encryption and decryption part.

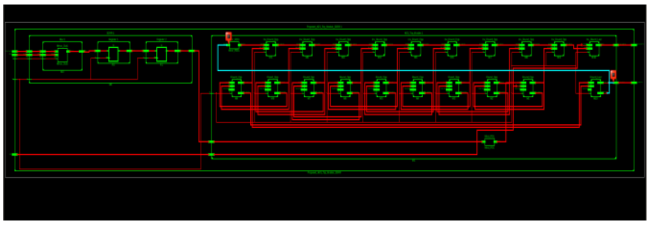


Figure 11: RTL schematic of proposed AES-128 bit with SDRR

The simulated waveforms for proposed AES-128 bit with SDRR is as shown in figure 12.

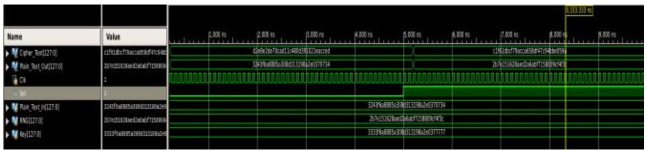


Figure 12: Simulated waveforms of proposed AES-128 bit with SDRR

It is observed from the waveform that based upon the value of the SEL signal, the input data or the random data is selected. It is designed in such a way that whenever the SEL signal is 0, input data or the plain text is considered for encryption and decryption. When the SEL signal is 1, the random data is considered for AES encryption and decryption.

III. LAYERS IN AES

AES-128 bit algorithm is a block cipher working on a 128-bit wide data and key. Encryption is done in iterative operations termed as rounds. There are 11 rounds for AES- 128 bit. Which internally consists of 4 layers (except for first and final round): *Substitute bytes, Shift Rows, Mixed Columns and Add Round Key.*

A. *Substitute Bytes*

Substitute byte transformation is computed by multiplication inversion followed by the affine transformation. The advantage of using this methodology is memory area is saved. The operations performed are represented in the block diagram as shown in figure 13.

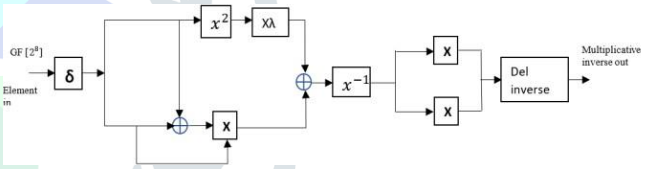


Figure 13: Multiplicative inversion module for the S-box The multiplier block in figure 13, internal block
diagram of it as shown in figure 14. It is a 4-bit multipier, which takes two 4-bit number and gives out a 4-bit product.

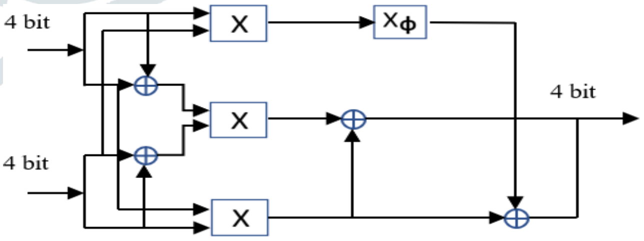


Figure 14: Hardware implementation of multiplication in GF (2^4)

The multiplier in figure 14 internally consists of AND logic gates and XOR logic gates as shown in figure 15. It is a two bit multiplier which takes two, two bit number as input and gives out a two bit product.

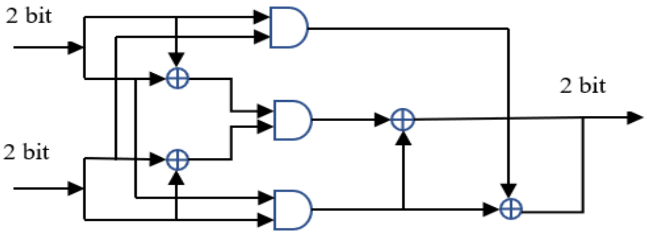
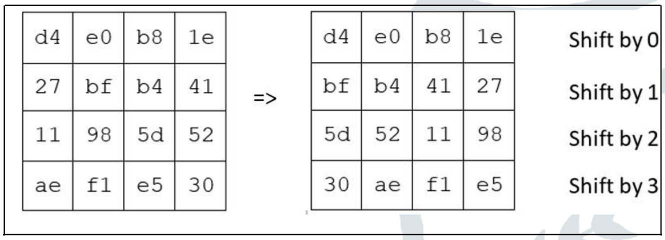


Figure 15: Hardware implementation of multiplication in GF (2)

At the end of all these operations we will observe that the values are matching with the ones in the s-box. This has hos advantage because there is no separate memory required for storing the values, all the calculations are done internally.

B. Shift rows:

The data is arranged in the form of a 4X4 matrix meaning 4 rows and columns. There are 16 storage elements each of which will store an 8-bit data to make an overall data of 128 bit.



d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

=>

d4	e0	b8	1e	Shift by 0
bf	b4	41	27	Shift by 1
5d	52	11	98	Shift by 2
30	ae	f1	e5	Shift by 3

Figure 16: Shift row operation

The figure 16 shows two matrices one before shift row operation and one after the shift row operation. We can observe that the data in row 1 is not at all shifted, meaning to say that the data is shifted by 0. The data in row 1 is shifted by value 1, row 2 is shifted by shift value 2 and finally the data in row 3 is shifted by shift value 3.

C. Mixed columns:

In AES algorithm mixed column operation is performed after the shift rows step. In this step each column is treated as a four term polynomial, in which the co-efficients are the elements in GF (2^8). It basilly consists of modular multiplication of two 4 term polynomials, meaning the multiplication of two columns takes place.

D. Add round key:

Add round key is just a simple operation in which there are two inputs and they are 128 bit data and key, and there is XOR operation involved between the two data, and the output is also a 128 bit data.

IV. OBSERVATIONS

In this paper, different architectural blocks of Advanced Encryption Standard Algorithm has been implemented. First one is the Rijndael Algorithm where there are two key expansion blocks separately for encryption and decryption which has a larger requirement of area. Second one is the conventional AES algorithm for 128-bit, where in there is a slight change in the architecture when compared with the latter. This will share the common key expansion block for encryption and decryption.

Table 1: Comparision of delay

Method name	Delay	Gate or Logic Delay	Path or Route Delay
Proposed AES with SDRR	107.489ns	43.445ns	64.043ns
Conventional AES	106.865ns	43.155ns	63.710ns
Rijndael based	298.073ns	198.209ns	184.329ns

Table 2: Comparision of power

Method name	Power (mW)
Proposed AES with SDRR	20445
Conventional AES	47800
Rijndael based	3781

The third one is the AES algorithm for 128-bit with SDRR, in which there is a new concept of SDRR being introduced. We can observe that security is enhanced and there is significant decrease in delay from table 1 and power from table 2 which is an added advantage of this methodology. When we consider the conventional and the proposed AES with SDRR, the proposed methodology is having greater impact on reduction of power.

V. CONCLUSION

In this paper, we have introduced the SDRR as an RTL countermeasure to increase the security of cryptographic implementations to PAAs. The proposed SDRR technique has been exploited to protect an AES-128 cryptographic core. The proposed approach allows the combinational path to process the random data throughout the clock cycle and the sequential logic to store the real and random data simultaneously, without duplicating the combinational path for the random data. The substitute bytes step in AES has been implemented in such way that there is maximum optimization in usage of memory which is one of the advantages. We can observed significant decrease in delay and power.

REFERENCES

[1] Davide Bellizia, Simone Bongiovanni, Pietro Monsurrò, Giuseppe Scotti , Alessandro Trifiletti, and Francesco Bruno Trotta, on “Secure Double Rate Registers as an RTL Countermeasure Against Power Analysis Attacks”

[2] Ye Yuan, Yijun Yang, Liji Wu*, Xiangmin Zhang on “A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation”

[3] Security of Cryptosystems Against Power-Analysis Attacks thesis by Sonia Belaïd

[4] Prof.N..Penchalaiah and Dr.R.Seshadri on “Effective Comparison and Evaluation of DES and Rijndael Algorithm(AES)”