FPGA Implementation of SDRR in a Conventional Advanced Encryption Standard

Chinthana K S
M. Tech Scholar
Dr. Ambedkar institute of technology,
Bengaluru-56, Karnataka, India

Dr. G V Jayaramaiah
Head of the Dept., ECE
Dr. Ambedkar institute of technology,
Bengaluru-56, Karnataka, India

***Abstract*— A Type of side channel attack is the Power analysis attack(PAAs) which is based on measurement of power consumption, and they are of main concern in securing the secrete data that is stored in cryptographic devices . In this paper, we introduce conventional advanced encryption standard (AES-128) along with SDRR architecture to provide better immunity of the cryptographic hardware based on DDA encoding logic . The required input is provided to the SDRR and the out of the SDRR is given to AES which performs Encryption and Decryption and provide the output. Our technique eliminates the combinational path duplication that is used to process the random data, unlike other RTL counter measures. The Verilog hardware description language used for implementing the proposed system and Modelsim 6.4 C used for simulation, and Synthesized using Xilinx tool. The proposed system is implemented in FPGA Spartan 3 XC3S 200 TQ-144.**

Keywords*— Advanced encryption standard (AES), power analysis attack (PAA), register-transfer level (RTL) countermeasure, Modelsim

I. INTRODUCTION

SIDE-Channel Attacks (SCAs) [1] is a kind of attack, that by observing the unintended physical emissions such as power consumed by device and etc, try to recover the information that is being processed in a cryptographic device. The most essential form of SCA is the Power analysis attacks (PAAs) [2], as they are of relatively low cost and simple to achieve. The major advantage of PAAs is that it depends on the instantaneous current of the process data drawn from the power source of CMOS digital circuits.

With the advancement in Internet of Things applications, they was a need to design highly constrained devices i.e. new cryptographic circuits, that were needed to be area efficient, low power, and SCAs resistant [6], [7]. Furthermore, IN CMOS devices there was a increase in leakage currents that built an additional side channel that can be utilized by PAAs, based on static current consumption [8].

At each level of abstraction of design flow, countermeasures were introduced. One of the class of countermeasures used logic styles, and the power consumed by it was less dependent on the processed data. Because of improperly balanced parasitic capacitance, that leads to increased data dependence of power consumption , the logic styles were not more advantageous. Then random precharge logic (RPL) was introduced as one of the first RTL countermeasure .But this too had disadvantage of requiring the combinational path duplication. Many masked AES implementations were proposed .In masked AES, during the encryption process, to the plaintext the random intermediate data were continuously added to mask the side-channel leakage and at the end of the encryption, the random intermediate data that results from masking operation are removed from the ciphertext. But the masked AES implementations are attackable by higher order PAAs.

Our proposed technique uses the secure double rate registers (SDRRs) in conventional advanced encryption standard that provides a better security by protecting both the combinational and sequential parts of the implementation, and does not require the duplication, thus reducing power consumption overhead.

II. PROPOSED TECHNIQUE

A. AES-128 Fundamentals –

AES is a symmetric block cipher .This implies it uses a similar key for both encryption and decoding. The calculation considers an assortment of block and key sizes . The block and key can in reality be picked autonomously from 128, 160, 192, 224, 256 bits and need not be the equivalent.

Encryption comprises in iterated activities, known as "rounds". The calculation starts with an Include round key stage pursued by 9 rounds of four phases and a tenth round of three phases. This applies for both encryption and decoding with the exemption that each phase of a round the unscrambling calculation is the converse of it's partner in the encryption calculation. The four stages are as follows: 1. Substitute bytes, 2. Shift rows, 3. Mix Columns, 4. Add Round

Key. The tenth round simply leaves out the Mix Columns stage.

The initial nine rounds of the decoding calculation comprise of the accompanying: 1. Inverse Shift rows, 2. Inverse Substitute bytes,3. Inverse Add Round Key, 4. Inverse Mix Columns.

B. Architecture of the Reference AES Encryption Unit --

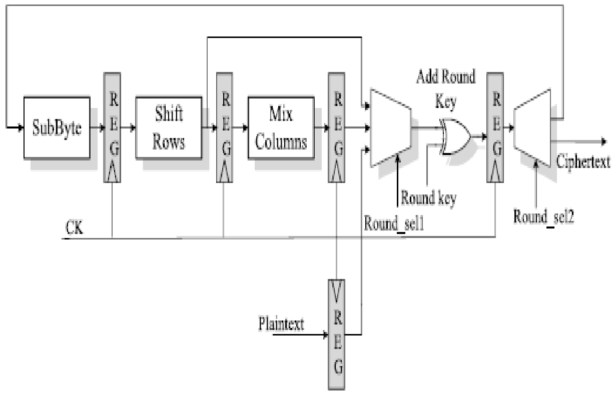


Fig.1. Architecture block diagram of the reference AES-128 encryption unit (AES-0)

The architecture of the reference AES encryption unit (AES-0) is shown in Fig. 1.The implementation of these four blocks is done using combinational network and a pipeline register to store data at the output of each block. To process it would require four clock cycles, and 128-bit plaintext block(11 rounds) would require 44 clock cycles for the entire encoding process.

C. Secure Double Rate Register--

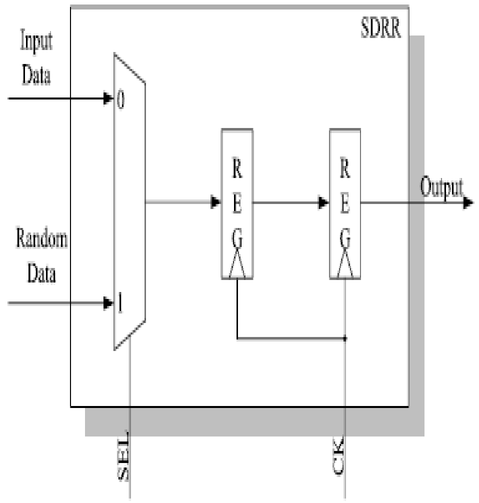


Fig.2. Block scheme of the SDRR.

Double-data-rate computation can be used as a countermeasure against PAAs. The block diagram of the SDRR is depicted in Fig. 2. The SDRR consists of two cascaded registers and an input multiplexer. The multiplexer allows for the selection of the input data of the first register. The registers in the SDRR are clocked by the CK signal . The SEL signal is used to select between real and random data. The real input data is stored in one of the two registers of the SDRR, a random data is stored in the other one and vice versa.

D. Proposed counter measured AES--

The proposed AES design is pictured in Fig.3. SDRRs store the data during both positive edge and negative edge of the SEL signal and therefore, conventional registers are replaced by SDRRs. The proper data and random data are processed and stored concurrently, using SDRR, and is provided as input for AES along with the key to perform encryption and decryption by exploiting the diffusion property of the cryptographic algorithm. The internal structure of the proposed counter measured approach is as shown in the figure 4.

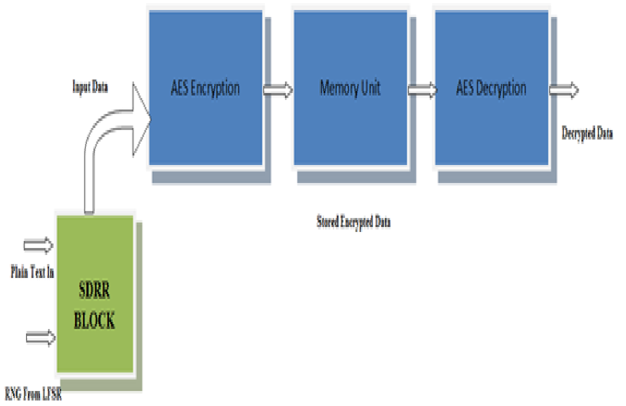


Fig.3. Block diagram of the proposed counter measured AES architecture

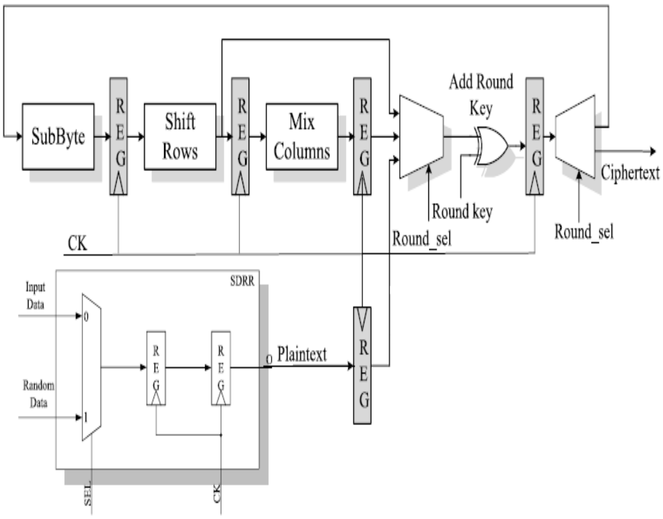


Fig.4. Internal view

The internal structure of the proposed counter measured approach is as shown in the figure 4. If the SEL is 0 correct input is selected and if SEL is 1 random data is selection and is provided for encryption and decryption. Thus, providing a improved security.

III. FPGA IMPEMENTATION

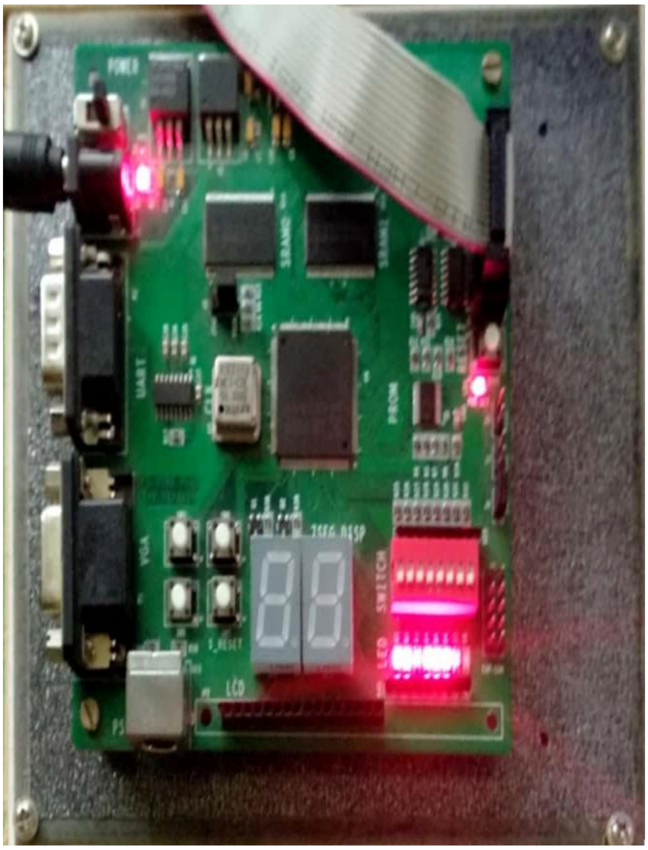


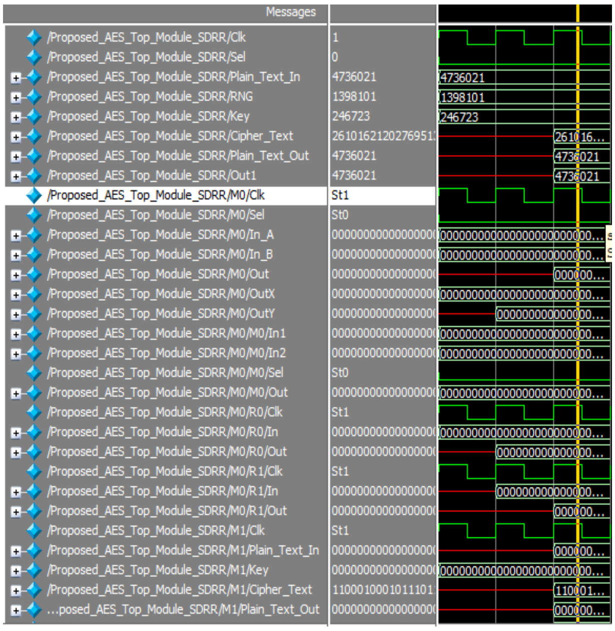
Fig.5: FPGA Implementation of Proposed system

Here we have used Spartan-3 FPGA board. This provides powerful, self contained development platform for designs. The FPGA implementation of proposed system for particular input is as shown in the fig.5.

VI. RESULT AND ANALYSIS

A. Verilog simulation result-

The figure 6 below is the verilog simulation result of proposed design which shows plaintext output equals to plaintext input when sel is 0.



```
Messages
/Proposed_AES_Top_Module_SDRR/Clk                 1
/Proposed_AES_Top_Module_SDRR/Sel                 0
/Proposed_AES_Top_Module_SDRR/Plain_Text_In       4736021
/Proposed_AES_Top_Module_SDRR/RNG                 1398101
/Proposed_AES_Top_Module_SDRR/Key                 246723
/Proposed_AES_Top_Module_SDRR/Cipher_Text         261016212027695l
/Proposed_AES_Top_Module_SDRR/Plain_Text_Out      4736021
/Proposed_AES_Top_Module_SDRR/Out1                4736021
/Proposed_AES_Top_Module_SDRR/M0/Clk              St1
/Proposed_AES_Top_Module_SDRR/M0/Sel              St0
/Proposed_AES_Top_Module_SDRR/M0/In_A             000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/In_B             000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/Out              000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/OutX             000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/OutY             000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/M0/In1           000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/M0/In2           000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/M0/Sel           St0
/Proposed_AES_Top_Module_SDRR/M0/M0/Out           000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/R0/Clk           St1
/Proposed_AES_Top_Module_SDRR/M0/R0/In            000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/R0/Out           000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/R1/Clk           St1
/Proposed_AES_Top_Module_SDRR/M0/R1/In            000000000000000000
/Proposed_AES_Top_Module_SDRR/M0/R1/Out           000000000000000000
/Proposed_AES_Top_Module_SDRR/M1/Clk              St1
/Proposed_AES_Top_Module_SDRR/M1/Plain_Text_In    000000000000000000
/Proposed_AES_Top_Module_SDRR/M1/Key              000000000000000000
/Proposed_AES_Top_Module_SDRR/M1/Cipher_Text      11000100010111011
...posed_AES_Top_Module_SDRR/M1/Plain_Text_Out    000000000000000000
```

Fig.6:Simulation waveform of proposed system using Modelsim

B. Area, Delay and Power comparison-

Method Name	Area in Number of LUT			Delay			Power
Spartan 3 XC 3S 5000-4FG1156	LUT	Slices	Gates	Delay	Gate or logic Delay	Path or Route Delay	mw
Proposed Pipelined with SDRR	29841	15225	260788	107.48ns	43.33ns	64.043ns	20445
Pipelined based Encryption	29672	15012	250455	106.865ns	43.155ns	63.710ns	47800

Table.1: Area, Delay and Power comparison table

The area, delay and power are the major consideration in designing any system and there comparison need to considered .As per the above comparison table the area requirement for the proposed system is more when compared to pipeline based encryption. And when it comes to delay comparison the proposed system has less delay when compared to the other encryption methods.

C. Area Comparison Graph-

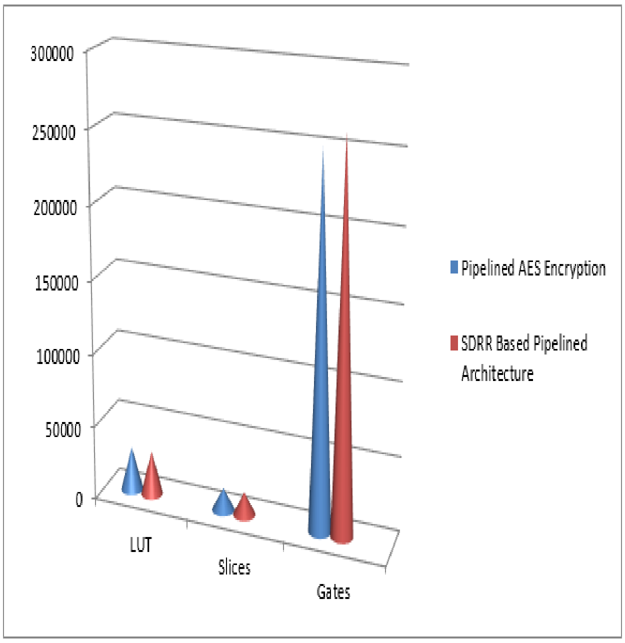


Fig.7: Comparison Graph for area

D. Delay Comparison Graph-

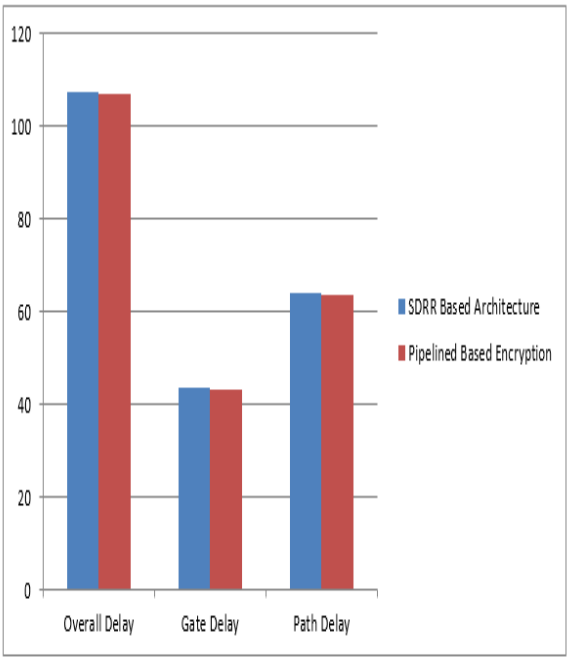


Fig.8: Comparison graph for delay

E. Power Comparison Graph-

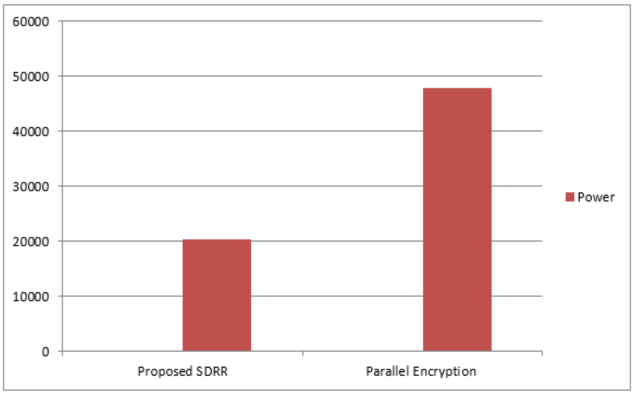


Fig.9: Comparison graph for power consumption

The figure 7 and figure 8 shows the comparison graph for area and delay. The power consumption is also one of the major consideration and the power consumed by the proposed system is less than other pipelined system. The figure 9 shows the power comparison graph.

V. CONCLUSION

In this paper SDRR in Advanced Encryption Standard is designed using Verilog code and the proposed system is implemented in FPGA Spartan 3 XC3S 200 TQ-144. The SDRR provides the input for the encryption by making the selection between plaintext and random data. The selected input is provided for encryption and decryption along with the key. The proposed work allows, process the combinational circuit on every clock cycle and sequential circuits for storing the process data, without duplicating the combinational logic on random data. Another contribution of this paper is that it designs Encryption Design using Shift rows, Mixed Column, Add Round Key and We also design a Decryption Part. Also area, delay and power comparison is made. This system provide a high security.

VI. REFERENCES

[1] P. C. Kocher, “Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems,” in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer-Verlag, 1996, pp. 104–113.
[2] P. C. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer, 1999,pp. 388–397.
[3] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealingthe Secrets of Smart Cards. New York, NY, USA: Springer, 2008.
[4] ITRS. (2013). International Technology Roadmap for Semiconductors.[Online]. Available: http://public.itrs.net/
[5] M. Renauld, F.-X. Standaert, N. Veyrat-Charvillon, D. Kamel, and D. Flandre, “A formal study of power variability issues and sidechannel attacks for nanoscale devices,” in Advances in Cryptology— EUROCRYPT. Berlin, Germany: Springer-Verlag, 2011, pp. 109–128.
[6] T. Eisenbarth and S. Kumar, “A survey of lightweight-cryptography implementations,” IEEE Design Test Comput., vol. 24, vol. 6, pp. 522–533, Nov./Dec. 2007.

[7] A. Y. Poschmann, “Lightweight cryptography: Cryptographic engineering for a pervasive world,” Ph.D. dissertation, Faculty Electr. Eng. Inf. Technol., Ruhr Univ. Bochum, Bochum, Germany, 2009.

[8] D. Bellizia, S. Bongiovanni, P. Monsurrò, G. Scotti, and A. Trifiletti, “Univariate power analysis attacks exploiting static dissipation of nanometer CMOS VLSI circuits for cryptographic applications,” IEEE Trans. Emerg. Topics Comput., vol. 5, no. 3, pp. 329–339, Jul./Sep. 2017.

[9] M. Bucci, M. Guglielmo, R. Luzzi, and A. Trifiletti, “A power consumption randomization countermeasure for DPA-resistant cryptographic processors,” in *Proc. Integr. Circuit Syst. Design Power Timing Modeling, Optim. Simulation*, 2004, pp. 481–490.

[10] M. Avital, I. Levi, O. Keren, and A. Fish, “CMOS based gates for blurring power information,” *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 7, pp. 1033–1042, Jul. 2016.

[11] M. Bucci, R. Luzzi, M. Guglielmo, and A. Trifiletti, “A countermeasure against differential power analysis based on random delay insertion,” in *Proc. IEEE Int. Symp. Circuits Syst.*, vol. 4. May 2005, pp. 3547–3550.