International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 120-124
Published Online July 2019 in IJEAST (http://www.ijeast.com)

TRIPLE AES IMPLEMENTATION BASED ON SECURE DOUBLE RATE REGISTERS

Praneetha H T
Department of ECE
SJBIT, Bengaluru, Karnataka, India

Dr.Shilpa k Gowda
Department of ECE
SJBIT, Bengaluru, Karnataka, India

Abstract*— Successful protected data communication requires a certain algorithm to encrypt the data in order to protect it against unauthorized access. One of these algorithms is Triple. Advance Encryption Standard used three encryption keys to differentiate from AES. It utilizes the equivalent Rijndael AES algorithm; however, it has more noteworthy unwavering quality and size of the Key's. AES utilizes symmetric Key's to enable unauthorized users to get to information when obtain that the key. Therefore, the projected method uses 3 data encryption Key's and same three keys for decryption process. To expand the security of cryptographic algorithm against PAAs, present Secure double rate registers (SDRRs) as a countermeasure for Register Transfer Level (RTL). Utilize the SDRRs within a customary Advanced Encryption Standard (AES)-128 designs, to improve the Cryptographic-equipment's invulnerability to cutting edge PAAs. The combinational way assesses random data all through the whole clock cycle in the SDRR abusing AES-128, and the interleaved handling of arbitrary and genuine information guarantees both combinational and sequential logic security. Unlike past RTL counter measures; this method does not need replication of the combinational-way to process the irregular information, along these lines constraining overhead zone. This proposed system implemented using the tool Verilog-HDL and Simulated in Modelsim as well as Synthesized in Xilinx.

Key Words: ***AES, Cryptography, Decryption, Encryption, Triple AES, SDRR.***

I. INTRODUCTION

Data security is considered an important factor in every Communication's System, unwired devices and numerous different applications. To secure and protect the data from assorted hackers and unauthorized admission, numerous technologies and algorithms have been built. Programmers, electronic spying and so on, have developed new techniques to attacking the data with changing technology. Cryptography is a method used in mathematics for encrypting and decrypting data. It allows sensitive information to be stored or transmitted over networks that are not secured; hence it should not read anyone other than the intended recipient. Several Encryption algorithms have been created to handle data-security attacks. One of the algorithm is the Advanced-Encryption Standards (AES) issued on behalf of FIPS by the need for a strong encryption algorithm so that a National-Institute of Standard and Technology (NIST).

Conventional Encryption basic Requirements are:
Individual who knows about the algorithm and the ability to access more than one cipher text cannot convert or translate cipher text or determine how to use the key. The secret key in Replica must be present in a secure manner with both the transmitter and the receiver.

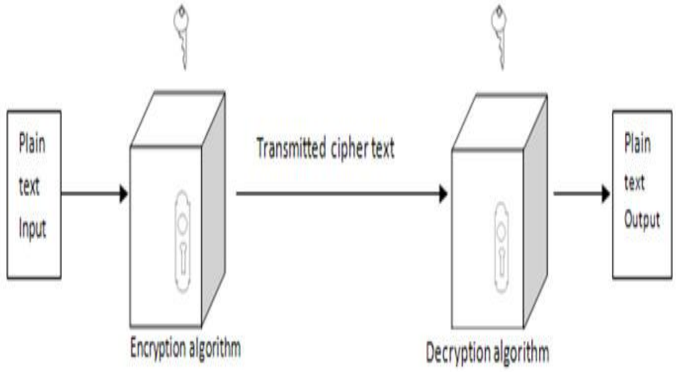


Fig.1.Standard cryptosystem model.

Figure1 shows the standard cryptosystem model. Two Belgian cryptographers developed the Advanced Encryption Standard based on cipher. Rijndael is a family of cipher among dissimilar blocks in addition to key, all different. The size of the block is 128 bits and the different length of key's are one hundred and twenty eight, one hundred and ninety two and two hundred and fifty six bits. AES works under four-column-main byte-array Matrix called the State. For plaintext Conversion into cipher text, multiple reiterations of change rounds are required and this is indicated by key size utilized in AES cipher:

- One hundred and twenty eight bit keys required ten reiteration cycles.
- One hundred and ninety two bit keys required twelve reiteration cycles.
- Two hundred and fifty six bit keys required fourteen reiteration cycles.

There are processed by series steps in each round’s. Each round comprises of four unique stages, but it similar, depending upon encryption key. By means of use of the identical Encryption key, the text of cipher is converted back to the novel plaintexts and this transformation is accomplished using set of reverse rounds.

The author's goal is to achieve simplified method of simulating these techniques in order to secure the data. The Proposed algorithm implemented using the Verilog-HDL, Simulated by Modelsim and Synthesized by Xilinx.

The paper is arranged according to the following: the proposed implementation will be discussed in Section 2. Section 3 discusses results of synthesis and outputs of simulation, and Section4 concludes the analysis. Ends with acknowledgement.

II. IMPLEMENTATION OF THE TRIPLE AES WITH SDRR

A. Basics of algorithm AES-128

The algorithm’s AES-128 is the block Cipher that workings with keywords and huge data of 128bit. Encryption comprises of iterated operations, called "rounds”. Every one round consists of the sub operations functioning on a on its own byte, called “layer". The AES-128 consists of 10 plus 1 rounds, each consisting of four layers (except round0 and round10): substituteBytes, ShiftRows, MixColumns, and AddRoundKey. The objective capacity of PAAs is generally the yield of the round 0 AddRoundKey layers or the yield of round 1 SubBytes layer; but round0 is designed in the mechanism, an assault is flourishing, but assailant be able to recuperate this secret key.

B. AES Reference Encryption Architecture

Fig.2.1 is the AES reference Encryption architecture and it is also called Parallel Encryption. The core's data path have iterative type structure, among the internal pipeline consisting of 4 individual blocks, each one performing AES round layer.

Using a combination network and a pipeline register, each of these four blocks is implemented to accumulate the data at the yield of all block. The processing of a round requires four clock cycles and the complete programming method of the 128-bit Plaintexts block (11 rounds) requires 44 clock cycles.

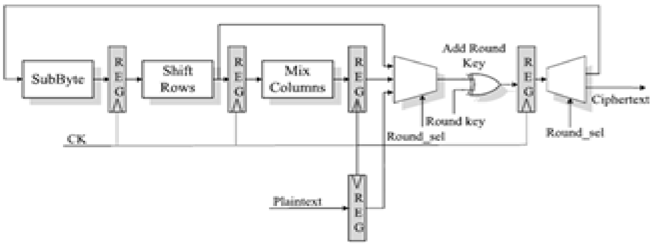


Fig.2.1. AES-128 Reference encryption Architecture

C. Proposed System

The SDRR has two registers are cascaded along with an input multiplexer for selecting the first register input data. The SDRR flip-flops are clocked by the clock signal. For selecting the actual and arbitrary data, the reference architecture clock signal (SEL signal) is used. By utilizing the SDRR, the actual information is placed in one of the registers in SDRR's, irregular information placed into the other. The SDRR block diagram is seen in below fig.

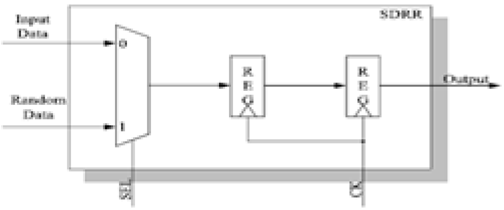


Fig.2.2.SDRR Architecture

Triple AES is a process for reusing AES implementations with three instances of AES serial installation to improve data security. Using three keys in the encryption process leads to triple AES being formed. The operation of the AES is performed by 3 keys. The three keys K1, K2 and K1 are used for converting it into cipher text C on a plain text P. By using the Rijndael’s algorithm, key K1 is used to encrypt E1 and the result is fed to decrypt D1 with key K2 and key K1 is used for third encryption E2. Multiple data encryption increases its security and makes decoding or cracking the data difficult. The model for implementing triple AES is shown in Fig. 2.3.

The procedure of decryption is the same as the procedure of encryption but executed in reverse. Some keys may weaken the Encryption, that is, if the 2nd or 1st key or the 3rd or 2nd key is identical.

Fig.2.3 illustrates the Triple AES encryption.

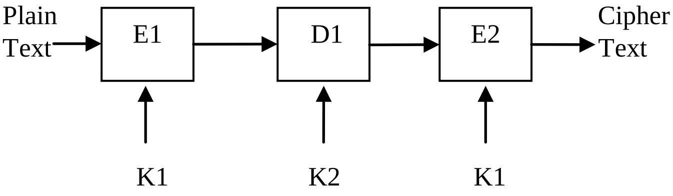


Fig.2.3. Encryption process of triple AES architecture

Triple AES Decryption is the reverse encryption process and Fig.2.4 illustrates the Triple AES decryption.

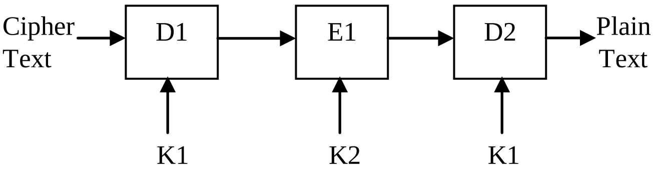


Fig.2.4.Block Diagram of Triple AES Decryption architecture

Fig.2.5 is the Proposed Triple AES with SDRR architecture.

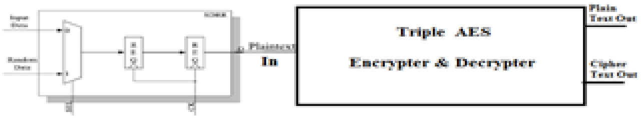


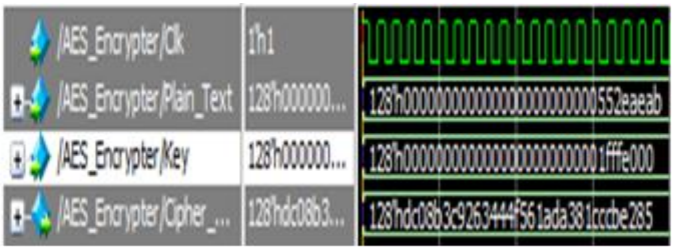
Fig.2.5 Triple AES with SDRR architecture

III. RESULT

Advanced Encryption Standard is generally used Encryption standard in many fields of day to day life. It is utilized to makes the system and information correspondence progressively secure. To improve the speed and the efficiency of the AES encryption technique various new architectures are proposed. There are

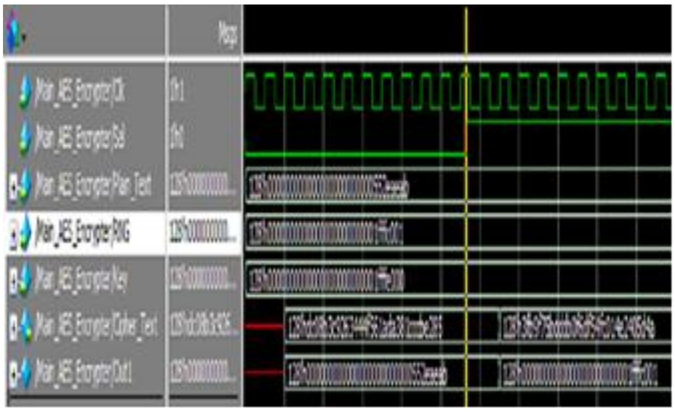
- Parallel Encryption.
- Parallel Encryption with SDRR
- Triple AES with SDRR.

This synthesized in Xilinx and Simulated in Modelsim.



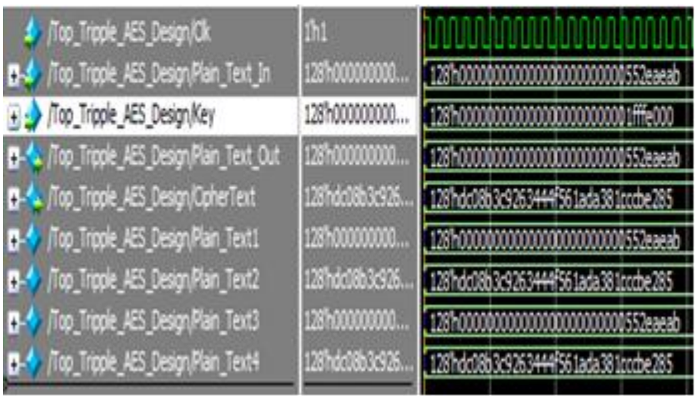
```
/AES_Encrypter/Clk          1'h1
/AES_Encrypter/Plain_Text   128'h000000...   128'h000000000000000000000000552eaeab
/AES_Encrypter/Key          128'h000000...   128'h0000000000000000000000001fffe000
/AES_Encrypter/Cipher_...   128'hdc08b3...   128'hdc08b3c9263444f561ada381ccbe285
```

Fig. 3.1 Parallel encryption simulated output



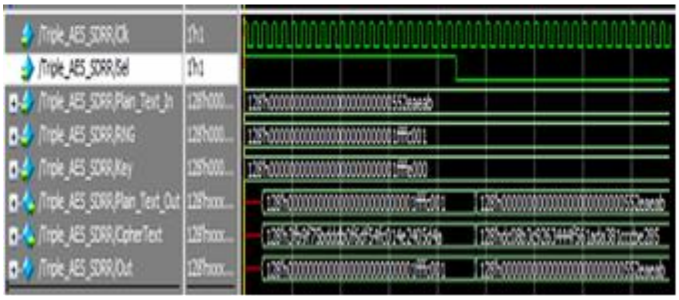
```
/Main_AES_Encrypter/Clk          1'h1
/Main_AES_Encrypter/Sel          1'h1
/Main_AES_Encrypter/Plain_Text   128'h00000000...   128'h000000000000000000000000552eaeab
/Main_AES_Encrypter/RNG          128'h00000000...   128'h0000000000000000000000001fffe001
/Main_AES_Encrypter/Key          128'h00000000...   128'h0000000000000000000000001fffe000
/Main_AES_Encrypter/Cipher_Text  128'hdc08b3c926...  128'hdc08b3c9263444f561ada381ccbe285   [illegible]
/Main_AES_Encrypter/Out1         128'h00000000...   128'h000000000000000000000000552eaeab   128'h0000000000000000000000001fffe001
```

Fig. 3.2 Parallel encryption with SDRR simulated output



```
/Top_Tripple_AES_Design/Clk             1'h1
/Top_Tripple_AES_Design/Plain_Text_In   128'h000000000...   128'h000000000000000000000000552eaeab
/Top_Tripple_AES_Design/Key             128'h000000000...   128'h0000000000000000000000001fffe000
/Top_Tripple_AES_Design/Plain_Text_Out  128'h000000000...   128'h000000000000000000000000552eaeab
/Top_Tripple_AES_Design/CipherText      128'hdc08b3c926...  128'hdc08b3c9263444f561ada381ccbe285
/Top_Tripple_AES_Design/Plain_Text1     128'h000000000...   128'h000000000000000000000000552eaeab
/Top_Tripple_AES_Design/Plain_Text2     128'hdc08b3c926...  128'hdc08b3c9263444f561ada381ccbe285
/Top_Tripple_AES_Design/Plain_Text3     128'h000000000...   128'h000000000000000000000000552eaeab
/Top_Tripple_AES_Design/Plain_Text4     128'hdc08b3c926...  128'hdc08b3c9263444f561ada381ccbe285
```

Fig. 3.3 Triple AES Simulated Output



```
/Triple_AES_SDRR/Clk             1'h1
/Triple_AES_SDRR/Sel             1'h1
/Triple_AES_SDRR/Plain_Text_In   128'h000...   128'h000000000000000000000000552eaeab
/Triple_AES_SDRR/RNG             128'h000...   128'h0000000000000000000000001fffe001
/Triple_AES_SDRR/Key             128'h000...   128'h0000000000000000000000001fffe000
/Triple_AES_SDRR/Plain_Text_Out  128'hxxx...   128'h0000000000000000000000001fffe001   128'h000000000000000000000000552eaeab
/Triple_AES_SDRR/CipherText      128'hxxx...   [illegible]   128'hdc08b3c9263444f561ada381ccbe285
/Triple_AES_SDRR/Out             128'hxxx...   128'h0000000000000000000000001fffe001   128'h000000000000000000000000552eaeab
```

Fig. 3.4 Triple AES with SDRR Simulated Output

Advance Encryption Standard (AES) has been developed to improve security and safety, power testing resistance, hardware and software recital depicted in Table 1.

Method Name	**Delay**	**Power**
Spartan 3 XC 3S 5000-4FG1156	**ns**	**Mw**
Proposed Parallel Encryption with SDRR	107.489	20445
Parallel Encryption	106.865	47800

Table.1 Power analysis

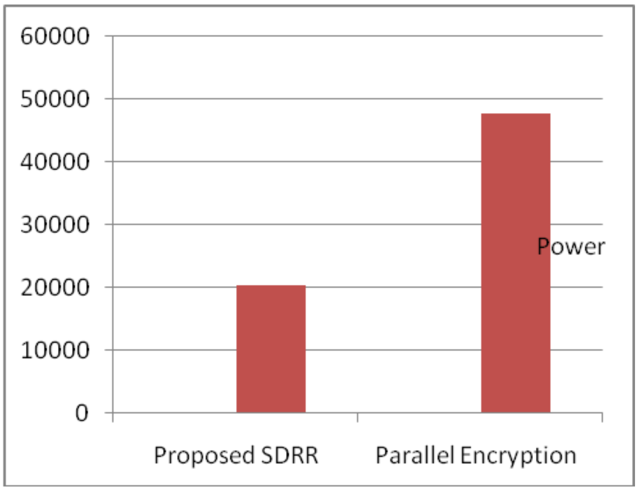


Fig.3.5 Power Graph

IV. CONCLUSION

Due to the needs in communications for more safe and secure, The Project implements the Triple AES with SDRR as an RTL countermeasure to build the security of cryptographic usage to PAAs. In this paper, the Triple AES using three keys has been designed and results are verified. The protected Implementations showed a strongly for Delay & Power. The Another contribution of this project is that it designs Triple AES Encryption & Triple AES Decryption Design using Shift rows, Inverse ShiftRows, MixColumn, Inv MixColumn, and Add Round Key. Finally with the help of AES Encryption and Decryption Blocks implement a New Triple AES. The results of this Project can be served for protecting the Data with the High Security.

V. ACKNOWLEDGEMENT

This research has been supported by the SJB Institute of Technology, Bangalore. With her guidance, I sincerely thank my guide, Mrs. Shilpa k Gowda, for supporting this work.

VI. REFERENCES

[1] David Bellizia,Simone BonGiovanni,Pietro Monsurro,Giuseppe Scotti,Alessandro Trifiletti,and Francesco Bruno Trotta,(2018).”Secure Double Rate Registers as an Countermeasure Against power Analysis Attacks”.

[2] Gagandeep Singh Walia*, Narinder Pal Singh, Hunny Pahuja and Amandeep Singh, (2016).“Implementation and Analysis of Triple AES in VHDL”, Indian Journal of Science and Technology, Vol9 (47), DOI:10.17485/ijst/2016/v9i47/10680.

[3] Henry kuo and Ingrid Verbauwhede, (2003).“Design and Performance testing of a 2.29 GB/s Rijndael Processor”, IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL. 38, NO. 3, pp 569-572.

[4] Svetlin A. Manavski,(2007) “CUDA Compatible GPU as an Efficient Hardware Accelerator for AES Cryptography”, IEEE International Conference on Signal Processing and Communications (ICSPC2007), pp.24-27,

[5] Yi-Cheng Chen and Chung-Cheng Hsieh,(2008). “High Throughput 32-bit AES Implementation in FPGA”, IEEE, pp.1806-1809.

[6] Shanxin Quo, Gulch Shoo, Yihong Hu Zhigang Guo Zongjue Qian, (2009). “High Throughput Pipelined Implementation of AES on FPGA”.IEEE.

[7] Sanu K. Mathew and Farhana Sheikh, (2012). “53 Gbps Native $(2^4)^{\wedge 2}$Composite-Field AES-encrypt/decrypt Accelerator for Content-protection in 45 nm High-Performance Microprocessors”.

[8] P.Maistri and R.Leveugle, (2008) “Double-data-rate computation as a countermeasure against fault analysis,” IEEE Trans. Comput., vol. 57, no. 11, pp. 1528–1539.

[9] M. McLoone and J. V. McCanny, (2001). "Rijndael FPGA Implementation Utilizing Look-Up Tables", IEEE Workshop on Signal Processing Systems, pp. 349-360.

[10]. Chih-Peng Fan, Jun-Kui Hwang, (2007). "Implementations of High Throughput Sequential and Fully Pipelined AES Processors on FPGA",Proceedings of 2007 International Symposium on Intelligent Signal Processing and Communication Systems ,Xiamen, China.

[11] P. C. Kocher, (1996). “Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other

systems," in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer-Verlag, pp. 104–11

[12] P. C. Kocher, J. Jaffe, and B. Jun, (1999). "Differential power analysis," in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer, pp. 388–397.

[13] K. Schramm and C. Paar, (2006). "Higher order masking of the AES," in Topics in Cryptology—CT-RSA. Berlin, Germany: Springer, pp. 208–225.

[14] Advanced Encryption Standard, (2011). Standard FIPS 197, National Institute of Standards and Technology (NIST) of U.S. Department of Commerce.

[15] D. D. Hwang et al., (2006). "AES-based security coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks," IEEE J. Solid-State Circuits, vol. 41, no. 4, pp. 781–792.