International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-8, June 2020

Eluding Side Channel Attacks by using Masking 128Bit AES Design

Pallavi, Seerapu Anil Nagendra, S V Uma

Abstract: ***Advanced encryption standard is detailing for data crypto graphing. The algorithm used universally for cryptography and secure data transmission, the algorithm puissant to intruders, who often attack via side channels. One of the observed attacks was estimate the power implanted in AES core and processed probable scrutinizing to guess the key on multiple iterations. So in order to elude side channel attacks and reduce power consumed in AES standard, design proposed with masking and pipeline scheme. This design helps in shrinking power consumption as compare to AES algorithm and upgrade to withstand from attacks. Another major improvement in the design is LUT's used for masking and original algorithm almost equal, area phenomenon also solved out. The proposed algorithm implemented in VERTEX-7 FPGA board and simulated using Xilinx Vivado 2015.2 and Modelsim.***

Keywords: AES crypto graphing, side channel attacks, intruder, pipelining, trade-off, S box, Galois fields, cipher, masking.

I. I.INTRODUCTION

A method of converting a information into a secret code for passing through a public network is called cipher text. Plain text is turned into cipher text at source end via an encryption algorithm and at destination end it is decrypted back to plain text. Only authorised people can read the cipher text using a proper key and process it.

Advanced encryption standard algorithm is one of the best encrypting and decrypting standard. The AES algorithm works with Rijindal block cipher. A block cipher is an encryption algorithm that works on a single block of data at a time. The key size can be 128 bits,192 bits, or 256 bits. 128 bit key will take 10 rounds to complete encryption and decryption. The AES algorithm is neither a computer program nor source code. It is mathematical encapsulation of a process and ambiguous data consists of four block for encryption like substitution block, shift row, mixed column and add round key. Every block is of 128 bits arranged in a four by four matrix. key is generated in all ten round differently. If encryption and decryption processed with a same key is called symmetric encryption algorithm otherwise if it uses two different keys (public and private) is called asymmetric encryption algorithm.The advanced encryption standard (AES) application now a day's observed in every messaging Apps like facebook, WhatsApp, etc. Also extensively used in zipping data and transferring programs like winzip because it is more secured.

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author
Pallavi*, VLSI And Embedded System (M Tech),RNSIT, BANGLORE, India. Sugandhi2391@Gmail.Com
S.Anil Nagendra, VLSI Design(M Tech), GITAM University, Visakhapatnam, India.
DR. S V Uma , ECE Department ,RNSIT, Bangalore, India.

While AES also not look out from intruder so long time, the side channel attacks gear up from past few days more.Side channel attacks are attacks on the implementation of AES, not on the input or the AES cipher text. It attempts to correlate various measurements of the encrypting tool with time in an attempt to guess the key. It can be unsafe through side channels, attackers can easily hacked down. AES algorithm had tradeoffs the design with masking scheme is introduced to diminish power, while pipeline technology used to boost up the performance.

II. METHODOLOGY

An AES encryption algorithm round depends on the key length according to pictorial representation of Fig.1. Each round consists of four steps.

128 bit AES perform 10 rounds. AES works on the bytes every block arranges by 16 bytes of matrix.

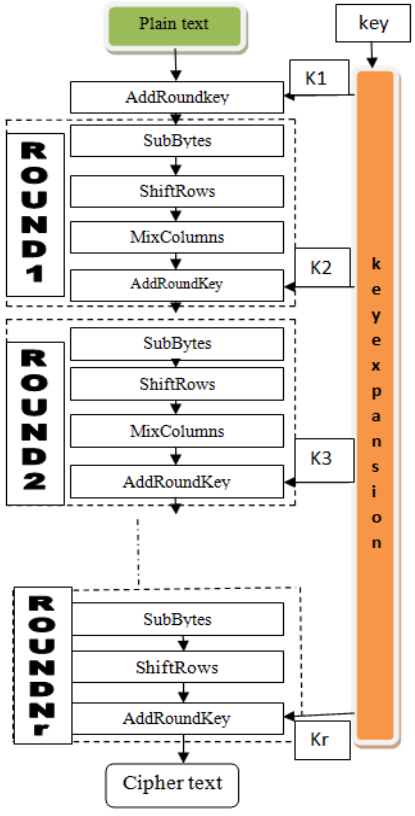

Fig.1.Flow Chart For AES Algorithm

AES algorithm takes four steps for each round

Substitution Block: Replacement of current state bit with 8 bit substitution block.

Shift Rows: It is a circular left shift operation.

Mixed Column: It is a matrix multiplication of a constant matrix with a plain text single column.

Add Round Key: It is a Xor operation with results obtained by a mixed column with a key.
Key for first round operation is just Xor operation of plain text with a add round key and further round key scheduling operations will take place.
S-Box implementation sometimes performed by lookup table implementing with LUT, the area consumed more and side channel attacks increases, security complexity arises. So implementation of s-box with a combinational will make a design with a less area and improved resistances against the side channel effects. The Galois field of s-box implementation takes multiplicative inverse in GF (2^8) followed by a affine transformation bit it will costs lot of hardware resources. Another way to this approach is factor out to lower level Galois fields as follows GF(2^4),GF(2^2) and GF(2) and change back to GF(2^8).

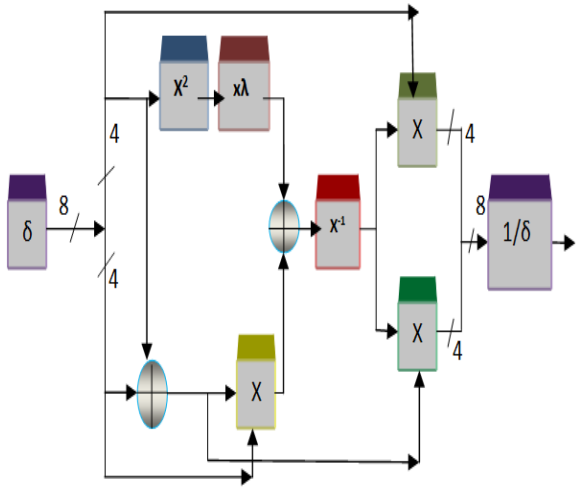

Fig.2.Module for the S-box

Pictorial representation of Fig.2. demonstrates converted Galois field operations in s-box for multiplicative inversion module. Delta represents in figure isomorphic and inverse delta represents inverse isomorphic plotted to composite fields.

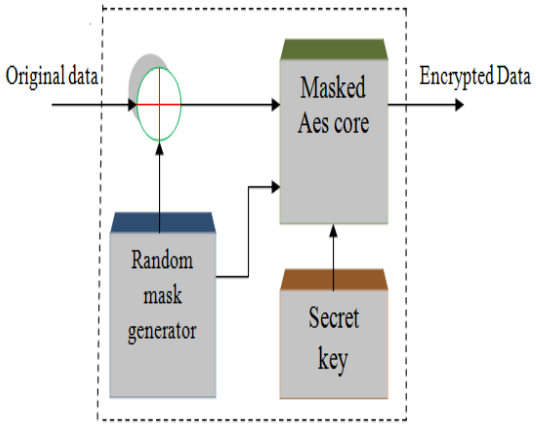

Fig.3.Masking AES Core Architecture

Pictorial representation of Fig.3. demonstrates a proposed masking AES architecture, the thoughts behind this proposal is to step up the design more secure and resistive from side channel attacks. Pictorial representation of Fig.4.demonstrates microscopic view of AES core.
Proposed design consists of a masked AES core and 128 bit LFSR. Random mask generator used to generate random mask. At source end original data is masked by a Xor with a random mask. The Xor output fed to the AES core, in it adds an encryption with a key results a cipher text. The obtained cipher text passes through communication channel with more added security. At destination end the cipher text is given input into the unmasking module to obtain original data.

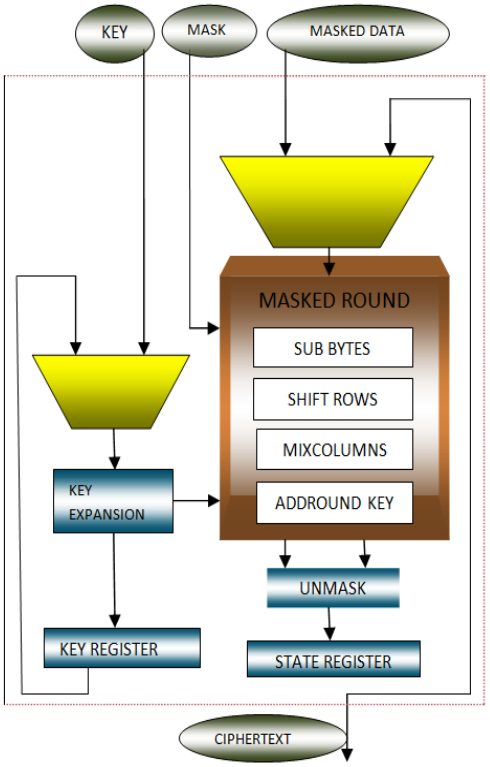

Fig.4.Microscopic View of Masking AES Core

III. COMPARISION OF AREA AND POWER SIMULATED RESULTS

Table-I:Comparision of LUT's Utilization of AES with Pipeline and AES with Masking

Technology	Resources	Utilization	Available	Utilization%
AES algorithm with pipeline	LUT	24669	607200	8.13
AES algorithm with masking	LUT	24580	607200	8.02

IV. RESULTS

Fig.5.AES Algorithm Encryption

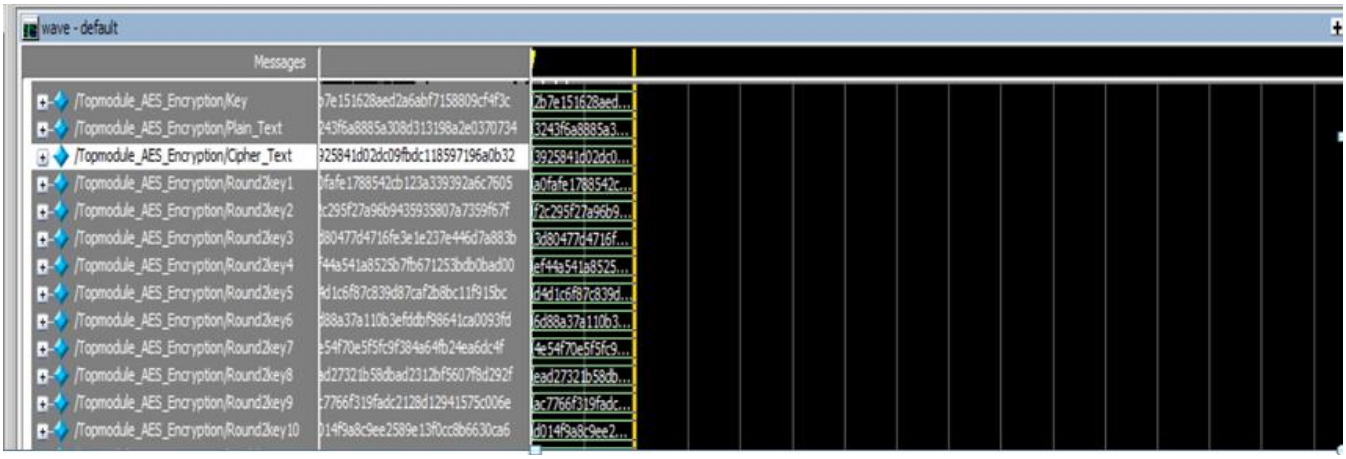

Fig.6.AES Algorithm with Pipeline

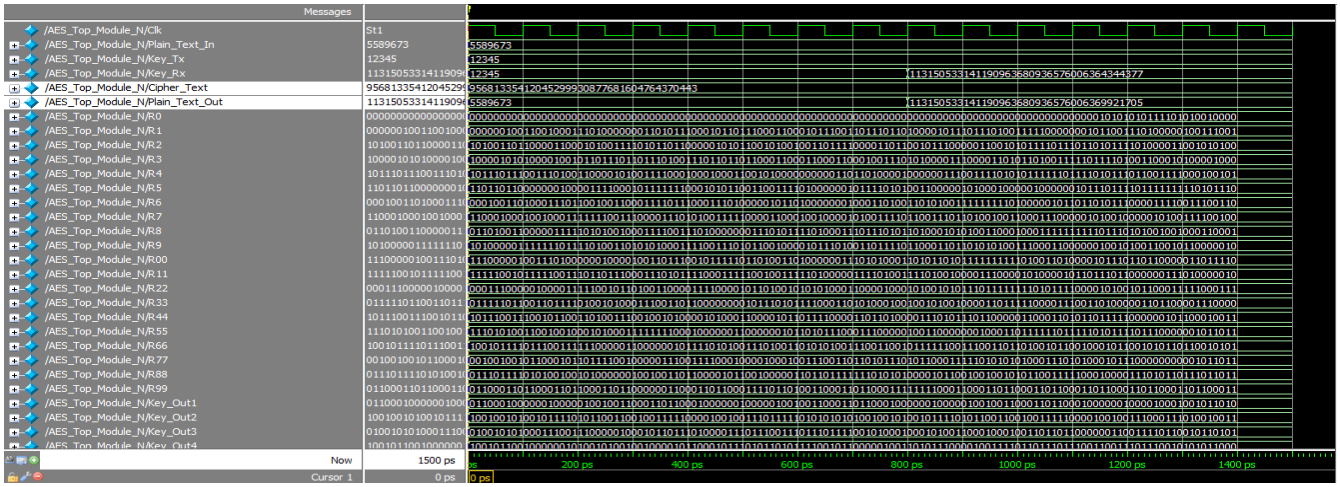

Fig.7.AES Algorithm with Masking

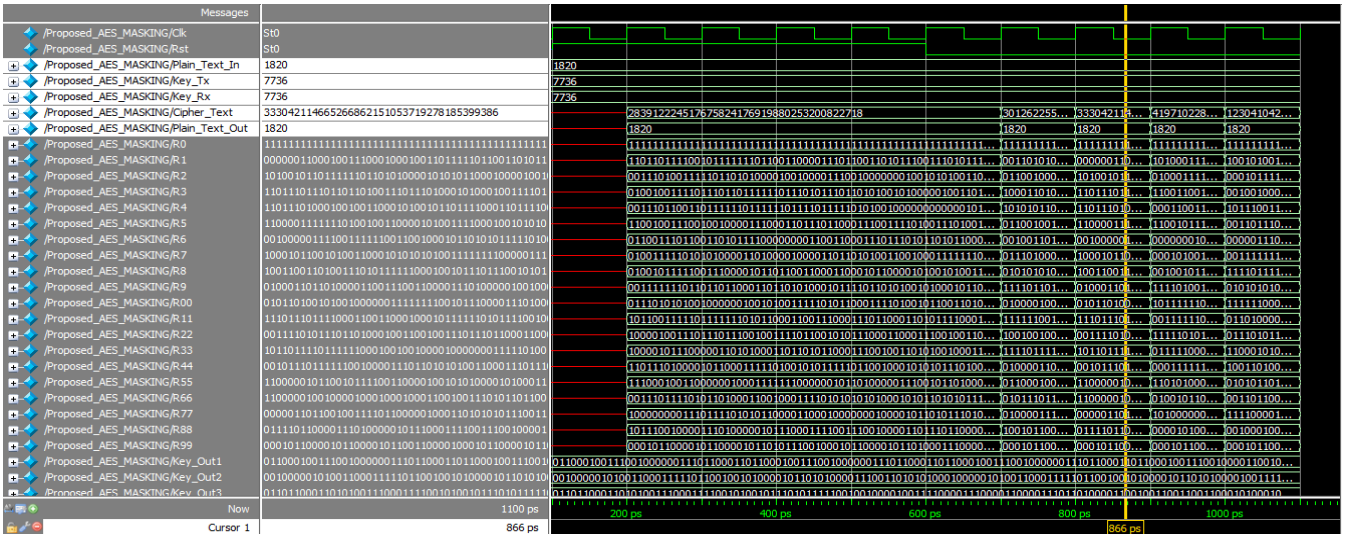

Table-II: Comparison Of Power Consumption

Technology	Power
AES algorithm without pipeline	3222
AES algorithm with pipeline	3148.368
AES algorithm with pipeline	3281.958

V. CONCLUSION

A novel approach to elude side channel attacks by using masking 128 bit AES design implementation illustrates the design upgrades the security through communication networks and elude side channel attacks from intruders.
The proposed design consumes less power as contrast to AES encryption algorithm. This is attained by using pipeline architecture in compare with AES encryption algorithm as shown in Table-I.
The major development in proposed design the LUTs used in either AES algorithm or makes AES algorithm are almost equal and hardware usage cutting down to lower level as compared to previous design proposed as shown in Table-II.

REFERENCES

1. Y. Chou And S. L. Lu, " A High Performance, Low Energy, Compact Masked 128 Bit Aes In 22nm Cmos Technology",2019 International Symposium On Vlsi Design, Automation And Test(Vlsi-Dat),Hsinchu,Taiwan,Pp.1-4.
2. Announcing The Advanced Encryption Standard(Aes), Fips Pubs, Nist, Usa, November 26,2011.
3. W.Yu And Kose, "A Lightweight Masked Aes Implementation For Securing Iot Against Cpa Attacks", In Ieee Transaction On Circuits And Systems I:Regular Papers,Vol.64,No.11,Pp.2934-2944,Nov.2017.
4. Regazzoni,Francesco,Yi Wang,And Francois-Xavier Standaert, "Fpga Implementation Of The Aes Masked Against Power analysis attacks" In proceedings of COSADE,Vol.2011,pp.56-66,2011.
5. Mangard,Stefer,Norbert Pramsaller,and Elisabeth Oswald. "Successfully attacking masked AES hardware implementations"In International Workshop on Cryptographic Hardware and Embedded Systems,pp.157-171,Spronger,Berlin,Heidelberg,2005.
6. Balamurugan.J,and E.logashanmugham. "Design of High Speed and Lowe Area Masked AES Using Complexity Reduced Mix-Column Architecture",Intenrational Journal of Computer Science and Engineering Communications 2,no.2(2014):428-433.
7. Trichina, Elena, Domenico De Seta, And Lucia Germane. " Simplified Adaptive Multiplicative Masking For Aes." In International Workshop On Cryptographic Hardware and Embedded Systems,pp.187-197,Springer,Berlin,Heidelberg,2002
8. Peng,Yimai,Haobo Zhao,XUn Sun,and Chen Sun. " A side-channel attack resistant AES with 500Mbps,1.92 pj/bit PVT variation tolerant true random number generator",In 2017 IEEE Computer society Annual Symposium on VLSI(ISVLSI),pp.249-254. IEEE,2017.
9. Putra,Septafiasnsyah Dwi,Adang Suwandi Ahmad,Sarwono Sutikno,and Yusuf Kurniawan. "Attacking AES-Masking encryption device with correlation power analysis",International journal of communication networks and information security 10, no.2(2018): 397-402.
10. Jiao, ge, lang li, and yi zou. " an optimized aes masking method for resistive side channel analysis" , in international conference on computer engineering and networks, pp.876-884. Springer, cham, 2018.
11. Oshida,Hirokazu, Rei Ueno, Naofumi Homma , And Takafumi Aoki. " On Masked Galois – Field Multiplication For Authenticated Encryption Resistant To Side-Channel Analysis" , In International Workshop On Constructive Side-Channel Analysis And Secure Design, Pp.44-57. Springer, Cham, 2018.
12. Shvartsman, Phillip, And Xinmiao Zhang. "Side Channel Attack Resistant Aes Design Based Based On Finite Field Construction Variation" , In 2019 Ieee International Workshop On Signal Processing Systems (Sips), Pp.67-72. IEEE, 2019.

AUTHORS PROFILE

PALLAVI Completed B.Tech In ECE From Godutai Engineering College For Women, Kalaburigi. Currently Pursuing M TECH In VLSI And Embedded Systems From RNSIT, Bangalore.

SEERAPU ANIL NAGENDRA Pursuing M Tech in VLSI Design from GITAM Deemed to be University, Visakhapatnam.
Currently Doing Internship in SoC Design verification SION SEMICONDUCTORS PVT LTD, Bangalore.

DR S V UMA Working as associate professor in RNSIT, Bangalore. received Best Paper Award for the paper titled A Cross Layer UDP-IP protocol for efficient Congestion Control in Wireless Networks, in International Journal of Computer Science and Information Security, Vol.11, No.12, December 2013, pages 58-68, ISSN 1947-5500.