International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 3, March 2016

Review on Realization of AES Encryption and Decryption with Power and Area optimization

[1] Mohini Mohurle [2] Prof. Vishal V.Panchbhai
[1] M.Tech [2] Professor
[1] [2] Department of Electronics and communication Engineering
Priyadarshini College of Engineering
Nagpur, India
[1] mohinimohurle@gmail.com [2] Vishal_panchbhai@rediffmail.com

Abstract: **In this project, a hardware implementation of the AES-256 encryption and decryption algorithm is proposed. The AES cryptography algorithm can be used to encryption and decryption blocks of 128 bits and is capable of using cipher keys of 256 bits. Feature of the proposed pipeline design is depending on the round keys, which are consumed different round of encryption, are generated in parallel way with the encryption process. This lowers delay of the each round of encryption and reduces the encryption delay of a plaintext block. Xilinx ISE.14.7 (64-bit) is used for simulation by using VHDL and hardware implementation on FPGA(Xilinx Spartan 6 or Altera Cyclone 2 FPGA device).**

Keywords—: **Cryptography, Cipher, FPGA, Advanced Encryption Standard (AES), VHDL.**

I. INTRODUCTION

An encryption is the conversion of data into a secret code. It is the most effective way to achieve the data security. To read an encrypted file, one must have an access to a secret key or password that enables us to decrypt the information. The unprocessed data is called the plain text, the encrypted data is referred to as the cipher text. To break the password, there are different types of attacks that include Brute force attack, Known plaintext attack, Chosen cipher text attack, Cipher text attack. The Brute force attack on AES-128 bit up to 5^{th}roundand the further analysis get stop. There are various algorithms available in cryptography like MARS, RSA, TWOFISH, SERPENT and RIJNDAEL. Advanced Encryption Standard is called as a Irondale Cryptography. AES is better than Data Encryption Standard (DES). The DES algorithm broken because of short keys. AES can be implemented both on hardware and software. Main aim of AES hardware implementation to minimize hardware and lower the power consumption and also maintain high throughput at highest operating frequency [1].

AES is a symmetric encryption algorithm process data in block of 128 bits. A 128-bit block is encrypted by transforming it in a same way into a new block of the same size. The only secret necessary to keep for security is the key.AES algorithm with encryption and decryption was design in Virology Hardware Description Language. The 128-bit plaintext, 128-bit key expansion and 128-bit output data all divided into four 32-bit consecutive units respectively controlled by the clock. The pipelining technology was utilized in the 13 round transformations so that the new algorithm formed a balance between speed and chip area.AES use different key-lengths, the standard defines three lengths and the resulting algorithms are named AES-128,AES-192 and AES-256 respectively with different length in bits of the key. In AES-256 encryption and decryption with 256-bit key is considered.AES provides combination of security, performance and efficiency. For any security, here key size is important because of this it determines the strength of security, area optimization and power consumption [5].

II. LITERATURE REVIEW

Pritamkumar Khose et al. implementing AES hardware to achieve less area and low power consumption which maintain throughput of data, to achieve high speed data processing and reduce time for key generating.The implementation of AES algorithm uses pipeline structure for repeated computation by lower down speed and data rate is capable to support USB protocol[1]. Hrushikesh Deshpande et al. proposed AES architecture is based on optimizing area in terms of reducing number of slices

required for design of AES algorithm in VHDL. The AES algorithm optimized throughput per number of slices. Efficiency parameter being the reliable one for purposes of comparison with other platform like ASIC,ALTERA designs[5]. Yuwen Zhu,Hongqi Zhang and Yibao Bao et al. proposedAES realization method on the reconfigurable hardware ideas, the design uses a state machine to control encryption round module according to the different lengths. The design using HDL Verilog to support serial key length 128/192/256 bits AES encryption and decryption circuit[7]. R.V.Kshirsagar,M.V.Vyawahare et al. proposed high data throughput AES hardware architecture by partitioning 10 rounds into sub blocks of repeated AES modules. The key feature is having high throughput by partitioning the AES into 10 sub-blocks with intermediate buffer between them, thus creating a deep pipelining structure for complete 10 AES blocks. [9].

III. PROPOSED WORK

The AES block diagram, the encryption part of this algorithm, the data to be secured or encrypted is called a plain text (M). The length of plain text will be of 128 bits, with a cipher key/shared key (K) of 256 bits. The plain text (M) and shared key (K) will be converted into cipher text (C) using Encryption part of Rijndael algorithm. In the decryption part, the cipher text (C) will be considered as the input, which will be again operated with the shared key (K). Following are the terminologies which are widely used in ciphering:

- PLAIN TEXT:-Plain text is the information a sender wishes to transmit to one or more receiving Medias. Plain text refers to any message that is not encrypted.
- ENCRYPTION ALGORITHM:-The encryption part of Rijndael algorithm encodes plain text into the cipher text by performing several operations which will be discuss in algorithm.
- SHARED KEY:- Shared key is a particular 256 bit key generated by the key schedule. It can also be called as Secret or cryptographic key that is used by the Key Expansion to generate a set of Round Keys
- CIPHER TEXT:- It is the result of encryption performed on the plain text and shared kay using algorithm. It is the encrypted form of the plain text.
- DECRYPTION ALGORITHM:-The decryption part of Rijndael algorithm decodes the cipher text into plain text.

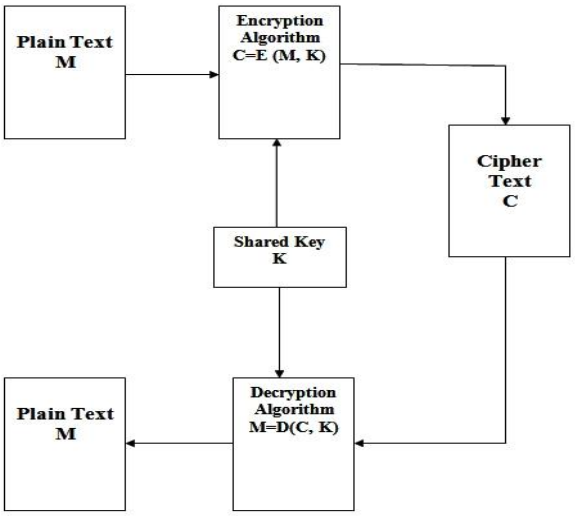

Fig 1: Block Diagram of AES

AES encryption algorithm

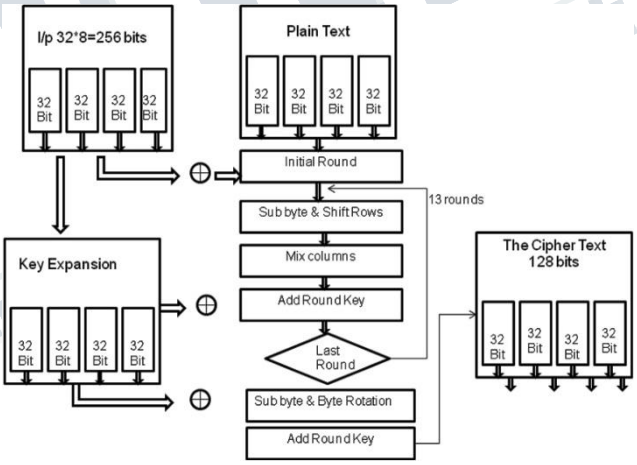

Fig 2: Block diagram of Rijndael AES encryption algorithm

Steps:

- Initial Round:-In initial round128 bit cipher key is EXOR with 128 bit plain text in the form state matrix [4x4].
- Sub-Byte:-The Sub byte transformation is done using a once-precalculated substitution table called S-box. AES S- box is 256 bit, the table consist of two transformations such as multiplicative inverse in Galois field GF (2^8) and affine transformation.

- Encryption S-Box:

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig 3:AES Encryption S-Box

- Shift Rows:-In shift row operation, rows of state are cyclically shifted with a certain number of steps. The bytes are arranged in the form of matrix. The first row of the matrix is unchanged, the second row is shifted by one byte, the third is shifted by two bytes and the fourth row is shifted by 3 positions to the left.

- Mixcolumns:-Mixcolumns transformation deals independently with every column of the state array. To calculate the Mixcolumn transformation, the columns of the present state are considered as polynomials over GF(2^8).If the multiplication of the columns exceeds 2^8 then the resultant polynomial go beyond the GF and the algorithm will not work.hence to bring back the polynomial in the field it is multiplied by an irreducible polynomial.

- Add Round Key:- The round key is applied to the resultant polynomial from mix column by performing bitwise EXOR operation between the resultant polynomial and new cipher key generated by key schedule into four rounds of 32 bit round operating elements.

- Last Round:- The final round is 128 bit processor after thirteen rounds of operation included shiftrows, subbytes and micolumns,128bit intermediate encrypted data will be used in EXOR operation with the final expanded key (4*32 bit),which is provided by key expansion module. The output of final round in processor is desired 128 bit ciphertext, The ciphertext is divided into four packets of 32 bit data by an external enable signal.

IV. METHODOLOGY

- Implementation of AES encryption algorithm using VHDL to convert plaintext into ciphertext with initial key.
- Implementation of AES decryption algorithm using VHDL will giving the output of encryption to the decryption module to get same output will be regenerated the original plaintext with same key.
- Utilizing pipeline technology in the round transformation for high throughput.
- Optimizing the design to keep balance between throughput and area.
- To implement the AES encryption and decryption on FPGA for the verification of the design.

V. CONCLUSION

The Rijndael cipher design is well suited for hardware use. This implementation can be carried out through different trade-offs between area and speed. The trade-offs is that AES requires additional power and may not be supported by hardware, also there is wide range of equipment used for encryption which is needed for authentication and security. AES can be programmed in software or built with pure hardware.The AES is the latest standard for cryptography and has been taken wide support to secure digital data.

REFERENCES

[1] Pritamkumar N. Khose, Prof. Vrushali G. Raut, "Implementation of AES Algorithm on FPGA for Low Area Consumption",2015 International Conference on Pervasive Computing (ICPC).

[2] Wenfeng Zhao, Yajun Ha andMassimo Alioto,"Novel Self-Body-Biasing and Statistical Design for Near-Threshold Circuits With Ultra Energy-Efficient AES as Case Study",IEEE transactions on very large scale integration (VLSI) systems, vol. 23, no. 8, august 2015.

[3] Mostafa Taha, and Patrick Schaumont,"Key Updating for Leakagez Resiliency With Application to AES Modes of Operation",IEEE transactions on information forensics and security, vol. 10, no. 3, march 2015.

[4]Franck Courbon, Jacques J. A. Fournier,Philippe Loubet-Moundi, and Assia Tria, "Combining Image

Processing and Laser Fault Injections for Characterizing a Hardware AES",IEEE transactions on computer-aided design of integrated circuits and systems, vol. 34, no. 6, June 2015.

[5]Hrushikesh.S.Deshpande, Kailas.J.Karande Altaaf.O.Mulani,"Efficient implementation of AES algorithm on FPGA",International Conference on Communication and Signal Processing, April 3-5, 2014, India .

[6] Kyungtae Kang, Member, IEEE, Junhee Ryu, and Dong Kun Noh, "Accommodating the Variable Timing of Software AES Decryption on Mobile Receiver",IEEE systems journal, vol. 8, no. 3, September 2014.

[7] Yuwen Zhu, Hongqi Zhang, Yibao Bao, "Study of the AES realization method on the reconfigurable hardware",2013 International conference on Computer Science and application.

[8] An Wang, Man Chen, Zongyue Wang, and Xiaoyun Wang, "Fault Rate Analysis: Breaking Masked AES Hardware Implementations Efficiently",IEEE transactions on circuits and systems—ii: express briefs, vol. 60, no. 8, august 2013.

[9] Dr.R.V.Kshirsagar, M.V.Vyawahare, "FPGA implementation of high speed VLSI Architecture for AES algorithm", 2012 fifth International Conferernce on emerging trends in engineering and technology.

[10] Bin Liu and Bevan M. Baas, "Parallel AES Encryption Engines for Many-Core Processor Arrays",IEEE transactions on computers, vol. 62, no. 3, march 2013.