Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 3, Issue 2, May 2019

Design and Implementation of Secure Cryptographic Algorithm Using Vedic-Mathematics

Snehapriya M
Dept. of ECE, The Oxford College of Engineering,
Bangalore, India,
snehapriya196@gmail.com

Manju Devi
Dept. of ECE, The Oxford College of Engineering,
Bangalore, India,
manju3devi@gmail.com

Abstract: In the world of digitization, security is the main aspect and security of data plays an important role in communication and the field of electronics. One of the highly flexible security standard algorithm, AES provides a secure communication over the network. This paper explains the importance of the AES with the combination of Vedic-mathematics. There are mainly four steps in AES, which include add-round key, sub-bytes, shift-rows, mix-columns. This paper mainly concentrates on mix-columns. The analysis and simulation is done using MATLAB, Modelsim tools. This method of implementing AES using Vedic-mathematics improves the performance in terms of speed, power and area.

Keywords: Cryptography; AES; MATLAB; Modelsim; Vedic-Mathematics.

I. INTRODUCTION

Cryptography is a well-known data security algorithm which is used till date. Cryptography is a science of converting message into unrecognizable form and provides resistance for stealing the information. Secure information is an important part of communication. Making changes in secret keys rises a provision of complexity and security of the algorithm. Cryptographic algorithms consume large memory space and more execution time. AES is a symmetric key cipher which does both encryption and decryption on blocks of data.

The most commonly used encryption standard is advanced encryption standard. This standard is defined as the strongest encryption algorithm. Even though it is a strongest algorithm, hackers have been successful in breaking the algorithm and retrieving the hidden data. This rises a requirement to develop more secure algorithm. Thus, to develop a secure algorithm AES is combined with the Vedic-mathematics to perform multiplications involved in AES. This increases the efficiency of the algorithm with respect to area and power.

II. EXISTING SYSTEM

The AES is algorithm is a symmetric block cipher which has different block lengths and key lengths specified to be 128, 192, 256 bits. The AES parameters depend on the key length. The four different stages of AES are add round-key, substitution-bytes, shift-rows and mix-columns. A 4×4 matrix is known as a state array. Each byte in a state array is a component within a Galois' field 28. Depending on the size of the key, the number of rounds are 10, 12, 14 for 128, 192, 256 bits respectively. In every round all the four steps of AES are performed. The existing method depends on the look table approach.

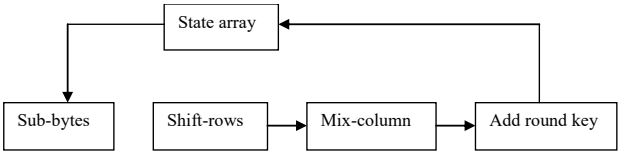

Fig 1. Single round AES for encryption

Each round of AES includes the following basic steps:

i) *Add Round Key:* Add round-key step involves bit-XORing round key with the state array matrix. Key is often generated using the key expansion algorithm.

ii) *Sub-Bytes:* The data obtained by the Add round-key is then modified by sub-byte transformation. This step uses a table of pre-defined value called S-BOX table. It performs byte by byte substitution of each byte of the state array matrix. The inverse of this step is performed at the decryption which uses Inverse S-BOX table.

iii) *Shift Rows:* It is cyclic shift of elements to the left by one position for the matrix obtained by the sub-bytes step. The first row elements remain the same as the sub-byte matrix. The shifting of elements is done row wise.

iv) *Mix-Columns:* Mix-columns are implemented by performing matrix multiplication using Galois' field i.e. GF(2^8). For the mixed columns step to perform requires a pre-defined look up table for both

encryption and decryption. All the 256 values have to be stored to perform multiplication. A state matrix for encryption and decryption are defined for mix-columns.

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

Fig 2. SBox values

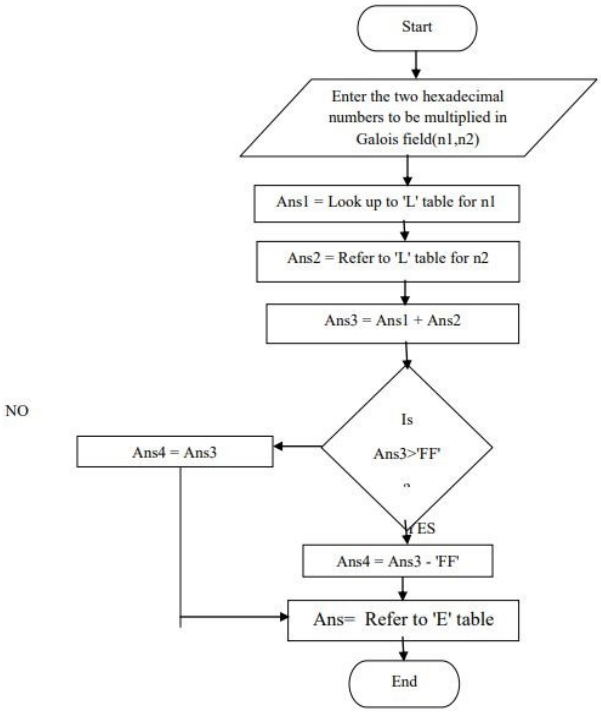

Fig 3. Flowchart of existing system

The state matrices are:

$$A = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$ for encryption, and

$$B = \begin{bmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{bmatrix}$$ for decryption.

III. PROPOSED SYSTEM

Vedic-mathematics is an ancient form of mathematics. There are 16 sutras or formulas in Vedic- mathematics. These formulas are very easy to learn, analyze and are used for fast computation. For multiplication UrdhwaTriyakbhyam is the most popular sutra. UrdhwaTriyakbhyam means "vertically clockwise". Multiplication starts from the extreme digits each time when we multiply. Then the results are concatenated to get the final product.

In this method of multiplication the intermediate values are obtained by ANDing the inputs and adding the bi-product. In Vedic-mathematics addition is not used. Instead XOR operation is used. This is also done Galios' field GF(2^8). Hence the output we get is limited to 8bits. The advantage of this method is that, multiplication of large number of bits can be performed with the smaller and efficient multiplier. This is used for unsigned numbers and also for binary numbers.

E Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	03	05	0F	11	33	55	FF	1A	2E	72	96	A1	F8	13	35
1	5F	E1	38	48	D8	73	95	A4	F7	02	06	0A	1E	22	66	AA
2	E5	34	5C	E4	37	59	EB	26	6A	BE	D9	70	90	AB	E6	31
3	53	F5	04	0C	14	3C	44	CC	4F	D1	68	B8	D3	6E	B2	CD
4	4C	D4	67	A9	E0	3B	4D	D7	62	A6	F1	08	18	28	78	88
5	83	9E	B9	D0	6B	BD	DC	7F	81	98	B3	CE	49	DB	76	9A
6	B5	C4	57	F9	10	30	50	F0	0B	1D	27	69	BB	D6	61	A3
7	FE	19	2B	7D	87	92	AD	EC	2F	71	93	AE	E9	20	60	A0
8	FB	16	3A	4E	D2	6D	B7	C2	5D	E7	32	56	FA	15	3F	41
9	C3	5E	E2	3D	47	C9	40	C0	5B	ED	2C	74	9C	BF	DA	75
A	9F	BA	D5	64	AC	EF	2A	7E	82	9D	BC	DF	7A	8E	89	80
B	9B	B6	C1	58	E8	23	65	AF	EA	25	6F	B1	C8	43	C5	54
C	FC	1F	21	63	A5	F4	07	09	1B	2D	77	99	B0	CB	46	CA
D	45	CF	4A	DE	79	8B	86	91	A8	E3	3E	42	C6	51	F3	0E
E	12	36	5A	EE	29	7B	8D	8C	8F	8A	85	94	A7	F2	0D	17
F	39	4B	DD	7C	84	97	A2	FD	1C	24	6C	B4	C7	52	F6	01

L Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0		00	19	01	32	02	1A	C6	4B	C7	1B	68	33	EE	DF	03
1	64	04	E0	0E	34	8D	81	EF	4C	71	08	C8	F8	69	1C	C1
2	7D	C2	1D	B5	F9	B9	27	6A	4D	E4	A6	72	9A	C9	09	78
3	65	2F	8A	05	21	0F	E1	24	12	F0	82	45	35	93	DA	8E
4	96	8F	DB	BD	36	D0	CE	94	13	5C	D2	F1	40	46	83	38
5	66	DD	FD	30	BF	06	8B	62	B3	25	E2	98	22	88	91	10
6	7E	6E	48	C3	A3	B6	1E	42	3A	6B	28	54	FA	85	3D	BA
7	2B	79	0A	15	9B	9F	5E	CA	4E	D4	AC	E5	F3	73	A7	57
8	AF	58	A8	50	F4	EA	D6	74	4F	AE	E9	D5	E7	E6	AD	E8
9	2C	D7	75	7A	EB	16	0B	F5	59	CB	5F	B0	9C	A9	51	A0
A	7F	0C	F6	6F	17	C4	49	EC	D8	43	1F	2D	A4	76	7B	B7
B	CC	BB	3E	5A	FB	60	B1	86	3B	52	A1	6C	AA	55	29	9D
C	97	B2	87	90	61	BE	DC	FC	BC	95	CF	CD	37	3F	5B	D1
D	53	39	84	3C	41	A2	6D	47	14	2A	9E	5D	56	F2	D3	AB
E	44	11	92	D9	23	20	2E	89	B4	7C	B8	26	77	99	E3	A5
F	67	4A	ED	DE	C5	31	FE	18	0D	63	8C	80	C0	F7	70	07

Fig 4. E and L-tables

The structure of UrdhwaTriyakbhyam looks like array multiplier structure. The overall delay is reduced by the implementation of this sutra. We can obtain the product of two umbers in the single step. Hence this approach is area and speed efficient.

This method is applied for both mix-columns in encryption and inverse mix-columns in decryption.

The architecture was implemented on a Spartan 3 FPGA and the area and speed values for the same are showcased in table 2.

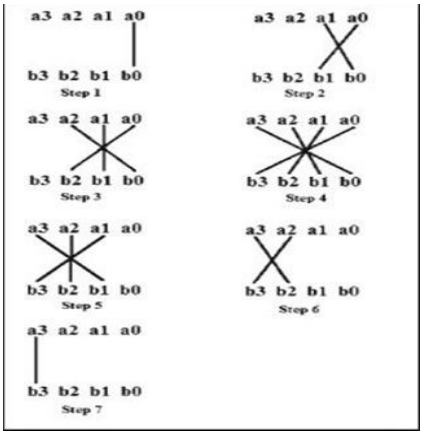

Fig 5. Vedic-multiplication

Bit pattern	Key length (words)	Block length (words)	No. of rounds
AES-128	4	4	10
AES-192	6	5	12
AES-256	8	4	14

Table 1. No. of rounds of AES

Methods	No. of cycles (max)	No. of registers
LUT	6	4088
Vedic multiplier	4	8

Table 2. No. of registers and cycles of operation

IV. SIMULATION RESULTS

The following figures show input and output waveforms depicting the outcomes of AES.

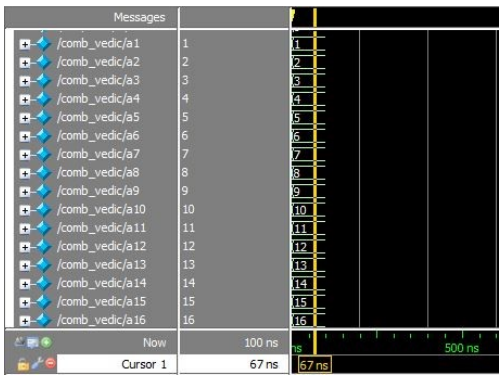

Fig 6. Input values

Fig 7. Output waveform

V. CONCLUSION

In this paper encryption is performed using 128 bit key with the use of Vedic mathematics. This network security algorithm has wide application in communication security. The code can be optimized for efficient area and time consumption parameters and used for high end applications.

REFERENCES

[1] Nidhi Gaur, AnuMehra, "Enhanced AES architecture using extended set ALU at 28nm FPGA", International conference on signal processing and integrated networks, SPIN, IEEE 2018.

[2] Sheetal U Jonwal, Prathibha P Shingare, "Advanced encryption standard implementation on FPGA with hardware in loop", International conference on trends in electronics and informatics, ICEI, IEEE, 2017.

[3] Sonam Negi, Satendra Kumar Chauhan, "Implementation of AES employing systolic array and pipeling approach", IEEE, 2018.

[4] S. Rao Rupanagudi et al., "A Further Optimized Mix Column Architecture Design for the Advanced Encryption Standard," 2019 11th International Conference on Knowledge and Smart Technology (KST), Phuket, Thailand, 2019, pp. 181-185.

[5] S. R. Huddar, S. R. Rupanagudi, R. Ravi, S. Yadav and S. Jain, "Novel architecture for inverse mix columns for AES using ancient Vedic Mathematics on FPGA," 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Mysore, 2013, pp. 1924-1929.

[6] S. R. Rupanagudi et al., "A novel and highly secure encryption methodology using a combination of AES and visual cryptography," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, 2016, pp. 1682-1688.

[7] William Stallings, "Advanced encryption standard", Cryptography and network security principles and practice, 3rd edition , chapter 5.

[8] Ambika R, C S Mala, "FPGA implementation of AES using Vedic mathematics" International journal of innovative research in science and engineering, IJIRSE, Nov 2013.

[9] Soumya Sadanandan, Anjali V, "Design and implementation of advanced encryption standard using Vedic mathematics", International journal of innovative research in advanced engineering, vol-1,issue-6, July 2014.

[10] Amit Kumar, Manoj Kumar, "Implementation of AES algorithm using VHDL", International conference on computing methodologies, ICCMC, proceedings of IEEE, 2017.