IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 7, July 2016

Design, Implementation and Comparison of Mix Column Architecture using Different Techniques

Anil Kumar S K[1], Dr. Kalpana A B[2]

M.Tech Student, Department of ECE, Bangalore Institute of Technology, Bangalore, India [1]

Assistant Professor, Department of ECE, Bangalore Institute of Technology, Bangalore, India[2]

Abstract: Cryptography is a technique of securing the data from hackers. The most popular method employed for cryptography is Encryption. Many researchers around the world have contributed towards improvising encryption methods. This paper explains the two architectures with which the data can be encrypted.

Keywords: AES, VLSI, Cryptography, LUT, Splitting

I. INTRODUCTION

Technology has changed our lives in many aspects – from the advent of natural user interfaces [1], [2], safeguarding our lives [3], and in helping those who are physically weak/challenged [4], [5], [6]. It has also changed the mode of communication from hand-written letters to wired communication to wireless [7], [8], [9]. Now-a-days, most of the communication modes are dependent on Internet. Even the secret messages are being stored and sent through servers.

It is noticeable that in recent past, the rate of Internet hacking has increased. Thus, securing data using cryptographic techniques is gaining more importance now-a-days. Cryptography involves converting a message text into an unreadable cipher, using hidden writing maintaining security and privacy [10]. A large number of Encryption and Decryption algorithms for the cryptography are available. In order to keep pace with maturity of the security technology such as the hackers, the electronic eavesdroppers, electronic frauds and the virus have been coming into the field with new improved techniques for to attack the security mechanism [11].

Advanced Encryption Standard (AES) was adopted as a standard by the US government, a symmetric-key encryption method (Encryption and Decryption using same key) succeeding the DES (Data Encryption Standard) and 3DES (3-times DES). AES has 10 rounds of complex algebraic and matrix operation which involve high processing power and introduce delay in encryption and decryption process. The sub module Mix Column operation in AES provides the maximum confusion with the data involving Galois field Multiplication. Galois field multiplication is one of the complex operations involving polynomial division after the multiplication for its reduction.

The paper discusses about improvising the AES module. The following are the sections involved in the paper: Section II describes the brief AES Algorithm, Section III describes Mix Column Transformation, Section IV showcases Conventional approach; Section V portrays Look up Table approach. Section VI summarizes on the Results and Section VII concludes the paper.

II. AES ALGORITHM

AES algorithm is an iterative method to compute the cipher text of the message, which is always fixed to be a 16 byte (128bits) input. The number of iterations usually depends on the length of the key used which can be of 128,192,256 bits and corresponding rounds to be 9, 11 and 13 respectively. Fig 1 shows the steps performed in each of the iteration.

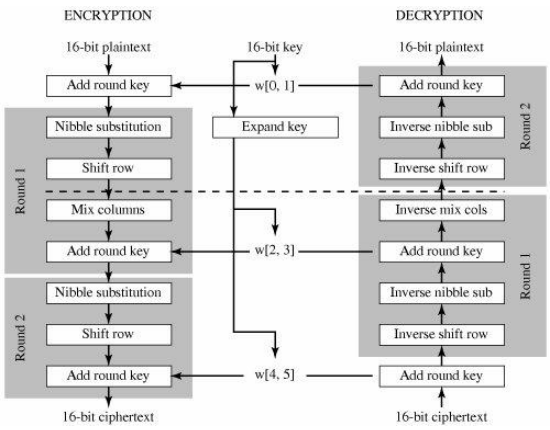

Fig 1. AES Algorithm

The following are the steps involved in AES:

- Add Round Key: The input data is XORed with the key.
- Byte Substitution: Using S-box table, each byte is replaced with the corresponding one in the table.
- Shift Row: Each row of the array is rotated by a certain number of byte positions. No shift in first row, one left shift of bytes in the second row, two left shifts of bytes in the third row, and three left shift operation in the last row.
- Mix Column Transformation: Discussed in next section.

III.MIX COLUMN TRANSFORMATION

In AES, Mix Column operation is implemented with the help of the diffusion operation which shuffles the data based on mathematical model on Galois Field [12].This is one of the most power hungry modules which is operated as nonlinear process that makes use of arithmetic over Galois Field (28) to provide the maximum confusion. In

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 7, July 2016

this operation, the input data is represented by an individual 4x1 matrix, which is multiplied (GF) by a constant 4x4 matrix shown Fig 2. Thus, the coefficients of each term of the polynomial can take the value 0 or 1. Here, we have considered GF (28), which is modulo 8. Any hexadecimal value can be represented by bit string of length 8, each bit corresponding to a binary weighted bit value. The LSB of the coefficient represents the constant of the polynomial, and going from right to left, the coefficient of x_i is represented by the bit b_i where b_i is i bits to the left of the least significant bit.

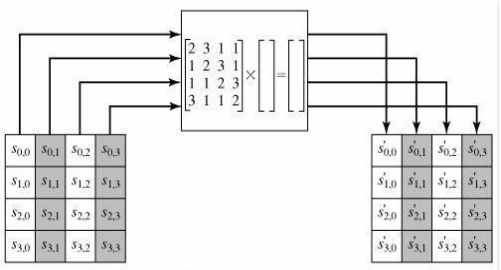

Fig 2. Mixcolumn transformation during encryption

As an example, the bit string 10101011 represents $x^7+x^5+x^3+x^1+1$. In the polynomial representation, multiplication in GF (2^8) corresponds with the multiplication of polynomials modulo an irreducible polynomial of degree 8. A polynomial is irreducible if its only divisors are one and itself. For the AES algorithm, the irreducible polynomial is given by the equation $m(x) = x^8 + x^4 + x^3 + x^1 + 1$.

Example: Multiplication of two polynomials, in this example leads to result of a new polynomial which has degree greater than 7 that is 10.

$$\begin{array}{r} x^4+x+1 \\ \times \quad x^6+1 \\ \hline x^4+x+1 \\ \oplus \quad x^{10}+x^7+x^6 \\ \hline x^{10}+x^7+x^6+x^4+x+1 \end{array}$$

Fig 3: Multiplication of two polynomials

In order to reduce it to a polynomial less than 8, we perform polynomial division by an irreducible constant $x^8 + x^4 + x^3 + x^1 + 1$, followed by XOR operation between the dividend and the product of divisor and quotient. The remainder is checked again for having degree greater than 7, if so then it is again divided by the irreducible constant. This process is continued till the remainder is less than of degree 8.

$$\begin{array}{r} x^2 \\ x^8+x^4+x^3+x+1 \overline{)\, x^{10}+x^7+x^6+x^4+x+1} \\ x^{10}+x^6+x^5+x^3+x^2 \\ \hline x^7+x^5+x^4+x^3+x^2+x+1 \end{array}$$

Fig 4. Division of two polynomials

IV. INVERSE MIX COLUMN OPERATION

The reverse process of the Mix Column transformation is the Inverse Mix Column. Inverse Mix Column operates on the State column by column, treating each column as a four term polynomial. Here the constants in polynomial can be created similarly as in mix column operation. The multiplying constant matrix varies in this inverse operation and is as shown in Fig 5.

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} w'_3 \\ w'_2 \\ w'_1 \\ w'_0 \end{bmatrix} = \begin{bmatrix} w_3 \\ w_2 \\ w_1 \\ w_0 \end{bmatrix}$$

Fig 5. Mixcolumn transformation during decryption

V. CONVENTIONAL APPROACH

In this approach, we use normal 8 bit multiplier to obtain the product, before polynomial division. It is found that Baugh Wooley multiplier is more efficient compared to other multipliers. Fig 6 shows the block diagram of the Baugh Wooley Multiplier for 5 bit, the same can be extended for 8 bit.

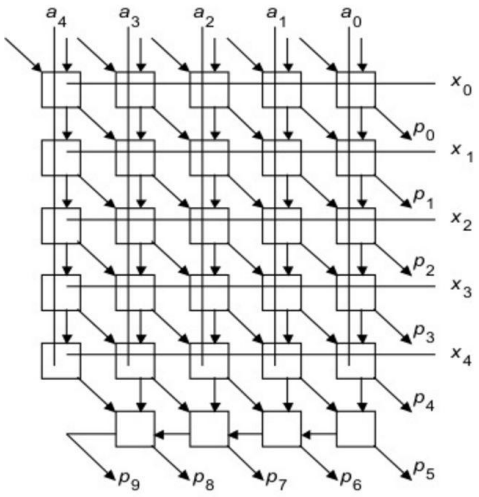

Fig 6. 5X5 Bit Baugh Wooley multiplier

VI. LOOK UP TABLE APPROACH

In this approach, two look up tables are defined with 256 values each. Each entry is an 8bit value. The multiplication of Galois Field is achieved by addition of the value obtained from the look up table. If the obtained result is greater than GF (2^8), then 256 is subtracted from it. The result value is retrieved back in another look up table, to obtain the final result.

Method: If the two Hexadecimal values being multiplied are CF &18, using LUT A1 (CF) index which returns D1, and then that of second value A1 (18) which returns 4C. Now add the values, D1+4C = 11D. Since 11D > FF, we perform: 11D-FF which gives us 1E. Using LUT A2 (1E) = 66. Thus, the end result of multiplying CF &18 over a Galois Field is 66.

DOI 10.17148/IJIREEICE.2016.4705

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 7, July 2016

	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

Fig 7. Table A1

	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 8. Table A2

VII. RESULTS

Table 1 shows the comparison between the mix column architecture using two different approaches.

TABLE I
COMPARISON OF DIFFERENT APPROACHES

Approach	No of LUT's	Path Delay
Baugh Wooley	112	7.4775ns
Look Up Table	87	19.059ns

VIII. CONCLUSION

The table clearly indicates that the area consumed by the LUT approach, as well as speed of operation is comparatively more than Baugh Wooley approach.

ACKNOWLEDGEMENT

I would like to thank **Dr A.G. Nataraj**, Principal, Bangalore Institute of Technology, for providing this opportunity and **Dr K.V.Prasad**, Head of Department, ECE, Bangalore Institute of Technology, for his constant support and motivation. I also thank Mr. Sudhir Rao Rupanagudi of WorldServe Education for guiding me through the work conducted. And last but not the least I would like to thank my friends, parents, who have helped me in completing this paper.

REFERENCES

[1] P. C. Ravoor, B. S. Ranjani and S. Rao Rupanagudi, "Optimized fingertip blob recognition for image processing based touch-screens," Recent Advances in Computing and Software Systems (RACSS), 2012 International Conference on, Chennai, 2012, pp. 104-108.

[2] P. C. Ravoor, S. R. Rupanagudi and B. S. Ranjani, "Detection of multiple points of contact on an imaging touch-screen," Communication, Information & Computing Technology (ICCICT), 2012 International Conference on, Mumbai, 2012, pp. 1-6.

[3] S. R. Rupanagudi et al., "A novel video processing based smart helmet for rear vehicle intimation & collision avoidance," 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, 2015, pp. 799-805.

[4] Rupanagudi SR, Bhat VG et al (2015) Design and Implementation of a Novel Eye Gaze Recognition System Based on Scleral Area for MND Patients Using Video Processing. Advances in Intelligent Informatics. doi:10.1007/978-3-319-11218-3_51

[5] Rupanagudi SR, Bhat VG et al (2015) Design and Implementation of a Novel Eye Gaze Recognition System Based on Scleral Area for MND Patients Using Video Processing. Advances in Intelligent Informatics. doi:10.1007/978-3-319-11218-3_51

[6] S. R. Rupanagudi et al., "A novel video processing based cost effective smart trolley system for supermarkets using FPGA," Communication, Information & Computing Technology (ICCICT), 2015 International Conference on, Mumbai, 2015, pp. 1-6.

[7] S. R. Rupanagudi et al., "Design of a low power Digital Down Converter for 802.16m - 4G WiMAX on FPGA," Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, New Delhi, 2014, pp. 2303-2308.

[8] S. R. Rupanagudi et al., "A low area & low power SOC design for the baseband demodulator of an indoor local positioning system," 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, 2015, pp. 689-695.

[9] S. R. Rupanagudi, Ranjani B. S., P. Nagaraj, V. G. Bhat and Thippeswamy G, "A novel cloud computing based smart farming system for early detection of borer insects in tomatoes," Communication, Information & Computing Technology (ICCICT), 2015 International Conference on, Mumbai, 2015, pp. 1-6.

[10] K.J. Jegadish Kumar, R. Balasubramanian, "Lightweight Mixcolumn Architecture for Advanced Encryption Standard", International Journal of Computer Applications (0975 – 8887) Volume 136 – No.11, February 2016

[11] Sliman Arrag, Abdellatif Hamdoun, Abderrahim Tragha, Salah eddine Khamlich, "Design and Implementation A different Architectures of mixcolumn in FPGA"

[12] Rajasekar P, Dr. H. Mangalam, "Design of Low Power Optimized MixColumn/Inverse MixColumn Architecture for AES", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 2 (2016) pp 922-926