IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 8, April 2023

VLSI Implementation of AES Algorithm in Cryptography Developed in Xilinx

Mrs. M. Saritha[1], Ranjith. S[2], Vishvanth. R[3], Vijay. R[4]

Assistant Professor, Department of Electronics and Communication Engineering[1]

Students, Department of Electronics and Communication Engineering[2,3,4]

Dhanalakshmi Srinivasan Engineering College (Autonomous), Preambular, India

sarithamani91@gmail.com[1] and ranjith1704s@gmail.com[2], vasanthvishvanth33@gmail.com[3], vijaysparrow12@gmail.com[4]

Abstract: *In the present era of information processing through computers and access to private information over the internet like bank account information, even the transaction of money, and business deals through video conferencing, encryption of the messages in various forms has become inevitable. There are mainly two types of encryption algorithms, a private key (also called a symmetric key having a single key for encryption and decryption) and a public key(a separate key for encryption and decryption). In terms of computational complexity, a private key algorithm is less complex than a public key algorithm. The simple architecture of the private key algorithm attracts the VLSI implementation through the basic digital components like basic gates and flip-flops. Moreover, the high throughput architecture can be realized for the encryption of very large amounts of data, e.g., images and videos, in real-time. The National Institute of Standards and Technology (NIST) adopted Advanced Encryption Standard (AES) as the standard for the encryption and decryption of blocks of data. The draft is published under the name FIPS-197 (Federal Information Processing Standard number 197). AES is an asymmetric key block cipher. It encrypts data of block size 128 bits. The AES algorithm is used in diverse application fields like WWW servers, automated teller machines (ATMs), cellular phones, and digital video recorders.*

Keywords: VLSI

I. INTRODUCTION

In the past cryptography means only encryption and decryption using secret keys, nowadays it is defined in different mechanisms like asymmetric-key decipherment (public-key cryptography) and symmetric-key decipherment (called privet-key cryptography). The public key algorithm is complex and has a very high computation time. Private Key algorithms involve only one key, both for encryption as well as decryption whereas, public key algorithms involve two keys, one for encryption and another for decryption. There were many cryptographic algorithms proposed such as Data Encryption Standard (DES), 2-DES,3-DES, Elliptic Curve Cryptography (ECC), the Advanced Encryption Standard (AES), and other algorithms. Many investigators and hackers are always trying to break these algorithms using brute force and side-channel attacks. The AES is an iterative algorithm and uses four operations in different rounds, namely Sub Bytes, Shift Rows; Mix Columns, and Key Additions transformations. Sub Bytes transformation is done through S-box. S-box is the vital component in the AES architecture that decides the speed/throughput of the AES [1]. The ROM-based approach requires a high amount of memory and also it causes low latency because of ROM access time. Therefore, composite field arithmetic is more suitable for S-box (substitution) implementation its hardware optimization for VLSI implementation is very important to reduce the area and power of the AES architecture.

II. EXISTING SYSTEM

With worldwide communication of private and confidential data over computer networks or the Internet, there is always a possibility of a threat to data confidentiality, data integrity, also data availability. Data encryption maintains data confidentiality, integrity, and authentication. Information has become of the most important assets in the growing demand need to store every single important event in everyday life. Messages need to be secured from unauthorized parties. Encipherment is one of the security mechanisms to protect information from public access. Encryption hides the original content of a message to make it unreadable to anyone, except the person who has the special knowledge to read it.

In the past cryptography means only encryption and decryption using secret keys, nowadays it is defined in different mechanisms like asymmetric-key encipherment (public-key cryptography) and symmetric-key encipherment (called privet-key cryptography). The public key algorithm is complex and has a very high computation time. Private Key algorithms involve only one key; both for encryption as well as decryption whereas, public key algorithms involve two keys, one for encryption and another for decryption. There were many cryptographic algorithms proposed such as Data Encryption Standard (DES), 2-DES,3-DES, Elliptic Curve Cryptography (ECC), the Advanced Encryption Standard (AES), and other algorithms. Many investigators and hackers are always trying to break these algorithms using brute force and side channel attacks. Some attacks were successful as was the case for the Data Encryption Standard (DES) in 1993 [21].

The Advanced Encryption Standard (AES) is considered one of the strongest published cryptographic algorithms. The National Institute of Standards and Technology (NIST) adopted Advanced Encryption Standard (AES) as the standard for the encryption and decryption of blocks of data after the failure of the Data Encryption Standard (DES). The draft is published under the name FIPS-197 (Federal Information Processing Standard number (197) [5]. Moreover, it is used in many applications such as ATM Machines, RFID cards, cell phones, and large servers. AES is widely used for the encryption of audio/video data content in real-time.

III. PROPORSED SYSTEM:

The new architecture of S-BOX has been proposed after 3 modifications to the conventional architecture of S-BOX.

- Introduced an operator (op) after merging some blocks.
- Implementation of multiplicative GF (24) using multiplex or.
- Reduced the critical path of multiplication in GF (22)

Introduced an operator)after merging some blocks.

An operator (op) has been introduced after merging blocks like squarer, multiplication with constant λ, a GF (24) multiplier, and a four bits XOR. The equation of op has been introduced using

Galois field irreducible conversion technique and in the form of an input bit stream. One major operation involved here is finding the multiplicative inverse in GF(28).

This can be done by breaking the GF (28) elements into GF (24). I.e., Any arbitrary polynomial in GF (28) can be represented as bx+c using an irreducible polynomial x2+Ax+B. Here, b is the most significant nibble and c is the least significant nibble. The multiplicative inverse can be found by using the following expression [16].

Where, A=1, B=λ, as the irreducible polynomial used is x2+x+λ. Figure 3 shows the block diagram to find the multiplicative inverse in GF (28) using GF (24) [16]. The mapping structure in different fields along with the irreducible polynomials is as follows. (7) Where ,in(0), in(1), in(2), in(3), in(4), in(5), in(6) are the input bit sin the is zoomorphic mapping module(δ).

IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 8, April 2023

IV. BLOCK DIAGRAM

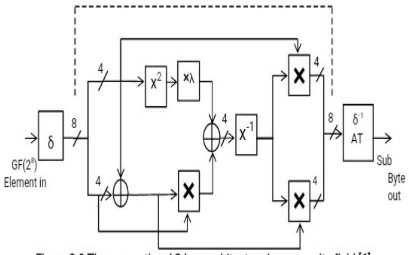
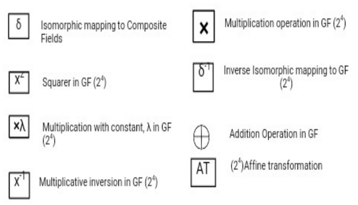
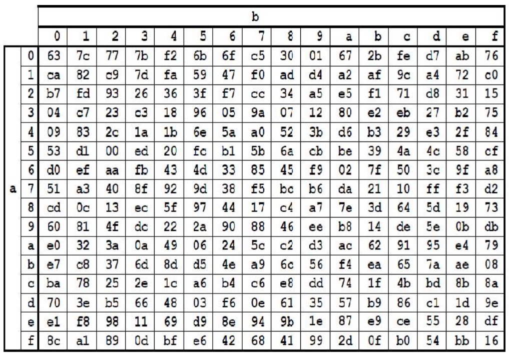
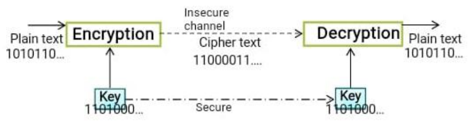


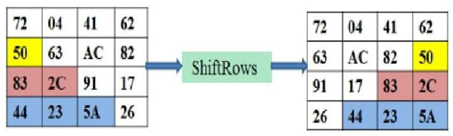
Figure 2-9 The conventional S-box architecture in composite field [6].


δ Isomorphic mapping to Composite Fields
X Multiplication operation in GF (2^4)
X^2 Squarer in GF (2^4)
$δ^{-1}$ Inverse Isomorphic mapping to GF (2^8)
×λ Multiplication with constant, λ in GF (2^4)
Addition Operation in GF
X^{-1} Multiplicative inversion in GF (2^4)
AT (2^4)Affine transformation

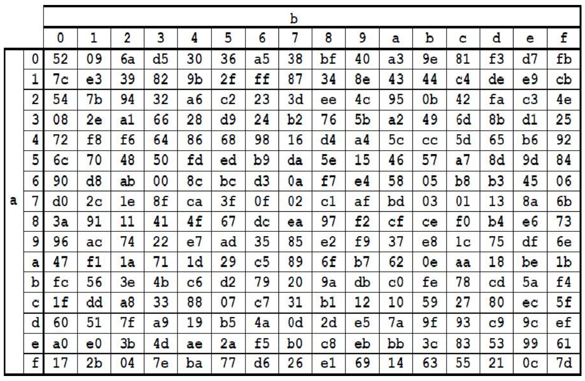


		b															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	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
a	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





V. OUTPUT



		b															
		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
a	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

IJARSCT

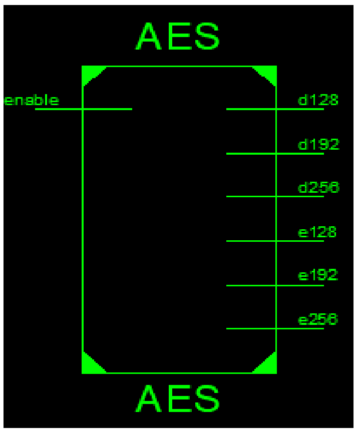
ISSN (Online) 2581-9429

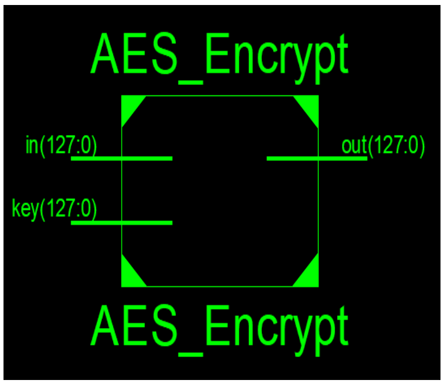
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

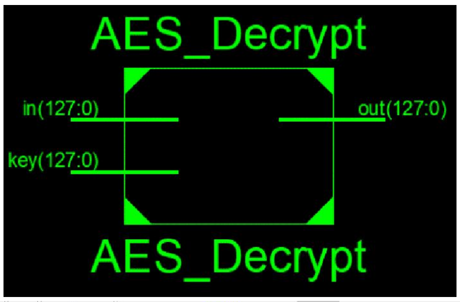
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

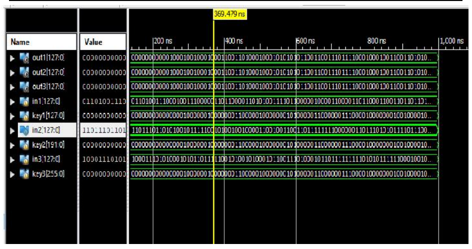
Volume 3, Issue 8, April 2023

Impact Factor: 7.301








```
                              369.479 ns
Name          Value          |200 ns      |400 ns      |600 ns      |800 ns      |1,000 ns
out1[127:0]   00000000000    0000000000010001001000100011001101000100010101010110011001110111100010001001100110101010...
out2[127:0]   00000000000    0000000000010001001000100011001101000100010101010110011001110111100010001001100110101010...
out3[127:0]   00000000000    0000000000010001001000100011001101000100010101010110011001110111100010001001100110101010...
in1[127:0]    01101001110    0110100111000100111000001101100001101010011110110000100001100001101100011001101101101...
key1[127:0]   00000000000    0000000000000010000000100000000110000010000001010000011000000111000010000000010010000010...
in2[127:0]    11011101101    110111011010100101111100101001001000011001001100110111111110000001101110101011101111100...
key2[191:0]   00000000000    0000000000000010000000100000000110000010000001010000011000000111000010000000010010000010...
in3[127:0]    10001110101    100011101010010101101111100101001010001011001110100010110111111111010101111111000100010...
key3[255:0]   00000000000    0000000000000010000000100000000110000010000001010000011000000111000010000000010010000010...
```

VI. CONCLUSION

We have proposed optimized VLSI architecture of the S-box for the AES algorithm. The architecture of the s-box in the composite field has been modified to have high speed and low areas. Using the proposed s-box, AES architecture has been implemented using the merging technique in FPGA. The proposed AES architecture has delayed the improvement of approx. 1.6ns along with an improvement of 287 FPGA slices when implemented in the Spartan-6 FPGA of Xilinx. The full custom design of the s-box has been done in 180 nm technology in Cadence using a novel XOR gate which has high speed and low power consumption as compared to the existing one. The designed s-box chip consumes 22.6µW and has an 8.2n delay after post-layout simulation.

REFERENCES

[1]. B.A. Forouzan and D. Mukhopadhyay, Cryptography and Network Security,2nd Ed., Tata Mc Graw Hill, New Delhi, 2012.

[2]. M. I. Soliman, G. Y. Abozaid, "FPGA implementation and performance evaluation of a high throughput crypto coprocessor," Journal *of Parallel and Distributed Computing*, Vol.71 (8), pp.1075-1084, Aug.2011.

[3]. V. K. Pachghare, Cryptography, and information security, E. E. Ed., PHI Learning, New Delhi,2009.

[4]. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A Lightweight High-Performance Fault Detection Scheme for the Advanced Encryption Standard Using Composite Fields," *IEEE Transactions on Very Large-Scale Integration (VLSI) Systems*, Vol. 19(1), pp.85-91, Jan.2011.

[5]. Federal Information Processing Standards Publication 197 (FIPS197), available online, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[6]. X. Zhang, K. K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm," IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, Vol. 12 (9), pp.957-967, Sep.2004.

[7]. M. Jridi and A. AlFalou, "A VLSI implementation of a new simultaneous images compression and encryption method,"2010 IEEE International Conference on Imaging Systems and Techniques (IST), pp.75-79, July 2010.

[8]. Chih-PinSu, Tsung-FuLin, ChihTsunHuang, and Cheng-WenWu, "A High-Throughput Low-Cost AES Processor," IEEE Communications Magazine, Vol.41(12), pp.86-91, Dec.2003.

[9]. L.Ali, I.Aris, F. S. Hossain and. Roy, "Design of an ultra-high speed AES processor for next-generation IT security," Computers and Electrical Engineering, Vol.37(6), pp.1160-1170, Nov.2011.

[10]. K.H. Chang, Y.C. Chen, C. C. Hsieh, C. W. Huang, and C. J. Chang, "Embedded a Low Area 32-bit AES for Image Encryption/Decryption Application," IEEE International Symposium on Circuits and Systems, pp.1922-1925, May 2009.