International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 6, Number 2 (2013), pp. 259-268

http://www.irphouse.com

Optimization of AES Encryption Algorithm with S-Box

Dr. J. Abdul Jaleel[1], Anu Assis[2] and Sherla A.[3]

Dept. Of Electrical and Electronics Engineering[1,3],
Dept. Of Electronics and Communication[2]
drjaleel56@gmail.com, anushafi@gmail.com sherlashabeer@gmail.com

Abstract

In any wireless communication, security is crucial during data transmission. The encryption and decryption of data is the major challenge faced in the wireless communication for security of the data. These algorithms are used to ensure the security in the transmission channels. Similarly hardware utilization and power consumption are another major things to be considered since most of the mobile terminals are battery operated. In this paper, we use the Advanced Encryption Standard (AES) which works on a 128 bit data encrypting it with 128, 192 or 256 bits of keys for ensuring security. In this paper, we compare AES encryption with two different S-Boxes: S-box with 256 byte lookup table (Rijndael S-Box) and AES with 16 byte S-Box (Anubis S-Box). Optimized and synthesized VHDL code is used for AES encryption. Xilinx ISE 13.2i software is used for VHDL code implementation and Modelsim simulator is used for the simulation.

Keywords: AES(Advanced Encryption Standard), Rijndael, Cryptography, VHDL.

Introduction

As we move into twenty-first century, almost all information processing and telecommunication are in digital formats. In any wireless communication, security is crucial during data transmission. The encryption and decryption of data is the major challenge faced in the wireless communication for security of the data. Most data, for example photos, music and private information can be transmitted through copper, optical or wireless network to a recipient anywhere in the world. In order to protect the data and keep privacy, the information system should be equipped with cryptography and robustness techniques. The cryptographic system is used to protect data transmission over insecure channel. Two type of crypto systems are Symmetric and Asymmetric cryptosystems. AES uses Symmetric Cryptosystem. It is the successor of DES. In DES 56 bit key is used for the encryption, it is insecure in many application. So in 1926 National Institute of Standards and Technology (NIST) proposed a new standard Advanced Encryption Standard (AES) to replace the old Data Encryption Standard (DES). After the evaluation of 15 candidate algorithms, NIST selected the Rijndael as the AES algorithm [6]. Rijndael is the fastest and most efficient algorithm. AES encrypts a data block of 128 bit which is fixed with three different key sizes 128, 192 or 256 bits. Based on Rijndael algorithm 10 rounds of operations are used for 128 bit key for converting plain text to cipher text , 12 rounds for 192 bit key and 14 rounds of operations for 256 bit key [1].

Encryption is the process of converting messages (plaintext) into uneasily readable format known as cipher [4]. Decryption is the reverse operation of encryption. Here cipher text is converted into the original form of the messages. There are several series of mathematical operations that are used for the encryption and decryption processes.

AES Algorithm

DES (Data Encryption Standard) is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES). The Advanced Encryption Standard (AES) Algorithm, adopted by the U.S. government in 2001, is a block cipher transforms 128-bit data blocks under a 128-bit, 192-bit or 256-bit secret key, by means of permutation and substitution. AES replaced the aging DES as the Federal Information Processing Encryption Standard (FIPS). The AES algorithm will be used for many applications within the government an in the private sector. Breaking an AES encrypted cipher text by trying all possible keys is currently computationally infeasible with technology advances.

The AES specifies the Rijndael algorithm, which is a symmetric block cipher that processes fixed 128 bit data blocks using cipher keys with lengths of 128, 192 and 256 bits. The original Rijndael algorithm had the option of combining data block sizes of 128, 192 or 256 bits with any of key lengths. Due to the hard task of verifying that all possible combinations were secure against cryptographic attacks, only the block size of 128 bits data and key were included in the AES standard (NIST, 2002).

AES algorithm is an iterative algorithm, it consist of four mathematical operations-SubBytes(), ShiftRows(), MixColumns() and AddRoundKey().

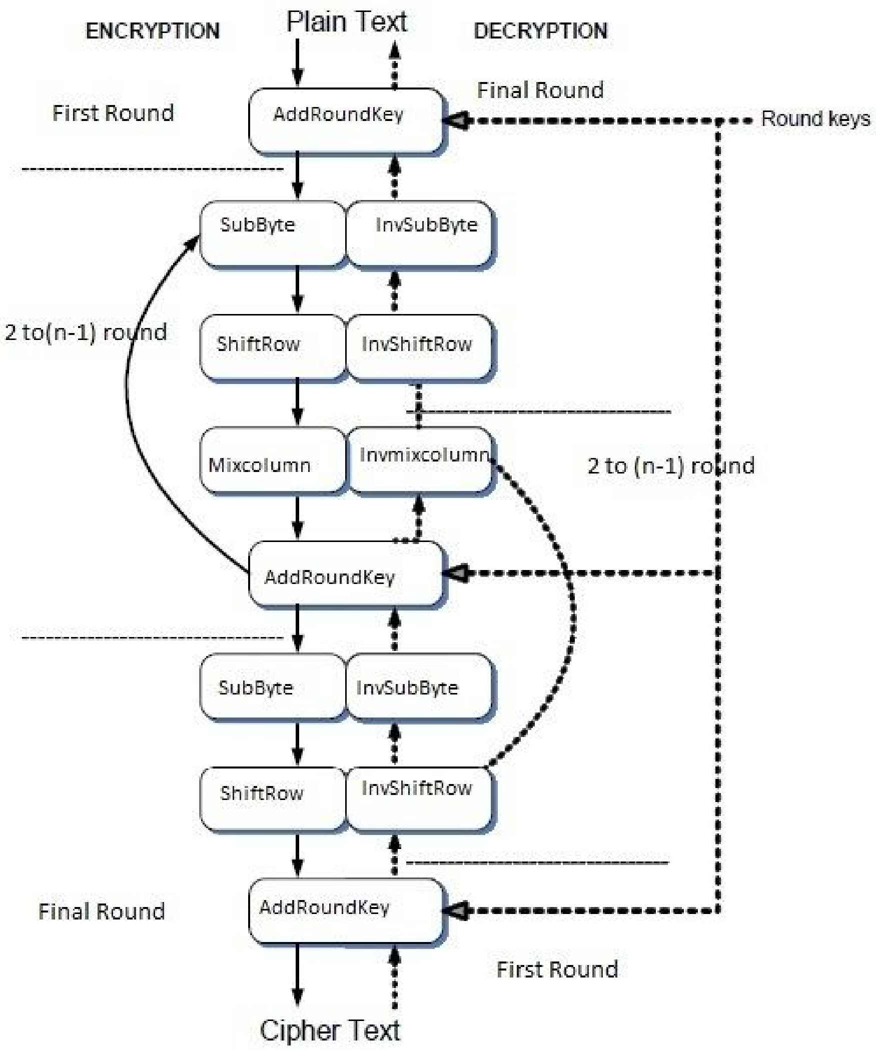


Fig.1. Flow Chart of AES Algorithm

SubBytes()

It is a non-linear substitution of bytes that operates independently on each byte of the State using a substitution table (S box). This S-box which is invertible is constructed by first taking the multiplicative inverse in the finite field GF (2^8) with irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. The element {00} is mapped to itself. Then affine transformation is applied (over GF (2)).

ShiftRows()

Cyclically shifts the rows of the State over different offsets. The operation is almost the same in the decryption process except for the fact that the shifting offsets have different values.

MixColumns()

This transformation operates on the State column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF (2^8) and multiplied by modulo $x^4 + 1$ with a fixed polynomial

$$a(x) = \{03\}\, x^3 + \{01\}\, x^2 + \{02\}\, x. \qquad (1)$$

AddRoundKey()

In this step XOR each byte of the round key with its corresponding byte in the state array [5].

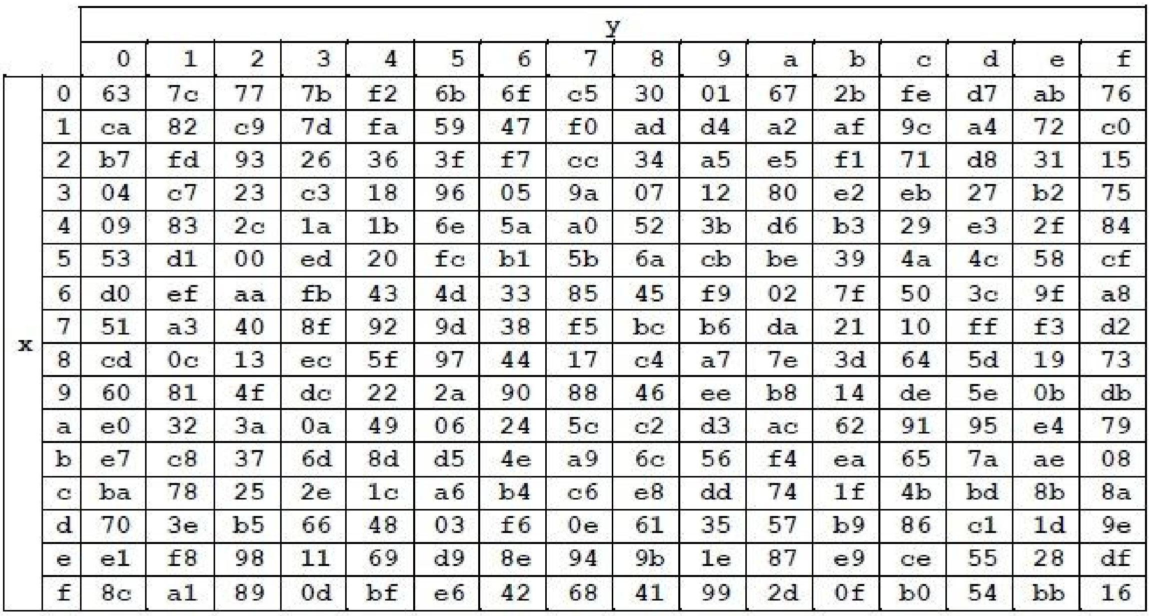
Proposed Work

An efficient implementation of the S-box is the main challenge for compact or high-speed hardware implementations of Rijndael. S-Box is the important component of AES. The eight byte input is substituted by eight byte output using S-Box during SubByte transformation. The proposed system compares AES encryption with two different S-Boxes. S-box with 256 byte lookup table (Rijndael S-Box) and AES with 16 byte S-Box (Anubis S-Box) [2].

Anubis is another block cipher designed according to the Wide Trail design strategy. It is in many ways similar to Rijndael and its predecessor, Square. Similar to Rijndael and Square, Anubis encrypts blocks of 128 bits, which are internally represented as 16 bytes arranged in a 4-by-4 matrix. The round transformation of Anubis is composed of similar steps as in Rijndael and Square.

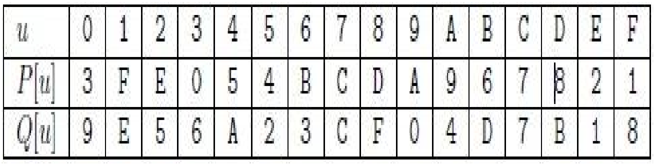
- The most important differences between Anubis and Rijndael are the following: The involutional structure: In Anubis, all steps are involutions. This implies that the implementation of the decryption operation can be the same as the encryption operation, except for a change in the key schedule. This should in principle reduce the code size or area in software, respectively hardware applications that implement both encryption and decryption.
- The different S-box: The S-box of Anubis is generated in a pseudo-random way. The advantage of this method is that providing a simple mathematical description seems more difficult. The polynomial expansion of the S-box is certainly more involved. The disadvantages are the suboptimal differential and linear properties, and possibly a more complex hardware implementation.
- A more complex key scheduling: The advantage is the improved resistance against key based attacks, in particular the shortcuts for long keys.

The disadvantage is the higher cost: slower execution, a reduced key agility, larger code or gate count. In the proposed work, we replace only the Rijndael S-box with Anubis S-box so the disadvantages of Anubis will not reflect in this work. While comparing AES with Rijndael S-box and AES with Anubis S-box , Modelsim simulator is used for the simulation. The result conveys that the performance of the proposed work has been improved. The 16 byte S-box uses less memory space compared with 256 byte S-box. It also reduces the hardware utilization and power consumption and reduces the execution time for encryption process



		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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. 2. Rijndael S-box(256 byte)



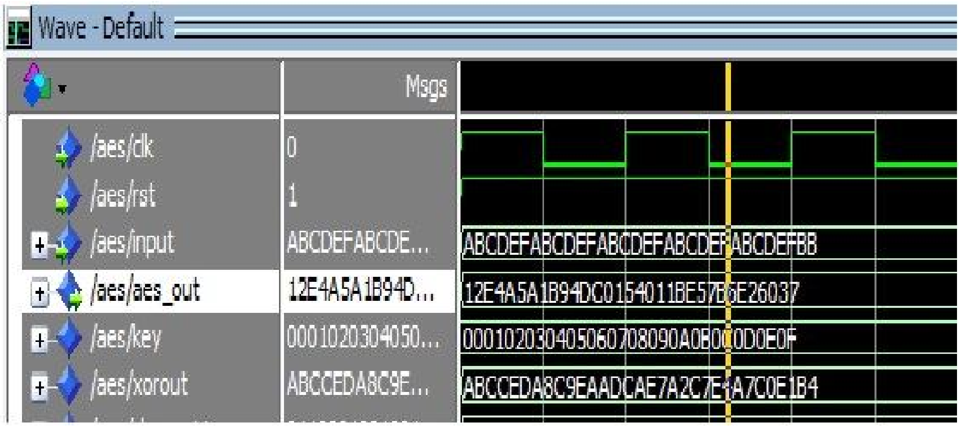
u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$P[u]$	3	F	E	0	5	4	B	C	D	A	9	6	7	8	2	1
$Q[u]$	9	E	5	6	A	2	3	C	F	0	4	D	7	B	1	8

Fig. 3. AnuBis S-box(16 byte)

From the lookup table of Anubis, element u represent input byte. In AES with Anubis S-box, during SubByte transformation, the first four bit of input byte(represented by u) is substituted by corresponding p[u] and last four bits(represented by u) is substituted by corresponding Q[u].

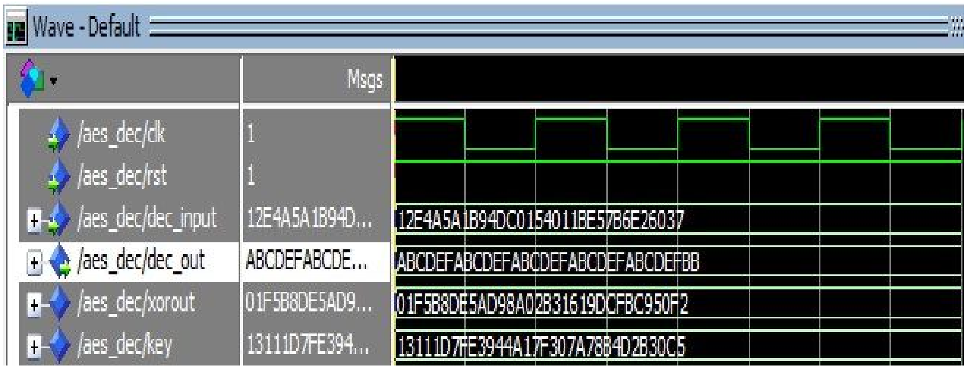
Simulation Results

Optimized and synthesized VHDL code is used for AES encryption. Xilinx ISE 13.2i software is used for VHDL code implementation and Modelsim simulator is used for the simulation. As input 128 bit data was given and a 128 bit key was given. In this, AES encryption and decryption using Rijndael S-box and AES encryption using Anubis S-box are implemented. The following was the simulation results produced.



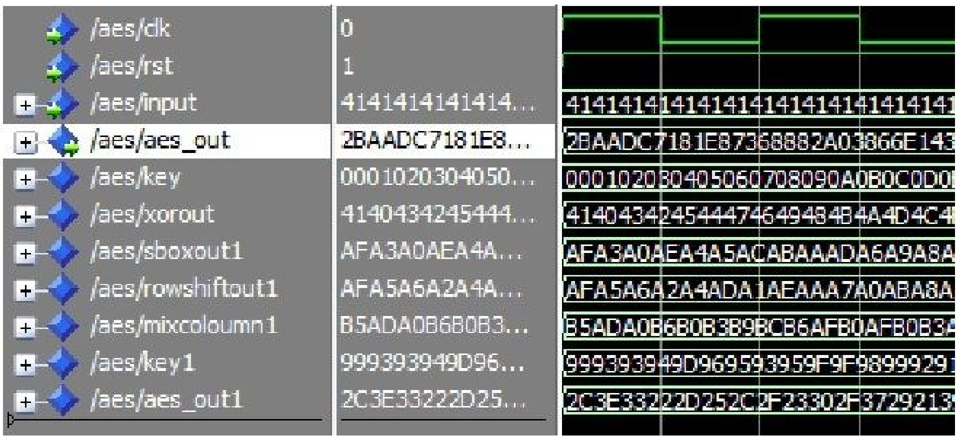
```
Wave - Default
                       Msgs
/aes/clk               0
/aes/rst               1
/aes/input             ABCDEFABCDE...      ABCDEFABCDEFABCDEFABCDEFABCDEFBB
/aes/aes_out           12E4A5A1B94D...     12E4A5A1B94DC0154011BE57B6E26037
/aes/key               0001020304050...    000102030405060708090A0B0C0D0E0F
/aes/xorout            ABCCEDA8C9E...      ABCCEDA8C9EAADCAE7A2C7E4A7C0E1B4
```

Fig. 4 Simulation result of AES-128 Encryption (Using Rijndael S-Box)



```
Wave - Default
                       Msgs
/aes_dec/clk           1
/aes_dec/rst           1
/aes_dec/dec_input     12E4A5A1B94D...     12E4A5A1B94DC0154011BE57B6E26037
/aes_dec/dec_out       ABCDEFABCDE...      ABCDEFABCDEFABCDEFABCDEFABCDEFBB
/aes_dec/xorout        01F5B8DE5AD9...     01F5B8DE5AD98A02B31619DCFBC950F2
/aes_dec/key           13111D7FE394...     13111D7FE3944A17F307A78B4D2B30C5
```

Fig. 5 Simulation result of AES-128 Decryption (Using Rijndael S-Box)



```
/aes/clk               0
/aes/rst               1
/aes/input             414141414141 4...   4141414141414141414141414141414
/aes/aes_out           2BAADC7181E8...     2BAADC7181E87368882A03866E143
/aes/key               000102030405 0...   000102030405060708090A0B0C0D0E
/aes/xorout            414043424544 4...   414043424544474649484B4A4D4C4
/aes/sboxout1          AFA3A0AEA4A...      AFA3A0AEA4A5ACABAAADA6A9A8A
/aes/rowshiftout1      AFA5A6A2A4A...      AFA5A6A2A4ADA1AEAAA7A0ABA8A
/aes/mixcoloumn1       B5ADA0B6B0B3...     B5ADA0B6B0B3B9BCB6AFB0AFB0B3A
/aes/key1              999393949D96...     999393949D969593959F9F9899929
/aes/aes_out1          2C3E33222D25...     2C3E33222D252C2F23302F3729213
```

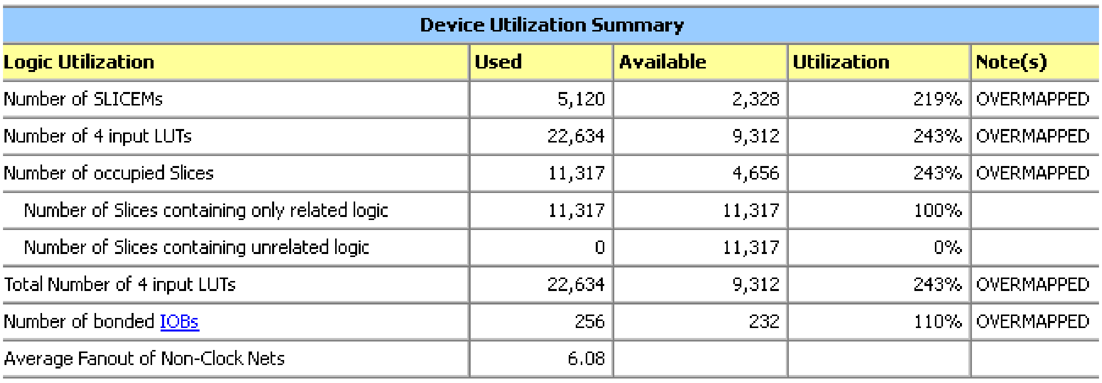
Fig. 6 Simulation result of AES-128 Encryption (Using AnuBis S-box)

Performance Evaluation

In this article, comparison of AES encryption with two different S-Boxes is done. S-box with 256 byte lookup table (Rijndael S-Box) and AES with 16 byte S-Box (Anubis S-Box). Device utilization summary of both S-boxes are shown below and from that, several facts are inferred which reveals the benefits of Anubis S-box. All our implementations were carried out on a XILINX Spartan-3E XC3S500E-4FG320 FPGA.

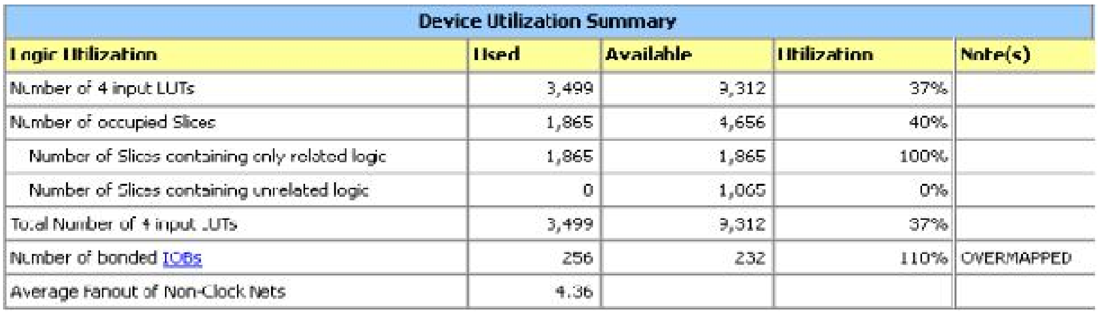
The device utilization summary of AES encryption using different S-boxes is shown below. Here "overmapped" represent extra hardware (devices) are need for the implementation of AES algorithm.

Table 1. Device utilization summary of AES with 256 byte S-Box



Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of SLICEMs	5,120	2,328	219%	OVERMAPPED
Number of 4 input LUTs	22,634	9,312	243%	OVERMAPPED
Number of occupied Slices	11,317	4,656	243%	OVERMAPPED
Number of Slices containing only related logic	11,317	11,317	100%	
Number of Slices containing unrelated logic	0	11,317	0%	
Total Number of 4 input LUTs	22,634	9,312	243%	OVERMAPPED
Number of bonded IOBs	256	232	110%	OVERMAPPED
Average Fanout of Non-Clock Nets	6.08			

Table 2. Device utilization summary of AES with 16 byte S-Box



Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of 4 input LUTs	3,499	9,312	37%	
Number of occupied Slices	1,865	4,656	40%	
Number of Slices containing only related logic	1,865	1,865	100%	
Number of Slices containing unrelated logic	0	1,865	0%	
Total Number of 4 input LUTs	3,499	9,312	37%	
Number of bonded IOBs	256	232	110%	OVERMAPPED
Average Fanout of Non-Clock Nets	4.36			

The 16 byte S-box uses less memory space compared with 256 byte S-box. It must be reduces the hardware utilization and power consumption. Also reduces the execution time for encryption process.

Conclusions

Rijndael is the fastest and most efficient algorithm. Considering the disadvantages of Rijndael S-Box, it is replaced by Anubis S-box. The performances of both the systems are compared (AES encryption using both S-boxes). From the observations, we can infer that using Anubis S-box result in usage of less memory space, reduced hardware utilization, reduced power consumption and it also reduces the execution time for encryption process.

In this work, implementation of AES encryption using both S-boxes is done and AES decryption using Anubis S-box is done. The simulation proves that it can be implemented in Spartan3E XC3S500E-4FG320 FPGA. As future work, AES decryption using Anubis S-box can be done. AES encryption and decryption can be implemented in an FPGA device.

Acknowledgement

The authors would like to thank the management, and Faculty Members, of Department of Electrical and Electronics Engineering, TKM College of Engineering, Kollam, for many insightful discussions and the facilities extended to us for completing the task.

The authors would like to thank the management, and Faculty Members, of Department of Electrical and Electronics Engineering, TKM College of Engineering, Kollam, for many insightful discussions and the facilities extended to us for completing the task.

References

[1] L.Thulasimani" A Single chip Design and Implementation of AES-128/192/256 Encryption Algorithms" International Journal of Engineering Science and Technology Vol. 2(5), 1052-1059, 2010.

[2] Joan Daemen, Paulo S.L.M. Barreto and Vincent Rijmen, "Rijndael: beyond the AES," Mikul´aˇssk´a kryptobes´ıdka, 2002.

[3] J. Daemen, V.Rijmen,"The Rijndael Block Cipher: AES Proposal", First AES Candidate Conference (AES1) : August 20-22, 1998

[4] William Stallings"Cryptography and network security", Third edition.pearson education.

[5] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" Federal Information Processing Standards Publication 197 November26, 2001.

[6] A.J. Elbirt, W. Yip, B. Chetwynd, C. Paar" An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists" The Third Advanced Encryption Standard (AES3) Candidate Conference, 13-14 April 2000, New York, USA.

Author's Biography

Prof. Abdul Jaleel. J received the Bachelor degree in Electrical Engineering from University of Kerala, India in 1994. He received the M.Tech degree in Energetics from Regional Engineering College Calicut, Kerala, India in 2002, and PhD from WIU, USA in 2006.He joined the EEE department of TKM College of Engineering as faculty member in 1990. He was with Saudi Aramco in 1996 to 1998 and worked in the field of power generation, transmission, distribution and instrumentation in the Oil and Gas sector of Saudi Arabia. He was with Water Supply department of Sultanate of Oman in 1985 to 1986 and worked with the maintenance of Submersible bore-well pumps and power supplies. He was with Saudi Electricity Company in 1979 to 1985 and worked in the Generation, Transmission and distribution fields. He worked with project management, Quality Management and he is a certified Value Engineer and Auditor for QMS. He is a consultant for Oztern_Microsoft, Technopark, Kerala and Consultant for Educational Projects of KISAT and MARK Research and Education Foundation.Currently he is a P.G. Coordinator of M. Tech Programme in the TKM College of Engineering under University of Kerala and Director of Kerala Institute of Science and Technology. His areas of interest are power system Control and optimization, power system reliability, voltage stability, computer aided design and analysis.

Anu Assis received the Bachelor degree in Electronics & Communication Engineering from the University of Calicut in 1998.She received the M.Tech degree in Microelectronics and VLSI Design from National Institute of Technology, Calicut, Kerala, India in 2009.She joined the department of Electronics & Communication Engineering of TKM College of Engineering under University of Kerala as a faculty member in 2002.Her main areas of interest are Nanoelectronics and Analog Circuit Design.

Sherla A received B. Tech Degree in Electrical and Electronics Engineering from Younus College of Engineering and Technology, Kollam, India. Currently she is pursuing M.Tech in Industrial Instrumentation and Control at Thangal Kunju Musaliar College of Engineering, Kollam, India.