Comparison of Power Consumption and Strict Avalanche Criteria at Encryption/Decryption Side of Different AES Standards

Navraj Khatri [1], Rajeev Dhanda [2], Jagtar Singh [3]

[1] [2] Department of Electronics and Communication Engineering, NCCE, Israna, Panipat, INDIA

[3] Senior Lecturer, Electronics and Communication engineering, NCCE, Israna, Panipat, INDIA

Abstract:

The selective application of technological and related procedural safeguards is an important responsibility of every organization in providing adequate security to its electronic data systems. Now as the world is moving towards high speed of communication (larger data rate),more secure and fast algorithms are required to keep the information secret. In the present work, a new model is proposed and implemented, which is very similar to the conventional AES. The fundamental difference in the AES and proposed model is in block size which has been increased from 128 bits in conventional AES to 200 bits in proposed algorithm[1-4].The proposed algorithm is giving very good randomness and hence enhances the security in comparison to conventional AES. The performance is measured based upon Power Consumption at Encryption/Decryption time, and Strict Avalanche Criteria of various AES Standards. In this paper, we showed the effect in security increment through AES methodology.

Keywords: Plain text, cipher text, stream cipher, Symmetric Encryption, Computer Security.

1. Introduction:

The introduction of wireless data communication at the beginning of 20th century resulted in an increasing interest in cryptography due to insecure nature of Wireless medium.In this paper,symmetric block cipher algorithm is proposed likewise Advance Encryption Standard (AES).The proposed algorithm differs from AES as it has 200 bits block size and key size both. Number of rounds is constant and equal to ten in this algorithm.The key expansion and substitution box generation are done in the same way as in conventional AES block cipher.AES has 10 rounds for 128-bit keys,12 rounds for 192-bit keys, and 14 rounds for 256-bit keys[5].Section 2 describes the Our Proposed Algorithm properly.Section 3 gives the Comparison of Power Consumption at Encryption and Decryption side and Strict Avalanche Criteria of different AES Standards. Section 4 gives the Advantages and Disadvantages of AES.Section 5 and Section 6 gives us the Conclusion and Acknowledgement..

2. Proposed Algorithm

2.1 General Definitions

Block size and key size are the important parameters of any encryption algorithm because the level of security provided by a cipher completely depends upon these two parameters.In our proposed encryption algorithm,we are using 200 bits block and key size instead of 128 bit used in conventional Rijndael'salgorithm.[6-8].This increased block and key size will improve the security level of the cipher with a negligible loss in efficiency.The original data which needs to be encrypted will be termed as plaintext.Our encryption algorithm is a symmetric block cipher algorithm.This algorithm will operate on fixed size blocks of plaintext to generate ciphertext.In the process of encryption, the first step is formation of data blocks from the original plaintext.Our basic block length is 200 bits which can be shown by a 5 by 5 matrix of byte. The data bytes are filled first in the column then in the rows.Once the data block is formed, different rounds take place to modify data to the cipher text.

$$\begin{vmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & a_{0,4} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,0} & a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{vmatrix}$$

Figure 1. Making of data block from stream

2.2 The Round Transformation

There are ten rounds, and in each of the round there are series of transformations takes place except the final round.A pseudo algorithm for each of the common round is given below and later the final round transformation algorithm is given.The state is referred as the output of the previous transformation. Each function in the round is explained later.The final round is equal to others when mix-column transformation is removed from general one.

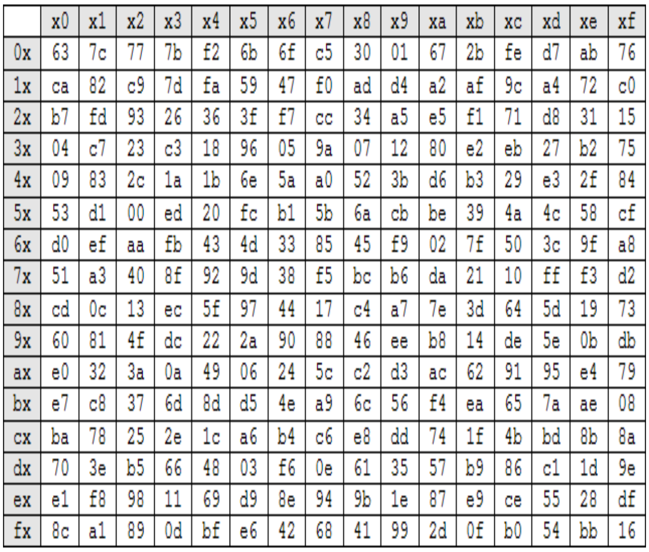
Algorithm 1: (For Common Rounds)
Round(state, Round Key)

```
{
ByteSub(state);
ShiftRow(state);
MixColumn(state);
AddRoundKey(state, Round Key);
}
Algorithm 2: (For Final Round)
FinalRound(state, Round Key)
{
ByteSub(state);
ShiftRow(state);
AddRoundKey(state, Round Key);
}
```

2.3 The Byte Sub Transform

The ByteSub transformation is a non linear byte substitution that acts on every byte of the state in isolation to produce a new byte value using an S-box substitution table.In this transformation, each of the byte in the state matrix is replaced with another byte as per the S-box (Substitution Box).The S-box is generated by calculating the respective reciprocal of that byte in GF (2^8) and then affine transform is applied.Similarly,Inverse S-Matrix can be formed during the decryption of the cipher text.For increasing the efficiency,we use Rijndael S-box.

Table 1. S-Box



	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

2.4 The Shift Row Transform

For encryption, the 1st row remain unchanged, 2nd row is shifted 1 byte to the left, 3rd is 2 byte to the left, 4th is 3 byte to the left and 5th row is shifted 4 byte to the left.For decryption the operation is similar to that for encryption but in reverse direction.

2.5 The Mix Column Transform

$$\begin{vmatrix} 02 & 04 & 03 & 01 & 01 \\ 01 & 02 & 04 & 03 & 01 \\ 01 & 01 & 02 & 04 & 03 \\ 03 & 01 & 01 & 02 & 04 \\ 04 & 03 & 01 & 01 & 02 \end{vmatrix} \qquad \begin{vmatrix} E0 & 7D & 09 & 8A & 4C \\ 4C & E0 & 7D & 09 & 8A \\ 8A & 4C & E0 & 7D & 09 \\ 09 & 8A & 4C & E0 & 7D \\ 7D & 09 & 8A & 4C & E0 \end{vmatrix}$$

(a) (b)

Figure 2. (a) Polynomial Matrix (b) Inverse Polynomial Matrix for Mix column transformation.

This is a complex procedure as it involves severely the byte multiplication under GF (2^8). The whole state is to be multiplied with pre-defined matrix called polynomial matrix. It completely changes the scenario of the cipher even if the all bytes look very similar. The Inverse Polynomial Matrix does exist in order to reverse the mix column transformation. Each Column is replaced by the multiplicative value such as b(x)=c(x)*a(x), where, '*' refers to multiplication under GF (2^8).

2.6 The AddRoundKey Transform

During this, the round key is simply bitwise XORed with the state came from above.The round keys are generated similarly as in the Rijndael Algorithm of 128 bits.To inverse this state, one need to again XOR the Round Key in the state.

2.7 Key Schedule

The Round Keys are derived from the Cipher Key by means of the key schedule.This consists of two components: the Key Expansion and the Round Key Selection.The basic principle is the following.

●The total number of Round Key bits is equal to the block length multiplied by the number of rounds plus 1.

●The Cipher Key is expanded into an Expanded Key.

3. Experiment and Result

3.1 Power Consumed

The consumed power during any encryption and decryption is also one of the parameter to check their hardware efficiency. And hence, the consumed power is calculated for all mentioned algorithms in the following manner:

$$P_c = N_c . V_i . I_{avg}$$

Where, P_c represents consumed power, N_c denotes number of CPU cycles consumed during process, V_i denotes the input voltage for processor,equal to 3.3V and I_{avg}represents the average current drawn at processor per cycle which is approximately 48 Na.

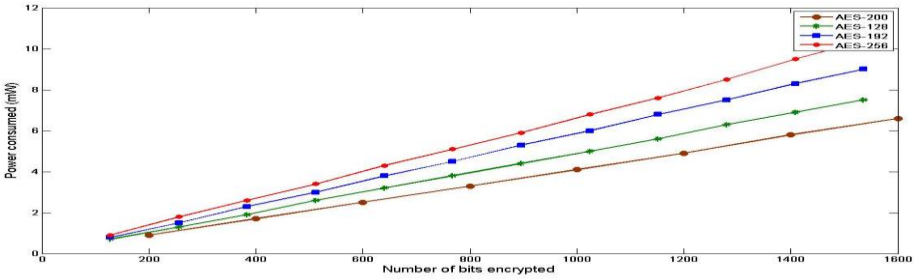


Figure 3. Comparison of power Consumption at encryption side

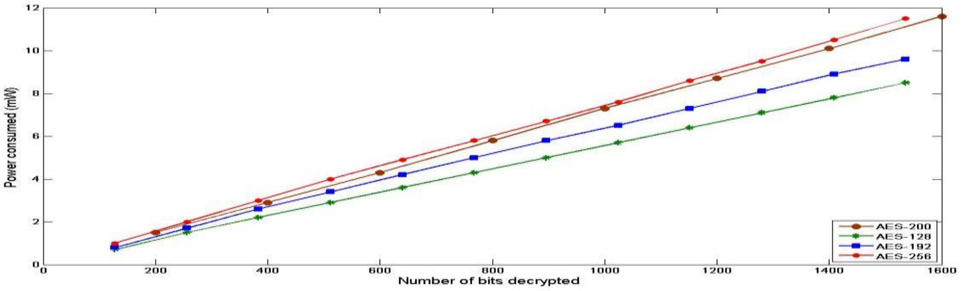


Figure 4. Comparison of power Consumption at decryption side

Since the consumed power directly depends on the number of CPU cycles taken for the process, so power during encryption and decryption is proportional to the CPU cycles, and varies in accordance. From the graph, it is observed that number of CPU cycles taken to encrypt the block is up to 30% lesser than other conventional algorithms.However, number of CPU cycles needed during decryption is higher and above 20% from the conventional AES algorithms.

3.2 Strict Avalanche Criteria

The strict avalanche criterion (SAC) is a generalization of the avalanche effect. It is satisfied if, whenever a single input bit is complemented, each of the output bits changes with a 50% probability [18]. The SAC builds on the concepts of completeness and avalanche.

$$K_{SAC}(i,j) = \frac{1}{2^n} W\left(a_j^{ei}\right) = \frac{1}{2}$$

where, $K_{SAC}(i,j)$can take values in the range [0,1], it should be interpreted as the probability of change of the jth output bit when the ith bit in the input string is changed.

$W\left(a_j^{ei}\right)$ is input word to the system and here less than 256 always.

The Security of the proposed model is examined by performing the test: Strict Avalanche Criterion and Bit Independence Criterion. SAC tells about the probability of the bit change while the BIC states the correlation that output bit possess. Both of the criteria are analyzed and the proposed algorithm falls within the desired level of security.

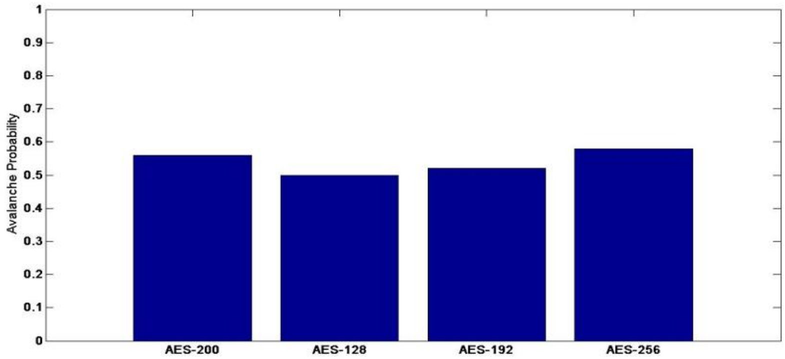


Fig Figure 5. Avalanche probability for various algorithms

From the plot, it can be seen that probability to get a bit changed for a highly correlated input, in proposed work, is very similar to the conventional AES, which results this in a secure algorithm and validates it to be used in communication.

4. Advantages and Disadvantages

Advantages

- Resistance against all known attacks.
- Speed and code compactness on a wide range of platforms.
- Design simplicity.
- Our proposed algorithm can be implemented to run at speeds unusually fast for a block cipher on a Pentium (Pro).There is a trade-off between table size / performance.
- The round transformation is parallel by design, an important advantage in future processors and dedicated hardware.

Limitations

- The inverse cipher is less suited to be implemented on a smart card than the cipher itself: it takes more code and cycles.
- In software, the cipher and its inverse make use of different code and/or tables.
- In hardware, the inverse cipher can only partially re-use the circuitry that implements the cipher.

5. Conclusion

The announcement of AES attracted concentration of cryptanalysts to measure its level of security.As mentioned earlier, there is always a trade-off between the security and performance of wireless network. AES provides a very high level of security in an efficient way, but it also has some flaws in terms of security and the performance[11-14].The improvement AES must possess similar level of security as in conventional AES.The proposed model has bigger block size which is 200 bits rather than conventional 128 bits. Also, the block is made by 5 rows and 5 columns unlike the AES's 4 rows and 4 columns.As the size of the matrix has increased, all the transformations of the AES don't need to change except the mixcolumn transformation. During mixcolumn transformation, the diffusion takes place in form of matrix multiplication under finite field. Having a bigger block, hence, requires a new matrix of size 5 X 5, to enable matrix multiplication.Here number of CPU cycles taken to encrypt the block is up to 30% lesser than other conventional algorithms.However, number of CPU cycles needed during decryption is higher and above 20% from the conventional AES algorithms.Hence, it can be said that the proposed model is secure and can be considered for communication where high data rate is required[20-24].

6. Acknowledgement

I proudly acknowledge my sincere and heartfelt thanks to Mr. Jagtar Singh, Senior Lecturer, N.C College of Engineering, Panipat for their valuable and sustained guidance, constant encouragement and careful supervision during the entire course which made the project successful.I would like to express my immense thanks to my friend Mr. Rajeev Dhanda,Associate Professor,ECE Dept,RVIT,U.P for providing me all the help to pursue my dessirtation to its successful accomplishment.

Reference:

[1] C.Shannon,Communication theory of secrecy systems,Bell Systems Technical Journal,vol.28,1949.

[2] Schneier B. and Whiting D.,Performance Comparison of AES Finalist,2000.

[3] ”National Policy on the Use of the AES to Protect National Security Systems and National Security Information”,Lynn Hathnway(June 2003),Retrieved 2011-02-15.

[4] ”Performance Comparison of the AES submissions”,1999-02-01.Retrieved 2010-12-28.

[5] ”An Efficient Approach For Increasing Security to Symmetric Data Encryption”,International Journal of Computer Science and Network Security,Vol.8 No.4,April,2008.

[6] J.Daemen and V.Raemen,The Design of Rijndael:AES-The Advanced Encryption Standards.Springer-Verlag,2002.

[7] J. Daemen, V. Rijmen, The block cipher Rijindael, Proceedings of the Third International Conference on smart card Research and Applications, CARDIS’98, Lecture Notes in computer Science, vol.1820, Springer, Berlin, 2000, pp.277_284.

[8] Federal Information Processing Standards Publications (FIPS 197), Advanced Encryption Standard (AES) ,26 Nov. 2001.

[9] Shivkumar S, Umamaheswari G., Performance Comparison of Advanced Encryption Standard(AES) and AES key dependent S-box - Simulation using MATLAB, International Journal of Computer Theory , 2011.

[10] Fahmy A., Shaarawy M., El-Hadad K., Salama G. and Hassanain K., A Proposal For A Key-Dependent AES, SETIT, Tunisia, 2005.

[11] Schneier B., Applied Cryptography: Protocols, Algorithms and Source Code in *C.* John Wiley and Sons, 1996.

[12] Stallings W., Cryptography and Network Security, Third Edition, Pearson Education, 2003.

[13] Anne Canteaut, Ongoing Research Areas in Symmetric Cryptography, 1999.

[14] Heys H. M., A Tutorial on Linear and Differential Cryptanalysis, St. John’s, NF, Canada, 2008.

[15] Chandrashekharan, J., et al. A chao Based Approach for Improving Non-linearity in the S-box Design of Symmetric Key Cryptosystem, Advances in Networks and communication, First International Conference on Computer Science and Information Technology (CSIT), Springer Bangalore, p. 516, ISBN- 978-3-642-17877-1, India, 2011.

[16] Nyberg K., Perfect Nonlinear S-boxes, Advances in Cryptography, Brioghtenpp 378-386, 1991.

[17] IBM Corporation MARS, A Candidate of AES cipher, http://www.research.ibm.com/security/mars.html, 1999.

[18] Burwick, C., Coppersmith, D., D.Avignon, E., Gennaro, R., Halevi, S., Jutla, C., Matyas,S., O.Connor, L., Peyravian, M., Safford, D., Zunic, N.: MARS- a candidate cipher for AES. Proceedings of the First AES Conference (1999). Revised September 22, 1999.

[19] Parker G. M., Generalised S-Box Nonlinearity, SBoxLin.tex, 11.02.03, IST -1999-12324, 2003.

[20] Keliher, L., Substitution permutation network cryptosystem using S-boxes.

[21] Stoianov N., One Software Tool for Testing Square S-boxes, Technical University of Sofia (TUS), Bulgaria 2008.

[22] Ahmed N., Testing an S-Box for Cryptographic Use, International Journal of Computer and Electrical Engineering.

[23] Adams, C. M.: Designing S-Boxes For Ciphers Resistant To Differential Cryptanalysis (Extended Abstract), Feb 2010.

[24] M. Dawson, S. Tavares, An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential-like Attacks, Advances in Cryptology, Springer-Verlag, 1991.